Cisco Virtual Wide Area Application Services Configuration Guide

WAAS Software Version 6.4.1x
November 22, 2019

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco Virtual Wide Area Application Services Configuration Guide

CONTENTS

Preface

This preface describes who should read the *Cisco Virtual Wide Area Application Services Configuration Guide*, how it is organized, and its document conventions. It contains the following sections:

Audience

This guide is for experienced IT managers and network administrators who are responsible for configuring and maintaining Cisco Virtual Wide Area Application Services (vWAAS).

Document Organization

This guide is organized as follows:

Document Conventions

Command descriptions use these conventions:

boldface font	Commands and keywords are in boldface.
italic font	Arguments for which you supply values are in italics.
[ ]	Elements in square brackets are optional.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.

Screen examples use these conventions:

`screen font`	Terminal sessions and information the switch displays are in screen font.
`boldface screen font`	Information you must enter is in boldface screen font.
italic screen font	Arguments for which you supply values are in italic screen font.
`< >`	Nonprinting characters, such as passwords, are in angle brackets.
`[ ]`	Default responses to system prompts are in square brackets.
`!, #`	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

This document uses the following conventions:

Note Means reader *take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Tip Means t*he following information will help you solve a problem*. Tips might not be troubleshooting or even an action, but could help you save time.

Related Documentation

For additional information on Cisco WAAS software and hardware, see the following documentation:

- *Cisco Wide Area Application Services Upgrade Guide*
- *Cisco Wide Area Application Services Quick Configuration Guide*
- *Cisco Wide Area Application Services Configuration Guide*
- *Cisco Wide Area Application Services Command Reference*

- *Cisco Wide Area Application Services API Reference*
- *Cisco Wide Area Application Services Monitoring Guide*
- *Cisco WAAS on Service Modules for Cisco Access Routers*
- *Cisco SRE Service Module Configuration and Installation Guide*
- *Configuring Cisco WAAS Network Modules for Cisco Access Routers*
- *WAAS Enhanced Network Modules*
- *Using the Print Utilities to Troubleshoot and Fix Samba Driver Installation Problems*
- *Regulatory Compliance and Safety Information for the Cisco Wide Area Virtualization Engines*
- *Cisco Wide Area Virtualization Engine 274 and 474 Hardware Installation Guide*
- *Cisco Wide Area Virtualization Engine 574 Hardware Installation Guide*
- *Regulatory Compliance and Safety Information for the Cisco Content Networking Product Series*
- *Cisco Wide Area Application Engine 512 and 612 Hardware Installation Guide*
- *Cisco Wide Area Application Engine 7326 Hardware Installation Guide*
- *Cisco Wide Area Application Engine 7341, 7371, and 674 Hardware Installation Guide*
- *Installing the Cisco WAE Inline Network Adapter*
- *Cisco Nexus 1000V Software Installation Guide, Release 4.2(1) SV1(4)*
- *Cisco Nexus 1000V Getting Started Guide, Release 4.2(1) SV1(4)*
- *Cisco Nexus 1000V and VMware Compatibility Information, Release 4.2(1) SV1(4)*
- *Cisco Virtual Security Gateway Firewall Policy Configuration Guide, Release 4.2(1) VSG1(1)*
- *Cisco Nexus 100V and Microsoft Hyper-V Compatibility Information*
- *Cisco Nexus 100V for Microsoft Hyper-V Installation and Upgrade Guide*

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

Introduction to Cisco vWAAS

This chapter provides an overview of the Cisco Virtual Wide Area Applications Services (vWAAS) solution and describes the main features that enable Cisco vWAAS to overcome the most common challenges in transporting data over a wide area network.

This chapter contains the following sections:

About Cisco vWAAS

Cisco Virtual WAAS (vWAAS) is a virtual appliance—for both enterprises and service providers—that accelerates business applications delivered from private and virtual private cloud infrastructure. Cisco vWAAS enables you to rapidly create WAN optimization services with minimal network configuration or disruption. Cisco vWAAS can be deployed in the physical data center and in private clouds and in virtual private clouds offered by service providers.

Cisco vWAAS service is associated with application server virtual machines as they are instantiated or moved. This approach helps enable cloud providers to offer rapid delivery of WAN optimization services with little network configuration or disruption in cloud-based environments.

Cisco vWAAS enables migration of business applications to the cloud, reducing the negative effect on performance of cloud-based application delivery to end-users. It enables service providers to offer an excellent application experience over the WAN as a value-added service in their catalogs of cloud services.

ISR-WAAS is the specific implementation of vWAAS running in a Cisco IOS-XE Software container on a Cisco ISR 4000 Series router (ISR-4321, ISR-4331, ISR-4351, ISR-4431, ISR-4451). In this context, “container” refers to the hypervisor that runs virtualized applications on a Cisco ISR 4000 Series router.

Note ISR-4461 is supported for vWAAS for WAAS 6.4.1b and later.

Table 1-1 shows the hypervisors supported for Cisco vWAAS. For more information on each of these hypervisors, see Hypervisors Supported for Cisco vWAAS and vCM in this chapter, and in the chapters listed in Table 1-1.

Table 1-1 Hypervisors Supported for Cisco vWAAS

Hypervisor	For More Information:
Cisco ISR-WAAS	Chapter 3, "Cisco vWAAS on Cisco ISR-WAAS"
VMware vSphere ESXi	Chapter 4, "Cisco vWAAS on VMware ESXi"
Microsoft HyperV	Chapter 5, "Cisco vWAAS on Microsoft Hyper-V"
RHEL KVM	Chapter 6, "Cisco vWAAS on RHEL KVM and KVM CentOS"
KVM on CentOS	Chapter 6, "Cisco vWAAS on RHEL KVM and KVM CentOS"
Cisco Enterprise NFVIS	Chapter 8, "Cisco vWAAS with Cisco Enterprise NFVIS"

Cisco vWAAS supports WAN optimization in a cloud environment where physical WAE devices cannot usually be deployed. Virtualization also provides various benefits like elasticity, ease of maintenance, and a reduction of branch office and data center footprint.

The following hardware and cloud platforms are supported for Cisco vWAAS. For more information on each of these supported platforms, see Cisco Hardware Platforms Supported for vWAAS.

- Cisco Unified Computing System (UCS)
- Cisco UCS E-Series Servers
- Cisco UCS E-Series Network Compute Engines (NCEs)
- Cisco ISR-4000 Series
- Cisco ENCS 5400-W Series
- Microsoft Azure Cloud
- OpenStack

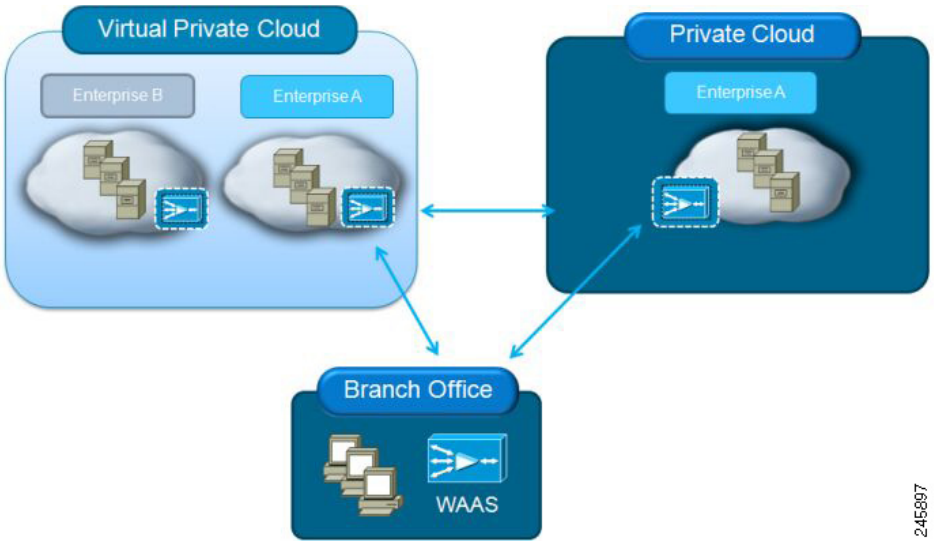
For details on the interoperability of the hypervisors and platforms supported for vWAAS, see Table 1-12.

As shown in Figure 1-1, you can enable vWAAS at the branch and/or the data center:

- *At the branch*—with Cisco ENCS 5400-W Series, Cisco Unified Computing System (UCS) E-Series servers and E-Series Network Compute Engines (NCEs), on either the Cisco 4000 Series Integrated Services Routers (ISRs) or Cisco ISR G2 branch router.
- *At the data center*—with a Cisco UCS server.

vWAAS supports on-demand provisioning and teardown, which reduces the branch office and data center footprint. Cisco vWAAS software follows the VMware ESXi standard as the preferred platform to deploy data center applications and services.

Figure 1-1 vWAAS in Virtual Private Cloud at WAN Edge, in Branch Office and Data Center



Benefits of Cisco vWAAS

The following are some of the benefits of deploying Cisco vWAAS on your system:

- On-demand orchestration of WAN optimization
- Fault tolerance with virtual machine (VM) mobility awareness
- Lower operating expenses for customers who are migrating their applications to the cloud
- Private and virtual private cloud environments:
  - Use vWAAS to create value-added WAN optimization services on a per-application basis, for optimized delivery to remote branch-office users.
  - Associate vWAAS services with application server virtual machines as they are moved in response to dynamic load demand in the cloud, to offer rapid delivery of WAN optimization services, with minimal network configuration or disruption.
- Public cloud environments:
  - Deploy vWAAS in public clouds, with the Cisco Nexus 1000V Series, to obtain benefits similar to benefits vWAAS produces in private cloud environments.

Cisco vWAAS and WAAS Interoperability

Consider the following guidelines when using Cisco vWAAS with WAAS:

- *For vWAAS with 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
- *Cisco WAAS Central Manager interoperability*—In a mixed version Cisco WAAS network, the Central Manager must be running the highest version of the Cisco WAAS software, and associated Cisco WAAS devices must be running Version 5.1.x or later.

- *Cisco WAAS system interoperability*—Cisco WAAS Version 5.2.1 is not supported running in a mixed version Cisco WAAS network in which any Cisco WAAS device is running a software version earlier than Version 5.1.x. Directly upgrading a device from a version earlier than Version 5.5.3 to 5.2.1 is not supported.

Cisco vWAAS and vCM Model Profiles

This section contains the following topics:

Cisco vWAAS Models: CPUs, Memory, and Disk Storage

Table 1-2 shows the default number of vCPUs, memory capacity, and disk storage for each vWAAS model for vWAAS for WAAS Version 6.4.1 and earlier. Table 1-8 shows the resizing capability for vWAAS for WAAS Version 6.4.1a and later.

Table 1-2 CPUs, Memory, and Disk Storage for vWAAS Models

vWAAS Model	CPUs	Memory	Disk Storage
vWAAS-150 (earliest WAAS Version 6.1.x)	1	3 GB	160 GB disk
vWAAS-200	1	3 GB	260 GB disk
vWAAS-750	2	4 GB	500 GB disk
vWAAS-1300	2	6 GB	600 GB disk
vWAAS-2500	4	8 GB	750 GB disk
vWAAS-6000	4	11 GB	900 GB disk
vWAAS-6000-R (earliest WAAS Version 6.4.x)	4	11 GB	875 GB disk
vWAAS-12000	4	12 GB	750 GB disk
vWAAS-50000	8	48 GB	1500 GB disk

For the vWAAS models noted below, follow these operating guidelines for CPU, memory, and disk storage:

- When using vWAAS-150 or vWAAS-200 with the KVM hypervisor, you must increase the default memory of 3 GB to 4 GB.
- When vWAAS-6000, 1300, 12000, or 50000 are used with Akamai Connect and when connections are more than 70% of TFO, response time will be on the higher side. Adding CPUs to these models when used with Akamai Connect may improve response time.
- Table 1-3 shows where to find more information on specific vWAAS models and their applications.

Table 1-3 For More Information on Specific vWAAS Models

vWAAS Model	For more information:
vWAAS-150	• See Cisco vWAAS-150 with Akamai Connect in Chapter 9, "Cisco vWAAS with Akamai Connect".
vWAAS-6000-R	• See Chapter 8, "Cisco vWAAS on Cisco ENCS 5400-W Series". • See *Cisco vWAAS Bundled Image Upgrade for ENCS 5400-W Series, with RMA Process for Cisco EOS/EOL WAVE Devices*.
vWAAS-12000 and vWAAS-50000	• For information on vWAAS-12000 and vWAAS-50000 used with Akamai Connect, see Akamai Connect Cache Engine on Cisco Mid- and High-End Platforms in Chapter 9, "Cisco vWAAS with Akamai Connect".
vWAAS models with Akamai Connect	• For memory and disk storage requirements for vWAAS models with Akamai Connect, see Cisco vWAAS with Akamai Connect Hardware Requirements in Chapter 9, "Cisco vWAAS with Akamai Connect."
vWAAS models on Cisco ENCS 5400 Series	• See Chapter 7, "Cisco vWAAS on Cisco ENCS 5400-W Series". • See *Cisco vWAAS Bundled Image Upgrade for ENCS 5400-W Series, with RMA Process for Cisco EOS/EOL WAVE Devices*.

Cisco vWAAS-150000 for WAAS 6.4.1a

Cisco vWAAS-150000, available for vWAAS for WAAS Version 6.4.1a, supports 150,000 connections. Table 1-4 shows specifications for Cisco vWAAS-150000.

Consider the following operating guidelines for Cisco vWAAS-150000:

- Cisco vWAAS-150000 replaces Cisco WAVE-8541, which has end-of-sale (EOS) and end-of-life (EOL) dates. For more information on WAVE-8541 EOS/EOL dates, see the *End-of-Sale and End-of-Life Announcement for the Cisco WAVE 294, 594, 694, 7541, 7571 and 8541*.
- For vWAAS with WAAS Version 6.4.1a, the supported hypervisor for vWAAS-150000 is VMware ESXi Version 5.5 or later. For more information on vWAAS on the VMware ESXi hypervisor, see Chapter 4, "Cisco vWAAS on VMware ESXi".
- Traffic interception methods used with vWAAS-150000 are AppNav, Policy-Based Routing (PBR), and Web Cache Communications Protocol (WCCP).
- Upgrading vWAAS-150000 to a version later than vWAAS for WAAS Version 6.4.1a is supported.
- Downgrading vWAAS-150000 to a version earlier than vWAAS for WAAS Version 6.4.1a is not supported.

Table 1-4 vWAAS-150000 Specifications

Specification	Description
Connections	150,000
Supported hypervisor	VMware ESXi Version 5.5 or later For more information on VMware ESXi, see Chapter 4, "Cisco vWAAS on VMware ESXi".

Specification	Description
OVA Package	Cisco-WAAS-Unified-6.41a-b-6.ova For more information on Cisco unified OVA files, see Hypervisor-wise Unified OVA Package Format for vWAAS for WAAS Version 6.4.x and Later.
Supported Hardware Platform	Cisco UCS C220 M5 For more information, see the Cisco UCS C220 M5 Rack Server Data Sheet.
vCPUs	24
Memory	96 GB
Flash Disk	4 GB
Data Disk	3 TB The data disk includes: • Object cache—700 GB • DRE cache—2 TB
(Optional) Akamai Connect Disk	1.5 TB
Traffic Interception Methods Supported	vWAAS-150000 for WAAS Version 6.4.1a supports the following traffict interception methods: WCCP, AppNav, and PBR.

VMware VMFS Block Size and vWAAS Disk Size

Table 1-5 shows the VMware Virtual Machine File System (VMFS) block size and associated vWAAS maximum disk file size. For more information on VMware and vWAAS interoperability, see Table 1-12.

Table 1-5 VMware VMFS Block Size and vWAAS Maximum File Size

VMFS Block Size	vWAAS Maximum Disk File Size
1 MB	256 GB
2 MB	512 GB
4 MB	1024 GB
8 MB	2046 GB

Note For vWAAS models that have a disk size greater than 256 GB, a VMFS block size greater than 1 MB is required.

Cisco vCM Models: Managed Nodes, vCPUs, Memory, and Disk Storage

Table 1-6 shows the number of managed nodes and disk storage for each vCM model, as well as the required and recommended number of vCPUs and the required and recommended memory capacity.

Note Cisco vWAAS installation packages are configured with the minimal required amounts of CPU and memory resources to accommodate the various hypervisor setups. These minimal requirements are sufficient for initial setup and a limited number of nodes.

However, as the number of managed devices on your system increases, the Central Manager service can experience intermittent restarts or flapping—device states when under resource shortage. To remedy this, please configure the recommended values for number of CPUs and memory shown in Table 1-6.

Table 1-6 vCM Models: Managed Nodes, vCPUs, Memory, and Disk Storage

vCM Model	Managed Nodes	Required vCPUs	Recommended vCPUs	Required Memory	Recommended Memory	Disk Storage
vCM-100	100	2	2	2 GB	2 GB	250 GB
vCM-500	500	2	4	2 GB	5 GB	300 GB
vCM-1000	1000	2	6	4 GB	8 GB	400 GB
vCM-2000	2000	4	8	8 GB	16 GB	600 GB

DRE Disk, Object Cache, and Akamai Connect Cache Capacity

This section contains the following topics:

- Table 1-7 shows the DRE disk capacity, default object cache capacity, and default Akamai Connect Cache capacity by WAVE model.
- Table 1-8 shows the DRE disk capacity, default object cache capacity, and default Akamai Connect Cache capacity by vWAAS model.
- For information on default and resized DRE disk capacity, object cache capacity, and Akamai Connect Cache capacity by vWAAS model, see Table 1-9.

Table 1-7 DRE Disk, Default OC, and Default Akamai Connect Cache by WAVE Model

WAVE Model	DRE Disk Capacity	Default Object Cache Capacity	Default Akamai Connect Cache Capacity
WAVE 294-4G	40 GB	102 GB	59 GB
WAVE 294-4G-SSD	40 GB	57 GB	55 GB
WAVE 294-8G	55 GB	77 GB	65 GB
WAVE 294-8G-SSD	55 GB	46 GB	47 GB
WAVE 594-8G	80 GB	143 GB	200 GB
WAVE 594-8G-SSD	80 GB	125 GB	125 GB

vWAAS Resizing for WAAS Version 6.4.1a and Later

This section contains the following topics:

- About vWAAS Resizing

About vWAAS Resizing

vWAAS for WAAS Version 6.4.1a and later requires additional resources, so we highly recommend that you resize CPU and memory resources, as shown in Table 1-8, and resize DRE object cache and Akamai Connect Cache, as shown in Table 1-9.

Caution Resizing CPU and memory resources is highly recommended, although optional, for vWAAS models on all hypervisors. For vWAAS for WAAS 6.4.1b and later, options are provided during vWAAS deployment for you to choose either original or resized resources.

For vWAAS for WAAS Version 6.4.1b, you cannot deploy vWAAS-12000 or vWAAS-50000 in Microsoft Hyper-V with the original resources. For a successful deployment of vWAAS 12000 or vWAAS-50000 in Microsoft Hyper-V with original resources, do a new deployment with WAAS Version 6.4.1 or earlier, and then perform the bin upgrade to WAAS Version 6.4.1b.

Note ISR-WAAS and vCM are not resized for vWAAS for WAAS Version 6.4.1a.

Resizing vWAAS on the recommended platforms enables vWAAS to scale to optimized TCP connections for the associated device, and to reduce CPU and RAM utilization.

Note For optimum performance, we recommend you use the SSD disk with the UCS models listed in Table 1-8.

Table 1-8 Resized vWAAS CPU and Memory Specifications for WAAS Version 6.4.1a and Later

vWAAS Model	Original CPU	Resized CPU	Tested CPU Clock Speed	Original Memory	Resized Memory	Minimum Recommended Cisco Platform
vWAAS-150	1 CPU	2 CPUs	1.7 GHz	3 GB	4 GB	UCS-E140N-M2
vWAAS-200	1 CPU	2 CPUs	1.8 GHz	3 GB	4 GB	UCS-E140S-M2
vWAAS-750	2 CPUs	4 CPUs	1.8 GHz	4 GB	8 GB	UCS-E140S-M2
vWAAS-1300	2 CPUs	4 CPUs	1.9 GHz	6 GB	12 GB	UCS-E160S-M3
vWAAS-2500	4 CPUs	6 CPUs	1.9 GHz	8 GB	16 GB	UCS-E160S-M3
vWAAS-6000	4 CPUs	8 CPUs	2.0 GHz	11 GB	24 GB	UCS-E180D-M3
vWAAS-6000R	4 CPUs	8 CPUs	2.0 GHz	11 GB	24 GB	UCS-E180D-M3
vWAAS-12000	4 CPUs	12 CPUs	2.6 GHz	12 GB	48 GB	UCS-C220 or UCS-C240

vWAAS Model	Original CPU	Resized CPU	Tested CPU Clock Speed	Original Memory	Resized Memory	Minimum Recommended Cisco Platform
vWAAS-50000	8 CPUs	16 CPUs	2.6 GHz	48 GB	72 GB	UCS-C220 or UCS-C240
vWAAS-150000 (earliest supported version: Cisco WAAS 6.4.1a)	24 CPUs	---	3.0 Ghz	96 GB	---	UCS C220 M5 For more information, see the Cisco UCS C220 M5 Rack Server Data Sheet.

Table 1-9 shows the default and resized DRE disk capacity, object cache capacity, and Akamai Connect cache capacity, by vWAAS model.

Table 1-9 Default and Resized DRE, OC, and Akamai Connect Cache, by vWAAS Model

vWAAS Model	DRE Disk Capacity	Default Object Cache Capacity	Default Akamai Connect Cache Capacity
vWAAS-150	52.3 GB	52 GB	30 GB
vWAAS-150 Resized	51.25 GB	52 GB	30 GB
vWAAS-200	52.23 GB	82 GB	100 GB
vWAAS-200 Resized	51.25 GB	82 GB	100 GB
vWAAS-750	96.75 GB	122 GB	250 GB
vWAAS-750 Resized	92.75 GB	122 GB	250 GB
vWAAS-1300	140 GB	122 GB	300 GB
vWAAS-1300 Resized	136.25 GB	122 GB	300 GB
vWAAS-2500	238 GB	122 GB	350 GB
vWAAS-2500 Resized	223.25 GB	122 GB	350 GB
vWAAS-6000	320 GB	122 GB	400 GB
vWAAS-6000 Resized	302.05 GB	122 GB	400 GB
vWAAS-6000R	320 GB	122 GB	350 GB
vWAAS-6000R Resized	302.05 GB	122 GB	350 GB
vWAAS-12000	450 GB	226 GB	750 GB
vWAAS-12000 Resized	407.25 GB	226 GB	750 GB
vWAAS-50000	1000 GB	227 GB	850 GB
vWAAS-50000 Resized	1000 GB	227 GB	850 GB
vWAAS-150000	1.95 T	700 GB	1500 GB

Resizing Guidelines: Upgrading to WAAS Version 6.4.1a and Later

This section contains the following procedures:

Upgrading to WAAS Version 6.4.1a and Later with Existing CPU and Memory

You can use the CLI or the Central Manager to upgrade to WAAS Version 6.4.1a, with existing CPU and memory:

Using the CLI to perform the upgrade with existing CPU and memory:

1. During the upgrade, if the vCPU and memory resources are undersized, you will be prompted to resize these vWAAS parameters before the upgrade.
2. You can continue the upgrade procedure and retain the existing vWAAS resources.

