Cisco UCS Manager VM-FEX for Hyper-V GUI Configuration Guide, Release 4.0

First Published: 2018-08-14

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
     800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

Introduction

Overview of Virtualization

Virtualization allows you to create multiple Virtual Machines (VMs) to run in isolation, side by side on the same physical machine.

Each virtual machine has its own set of virtual hardware (RAM, CPU, NIC) upon which an operating system and fully configured applications are loaded. The operating system sees a consistent, normalized set of hardware regardless of the actual physical hardware components.

In a virtual machine, both hardware and software are encapsulated in a single file for rapid provisioning and moving between physical servers. You can move a virtual machine, within seconds, from one physical server to another for zero-downtime maintenance and continuous workload consolidation.

The virtual hardware makes it possible for many servers, each running in an independent virtual machine, to run on a single physical server. The advantages of virtualization include better use of computing resources, greater server density, and seamless server migration.

Overview of Cisco Virtual Machine Fabric Extender

A virtualized server implementation consists of one or more VMs that run as guests on a single physical server. The guest VMs are hosted and managed by a software layer called the hypervisor or virtual machine manager (VMM). Typically, the hypervisor presents a virtual network interface to each VM and performs Layer 2 switching of traffic from a VM to other local VMs or to another interface to the external network.

Working with a Cisco virtual interface card (VIC) adapter, the Cisco Virtual Machine Fabric Extender (VM-FEX) bypasses software-based switching of VM traffic by the hypervisor for external hardware-based switching in the fabric interconnect. This method reduces the load on the server CPU, provides faster switching, and enables you to apply a rich set of network management features to local and remote traffic.

VM-FEX extends the IEEE 802.1Qbh port extender architecture to the VMs by providing each VM interface with a virtual Peripheral Component Interconnect Express (PCIe) device and a virtual port on a switch. This solution allows precise rate limiting and quality of service (QoS) guarantees on the VM interface.

Important   In Cisco UCS Manager Release 4.0(1), VM-FEX is not supported with Cisco UCS 6454 Fabric Interconnects.

Virtualization with a Virtual Interface Card Adapter

A Cisco VIC adapter is a converged network adapter (CNA) that is designed for both bare metal and VM-based deployments. The VIC adapter supports static or dynamic virtualized interfaces, which includes up to 116 virtual network interface cards (vNICs).

There are two types of vNICs used with the VIC adapter—static and dynamic. A static vNIC is a device that is visible to the OS or hypervisor. Dynamic vNICs are used for VM-FEX by which a VM is connected to a veth port on the Fabric Interconnect.

VIC adapters support VM-FEX to provide hardware-based switching of traffic to and from virtual machine interfaces.

Single Root I/O Virtualization

Single Root I/O Virtualization (SR-IOV) allows multiple VMs running a variety of guest operating systems to share a single PCIe network adapter within a host server. SR-IOV allows a VM to move data directly to and from the network adapter, bypassing the hypervisor for increased network throughput and lower server CPU burden. Recent x86 server processors include chipset enhancements, such as Intel VT-x technology, that facilitate direct memory transfers and other operations required by SR-IOV.

The SR-IOV specification defines two device types:

- Physical Function (PF)—Essentially a static vNIC, a PF is a full PCIe device that includes SR-IOV capabilities. PFs are discovered, managed, and configured as normal PCIe devices. A single PF can provide management and configuration for a set of virtual functions (VFs).

- Virtual Function (VF)—Similar to a dynamic vNIC, a VF is a full or lightweight virtual PCIe device that provides at least the necessary resources for data movements. A VF is not managed directly but is derived from and managed through a PF. One or more VFs can be assigned to a VM.

SR-IOV is defined and maintained by the Peripheral Component Interconnect Special Interest Group (PCI-SIG), an industry organization that is chartered to develop and manage the PCI standard. For more information about SR-IOV, see the following URL:

https://www.intel.com/content/www/us/en/pci-express/pci-sig-sr-iov-primer-sr-iov-technology-paper.html

The Microsoft Hyper-V hypervisor supports SR-IOV.

The following Cisco Virtual Interface Cards support SR-IOV with VM-FEX:

- Cisco UCS Virtual Interface Card 1240

- Cisco UCS Virtual Interface Card 1280

• Cisco UCS Virtual Interface Card 1225

• Cisco UCS Virtual Interface Card 1225T

• Cisco UCS Virtual Interface Card 1227

• Cisco UCS Virtual Interface Card 1227T

• Cisco UCS Virtual Interface Card 1340

• Cisco UCS Virtual Interface Card 1380

• Cisco UCS Virtual Interface Card 1385

• Cisco UCS Virtual Interface Card 1387

VM-FEX for Hyper-V

Overview of the Cisco UCS VM-FEX with Microsoft SCVMM Architecture

Cisco UCS Manager (UCSM) and Microsoft System Center Virtual Machine Manager (SCVMM) integration extends the Virtual Machine Fabric Extender (VM-FEX) technology to the Microsoft virtualization platform. The architecture allows Cisco UCSM to configure the networking objects that Microsoft SCVMM uses to set up its networking stacks. Microsoft SCVMM uses the networking objects that are created by Cisco UCSM and deploys them on the Microsoft Hyper-V host that hosts the VMs.

The Hyper-V uses Single Root I/O Virtualization (SR-IOV) technology to deploy virtual connections. The VM's interface gets mapped to the virtual function. The SR-IOV support was added to Cisco UCS Release 2.1 to allow the deployment of VM-FEX in Microsoft Hyper-V hosts, but it lacked a centralized VM network management. Release supports the management plane integration with Microsoft SCVMM and provides a centralized VM network management for the Hyper-V hosts. The deployment leverages the SR-IOV technology that is available on the Cisco virtual interface card (VIC) adapters and enables Cisco UCS fabric interconnects (FIs) to be VM aware.

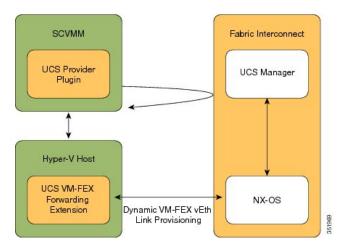Figure 1 shows the Cisco UCS VM-FEX with Microsoft SCVMM architecture.

