Cisco vWAAS on RHEL KVM and KVM CentOS

This chapter describes the hypervisors supported for Cisco vWAAS and the procedures used to install each hypervisor on Cisco vWAAS, and contains the following sections:

About vWAAS on RHEL KVM

Cisco vWAAS on RHEL KVM (Red Hat Enterprise Linux Kernel-based Virtual Machine) is a virtual WAAS appliance that runs on a KVM Hypervisor. The Cisco vWAAS on RHEL KVM solution extends the capabilities of ISR-WAAS and vWAAS running on the Cisco UCS-E Series and the ENCS-5400 Series.

- Cisco vWAAS on RHEL KVM is available for vWAAS with WAAS Version 6.2.1 and later,
- Cisco vWAAS on KVM on CentOS (Linux Community Enterprise Operating System) is available for vWAAS with WAAS version 6.2.3x and later.

Note Cisco vWAAS on RHEL KVM can also be deployed as a tar archive (tar.gz) to deploy Cisco vWAAS on Cisco Network Functions Virtualization Infrastructure Software (NFVIS). The NFVIS portal is used to select the tar.gz file to deploy vWAAS.

Supported Host Platforms, Software Versions, and Disk Type

Table 6-1 shows the platforms and software versions supported for vWAAS on Microsoft Hyper-V.

Table 6-1 Platforms and Software Versions Supported for vWAAS on VMware ESXi

PID and Device Type	Minimum WAAS Version	Host Platforms	Minimum Host Version	Disk Type
• PID: OE-VWAAS-KVM • Device Type: OE-VWAAS-KVM	• 6.2x	• Cisco UCS • Cisco UCS-E Series	• RHEL CentOS 7.1	• virtio

vWAAS on KVM System Requirements

vWAAS on RHEL KVM has a predefined configuration with specific requirements for CPU and memory. However, there are some features that are customizable. Table 6-2 shows the supported configuration for vWAAS on RHEL KVM, and, where applicable, highlights the customizable features.

Note Data disk size will vary according to the model shown in Table 9-4, "Hardware Requirements for vWAAS with Akamai Connect." While deploying RHEL KVM, Cisco vWAAS/vCM needs to verify that enough disk space is available in the respective partition.

Table 6-2 vWAAS on RHEL KVM Supported Configuration

Feature/Component	Description
Platform	Three-disk platform of: • 10GB system • 4GB flash • Data disk (customizable, depending on number of connections)
RHEL version for vWAAS on KVM	RHEL 7.2
Memory Requirements	• vWAAS-150: 4 GB • vWAAS-200: 4 GB • vWAAS-750: 4 GB • vWAAS-1300: 6 GB • vWAAS-2500: 8 GB • vWAAS-6000: 11 GB • vWAAS-12000: 18 GB • vWAAS-50000: 48 GB
Interception Method	WCCP (Web Cache Communication Protocol) or Appnav
Device Emulation	vWAAS on RHEL KVM uses QEMU-KVM.
Management	WAAS CM and serial console
Licensing	For information on Cisco vWAAS licensing, please contact your Cisco account representative.
MAC address	Customizable

vWAAS on RHEL KVM for WAAS Version 5.x to 6.2.x

This section contains the following topics:

Tar Archive Package for vWAAS on KVM for WAAS Version 5.x to 6.2.x

For vWAAS on KVM, for WAAS Version 5.x through 6.2.x, Cisco provides a tar archive or NPE tar archive package for each vWAAS connection profile (examples shown in Table 6-3) and for each vCM connection profile (examples shown in Table 6-4).

Table 6-5 shows the files included for deploying Cisco vWAAS on RHEL KVM, and for deploying Cisco vWAAS on NFVIS (Network Functions Virtualization Infrastructure Software). For more information on Cisco NFVIS and Cisco NFV (Network Functions Virtualization), see the *Cisco Enterprise Network Functions Virtualization Solution Overview*. For more information on vWAAS on NFVIS, see Chapter 7, "Cisco vWAAS with Cisco Enterprise NFVIS".

Note For a listing of hypervisor OVA, zip, and tar.gz files for vWAAS, see the Cisco Wide Area Application Services (WAAS) Download Software Page and select the WAAS software version used with your vWAAS instance.

