Configuring Cisco vWAAS and Viewing Cisco vWAAS Components

This chapter describes how to configure Cisco vWAAS settings, such as Cisco WAAS Central Manager address and traffic interception settings, and how to identify a Cisco vWAAS on the Cisco WAAS Central Manager or through the Cisco WAAS CLI.

This chapter contains the following sections:

Configuring Cisco vWAAS

This section contains the following topics:

Configuring Cisco vWAAS Settings

After the Cisco vWAAS VM has been installed, you must configure the following Cisco vWAAS settings:

- IP address and netmask
- Default gateway
- Cisco WAAS Central Manager address
- Settings for corresponding VLAN in the VM for network reachability
- Centralized Management System (CMS)
- Traffic interception (see Configuring Cisco vWAAS Traffic Interception, page 2-2)

To configure Cisco vWAAS settings, follow these steps:

Step 1 In the VMware vSphere Client, click the **Console** tab and log in to the Cisco vWAAS console, using the username **admin** and the password **default**.

Step 2 Configure the IP address and netmask using the **interface virtual** command, as shown in the following example:

```
VWAAS(config)# interface virtual 1/0
VWAAS(config-if)# ip address 2.1.6.111 255.255.255.0
VWAAS(config-if)# exit
```

Note For Cisco vWAAS in WAAS Version 6.1.x and later, the Cisco vWAAS and Cisco vCM devices require both the virtual (network) interfaces to be "present". One or both the virtual interfaces should be active for the Cisco vWAAS and Cisco vCM devices to be operational after power up.

Step 3 Configure the default gateway using the **ip** command:

```
VWAAS(config)# ip default-gateway 2.1.6.1
```

Ping the IP addresses of the default gateway and Central Manager to verify if they can be reached, before continuing to the next step.

Step 4 Add the Central Manager address using the **central-manager** command:

```
VWAAS(config)# central-manager address 2.75.16.100
```

Step 5 Enable CMS to register with the Central Manager using the **cms** command:

```
VWAAS(config)# cms enable
```

Note Cisco vWAAS registration with the Central Manager is mandatory before traffic can be optimized. To ensure that Cisco vWAAS registration with the Cisco WAAS Central Manager is successful, confirm that this configured interface for the Cisco WAAS Central Manager is the primary Cisco WAAS Central Manager interface.

Step 6 Configure traffic interception, that is, WCCP, AppNav, or L2 Inline. For more information on traffic interception methods for Cisco vWAAS, see Configuring Cisco vWAAS Traffic Interception, page 2-2.

Configuring Cisco vWAAS Traffic Interception

You can configure the following traffic interception methods for Cisco vWAAS. Table 2-1 provides descriptions of each traffic interception method.

- WCCP: Available for Cisco vWAAS in all Cisco WAAS versions.
- AppNav: Available for Cisco vWAAS in all Cisco WAAS versions
- L2 Inline: Available for Cisco WAAS Version 6.2.x and later, for Cisco vWAAS with RHEL KVM. Table 2-2 shows the commands for configuring and displaying information on L2 Inline interception for Cisco vWAAS.

Table 2-1 Traffic Interception Methods for Cisco vWAAS

Traffic Interception Method	Description
WCCP	Specifies interactions between one or more routers (or L3 switches) and one or more application appliances, web caches, and caches of other application protocols, to establish and maintain the transparent redirection of selected types of traffic. The selected traffic is redirected to a group of appliances. Any type of TCP traffic can be redirected. WCCP uses a WCCP-enabled router or L3 switch. **Note** You can configure WCCP-GRE or L2 Inline as the redirection method for Cisco vWAAS running on a Cisco UCS-E inside a Cisco ISR G2, where the Cisco UCS-E interface is configured as IP unnumbered in Cisco IOS. For more information on WCCP, see Chapter 5, "Configuring Traffic Interception" in the *Cisco Wide Area Application Services Configuration Guide*.
AppNav	A policy and class-based traffic interception method that reduces dependency on the intercepting switch or router by distributing traffic among Cisco WAAS devices for optimization. For more information on AppNav, see Chapter 4, "Configuring AppNav" and Chapter 5, "Configuring Traffic Interception" in the *Cisco Wide Area Application Services Configuration Guide*.
L2 Inline	Places the Cisco vWAAS in the data path between WAN and LAN, with an interface facing each segment to inspect and optimize the traffic, as needed. For L2 Inline, traffic is forwarded directly without being sent back to the router. The Cisco vWAAS interfaces, with virtual NICs, appear as virtual interfaces in the Cisco WAAS Central Manager for the running configuration. By default, the NICs supporting Inline mode do not appear in the running configuration when L2 Inline interception is not enabled. **Note** Cisco vWAAS in Cisco WAAS Version 6.2.1 does not include fail-to-wire capability. For more information on configuring L2 Inline interception on the Cisco WAAS Central Manager, see Chapter 5, "Configuring Traffic Interception" in the *Cisco Wide Area Application Services Configuration Guide*.

Table 2-2 shows the commands for configuring and displaying information on L2 Inline interception for Cisco vWAAS.

Table 2-2 Cisco WAAS CLI Commands for L2 Inline Traffic Interception

Mode	Command	Description
Global Configuration	**(config) interception-method inline**	Enables L2 inline traffic interception on Cisco vWAAS.
Interface Configuration	**(config-if) cdp**	Enables Cisco Discovery Protocol on the interface of a Cisco WAAS device. (To globally enable the Cisco Discovery Protocol interval and holdtime options, use the **cdp** global configuration command.)
	(config-if) description	Configures the description for a network interface.
	(config-if) encapsulation	Sets the encapsulation type for the interface.
	(config-if) exit	Terminates interface configuration mode and returns you to global configuration mode.
	(config-if) inline	Enables inline traffic interception for an inlineGroup interface. For more information on the **inline** interface configuration command, including specifying an inline group and inline interception for VLAN IDs, see *Cisco Wide Area Application Services Command Reference*.
	(config-if) ip	Configures the IPv4 address or subnet mask on the interface of a Cisco WAAS device, or negotiates an IP address from DHCP on the interface of a Cisco WAAS device.
	(config-if) ipv6	Configures the IPv6 address on the interface of a Cisco WAAS device, or negotiates an IP address from DHCP on the interface of a Cisco WAAS device.
	(config-if) load-interval	Configures the interval at which to poll the network interface for statistics,
	(config-if) shutdown	Shuts down a specific hardware interface on a Cisco WAAS device, and shuts down the inlinegroup interface to bypass the traffic, and does not optimize the traffic.
privileged-level EXEC	**show interception-method**	Displays the configured traffic interception method.
	show interface InlineGroup	Displays inline group information and the slot and inline group number for the selected interface.
	show interface inlineport	Displays the inline port information and the slot and inline group number for the selected interface.
	show running-config	Displays the current running configuration.