Figure 1: Cisco UCS VM-FEX with Microsoft SCVMM Architecture

Cisco UCSM

Cisco UCSM deploys the service profiles and provisions the baremetal as part of the service profile deployment. While configuring the service profile network settings for the Hyper-V hosts, the administrators have to make sure that the SR-IOV support is enabled. The network administrator defines the networking objects, for example, the VLANs and the port profiles in Cisco UCSM. These objects get pushed to Cisco NX-OS in the fabric interconnect (FI). The server administrator installs the Cisco UCS provider plugin on Microsoft SCVMM.

Microsoft SCVMM

The Cisco UCS provider plugin enables Microsoft SCVMM to pull the networking objects from Cisco UCSM, use them natively, and deploy them on the Hyper-V hosts. The hosts that are being added to the host groups are the same servers that Cisco UCSM has deployed using the service profiles. It also pulls the network configuration that is specified in Cisco UCSM and pushes it to the Hyper-V host. When you deploy a Logical Switch on the Hyper-V host, the driver extension gets pushed to the host.

The Cisco UCS VM-FEX forwarding extension is a driver extension that is situated on the Hyper-V host. It ensures that the packets are forwarded to the fabric interconnect (FI) and the switching occurs in the FI. The FI is aware of all the MAC addresses of the VMs. The VM-FEX forwarding extension driver gets the configuration from Microsoft SCVMM and instructs Cisco NX-OS to provision a virtual Ethernet interface for virtual NICs (vNICs) that come up on the host.

Dynamic VM-FEX vEth Link Provisioning connects the Hyper-v host and Cisco NX-OS. When a VM is online or when you power on a VM, its network card sends a VIC attach using the Cisco VIC protocol and it gets dynamically connected to the FI.

Hyper-V Host

Microsoft Hyper-V is a virtualization package for Windows Server 2012 and later releases on an x86-64 hardware platform. Hyper-V uses x86 hardware virtualization extensions (for example, Intel VT-x) to implement a hypervisor that hosts VMs as userspace processes.

With VM-FEX for Hyper-V, the hypervisor performs no switching of VM traffic. Working with an installed VIC adapter, the hypervisor acts as an interface virtualizer, and performs the following functions:

- For traffic going from a VM to the VIC, the interface virtualizer identifies the source vNIC so that the VIC can explicitly tag each of the packets generated by that vNIC.

- For traffic received from the VIC, the interface virtualizer directs the packet to the specified vNIC.

All switching is performed by the external fabric interconnect, which can switch not only between the physical ports, but also between the virtual interfaces (VIFs) that correspond to the vNICs on the VMs.

VM-FEX for Hyper-V Support in Cisco UCS Manager 4.0

In Cisco UCS Manager Release 4.0(1), VM-FEX for Hyper-V, on 2012R2, is supported with Cisco UCS VIC 12xx and VIC 13xx adapters. Single Root I/O Virtualization, on page 2 details the supported VIC adapters.

In Cisco UCS Manager Release 4.0(1), VM-FEX for Hyper-V, on 2012R2, is not supported with Cisco UCS VIC 14xx adapters.

Networking Terminology

Refer to the following Microsoft networking terminology for more information on the networking objects.

Logical Switch

A logical switch is the native distributed virtual switch (DVS) by Microsoft. It is a template that you can use to instantiate a virtual switch from. You can define a native switch and attach an extension to it. It is known as a switch extension.

Fabric Network

A fabric network is a logical network that has network segments (VLANs) that span across multiple sites. A fabric network can have one or more network sites.

Network Site

A network site includes site-specific network segments. It is also known as a fabric network definition (FND). A network site can have one or more network segments.

Network Segment

A network segment is also known as a VM Network Definition (VMND). It consists of a VLAN and an IP pool.

VM Network

A VM network references a network segment. It is used by the tenant as a network that the network tenants can attach their VMs to. It is the tenant's view of the network.

Virtual Port Profile

A virtual port profile is a profile that defines the quality of service (QoS)/service level agreement (SLA) for a vNIC.

Uplink Port Profile

An uplink port profile carries a list of allowed network segments for a physical network interface card (PNIC).

Reference

For more information on the networking objects, see **Configuring Logical Networking in VMM Overview** at http://technet.microsoft.com/en-us/library/jj721568.aspx.

Configuring Networking Objects in Cisco UCS Manager

Understanding the Cisco UCSM and Microsoft SCVMM Workflow

See the following steps for a complete workflow of Cisco UCSM with Microsoft SCVMM:

1. Configure the service profile network settings for the Hyper-V hosts.
2. Configure VLANs and IP pools.
3. Configure the fabric network sets, the fabric network, the network site, and the network segment.
4. Associate a VM network to the network segment.
5. Create a Microsoft SCVMM provider.
6. Create a logical switch.
7. Configure an uplink port profile (UPP).
8. Create a virtual port profile (VPP) (for example, port classification for Microsoft).
9. Create a port profile client for the virtual port profile (VPP) and choose the logical switch that was created under the Microsoft SCVMM provider.
10. Install the Cisco UCS provider plugin in SCVMM.

11. Create a Network Service instance on the provider. The provider fetches all the network definitions from Cisco UCSM. The users can schedule the polls for periodic updates.
12. Create a logical switch in SCVMM by checking the **Enable single root I/O virtualization (SR-IOV)** check box and adding Cisco UCSM's logical switch as an extension. Choose an appropriate uplink port profile and virtual port profile.
13. Create a VM network in SCVMM and choose the network segment from the drop-down list.
14. Attach the Hyper-V hosts to SCVMM.
15. Deploy the logical switch to the Hyper-V host.
16. Create a VM instance in SCVMM. Assign the VM NIC to a VM network and the port classification.
17. Power on the VM and load the eNIC driver on the VM. The eNIC driver now establishes a network link with the Cisco UCS fabric interconnect (FI). The FI enforces the port classification as per the assigned port profile properties.
18. Verify the VM vNICs in the Cisco UCSM GUI.

Configuring Service Profile Network Settings for Hyper-V Hosts

As a prerequisite for the Hyper-V host that you plan on using in the Cisco UCS cluster, configure the service profile network settings first. In the **Modify vNIC** window in the GUI, configure the dynamic vNIC connection policy on the static vNIC.