Table 6-3 OVA Package Format Examples for vWAAS on RHEL KVM for WAAS Version 5.x to 6.2.x

Package Format	File Format Example
Cisco KVM 150 package file	• Cisco-KVM-vWAAS-150-6.2.3d-b-68.tar.gz
Cisco KVM 150 package file for NPE	• Cisco-KVM-vWAAS-150-6.2.3d-b-68-npe.tar.gz
Cisco KVM 200 package file	• Cisco-KVM-vWAAS-200-6.2.3d-b-68.tar.gz
Cisco KVM 200 package file for NPE	• Cisco-KVM-vWAAS-200-6.2.3d-b-68-npe.tar.gz
Cisco KVM 750 package file	• Cisco-KVM-vWAAS-750-6.2.3d-b-68.tar.gz
Cisco KVM 750 package file for NPE	• Cisco-KVM-vWAAS-750-6.2.3d-b-68-npe.tar.gz
Cisco KVM 1300 package file	• Cisco-KVM-vWAAS-1300-6.2.3d-b-68.tar.gz
Cisco KVM 1300 package file for NPE	• Cisco-KVM-vWAAS-1300-6.2.3d-b-68-npe.tar.gz
Cisco KVM 2500 package file	• Cisco-KVM-vWAAS-2500-6.2.3d-b-68.tar.gz
Cisco KVM 2500 package file for NPE	• Cisco-KVM-vWAAS-2500-6.2.3d-b-68-npe.tar.gz
Cisco KVM 6000 package file	• Cisco-KVM-vWAAS-6000-6.2.3d-b-68.tar.gz
Cisco KVM 6000 package file for NPE	• Cisco-KVM-vWAAS-6000-6.2.3d-b-68-npe.tar.gz

Table 6-4 Cisco OVA Package Formats for vCM for WAAS Version 5.x to 6.2.x

Package Format	File Format Example
Cisco KVM 100N package file	• Cisco-KVM-vCM-100N-6.2.3d-b-68.tar.gz
Cisco KVM 100N package file for NPE	• Cisco-KVN-vCN-100N-6.2.3d-npe-b-68-npe.tar-gz

Table 6-5 Installation Files for vWAAS on KVM and vWAAS on NFVIS for WAAS 5.x to 6.2.x

Installation Files	RHEL KVM Installation	NFVIS Installation
• **Cisco signature envelope file** Verifies that this deployment is from Cisco.	X	X
• **Manifest file with checksums**	X	X
• **image_properties.xml** A VM configuration template file used on the Cisco NFVIS platform.		X
• **package.mf** template file and **bootstrap-cfg.xml** These two files work together on the Cisco NFVIS platform with the image_properties.xml file as Day-0 configuration template.		X
• **INSTRUCTIONS.TXT** Describes the procedure for deploying the virtual instance and for using the launch.sh file.	X	
• **launch.sh** file For details on how to use this script, see Using the Launch Script to Deploy vWAAS on KVM for WAAS Version 5.x to 6.2.x.	X	
• **vm.xml** Configuration file needed for vWAAS deployment using virtual bridge or Open Virtual Switch (OVS) present in host mac.	X	
• **VM disk images** A 4 GB flash disk, 10 GB system disk, and data disk (data disk size is dependent on your connection profile).	X	X
• **ezdeploy.sh** file The script used to deploy vWAAS on UCS-E. For details on how to use this script, see Using the EzDeploy Script to Deploy vWAAS on KVM on UCS-E for WAAS Version 5.x to 6.2.x and Using the EzDeploy Script to Deploy vWAAS on RHEL KVM on CentOS for WAAS Version 6.4.1 and Later.	X	

Installing vWAAS on KVM for WAAS Version 5.x to 6.2.x

This section contains the following topics:

Using the Launch Script to Deploy vWAAS on KVM for WAAS Version 5.x to 6.2.x

To use the launch script (launch.sh) to deploy Cisco vWAAS on RHEL KVM, follow these steps:

Step 1 Launch the vWAAS VM. (You must have root permissions to launch the vWAAS VM.)

Step 2 Create a new directory to hold the extracted contents of **tar.gz**.

Step 3 Copy **tar.gz** into the specified directory.