For more information on these commands, see *Cisco Wide Area Application Services Command Reference*.

Identifying a Cisco vWAAS Device

This section has the following topics:

Identifying a Cisco vWAAS Model

As shown in Table 2-3, a Cisco vWAAS model is determined by the number of vCPUs and the maximum number of TCP connections.

Table 2-3 Cisco vWAAS Models with vCPUs and Maximum TCP Connections

Cisco vWAAS Model	Number of vCPUs	Maximum Number of TCP Connections
vWAAS-150	1	150
vWAAS-200	1	200
vWAAS-750	2	750
vWAAS-1300	2	1,300
vWAAS-2500	4	2,500
vWAAS-6000	4	6,000
vWAAS-6000-R (earliest supported version: Cisco WAAS 6.4.x)	4	6,000
vWAAS-12000	4	12,000
vWAAS-50000	8	50,000

Identifying a Cisco vWAAS Device on the Cisco WAAS Central Manager

There are two windows on the Cisco WAAS Central Manager that show identifying information for a vWAAS device. Table 2-4 shows the displayed Cisco vWAAS device types.

- Choose **Devices** > *device-name*. On the dashboard for the device, in the **Device Info** > **Hardware Details** section, the **Model** column shows the vWAAS device type.
- Choose **Device** > **All Devices**, which shows a listing of all the devices, including **Device Type**.

Table 2-4 Cisco vWAAS Device Types Shown in Cisco WAAS Central Manager and WAAS CLI

Cisco vWAAS Device	Cisco vWAAS Device Type Shown in Cisco WAAS Central Manager
vWAAS on VMware ESXi	OE-VWAAS-ESX
vWAAS on Microsoft Hyper-V	OE-VWAAS-HYPERV
vWAAS on RHEL KVM	OE-VWAAS-KVM

Cisco vWAAS Device	Cisco vWAAS Device Type Shown in Cisco WAAS Central Manager
vWAAS on KVM on CentOS	OE-VWAAS-KVM
vWAAS on Microsoft Azure	OE-VWAAS-AZURE

Identifying a Cisco vWAAS Device with the Cisco WAAS CLI

Table 2-5 shows the commands used to display vWAAS device information. For more information on these commands, see *Cisco Wide Area Application Services Command Reference*.

Table 2-5 Cisco WAAS CLI Commands for Cisco vWAAS Device Information

Mode	Command	Description
user-level EXEC and privileged-level EXEC	**show version**	Displays version information about the WAAS software currently running on the vWAAS device, including date and time system last started, and the length of time the system has been running since the last reboot. • (Optional) Use the **show version last** command to display version information for the last saved image. • (Optional) Use the **show version pending** command to display version information for the pending upgraded image.
privileged-level EXEC	**show hardware**	Displays system hardware status for the vWAAS device, including: • Startup date and time, the run time since startup, microprocessor type and speed, and a list of disk drives.
privileged-level EXEC	**show tfo detail**	Displays Transport Flow Optimization (TFO) information, including: • State: Registered or Not Registered • Default Action: Drop or Use • Connection Limit: The maximum TFO connections handled before new connection requests are rejected. • Effective Limit: The dynamic limit relating to how many connections are handled before new connection requests are rejected. • Keepalive Timeout: The connection keepalive timeout, in seconds.

Cisco vWAAS System Partitions

For all Cisco vWAAS models, the system partition size for **/sw** and **/swstore** is increased from 1 GB to 2GB, under the following conditions:

- The **disk delete-preserve-software** command deletes all the disk partitions and preserves the current software version.
- The partition size of 2 GB each for **/sw** and **/swstore** is effective only after a new OVA/ISO installation.
- During an upgrade, the newly defined partition size becomes effective *only after* you run the **disk delete-partitions** ***diskname*** command.

Caution During a downgrade, the partition size of **/sw** and **/swstore** each remains at 2GB, which leads to a file system size mismatch.

For detailed information on object cache data partitions and Akamai cache data partitions, see the chapter "Maintaining Your WAAS System" in the *Cisco Wide Area Application Services Configuration Guide*.

Operating Considerations for Cisco vWAAS and Cisco WAAS

Consider the following guidelines when using Cisco vWAAS in Cisco WAAS:

- For Cisco vWAAS in WAAS Version 6.1.x and later, the Cisco vWAAS and Cisco vCM devices require both virtual (network) interfaces to be present, but both need not be active. If only one virtual interface is active, the Cisco vWAAS and Cisco vCM devices will not be operational after power up. For more information, see Configuring Cisco vWAAS, page 2-1.
- If the virtual host was created using an OVA file of Cisco vWAAS in WAAS Version 5.0 or earlier, and you have upgraded Cisco vWAAS in Cisco WAAS, you must verify that the **SCSI Controller Type** is set to **VMware Paravirtual**. Otherwise, Cisco vWAAS will boot with no disk available and will fail to load the specified configuration.

  If needed, change the **SCSI Controller Type** to **VMware Paravirtual** by following these steps:

  a. Power down the Cisco vWAAS.
  b. From the **VMware vCenter**, choose **vSphere Client** > **Edit Settings** > **Hardware**.
  c. Choose **SCSI controller 0**.
  d. From the **Change Type** drop-down list, verify that the **SCSI Controller Type** is set to **VMware Paravirtual**. If this is not the case, choose **VMware Paravirtual**.
  e. Click **OK**.
  f. Power up the Cisco vWAAS, in Cisco WAAS Version 6.1.x or later.

Cisco vWAAS with Single-Root I/O Virtualization

This section has the following topics:

About Single-Root I/O Virtualization

Single-Root I/O Virtualization (SR-IOV) is a standard developed by the Peripheral Component Interconnect Special Interest Group (PCI-SIG) to improve virtualization of PCI devices.