- In the **Adapter Performance Profile** panel, select an **SRIOV** adapter policy for static vNICs.

- In the **Connection Policies** panel, select **Dynamic vNIC** connection policy on one or more static vNICs that you plan on using.

- In the **Connection Policies** panel, click **Add** to create a dynamic vNIC connection policy. A new window opens.

- Select **windows** as the adapter policy for the dynamic vNIC.

- Specify the number of dynamic vNICs.
- Click **OK**.

After completing the steps outlined in this section, SR-IOV is enabled on the vNICs. For more information on configuring policies, see Configuring Policies, on page 27.

✎

Note The service profile for VM-FEX configuration must have at least 2 eNICs created on it, one for VM-FEX and another for communication with SCVMM. If there is just one eNIC on the service profile to implement SRIOV and talk to SCVMM, the configuration will not work when a logical switch is deployed on the eNIC.

Configuring a VLAN

For more information on creating VLANs, see the GUI configuration guide for the Cisco UCSM version that you are using.

Configuring an IP Pool

You can configure an IP pool by using the **VM** tab.

✎

Note   IP pools are used by Microsoft SCVMM; they are not used by Cisco UCSM.

Procedure

Step 1	In the **Navigation** pane, click **VM**.
Step 2	Expand **All** > **Fabric Network Sets**.
Step 3	Right-click **IP Pools** and choose the **Create IP Pool** option. The **Create IP Pool** window appears.
Step 4	In the **Define Name and Description** panel, enter the name of the IP pool.
Step 5	(Optional) Enter a description of the IP pool.
Step 6	In the **NetBios Mode** field, choose **Active** if you want to enable the NetBios mode for the IP pool or choose **Not-Active** if you do not want to enable the NetBios mode.
Step 7	In the **Supports DHCP** field, choose **Supported** if you want to get the DHCP IP address from the DHCP server or choose **Not-Supported** to get a static IP pool.
Step 8	Click **Next**.
Step 9	In the **Create IP Pool** window, choose **Add** to add a valid DNS suffix for the IP pool.
Step 10	Click **OK**.
Step 11	Click **Next**. The **IPV4 WINS Servers** window appears.
Step 12	In the IPV4 WINS Servers field, add a valid IP address for the WINS server.
Step 13	Click **Next**. The **Add IPV4 Blocks** window appears.
Step 14	Click **Add**. The **Create Block of IPV4 Addresses** window appears. **Note** Both IPv4 and IPv6 pools are supported but they cannot coexist at the same time. Multiple blocks of IP addresses are not supported.
Step 15	In the **From** field, enter a valid IP address.
Step 16	In the **Size** field, enter the size of the block.
Step 17	In the **Subnet Mask** field, enter a valid IP address.
Step 18	in the **Default Gateway** field, enter a valid IP address.
Step 19	Enter a valid IP address in the **Subnet Mask** field.
Step 20	(Optional) In the **Primary DNS** and **Secondary DNS** fields, enter valid IP addresses.
Step 21	In the **Add IPV4 Blocks** window, click **OK**.

Step 22   In the **Create a Block of IPV4 Addresses** window, click **Next**.

Step 23   Click **Finish**.

A Create IP Pool message window indicates that the IP pool has been successfully created.

Step 24   In the message window, click **OK**.

The configured IP pool is displayed in the Cisco UCSM GUI.

Configuring a Fabric Network

Configure a Fabric Network using the VM tab.

Procedure

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

Step 2   Expand **All** > **Fabric Network Sets**.

Step 3   In the left panel, right-click **Fabric Networks** then select **Create Fabric Network**.

The **Create Fabric Network** window appears.

Step 4   Enter the name of the fabric network.

Step 5   (Optional) Enter the description of the fabric network.

Step 6   Click **Next**.

Step 7   Click **Finish**.

Configuring a Network Site

You can configure a network site by using the **VM** tab.

Procedure

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

Step 2   Expand **All** > **Fabric Network Sets**.

Step 3   Right click **Fabric Networks**. In the **Network Sites** panel click **Add**. The **Add a Network Site** window appears.

Step 4   Enter the name of the network site in the **Name** field.

Step 5   (Optional) Enter the description of the network site in the **Description** field.

Step 6   In the **Network Segment** pane, click **Add** to associate network segments to the network sites.

You can configure many network segments under a network site. A network site can contain network segments with both regular and isolated VLANs. A network segment cannot have an isolated VLAN when another segment that belongs to the same network site contains an isolated VLAN.

Step 7   Click **OK**.

The network site is displayed in the Cisco UCSM GUI.

Configuring a Network Segment

You can configure a network segment in the **VM** tab.

Procedure

Step 1   In the **Create Fabric Network** window, click **Add** then select the **Network Segment** menu option.

The **Add a Network Segment** window displays.

Step 2   Enter the name of the network segment.

Step 3   (Optional) Enter the description of the network segment.

Step 4   Enter the number of maximum ports for the network segment.

Step 5   Add VLANs from the drop-down window to the network segment.

Only one VLAN and one IP pool can be selected for each network segment due to a constraint with Microsoft SCVMM.

Step 6   Select an IP Pool from the drop-down window for the network Segment.

Note   Modifying the IP Pool attribute on the network segment can have undesirable effects in SCVMM if the network segment is assigned to a Virtual Machine. Please ensure that this object is not used by the Virtual Machines, including the powered-off Virtual Machines, before modifying this object.

Step 7   Click **OK**.

Associating a VM Network to a Network Segment

You can associate a VM Network to a network segment by using the VM tab.

Procedure

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

Step 2   Expand the **All** node.

Step 3   Right-click **VM Networks** and select the **Create Virtual Network** option.

The **Create Virtual Network** window appears.

Step 4   In the **Name** field, enter the name of the virtual network.

Step 5   (Optional) In the **Description** field, enter the description of the VM network.

Step 6   Select the fabric network that contains the network segment that you wish to associate the VM network to.

Step 7 Select the network segment. As per SCVMM restrictions, you can associate only one network segment with a VM network.

