



Configuring Cisco vWAAS and Viewing vWAAS Components

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

This chapter contains the following sections:

- [Configuring vWAAS](#)
- [Identifying a vWAAS Device](#)
- [vWAAS System Partitions](#)
- [Operating Considerations for vWAAS and WAAS](#)
- [vWAAS with SR-IOV](#)
- [vWAAS Upgrade and Downgrade Considerations](#)

Configuring vWAAS

This section contains the following topics:

- [Configuring vWAAS Settings](#)
- [Configuring vWAAS Traffic Interception](#)

Configuring vWAAS Settings

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

- IP address and netmask
- Default gateway
- Central Manager address
- Settings for corresponding VLAN in VM for network reachability
- CMS (Centralized Management System)
- Traffic interception (described in [Configuring vWAAS Traffic Interception](#))

To configure vWAAS settings, follow these steps:

-
- Step 1** In the vSphere Client, choose the **Console** tab and log in to the vWAAS console. The username is **admin**, and password is **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 vWAAS for WAAS Version 6.1.x and later, the vWAAS and vCM devices require both virtual (network) interfaces to be present. One or both virtual interfaces may be active for the vWAAS and 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 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** vWAAS registration with the Central Manager is mandatory before traffic can be optimized.

---



- Step 6** Configure traffic interception: WCCP, AppNav, or L2 Inline. For more information on traffic interception methods for vWAAS, see [Configuring vWAAS Traffic Interception](#).
- 

## Configuring vWAAS Traffic Interception

You can configure the following traffic interception methods for vWAAS. [Table 2-1](#) provides descriptions of each traffic interception method.

- WCCP—Available for vWAAS with all WAAS versions.
- AppNav—Available for vWAAS with all WAAS versions
- L2 Inline—Available for WAAS Version 6.2.x and later, for vWAAS with RHEL KVM. [Table 2-2](#) shows the commands for configuring and displaying information on L2 Inline interception for vWAAS.

Table 2-1 Traffic Interception Methods for vWAAS

| Traffic Interception Method | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| WCCP                        | <p>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.</p> <p>WCCP uses a WCCP-enabled router or L3 switch.</p> <p> <b>Note</b> You can configure WCCP-GRE or L2 Inline as the redirection method for vWAAS running on a UCS-E inside a Cisco ISR G2, where the UCS-E interface is configured as IP unnumbered in IOS.</p> <p>For more information on WCCP, see Chapter 5, “Configuring Traffic Interception” in the <i>Cisco Wide Area Application Services Configuration Guide</i>.</p>                                                                                                                                                                                                                                 |
| AppNav                      | <p>A policy and class-based traffic interception method that reduces dependency on the intercepting switch or router by distributing traffic among WAAS devices for optimization.</p> <p>For more information on AppNav, see Chapter 4, “Configuring AppNav” and Chapter 5, “Configuring Traffic Interception” in the <i>Cisco Wide Area Application Services Configuration Guide</i>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| L2 Inline                   | <p>Places the 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.</p> <p>The vWAAS interfaces, with virtual NICs, appear as virtual interfaces in the WAAS CM 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.</p> <p> <b>Note</b> L2 Inline interception is available for vWAAS for RHEL KVM, for WAAS Version 6.2.1 and later. For vWAAS, L2 Inline interception does not include fail-to-wire capability.</p> <p>For more information on configuring L2 Inline interception on the WAAS CM, see Chapter 5, “Configuring Traffic Interception” in the <i>Cisco Wide Area Application Services Configuration Guide</i>.</p> <p>Table 2-2 shows the commands for configuring and displaying information on L2 Inline interception for vWAAS.</p> |