Note *For vWAAS for WAAS 6.4.1a only,* after the upgrade there will be undersized-resource alarms for vCPU and memory for the vWAAS device. Use the **show alarms** command to display information undersized alarms for the vWAAS model.

Using the Central Manager to perform the upgrade with existing CPU and memory:

1. During the upgrade, if the vCPU and memory resources are undersized, there will be an informational note on the upgrade page, but there will not be a prompt to resize these vWAAS parameters before the upgrade.
2. You can continue the upgrade procedure and retain the existing vWAAS resources.

Note *For vWAAS for WAAS 6.4.1a only,* after the upgrade there will be undersized-resource alarms for vCPU and memory for the vWAAS device. Use the **show alarms** command to display information undersized alarms for the vWAAS model.

Upgrading to WAAS Version 6.4.1a and Later with Resized CPU and Memory

You can use the CLI or the Central Manager to upgrade to WAAS Version 6.4.1a, with resized CPU and memory:

Using the CLI to perform the upgrade with resized CPU and memory:

1. During the upgrade, if the vCPU and memory resources are undersized, you will be prompted to resize these vWAAS parameters before the upgrade.
2. You can then cancel the upgrade procedure.
3. After shutting down the vWAAS instance, manually increase the vCPU and memory, from the hypervisor, to meet your specifications.
   - *To change settings in VMware ESXi:* Navigate to **Edit Settings... > Hardware** tab.
   - *To change settings in Microsoft Hyper-V*: Navigate to **Virtual Machine > Settings... > Hardware**.
   - *To change settings in RHEL KVM/CentOS:*
     a. Open **Virtual Manager**.
     b. Navigate to **Virtual Machine > CPUs**.

c. Navigate to **Virtual Machine** > **Memory**.

- *To change settings in Cisco NFVIS, for the Cisco vBranch solution:*

a. Navigate to **VM Life Cycle** > **Image Repository** > **Profiles** and add another profile with: resized CPU, memory, and same disk size.

b. Navigate to **VM Life Cycle** > **Deploy** > **VM Details** and select the resized profile created.

c. Click **Deploy**.

Note *If you use the Route Manager Debugging (RMD) process with vBranch:* To ensure that the RMD process will start successfully in vBranch deployment, you must manually connect both the interfaces before starting the vWAAS.

- *To change settings Microsoft Azure:*

a. Navigate to **Deployments** > **Microsoft Template Overview** > **Custom Deployment**,

b. Navigate to **Home** > **Virtual Machines** > **vWAAS Instance** > **Size**.

4. Restart the upgrade procedure. With the resized vCPU and memory, the host should have sufficient resources for a successful upgrade.
5. Resources will not change automatically in subsequent upgrades/downgrades of the system change, manual intervention is required to change the resource.

Using the Central Manager to perform the upgrade with resized CPU and memory:

1. During the upgrade, if the vCPU and memory resources are undersized, there will be an informational note on the upgrade page, but there will not be a prompt to resize these vWAAS parameters before the upgrade.

Note You cannot cancel the upgrade procedure, in process, from the Central Manager.

2. Resources will not change in subsequent upgrades/downgrades of the system.

Resizing Guidelines: Installing WAAS 6.4.1a

This section contains the following topics:

New Installation with Existing CPU and Memory

1. Install the vWAAS OVA with a WAAS version earlier than WAAS Version 6.4.1a, which, by default, will deploy with resized resource.
2. Upgrade to WAAS Version 6.4.1a and retain existing CPU and memory resources.
3. After installation is complete, there will be undersized-resource alarms for CPU and memory for the vWAAS device. You use the **show alarms** command to display information about undersized alarms for the vWAAS model.

4. After resources are upgraded, there will not be any automatic change in resources for subsequent upgrades/downgrades of the system.

New Installation with Resized CPU and Memory

1. Install vWAAS OVA with version WAAS 6.4.1a.
2. The host should have sufficient resources of resized CPU and resized memory for a successful deployment.
3. After resources are upgraded, there will not be any automatic change in resources for subsequent upgrades/downgrades of the system.

Resizing Guidelines by Hypervisor for WAAS 6.4.1b and Later

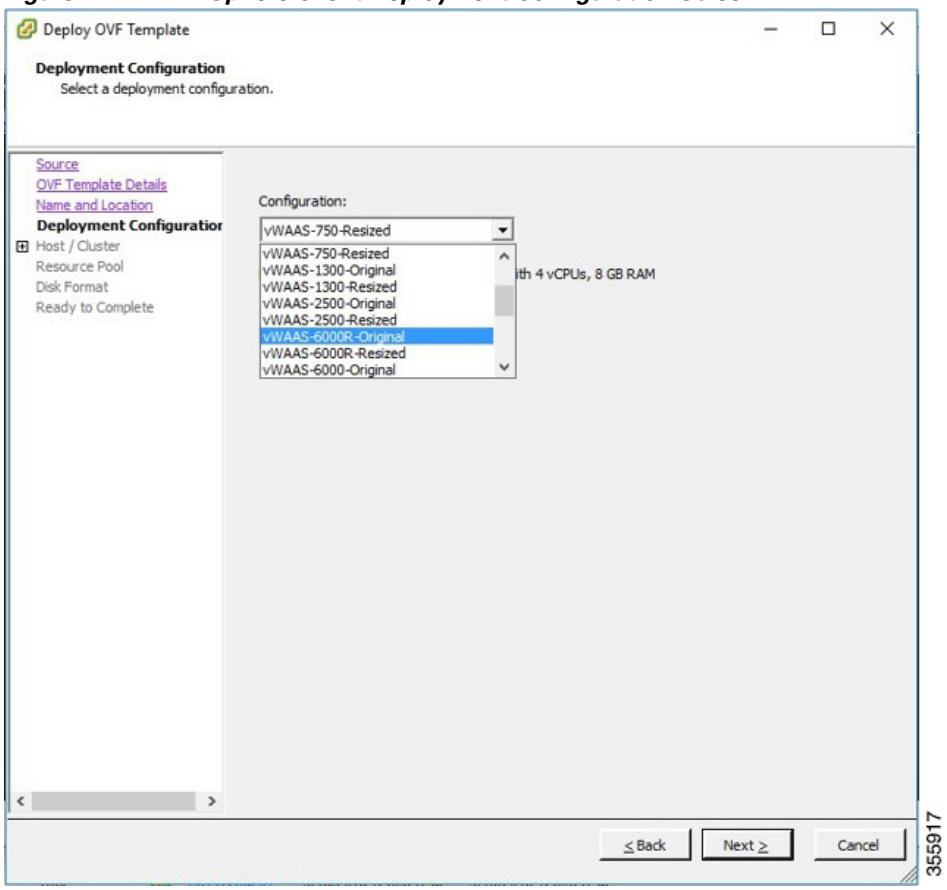
This section contains the following topics:

Resizing for vWAAS on VMware ESXi

To resize CPU and memory for vWAAS on VMware ESXi, follow these steps:

Step 1 From the vSphere Client, choose **Deploy OVF Template > Deployment Configuration** (Figure 1-2).

Figure 1-2 vSphere Client Deployment Configuration Screen



Step 2 At the **Configuration** drop-down list, choose the vWAAS model for this hypervisor (Figure 1-2).

For example, if you are choosing vWAAS-6000, you can choose **vWAAS-6000-Original** or **vWAAS-6000-Resized**.

Resizing for vWAAS on Microsoft Hyper-V

To resize CPU and memory for vWAAS on Microsoft Hyper-V, follow these steps:

Step 1 Login to the WAAS Installer for Microsoft Hyper-V, which displays a list of supported WAAS models (Figure 1-3).

Figure 1-3 vWAAS and vCM Resources for vWAAS on Hyper-V

```
PS C:\Users\Administrator\Desktop\platform-hv\6.4.3-b555\Cisco-HyperV-vWAAS-unified-6.4.3-b555> .\deploy-cisco-vwaas-scv
mm.psl

----- Cisco WAAS Installer for Hyper-V -----

WAAS supports below models
S.No    Model                Original Resources      Resized Resources

                             vCPU    MEMORY          vCPU    MEMORY

1.      vWAAS-150            1       3GB             2       4GB
2.      vWAAS-200            1       3GB             2       4GB
3.      vWAAS-750            2       4GB             4       8GB
4.      vWAAS-1300           2       6GB             4       12GB
5.      vWAAS-2500           4       8GB             6       16GB
6.      vWAAS-6000R          4       11GB            8       24GB
7.      vWAAS-6000           4       11GB            8       24GB
8.      vWAAS-12000          4       12GB            12      48GB
9.      vWAAS-50000          8       48GB            16      72GB
10.     vCM-100N             2       2GB             NA      NA
11.     vCM-500N             2       2GB             NA      NA
12.     vCM-1000N            2       4GB             NA      NA
13.     vCM-2000N            4       8GB             NA      NA

Enter vWAAS/vCM model number to install[1]: 7
Do you want to install vWAAS-6000 with re-sized resources[y/n]: y

Script: C:\Users\Administrator\Desktop\platform-hv\6.4.3-b555\Cisco-HyperV-vWAAS-unified-6.4.3-b555
Loading System Center Virtual Machine Manager Powershell Module...
Powershell module loaded.
```

355918

Step 2 At the **Enter vWAAS/vCM model to install** prompt, enter the line number for the model you want to install. For example, from the listing shown in Figure 1-3. entering **7** would select vWAAS-6000.

Step 3 At the **Do you want to install vWAAS-6000 with resized resources [y/n]** prompt, enter Y to select resized resources.

Step 4 After you select Y, the system displays the associated script, for example:

```
Script: C:\Users\Administrator\Desktop]platform-hv\6.4.3-b55\Cisco-HyperV-vWAAS-unified-6.4.3-b55
Loading System Center Virtual Machine Manager Powershell Module...
Powershell module loaded.
```

Resizing for vWAAS on RHEL CentOS or SUSE Linux

To resize CPU and memory for vWAAS on RHEL CentOS or on SUSE Linux, follow these steps:

Step 1 At the **root@localhost** screen, enter the resizing launch script:

```
[root@localhost]# ./launch.sh nresized macvtap br-ex br-extl
```

Step 2 The system displays original and resized resources for each vWAAS model (Figure 1-4):

Figure 1-4 vWAAS and vCM Resources on CentOS or SUSE Linux

```
[root@localhost]# ./launch.sh nresized macvtap br-ex br-ext1

                    ORIGINAL RESOURCES            RESIZED RESOURCES

SNO MODEL NAME       CPU        MEMORY          CPU        MEMORY

1.  vWAAS 150          1          4GB            2          4GB
2.  vWAAS 200          1          4GB            2          4GB
3.  vWAAS 750          2          4GB            4          8GB
4.  vWAAS 1300         2          6GB            4         12GB
5.  vWAAS 2500         4          8GB            6         16GB
6.  vWAAS 6000R        4         11GB            8         24GB
7.  vWAAS 6000         4         11GB            8         24GB
8.  vWAAS 12000        4         12GB           12         48GB
9.  vWAAS 50000        8         48GB           16         72GB
10. vCM 100N           2          2GB           NA         NA
11. vCM 500N           2          2GB           NA         NA
12. vCM 1000N          2          4GB           NA         NA
13. vCM 2000N          4          8GB           NA         NA

Select the model type :2
[root@localhost msannare]#

root@localhost msannare]# ./ezdeploy.sh

                    ORIGINAL RESOURCES            RESIZED RESOURCES

SNO MODEL NAME       CPU        MEMORY          CPU        MEMORY

1.  vWAAS 150          1          4GB            2          4GB
2.  vWAAS 200          1          4GB            2          4GB
3.  vWAAS 750          2          4GB            4          8GB
4.  vWAAS 1300         2          6GB            4         12GB
5.  vWAAS 2500         4          8GB            6         16GB
6.  vWAAS 6000R        4         11GB            8         24GB
7.  vWAAS 6000         4         11GB            8         24GB

Select the model type :
[root@localhost]#
```

355921

Step 3 At the **Select the model type** prompt, enter the line number of the model type for your system. For example, selecting 7 will select vWAAS-6000.

The system displays the message:

```
Do you want to install vWAAS-6000 with resized resources [y/n]
Enter Y to select resized resources.
```

Step 4 Launch the EzDeploy script:

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

The EzDeploy script also displays both the original and resized resources as shown in Figure 1-5.

Figure 1-5 EZDeploy Listing of Original and Resized Resources

Deployment configurations	vCPU	RAM
vWAAS-150-Original	1	3
vWAAS-150-Resized	2	4
vWAAS-200-Original	1	3
vWAAS-200-Resized	2	4
vWAAS-750-Original	2	4
vWAAS-750-Resized	4	8
vWAAS-1300-Original	2	6
vWAAS-1300-Resized	4	12
vWAAS-2500-Original	4	8
vWAAS-2500-Resized	6	16
vWAAS-6000R-Original	4	11
vWAAS-6000R-Resized	8	24
vWAAS-6000-Original	4	11
vWAAS-6000-Resized	8	24
vWAAS-12000-Original	4	12
vWAAS-12000-Resized	12	48
vWAAS-50000-Original	8	48
vWAAS-50000-Resized	16	72
vWAAS-150000-Original	24	96
vCM-100N-Original	2	2
vCM-500N-Original	2	2
vCM-1000N-Original	2	4
vCM-2000N-Original	4	8

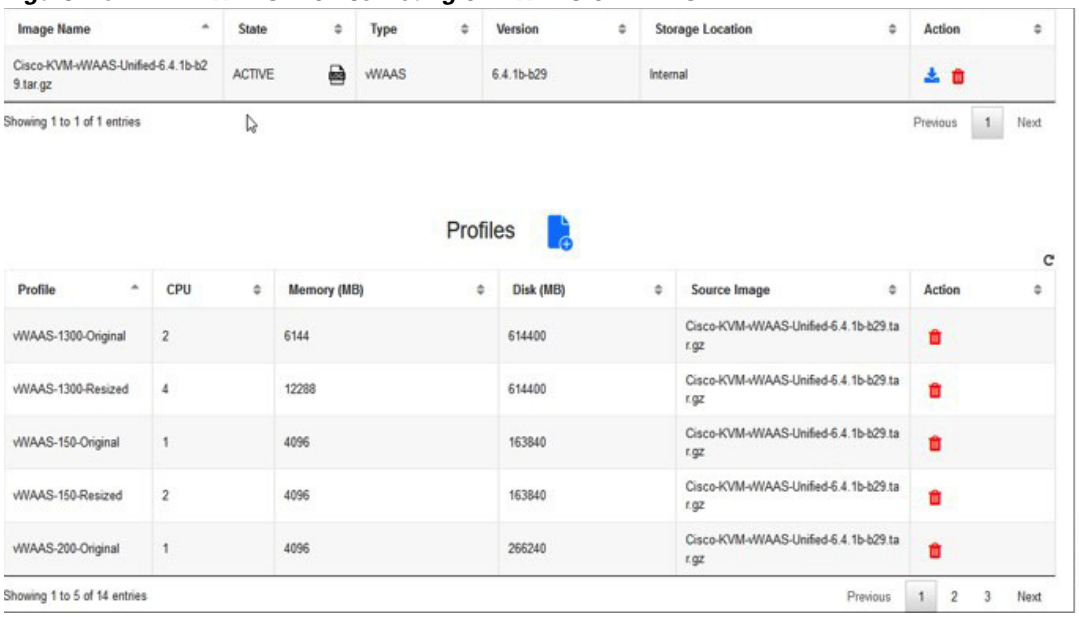
355919

Step 5 The system deploys the selected model, with resized resources.

Resizing for vWAAS on NFVIS

For resizing for vWAAS on NFVIS, install the vWAAS OVA with version WAAS 6.4.1b. Figure 1-6 shows the NFVIS Profiles listing for original and resized vWAAS resources.

Figure 1-6 vWAAS Profiles Listing on vWAAS on NFVIS



For information on resizing vWAAS on NFVIS, see the *Cisco Enterprise Network Function Virtualization Infrastructure Configuration Guide*.

OVA Package Files for vWAAS and vCM Models

Table 1-10 shows the OVA and NPE OVA file for each vWAAS model:

Table 1-10 OVA Package Files for vWAAS Models

vWAAS Model	OVA Filename	NPE OVA Filename
vWAAS-150	vWAAS-150.ova	Cisco-WAAS-vWAAS-150-npe.ova
vWAAS-200	vWAAS-200.ova	Cisco-WAAS-vWAAS-200-npe.ova
vWAAS-750	vWAAS-750.ova	Cisco-WAAS-vWAAS-750-npe.ova
vWAAS-1300	vWAAS-1300.ova	Cisco-WAAS-vWAAS-1300-npe.ova
vWAAS-2500	vWAAS-2500.ova	Cisco-WAAS-vWAAS-2500-npe.ova
vWAAS-6000	vWAAS-6000.ova	Cisco-WAAS-vWAAS-6000-npe.ova
vWAAS-12000	vWAAS-12000.ova	Cisco-WAAS-vWAAS-12000-npe.ova
vWAAS-50000	vWAAS-50000.ova	Cisco-WAAS-vWAAS-50000-npe.ova

Table 1-11 shows the OVA and NPE OVA file for each vCM model (all models are available with WAAS version 4.3.1 and later, except as noted):

Table 1-11 OVA Package Files for vCM Models

vCM Model	OVA Filename	NPE OVA Filename
vCM-100N	vCM-100N.ova	Cisco-WAAS-vCM-100N-npe.ova
vCM-500N	vCM-500N.ova	Cisco-WAAS-vCM-500N-npe.ova
vCM-1000N	vCM-1000N.ova	Cisco-WAAS-vCM-1000N-npe.ova
vCM-2000N	vCM-2000N.ova	Cisco-WAAS-vCM-2000N-npe.ova

Cisco Hardware Platforms Supported for vWAAS

This section contains the following topics:

Platforms Supported for vWAAS, by Hypervisor Type

For each hypervisor used with vWAAS, Table 1-12 shows the types of platforms supported for vWAAS, including minimum WAAS version, host platform, and disk type.

Note ISR-4321 with IOS-XE 16.9.x is supported for vWAAS for WAAS Version 6.4.1b and later.

Table 1-12 Platforms Supported for vWAAS, by Hypervisor Type

Hypervisor	PID and Device Type	Minimum WAAS Version	Host Platforms	Minimum Host Version	Disk Type
Cisco ISR-WAAS	• PID: OE-VWAAS-KVM • Device Type: ISR-WAAS	• 6.4.1b (ISR-4461) • 5.4.1 • 5.2.1 (ISR-4451)	• ISR-4461 (vWAAS-750, 1300, 2500) • ISR-4451 (vWAAS-750, 1300, 2500) • ISR-4431 (vWAAS-750, 1300) • ISR-4351 (vWAAS-750) • ISR-4331 (vWAAS-750) • ISR-4321 (vWAAS-200)	• IOS-XE 3.9	• ISR-SSD • NIM-SSD
Cisco NFVIS	• PID: OE-VWAAS-KVM • Device Type: OE-VWAAS-KVM	• 6.4.1 (Cisco ENCS 5400 Series and Cisco) • 6.2.x (Cisco UCS-E Series)	• Cisco ENCS (Enterprise Network Compute System) 5400 Series • Cisco UCS-E Series	• NFV FC2	• virtio
VMware vSphere ESXi	• PID: OE-VWAAS-ESX • Device Type: OE-VWAAS-ESX	• 5.0.3g	• Cisco UCS (Unified Computing System) • Cisco UCS-E Series	• ESXi 5.0	• VMDK
Microsoft Hyper-V	• PID: OE-VWAAS-HYPERV • Device Type: OE-VWAAS-HYPERV	• 6.1.x	• Cisco UCS • Cisco UCS-E Series	• Microsoft Windows 2008 R2	• VHD
RHEL KVM	• PID: OE-VWAAS-KVM • Device Type: OE-VWAAS-KVM	• 6.2.x	• Cisco UCS • Cisco UCS-E Series	• RHEL CentOS 7.1	• virtio
SUSE Linux	• PID: OE-VWAAS-GEN-LINUX • Device Type: OE-VWAAS-GEN-LINUX	• 6.4.1b	• Cisco UCS • Cisco UCS-E Series	• SUSE Linux Enterprise Server (SLES) 12	• virtio

Hypervisor	PID and Device Type	Minimum WAAS Version	Host Platforms	Minimum Host Version	Disk Type
Microsoft Azure	• PID: OE-VWAAS-AZURE • Device Type: OE-VWAAS-AZURE	• 6.2.x	• Microsoft Azure cloud	• N/A	• VHD
OpenStack	• PID: OE-VWAAS-OPENSTACK • Device Type: OE-VWAAS-OPENSTACK	• 6.4.1b	• OpenStack	• OpenStack Mitaka	• virtio

Components for Deploying vWAAS, by Hypervisor Type

For each hypervisor used with vWAAS, Table 1-13 shows the components used to deploy vWAAS, including package format, deployment tool, pre-configuration tool (if needed), and network driver.

Table 1-13 Components for Deploying vWAAS, by Hypervisor Type

Hypervisor	Package Format	Deployment Tool	Pre-Configuration	Network Driver
Cisco ISR-WAAS	• OVA	• Ezconfig	• onep	• virtio_net
Cisco NFVIS	• TAR	• NFVIS	• Bootstrap Day0 config	• virtio_net
VMware vSphere ESXi	• OVA	• ---	• ---	• vmxnet3
Microsoft HyperV	• Zip	• Powershell script	• ---	• netvsc
RHEL KVM	• TAR	• EZdeploy • launch.sh	• ---	• virtio_net
SUSE Linux	• TAR	• EZdeploy • launch.sh	• ---	• virtio_net
Microsoft Azure	• JSON template	• ---	• ---	• netvsc
OpenStack	• TAR	• OpenStack portal (Horizon U1)	• ---	• virtio_net

Note Cisco Virtual Interface Cards (VICs) are not qualified for vWAAS.

Components for Managing vWAAS, by Hypervisor Type

For each hypervisor used with vWAAS, Table 1-14 shows the components used to manage vWAAS, including vCM model, vWAAS model, number of instances supported, and traffic interception method used.