Note	Modifying the network segment and the logical network attributes on the VM network can have undesirable effects in SCVMM if they have already been assigned to a VM. You must ensure that the network segment and the logical network attributes are not used by the VMs, including powered-off VMs before modifying these objects.

Step 8 Click **OK**.

The VM network is displayed in the Cisco UCS Manager GUI window.

Creating SCVMM Provider

You can create a SCVMM provider by using the **VM** tab.

Procedure

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

Step 2 Expand the **All** node.

Step 3 Right click **Microsoft**.

Step 4 Select **Add SCVMM Connection**.

Step 5 In the **Name** field, enter the name of the SCVMM provider.

Step 6 (Optional) In the **Description** field, enter the description of the SCVMM provider.

Step 7 In the **IP Address** field, enter the IP address of the server. You cannot enter the DNS hostname in the field.

Step 8 Click **OK**.

Configuring a Logical Switch

You can configure a logical switch by using the **VM** tab.

Procedure

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

Step 2 Expand the **All** node.

Step 3 Right-click the **SCVMM provider instance** under **Microsoft** and choose the **Create Logical Switch** option.

The **Create Logical Switch** window appears.

Step 4 In the **Name** field, enter the name of the logical switch.

Step 5 (Optional) In the **Description** field, enter the description of the logical switch .

Step 6 In the **Create Logical Switch** window, click **OK**.

A message window indicates that the logical switch is successfully created. The newly created logical switch is displayed in the Cisco UCSM GUI.

Configuring an Uplink Port Profile

You can configure an uplink port profile using the **VM** tab.

Procedure

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

Step 2   Expand the **All** node.

Step 3   Right-click an existing logical switch instance under **Microsoft > SCVMM** and click **Create an Uplink Port Profile**.

Step 4   In the **Create Uplink Port Profiles** window, enter the name of the uplink port profile.

Step 5   (Optional) In the **Description** field, enter the description of the uplink port profile.

Step 6   Add a network site to the uplink port.

> **Note**   Adding or removing a network site on the uplink port can have undesirable effects in SCVMM if the network site is assigned to a VM. You must ensure that this object is not used by the VMs, including the powered-off VMs, before modifying this object.

Step 7   Click **OK**.

You can now view the SCVMM provider and the logical switch configuration in the Cisco UCSM GUI.

Creating a Virtual Port Profile

You can create a virtual port profile using the **VM** tab.

Procedure

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

Step 2   Expand the **All** node.

Step 3   Click **Port Profiles**.

Step 4   Click **Add**.

Step 5   In the **Name** field, enter the name of the port profile.

Step 6   (Optional) In the **Description** field, enter the description of the port profile.

Step 7   (Optional) From the drop-down list, choose the **QoS policy**.

Step 8   (Optional) From the drop-down list, choose the **Network Control** policy.

Step 9   Enter the number of maximum ports for the port profile.

Step 10 In the **Host Network IO performance** field, click**None**. The **Host Network IO performance** mode is not supported on SR-IOV.

Step 11 (Optional) From the drop-down list, choose the **Pin Group**.

Step 12 Set the **Type** as **SLA Only** for Microsoft Hyper-V.

> **Note** While creating a port profile, set the type as **SLA Only** to make it a virtual port profile. The VLANs cannot be selected for the **SLA Only** port profile.

Step 13 Click **OK**.

Creating a Profile Client

You can create a port profile client using the **Create Profile Client** window.

Procedure

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

Step 2 Expand the **All** node.

Step 3 Click **Port Profiles**.

Step 4 Choose a port profile.

Step 5 Right-click the port profile then select the **Create Port Profile Client** option.

The **Create Profile Client** window appears.

Step 6 In the **Name** field, enter the name of the port profile client.

Step 7 (Optional) In the **Description** field, enter the description of the port profile client.

Step 8 Required: Select the logical switch in the **Distributed Virtual Switch** field. You can select a particular logical switch or all logical switches in this field. The configuration for the selected logical switch is done from **Microsoft -> SCVMM provider -> Logical switch**.

Step 9 Click **OK**.

A message window displays indicating that the profile client is successfully created. The profile client is attached to the logical switch.

Configuring Microsoft SCVMM

About Microsoft SCVMM Dependencies

Refer to the following Microsoft SCVMM dependencies for installing Microsoft SCVMM:

• Active Directory (AD) Services (2008 or 2012)

  The AD Domain Controller should have the following services:

  • AD DNS

  • AD DHCP (optional)

  • MSSQL 2008 (and later versions) database for SCVMM data store

    • SQL command line utilities

    • Windows Assessment and Deployment Kit (ADK 8.0)

Note	If you see the error message `Error while enabling Windows feature: Netfx3`, enter the following command as an administrator: **C:\> dism /online /enable-feature /featurename:netfx3 /all /source:d:\sources\sxs**, where **d:\sources\sxs** is the Windows installation folder that is mapped to your machine on the D drive.

Installing Cisco Provider Plugin in SCVMM

The Cisco provider plugin pulls the networking objects from the Cisco UCSM into Microsoft SCVMM. Complete the following steps to install the Cisco provider plugin on Microsoft SCVMM:

Before you begin

Verify that the SCVMM server is in the same domain as the host, the host has an eNIC driver, and enable the administrator account.

Note	See the Microsoft documentation for the prerequisites on bringing up the SCVMM server: http://technet.microsoft.com/en-us/library/gg610617.aspx

Procedure

Step 1   Install the Cisco UCSM Network Service provider package, for example, **CiscoProviderUCSMInstaller_1.1.14** on Microsoft SCVMM from your local drive. The installers are located in the **Installers** directory in the ISO image, for example, `ucs-bxxx-drivers\Windows\Installers\Cisco`.

When the installation is complete, the Cisco UCSM **Network Service Provider Package Setup** window appears.

Step 2   Click **Finish** to exit the setup wizard.

Creating a Network Service Instance

After you install the Cisco UCSM plugin, you can launch the SCVMM GUI and add a Network Service instance in the Microsoft SCVMM GUI.

Procedure

Step 1   In the Microsoft SCVMM GUI, click **Fabric**.

Step 2   This step is different for System Center 2012 R2 and System Center 2012 SP1 virtual machines.