**Table 2-2** CLI Commands for L2 Inline Traffic Interception

| Mode                    | Command                                    | Description                                                                                                                                                                                                                                                                                                     |
|-------------------------|--------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Global Configuration    | <b>(config) interception-method inline</b> | Enables L2 inline traffic interception on vWAAS.                                                                                                                                                                                                                                                                |
| Interface Configuration | <b>(config-if) cdp</b>                     | Enables CDP (Cisco Discovery Protocol) on the interface on a WAAS device. (To globally enable the CDP interval and holdtime options, use the <b>cdp</b> global configuration command.)                                                                                                                          |
|                         | <b>(config-if) description</b>             | Configures the description for a network interface.                                                                                                                                                                                                                                                             |
|                         | <b>(config-if) encapsulation</b>           | Sets the encapsulation type for the interface.                                                                                                                                                                                                                                                                  |
|                         | <b>(config-if) exit</b>                    | Terminates interface configuration mode and returns you to global configuration mode.                                                                                                                                                                                                                           |
|                         | <b>(config-if) inline</b>                  | Enables inline traffic interception for an inlineGroup interface.<br><br>For more information on the <b>inline</b> interface configuration command, including specifying an inline group and inline interception for VLAN IDs, see the <a href="#">Cisco Wide Area Application Services Command Reference</a> . |
|                         | <b>(config-if) ip</b>                      | Configures the IPv4 address or subnet mask on the interface of a WAAS device, or negotiates an IP address from DHCP on the interface of a WAAS device.                                                                                                                                                          |
|                         | <b>(config-if) ipv6</b>                    | Configures the IPv6 address on the interface of a WAAS device, or negotiates an IP address from DHCP on the interface of a WAAS device.                                                                                                                                                                         |
|                         | <b>(config-if) load-interval</b>           | Configures the interval at which to poll the network interface for statistics,                                                                                                                                                                                                                                  |
|                         | <b>(config-if) shutdown</b>                | Shuts down a specific hardware interface on a WAAS device.                                                                                                                                                                                                                                                      |
| EXEC                    | <b>show interception-method</b>            | Displays the configured traffic interception method.                                                                                                                                                                                                                                                            |
|                         | <b>show interface InlineGroup</b>          | Displays inline group information and the slot and inline group number for the selected interface.                                                                                                                                                                                                              |
|                         | <b>show interface inlineport</b>           | Displays the inline port information and the slot and inline group number for the selected interface.                                                                                                                                                                                                           |
|                         | <b>show running-config</b>                 | Display the current running configuration.                                                                                                                                                                                                                                                                      |

For more information on these commands, see the [Cisco Wide Area Application Services Command Reference](#).

## Identifying a vWAAS Device

This section has the following topics:

- [Identifying a vWAAS Model](#)

- [Identifying a vWAAS Device on the Central Manager](#)
- [Identifying a vWAAS Device with the WAAS CLI](#)

## Identifying a vWAAS Model

As shown in [Table 2-3](#), a vWAAS model is determined by two features: the number of vCPUs and the maximum number of TCP connections.

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

| vWAAS Model                                   | Number of vCPUs | Maximum Number of TCP Connections |
|-----------------------------------------------|-----------------|-----------------------------------|
| vWAAS-150                                     | 1               | 200                               |
| 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<br>(earliest WAAS Version 6.4.x) | 4               | 6,000                             |
| vWAAS-12000                                   | 4               | 12,000                            |
| vWAAS-50000                                   | 8               | 50,000                            |

## Identifying a vWAAS Device on the Central Manager

There are two screens on the Central Manager that show identifying information for a vWAAS device. [Table 2-4](#) shows the displayed vWAAS device types.

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

**Table 2-4** vWAAS Device Types shown in Central Manager and CLI

| vWAAS Device               | vWAAS Device Type shown in Central Manager |
|----------------------------|--------------------------------------------|
| vWAAS on VMware ESXi       | OE-VWAAS-ESX                               |
| vWAAS on Microsoft Hyper-V | OE-VWAAS-HYPERV                            |
| vWAAS on RHEL KVM          | OE-VWAAS-KVM                               |
| vWAAS on KVM on CentOS     | OE-VWAAS-KVM                               |
| vWAAS on Microsoft Azure   | OE-VWAAS-AZURE                             |

## Identifying a vWAAS Device with the WAAS CLI

Table 2-5 shows the commands used to display vWAAS device information: For more information on these commands, see the [Cisco Wide Area Application Services Command Reference](#).

Table 2-5 CLI Commands for vWAAS Device Information

| CLI EXEC Command | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| show version     | <p>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.</p> <ul style="list-style-type: none"> <li>• (Optional) Use <b>show version last</b> to display version information for the last saved image.</li> <li>• (Optional) Use <b>show version pending</b> to display version information for the pending upgraded image.</li> </ul>                     |
| show hardware    | <p>Displays system hardware status for the vWAAS device, including:</p> <ul style="list-style-type: none"> <li>• startup date and time, the run time since startup, microprocessor type and speed, and a list of disk drives.</li> </ul>                                                                                                                                                                                                                                                                                |
| show tfo detail  | <p>Displays TCP Fast Open (TFO) information, including:</p> <ul style="list-style-type: none"> <li>• State—Registered or Not Registered</li> <li>• Default Action—Drop or Use</li> <li>• Connection Limit—The maximum TFO connections handled before new connection requests are rejected.</li> <li>• Effective Limit—The dynamic limit relating to how many connections are handled before new connection requests are rejected.</li> <li>• Keepalive Timeout—The connection keepalive timeout, in seconds.</li> </ul> |

## vWAAS System Partitions

For all vWAAS models the system partition size for /sw and /swstore is increased from 1 GB to 2GB. Note the following considerations for the new system partition size:

- The **disk delete-preserve-software** command deletes all disk partitions and preserves the current software version.
- The partition size of 2GB 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 would lead to a file system size mismatch.