SR-IOV enables the VMs to share the I/O device in a virtualized environment. SR-IOV achieves this by bypassing the hypervisor's involvement in data movement:

- SR-IOV provides independent memory space, interrupts, and Cisco Data Migration Assistant (DMA) streams for each VM.
- The SR-IOV architecture allows a device to support multiple virtual functions, and therefore, minimizes the hardware cost of each additional function.
- SR-IOV-enabled Ethernet controllers support direct assignment of part of the port resources to guest operating systems that use the SR-IOV standard. This capability enhances the performance of the guest VMs.

Table 2-6 shows the two types of functions used with SR-IOV.

Table 2-6 SR-IOV Physical Functions and Virtual Functions

Function	Description
Physical Functions	• A full PCI Express (PCIe) function that includes the SR-IOV extended capability, which is used to configure and manage the SR-IOV functionality. • Physical functions are discovered, managed, and configured as normal PCIe devices. Physical functions configure and manage the SR-IOV functionality by assigning virtual functions.
Virtual Functions	• A lightweight PCIe function that contains all the resources necessary for data movement, but has a carefully minimized set of configuration resources. • Each Virtual Function is derived from a Physical Function. The number of Virtual Functions an Ethernet controller can have is limited according to the device hardware.

Interoperability and Platforms Supported for Cisco vWAAS with SR-IOV

This section contains the following topics:

Cisco WAAS Central Manager and Cisco vWAAS with SR-IOV

Devices with SR-IOV are registered with the Cisco WAAS Central Manager in the same manner as other Cisco vWAAS devices. Use the **cms deregister** EXEC command to deregister these devices as you would for other Cisco vWAAS devices.

The following list shows how vWAAS devices with SR-IOV are displayed on the Cisco WAAS Central Manager:

- Cisco vWAAS with SR-IOV on KVM (RHEL, CentOS or Cisco NFVIS) is displayed as **OE-VWAAS-KVM**.
- Cisco vWAAS with SR-IOV on VMware ESXi is displayed as **OE-VWAAS-ESX**.

Platforms Supported for Cisco vWAAS with SR-IOV

Consider the following operating considerations for platforms supported for Cisco vWAAS with SR-IOV:

- Although Intel X710 is capable of 10 Gbps speed, vWAAS with SR-IOV using Intel X710 on NFVIS is supported for 1 Gbps speed, as part of vBranch solution.
- The supported firmware version for Intel X710 NIC is 5.05

Table 2-7 shows the WAAS version and platforms supported for vWAAS with SR-IOV.

Table 2-7 Cisco WAAS Version and Platforms Supported for Cisco vWAAS with SR-IOV

Ethernet Controller	Hypervisor	Earliest Cisco WAAS Version Supported	Supported Cisco vWAAS Models
Intel I350	CentOS	6.4.1	• vWAAS-150 • vWAAS-200 • vWAAS-750 • vWAAS-1300 • vWAAS-2500 • vWAAS-6000
Intel X710	NFVIS	6.4.1	• vWAAS-150 • vWAAS-200 • vWAAS-750 • vWAAS-1300 • vWAAS-2500 • vWAAS-6000
	CentOS	6.4.3	• vWAAS-12000 • vWAAS-50000
	ESXi	6.4.3	• vWAAS-12000 • vWAAS-50000 • vWAAS-150000

Upgrade and Downgrade Considerations for Cisco vWAAS with SR-IOV

Consider the following when you upgrade or downgrade a Cisco vWAAS with SR-IOV:

- Upgrade
  - The upgrade procedure for Cisco vWAAS with SR-IOV is the same as for other vWAAS devices.

- Downgrade
  - Before a downgrade from Cisco vWAAS in Cisco WAAS Version 6.4.1x or 6.4.3 to an earlier version, from the host, remove those SR-IOV interfaces that do not support this functionality when operating in a Cisco WAAS version earlier than WAAS Version 6.4.1x. Downgrade of Cisco vWAAS instances with SR-IOV is blocked for unsupported WAAS versions. Table 2-7 displays the earliest Cisco WAAS versions supported for SR-IOV.
  - At the device level, if you downgrade a Cisco vWAAS instance with SR-IOV to a version earlier than 6.4.1x or 6.4.3 (depending on your Cisco WAAS configuration), a warning message is displayed at the start of the downgrade process. This warning message is displayed if the device supports SR-IOV functionality, even if the device does not use the SR-IOV interface, because downgrade of vWAAS instances with SR-IOV is blocked for unsupported Cisco WAAS versions.
  - At the device group level, if you downgrade a device group that contains at least one device that supports SR-IOV functionality, a warning message is displayed at the start of the downgrade process, because downgrade of Cisco vWAAS instances with SR-IOV is blocked for unsupported WAAS versions.

For more information on the upgrade or downgrade process, see *Release Notes for Cisco Wide Area Application Services*.

Deploying Cisco vWAAS with SR-IOV

This section contains the following topics:

Deploying Cisco vWAAS with SR-IOV on KVM

This section contains the following topics:

Configuring Host Settings for Cisco vWAAS on KVM or CentOS with SR-IOV on the Cisco UCS C-Series

One-time host settings are required to use the SR-IOV functionality on RHEL KVM or CentOS on the Cisco UCS C-Series.

To configure the required host settings for deploying Cisco vWAAS on RHEL KVM or CentOS with SR-IOV on the Cisco UCS C-Series, follow these steps:

Step 1 Enable Intel Virtualization Technology for Directed I/O (VT-d) in the host BIOS.

Enable **VT-d**:

Use the **cat /proc/cpuinfo | grep -E 'vmx|svm' | wc -l** command to verify that you have enabled VT-d.

The command value should be greater than **0**.

Step 2 Enable I/O MMU:

a. In the **/etc/default/grub** file, add **intel_iommu=on** to **GRUB_CMDLINE_LINUX**.

b. After you make changes to **GRUB_CMDLINE_LINUX**, the following message is displayed:

```
GRUB_CMDLINE_LINUX="crashkernel=auto rd.lvm.lv=centos/root rd.lvm.lv=centos/swap rhgb
quiet intel_iommu=on"
```

c. For the changes to take effect, compile using **grub2-mkconfig -o /boot/grub2/grub.cfg**.

d. Reboot the host.

Step 3 Enable the SR-IOV virtual functions (for more information on virtual functions, see About Single-Root I/O Virtualization, page 2-8).

a. Verify the maximum number of virtual functions allowed for the specified interface.