- For System Center 2012 R2 and above, under **Networking**, right-click **Network Service** and choose **Add Network Service**.

- For System Center 2012 SP1, under **Networking**, right-click **Switch Extensions Manager** and choose **Add Virtual Switch Extension**.

The **Add Network Service** window appears. Enter the connection settings.

Step 3   In the Name tab in the left pane, enter the **Name** and **Description** for the Network Service.

Step 4   In the **Manufacturer** and **Model** tab in the left pane, choose the following from the drop-down list: Cisco Systems, Inc in the **Manufacturer** field.

- **Manufacturer** - for example, Cisco Systems Inc.

- **Model** - for example, Cisco UCSM

Step 5   In the **Credentials** tab, select **Run-As-account** from the browse list. Look for the account to access Cisco UCSM.

- If the account does not appear in the list, click **create-run-as-account**. To create an account, enter a Name and Description for the new **run-as-account**. In addition, put in the user name and password to access Cisco UCS Manager.

- Check the **validate domain credentials** and click **Finish**. The account is displayed in the **Select a Run as Account** window.

- Select the account to access Cisco UCS Manager.

Step 6   For the **Connection String** field in the left pane, enter the IP address of the Cisco UCSM , for example, http://10.2.2.2.

Step 7   The **Certificates** in the left pane does not require user input.

Step 8   For **Gather Information** in the left pane, click **Scan Provider** and verify the retrieved information from UCS Manager .

Step 9   For the **Host Group** in the left pane, choose the host groups that can use the Network Service.

Step 10   For the **Summary** in the left pane, confirm the settings, review the script, and click **Finish**.

Step 11   Check the status of the operation in the Jobs window. Once the task is complete, the Cisco UCSM is added to the Network Service.

Step 12   In the SCVMM GUI, choose the Cisco UCSM and click **Refresh**.

The networking objects are pulled from the Cisco UCSM into SCVMM. Only one Cisco UCSM per SCVMM is supported.

Note   Known Issue: Refreshing the Network Service in SCVMM might result in errors that are harmless. You will see the following error: .

We do not recommend that you make changes to one or more network segments; Microsoft does not support these changes. We also recommend that you do not make any changes to one or more fabric networks, network sites, or the fabric network tree.

Creating a Logical Switch in SCVMM

A logical switch contains the configuration information that controls the behavior of the virtual switches across hosts in your data center.

Procedure

Step 1	Right click the Microsoft SCVMM instance and select **Create Logical Switch** option. The **Create Logical Switch Wizard** window appears.
Step 2	In the **General** tab, enter a name of the logical switch.
Step 3	(Optional) In the **Description** field, enter the description of the logical switch.
Step 4	Click **OK**.
Step 5	Click **Next**.
Step 6	In the **Settings** tab, select the minimum bandwidth mode from the drop down menu. Check the box to enable SR-IOV for the logical switch.
Step 7	In the **Extensions** tab, uncheck the **Microsoft Windows Filter** check box because the filtering extension is not allowed with the forwarding extension. This is a Microsoft restriction.
Step 8	Choose the **Virtual Switch Extensions** that you want to use with the logical switch. Choose the logical switch as the forwarding extension. This object is pulled from the Cisco UCSM.
Step 9	Click **Next**.
Step 10	In the **Virtual Port** tab, click **Add**. The **Add Virtual Port** window appears. Select the appropriate port classification from the drop down menu. Or create a new port classification.
	If you created a port profile client earlier for the logical switch, you will see the name of the logical switch. When you check to select the logical switch, the port profile defined earlier will appear in the drop down menu. Check the box to include Hyper-V virtual network adapter port profile in this virtual port. Click browse to select the virtual network adapter port profile from the pre-defined list. If the list does not contain the right virtual network adapter port profile, you can create one by clicking the Create button. Provide the appropriate offload settings, security settings, and bandwidth setting.
Step 11	In the **Uplink** tab, click **New Uplink Port Profile**. The **Add Uplink Port Profile** window appears.
Step 12	Choose the **Uplink Port Profile**. Click **New Virtual Network Adapter** to configure the network adapter settings in connectivity, VLAN ID, IP address configuration, and port profile classification.
Step 13	Click **OK**.
Step 14	Click **Next**.
Step 15	In the **Port Classification** field, click **Browse** and choose the default SR-IOV port profile.
Step 16	Choose the logical switch and the associated port profile.
Step 17	Choose **Include a virtual network adapter port profile in this virtual port.**
Step 18	Choose the SR-IOV profile as the native virtual network adapter port profile.
Step 19	Click **OK**.
	The SR-IOV port profile is displayed in the **Virtual Port** tab.
Step 20	Click **Next**.
Step 21	In the left pane, click the **Summary** tab and confirm the settings.
Step 22	Click **Finish**.

The logical switch, the uplink port profile, and the port classification are displayed in the SCVMM GUI.

(Optional) Applying IP Pools for the VMs

You can apply the IP pools for the VMs. This step is optional.

Procedure

Step 1   Click **Library** in the Microsoft SCVMM GUI, select **VM Templates** under **Templates** menu.

Step 2   Right-click **Create VM Template**.
The **Create VM Template Wizard** window appears in the Microsoft SCVMM GUI.

Step 3   Click **Browse** and select a source for the new VM template.

Step 4   Required: Click **OK**.

Step 5   In the **VM Template Name** field, enter the VM template name.

Step 6   (Optional) In the **Description** field, enter the VM template description.

Step 7   Click **Next**.
Follow the prompts in the wizard to create the VM template.

Step 8   Use the template as a source to install the VM.
When you select a host and review virtual machine settings on a specific network adapter, the Cisco UCSM configuration specific to the logical network is pulled into SCVMM. You can apply IP pools for the VMs by using the template.

Note   For more information about how to configure IP pools, see the Microsoft SCVMM documentation.

Creating a VM Network in SCVMM

You can configure the settings for the VM network.

Procedure

Step 1   Click **VMs and Services** in the Microsoft SCVMM GUI.

Step 2   Right-click **VM Networks** and select **Create VM Network**.
The **Create VM Network Wizard** window appears in the Microsoft SCVMM GUI.

Step 3   In the **Name** tab, specify the name of the VM network.