For detailed information on Object Cache data partitions and Akamai Cache data partitions, see Chapter 15, “Maintaining Your WAAS System” in the [Cisco Wide Area Application Services Configuration Guide](#).

# Operating Considerations for vWAAS and WAAS

Consider the following guidelines when using Cisco vWAAS with WAAS:

- For vWAAS for WAAS Version 6.1.x and later, the vWAAS and vCM devices require both virtual (network) interfaces to be present, but both need not be active. If only one virtual interface is active, the vWAAS and vCM devices will not be operational after power up. For more information, see [Configuring vWAAS](#).
- If the virtual host was created using an OVA file of vWAAS for WAAS Version 5.0 or earlier, and you have upgraded vWAAS within WAAS, you must verify that the SCSI Controller Type is set to VMware Paravirtual. Otherwise, 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 vWAAS.
- b. From the VMware vCenter, navigate to 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 vWAAS, with WAAS Version 6.1.x or later.

## vWAAS with SR-IOV

This section has the following topics:

- [About SR-IOV](#)
- [Interoperability and Platforms Supported for vWAAS with SR-IOV](#)
- [Upgrade/Downgrade Considerations for vWAAS with SR-IOV](#)
- [Deploying vWAAS with SR-IOV](#)

## About SR-IOV

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 DMA streams for each virtual machine.
- 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 | <ul style="list-style-type: none"> <li>• A full PCI Express (PCIe) function that includes the SR-IOV extended capability, which is used to configure and manage the SR-IOV functionality.</li> <li>• Physical Functions are discovered, managed, and configured as normal PCIe devices. Physical Functions configure and manage the SR-IOV functionality by assigning Virtual Functions.</li> </ul> |
| Virtual Functions  | <ul style="list-style-type: none"> <li>• A lightweight PCIe function that contains all the resources necessary for data movement, but has a carefully minimized set of configuration resources.</li> <li>• Each Virtual Function is derived from a Physical Function. The number of Virtual Functions an Ethernet controller can have is limited by the device hardware.</li> </ul>                 |

## Interoperability and Platforms Supported for vWAAS with SR-IOV

This section contains the following topics:

- [WAAS Central Manager and vWAAS with SR-IOV](#)
- [Platforms Supported for vWAAS with SR-IOV](#)

### WAAS Central Manager and vWAAS with SR-IOV

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

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

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

### Platforms Supported for vWAAS with SR-IOV

[Table 2-7](#) shows the WAAS version and platforms supported for vWAAS with SR-IOV.



**Note**

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.



**Note**

The supported firmware version for Intel X710 NIC is 5.05



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

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

## Upgrade/Downgrade Considerations for vWAAS with SR-IOV

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

- Upgrade Consideration
  - The upgrade procedure for vWAAS instances with SRIOV is the same as for any other vWAAS devices.
- Downgrade Considerations
  - Before a downgrade from Version 6.4.1x or 6.4.3 to an earlier version, from the host, remove SR-IOV interfaces from the devices that will not support this functionality when operating in an earlier WAAS version. Downgrade of vWAAS instances with SR-IOV is blocked for unsupported WAAS versions. [Table 2-7](#) displays minimum WAAS versions supported for SR-IOV.
  - *At the device level*, if you downgrade a vWAAS instance with SR-IOV to a version earlier than 6.4.1x or 6.4.3 (depending on your 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 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 vWAAS instances with SR-IOV is blocked for unsupported WAAS versions.

For more information on the upgrade or downgrade process, see the [Release Note for Cisco Wide Area Application Services](#).

## Deploying vWAAS with SR-IOV

This section contains the following topics:

- [Deploying vWAAS with SR-IOV on KVM](#)
- [Deploying vWAAS with SR-IOV on ESXi](#)

## Deploying vWAAS with SR-IOV on KVM

This section contains the following topics:

- [Configuring Host Settings for vWAAS on KVM \(CentOS or RHEL\) with SR-IOV for UCS C-Series](#)

- [Deploying vWAAS with SR-IOV on KVM \(CentOS or RHEL\) Using Deployment Script for UCS C-Series](#)
- [Deploying vWAAS with SR-IOV on KVM Using NFVIS Portal for ENCS-W Series](#)

### Configuring Host Settings for vWAAS on KVM (CentOS or RHEL) with SR-IOV for UCS C-Series

One-time host settings are required to use the SR-IOV functionality on KVM Hypervisor for UCS C-Series.