Table 1-14 Components for Managing vWAAS, by Hypervisor Type

Hypervisor	vCM Models Supported	vWAAS Models Supported	Number of Instances Supported	Traffic Interception Method
Cisco ISR-WAAS	• N/A	• vWAAS-200, 750, 1300, 2500	• 1	• AppNav-XE
Cisco NFVIS	• N/A	• vWAAS-200, 750, 1300, 2500, 6000	• 1	• WCCP • APPNav-XE • Inline (with WAAS v6.2.1 and later)
VMware vSphere ESXi	• vCM-100, 500, 1000, 2000	• vWAAS-150, 200, 750, 1300, 2500, 6000, 12000, 150000, 50000	• many	• WCCP • APPNav-XE
Microsoft HyperV	• vCM-100, 500, 1000, 2000	• vWAAS-150, 200, 750, 1300, 2500, 6000, 12000, 50000	• many	• WCCP • APPNav-XE
RHEL KVM	• vCM-100, 500, 1000, 2000	• vWAAS-150, 200, 750, 1300, 2500, 6000, 12000, 50000	• many	• WCCP • APPNav-XE • Inline (with WAAS v6.2.1 and later)
SUSE Linux	• vCM-100, 500, 1000, 2000	• vWAAS-150, 200, 750, 1300, 2500, 6000, 12000, 50000	• many	• WCCP • APPNav-XE
Microsoft Azure	• N/A	• vWAAS-200, 750, 1300, 2500, 6000, 12000	• 1	• Routed mode (with WAAS v6.2.1 and later)
OpenStack	• vCM-100, 500, 1000, 2000	• vWAAS-150, 200, 750, 1300, 2500, 6000, 12000, 50000	• many	• WCCP • APPNav-XE

Cisco UCS E-Series Servers and NCEs

This section has the following topics:

- vWAAS and Cisco UCS E-Series Interoperability
- vWAAS and Cisco UCS E-Series Memory Guidelines and Requirements

vWAAS and Cisco UCS E-Series Interoperability

Cisco UCS E-Series servers and UCS E-Series Network Compute Engines (NCEs) provide platforms for Cisco vWAAS and Cisco ISR routers. Table 1-15 shows the supported operating systems, Hypervisors, Cisco ISR routers, and minimum version of IOS-XE used.

Table 1-15 vWAAS and UCS E-Series Interoperability

Cisco UCS E-Series	Supported Operating Systems for vWAAS	Supported Hypervisors for vWAAS	Supported Cisco ISR Routers for vWAAS	Minimum IOS -XE Version
UCS E-Series Servers	• Microsoft Windows Server 2008 R2, 2012, and 2012 R2 • RHEL (Red Hat Enterprise Linux) 7.1 and later • Linux CentOS (Community Enterprise Operating System) 7.1 and later	• Microsoft Hyper-V 2008 R2, 2012, and 2012 R2 • VMware vSphere ESXi 5.5 and 6.0 • KVM for RHEL or CentOS 7.1 and later	• ISR-4331, ISR-4351, ISR-4451, ISR-4461	• 3.10
UCS E-Series NCEs	• Microsoft Windows Server (2012 R2) • RHEL 7.1 and later • Linux CentOS 7.1 and later	• Microsoft Hyper-V2012 R2 • VMware vSphere ESXi 5.5 and 6.0 • KVM for RHEL or CentOS 7.1 and later	• ISR-4321, ISR-4331, ISR-4351, ISR-4431, ISR-4451, ISR-4461	• 3.10 (UCS-EN120S) • 3.15.1 (UCS-EN140N)

vWAAS and Cisco UCS E-Series Memory Guidelines and Requirements

Table 1-16 shows memory and disk storage capacity for Cisco UCS E-Servers NCEs. When calculating memory requirements for your vWAAS system, include the following parameters:

- A minimum of 2 GB of memory is needed for VMware v5.0, v5.1, or v6.0.
- A minimum of 4 GB of memory is needed for VMware v5.5.
- You must also allocate memory overhead for vCPU memory. The amount is dependent on the number of vCPUs for your system: 1, 2, 4, or 8 vCPUs.

Note For information on vCPUs, ESXi server datastore memory, and disk space by vWAAS model and vCM model, see Table 4-3 and Table 4-4 in Chapter 4, "Cisco vWAAS on VMware ESXi".

Example1: *A deployment of vWAAS-750 on the UCS-E140S, using VMware v6.0.*

1. UCS-E140S has a default value of 8 GB memory (which can be expanded to 48 GB).
2. vWAAS-750 requires 6 GB memory + VMware v6.0 requires 2 GB memory = 6 GB memory, which is below the default memory capacity of the UCS-E140S.
3. You can deploy vWAAS-750 on the UCS-E140S without adding additional memory to the UCS-E140S DRAM.

Example1: *A deployment of vWAAS-1300 on the UCS-E140S, using VMware v6.0.*

1. UCS-E140S has a default value of 8 GB DRAM, (which can be expanded to 48 GB).
2. vWAAS-1300 requires 6 GB memory + VMware v6.0 requires 2 GB DRAM = 8 GB memory, which equals the memory capacity of UCS-E140S.
3. To deploy vWAAS-1300 on the UCS-E140S, you must add additional memory to the UCS-E140S memory.

Note For the vWAAS datastore, you can use either SAN storage or local storage on the ESXi server. NAS (Network-Attached Storage) storage should only be used in nonproduction scenarios (for test purposes, for example).

Table 1-16 Memory and Disk Storage for Cisco UCS E-Servers NCEs

Cisco UCS E-Series Server (E) or NCE (EN)	Memory	Disk Storage
UCS-E140S (single-wide blade)	Default: 8 GB Maximum: 16 GB	Up to two of the following: • 7200-RPM SATA: 1 TB • 10,000-RPM SAS: 900 GB • 10,000-RPM SAS SED: 600 GB • SAS SSD SLC: 200 GB • SAS SSD eMLC: 200 or 400 GB
UCS-EN120S (single-wide blade)	Default: 4GB Maximum: 16 GB	Up to two of the following: • 7200-RPM SATA: 500 GB • 7200-RPM SATA: 1 TB • 10,000-RPM SAS: 900 GB
UCS-E140DP (double-wide blade with PCIe cards)	Default: 8 GB Maximum: 48 GB	Up to two of the following: • 7200-RPM SATA: 1 TB • 10,000-RPM SAS: 900 GB • 10,000-RPM SAS SED: 600 GB • SAS SSD SLC: 200 GB • SAS SSD eMLC: 200 or 400 GB
UCS-E140D (double-wide blade)	Default: 8 GB Maximum: 48 GB	Up to three of the following: • 7200-RPM SATA: 1 TB • 10,000-RPM SAS: 900 GB • 10,000-RPM SAS SED: 600 GB • SAS SSD SLC: 200 GB • SAS SSD eMLC: 200 or 400 GB
UCS-EN40N (Network Interface Module)		One of the following mSATA SSD drives: • mSATA SSD drive: 50 GB • mSATA SSD drive: 100 GB • mSATA SSD drive: 200 GB

Cisco UCS E-Series Server (E) or NCE (EN)	Memory	Disk Storage
UCS-E160DP (double-wide blade with PCIe cards)	Default: 8 GB Maximum: 48 GB	Up to two of the following: • 7200-RPM SATA: 1 TB • 10,000-RPM SAS: 900 GB • 10,000-RPM SAS SED: 600 GB • SAS SSD SLC: 200 GB • SAS SSD eMLC: 200 or 400 GB
UCS-E160D (double-wide blade)	Default: 8 GB Maximum: 96 GB	Up to three of the following: • 7200-RPM SATA: 1 TB • 10,000-RPM SAS: 900 GB • 10,000-RPM SAS SED: 600 GB • SAS SSD SLC: 200 GB • SAS SSD eMLC: 200 or 400 GB
UCS-E180D (double-wide blade)	Default: 8 GB Maximum: 96GB	Up to three of the following: • 7200-RPM SATA: 1 TB • 10,000-RPM SAS: 1.8 TB • 10,000-RPM SAS: 900 GB • 10,000-RPM SAS SED: 600 GB • SAS SSD SLC: 200 GB • SAS SSD eMLC: 200 or 400 GB

Cisco ENCS 5400 Series

This section contains the following topics:

About the Cisco ENCS 5400 Series

The Cisco Enterprise Network Compute System (ENCS) 5400 Series is designed for the Cisco Enterprise Network Functions Virtualization (NFV) solution, and is available for vWAAS for WAAS Version 6.4.1 and later.

The ENCS 5400 Series—ENCS 5406-W, 5408-W, and 5412-W—is an x86 hybrid platform for branch deployment and for hosting WAAS applications. This high-performance unit achieves this goal by providing the infrastructure to deploy virtualized network functions while at the same time acting as a server that addresses processing, workload, and storage challenges.

For more information on the Cisco ENCS 5400-W series, see the *Cisco 5400 Enterprise Network Compute System Data Sheet*.

For information on vWAAS with NFVIS on the ENCS 5400 Series, see Chapter 7, "Cisco vWAAS with Cisco Enterprise NFVIS".

ENCS 5400 Series Hardware Features and Specifications

Table 1-17 shows specifications that apply to all three ENCS 5400 series models. For views of the Cisco ENCS 5400 Series and further information, see the *Cisco 5400 Enterprise Network Compute System Data Sheet*.

Table 1-17 ENCS 5400 Series Features and Specifications

ENCS 5400 Feature/Specification	Description
vWAAS models supported	One of the following configurations: • ENCS 5406-W supports vWAAS 200, vWAAS-750 • ENCS 5408-W supports vWAAS-1300 • ENCS 5412-W supports vWAAS-2500, vWAAS-6000-R
CPU	One of the following specifications: • ENCS 5406-W: Intel Xeon Processor D-1528 (6-core, 1.9 GHz, and 9 MB cache) • ENCS 5408-W: Intel Xeon Processor D-1548 (8-core, 2.0 GHz, and 12 MB cache) • ENCS 5412-W: Intel Xeon Processor D-1557 (12-core, 1.5 GHz, and 18 MB cache)
BIOS	Version 2.4
Cisco NFVIS on KVM hypervisor	KVM hypervisor Version 3.10.0-327.el7.x86_64
CIMC	Version 3.2
Network Controller	Intel FTX710-AM2
WAN Ethernet port	Intel i350 dual port
DIMM	Two DDR4 dual in-line memory module (DIMM) slots, for ENCS models with the following capacities: • ENCS 5406-W—16 GB • ENCS 5408-W—16 GB • ENCS 5412-W—32 GB The memory module in each of the slots can be upgraded to a maximum of 32 GB, so that you can have a maximum capacity of 64 GB DIMM.
Gigabit Ethernet ports	Two Gigabit Ethernet ports—For each RJ45 port, there is a corresponding fiber optic port. At a given time, you can use either the RJ45 connection or the corresponding fiber optic port.
NIM	One Network Interface Module (NIM) expansion slot—You can install a NIM in the NIM slot, or if the slot is not needed, you can remove the NIM from the NIM module. Each ENCS 5400 model supports one NIM slot, for a Cisco 4-port 1G fail-to-wire NIM card.
Management Controller	Ethernet management port for Cisco Integrated Management Controller (CIMC), which monitors the health of the entire system.

ENCS 5400 Feature/Specification	Description
HDD Storage	Although there are two hot-swappable HDD slots, we do not recommend HDD storage for the ENCS 5400 Series.
SSD Storage	• No RAID and 1 960 GB SSD • RAID-1 and 2 SSDs (960 GB SSD)
Offload Capabilities	Optional crypto module to provide offload capabilities to optimize CPU resources like VM-toVM traffic and to maintain open software support.

Hypervisors Supported for Cisco vWAAS and vCM

Here is an overview of hypervisors are supported for Cisco vWAAS and vCM.

- **Cisco ISR-WAAS**

  ISR-WAAS is the specific implementation of vWAAS running in a Cisco IOS-XE Software container on a Cisco ISR 4000 Series router (ISR-4321, ISR-4331, ISR-4351, ISR-4431, ISR-4451, ISR-4461). In this context, "container" refers to the hypervisor that runs virtualized applications on a Cisco ISR 4000 Series router.

  Note ISR-WAAS is supported for vWAAS for WAAS 6.4.1b and later.

  For more information, see Chapter 3, "Cisco vWAAS on Cisco ISR-WAAS".

- **VMware ESXi**

  Cisco vWAAS for VMware ESXi provides cloud-based application delivery service over the WAN in ESX/ESXi-based environments. Cisco vWAAS on VMware vSphere ESXi is delivered an OVA file. The vSphere client takes the OVA file for a specified vWAAS model, and deploys an instance of that vWAAS model.

  For more information, see Chapter 4, "Cisco vWAAS on VMware ESXi".

- **Microsoft Hyper-V**

  Microsoft Hyper-V, available for vWAAS with WAAS Version 6.1.x and later, provides virtualization services through hypervisor-based emulations.

  Cisco vWAAS on Microsoft Hyper-V extends Cisco networking benefits to Microsoft Windows Server Hyper-V deployments.

  Microsoft HyperV, Chapter 5, "Cisco vWAAS on Microsoft Hyper-V".

- **RHEL KVM and KVM CentOS**

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

  - 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.

For more information, see Chapter 6, "Cisco vWAAS on RHEL KVM and KVM CentOS".

- **Cisco Enterprise NFVIS**

  Cisco Enterprise NFV Infrastructure Software (NFVIS) offers flexibility and choice in deployment and platform options for the Cisco Enterprise NFV solution. By virtualizing and abstracting the network services from the underlying hardware, NFVIS allows virtual network functions (VNFs) to be managed independently and to be provisioned dynamically.

  – *For vWAAS on WAAS Version 5.x to 6.2.x,* Cisco NFVIS is available for vWAAS running on Cisco UCS E-Series Servers.

  – *For vWAAS on WAAS Version 6.4.1 and later,* Cisco NFVIS is available for vWAAS running on Cisco UCS E-Series Servers and the Cisco ENCS 5400 Series.

  For more information, see Chapter 7, "Cisco vWAAS with Cisco Enterprise NFVIS".

Hypervisor OVA Packages for vWAAS

This section contains the following topics:

Hypervisor OVA Package Format for vWAAS for WAAS Versions 5.x to 6.2.x

For vWAAS for WAAS Versions 5.x to 6.2.x, Cisco provides an OVA package for an NPE and non-NPE version for each vWAAS model connection profile.

For a listing of hypervisor-wise NPE and non-NPE OVA files for vWAAS or vCM, see the Cisco Wide Area Application Services (WAAS) Download Software Page and select the WAAS software version used with your vWAAS instance.

Table 1-18 shows the file formats for hypervisors supported for vWAAS and vCM, for WAAS Version 5.x to 6.2.x.

Table 1-18 File Formats for OVA Packages for vWAAS and vCM for WAAS Version 5.x to 6.2.x

vWAAS or vCM	Hypervisor Support	File Format	NPE File Format	Sample Image and NPE Image Filename Formats
vWAAS	VMware ESXi	.ova	.ova	• Cisco-vWAAS-750-6.2.3d-b-68.ova • Cisco-vWAAS-750-6.2.3d-npe-b-68.ova • For more information on this filename format, see OVA Package for vWAAS on VMware ESXi for WAAS Version 5.x to 6.2.x.
	Microsoft Hyper-V	.zip	.zip	• Hv-Cisco-vWAAS-750-6.2.3d-b-68.zip • Hv-Cisco-vWAAS-750-6.2.3d-npe-b-68.zip • For more information on this filename format, see OVA Package for vWAAS on Hyper-v for WAAS Version 5.x to 6.2.x.
	RHEL KVM	.tar.gz	.tar.gz	• Cisco-KVM-vWAAS-750-6.2.3d-b-68.tar.gz • Cisco-KVM-vWAAS-750-6.2.3d-b-68-npe.tar.gz • For more information on this filename format, see Tar Archive Package for vWAAS on KVM for WAAS Version 5.x to 6.2.x.
vCM	VMware ESXi	.ova	.ova	• Cisco-vCM-100N-6.2.3d-b-68.ova • Cisco-vCM-100N-6.2.3d-npe-b-68.ova • For more information on this filename format, see OVA Package for vWAAS on VMware ESXi for WAAS Version 5.x to 6.2.x.
	Microsoft Hyper-V	N/A	.zip	• Hv-Cisco-100N-6.2.3d-b-68.zip • Hv-Cisco-100N-6.2.3d-npe-b-68.zip • For more information on this filename format, see OVA Package for vWAAS on Hyper-v for WAAS Version 5.x to 6.2.x.
	RHEL KVM	.tar.gz	.tar.gz	• Cisco-KVM-vCM-100N-6.2.3d-b-68.tar.gz • Cisco-KVN-vCN-100N-6.2.3d-npe-b-68-npe.tar-gz • For more information on this filename format, see Tar Archive Package for vWAAS on KVM for WAAS Version 5.x to 6.2.x.

Hypervisor-wise Unified OVA Package Format for vWAAS for WAAS Version 6.4.x and Later

For vWAAS with WAAS Version 6.4.x and later, Cisco provides a single unified OVA package, one each for the NPE and non-NPE version of the WAAS image for all the vWAAS and vCM models for that Hypervisor.

Each unified OVA package file provides an option to select a vWAAS or vCM model and other required parameters to launch vWAAS or vCM with WAAS in the required configuration.

Table 1-19 shows the unified OVA filename formats supported for hypervisors, appliances, vWAAS models, and vCM models.

Note On VMware ESXi, the OVA deployment for WAAS Version 6.4.1 and later must be done only through VMware vCenter.

For a listing of hypervisor-wise NPE and non-NPE OVA files for vWAAS or vCM, see the Cisco Wide Area Application Services (WAAS) Download Software Page and select the WAAS software version for your vWAAS instance.

Table 1-19 Unified OVA Filename Format Supported for Hypervisors, Appliances, vWAAS Models , and vCM Models

Unified OVA Filename Format	Hypervisor or Appliance	Supported vWAAS Models	Supported vCM Models
Cisco-WAAS-Unified-6.4.1-b-36.ova Cisco-WAAS-Unified-6.4.1-b-36-npe.ova	VMware ESXi	vWAAS-150, vWAAS-200, WAAS-750, vWAAS-1300, vWAAS-2500, vWAAS-6000, vWAAS-6000R, WAAS-12000, vWAAS-50000, vWAAS-150000	vCM-100, vCM-500, vCM-1000, vCM-2000
Cisco-HyperV-vWAAS-unified-6.4.1-b-36.zip Cisco-HyperV-vWAAS-unified-6.4.1-b-36-npe.zip	Microsoft Hyper-V	vWAAS-150, vWAAS-200, WAAS-750, vWAAS-1300, vWAAS-2500, vWAAS-6000, vWAAS-6000R, WAAS-12000, vWAAS-50000	vCM-100, vCM-500, vCM-1000, vCM-2000
Cisco-KVM-vWAAS-Unified-6.4.1-b-36.tar.gz Cisco-KVM-vWAAS-Unified-6.4.1-b-36-npe.tar.gz	KVM CentOS	vWAAS-150, vWAAS-200, WAAS-750, vWAAS-1300, vWAAS-2500, vWAAS-6000, vWAAS-6000R, WAAS-12000, vWAAS-50000	vCM-100, vCM-500, vCM-1000, vCM-2000
Cisco-KVM-vWAAS-Unified-6.4.1-b-36.tar.gz Cisco-KVM-vWAAS-Unified-6.4.1-b-36-npe.tar.gz	Cisco NFVIS vBranch	vWAAS-150, vWAAS-200, WAAS-750, vWAAS-1300, vWAAS-2500, vWAAS-6000, vWAAS-6000R	Not supported
Cisco_NFVIS_3.7.1-FC3_WAAS-6.4.1-b36.iso.tar Cisco_NFVIS_3.7.1-FC3_WAASNPE-6.4.1-b36.iso.tar	Cisco ENCS-W	vWAAS-200, WAAS-750, vWAAS-1300, vWAAS-2500, vWAAS-6000R	Not supported
ISR-WAAS-6.4.1.36.ova ISR-WAAS-6.4.1.36-npe.ova	Cisco ISR-WAAS	vWAAS-200, WAAS-750, vWAAS-1300, vWAAS-2500	Not supported

Cloud Platforms Supported for vWAAS

Cisco vWAAS supports the following cloud computing platforms:

- Microsoft Azure—Used with vCM and vWAAS models supported on Microsoft Hyper-V. Cisco vWAAS in Azure is supported for vWAAS with WAAS Version 6.2.1x and later.
- OpenStack—Used with vCM and vWAAS models supported on KVM on CentOS, Cisco vWAAS in OpenStack is supported for vWAAS for WAAS Version 6.4.1b and later.

For more information, see Chapter 9, "Cisco vWAAS in Cloud Computing Systems".

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

This section contains the following topics:

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 with 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	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 vWAAS running on a UCS-E inside a Cisco ISR G2, where the UCS-E interface is configured as IP unnumbered in 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 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 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 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. **Note** 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. For more information on configuring L2 Inline interception on the WAAS CM, 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 vWAAS.

Table 2-2 CLI Commands for L2 Inline Traffic Interception

Mode	Command	Description
Global Configuration	**(config) interception-method inline**	Enables L2 inline traffic interception on vWAAS.
Interface Configuration	**(config-if) cdp**	Enables CDP (Cisco Discovery Protocol) on the interface on a WAAS device. (To globally enable the CDP 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 the *Cisco Wide Area Application Services Command Reference*.
	(config-if) ip	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.
	(config-if) ipv6	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.
	(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 WAAS device.
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	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 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 (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 in 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	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 **show version last** to display version information for the last saved image. • (Optional) Use **show version pending** to display version information for the pending upgraded image.
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.
show tfo detail	Displays TCP Fast Open (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.

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 with 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 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 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 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.

Cisco vWAAS on Cisco ISR-WAAS

This chapter describes how to use Cisco vWAAS on Cisco ISR-WAAS, and contains the following sections:

About Cisco ISR-WAAS

ISR-WAAS is the specific implementation of vWAAS running in a Cisco IOS-XE Software container on a Cisco ISR 4000 Series router (ISR-4321, ISR-4331, ISR-4351, ISR-4431, ISR-4451). In this context, “container” refers to the hypervisor that runs virtualized applications on a Cisco ISR 4000 Series router.

Note For vWAAS for WAAS 6.4.1b and later, ISR-4461 is also supported.

Table 3-1 shows the default number of CPUs, memory capacity, disk storage and supported ISR platforms for each ISR model.

Note We recommend you use ISR-WAAS-200 with vWAAS for WAAS 6.4.1c and later; this configuration reduces overall ISR-4321 memory by 3%.