Step 4   In the **Isolation** tab, specify the name of the network manager for the VM network.

Step 5   (Optional) In the **Description** tab, specify the description of the VM network.

Step 6   Choose the logical network from the drop-down list.

The logical network is the fabric network that is created on the Cisco UCSM side.

Step 7   Click **Next**.

The system displays the VM network that is created for the fabric network on the Cisco UCSM side.

Step 8   In the **Isolation** tab, specify the isolation for the VM network.

Step 9   Click **Next**.

Step 10   Configure the settings for the VM network in the **Settings** tab.

Step 11   Click **Finish**.

The VM network is displayed in the Microsoft SCVMM GUI.

Note   If you have a VM network, you can point it only to one network segment. If you have any offline VMs and they use a particular VM network, do not change the association of the VM networks. You can change the association only when the VMs are deleted.

Installing the Host Server Operating System

Before you begin

For detailed information about installing Windows Server 2012 or Windows Server 2012 R2 with Hyper-V, see the Microsoft Windows Server 2012 or Microsoft Windows Server 2012 R2 documentation.

Procedure

Step 1   Install Windows Server 2012 or Windows Server 2012 R2 with Hyper-V on the host server.

Step 2   Open the Windows Server Manager.

What to do next

Install the Cisco drivers and utilities.

Obtaining the Cisco Drivers and Utilities for VM-FEX for Hyper-V

Important   VM-FEX for Hyper-Vis not supported with Cisco UCS VIC 14xx adapters.

Procedure

Step 1   From the Cisco support site, download the Cisco UCS B-Series Blade Server Software Bundle ISO file.

The Cisco UCS B-Series Blade Server Software Bundle contains drivers, installation utilities, and the Cisco UCS Provider Plugin for VM-FEX for Hyper-V.

Step 2 In the Cisco UCS Manager KVM settings, mount the software bundle ISO file as virtual media for access from your servers.

Step 3 From the host server, open the CSCO_VIO_INSTALLER_*version* directory in the ISO file.

Insert the release version number for *version* in the directory name. For example, the directory name is CSCO_VIO_INSTALLER_2.4.22 for Release 2.2(1).

Step 4 Open and read the readme.txt file for the latest information about installing and configuring VM-FEX for Hyper-V.

Installing the PF Driver and VM-FEX Switch Driver

Perform this task on the host server to install the Cisco VIO drivers and utilities.

Note The Cisco VM-FEX switch driver is installed by SCVMM when the SRIOV-enabled switches are created on the host.

Before you begin

The Cisco UCS B-Series Blade Server Software Bundle ISO file must be mounted on the server.

Procedure

Step 1 In Powershell on the host server, open the CSCO_VIO_INSTALLER_*version* directory in the contents of the mounted ISO file.

Step 2 Run CSCO_VIO_INSTALLER_64_*version*.msi as administrator.

Insert the release version number for *version* in the command name. For example, the command name is CSCO_VIO_INSTALLER_64_2.4.22.MSI for release 2.2(1).

Step 3 Choose **Typical** or **Custom**installation. If you choose **Typical** installation, it installs eNIC and fNIC drivers. If you choose **Custom** installation, complete steps 4 through 9.

Step 4 If necessary, expand **VIO drivers** to display the driver list.

Step 5 Click **VIC iSCSI dump** and choose **Entire feature will be unavailable**.

Caution The installation might fail if the iSCSI driver are not deselected.

Step 6 Click **VIC VM-FEX Forwarding Extension** and choose **Entire feature will be unavailable**.

Caution The installation might fail if the VIC VM-FEX forwarding extension driver are not deselected. The VIC VM-FEX forwarding extension is deployed from SCVMM 2012 as part of the logical switch deployment.

Step 7 Click **VIC Teaming** and choose **Entire feature will be unavailable**.

Step 8   Click **VICManagement** and choose **Entire feature will be unavailable**.

Step 9   Click **Next** and follow the instructions to install the drivers.

Attaching a Hyper-V Host to Microsoft SCVMM

Before you begin

- Install the operating system.
- Update the driver.
- Move the host to the same domain as the SCVMM.
- Disable the firewall.

Tip   Cisco recommends that you install Hyper-V before adding the host to SCVMM. If you do not install Hyper-V before adding the host to SCVMM, a light version of Hyper-V, without a GUI, is installed.

Procedure

Step 1   In Microsoft SCVMM GUI, click **VMs and Services** in the bottom-left pane and then click **All Hosts**.

Step 2   Right-click and choose **Add Hyper-V Hosts and Clusters**.

Step 3   In the **Credentials** tab, provide the **Run as Account** details.

Note   Enter domain administrator credentials in this tab.

Step 4   Click **Next**.

Step 5   In the **Discovery Scope** tab, add the hostname in the **Computer Name** pane.

The system discovers the host.

Step 6   In the **Target Resources** tab, choose the host and click **Next**.

If the Hyper-V role is not enabled on any of the selected servers, SCVMM enables the role on these servers as part of the Add Host process, that results in a restart of the server. If any of the servers have a pending restart, they are also restarted.

Step 7   Click **OK** to continue.

Step 8   In the **Host Settings** tab, assign the selected host to a host group.

Step 9   Click **Next**.

Step 10   In the **Migration Settings** tab, choose the live storage migration settings and click **Next**.

The default value for live storage migration is 2.

Step 11   Click **Finish**.

The virtual machine host is added in the Microsoft SCVMM GUI. After the host is added to Microsoft SCVMM, verify that a connection is established between the SCVMM and the host. While attaching a host, use the management interface. After the host is added, a warning message indicates that multipath I/O is not enabled for known storage arrays on the specified host. This is a known issue with Microsoft. The recommended

action is that if you want to provision the storage using SCVMM, you must enable multipath I/O for storage arrays that are being used on the host by adding the multipath I/O feature.

Enabling SRIOV in SCVMM Failover Cluster

Before you begin

- All network interfaces on nodes in the cluster must have the same configuration (name, uplink VLANs and so on)

- The virtual switch must be a logical switch that can be provisioned on all Hyper-V nodes in the cluster.