To configure the required host settings for deploying vWAAS on KVM with SR-IOV, follow these steps:

- 
- Step 1** Enable Intel Virtualization Technology for Directed I/O (VT-d) in the host BIOS.
- Enable VT-d:
- Use the command `cat /proc/cpuinfo | grep -E 'vmx|svm' | wc -l` to verify that you have enabled VT-d. The command value should be greater than 0.
- Step 2** Enable I/O MMU:
- In the file `/etc/default/grub`, add `intel_iommu=on` to `GRUB_CMDLINE_LINUX`.
  - After you make changes to `GRUB_CMDLINE_LINUX`, the following will be displayed:  
`GRUB_CMDLINE_LINUX="crashkernel=auto rd.lvm.lv=centos/root rd.lvm.lv=centos/swap rhgb quiet intel_iommu=on"`
  - For the changes to take effect, compile: `grub2-mkconfig -o /boot/grub2/grub.cfg`.
  - Reboot the host.
- Step 3** Enable SR-IOV Virtual Functions (for more information on Virtual Functions, see [About SR-IOV](#)).
- Enable SR-IOV VFs:
- 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`.
  - Set the desired number of Virtual Functions at `/sys/class/net/enp1s0f0/device/sriov_numvfs`.
    - On `enpls0f0`:  
`echo 7 > /sys/class/net/enp1s0f0/device/sriov_numvfs`
- Step 4** Remove SR-IOV configuration:
- If you need to remove SR-IOV configuration for a specific interface, for example, `enp1s0f0`, use the command `echo 0` at `/sys/class/net/enp1s0f0/device/sriov_numvfs`, and also remove the lines with `enp1s0f0` interface name present in `/etc/rc.d/rc.local`.
- 

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

vWAAS on KVM for SR-IOV is deployed using `launch.sh` script file on UCS C-Series.

To deploy vWAAS on KVM with SR-IOV functionality using the deployment script, follow these steps (from the `launch.sh` script file output):

- 
- Step 1** To check the pre-requisite host configuration, run the following command:

**./launch.sh check**

**Step 2** To launch 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 vWAAS(not vCM) with SRIOV interface(s), run the following command:

```
./launch.sh <VM_NAME> <INTF_TYPE> <INTF1_NAME> <INTF_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 vWAAS with SR-IOV on KVM Using NFVIS Portal for ENCS-W Series

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

**Step 1** At the Cisco Enterprise NFV Solution, navigate to the **VM Deployment** tab.

**Step 2** The VM Deployment screen 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 Row

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 shows **1 Images** highlighted.



**Note**

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

**Step 3** To register the VM image, at the **VN Name** field, enter the name of the VM.

**Step 4** From the List of Images on the Device table listing, select an image for the VM that will be deployed, or click **Upload** to upload an image.

**Step 5** Click **Next**.

**Step 6** The VM Deployment navigation row shows **2 Profiles** highlighted.

**Step 7** The Profiles screen is displayed, showing the Select Profiles table listing, which has columns for profile name, CPUs, memory (in MB), and disk size (in MB).

**Step 8** 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.

- If you click “+” to create a new profile, a new, empty row is displayed for you to enter information.
- Click **Save** to create the new profile.

- Step 9** Click **Next**.
- Step 10** The VM Deployment navigation row shows **3 Networks** highlighted.
- Step 11** The Select Network Interface screen is displayed, showing the Select Network Interface table listing, which has columns for VNIC number and network name.
- Step 12** 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/created in Steps 1-5, or click “+” to add a new VNIC for the specified VM.
- a. If you click “+” to create a new VNIC, a new empty row is displayed for you to enter information.
  - b. Click **Save** to create the new VNIC.
- Step 13** The VM Deployment navigation row still shows **3 Networks** 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, you must separate the VLAN numbers with a comma and no space, for example, “100,200”.
  - To associate multiple ports with a network, you must 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 for that network and bridge row. Click **Delete**. The page automatically refreshes (there is no confirmation question). You can delete one network and bridge at a time.
- Step 14** Click **Next**.
- Step 15** The VM Deployment navigation row shows **4 Configuration** highlighted.
- The Port Forwarding (Optional) screen is displayed.
- Step 16** At the **Port Number** field, enter the number of the port for port forwarding.
- Step 17** At the **External Port Number** field, enter the number of the external port. The external port is accessible from the WAN bridge only.
- Step 18** Click **Next**.
- Step 19** The VM Deployment navigation row shows **5 Review & Deploy** highlighted.
- The following message is displayed: **Starting VM deployment. Redirecting to Status Page.**
- Step 20** Click **OK**.
- Step 21** The page refreshes and the Status Page 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 22** After deployment is complete, use the Management tab to manage the VM with tasks including power off, power on, reboot, and delete.

## Deploying vWAAS with SR-IOV on ESXi

This section contains the following topics:

- [Configuring Host Settings for vWAAS with SR-IOV on ESXi for UCS C-Series](#)
- [Configuring SR-IOV Interfaces for vWAAS on ESXi for UCS-C Series](#)

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

Before you begin, note the ESXi host requirements, as shown in [Table 2-8](#):

**Table 2-8** *ESXi Host Requirements for vWAAS with SR-IOV for 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 VF in ESXi, follow these steps:

- Step 1** Enable and login to the ESXi shell.
- Step 2** Execute the `lspci | grep -i intel | grep -i 'ethernet\|network'` command. Note the port order of this command.
- Step 3** Use the following command to create VFs:

```
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.