Table 3-1 ISR Models: CPUs, Memory, Disk Storage and Supported ISR Platforms

ISR WAAS Model	CPUs	Memory	Disk Storage	Supported ISR Platform
ISR-WAAS-200 (for WAAS 5.x and 6.2.1)	1	3 GB	151 GB	ISR-4321
ISR-WAAS-200 (for WAAS 6.2.3x and later	1	4 GB	151 GB	ISR-4321
ISR-WAAS-200 (for WAAS 6.41c and later)	1	3.75 GB	151 GB	ISR-4321
ISR-WAAS-750	2	4 GB	151 GB	ISR-4351, ISR-4331, ISR-4431, ISR-4451

ISR WAAS Model	CPUs	Memory	Disk Storage	Supported ISR Platform
750 ISR WAAS (for WAAS 6.4.1b and later)	2	4 GB	151 GB	ISR-4351, ISR-4331, ISR-4431, ISR-4451, ISR-4461
1300 ISR WAAS	4	6 GB	151 GB	ISR-4431, ISR-4451
1300 ISR WAAS (for WAAS 6.4.1b and later)	4	6 GB	151 GB	ISR-4431, ISR-4451, ISR-4461
2500 ISR WAAS	6	8 GB	338 GB	ISR-4451
2500 ISR WAAS (for WAAS 6.4.1b and later)	6	8 GB	338 GB	ISR-4451, ISR-4461

Operating Guidelines for ISR-WAAS:

- For vWAAS with WAAS Version 6.2.3c or later, for ISR-4321 with profile ISR-WAAS-200, the ISR-WAAS RAM is increased from 3 GB to 4 GB. For this increase in ISR-WAAS RAM to be implemented, you must complete a new OVA deployment of WAAS version 6.2.3c or later. The increase in ISR-WAAS RAM is not automatically implemented with an upgrade to WAAS Version 6.2.3c or later.
  - For ISR-WAAS-200 in ISR-4321 with IOS-XE 16.x, 4 GB of memory is mandatory.
  - For ISR-WAAS-200 in ISR-4321 with IOX-XE 3.x, 3 GB of memory is recommended; 4 GB of memory is optional.

Note ISR-4321 with IOS-XE 16.9.x is supported for vWAAS for WAAS Version 6.4.1b and later.

Supported Host Platforms, Software Versions, and Disk Types

Table 3-2 shows the platforms and software versions supported for vWAAS on ISR-WAAS.

Table 3-2 Platforms and Software Versions Supported for vWAAS on ISR-WAAS

PID and Device Type	Minimum WAAS Version	Host Platforms	Minimum IOS Version	Disk Type
PID: OE-VWAAS-KVM Device Type: ISR-WAAS	6.4.1b 5.4.1 5.2.1 (ISR-4451)	ISR-4461 (vWAAS-750, 1300, 2500) ISR-4451 (vWAAS-750, 1300, 2500) ISR-4431 (vWAAS-750, 1300) ISR-4351 (vWAAS-750) ISR-4331 (vWAAS-750) ISR-4321 (vWAAS-200)	IOS-XE 3.9	ISR-SSD NIM-SSD

Cisco OVA Packages for vWAAS on ISR-WAAS

Cisco provides an OVA or NPE OVA package for vWAAS on ISR-WAAS in the formats shown in Table 3-3.

Table 3-3 Cisco OVA Package Formats for vWAAS on ISR-WAAS

Package Format	File Format Example
Cisco ISR WAAS (200, 750, 1300, 2500) NPE OVA file	ISR-WAAS-6.4.1a.68-npe.ova
Cisco ISR WAAS (200, 750, 1300, 2500) OVA file	ISR-WAAS-6.4.1a.68.ova

For a listing of hypervisor OVA and NPE OVA 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.

Deploying and Managing vWAAS on ISR-WAAS

This section contains the following topics:

- Components for Deploying and Managing vWAAS on ISR-WAAS
- ISR-WAAS DRE Disk, Object Cache, and Akamai Connect Cache

ISR-WAAS DRE Disk, Object Cache, and Akamai Connect Cache

Table shows the

Table 3-4 DRE Disk, Object Cache, and Akamai Connect Cache by ISR-WAAS Model

ISR-WAAS Model	DRE Disk Capacity	Default Object Cache Capacity	Default Akamai Connect Cache Capacity
ISR-WAAS-200	75 GB	32 GB	30 GB
ISR-WAAS-750	73 GB	32 GB	30 GB
ISR-WAAS-1300	71 GB	32 GB	30 GB
ISR-WAAS-2500	210 GB	52 GB	50 GB

- T

Components for Deploying and Managing vWAAS on ISR-WAAS

Table 3-5 shows the components used to deploy vWAAS on ISR-WAAS, and Table 3-6 shows the components used to manage vWAAS on ISR-WAAS.

Table 3-5 Components for Deploying vWAAS on ISR-WAAS

Package Format	Deployment Tool	Pre-Configuration	Network Driver
OVA	Ezconfig	onep	virtio_net

Table 3-6 Components for Managing vWAAS on ISR-WAAS

vCM Models Supported	vWAAS Models Supported	Number of Instances Supported	Traffic Interception Method
N/A	vWAAS-200, 750, 1300, 2500	1	AppNav-XE

Cisco vWAAS on VMware ESXi

This chapter describes how to use Cisco vWAAS on VMware vSphere ESXi, and contains the following sections:

About Cisco vWAAS on VMware ESXi

Cisco vWAAS for VMware ESXi provides cloud-based application delivery service over the WAN in ESX/ESXi-based environments. Cisco vWAAS on VMware vSphere ESXi is delivered an OVA file. The vSphere client takes the OVA file for a specified vWAAS model, and deploys an instance of that vWAAS model.

Supported Host Platforms, Software Versions, and Disk Type

Table 4-1 shows the platforms and software versions supported for vWAAS on VMware ESXi.

Table 4-1 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-ESX • Device Type: OE-VWAAS-ESX	• 5.0.3g	• Cisco UCS (Unified Computing System) • Cisco UCS-E Series	• ESXi 5.0	• VMDK

VMware ESXi for Cisco vWAAS and Cisco WAAS

This section contains the following topics:

VMware ESXi Versions Supported for Cisco WAAS

Table 4-2 VMware ESXi Versions Supported for Cisco WAAS

ESX version	WAAS v5.1	WAAS v5.2	WAAS v5.3	WAAS v5.4	WAAS v5.5	WAAS v6.x
ESXi 6.5 vWAAS fresh installation	x	x	x	x	x	x
ESXi 6.5 vWAAS upgrade	x	x	x	x	x	x
ESXi 6.0 vWAAS fresh installation	x	x	x	x	x	Supported OVA
ESXi 6.0 vWAAS upgrade	x	x	x	x	x	Upgrade with .bin file
ESXi 5.5 vWAAS fresh installation	x	x	Supported OVA	Supported OVA	Supported OVA	Supported OVA
ESXi 5.5 vWAAS upgrade	x	x	Upgrade with .bin file	Upgrade with .bin file	Upgrade with .bin file	Upgrade with .bin file
ESXi 5.0/5.1 vWAAS fresh installation	Supported OVA	Supported OVA	Supported OVA	Supported OVA	Supported OVA	Supported OVA
ESXi 4.1/5.0 vWAAS upgrade	Upgrade with .bin file	Upgrade with .bin file	Upgrade with .bin file	Upgrade with .bin file	Upgrade with .bin file	x
ESXi 4.1 vWAAS fresh installation	Supported OVA	Install vWAAS 5.1 OVA, then upgrade using .bin file, or Migrate from ESXi 4.1 to 5.0/5.1	x	x	x	x

Note For vWAAS with ESXi Version 5.5 on a Cisco UCS host: if the DRE latency threshold or an AO timeout alarm occurs, check for the I/O command abort in the vWAAS. To do this, use the **copy sysreport** EXEC command.

If the I/O abort is observed:
Upgrade the RAID controller's driver to Version 6.610.19.00 or later.

If the I/O abort is still observed after the RAID controller driver upgrade:
Capture and share the following logs for further analysis:
—Guest-VM sysreport
—VMware's host diagnostic report
—RAID controller's firmware log

ESXi Server Datastore Memory and Disk Space for vWAAS and vCM Models

This section contains the following topics:

- Table 4-3 shows ESXi server datastore memory and disk space per vWAAS model, for WAAS v4.3.1 through v5.3.5, and for WAAS v5.4.x through v6.x.
- Table 4-4 shows ESXi server datastore memory and disk space per vCM model, for WAAS v4.3.1 through v5.3.5, and for WAAS v5.4.x through v6.x.

Table 4-3 vCPUs, ESXi Server Datastore Memory, and Disk Space by vWAAS Model

	For WAAS v4.3.1 through v5.3.5			For WAAS v5.4.x through v6.x		
vWAAS Model	**vCPUs**	**Datastore Memory**	**Disk**	**vCPUs**	**Datastore Memory**	**Disk**
vWAAS-150 (for WAAS Version 6.x)	---	---	---	1	3 GB	160 GB
vWAAS-200	1	2 GB	160 GB	1	3 GB	260 GB
vWAAS-750	2	4 GB	250 GB	2	4 GB	500 GB
vWAAS-1300	2	6 GB	300 GB	2	6 GB	600 GB
vWAAS-2500	4	8 GB	400 GB	4	8 GB	750 GB
vWAAS-6000	4	8 GB	500 GB	4	11 GB	900 GB
vWAAS-12000	4	12 GB	750 GB	4	12 GB	750 GB
vWAAS-50000	8	48 GB	1500 GB	8	48 GB	1500 GB

Table 4-4 vCPUs, ESXi Server Datastore Memory, and Disk Space by vCM Model

	For WAAS v4.3.1 through v5.3.5			For WAAS v5.4.x through v6.x		
vCM Model	**vCPUs**	**Datastore Memory**	**Disk**	**vCPUs**	**Datastore Memory**	**Disk**
vCM-100N	2	2 GB	250 GB	2	2 GB	250 GB
vCM-500N	---	---	---	2	2 GB	300 GB
vCM-1000N	---	---	---	2	4 GB	400 GB
vCM-2000N	4	8 GB	600 GB	4	8 GB	600 GB

OVA Package Formats for vWAAS on VMware ESXI

This section contains the following topics:

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.

OVA Package for vWAAS on VMware ESXi for WAAS Version 5.x to 6.2.x

For vWAAS on VMware ESXi, for WAAS Version 5.x through 6.2.x, Cisco provides an OVA or NPE OVA package for each vWAAS connection profile (examples shown in Table 4-5) and for each vCM connection profile (examples shown in Table 4-6).

Table 4-5 Cisco OVA Package Format Examples for vWAAS on VMware ESXi

Package Format	File Format Example
Cisco vWAAS 150 package file	• Cisco-vWAAS-150-6.2.3d-b-68.ova
Cisco vWAAS 150 package file for NPE	• Cisco-vWAAS-150-6.2.3d-npe-b-68.ova
Cisco vWAAS 200 package file	• Cisco-vWAAS-200-6.2.3d-b-68.ova
Cisco vWAAS 200 package file for NPE	• Cisco-vWAAS-200-6.2.3d-npe-b-68.ova
Cisco vWAAS 750 package file	• Cisco-vWAAS-750-6.2.3d-b-68.ova
Cisco vWAAS 750 package file for NPE	• Cisco-vWAAS-750-6.2.3d-npe-b-68.ova
Cisco vWAAS 1300 package file	• Cisco-vWAAS-1300-6.2.3d-b-68.ova
Cisco vWAAS 1300 package file for NPE	• Cisco-vWAAS-1300-6.2.3d-npe-b-68.ova
Cisco vWAAS 2500 package file	• Cisco-vWAAS-2500-6.2.3d-b-68.ova
Cisco vWAAS 2500 package file for NPE	• Cisco-vWAAS-2500-6.2.3d-npe-b-68.ova
Cisco vWAAS 6000 package file	• Cisco-vWAAS-6000-6.2.3d-b-68.ova
Cisco vWAAS 6000 package file for NPE	• Cisco-vWAAS-6000-6.2.3d-npe-b-68.ova
Cisco vWAAS 12k package file	• Cisco-vWAAS-12k-6.2.3d-b-68.ova
Cisco vWAAS 12k package file for NPE	• Cisco-vWAAS-12k-6.2.3d-npe-b-68.ova
Cisco vWAAS 50k package file	• Cisco-vWAAS-50k-6.2.3d-b-68.ova
Cisco vWAAS 50k package file for NPE	• Cisco-vWAAS-50k-6.2.3d-npe-b-68.ova

Table 4-6 Cisco OVA Package Formats for vCM for WAAS Versions earlier than Version 6.4.1

Package Format	File Format Example
Cisco vCM 100N package file	• Cisco-vCM-100N-6.2.3d-b-68.ova
Cisco vCM 100N package file for NPE	• Cisco-vCM-100N-6.2.3d-npe-b-68.ova

OVA Package for vWAAS on VMware ESXi for WAAS Version 6.4.1 and Later

For vWAAS on VMware ESXi, for WAAS Version 6.4.1 and later, Cisco provides a single, unified OVA for NPE and non-NPE version of the WAAS image for all the vWAAS models for that hypervisor.

Each unified OVA package is a pre-configured virtual machine image that is ready to run on a particular hypervisor. The launch script for each unified OVA package file 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 in VMware ESXi:

- OVA—Cisco-ESXi-vWAAS-Unified-6.4.1-b-33.ova
- NPE OVA—Cisco-ESXi-vWAAS-Unified-6.4.1-b-33-npe.ova

The unified OVA package for VMware ESXi contains the following files.

- OVF file—Contains all resource information.
- Flash disk image
- Data system disk
- Akamai disk

Use the VMware ESXi OVF template wizard to deploy these files, described in Installing VMware ESXi for vWAAS for WAAS Version 6.4.1 and Later.

Installing vWAAS on VMware ESXi

This section has the following topics:

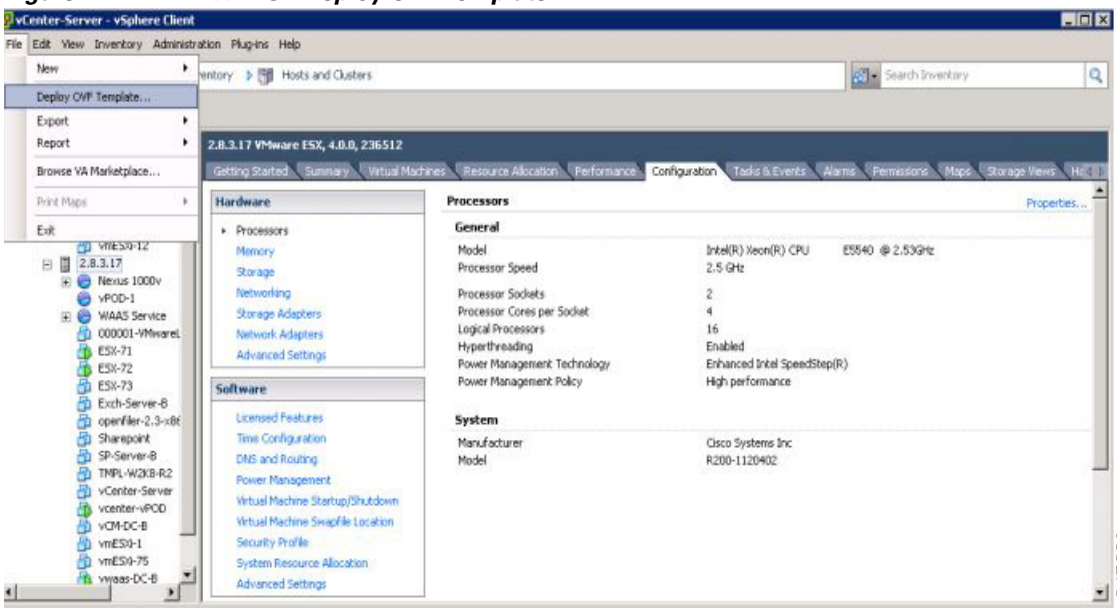
Installing VMware ESXi for vWAAS for WAAS Versions 5.x to 6.2.x

To install the vWAAS Virtual Machine (VM) with VMware vSphere ESXi, follow these steps:

Step 1 From the vSphere Client, choose **File > Deploy OVF Template**.

The Source window appears (Figure 4-1).

Figure 4-1 vWAAS - Deploy OVF Template



Step 2 Click **Browse**.

The Open window appears.

Step 3 Navigate to the location of the vWAAS OVA file and click **Open**.

- If the virtual host was created using an OVA of vWAAS for WAAS Version 5.1.x or later, proceed to Step 4.
- If the virtual host was created using an OVA file of vWAAS for WAAS Version 5.0 or earlier, and you have upgraded vWAAS from inside 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.

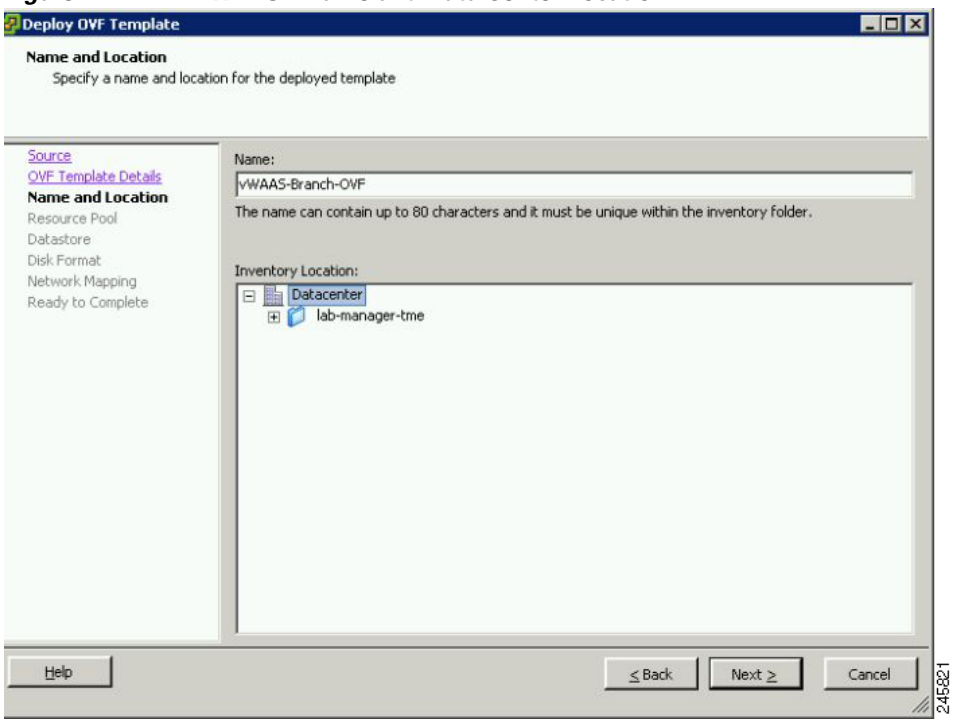
Step 4 Click **Next** to accept the selected OVA file.

The Name and Location window appears.

Step 5 Enter a name for the vWAAS VM, choose the appropriate data center, and then click **Next**.

The Cluster window appears (if a cluster is configured), or the Resource Pool window appears (if a resource pool is configured). Otherwise, the Datastore window appears (in this case, skip to Step 7).

Figure 4-2 vWAAS - Name and Data Center Location

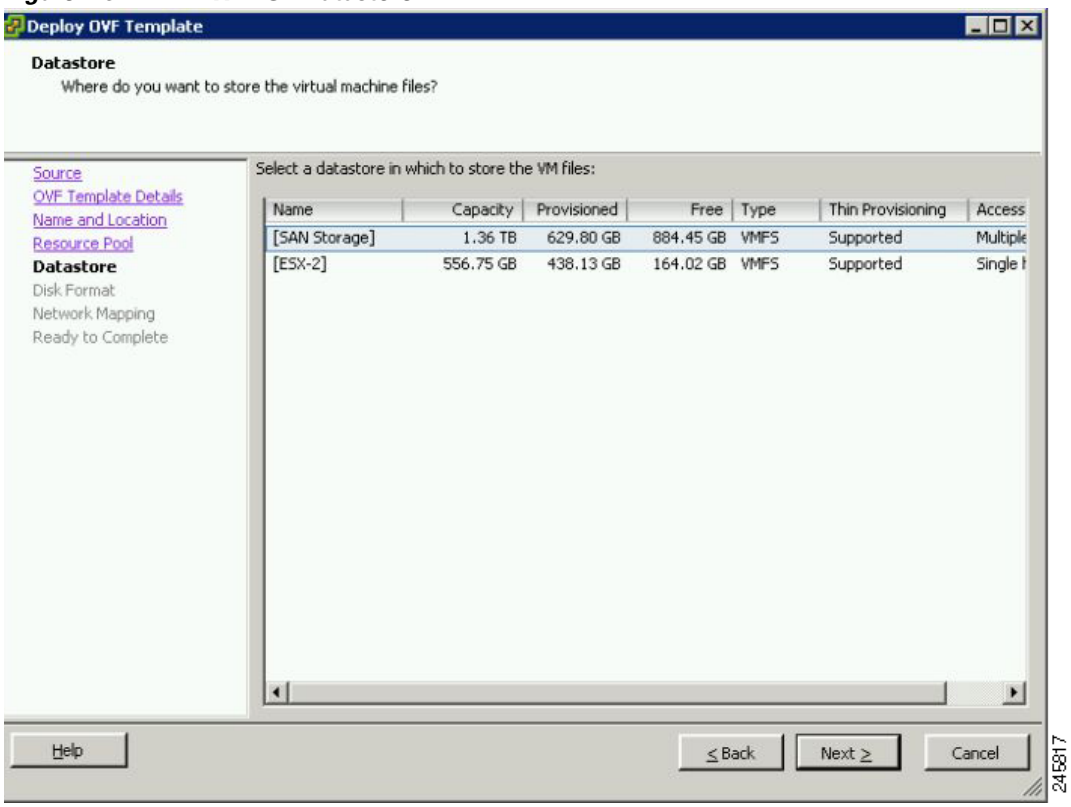


Step 6 If configured, choose a cluster for the vWAAS VM or, if configured, choose the resource pool and then click **Next**.

The Datastore window appears.

Step 7 Choose a datastore to host the virtual machine and click **Next**.

Figure 4-3 vWAAS - Datastore



Note The datastore must be formatted with a block size greater than 1 MB to support file sizes larger than 256 GB.

The Create a Disk window appears.

Step 8 The Disk Provisioning section has three disk format options: Thick Provision Lazy Zeroed, Thick Provision Eager Zeroed, and Thin Provision. Select **Thick Provision Eager Zeroed**.

Note You must choose the **Thick Provision Eager Zeroed** disk format for vWAAS deployment; this is the format recommended with vWAAS deployment for a clean installation.