Step 4 To extract the **tar.gz** gzip file, use the command:

tar -zxvf Cisco-KVM-vWAAS-*ModelNumber-Version-BuildNumber***.tar.gz**

Example:

```
tar -zxvf Cisco-KVM-vWAAS-200-6.2.3d.b-68.tar.gz
```

The contents of the tar.gz file are:

- INSTRUCTIONS.TXT
- Disk-0.qcow
- Disk-1.qcow
- Disk-2.qcow
- vm_tap.xml
- vm_macvtap.xml
- launch.sh
- ezdeploy.sh
- ezdeploy.qstatus.exp

Step 5 To launch vWAAS, run the **launch.sh** script:

a. To check the prerequisite conditions, use the **./launch.sh check** command.

b. To launch vWAAS using the OVS bridge, use the **./launch.sh** *vm-name* **bridge** *bridge1-name bridge2-name* command.

- *bridge1-name* and *bridge2-name*—The OVS bridges already created in the host.

Note Before using the **./launch.sh** *vm-name* **bridge** *bridge1-name bridge2-name* command, verify that the OVS bridges are created and in working state.

c. To launch vWAAS using macvtap, use the **./launch.sh vm-name macvtap** *interface1-name interface2-name* command,

- *vm-name*—The specified name of the vWAAS VM.
- *interface1-name* and *interface2-name*—The specified Ethernet interfaces of the host machine.

Step 6 The vWAAS is launched

Step 7 To view the vWAAS, use the VM GUI or the **virsh list** command.

Step 8 To connect to the console, use the VM GUI or the **virsh console** *vm-name* command.

Step 9 To power down the vWAAS, use the **virsh destroy** *vm-name* command.

Step 10 To undefine the vWAAS:

a. Use the **virsh undefine** *vm-name* command.

b. Remove the directory with the specified *vm-name*.

Note If you want to create another vWAAS of the same model, follow this procedure again for a different vWAAS. The specified directory, for example, "Basic," will then have two VMs, "Basic1" and "Basic2." Disks for these VMs will be stored in the subdirectories "Basic1" and "Basic2," respectively.

Using the EzDeploy Script to Deploy vWAAS on KVM on UCS-E for WAAS Version 5.x to 6.2.x

Use the EzDeploy script for simplified deployment of a vWAAS. Note that the EzDeploy script is not used for the vCM.

The following are prerequisites for launching the EzDeploy script:

- To launch the vWAAS VM, you must have root permission.
- The following software and utility packages must be installed before using the EzDeploy script:
  - QEMU
  - Libvirt
  - Genisoimage
  - Expect script (required only if you choose to run EzDeploy's capability for auto-monitoring WAAS CM registration status)
- Verify the following:
  - There is enough disk and RAM memory to deploy another vWAAS.
  - Compatibility of software versions.
  - Availability and readiness of network connectivity.

Note Because EzDeploy leverages the launch.sh script to launch a vWAAS, the launch.sh script, as well as all the necessary files associated with it, must be present, intact, and not manually removed or manually moved elsewhere.

To use the EzDeploy script (ezdeploy.sh) to deploy Cisco vWAAS on RHEL KVM on UCS-E, follow these steps:

Step 1 Launch the vWAAS VM.

Step 2 Create a new directory to hold the extracted contents of **tar.gz**.

Step 3 Copy **tar.gz** into the specified directory.

Step 4 To extract the **tar.gz** gzip file, use the **tar -zxvf Cisco-KVM-vWAAS-200-6.2.0.b-80.tar.gz** command.

The contents of the tar.gz file are:

- INSTRUCTIONS.TXT
- Disk-0.qcow
- Disk-1.qcow
- Disk-2.qcow
- vm_tap.xml

- vm_macvtap.xml
- launch.sh
- ezdeploy.sh
- ezdeploy.qstatus.exp

Step 5 Run the **ezdeploy.sh** script:

a. During execution of hte ezdeploy.sh, you are prompted for bootstrap configuration parameters:

- vWAAS KVM name—The name is dependent on whether or not you provide the vWAAS' bootstrap configuration.

  If you do not provide the vWAAS' bootstrap configuration, the name is set as the name of the guest KVM to be created. not the vWAAS' host name.