For example, if the SR-IOV-supported interface is **enpls0f0**, verify the value of **/sys/class/net/enp1s0f0/device/sriov_totalvfs**.

b. Set the required number of virtual functions in **/sys/class/net/enp1s0f0/device/sriov_numvfs**.

- On the **enpls0f0** interface, enter the following:
  echo 7 > /sys/class/net/enp1s0f0/device/sriov_numvfs

Step 4 To remove the SR-IOV configuration for a specific interface, for example, **enp1s0f0**, use the command **echo 0 at /sys/class/net/enp1s0f0/device/sriov_numvfs** command and remove the lines with the **enp1s0f0** interface name present in **/etc/rc.d/rc.local**.

Deploying Cisco vWAAS with SR-IOV on RHEL KVM or CentOS Using Deployment Script for Cisco UCS C-Series

Cisco vWAAS on RHEL KVM or CentOS for SR-IOV is deployed using the **launch.sh** script file on Cisco UCS C-Series.

To deploy Cisco vWAAS on RHEL KVM for SR-IOV functionality using the deployment script, follow these steps (from the **launch.sh** script file):

Step 1 To check the prerequisite host configuration, run the following command:

./launch.sh check

Step 2 To launch the VM with **bridge** or **macvtap** interfaces, run the following command:

./launch.sh <*vm_name*> <*intf_type*> <*intf1_name*> <*intf2_name*>

- where *intf_type* can be either **bridge** or **macvtap**.
- where *intf1_name* and *intf2_name* are the desired names based on the selected **intf_type**.

Step 3 To launch Cisco vWAAS (not Cisco vCM) with SRIOV interface(s), run the following command:

./launch.sh <*vm_name*> <*intf_type*> <*intf1_name*> <*inft_type*> <*intf2_name*>

- where first *intf_type* option can be **bridge** or **macvtap** or **sriov**.
- where second *intf_type* option should be **sriov**.
- *intf1_name* and *intf2_name* are the desired names based on the selected **intf_type**.

Deploying Cisco vWAAS with SR-IOV on RHEL KVM or CentOS Using Cisco NFVIS Portal for Cisco ENCS 5400-W Series

To deploy Cisco vWAAS on RHEL KVM or CentOS with SR-IOV using the Cisco NFVIS portal for the Cisco ENCS 5400-W Series, follow these steps:

Step 1 From the **Cisco Enterprise NFV Solution** window, click the **VM Deployment** tab.

The **VM Deployment** window displays a navigation row, shown in Figure 2-1, to highlight where you are in the VM deployment process.

Figure 2-1 VM Deployment Process Navigation Flow

1 Images > 2 Profiles > 3 Networks > 4 Configuration > 5 Review & Deploy

Before you enter information to begin the VM deployment process, the **VM Deployment** navigation row displays the element **1 Images** as being highlighted.

Note You must specify all the parameters for the Cisco vWAAS VM during VM deployment. After the Cisco vWAAS VM is deployed, you cannot make changes to the Cisco vWAAS VM. To change any parameter for a deployed Cisco vWAAS VM, you must delete that Cisco vWAAS VM and deploy a new Cisco vWAAS VM.

Step 2 To register the Cisco vWAAS VM image, at the **VN Name** field, enter the name of the Cisco vWAAS VM.

Step 3 From the **List of Images** on the Device table listing, select an image for the Cisco vWAAS VM that will be deployed, or click **Upload** to upload an image.

The **VM Deployment** navigation row shows **2 Profiles** as being highlighted.

Step 4 Click **Next**.

The **Profiles** window is displayed, showing the **Select Profiles** table listing, which has columns for profile name, CPUs, memory (in MB), and disk size (in MB).

Step 5 From the **Select Profiles** table listing, click the radio button next to the profile you want to use, or click "+" to add a new profile.

A new, empty row is displayed for you to enter information.

Step 6 Click **Save** to create the new profile.

Step 7 Click **Next**.

The **VM Deployment** navigation row shows **3 Networks** as being highlighted.

The **Select Network Interface** window is displayed, showing the **Select Network Interface** table listing, which has columns for VNIC number and network name.

Step 8 From the **Select Network Interface** table listing:

- Check the check box next to one or more NVIC numbers that you want to attached to the VM you selected or created in Steps 1 to Step 4, or
- Click "+" to add a new VNIC for the specified VM.

  If you click "+" to create a new VNIC, a new empty row is displayed for you to enter information.

Step 9 Click **Save** to create the new VNIC.

The VM Deployment navigation row still shows **3 Networks** as being highlighted.

The **Networks and Bridges** table listing is displayed, which you use to add or delete networks and associated bridges.

Consider the following as you use the **Networks and Bridges** table listing:

- The table listing displays columns for network name, VLAN (if applicable), bridge, and port (if applicable).
- The table listing shows the available networks and bridges on the NFVIS server. Initially, the table listing shows the default networks: **lan-net** and **wan-net** and associated bridges.
- The top right corner of the table toolbar shows the selected row and the total number of rows, for example, “Selected 2 / Total 4”.
- To associate multiple VLANs with a network, separate the VLAN numbers with a comma and no space, for example, “100,200”.
- To associate multiple ports with a network, separate the port numbers with a comma and no space, for example, **1,2**.
- A network and bridge operate as one entity. (To delete a network and bridge, click the radio button adjacent to that network and bridge row. Click **Delete**. The page automatically refreshes; there is no confirmation question. Note that you can delete only one network and bridge at a time.)

Step 10 Click **Next**.

The **VM Deployment** navigation row shows **4 Configuration** highlighted.

(Optional) The **Port Forwarding** window is displayed.

Step 11 In the **Port Number** field, enter the number of the port for port forwarding.

Step 12 In the **External Port Number** field, enter the number of the external port. The external port is accessible only from the WAN bridge.

Step 13 Click **Next**.

The **VM Deployment** navigation row shows **5 Review & Deploy** highlighted.

The following message is displayed: `Starting VM deployment. Redirecting to Status Page.`

Step 14 Click **OK**.

The window refreshes and the **Status** is displayed, showing the **VM Status** table listing, with columns for VM name, profile name, status, and VNC console.

As the VM is being deployed, the status shows **VM in Transient State**. After deployment is complete, the status shows **VM is running**.

Step 15 After deployment is complete, click the **Management** tab to manage the VM with tasks, including power off, power on, reboot, and delete.