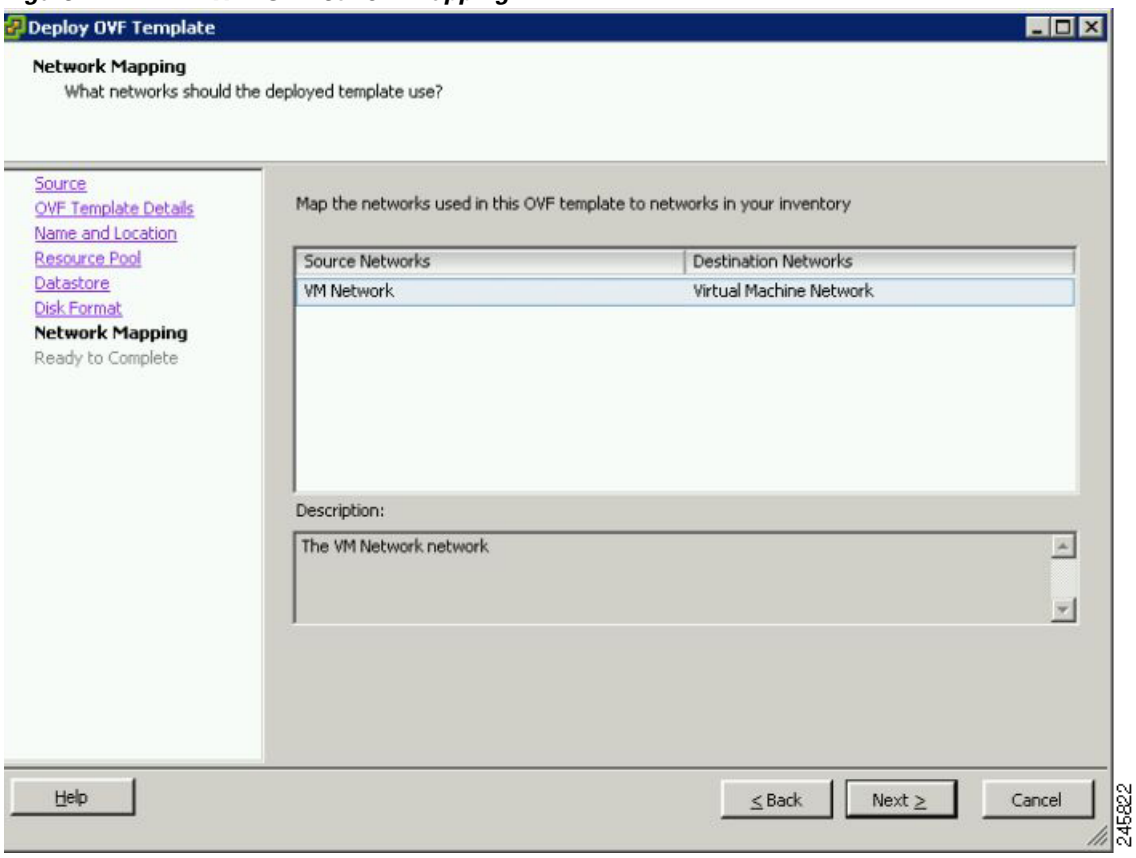
Step 9 Click **Next**.

The Network Mapping window appears.

Step 10 Choose the network mapping provided by ESXi and click **Next**. You have the option to change this later if necessary.

The Ready to Complete window appears.

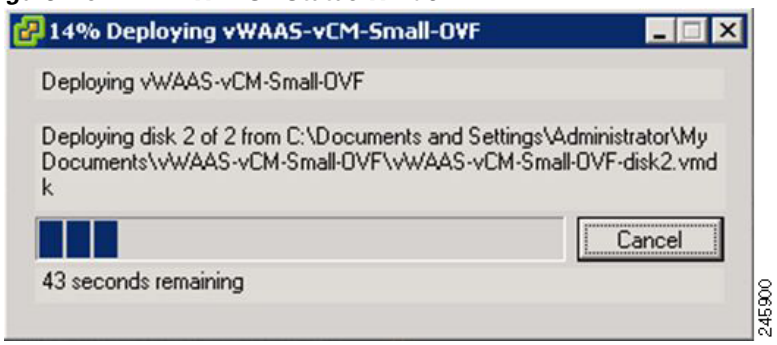
Figure 4-4 vWAAS - Network Mapping



Step 11 Click **Finish** to complete the installation.

The status window appears while the OVA file is being deployed.

Figure 4-5 vWAAS - Status Window



Step 12 When the deployment is finished, the Deployment Completed Successfully window appears.

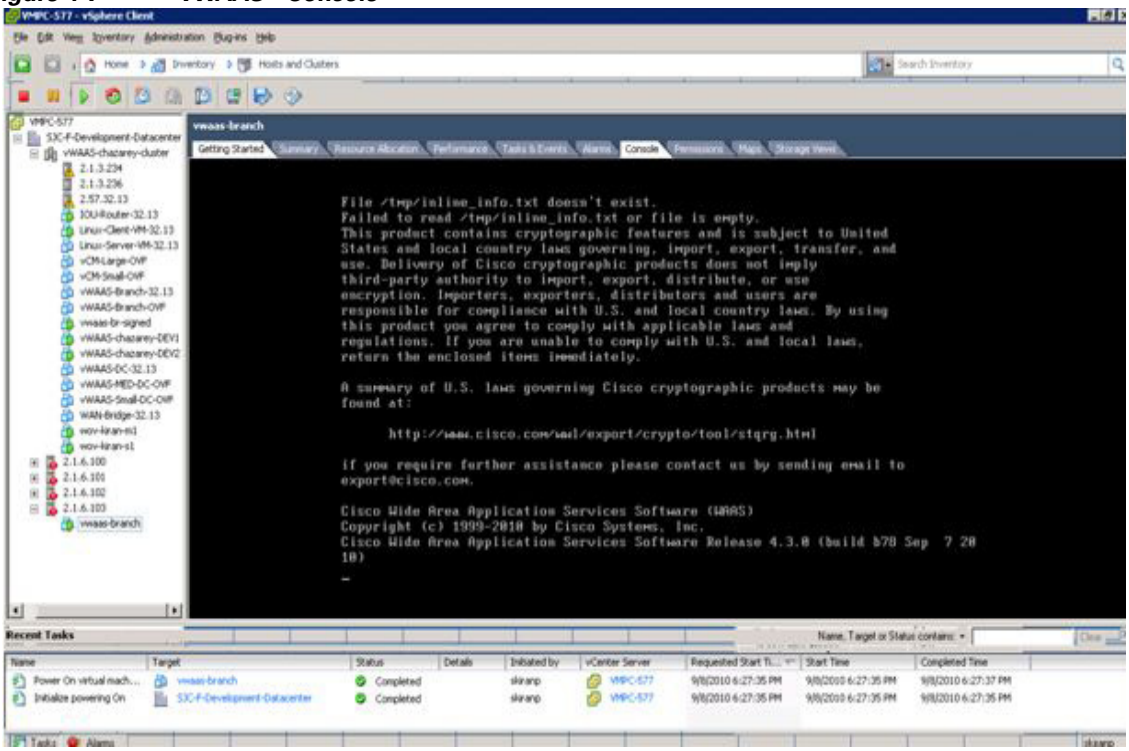
Figure 4-6 vWAAS - Completed

Step 13 Click **Close**.

Step 14 You are ready to start the VM. Highlight the vWAAS VM and click **Power on Virtual Machine**.

Step 15 After vWAAS finishes booting, click the **Console** tab to view boot up messages.

Figure 4-7 vWAAS - Console



Note Under rare conditions, the vWAAS VM may boot into diskless mode if other VMs on the host VM server do not release control of system resources or the physical disks become unresponsive. For information on how to resolve this situation, see Resolving Diskless Startup and Disk Failure in Chapter 10, "Troubleshooting Cisco vWAAS."

For vWAAS configuration information, see Chapter 2, "Configuring Cisco vWAAS and Viewing vWAAS Components".

Installing VMware ESXi for vWAAS for WAAS Version 6.4.1 and Later

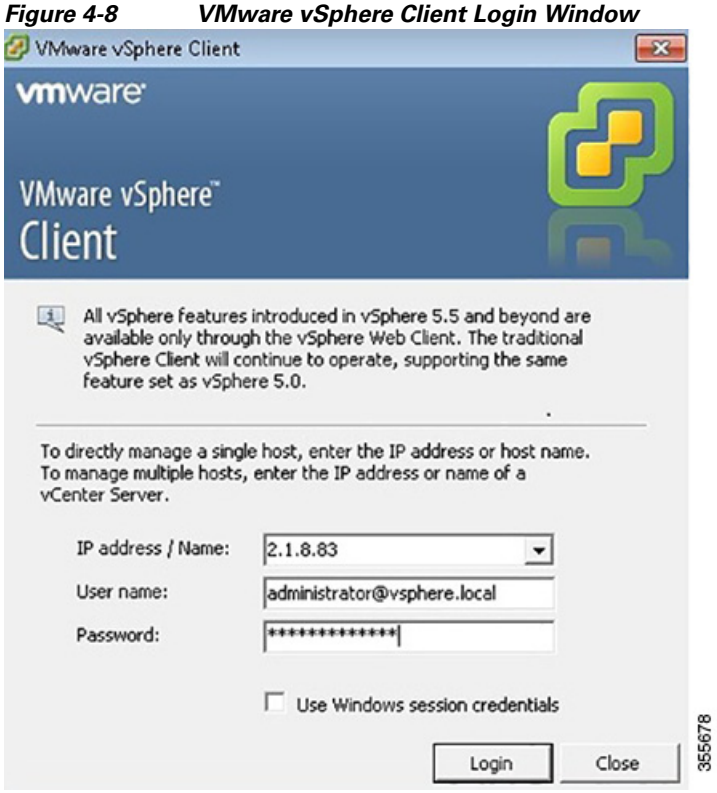
vWAAS for WAAS Version 6.4.1 and later supports VMware vCenter Version 6.0.0. To deploy any vWAAS or vCM Model for WAAS Version 6.4.1 and later on VMware ESXi, register the ESXi host with VMware vSphere vCenter version 6.0.

Note The OVA deployment for WAAS Version 6.4.1 and later must be done only through VMware vCenter.

To deploy the VMware ESXi hypervisor for vWAAS for WAAS Version 6.4.1 and later, follow these steps:

Step 1 Log in into the VMware vCenter using VMware vSphere Client (Figure 4-8).

Figure 4-8 VMware vSphere Client Login Window



Step 2 To begin the task of adding the ESXi host into the datacenter on VMware vCenter Client, you must first create a datacenter. Navigate to **Actions > New Datacenter...** .

Step 3 At the Create Datacenter page, click **Add**.

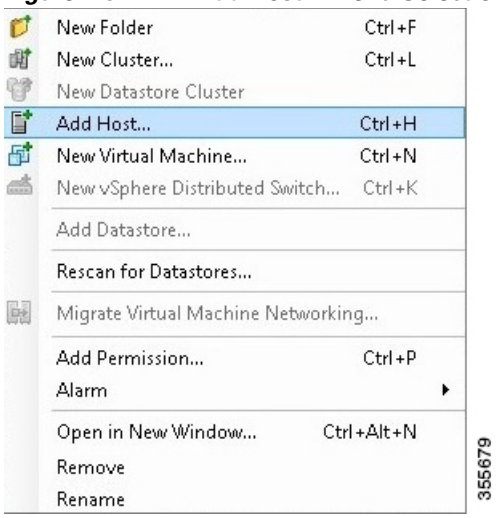
Step 4 In the **Create Datacenter** dialog box:

a. In the Name field enter a name for the datacenter. The name can contain up to 16 alphanumeric characters with no spaces and no special characters.

b. In the Description field enter a description for this datacenter.

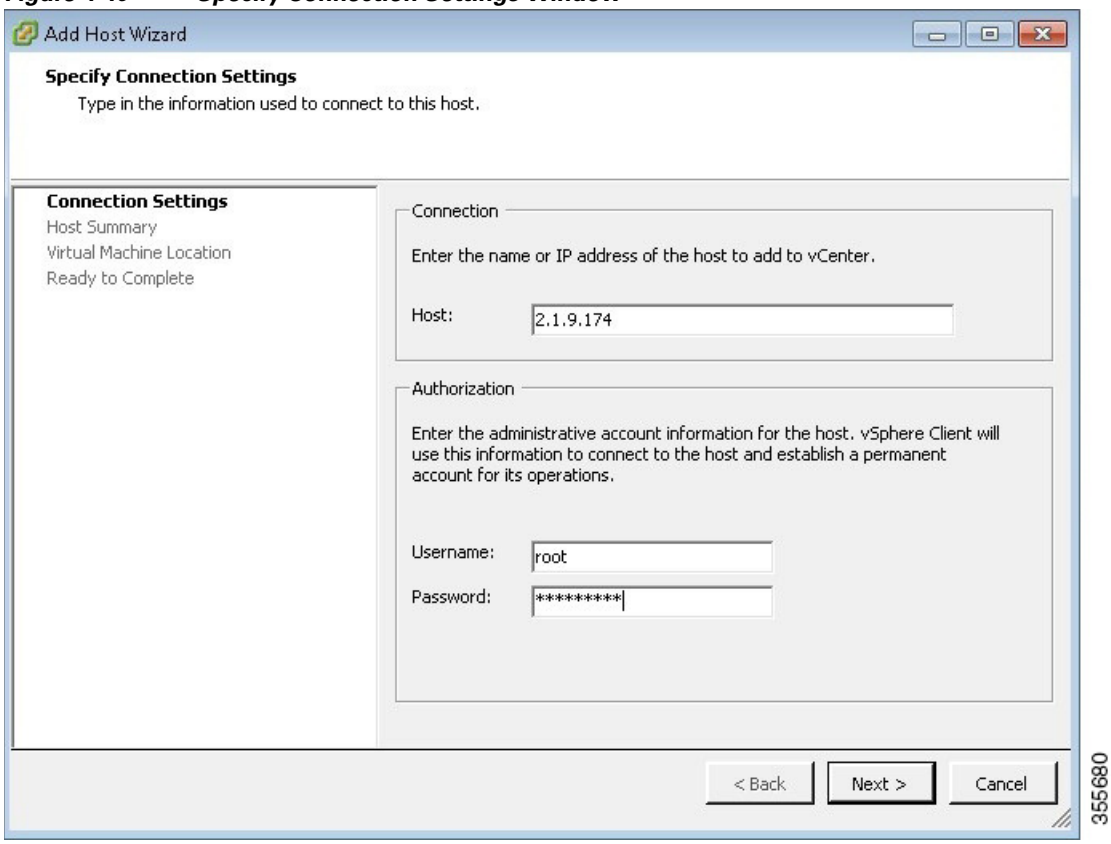
Step 5 To add the host into the datacenter on VMware vCenter Client, navigate to the **Getting Started** tab > **Add Host...** menu selection (Figure 4-9).

Figure 4-9 Add Host... Menu Selection



Step 6 Choose **Specify Connection Settings** and the Specify Connection Settings window appears (Figure 4-10).

Figure 4-10 Specify Connection Settings Window



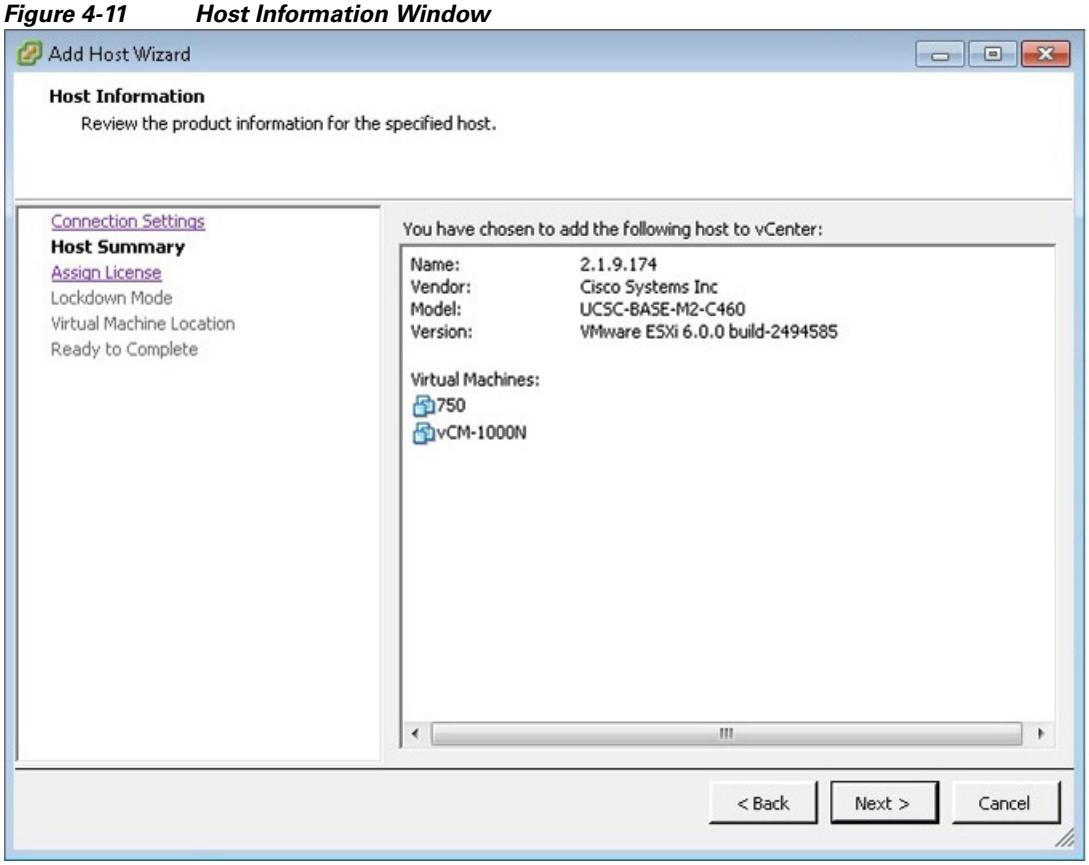
a. In the Connection pane **Host** field, enter the ESXi host name or IP address.

b. In the Authorization pane **Username** and **Password** fields, enter the ESXi username and password.

c. Click **Next**.

Step 7 The Host Information window appears (Figure 4-11), which displays information you can review for the specified host, including host name or IP address, vendor name, model name and number, the VMware version, and the associated virtual machines.

Figure 4-11 Host Information Window



a. If the displayed host information meets your system requirements, click **Next**.

Step 8 The Assign License window appears.

There are two options: **Assign an existing license key to this host** and **Assign a new license key to this host**.

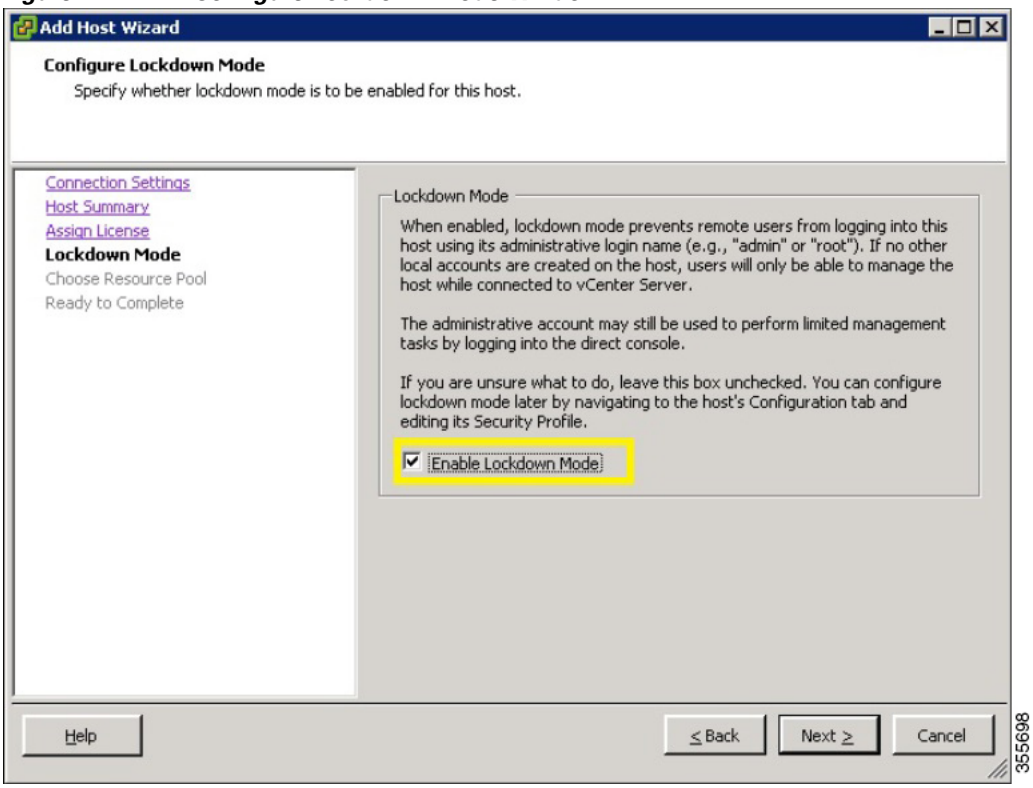
a. Use one of the radio buttons to assign an existing license key or to assign a new license key to this host.

b. Click **Next**.

Note Licenses are installed and managed only on individual devices, not device groups. For more information about licenses, see the "Configuring Other System Settings" chapter, section "Managing Software Licenses" of the *Cisco Wide Area Application Services Configuration Guide*.

Step 9 The Configure Lockdown Mode window appears (Figure 4-12).

Figure 4-12 Configure Lockdown Mode Window



Step 10 Lockdown mode is disabled by default.

- Leave the **Enable Lockdown Mode** check box unchecked to keep lockdown mode disabled.

  When lockdown mode is disabled, all router and module communication commands behave normally.

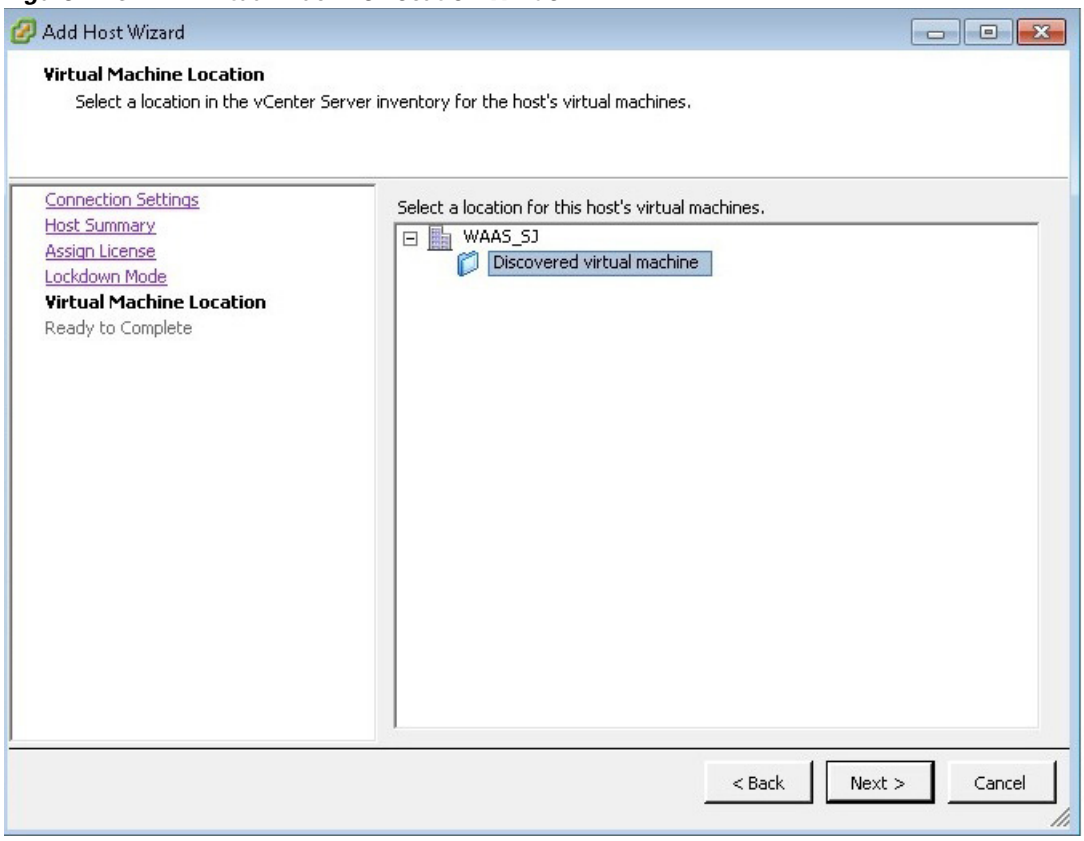
- Check the **Enable Lockdown Mode** check box to enable lockdown mode.