Example1:

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

Example2:

```
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:

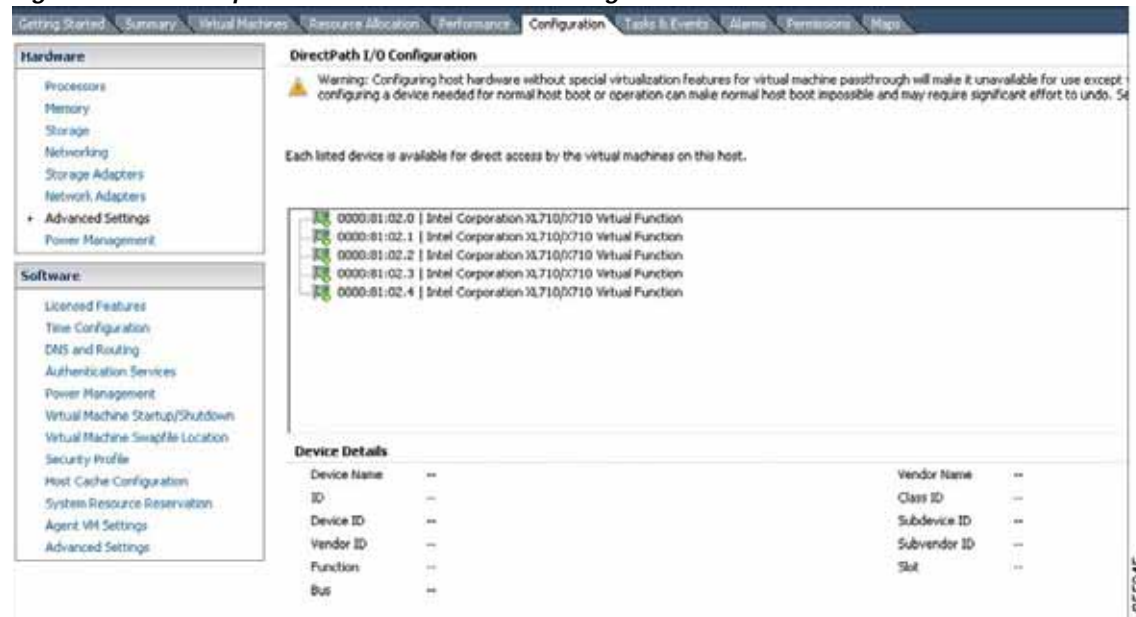
```
[root@localhost:~]
[root@localhost:~] esxcli system module parameters list -m i40e
Name Type Value Description