Deploying Cisco vWAAS with SR-IOV on VMware ESXi

This section contains the following topics:

Configuring Host Settings for Cisco vWAAS with SR-IOV on VMware ESXi for Cisco UCS C-Series

Before you begin, note the VMware ESXi host requirements for Cisco vWAAS with SR-IOV on Cisco UCS C-Series (Table 2-8).

Table 2-8 VMware ESXi Requirements for Cisco vWAAS with SR-IOV on Cisco UCS C-Series

Intel X710 NIC Specification	Specification Value
Driver Name	i40e
Tested Driver Version	2.0.7
Tested Firmware Version	5.0.5

Note Without compatible drivers, the Intel X710 will not be detected.

To create a virtual function in VMware ESXi, follow these steps:

Step 1 Log in to the VMware ESXi shell.

Step 2 Run the **lspci | grep -i intel | grep -i 'ethernet\|network'** command, and note the port order of this command.

Step 3 Run this command to create virtual functions:

```
# esxcli system module parameters set -m i40e -p max_vfs=Y,Z
```

- **Y,Z** represents the number of VF's to be created respectively for each port.

Example 1:

```
max_vfs=5,0 represents 5 VFs on adapter 1 port 1
```

Example 2:

```
max_vfs=0,5 represents 5 VFs on adapter 1 port 2
```

```
[root@localhost:~]
[root@localhost:~] lspci | grep -i intel | grep -i 'ethernet\|network'
0000:01:00.0 Network controller: Intel Corporation I350 Gigabit Network Connection [vmnic2]
0000:01:00.1 Network controller: Intel Corporation I350 Gigabit Network Connection [vmnic3]
0000:06:00.0 Network controller: Intel Corporation 82599EB 10-Gigabit SFI/SFP+ Network Connection [vmnic0]
0000:06:00.1 Network controller: Intel Corporation 82599EB 10-Gigabit SFI/SFP+ Network Connection [vmnic1]
0000:81:00.0 Network controller: Intel Corporation Ethernet Controller X710 for 10GbE SFP+ [vmnic4]
0000:81:00.1 Network controller: Intel Corporation Ethernet Controller X710 for 10GbE SFP+ [vmnic5]
[root@localhost:~]
[root@localhost:~] esxcli system module parameters set -m i40e -p max_vfs=5,0
[root@localhost:~]
```

355943

```
[root@localhost:~]
[root@localhost:~] lspci | grep -i intel | grep -i 'ethernet\|network'
000:01:00.0 Network controller: Intel Coporation I350 Gigabit Network Connection vmnic2]
```

Step 4 To verify the value of the VFs to be created, use the **esxcli system module parameters list -m i40e** command:

```
[root@localhost:~]
[root@localhost:~] esxcli system module parameters list -m i40e
Name              Type          Value  Description
----------------  ------------  -----  -----------------------------------------------------------------------------------------------
RSS               array of int         Number of Receive-Side Scaling Descriptor Queues: 0 = disable/default, 1-4 = enable (number of cpus)
VMDQ              array of int         Number of Virtual Machine Device Queues: 0/1 = disable, 2-16 enable (default = 8)
debug             int                  Debug level (0=none,...,16=all)
heap_initial      int                  Initial heap size allocated for the driver.
heap_max          int                  Maximum attainable heap size for the driver.
max_vfs           array of int  5,0    Number of Virtual Functions: 0 = disable (default), 1-128 = enable this many VFs
skb_mpool_initial int                  Driver's minimum private socket buffer memory pool size.
skb_mpool_max     int                  Maximum attainable private socket buffer memory pool size for the driver.
[root@localhost:~]
[root@localhost:~]
```

355944

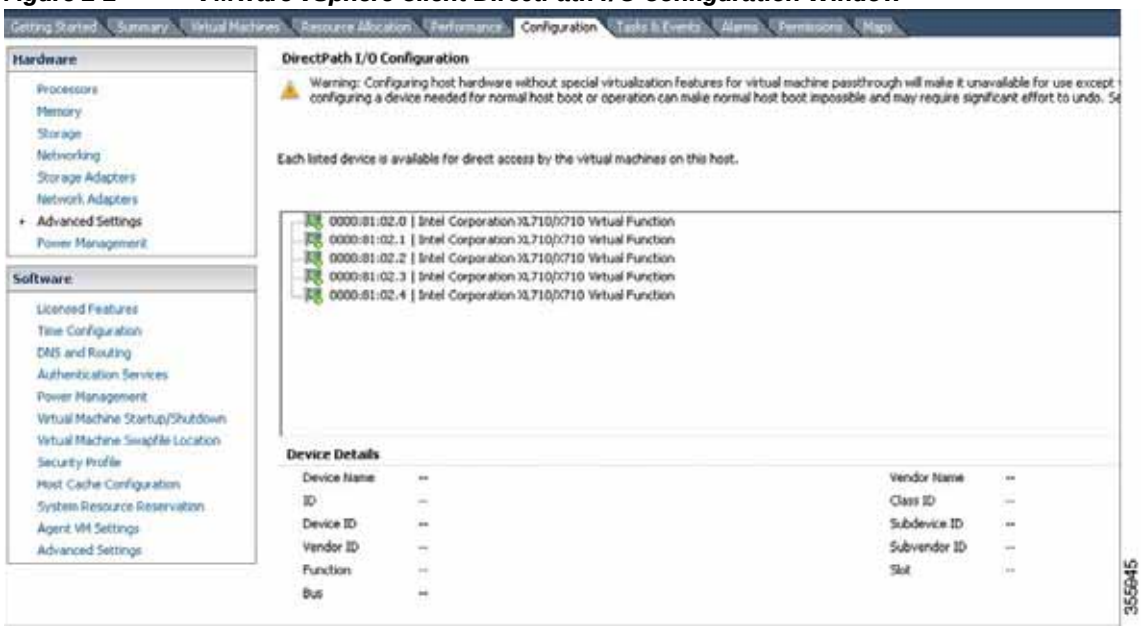
Step 5 To create the virtual functions, reboot the host.