Procedure

Step 1	Bring up two nodes with latest eNIC driver version.
Step 2	Create a cluster with these two nodes.
Step 3	Install SQL on a standalone node, which is not part of the cluster.
Step 4	Install SCVMM on the first node in the cluster. The Microsoft documentation, https://technet.microsoft.com/en-us/library/gg610678.aspx provides detailed information about this.
Step 5	Install SCVMM on the other node in the cluster. The Microsoft documentation, https://technet.microsoft.com/en-us/library/hh411279.aspx provides detailed information about this.
Step 6	Install the Cisco Provider Plugin on the first and second node. Please note that there is no need to bring down any node in the cluster while installing the Cisco Provider Plugin.
Step 7	Launch SCVMM and add a Hyper-V host.

Viewing the Host-side Configuration in Windows Server 2012

Following these guidelines for reviewing the host-side configuration in Windows Server 2012:

- Add the host to the domain. Verify that the domain host account has the administrator rights for adding a host to the domain.

- The Cisco eNIC driver for Windows Server 2012 has the following guidelines:

    - Note that the Cisco eNIC driver is an interface that facilitates communication between supported operating systems and Cisco UCS Virtual Interface Cards.
    - Make sure that the same driver is used for the hypervisor and VM.

- Configure the SR-IOV dynamic connection policy on the adapter in the service profile.
- Make sure that the Hyper-V role is enabled when the host is added to SCVMM.
- Make sure that the forwarding extension driver is installed on the host when the logical switch is created in SCVMM.

Deploying the Logical Switch to the Hyper-V Host

After you add a host to SCVMM, you must create a logical switch and attach it to that host. While attaching the host, it installs the extension drivers from SCVMM on the host.

Before you begin

Make sure that the data path interfaces are enabled for the Logical Switch and refresh the host.

Procedure

Step 1	In the Microsoft SCVMM GUI, in the**Host** tab, click **Properties**. The **Properties** window for the selected host is displayed.
Step 2	Click the **Hardware** tab. The available interfaces (network adapters) are displayed in the pane.
Step 3	Choose the management interface to display the details of the interface. The interfaces are attached to various logical switches.
Step 4	Choose the interface that is not associated with any of the logical network connectivity to attach it to the logical switch.
Step 5	Click the **Virtual Switches** tab.
Step 6	Click **New Virtual Switch** and select the **New Logical Switch** option.
Step 7	Select the logical switch from the drop-down list in the **Logical Switch** field.
Step 8	In the **Physical Adapters** panel, select the first physical adapter. When you select the logical switch, the uplink port profile is automatically selected for the logical switch. When you have multiple uplink port profiles, you can select one uplink port profile for the logical switch during the logical switch creation process.
Step 9	Click **OK**. If the same interface is used by multiple switches, a message window indicates that while SCVMM applies the changes, the host might temporarily lose the connectivity. This event might have an adverse effect on other network operations in progress.
Step 10	Click **OK**. The logical switch is now attached to the Hyper-V host.

Creating a VM in SCVMM

You can create a VM in SCVMM and attach the logical switch and the VM network to the VM vNICs.

Procedure

Step 1	Right-click the host in the Microsoft SCVMM GUI and choose **Create Virtual Machine**. The **Create Virtual Machine Wizard** window appears.
Step 2	Create a Virtual Machine (VM) and follow the hardware configuration steps.

> **Note** There are multiple ways to configure the VMs. For more information, see the Microsoft documentation.

Step 3	In the **Configure Hardware** tab, choose a network adapter for the VM.
Step 4	In the **Connectivity** panel on the right side, click **Browse** in the **Connected to a VM network** field and choose a VM network that you created earlier.
Step 5	Click **OK**.
Step 6	Choose the MAC address type in the **MAC Address** field. The MAC address can be **Dynamic** or **Static**.

> **Note** Use the Microsoft recommended settings for the MAC address pool.

Step 7	In the **Port Profile** field, choose the port classification as **SR-IOV**.
Step 8	Click **Next**.
Step 9	In the **Select Destination** tab, choose **Place the virtual machine on a host** and choose the **Destination** as **All Hosts**.
Step 10	Click **Next**. The destination host is highlighted.
Step 11	Click **Next**.
Step 12	In the **Configure Settings** tab, review the virtual machine settings and click **Next**.
Step 13	In the **Add Properties** tab, review the settings and click **Next**.
Step 14	In the **Summary** tab, confirm the settings and check the **Start the virtual machine after deploying it** check box.
Step 15	Click **Create**. The VM network is created and it is displayed in the GUI. A warning message indicates that the system cannot set bandwidth setting on the virtual adapter for the SR-IOV switch. The recommended action is to check the native virtual port profile, correct the issue, and try again.
Step 16	Choose the VM in the GUI and click **Properties**.
Step 17	Verify the configured properties of the VM.
Step 18	After the VM is up, install the virtual function (VF) driver on the VM. Use the same CSCO_VIO_INSTALLER_64 msi file that was used in Installing the PF Driver and VM-FEX Switch Driver, on page 21. For example, the command name is CSCO_VIO_INSTALLER_64_2.4.22.MSI for release 2.2(1).
Step 19	Choose **Typical** or **Custom** installation. If you choose **Custom** installation, install 'Cisco VIC VMNic Ethernet' and 'VIC Ethernet Utility'.

Verifying VM vNICs in Cisco UCSM GUI

You can verify the VM creation status in the Cisco UCSM GUI.

Procedure

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

Step 2   Expand the **All** node.

Step 3   Expand **Virtual Machines** and verify that the VM is displayed in the GUI. In the **General** tab, verify the properties of the vNIC fields. You can verify the **Name**, **MAC address**, **Profile Name**, **VMND Name**, and **Status of the vNIC** fields.

Configuring Policies

Configuring Dynamic vNIC Connection Policies

Dynamic vNIC Connection Policy

Note In an SR-IOV topology, such as a Hyper-V or KVM cluster, a Virtual Function (VF) takes the place of the dynamic vNIC. The VF is essentially a restricted version of the dynamic vNIC, in which all system communication and configuration of the VF is performed through the associated physical function (PF).

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.

Note Cisco UCS 6454 Fabric Interconnects do not support 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.

For Hyper-V, use the predefined Ethernet adapter policy named Windows.