RSS array of int Number of Receive-Side Scaling Descriptor Queues: 0 = disable/default, 1-4 = enable (number of cpus)
VMQ 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_rpool_initial int Driver's minimum private socket buffer memory pool size.
skb_rpool_max int Maximum attainable private socket buffer memory pool size for the driver.
[root@localhost:~]
[root@localhost:~]
```

355944

- Step 5** To create the VFs, reboot the host.
- Step 6** After the reboot is complete, you can verify the VFs by using:
- the **lspci** command or
  - the vSphere client DirectPath I/O Configuration screen ([Figure 2-2](#))  
Navigate to **Host > Configuration > Hardware > Advanced Settings**.

Figure 2-2 vSphere Client DirectPath I/O Configuration Screen



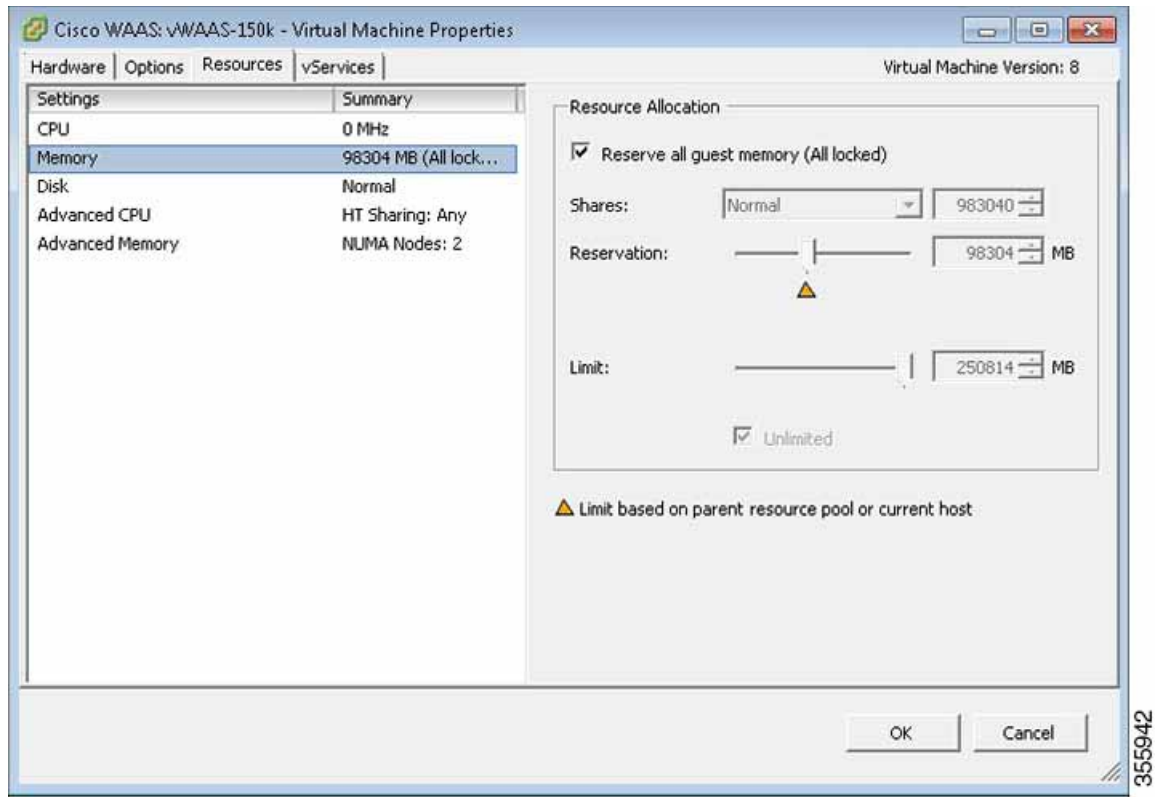
### Configuring SR-IOV Interfaces for vWAAS on ESXi for UCS-C Series

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

- Step 1** After deploying vWAAS, power down the vWAAS.
- Step 2** Right-click and choose **Edit Settings**.
- Step 3** Navigate to **Virtual Machine Properties > Resources** tab.
- Step 4** At the listing, choose **Memory**.

The Memory Resource Allocation screen is displayed (Figure 2-3).

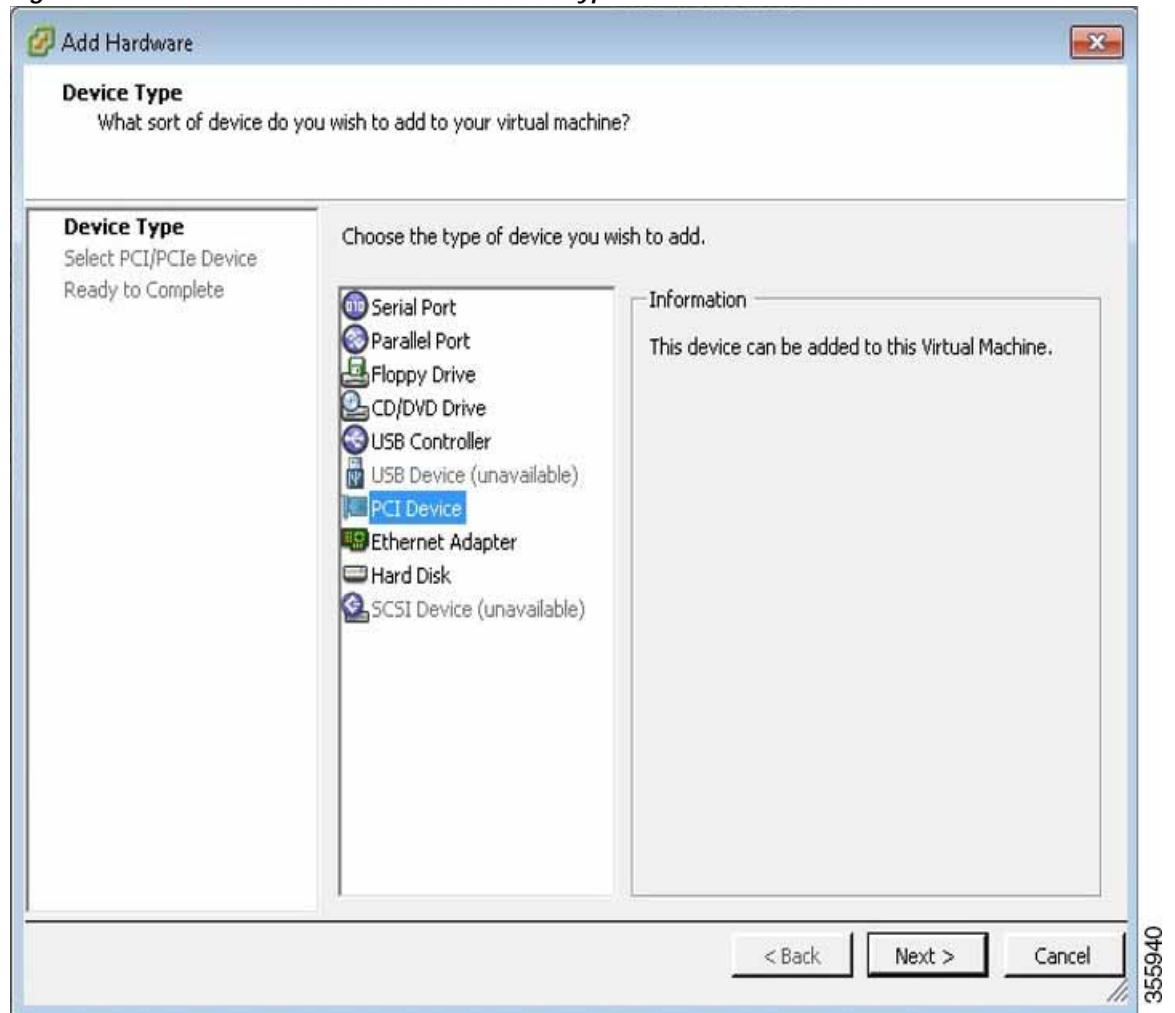
Figure 2-3 vWAAS Memory Resource Allocation Screen



- Step 5 Click **Reserve all guest memory**.
  - Step 6 Click **OK**.
  - Step 7 Navigate to **Virtual Machine Properties > Hardware** tab.
  - Step 8 Click **Add**.
- The Device Type screen is displayed (Figure 2-4).



Figure 2-4 vWAAS Add Hardware &gt; Device Type Screen

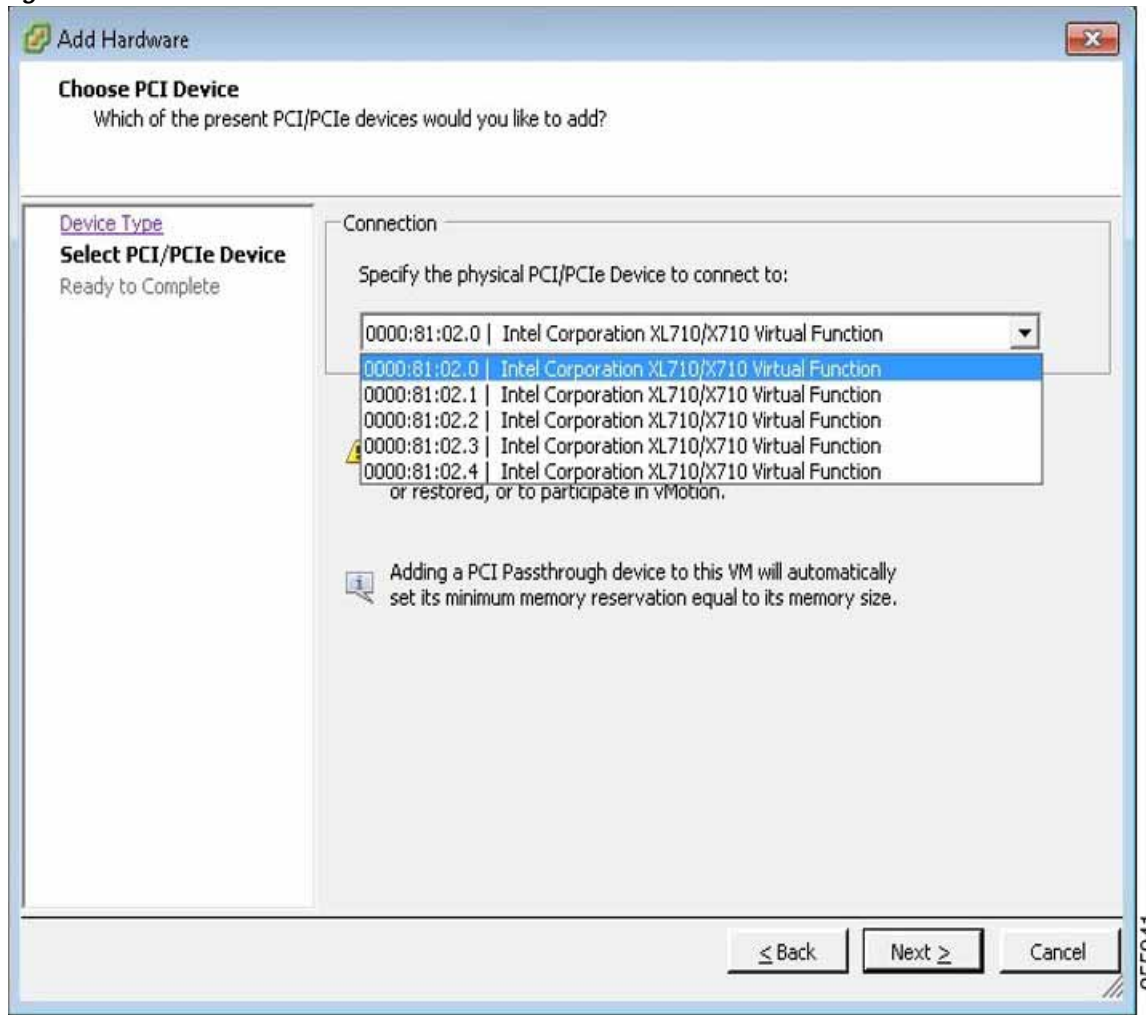


**Step 9** For device type, select **PCI Device**.

**Step 10** Click **Next**.

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

Figure 2-5 vWAAS Add Hardware &gt; Choose PCI Device Screen



- Step 11 Choose the VF you want to connect to.
- Step 12 Click **Next**.
- Step 13 Click **Finish**.