  When lockdown mode is enabled, the VMware vSphere Hypervisor host can be only be managed by the VMware vCenter Server using its internal user called **vpxuser**. All other configuration methods, such as the vSphere Client, PowerCLI, and vCLI are disabled.

Step 11 Click **Next**.

Step 12 The Virtual Machine Location window appears (Figure 4-13).

Figure 4-13 Virtual Machine Location Window

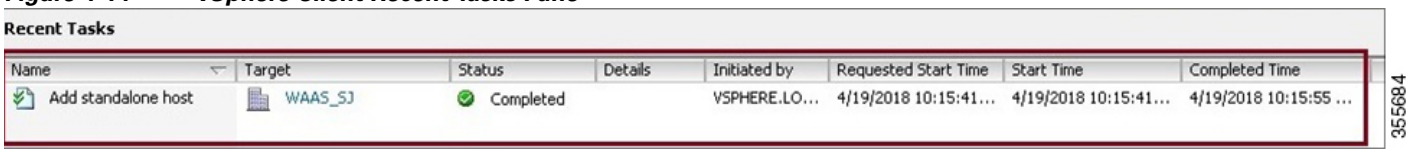


a. Select a location in the vCenter Server Inventory for the specified host's virtual machines.

b. Click **Next**.

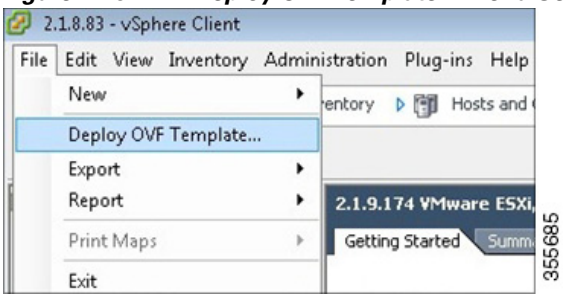
Step 13 The vSphere Client window is displayed with the Recent Tasks pane displaying a Completed status for this task (Figure 4-14).

Figure 4-14 vSphere Client Recent Tasks Pane



Step 14 Navigate to **File > Deploy OVF Template...** (Figure 4-15).

Figure 4-15 Deploy OVF Template... Menu Selection

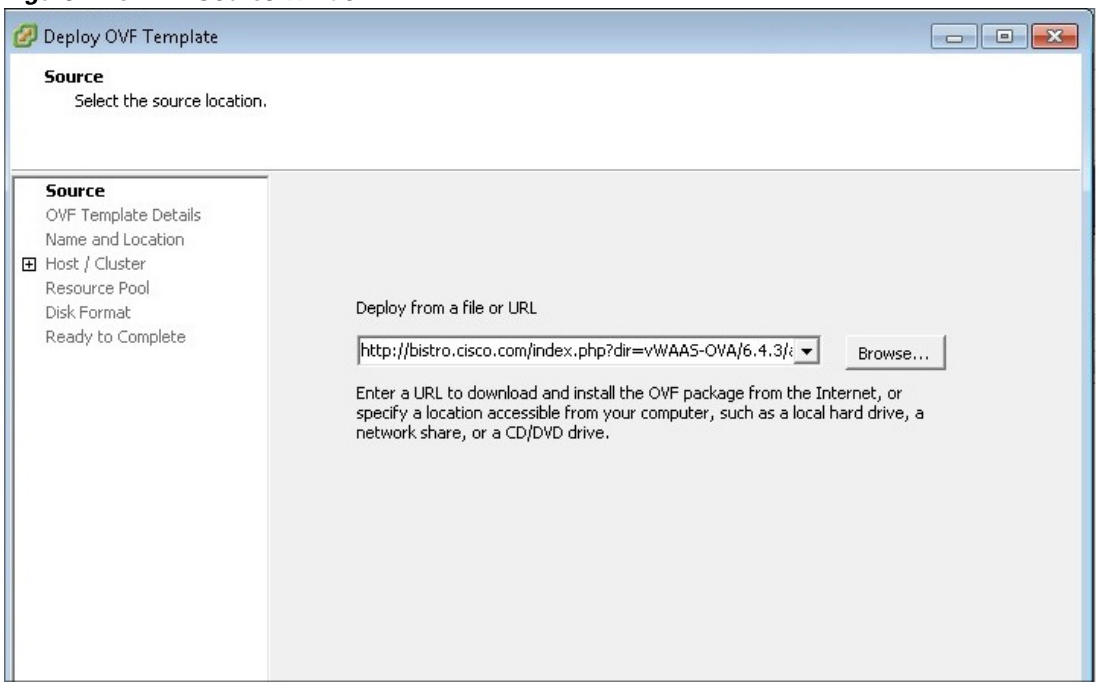


Step 15 Download the vWAAS OVA from the Cisco Wide Area Application Services (WAAS) Download Software Page.

Step 16 Navigate to **File** > **Deploy OVF Template**... > **Source**.

Step 17 The Source window appears (Figure 4-16), where you select the OVA file.

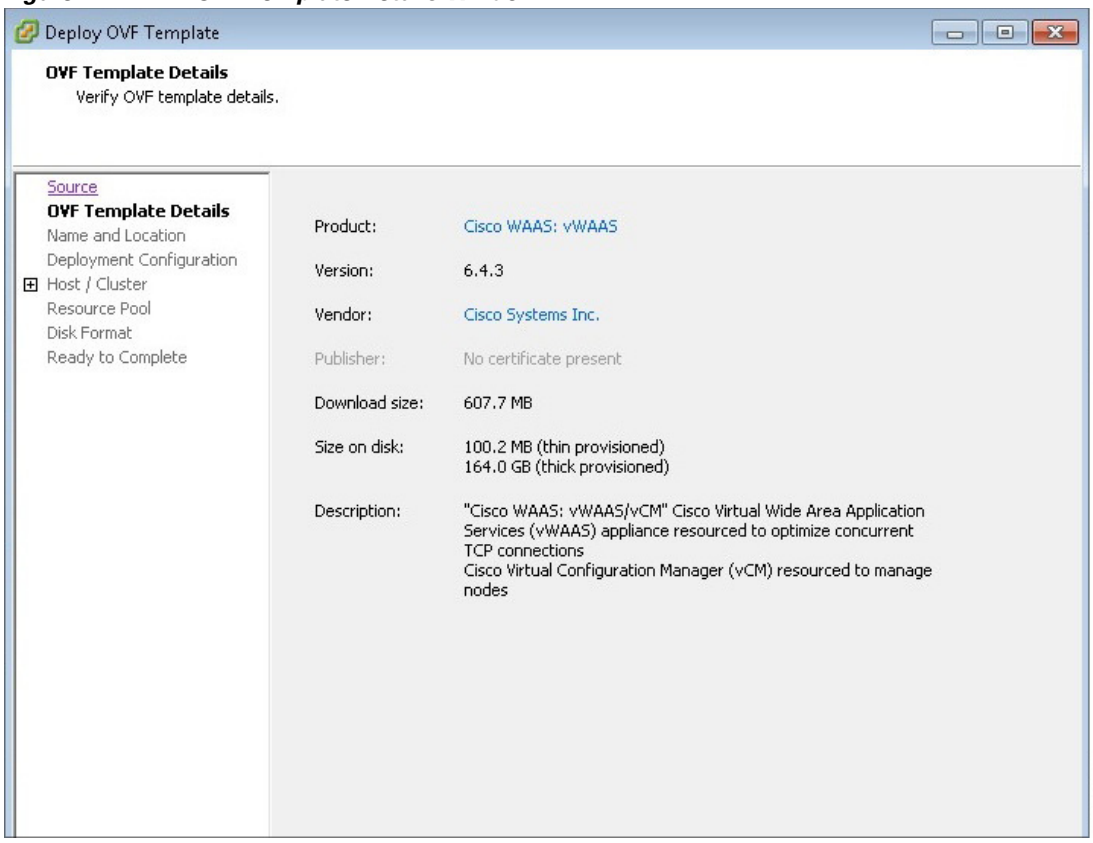
Figure 4-16 Source Window



a. From the **Deploy from a file or URL** drop-down list, select the OVA file.

Step 18 The OVF Template Details window appears (Figure 4-17), where you can verify the OVF template details including product name, version, vendor, download size, size on disk, and a description.

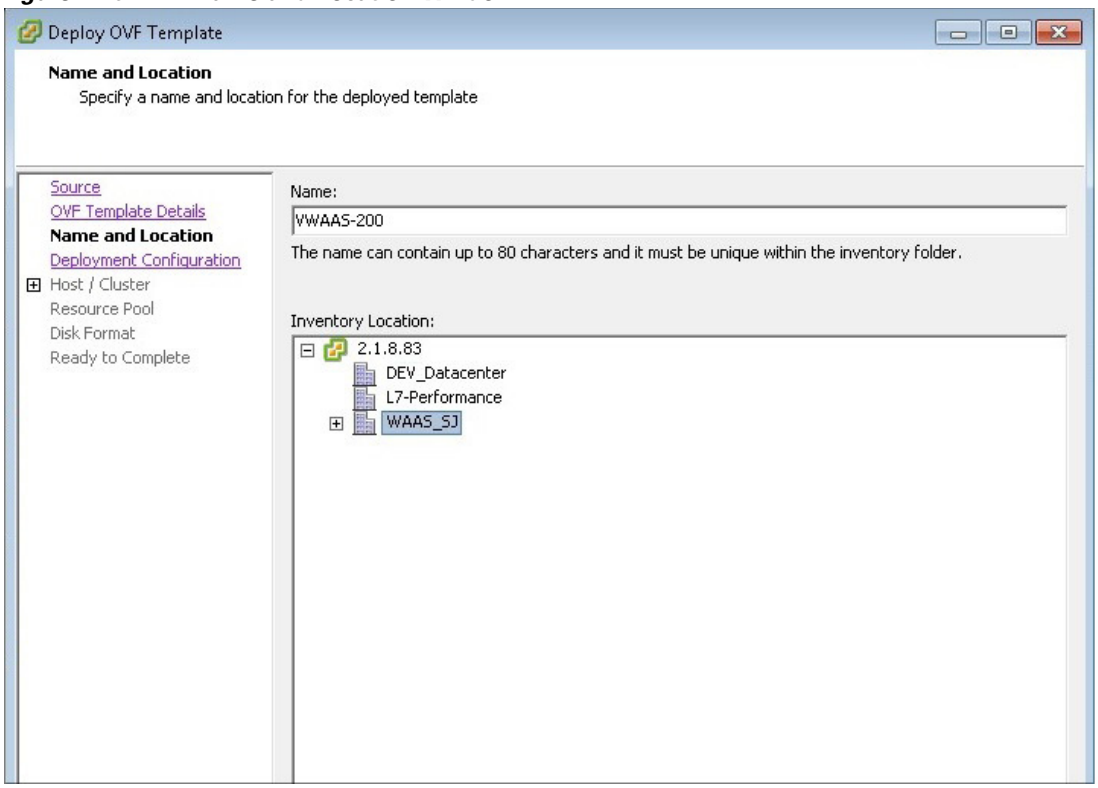
Figure 4-17 OVF Template Details Window



a. To accept the selected OVA file, click **Next**.

Step 19 The Name and Location window appears (Figure 4-18), where you specify a name and location for the deployed template.

Figure 4-18 Name and Location Window



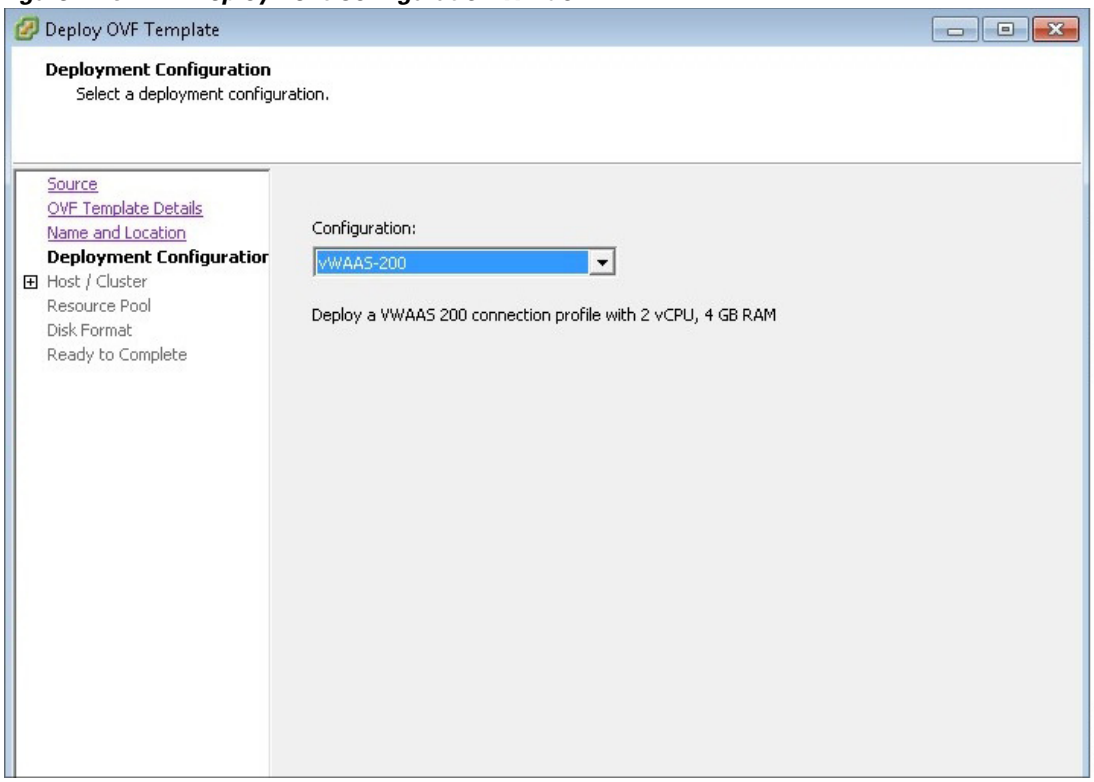
a. In the **Name** field, enter the name for the vWAAS VM.

b. At the **Inventory Location** listing, select the location to deploy (datacenter).

c. Click **Next**.

Step 20 The Deployment Configuration window appears (Figure 4-19).

Figure 4-19 Deployment Configuration Window

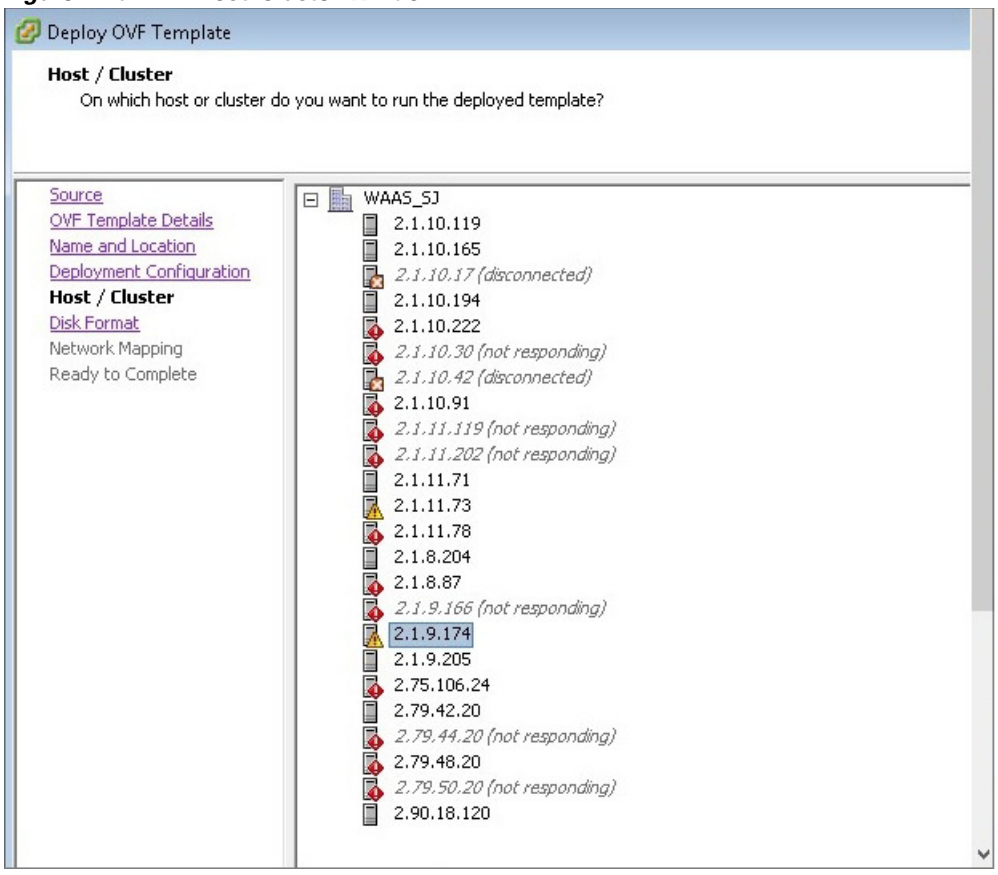


a. From the **Configuration** drop-down list, choose the vWAAS model to deploy. After you choose a vWAAS model, the window displays a description of the vWAAS model, such as "Deploy a vWAAS-200 connection profile with 2 vCPU, 4 GB RAM."

b. Click **Next**.

Step 21 The Host/Cluster window is displayed (Figure 4-20), where you can choose a host or cluster to run the deployed template.

Figure 4-20 Host/Cluster Window

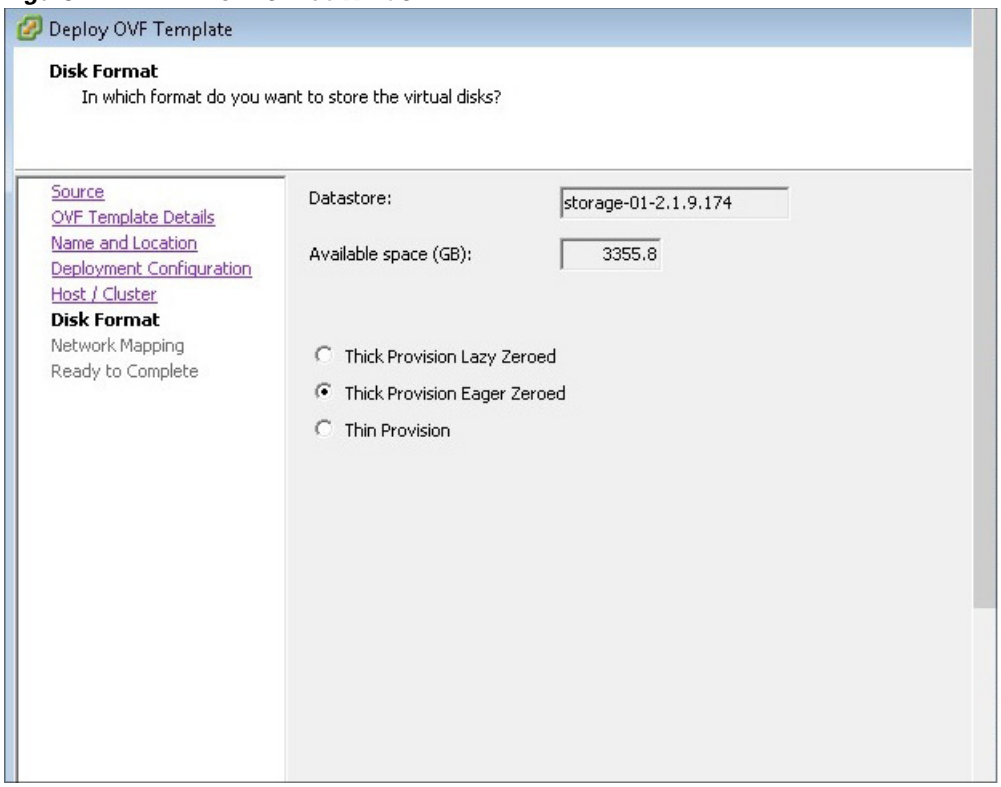


a. Select the ESXi host or cluster where you need to run the deployed template.

b. Click **Next**.

Step 22 The Disk Format window is displayed (Figure 4-21), which displays data store address and available disk space, in GB, and provisioning choices.

Figure 4-21 Disk Format Window

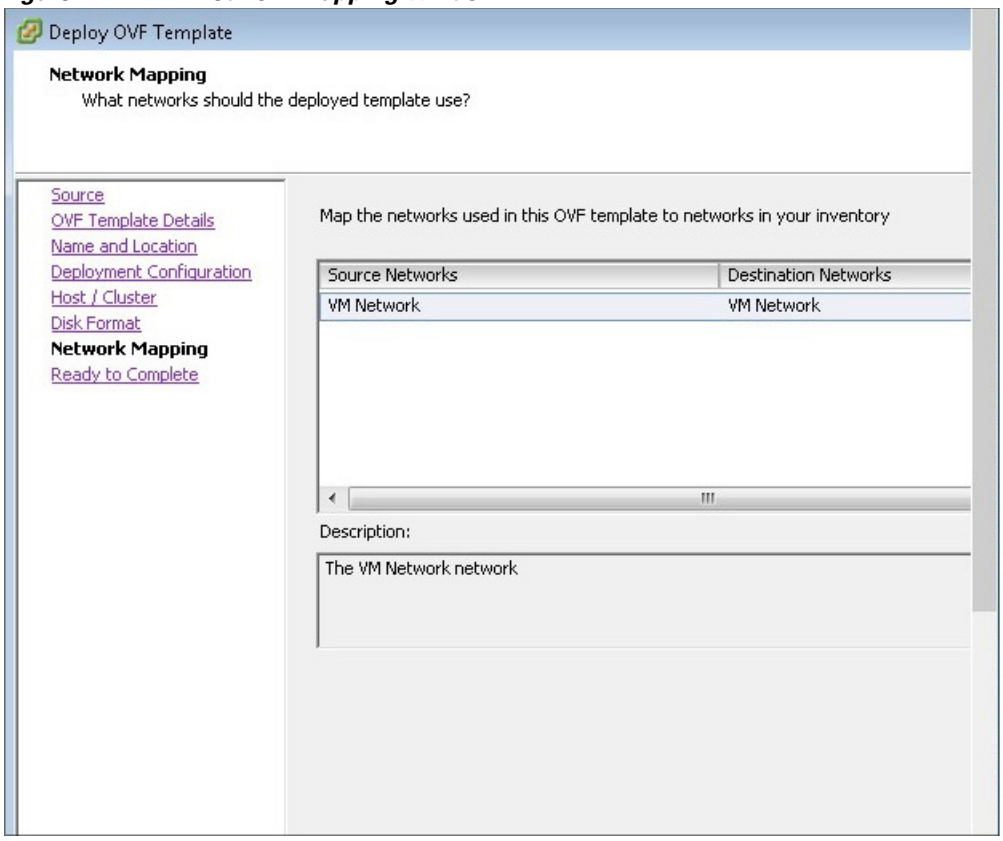


Note You must choose **Thick Provision Eager Zeroed** for vWAAS deployment.

a. Click **Next**.