  If you provide the vWAAS' bootstrap configuration, vWAAS' host name is set and used in both instances.
- vWAAS' local IP address and mask
- Default GW IP address: an address on the ISR-4000 series RP reachable by the vWAAS and having external network connectivity
- IP address of the WAAS CM with which the vWAAS will register
- One NTP server address, without authentication. If you want to have authentication or multiple NTP servers, use the WAAS CM to configure these after the vWAAS is powered up.
- (Optional) DNS server address

The ezdeploy.sh script performs a validation before accepting each parameter.

b. After input collection is completed, the following information is saved:

- The bootstrap configuration is saved in the file **bootstrap-cfg.xml** in the directory created for this KVM.
- The execution log and error log of the script are saved in the file **ezdeploy-log.txt** in the directory created for this KVM.
- For the vWAAS in this KVM, the error log is saved in **errorlog/ezdeploy-errorlog.txt**.

Note By default, all configuration and error logs saved in the specified KVM directory are *not* deleted, even if they have recorded errors, so allow for debugging. If you do not want to generate log files, you must confirm this choice at the end of the script execution, after input entry.

c. After completion of the EzDeploy script, the vWAAS is fully up and running. Registration with the specified WAAS CM and the NTP server are automatically started after installation of their corresponding CLIs.

d. To view the vWAAS, use the VM GUI or the **virsh list** command.

e. To connect to the console, use the VM GUI or the **virsh console** *vm-name* command.

f. To power down the vWAAS, use the **virsh destroy** *vm-name* command.

g. To undefine the vWAAS:

- Use the **virsh undefine** *vm-name* command.
- Remove the directory with the specified *vm-name*.

vWAAS on RHEL KVM for WAAS Version 6.4.1 and Later

This section contains the following topics:

Unified OVA Package for vWAAS on KVM for WAAS Version 6.4.1 and Later

For vWAAS on RHEL KVM for WAAS Version 6.4.x and later, Cisco provides a single, unified OVA or NPE OVA package for each hypervisor type, which can be used with all vWAAS models for that hypervisor.

Each unified OVA package file is a pre-configured virtual machine image that is ready to run on a particular hypervisor. The launch script for each unified OVA package provides the model and other required parameters to launch vWAAS with WAAS in the required configuration.

Here are examples of the unified OVA and NPE OVA package filenames for vWAAS on RHEL KVM:

- OVA—Cisco-KVM-vWAAS-Unified-6.4.1-b-33.tar.gz
- NPE OVA—Cisco-KVM-vWAAS-Unified-6.4.1-b-33-npe.tar.gz

The unified OVA package for vWAAS on RHEL KVM/KVM on CentOS contains the following files.

- Flash disk image
- Data system disk
- Akamai disk
- INSTRUCTIONS.TXT—Describes the procedure for deploying the virtual instance and using the launch.sh file.
- package.mf template file and bootstrap-cfg.xml—These two files work together on the Cisco NFVIS platform with the image_properties.xml file as Day-0 configuration template.
- ezdeploy.sh—The script used to deploy vWAAS on UCS-E.
- exdeploy_qstatus.exp—The dependent file for ezdeploy.sh script image_properties.xmlA VM configuration template file used on the Cisco NFVIS platform.
- launch.sh—The launch script to deploy Cisco vWAAS on Linux KVM.
- vm_macvtap.xml—Configuration file for vWAAS deployment using host machine interfaces with the help of the macvtap driver.
- vm_tap.xml—Configuration file for vWAAS deployment using virtual bridge or OVS (Open Virtual Switch) present in the host machine.

Installing vWAAS on KVM for WAAS Version 6.4.1 and Later

This section contains the following topics:

- Using the EzDeploy Script to Deploy vWAAS on RHEL KVM on CentOS for WAAS Version 6.4.1 and Later

Note For how to install vWAAS with NFVIS on Cisco ENCS 5400 Series, see the ***Cisco vWAAS Bundled Image Upgrade for ENCS 5400 Series, with RMA Process for Cisco EOS/EOL WAVE Devices***.