Step 6 After the reboot is complete, verify the virtual functions by using either of the following options:

- The **VMware vSphere Client DirectPath I/O Configuration** window (Figure 2-2)

  Choose **Host** > **Configuration** > **Hardware** > **Advanced Settings**.
- The **VMware ESXi lspci** command

Figure 2-2 VMware vSphere Client DirectPath I/O Configuration Window



355945

Configuring SR-IOV Interfaces for Cisco vWAAS on VMware ESXi on Cisco UCS-C Series

To configure SR-IOV interfaces for Cisco vWAAS on VMware ESXi on Cisco UCS-C Series, follow these steps:

Step 1 After deploying the Cisco vWAAS, power down the Cisco vWAAS.

Step 2 Power up the vWAAS.

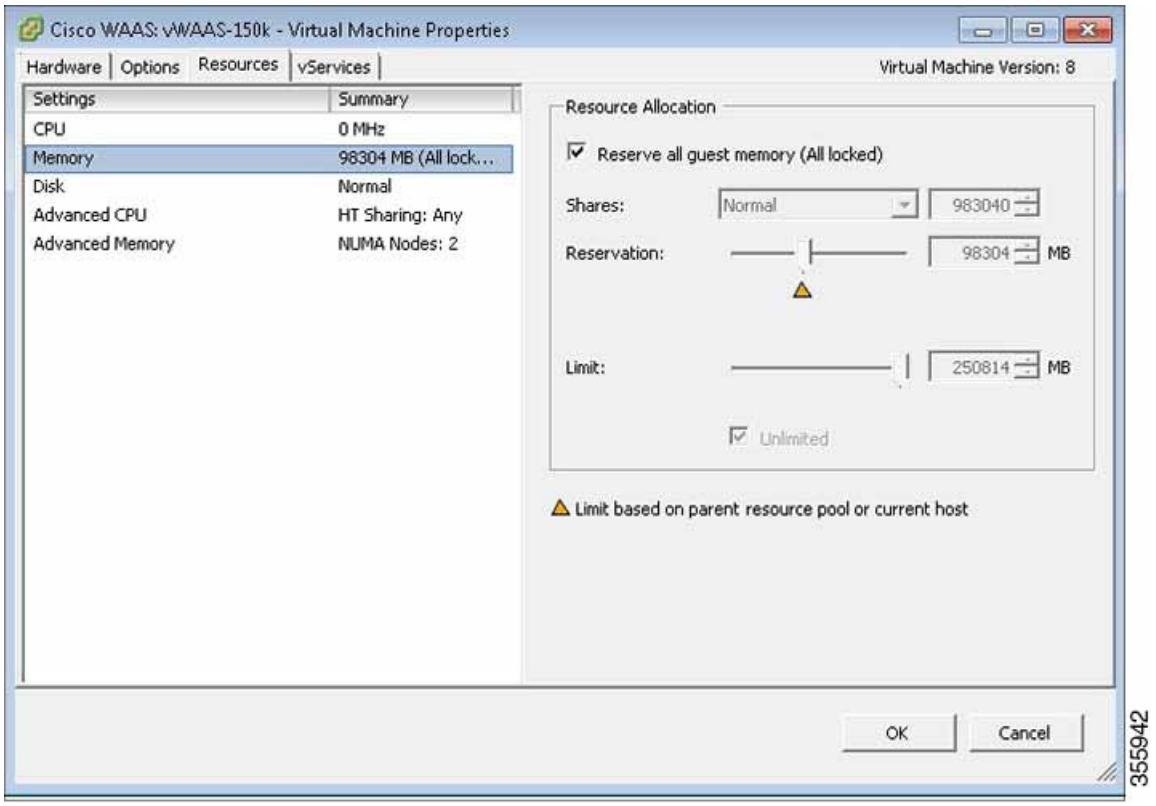
Step 3 Right-click and choose **Edit Settings**.

Step 4 Click the **Virtual Machine Properties** > **Resources** tab.

Step 5 At the **Settings** listing, select **Memory**.

The **Resource Allocation** window is displayed (Figure 2-3).

Figure 2-3 Cisco vWAAS Resource Allocation Window



Step 6 Click **Reserve all guest memory**.

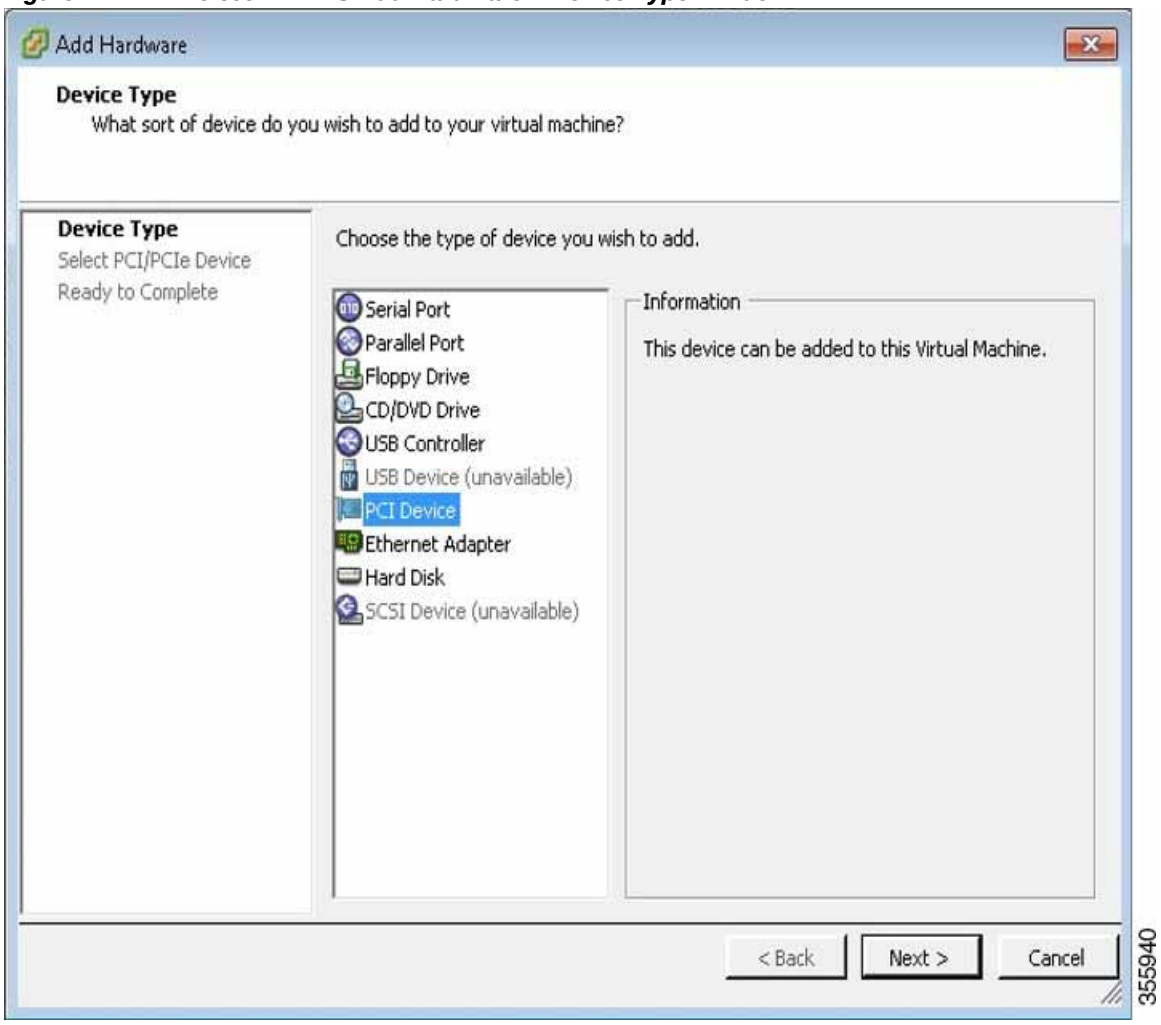
Step 7 Click **OK**.