Step 23 The Network Mapping window appears (Figure 4-22).

Figure 4-22 Network Mapping Window

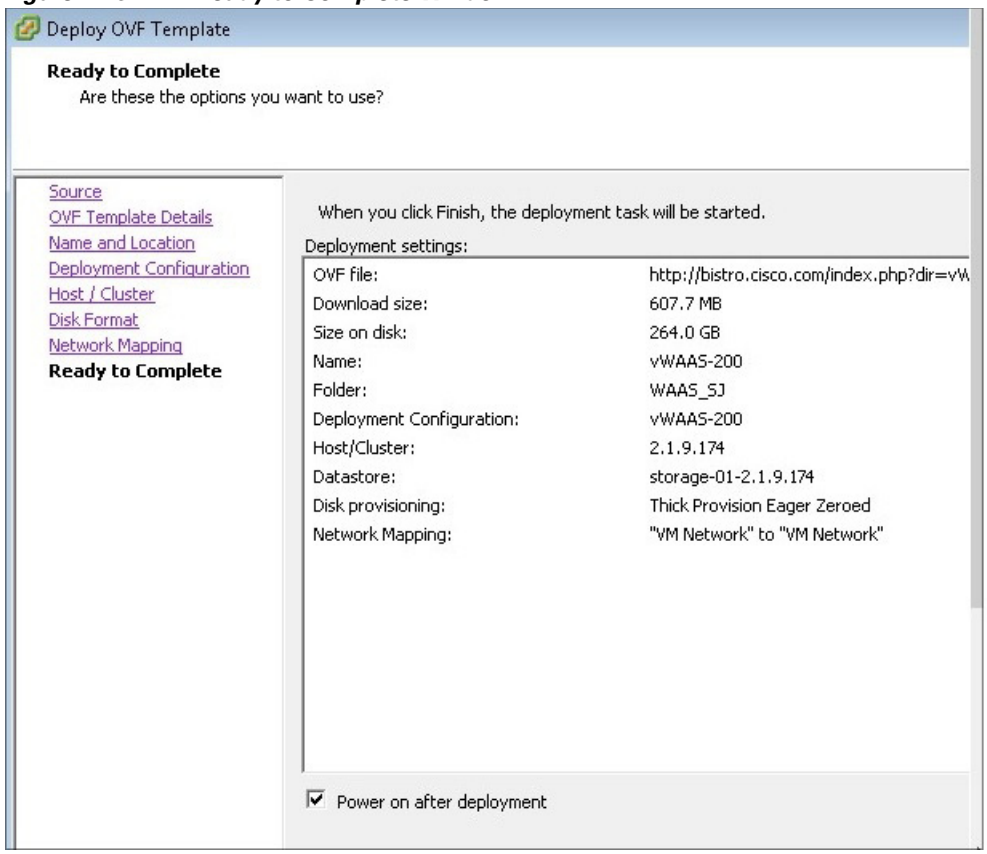


a. Choose the required network mapping settings for your system.

b. Click **Next**.

Step 24 The Ready to Complete window appears (Figure 4-23), where you can verify the details of your deployment.

Figure 4-23 Ready to Complete Window



a. If the displayed details are the ones you have specified for your deployment, click the **Power on after deployment** check box.

b. To start the deployment task, click **Finish**.

Step 25 The Status window appears while the OVA file is being deployed (Figure 4-24) and then shows a completion message after the deployment has completed successfully (Figure 4-25).

Figure 4-24 Deployment In Progress Status Window

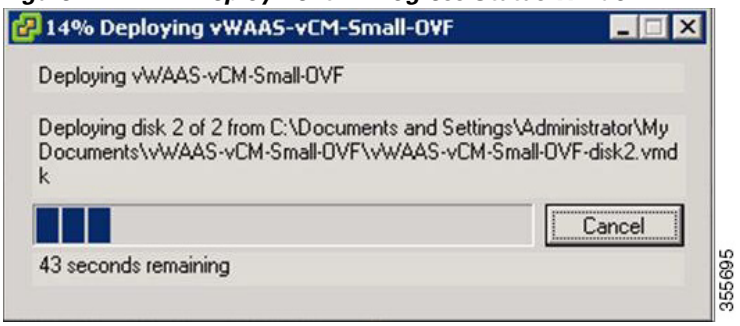


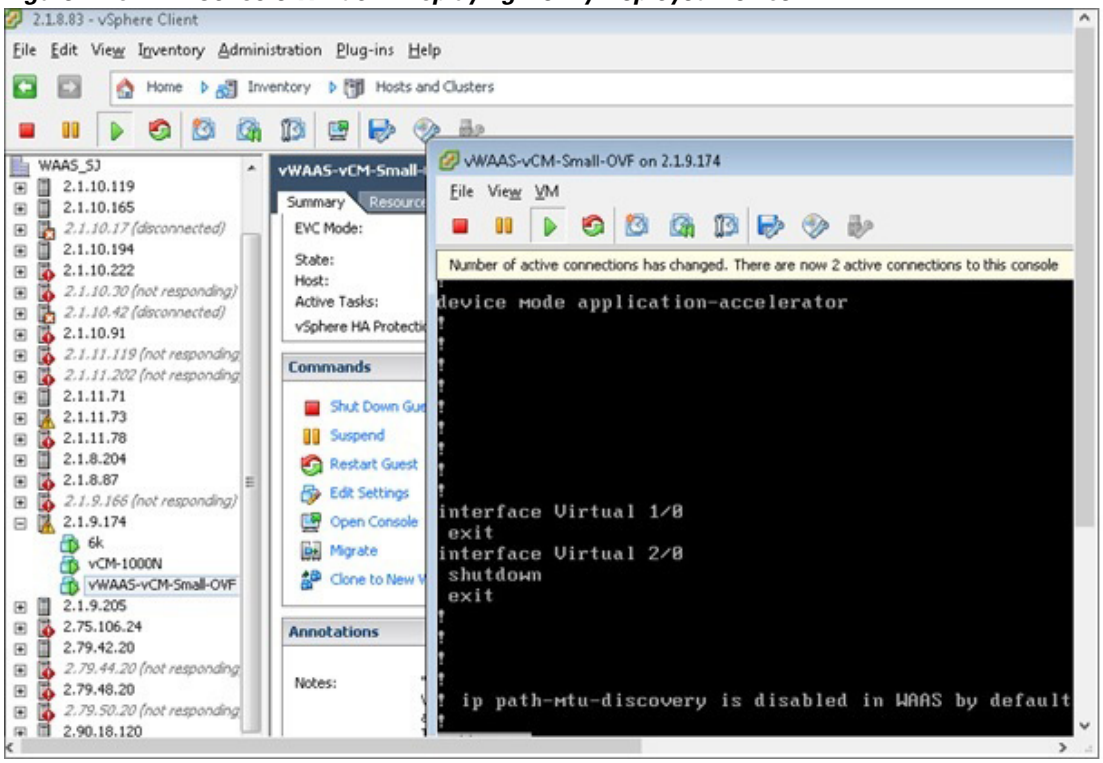
Figure 4-25 Deployment Completion Status Window

a. After deployment is completed, click **Close**.

Step 26 Navigate to Home > Inventory > Hosts and Clusters. The Inventory panel now shows the newly deployed device.

Step 27 Highlight the newly deployed device and open the Console window to display this device (Figure 4-26).

Figure 4-26 Console Window Displaying Newly Deployed Device



Upgrade/Downgrade Guidelines for vWAAS on VMware ESXi

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

- 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 into diskless mode.
- 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.

Cisco vWAAS on Microsoft Hyper-V

This chapter describes how to use Cisco vWAAS on Microsoft Hyper-V, and contains the following sections:

About vWAAS on Microsoft Hyper-V

Microsoft Hyper-V, available for vWAAS with WAAS Version 6.1.x and later, is a native hypervisor for x86_64 systems to enable platform virtualization. Cisco vWAAS on Microsoft Hyper-V extends Cisco networking benefits to Microsoft Windows Server Hyper-V deployments. It improves utilization, consolidates server workloads, and reduces costs. To achieve this, vWAAS on Hyper-V uses hardware virtualization to enable multiple operating systems to run on a single host, and allows the operating systems to share the same underlying physical hardware.

vWAAS on Hyper-V supports all the WAN-optimization functionality that is supported by physical WAAS devices. Physical memory for vWAAS on Hyper-V is provided by a Cisco UCS server.

You can configure the virtual machine on Hyper-V as virtual WAAS Central Manager (vCM) or as vWAAS:

- The Hyper-V device configured as vCM has the same functionality as WAAS Central Manager, and can manage any other device managed by WAAS Central Manager.
- The Hyper-V device configured as vWAAS has the same functionality as the non-Hyper-V vWAAS. Physical memory for vWAAS on Hyper-V is provided by the UCS server.

Supported Host Platforms, Software Versions, and Disk Type

Table 5-1 shows the platforms and software versions supported for vWAAS on Microsoft Hyper-V.

Table 5-1 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-HYPERV • Device Type: OE-VWAAS-HYPERV	• 6.1x	• Cisco UCS • Cisco UCS-E Series	• Microsoft Windows 2008 R2	• VHD

vWAAS on Hyper-V System Requirements

This section contains the following topics:

- System Infrastructure Requirements
- Hardware Virtualization Requirements

System Infrastructure Requirements

Your WAAS system must have the following to deploy vWAAS on Hyper-V:

- Microsoft Hyper-V Hypervisor—Hypervisor enables multiple operating systems to run on a single host. vWAAS runs as a guest on any host running Hyper-V 2008 R2 or greater.
- Hyper-V Virtual Switch—The Hyper-V Virtual Switch is a software-based Layer 2 switch that connects virtual machines to both virtual networks and the physical network. It provides policy enforcement for security, isolation, and service levels, and includes features for tenant isolation, traffic shaping, simplified troubleshooting, and protection against malicious virtual machines.

  Hyper-V Virtual Switch is available in Hyper-V Manager when you install the Hyper-V server role.

Hardware Virtualization Requirements

This section describes vWAAS on Hyper-V hardware virtualization requirements for CPU, disk, CD-ROM, and flash.

- CPU—vWAAS on Hyper-V supports 2, 4, and 8 CPU configurations. vWAAS on Hyper-V does require a minimum CPU limit.

Note vWAAS VM (Virtual Machine) with different CPU configurations works, but is not recommended.

- Disk sizes for vWAAS on Hyper-V— Disk sizes for vWAAS on Hyper-V are the same as those for ESXi, for each model. For more information on disk sizes for WAAS versions up to Version 6.x, see section ESXi Server Datastore Memory and Disk Space for vWAAS and vCM Models in Chapter 4, "Cisco vWAAS on VMware ESXi".
- CD-ROM—vWAAS on Hyper-V supports standard ISO image file for its CD-ROM device.
- Flash—Unlike physical WAAS devices, vWAAS on Hyper-V does not have access to a separate flash device. Instead, vWAAS flash is installed on the first hard disk, and also uses this first disk for booting. A separate larger disk hosts the DRE/CIFS caches, etc. Other flash functionalities are supported as in ESXi.

Deployment Options for vWAAS on Hyper-V

You can deploy vWAAS on Hyper-V as an installable product or in a standalone role:

- **vWAAS on Hyper-V as installable product in the Windows server**—Windows Server 2008 R2, Windows Server 2012 or Windows Server 2012 R2.
- **vWAAS on Hyper-V as standalone role in the Hyper-V server**—Used with Microsoft Hyper-V Server 2012 or Microsoft Hyper-V Server 2012 R2.

Table 5-2 shows Microsoft Hyper-V servers and Microsoft System Center Virtual Machine Manager (SCVMM) support for vWAAS.

Table 5-3 shows platforms supported for vWAAS and vCM on Microsoft Hyper-V, deployed as a standalone or installable product.

Table 5-2 vWAAS Support for Microsoft Hyper-V Servers and SCVMM

Microsoft Hyper-V Server	Microsoft SCVMM	vWAAS Supported
Microsoft Hyper-V Server 2008	SCVMM 2008	No
Microsoft Hyper-V Server 2008 R2	SCVMM 2008 R2	No
Microsoft Hyper-V Server 2008 R2	SCVMM 2012 or SCVMM 2012 R2	Yes
Microsoft Hyper-V Server 2012	SCVMM 2012 or SCVMM 2012 R2	Yes
Microsoft Hyper-V Server 2012 R2	SCVMM 2012 or SCVMM 2012 R2	Yes

Note If you want to install SCVMM in Windows 2008 R2, you must first register it to Windows 2012 or Windows 2012 R2.

Table 5-3 Platforms Supported for vWAAS in Hyper-V Server or Windows Server

Standalone Product in Hyper-V Server		*Installable Product in Windows Server*
Hyper-V Server 2008 R2	**Hyper-V Server 20012 or 2012 R2**	**Windows Server 2012 or 2012 R2**
UCS E-Series and UCS servers	UCS E-Series and UCS servers	UCS E-Series and UCS servers
vCM-100	vCM-100	vCM-100
vCM-500	vCM-500	vCM-500
vCM-1000	vCM-1000	vCM-1000

Standalone Product in Hyper-V Server		*Installable Product in Windows Server*
Hyper-V Server 2008 R2	**Hyper-V Server 20012 or 2012 R2**	**Windows Server 2012 or 2012 R2**
vCM-2000	vCM-2000	vCM-2000
vWAAS-150 (For WAAS Version 6.2.1 and later, supported on Cisco EHWIC and NIM.)	vWAAS-150 (For WAAS Version 6.2.1 and later, supported on Cisco EHWIC and NIM.)	vWAAS-150 (For WAAS Version 6.2.1 and later, supported on Cisco EHWIC and NIM.)
vWAAS-200	vWAAS-200	vWAAS-200
vWAAS-750	vWAAS-750	vWAAS-750
vWAAS-1300	vWAAS-1300	vWAAS-1300
vWAAS-2500	vWAAS-2500	vWAAS-2500
vWAAS-6000	vWAAS-6000	vWAAS-6000
vWAAS-12000	vWAAS-12000	vWAAS-12000
	vWAAS-50000	vWAAS-50000

OVA Package Formats for vWAAS on Microsoft Hyper-V

This section contains the following topics:

OVA Package for vWAAS on Hyper-v for WAAS Version 5.x to 6.2.x

For vWAAS on Microsoft Hyper-V, for WAAS Version 5.x through 6.2.x, Cisco provides an OVA or NPE OVA package for each vWAAS connection profile (examples shown in Table 5-4) and for each vCM connection profile (examples shown in Table 5-5).

The Cisco OVA package for vWAAS on Microsoft Hyper-V contains the following:

- SCVMM template file
- WAAS image .iso file
- Virtual Hard Disk (VHD) file for flash
- PowerShell deployment script for SCVMM
- PowerShell deployment script for standalone hosts

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 5-4 OVA Package Format Examples for vWAAS on Hyper-V for WAAS Version 5.x to 6.2.x

Package Format	File Format Example
Cisco Hyper-V 150 package file	• Hv-Cisco-vWAAS-150-6.2.3d-b-68.zip
Cisco Hyper-V 150 package file for NPE	• Hv-Cisco-vWAAS-150-6.2.3d-npe-b-68.zip
Cisco Hyper-V 200 package file	• Hv-Cisco-vWAAS-200-6.2.3d-b-68.zip
Cisco Hyper-V 200 package file for NPE	• Hv-Cisco-vWAAS-200-6.2.3d-npe-b-68.zip
Cisco Hyper-V 750 package file	• Hv-Cisco-vWAAS-750-6.2.3d-b-68.zip
Cisco Hyper-V 750 package file for NPE	• Hv-Cisco-vWAAS-750-6.2.3d-npe-b-68.zip
Cisco Hyper-V 1300 package file	• Hv-Cisco-vWAAS-1300-6.2.3d-b-68.zip
Cisco Hyper-V 1300 package file for NPE	• Hv-Cisco-vWAAS-1300-6.2.3d-npe-b-68.zip
Cisco Hyper-V 2500 package file	• Hv-Cisco-vWAAS-2500-6.2.3d-b-68.zip
Cisco Hyper-V 2500 package file for NPE	• Hv-Cisco-vWAAS-2500-6.2.3d-npe-b-68.zip

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

Package Format	File Format Example
Cisco Hyper-V 100N package file	• Hv-Cisco-100N-6.2.3d-b-68.zip
Cisco Hyper-V 100N package file for NPE	• Hv-Cisco-100N-6.2.3d-npe-b-68.zip

Unified OVA Package for vWAAS on Hyper-V for WAAS Version 6.4.1 and Later

For vWAAS on Microsoft Hyper-V for WAAS Version 6.4.1 and later, Cisco provides a single, unified OVA for NPE and non-NPE version of the WAAS image for all the vWAAS models for that hypervisor.

Each unified OVA package is a pre-configured virtual machine image that is ready to run on a particular hypervisor. The launch script for each unified OVA package file 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 file filenames for Microsoft Hyper-V:

- OVA—Cisco-HyperV-vWAAS-Unified-6.4.1-b-33.zip
- NPE OVA—Cisco-HyperV-vWAAS-Unified-6.4.1-b-33-npe.zip

The unified OVA package for Microsoft Hyper-V contains the following files.

- SCVMM template file
- WAAS image iso
- Virtual hard disk file for Flash
- PowerShell deployment script for SCVMM and a set of template .xml files
- PowerShell deployment script for Standalone Hosts and a set of template .xml files

Installing vWAAS on Microsoft Hyper-V

This section contains the following topics:

Installing vWAAS on Hyper-V for vWAAS on WAAS Version 5.x to 6.2.x

vWAAS on Hyper-V is installed using the Microsoft Virtual Machine Manager (VMM), with the Virtual Hard Disk (VHD) file. During installation, there is an option to import pre-configured and pre-installed vWAAS images to Hyper-V. After you have completed installation, complete the activation and registration process with the procedures described in Activating and Registering vWAAS on Hyper-V.

This section contains the following topic:

Installing vWAAS on Hyper-V with a VHD Template

There are seven VHD templates available for vWAAS, and four VHD templates available for vCM.

You can import a pre-configured, model-based VHD file for your deployment. For more information on installing Hyper-V with a VHD template, contact your Cisco account representative.

To install vWAAS on Hyper-V with a VHD template, follow these steps:

Step 1 Download the vWAAS package to the computer where the SCVMM2012 or the 2012 R2 console is installed.

Step 2 Unzip the vWAAS package.

Step 3 Login to the SCVMM console.

Step 4 Launch the PowerShell window that is displayed in the SCVMM.

Step 5 Navigate to the PowerShell script in the uncompressed vWAAS package: ".\Cisco-vWAAS-model-name-6.0.0-ISO\Cisco-vWAAS-model-name-6.0.0-ISO"

Step 6 Run the PowerShell script: "deploy-vwaas-*model-name*"

Step 7 Follow the procedure that is requested by the deployment script.

Step 8 If your deployment uses a vWAAS-12000 or vWAAS-50000 model, you must enter a maximum amount of memory in NUMA (Non-Uniform Memory Access) configuration of at least RAM size or higher, in MB, otherwise the device will not be able to boot up.

Note Entering the maximum memory amounts as shown in Step 9 should be completed *only after* you have deployed vWAAS in Hyper-V (as shown in Step 1 through Step 7).

Step 9 To enter the maximum amount of memory, follow these steps:

a. From the SC VMM console, navigate to **Hardware > Processor > NUMA**.

b. The NUMA Configuration screen is displayed.

c. At the **Maximum amount of memory (MB)** field, enter an amount, in MB:

- For vWAAS-12000, enter an amount of at least 12288 MB.
- For vWAAS-50000, enter an amount of at least 49152 MB.

Installing vWAAS on Hyper-V for WAAS Version 6.4.1 and Later

To deploy Microsoft Hyper-V for vWAAS for WAAS 6.4.1 and later, follow these steps:

Step 1 From the Cisco WAAS Installer for Hyper-V, as shown below, enter the number of your vWAAS or vCM model:

```
----- Cisco WAAS Installer for vWAAS -----

    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

    Enter vWAAS/vCM model number to install [ ]:
```

Step 2 The automated Hyper-V package generation copies all the vWAAS model template XML files in the zip file. Based on your input, the corresponding XML template is registered and used for the specified vWAAS model deployment.

Activating and Registering vWAAS on Hyper-V

You manage vWAAS on Hyper-V through the WAAS Central Manager (CM). vWAAS on Hyper-V supports all the functionality that is supported by WAAS devices.

This section describes how to activate and register vWAAS on Hyper-V. For installation information, see Installing vWAAS on Microsoft Hyper-V.

When a Hyper-V vWAAS virtual machine (VM) is started on the Hyper-V, it boots up and prompts you to enter basic boot configuration information, including configuring a Hyper-V interface and WAAS CM IP address.

To activate and register vWAAS on Hyper-V, following these steps:

Step 1 Configure the IP address/gateway on the vWAAS interface. As needed, also configure *name-server*, *domain-name*, and any other static routes.

Step 2 If necessary, configure WCCP interception. For more information on configuring WCCP interception, see WCCP Interception. No configuration is necessary for appnav-controller interception.

Step 3 Configure the WAAS Central Manager IP address so that vWAAS can be registered with the WAAS Central Manager.

Step 4 Hyper-V vWAAS connects with the WAAS CM and registers itself. Hyper-V vWAAS is considered in service after it is registered successfully and it optimizes the connections.

Step 5 The following are scenarios when a vWAAS cannot not successfully register with the WAAS CM:

- If Hyper-V vWAAS cannot register with the WAAS CM, it generates an alarm and does not optimize connections. Contact Cisco Technical Support (TAC) if you need assistance to resolve this situation.
- Hyper-V vWAAS may register successfully with the WAAS CM, but lose connectivity due to a shutdown or power off. If it remains functional, vWAAS will continue to optimize connections in the offline state.
- If you de-register the Hyper-V vWAAS (with the **cms deregister** EXEC command), it is removed from service.

Step 6 After vWAAS on Hyper-V is operational on a device, the WAAS CM displays the following information for the device:

- The Hyper-V device is displayed in the **Devices** > **All Devices** listing under Device Type as **OE-VWAAS**.
- The Hyper-V device is displayed in the **Devices** > *device-name* > **Dashboard** as **OE-VWAAS-HYPER-V**.