Using the Launch Script to Deploy vWAAS on RHEL KVM on CentOS for WAAS Version 6.4.1 and Later

To use the launch script (launch.sh) to deploy Cisco vWAAS or vCM on RHEL KVM on CentOS, follow these steps:

Step 1 At **[root@localhost** *hostname***]** enter the following:

```
[root@localhost hostname]# ./launch.sh unified mactap enp1s0f0 enp1s0f0
```

Step 2 The Model Menu is displayed:

```
--- Model Menu ---

1. vWAAS-150
2. vWAAS-200
3. vWAAS-750
4. vWAAS-1300
5. vWAAS-2500
6. vWAAS-6000R
7. vWAAS-6000
8. vWAAS-12000
9. vWAAS-50000
10. vCM-100N
11. vCM-500N
12. vCM-1000N
13. vCM-2000N

Select the model type :
```

Step 3 After you select the vWAAS or vCM model type, the launch script completes the RHEL CentOS KVM deployment.

Using the EzDeploy Script to Deploy vWAAS on RHEL KVM on CentOS for WAAS Version 6.4.1 and Later

To use the ExDeploy script (exdeploy.sh) to deploy Cisco vWAAS or vCM on RHEL KVM on CentOS, for vWAAS models up to 6,000 connections, follow these steps:

Step 1 At **[root@localhost ezdeploy]** enter the following:

```
[root@localhost exdeploy]# ./ezdeploy.sh
```

Step 2 The Model Menu is displayed:

```
--- Model Menu ---

1. vWAAS-150
2. vWAAS-200
```

```
3. vWAAS-750
4. vWAAS-1300
5. vWAAS-2500
6. vWAAS-6000R
7. vWAAS-6000

Select the model type :
```

Step 3 After you select the vWAAS model type, the EzDeploy script completes the RHEL KVM/KVM on CentOS deployment.

Operating Guidelines for vWAAS on KVM/KVM on CentOS

This section contains the following topics:

Interoperability Guidelines for vWAAS on KVM/KVM on CentOS

Consider the following interoperability guidelines for Cisco vWAAS on KVM:

Interoperability guidelines for WAAS versions and vWAAS on KVM:

- **Cisco vWAAS on RHEL KVM** is available for vWAAS with WAAS Version 6.2.1 and later.
- **Cisco vWAAS on KVM on CentOS** (Linux Community Enterprise Operating System) is available for vWAAS on WAAS Version 6.2.3x and later.

Interoperability guidelines for OVS and vWAAS on KVM:

- The CDP protocol is not supported for Open Virtual Switch (OVS) on RHEL KVM on CentOS, therefore the **show cdp** command cannot be used for vWAAS on RHEL KVM on CentOS.
- For vWAAS with WAAS Version 6.2.3x and later, there is inline vWAAS support for the OVS switch, with additional settings in vWAAS. For example
  1. Install CentOS 7.2 on UCS-C240.
  2. Configure OVS switch on KVM host.
  3. Deploy KVM vWAAS OVAs with OVS switch on KVM host.
  4. Power off the vWAAS.
  5. Add two additional interfaces.
  6. Using the virt-manager, map the bridge ID in vWAAS:
     `[root@localhost kvm]# virsh edit vwaas-name`

     Domain vWAAS XML configuration changed.
  7. Using the virt-manager, edit the virtual type:
     virtualport type='openvswitch'/
  8. Sample output:

```
<interface type='bridge'>
      <mac address='52:54:00:ea:3f:7b'/>
```

```
      <source bridge='br2'/>
      <virtualport type='openvswitch'/>
      <model type='virtio'/>
     <address type='pci' domain='0x0000' bus='0x00' slot='0x08' function='0x0'/>
    </interface>
<interface type='bridge'>
      <mac address='52:54:00:7f:7c:99'/>
      <source bridge='br3'/>
      <virtualport type='openvswitch'/>
      <model type='virtio'/>
     <address type='pci' domain='0x0000' bus='0x00' slot='0x0a' function='0x0'/>
    </interface>
```

Traffic Interception Methods for vWAAS on KVM

For traffic interception for Cisco vWAAS on KVM, you can use WCCP (WCCP GRE or WCCP L2) or Appnav.

Note When you use any of the traffic interception methods for vWAAS on KVM, you must disable Generic Receive Offload (GRO) on the Cisco UCS NIC. Use the command **ethtool -K *nic_interface_name* gro off** on KVM host to disable GRO. For example: **`ethtool -K enp3s0f2 gro off`**. If you do not disable GRO, traffic is not recognized, and packets are discarded.