- Step 14 To begin using the VF, start the VM.

## vWAAS Upgrade and Downgrade Considerations

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

For full information on the upgrade or downgrade process for WAAS and vWAAS devices, see the [Release Note for Cisco Wide Area Application Services](#).

- [vWAAS Upgrade and vWAAS Nodes](#)
- [vWAAS Upgrade and SCSI Controller Type](#)
- [vWAAS Upgrade and vCM-100 with RHEL KVM or KVM on CentOS](#)

- [Migrating a Physical Appliance Being Used as a WAAS CM to a vCM](#)
- [vWAAS Downgrade Considerations](#)

## vWAAS Upgrade and vWAAS Nodes

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

## vWAAS Upgrade and SCSI Controller Type

If the virtual host was created using an OVA file of vWAAS for WAAS Version 5.0 or earlier, and you have upgraded vWAAS within WAAS, you must verify that the SCSI Controller Type is set to **VMware Paravirtual**. Otherwise, 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:

- 
- Step 1** Power down the vWAAS.
  - Step 2** From the VMware vCenter, navigate to **vSphere Client > Edit Settings > Hardware**.
  - Step 3** Choose **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 vWAAS, with WAAS Version 6.2.3, or WAAS 6.1.x or later. WAAS Version 6.1.x is the minimum version used.
- 

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

If you upgrade to WAAS Version 6.2.3, or downgrade from WAAS Version 6.2.3 to an earlier version, and use a vCM-100 model with the following parameters, the vCM-100 may not come up due to GUID Partition Table (GPT) boot order errors.

- vCM-100 has default memory size of 2 GB
- 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

**Caution**

If you are upgrading a vCM-100 model from an earlier WAAS version to WAAS Version 6.2.3, the upgrade process on this type of configuration will automatically clear system and data partition.