Server Migration

✎

Note   If you migrate a server that is configured with dynamic vNICs, the dynamic interface used by the vNICs fails and Cisco UCS Manager notifies you of that failure.

When the server comes back up, Cisco UCS Manager 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 Connection Policy

Procedure

Step 1   In the **Navigation** pane, click **LAN**.

Step 2   Expand **LAN** > **Policies**.

Step 3   Expand the node for the organization where you want to create the policy.

If the system does not include multitenancy, expand the **root** node.

Step 4   Right-click the **Dynamic vNIC Connection Policies** node and choose **Create Dynamic vNIC Connection Policy**.

Step 5   In the **Create Dynamic vNIC Connection Policy** dialog box, complete the following fields:

Name	Description
Name field	The name of the policy.
	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 is saved.
	Note Do not specify "default" as the value for the dynamic vNIC connection policy name. Cisco UCS Manager automatically resolves any empty policy references to "default". Any service profiles or service profile templates with only static vNICS defined will automatically reference the policy "default" when it is present. If you specify "default" for the dynamic vNIC connection policy name, then unexpected dynamic vNICs might be created on those service profiles or service profile templates.
Description field	A description of the policy. Cisco recommends including information about where and when to use the policy.
	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).

Name	Description
Number of Dynamic vNICs field	The number of dynamic vNICs that this policy affects. Enter an integer between 0 and 256. The default is 54. **Note** Components of your system might limit this number to fewer than 256 vNICs.
Adapter Policy drop-down list	The adapter policy for Dynamic vNIC Connection Policy.
Protection field	Dynamic vNICs are always protected in Cisco UCS, but this field allows you to select a preferred fabric, if any. 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 B**—Cisco UCS attempts to use fabric B but fails over to fabric A if necessary • **Protected**—Cisco UCS uses whichever fabric is available

Step 6 Click **OK**.

Step 7 If a confirmation dialog box appears, click **Yes.**

Changing a Dynamic vNIC Connection Policy

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Expand **LAN** > **Policies**.

Step 3 Expand the node for the organization that contains the policy that you want to change.

If the system does not include multitenancy, expand the **root** node.

Step 4 Expand the **Dynamic vNIC Connection Policies** node and click the policy that you want to change.

Step 5 In the **Work** pane, click the **General** tab.

Step 6 Change one or more of the following fields:

Name	Description
Description field	A description of the policy. Cisco recommends including information about where and when to use the policy. 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).

Name	Description
Number of Dynamic vNICs field	The number of dynamic vNICs that this policy affects. Enter an integer between 0 and 256. The default is 54. **Note** Components of your system might limit this number to fewer than 256 vNICs.
Adapter Policy drop-down list	The adapter policy for Dynamic vNIC Connection Policy.

You cannot change the other properties of the policy, such as the **Name** field.

Step 7   Click **Save Changes**.

Step 8   If a confirmation dialog box displays, click **Yes**.

Deleting a Dynamic vNIC Connection Policy

You can delete a dynamic vNIC connection policy.

Procedure

Step 1   In the **Navigation** pane, click **LAN**.

Step 2   Expand **LAN** > **Policies** > *Organization_Name*.

Step 3   Expand the **Dynamic vNIC Connection Policies** node.

Step 4   Right-click the policy that you want to delete and choose **Delete**.

Step 5   If a confirmation dialog box displays, click **Yes**.

Viewing Dynamic vNIC Properties in a VM

You can view dynamic vNIC properties in a VM.

Before you begin

The VM must be operational.

Procedure

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

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

Step 3   Expand **Virtual Machines**.

Step 4   Expand the virtual machine that contains the dynamic vNIC.

Step 5   Choose the dynamic vNIC.

Step 6   In the **Work** pane, click the **General** tab.

In the **Properties** area, the vNIC properties appear.

Creating a Custom Ethernet Adapter Policy for SR-IOV

The predefined **SRIOV** Ethernet adapter policy supports up to 32 CPU threads. If the server has more than 32 CPU threads, you must follow this procedure to create and specify a custom adapter policy that supports a number of interrupts equal to the number of CPU threads.

For more information about creating an adapter policy, see "Configuring Ethernet Adapter Policies" in the *Cisco UCS Manager GUI Configuration Guide*.

Tip   If the fields in an area do not display, click the **Expand** icon to the right of the heading.

Before you begin

Determine the number of CPU threads used by your server. You can find this information by navigating to **Equipment > Chassis > Servers** and viewing the **Threads** heading for your server in the **Servers** table.

Procedure

Step 1   If you opened the **Create Ethernet Adapter Policy** directly from another menu, skip to Step 6.

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

Step 3   Expand **Servers** > **Policies**.

Step 4   Expand the node for the organization where you want to create the policy.

If the system does not include multitenancy, expand the **root** node.

Step 5   Right-click **Adapter Policies** and choose **Create Ethernet Adapter Policy**.

Step 6   Enter a name and description for the policy in the following fields:

Name	Description
Name field	The name of the policy. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen) and _ (underscore), and you cannot change this name after the object has been saved.

Name	Description
Description field	A description of the policy. Cisco recommends including information about where and when to use the policy. 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 7   In the **Resources** area, configure the following values as shown:

Name	Setting
Transmit Queues	1
Ring Size	256
Receive Queues	4
Ring Size	512
Completion Queues	5
Interrupts	Enter the number of CPU threads used by the server.

Step 8   In the **Options** area, configure the following values as shown:

Name	Setting
Transmit Checksum Offload	Enabled
Receive Checksum Offload	Enabled
TCP Segmentation Offload	Enabled
TCP Large Receive Offload	Enabled
Receive Side Scaling (RSS)	Disabled
Accelerated Receive Flow Steering	Disabled
Network Virtualization using Generic Routing Encapsulation	Disabled
Virtual Extensible LAN	Disabled
Fallback Timeout	5 seconds
Interrupt Mode	MSI X
Interrupt Coalescing Type	Min
Advance Filter	Disabled
Advance Filter	Disabled
Advance Filter	Disabled
Interrupt Scaling	Disabled

Step 9   Click **OK**.

Step 10   If a confirmation dialog box displays, click **Yes**.