If you upgrade the UCS NIC firmware to the latest version, you do not need to disable the GRO parameter.

For more information on configuring traffic interception methods, see the *Cisco Wide Area Application Services Configuration Guide*.

Upgrade/Downgrade Guidelines for vWAAS on KVM

Consider the following guidelines when upgrading or downgrading your WAAS system with vWAAS on KVM:

- Cisco vWAAS on KVM is used with WAAS Version 6.2.1 and later. You cannot downgrade Cisco vWAAS on KVM or vCM on KVM devices to a version earlier than WAAS Version 6.2.1.

Note 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 diskless mode.

Note For a vCM-100 model used with the RHEL KVM or KVM on CentOS hypervisor, with the default memory size of 2 GB:

When you upgrade to WAAS Version 5.2.1 from an earlier version, or downgrade from WAAS Version

5.2.1 to an earlier version, and use either the **restore factory-default** command or the **restore factory-default preserve basic-config** command, the vCM-100 may not come up due to GUID Partition Table (GPT) boot order errors.

CAUTION: *The **restore factory-default** command erases user-specified configuration 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:

1. Power down the vWAAS using the **virsh destroy** *vmname* command or the virt manager.

2. Power up the vWAAS using the **virsh start** *vmname* command or the virt manager.

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

vWAAS on SUSE Linux for WAAS Version 6.4.1b and Later

This section contains the following topics:

Operating Guidelines for vWAAS in SUSE Linux

Consider the following operating guidelines for vWAAS in SUSE Linux:

- vWAAS in SUSE Linux is supported for vWAAS for WAAS Version 6.4.1b and later.
- vWAAS in SUSE Linux is supported for all vWAAS and vCM models that are supported on KVM on CentOS.
- On the Central Manager, vWAAS devices in SUSE Linux are displayed as OE-VWAAS-GEN-LINUX.
- All vWAAS models for vWAAS in SUSE Linux are deployed with a single, unified OVA. Here are examples of the unified OVA and NPE OVA package filenames for vWAAS in SUSE Linux:
  - OVA—Cisco-KVM-vWAAS-Unified-6.4.1b-b-33.tar.gz
  - NPE OVA—Cisco-KVM-vWAAS-Unified-6.4.1-b-33-npe.tar.gz

Upgrade/Downgrade Guidelines for Cisco vWAAS in SUSE Linux

Consider the following upgrade/downgrade guidelines for Cisco vWAAS in SUSE Linux:

- The procedure for upgrading or downgrading vWAAS in SUSE Linux is the same as for any other WAAS device.
- Downgrading a device or device group for vWAAS in SUSE Linux to a WAAS Version earlier than Version 6.4.1b is not supported.

Deploying Cisco vWAAS in SUSE Linux

This section contains the following topics:

Guidelines for Deploying vWAAS in SUSE Linux

Consider the following guidelines to deploy Cisco vWAAS in SUSE Linux:

For vWAAS on KVM for WAAS Version 6.4.x and later, Cisco provides a single, unified OVA or NPE OVA package for each hypervisor type, which can be used with all vWAAS models for that hypervisor. For vWAAS for WAAS 6.4.1b and later, WAAS supports vWAAS in SUSE Linux.

Here are examples of the unified OVA and NPE OVA package filenames for vWAAS on KVM:

- OVA—Cisco-KVM-vWAAS-Unified-6.4.1-b-33.tar.gz
- NPE OVA—Cisco-KVM-vWAAS-Unified-6.4.1-b-33-npe.tar.gz

For more information about this unified OVA package, see Unified OVA Package for vWAAS on KVM for WAAS Version 6.4.1 and Later.

- After vWAAS in SUSE Linux is operational on a device, you can use the WAAS CM or the WAAS CLI to display the SUSE Linux device.
  - The WAAS CM displays the following information for the device:

    The SUSE Linux device is displayed in the **Devices** > **All Devices** listing under Device Type as OE-VWAAS-GEN-LINUX.

    The SUSE Linux device is displayed in the **Devices** > *device-name* > **Dashboard** as OE-VWAAS-GEN-LINUX.
  - Use the **show hardware** command to display the device, as well as other system hardware status information such as startup date and time, the run time since startup, microprocessor type and speed, and a list of disk drives.