*If you upgrade the vCM device to WAAS Version 6.2.3 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 vCM device to WAAS Version 6.2.3 via the GUI, a warning message is not displayed.*

**Caution**

The **restore factory-default** command erases user-specified information 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 Central Manager database.

To resolve this situation, follow these steps:

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

**Note**

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

## Migrating a Physical Appliance Being Used as a WAAS CM to a vCM

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

- Step 1 Introduce vCM as the Standby Central Manager by registering it to the Primary Central Manager.
- Step 2 Configure both device and device-group settings through Primary CM and ensure that devices are getting updates. Wait for two to three data feed poll rate so that the Standby CM gets configuration sync from the Primary CM.
- Step 3 Ensure that the Primary CM and Standby CM updates are working.
- Step 4 Switch over CM roles so that vCM works as Primary CM. For additional details please refer to “[Converting a Standby Central Manager to a Primary Central Manager](#)” section of the WAAS Configuration Guide.

## vWAAS Downgrade Considerations

Consider the following when you downgrade vWAAS to an earlier WAAS version:

- vWAAS models vCM-500N and vCM-1000N, introduced in WAAS v5.5.1, cannot be downgraded to a version less than v5.5.1.
- On the UCS E-Series Server Module running vWAAS, downgrading to a version earlier than 5.1.1 is not supported. On other vWAAS devices you cannot downgrade to a version earlier than 4.3.1.



---

**Note**

If the vWAAS device is downgraded in the following scenarios:

- from vWAAS for WAAS Version 6.4.1a to WAAS Version 6.2.3x, or
- from vWAAS for WAAS Version 6.x to 5.x

the WAAS alarm `filesystem_size_mismatch` is displayed; it 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.

---