Step 8 Click the **Virtual Machine Properties** > **Hardware** tab.

Step 9 Click **Add**.

The **Device Type** window is displayed (Figure 2-4).

Figure 2-4 Cisco vWAAS Add Hardware > Device Type Window

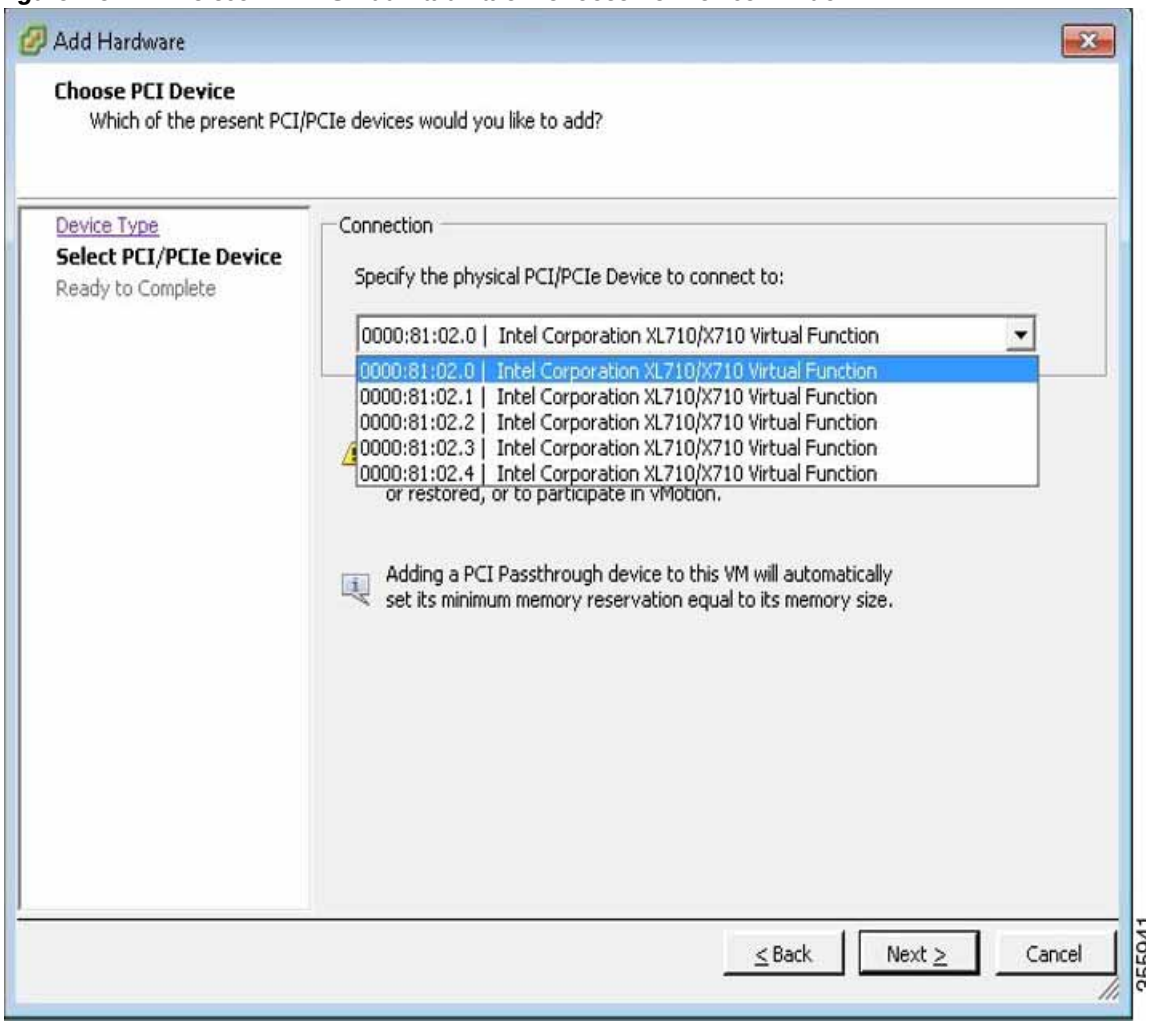


Step 10 For device type, select **PCI Device**.

Step 11 Click **Next**.

The **Choose PCI Device** window is displayed (Figure 2-5).

Figure 2-5 Cisco vWAAS Add Hardware > Choose PCI Device Window



Step 12 From the drop-down list, choose the virtual function you want to connect to.

Step 13 Click **Next**.

Step 14 Click **Finish**.

Step 15 To begin using the virtual function, start the VM.

Upgrade and Downgrade Guidelines for Cisco vWAAS

This section contains the following upgrade and downgrade topics for vWAAS and vCM models.

- Downgrade Guidelines for Cisco vWAAS, page 2-21

For information on the upgrade or downgrade process for WAAS and vWAAS devices, see *Release Notes for Cisco Wide Area Application Services*.