Procedure for Deploying vWAAS in SUSE Linux

The procedure for deploying vWAAS in SUSE Linux is the same as for Installing vWAAS on KVM for WAAS Version 6.4.1 and Later.

vWAAS with SR-IOV

For vWAAS with WAAS Version 6.4.1 and later, vWAAS on KVM (RHEL/CentOS) supports vWAAS with Single-Root I/O Virtualization (SR-IOV). SR-IOV is a standard developed by the Peripheral Component Interconnect Special Interest Group (PCI SIG) to improve virtualization of PCI devices

This section has the following topics:

About vWAAS with SR-IOV

Virtualized WAAS is supported on the Hypervisors VMware ESXi, Microsoft Hyper-V and RHEL/CentOS KVM. The existing vWAAS implementations are based on traditional Ethernet controllers on the host. Ethernet drivers for vWAAS vary from Hypervisor to Hypervisor; for example, vWAAS has virtio_net on KVM, vmxnet3 on VMWARE and netvsc on HyperV.

SR-IOV enables the vWAAS instance 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 6-6 shows the two types of functions used with SR-IOV.

Table 6-6 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 by the device hardware.

Interoperability and Platforms Supported for vWAAS with SR-IOV

This section contains the following topics:

WAAS Central Manager and vWAAS with SR-IOV

For vWAAS for WAAS Version 6.4.1 and later, 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.

On the Central Manager, vWAAS devices on KVM with SR-IOV are displayed as OE-VWAAS-KVM.

Platforms Supported for vWAAS with SR-IOV

Table 6-7 shows the WAAS version and platforms supported for vWAAS with SR-IOV.

Table 6-7 WAAS Version and Platforms Supported for vWAAS with SR-IOV

Hypervisor	Minimum WAAS Version	Ethernet Controller and Network Driver for UCS C-Series	Ethernet Controller and Network Driver for ENCS platforms
KVM on RHEL 7.2 or CentOS 7.2	6.4.1	• Intel I350 Ethernet Controller • Linux igbvf network driver for Intel Ethernet Controller	• Intel X710 Ethernet Controller • Linux i40evf network driver for Intel Ethernet Controller

Upgrade/Downgrade Considerations for vWAAS with SR-IOV

SR-IOV is supported for vWAAS for WAAS Version 6.4.1 and later. Consider the following when you upgrade or downgrade a vWAAS instance with SR-IOV:

- Upgrade Consideration
  - Use the WAAS Central Manager to upgrade the vWAAS instance from a previous release to WAAS Version 6.4.1.
- Downgrade Considerations
  - Before a downgrade from Version 6.4.1 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.
  - *At the device level*, if you downgrade a vWAAS instance with SR-IOV installed to a version earlier than 6.4.1, 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 SR-IOV interfaces will lose connectivity after the downgrade from 6.4.1 to an earlier version.
  - *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 SR-IOV interfaces will lose connectivity after the downgrade from 6.4.1 to an earlier version.

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

Deploying vWAAS on KVM with SR-IOV

This section contains the following topics:

- Configuring Host Settings for vWAAS on KVM with SR-IOV for UCS C-Series
- Deploying vWAAS on KVM with SR-IOV Using Deployment Script for UCS C-Series
- Deploying vWAAS on KVM with SR-IOV Using NFVIS Portal for ENCS Platforms

Configuring Host Settings for vWAAS on KVM 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:

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

b. 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**"

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

d. Reboot the host.

Step 3 Enable SR-IOV Virtual Functions (for more information on Virtual Functions, see About vWAAS with SR-IOV).

Enable SR-IOV VFs:

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 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 on KVM with SR-IOV 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 should be SRIOV, which is for data path.
- where second INTF_TYPE option can be BRIDGE or MACVTAP or SRIOV, which is for management interface.
- INTF1_NAME and INTF2_NAME are the desired names based on the selected INTF_TYPE.

Deploying vWAAS on KVM with SR-IOV Using NFVIS Portal for ENCS Platforms

To deploy vWAAS on KVM with SR-IOV using the NFVIS portal for ENCS platforms, 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 6-1, to highlight where you are in the VM deployment process.

Figure 6-1 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.

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

b. 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.