Upgrade Guidelines for Cisco vWAAS and Cisco vWAAS Nodes

Considering the following upgrade guidelines for Cisco vWAAS and Cisco vWAAS nodes.

- When upgrading Cisco vWAAS, do not upgrade more than five Cisco vWAAS nodes at the same time on a single Cisco UCS device. Upgrading more than five Cisco vWAAS nodes at the same time may cause the Cisco vWAAS devices to go offline and to diskless mode.
- Cisco vWAAS in Cisco WAAS Version 6.4.1 requires additional resources before upgrading from Cisco vWAAS in Cisco WAAS Version 6.2.3d to Cisco vWAAS in Cisco WAAS Version 6.4.1.
  - Upgrading from the Cisco WAAS Central Manager: If you initiate and complete the upgrade from the WAAS Central Manager without increasing resources for Cisco vWAAS, alarms (CPU and RAM) to indicate insufficient resource allocation is displayed on the Cisco WAAS Central Manager *after* the upgrade process is completed. No alarms are displayed at the beginning of the upgrade process.
  - Upgrading from the Cisco WAAS CLI: If you initiate an upgrade to Cisco WAAS Version 6.4.1 with the Cisco WAAS CLI, a warning about insufficient resources is displayed at the *start* of the upgrade process.

Cisco vWAAS Upgrade and SCSI Controller Type

If the virtual host was created using an OVA file of Cisco vWAAS in Cisco WAAS Version 5.0 or earlier, and you have upgraded Cisco vWAAS in Cisco WAAS, you must verify that the **SCSI Controller Type** is set to **VMware Paravirtual**. Otherwise, Cisco vWAAS boots with no disk available and fails to load the specified configuration.

If needed, change the **SCSI Controller Type** to **VMware Paravirtual** by following these steps:

Step 1 Power down the Cisco vWAAS.

Step 2 From the **VMware vCenter**, choose **vSphere Client** > **Edit Settings** > **Hardware**.

Step 3 Select **SCSI controller 0**.

Step 4 From the **Change Type** drop-down list, verify that the **SCSI Controller Type** is set to **VMware Paravirtual**. If this is not the case, choose **VMware Paravirtual**.

Step 5 Click **OK**.

Step 6 Power up the Cisco vWAAS in Cisco WAAS Version 5.2.1 or Cisco WAAS 6.1.x or later. (Cisco WAAS Version 6.1.x is the earliest version supported.)

Cisco vWAAS Upgrade and Cisco vCM-100 with RHEL KVM or KVM on CentOS

Consider the following guidelines for upgrading a Cisco vWAAS or Cisco vCM-100 with RHEL KVM or KVM on CentOS.

If you upgrade to Cisco WAAS Version 5.2.1 or downgrade from Cisco WAAS Version 5.2.1, and use a Cisco vCM-100 model with the following parameters, the Cisco vCM-100 may not come up due to boot order errors in the Globally Unique Identifiers (GUID) Partition Table (GPT).

- Cisco vCM-100 has default memory size of 2 GB.
- Cisco vCM-100 uses the RHEL KVM or KVM on CentOS hypervisor.
- You use the **restore factory-default** command or the **restore factory-default preserve basic-config** command.
- If you are upgrading a Cisco vCM-100 model to Cisco WAAS Version 5.2.1, the upgrade process on this type of configuration will automatically clear system and data partition.
  - If you upgrade the Cisco vCM device to WAAS Version 5.2.1 via the console: A warning message similar to the following will be displayed:

    ```
    WARNING: Upgrade of vCM device to 6.2.0 (or) higher version with '/sw' and
    '/swstore' size less than 2GB will clear system and data partition.
    ```

  - If you upgrade the Cisco vCM device to WAAS Version 5.2.1 using the Cisco WAAS Central Manager GUI: A warning message is not displayed.
- The **restore factory-default** command erases the user-specified information that is stored in the flash image, including the starting configuration of the device, and also removes data from the disk, user-defined partitions, and the entire Cisco WAAS Central Manager database.

  To resolve this situation, follow these steps:

  1. Power down the Cisco vWAAS using the **virsh destroy** *vmname* command or the virt manager.
  2. Power up the Cisco vWAAS using the **virsh start** *vmname* command or the virt manager.

Note This upgrade/downgrade scenario does not occur for Cisco vCM-100 models whose memory size is upgraded to 4 GB.

Migrating a Physical Appliance Being Used as a Cisco WAAS Central Manager to a Cisco a vCM

To migrate a physical appliance being used as a primary Cisco WAAS Central Manager to a Cisco vCM, follow these steps:

Step 1 Introduce Cisco vCM as the Cisco WAAS Standby Central Manager by registering it with the Cisco WAAS Primary Central Manager.

Step 2 Configure both device and device-group settings through the Cisco WAAS Primary Central Manager and ensure that devices are getting updates. Wait for two to three data-feed poll rates so that the Cisco WAAS Standby Central Manager gets configuration sync from the Cisco WAAS Primary Central Manager.

Step 3 Ensure that the Cisco WAAS Primary Central Manager and Cisco WAAS Standby Central Manager updates are working.

Step 4 Switch over Cisco WAAS Central Manager roles so that Cisco vCM works as Primary WAAS Central Manager. For additional details, see *"Converting a Standby Central Manager to a Primary Central Manager"*.

Downgrade Guidelines for Cisco vWAAS

Consider the following downgrade guidelines for Cisco vWAAS.

- The Cisco vWAAS models Cisco vCM-500N and Cisco vCM-1000N, introduced in Cisco WAAS Version 5.5.1, cannot be downgraded to a version earlier than Cisco WAAS Version 5.5.1.
- On the Cisco UCS E-Series Server Module running Cisco vWAAS, downgrading to a version earlier than Cisco WAAS Version 5.1.1 is not supported. On other Cisco vWAAS devices you cannot downgrade to a version earlier than Cisco WAAS Version 4.3.1.

Note If the Cisco vWAAS device is downgraded from Cisco vWAAS in Cisco WAAS Version 6.4.1a to Cisco WAAS Version 6.2.3x or from Cisco vWAAS in Cisco WAAS Version 6.x to 5.x, the WAAS alarm **filesystem_size_mismatch** is displayed. This indicates that the partition was not created as expected. To clear the alarm, use the **disk delete-data-partitions** command to re-create the DRE partitions.