Traffic Interception Methods for vWAAS on Hyper-V

This section has the following topics:

About Traffic Interception for vWAAS on Hyper-V

When vWAAS is deployed in Hyper-V hosts, the WAE device is replaced by the Hyper-V host. No change is required in the WAAS traffic interception mechanism in the switches or routers. The WCCP protocol also works like the vWAAS VMware ESXi deployment in the vWAAS Hyper-V deployment.

vWAAS on Hyper-V provides the same WAN acceleration functionality provided by the physical WAN acceleration WAE device. You can also deploy multiple vWAAS in one or more Hyper-V hosts to form a WAAS farm in either the Edge or the Core.

WCCP Interception

WCCP interception, WCCP GRE or WCCP L2, is supported for all vWAAS on Hyper-V deployments.

To select WCCP as the interception method for a WAE, follow these overview steps. For a full description of each step, see the *Cisco Wide Area Application Services Configuration Guide*.

Note Before you do the following procedure, you should have already configured your router for basic WCCP, as described in the *Cisco Wide Area Application Services Configuration Guide*.

Step 1 From the WAAS Central Manager menu, choose Devices > *device-name*.

Step 2 Choose **Configure** > **Interception** > **Interception Configuration**. The Interception Configuration window appears.

Interception Method Settings area

Step 3 From the Interception Method drop-down list, choose **WCCP** to enable the WCCP interception on the vWAAS device.

WCCP Settings area

Step 4 To enable WCCP on the device, check the **Enable WCCP Service** check box.

Step 5 With WCCP selected, the **Service Type** field displays TCP Promiscuous.

Step 6 In the Service ID1 field, specify the first service ID of the WCCP service pair, with an ID number of 1 to 99. After you submit, the Service ID2 field is filled in with the second service ID of the pair, which is one greater than Service ID1, with an ID number of 2 to 100.

Step 7 To use the default gateway of the WAE as the router to associate with the WCCP TCP promiscuous service, check the **Use Default Gateway as WCCP Router** check box.

If you leave this box unchecked, you can use the **WCCP Routers** field to specify a list of one or more routers by their IP addresses, separated by spaces.

WCCP Assignment Settings for Load Balancing area

Step 8 (Optional) From the **Assignment Method** drop-down list, choose the type of WAE load-balancing assignment method to use (**Mask** or **Hash**).

- Mask assignment method selected—To use a custom mask, enter a value for the source ID mask in the **Source IP Mask** field. The range, in hexadecimal, is 00000000–FE000000. The default is F00. Enter a value for the destination IP mask in the **Destination IP Mask** field. The range, in hexadecimal, is 0000000–FE000000. The default is 0.
- Hash assignment method selected—To specify the hash assignment method for the source IP address, check **Hash on Source IP:** either **Service ID1** or **Service ID2**. After you check a source IP, the complementary destinantion IP is automatically selected, **Hash on Destination IP:** check box either **Service ID2** or **Service ID1**.

WCCP Redirect and Egress Settings area

Step 9 From the **Redirect Method** drop-down list, choose **WCCP GRE** or **WCCP L2**.

Step 10 From the Egress Method drop-down list, choose **L2** or **IP Forwarding**.

Advanced WCCP Settings area

Step 11 Check the **Enable Flow Protection** check box to keep the TCP flow intact and to avoid overwhelming the device when it comes up or is reassigned new traffic. For more information on flow redirection, see the Information about WCCP Flow Redirection on WAEs" section of the *Cisco Wide Area Application Services Configuration Guide*.

Step 12 In the **Flow Protection Timeout** field, specify the amount of time (in seconds) that flow protection should be enabled. The default is 0, which means flow protection stays enabled with no timeout.

Step 13 In the **Shutdown Delay** field, enter a maximum amount of time (in seconds) that the chosen device waits to perform a clean shutdown of WCCP. The range is 0 to 86400 seconds. The default is 120 seconds.

Step 14 From the **Failure Detection Timeout** drop-down list, choose a failure detection timeout value: 30, 15, or 9 seconds. The default is 30 seconds. The failure detection timeout determines the length of time for the router to detect a WAE failure.

Step 15 In the **Weight** field, specify the weight to be used for load balancing. The weight value range is 0 to 10000.

- If the total of all the weight values of the WAEs in a service group is less than or equal to 100, the weight value represents a literal percentage of the total load redirected to the device for load-balancing purposes.
- If the total of all the weight values of the WAEs in a service group is between 101 and 10000, the weight value is treated as a fraction of the total weight of all the active WAEs in the service group.

Step 16 In the **Password** field, specify the password to be used for secure traffic between the WAEs within a cluster and the router for a specified service. Be sure to enable all other WAEs and routers within the cluster with the same password. Passwords must not exceed eight characters in length. Do not use the following characters: space, backwards single quote (‘), double quote (“”), pipe (|), or question mark (?).

Re-enter the password in the **Confirm Password** field.

Step 17 Click **Submit** to save the settings.

AppNav Controller Interception

AppNav interception is supported for all vWAAS on Hyper-V deployments, and works as in the current ESXi vWAAS models.

AppNav interception enables a vWAAS node to receive traffic optimization from an AppNav controller (ANC) in an AppNav deployment. If vWAAS VMs are part of an AppNav deployment and are configured as WAAS nodes (WNs) in an AppNav cluster, you must configure the AppNav-controller interception method. These WNs receive traffic only from the ANCs; they do not receive traffic directly from routers.

To select AppNav as the interception method, follow these steps:

Step 1 From the WAAS Central Manager menu, choose Devices > *device-name*.

Step 2 Choose **Configure** > **Interception** > **Interception Configuration**. The Interception Configuration window appears.

Step 3 From the Interception Method drop-down list, choose **appnav-controller** to enable appnav-controller interception on hte vWAAS device.

Step 4 Click **Submit**.

Operating Guidelines for vWAAS on Hyper-V

This section has the following topics:

- Hyper-V High Availability Features

vWAAS Deployments, UCS-E Upgrades, and Windows Server Updates

Caution Multiple deployments of vWAAS on the same Hyper-V host *in parallel* may cause unexpected results, due to availability of free space when creating VHDs. We recommend that you do *not* deploy multiple vWAAS on Hyper-V in parallel, unless you have verified that you have enough free disk space required for the respective vWAAS models.

To ensure reliable throughput with the following configuration—**vWAAS on Windows Server 2012 R2 Hyper-V in Cisco UCS-E Series 160S-M3**—we recommend that you do the following:

- Upgrade to the latest UCS-E firmware (Version 3.1.2), available on the Cisco Download Software Page for UCS E-Series Software, UCS E160S M3 Software.
- Verify that you have installed the critical Windows Server updates, available on the Microsoft Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2 Update Rollup page. You can also obtain the standalone update package through the Microsoft Download Center by searching for **KB2887595**.
-

Configuring NTP Settings for vWAAS on Hyper-V

The Network Time Protocol (NTP) allows synchronization of time and date settings for the different geographical locations of the devices in your WAAS network, which is important for proper system operation and monitoring. When you configure NTP on vWAAS with Hyper-V, the time gets updated from the NTP server.

Caution To ensure that the vWAAS on Hyper-V system clock remains in synchronization with the system clocks of other WAAS devices, especially after a reload of vWAAS on Hyper-V, you must *uncheck* the **Time synchronization** option. This option must be unchecked in the system that you are using for vWAAS on Hyper-V: System Center Virtual Machine Manager (SC VMM) or the Hyper-V Manager.

To uncheck the Time Synchronization option for NTP configuration, follow these steps:

Step 1 Uncheck the Time Synchronization option in either the SC VMM or the Hyper-V Manager:

From the SC VMM:

a. Select **vWAAS VM**.

b. Choose **Settings > Management > Integration Services**.

c. Verify that the **Time synchronization** option is unchecked.

d. Click **OK**.

From the Hyper-V Manager:

a. Select **vWAAS VM**.

b. Choose **Properties > Hardware Configuration > Advanced > Integration Services**.

c. Verify that the **Time synchronization** option is unchecked.

d. Click **OK**.

Hyper-V High Availability Features

vWAAS on Hyper-V provides multiple high availability solutions, including:

- Live Migration
- NIC Teaming

Live Migration

Hyper-V live migration moves running VMs with no impact on VM availability to the user. It does this by pre-copying the memory of the migrating VM to the destination physical host. The administrator, or the script, that initiates the live migration controls which computer is the destination for the live migration. There is no need for special configuration for the guest operating system, as that is not affected by the live migration.

There are three methods you can use to initiate a live migration:

- Failover Cluster console
- Virtual Machine Manager Administration console (if Virtual Machine Manager is managing physical hosts that are configured to support live migration)
- A PowerShell or WMI script

The following is a workflow for initiating and completing a live migration:

- **Create a connection between hosts**—The source physical host creates a TCP connection with the destination physical host, which is used to transfer the VM configuration data to the destination physical host. A skeleton VM is set up on the destination physical host, and memory is allocated to the destination VM.
- **Copy the working set to the destination host**—The memory assigned to the migrating VM, called the working set, is copied to the destination physical host. This memory is referred to as the working set of the migrating VM. A page of memory is 4 kB in size.
- **Mark modified memory pages**—The utilized pages within the working set are copied to the destination Hyper-V physical host. In addition to copying the working set to the destination physical host, Hyper-V on the source physical host monitors the pages in the working set. As the migrating VM modified the memory pages during live migration, Hyper-V tracks and marks them as modified.
- **Copy modified memory pages**—During live migration, Hyper-V iterates the memory copy process several times. Each time, a smaller number of modified pages need to be copies to the destination physical host. A final memory copy process copies the remaining modified memory pages to the destination physical host.

  The source physical host transfers the register and device state of the VM to the destination physical host. During this stage of live migration, the network bandwidth available between the source and physical host is critical to the speed of the migration. Therefore, 1 Gigabit Ethernet is recommended.

Note The number of pages to be transferred in this stage is dictated by how actively the VM is accessing and modifying memory pages. More modified pages means a longer VM migration time, to allow for all memory pages to be transferred to the destination physical host.

- **Complete the live migration**—After the modified memory pages have been completely copied to the destination physical host, the destination physical host has an up-to-date working set of the migrated VM: the working set for the migrated VM is present on the destination physical host in the exact state it was in when the migrated VM began the live migration process.

Note You can cancel the live migration process at any point before this phase of the process.

- **Transfer control of the migrated VM memory and storage**—Control of storage associated with the migrated VM, such as VHD files or pass-through disks, and control of memory (working set) are transferred to the destination physical host.
- **Bring migrated VM online**—The migrated VM is brought online on the destination physical host.

NIC Teaming

The failure of an individual Hyper-V port or virtual network adapter can cause a loss of connectivity for a virtual machine. To prevent this, multiple virtual network adapter are used in a NIC (Network Interface Card) teaming configuration, which provides both high availability and load balancing across multiple physical network interfaces. NIC teaming is also known as network adapter teaming technology and LBFO (Load Balancing Failover).

For vWAAS on Hyper-V, NIC teaming, in Windows Server 2012, enables a virtual machine to have virtual network adapters that are connected to more than one virtual switch, and will still have connectivity even if the network adapter under that virtual switch is disconnected. NIC teaming on Windows Server 2012 supports up to 32 network adapters in a team.

With NIC teaming, you can set up two virtual switches, each connected to its own SR-IOV-capable network adapter. NIC teaming then works in one of two ways:

- Each virtual machine can install a virtual function from one or both SR-IOV network adapters. If a adapter disconnection occurs, the traffic can fail over from the primary virtual function to the backup virtual function without losing connectivity.
- Each virtual machine can have a virtual function from one network adapter and a non-virtual functional interface to the other switch. If the network adapter associated with the virtual function becomes disconnected, the traffic can fail over to the other switch without losing connectivity.

Configuring GPT Disk Format for vWAAS-50000 on Hyper-V with Akamai Connect

The following list shows the disk requirements for vWAAS on Hyper-V for vWAAS-50000 with Akamai Connect:

- 4 GB Flash
- 48 GB Kdump

- 1500 GB
- 850 GB for disk (for Akamai Connect)

The Windows server does not detect disk size more than 2 TB in partition **C:** because it is in MBR format. Therefore, in order to have a disk size more than 2 TB, you need to create partition **D:** in GPT (GUID Partition Table) format.

To convert the HDD from MBR format to GPT format, follow these steps:

Step 1 Install windows in one partition of the HDD.

Step 2 After installation is complete, create a new volume to create a new disk partition:

a. Right-click the Windows command prompt and then click **Run as Administrator**.

b. Enter the **diskpart** command to enter DiskPart command mode.

c. At the DISKPART prompt, enter the **create volume** command to create a new volume on the disk.

Step 3 At the DISKPART prompt, enter the **list disk** command to display a list of disks and associated information (including size, available free space, whether the disk is basic or dynamic).

Step 4 Note the disk number of the disk for which you want to convert formats.

Step 5 At the DISKPART prompt, enter the **select disk** *disk-number* command.

Step 6 At the DISKPART prompt, enter the **clean** command to specify that all sectors on the disk are set to zero.

Note The **clean** command deletes all data on the disk.

Step 7 At the DISKPART prompt, enter the **convert gpt** command to convert the disk format to GPT format.

Step 8 With the GPT format, you can configure RAID capabilities for the HDD, including logical disk handling with RAID-5, logical disk handling with RAID-1, and disk hot-swap support. For more information on RAID support for Cisco WAAS, see the *Cisco Wide Area Application Services Configuration Guide*.

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.

Cisco vWAAS on Cisco ENCS 5400-W Series

This chapter describes Cisco vWAAS on the Cisco Enterprise Network Compute System, W Series appliance.

Cisco vWAAS on Cisco ENCS 5400-W Series

This section contains the following topics:

About the Cisco ENCS 5400-W and ENCS 5400 Series

The Cisco Enterprise Network Compute Series (ENCS) is used to host the Cisco Enterprise Network Functions Virtualization (NFV) solution. ENCS is also used to deploy the Cisco NFV Infrastructure Software (NFVIS), and Cisco and third party VNFs on Cisco Enterprise NFV.

For more information on Cisco NFVIS, see Chapter 8, "Cisco vWAAS on Cisco ENCS 5400-W Series".

Table 7-1 describes how the ENCS 5400 Series and the ENCS 5400-W Series (used with vWAAS) are used with Enterprise NFV. For more information on the Cisco ENCS 5400-W series, see the *Cisco 5400 Enterprise Network Compute System Data Sheet*.

Table 7-1 Cisco ENCS 5400 Series and ENCS 5400-W Series

Cisco ENCS Series	Description
ENCS 5400 Series	The Cisco ENCS 5400 Series—ENCS 5406, 5408, and 5412—is a line of compute appliances designed for the Cisco SD-Branch and Enterprise NFV solution.
ENCS 5400-W Series	The ENCS 5400-W Series—ENCS 5406-W, 5408-W, and 5412-W—is an x86 hybrid platform is designed for the Cisco Enterprise NFV solution, for branch deployment and for hosting WAAS applications. These high-performance units achieves this goal by providing the infrastructure to deploy virtualized network functions while at the same time acting as a server that addresses processing, workload, and storage challenges. **Note** vWAAS is designed to run in appliance mode or as a Virtualized Network Function (VNF) in three Cisco ENCS 5400-W series models—ENCS 5406-W, ENCS 5408-W, ENCS 5412-W—and three Cisco PIDs—ENCS 5406-K9, ENCS 5408-K9, ENCS 5412-K9.

Caution vWAAS is designed to run in appliance mode or as a Virtualized Network Function (VNF) in three Cisco ENCS 5400-W series models (ENCS 5406-W, ENCS 5408-W, and ENCS 5412-W) and three Cisco PIDs (ENCS 5406-K9, ENCS 5408-K9, and ENCS 5412-K9).

For guaranteed performance, the ENCS 5400 Series, UCS-C Series, UCS-E Series, and ISR configurations listed in the WAAS Sizing Guides and specifically noted in WAAS and vWAAS user guides and WAAS Release Notes are the only devices we recommend for use with vWAAS. Although vWAAS models may be able to operate with other Cisco or third-party hardware, successful performance and scale for those configurations is not guaranteed.

For more information on the Cisco ENCS 5400-W series, see the *Cisco 5400 Enterprise Network Compute System Data Sheet*.

vWAAS as VM on Cisco ENCS 5400-W Series

For vWAAS with Cisco Enterprise NFVIS on ENCS, vWAAS operates as a VM to provide WAN and application optimization, and, optionally, application optimization with Akamai Connect.

vWAAS with Cisco Enterprise NFVIS runs on Cisco ENCS 5400-W series, the Cisco x86 hardware platform for branch deployment, for routing and hosted applications.

Table 7-2 shows supported vWAAS models for Cisco ENCS 5406-W, 5408-W, and 5412-W.

Table 7-2 Supported vWAAS Models for Cisco ENCS 5400-W Series

ENCS Model	Processor	CPUs	RAM	Supported vWAAS Model
ENCS 5406-W	Intel Xeon Processor D-1528 (1.9 GHz, 9 MB L2 cache)	6-core	16 GB	vWAAS-200 or vWAAS-750
ENCS 5408-W	Intel Xeon Processor D-1548 (2.0 GHz, and 12 MB L2 cache)	8-core	16 GB	vWAAS-1300
ENCS 5412-W	Intel Xeon Processor D-1557 (1.5 GHz, and 18 MB L2 cache)	12-core	32 GB	vWAAS-2500 or vWAAS 6000R

ENCS 5400-W Models that Replace EOL/EOS WAVE Devices

Cisco WAVE appliances have end-of-sale (EOS) and end-of-life (EOL) dates, highlighted in the *End-of-Sale and End-of-Life Announcement for the Cisco WAVE 294, 594, 694, 7541, 7571 and 8541*.

Table 7-3 shows the ENCS 5400-W Series models that replace the EOS/EOL WAVE models, and the supported vWAAS models for each ENCS 5400 model.

Table 7-3 ENCS 5400-W Series Replacment Models for WAVE Devices

EOS/EOL WAVE model	ENCS 5400 model to replace WAVE model	Supported vWAAS Models for ENCS 5400	Connection Size
WAVE-294	ENCS 5406-W	vWAAS 200	200 connections
WAVE-594-8G	ENCS 5406-W	vWAAS-750	750 connections
WAVE-594-12G	ENCS 5408-W	vWAAS-1300	1300 connections
WAVE-694-16G	ENCS 5412-W	vWAAS-2500	2500 connections
WAVE-694-24G	ENCS 5412-W	vWAAS-6000-R	6000 connections

ENCS 5400-W Hardware Features and Specifications

Table 7-4 shows features and specifications that apply to all three ENCS 5400-W series models. For views of the Cisco ENCS 5400-W Series and further information, see the *Cisco 5400 Enterprise Network Compute System Data Sheet*.

Table 7-4 ENCS 5400-W Series Features and Specifications

ENCS 5400 Feature/Specification	Description
vWAAS models supported	One of the following configurations: • ENCS 5406-W supports vWAAS 200, vWAAS-750 • ENCS 5408-W supports vWAAS-1300 • ENCS 5412-W supports vWAAS-2500, vWAAS-6000-R
CPU	One of the following specifications: • ENCS 5406-W: Intel Xeon Processor D-1528 (6-core, 1.9 GHz, and 9 MB cache) • ENCS-5408-W: Intel Xeon Processor D-1548 (8-core, 2.0 GHz, and 12 MB cache) • ENCS-5412-W: Intel Xeon Processor D-1557 (12-core, 1.5 GHz, and 18 MB cache)
BIOS	Version 2.4
Cisco NFVIS on KVM hypervisor	KVM hypervisor Version 3.10.0-327.el7.x86_64
CIMC	Version 3.2
Network Controller	Intel FTX710-AM2
WAN Ethernet port	Intel i350 dual port
DIMM	Two DDR4 dual in-line memory module (DIMM) slots, for ENCS models with the following capacities: • ENCS 5406-W—16 GB • ENCS 5408-W—16 GB • ENCS 5412-W—32 GB The memory module in each of the slots can be upgraded to a maximum of 32 GB, so that you can have a maximum capacity of 64 GB DIMM.
Gigabit Ethernet ports	Two Gigabit Ethernet ports—For each RJ45 port, there is a corresponding fiber optic port. At a given time, you can use either the RJ45 connection or the corresponding fiber optic port.
NIM	One Network Interface Module (NIM) expansion slot—You can install a NIM in the NIM slot, or if the slot is not needed, you can remove the NIM from the NIM module. Each ENCS 5400 model supports one NIM slot, for a Cisco 4-port 1G fail-to-wire NIM card.
Management Controller	Ethernet management port for Cisco Integrated Management Controller (CIMC), which monitors the health of the entire system.
HDD Storage	Although there are two hot-swappable HDD slots, we do not recommend HDD storage for the ENCS 5400-W Series.

ENCS 5400 Feature/Specification	Description
SSD Storage	• No RAID and 1 960 GB SSD • RAID-1 and 2 SSDs (960 GB SSD) **Note** If you need to add or remove RAID-1 for your system, see Adding or Removing RAID-1 for ENCS 5400-W Series. Note that the RAID-1 option is available for vWAAS for WAAS Version 6.4.1a and later.
Offload Capabilities	Optional crypto module to provide offload capabilities to optimize CPU resources like VM-toVM traffic and to maintain open software support.

vWAAS Bundled Image Install Procedure

Before You Begin

- Verify that the specified ENCS 5400-W Series chassis (ENCS 5406-W, 5408-W, or 5412-W) is already installed and powered up. For information on how to install the an ENCS 5400-W Series device, see the *Cisco 5400 Enterprise Network Compute System Hardware Installation Guide*.
- If you need to add or remove RAID-1 for your system, see Adding or Removing RAID-1 for ENCS 5400-W Series. Note that the RAID-1 option is available for vWAAS for WAAS Version 6.4.1a and later.

To install vWAAS with NFVIS an ENCS 5400-W Series device on your WAAS system, follow these steps:

Step 1 Copy the vWAAS bundled image file—an ISO file that contains the NFVIS 3.7.1 image and WAAS 6.4.1x image—on your laptop.

Step 2 Connect your laptop's Ethernet port to the ENCS device's Cisco Integrated Management Controller (CIMC) port.

Step 3 Configure your laptop with a static IP address; for example, 192.168.1.3.

Note By default, the IP address on the ENCS device's CIMC port is configured as 192.168.1.2.

Step 4 Open your web browser and enter **https://192.168.1.2**.

The CIMC console login page appears.

Step 5 Log in with your user name and password.

Default user name is **admin**.

Default password is **password**.

Step 6 Click **Login**.

Note The Change Password dialog box appears the first time, only, that you log into the CIMC console. Change the password as needed and click **Save**.

Step 7 The CIMC Home page is displayed.

Step 8 Navigate to **Home > Compute > BIOS > Configure Boot Order**.

The Configure Boot Order dialog box appears.

Step 9 At the Device Types listing, select **CD/DVD Linux Virtual CD/DVD**.

Click **Add**.

Step 10 At the Device Type listing, select **HDD**.

Click **Add**.

Step 11 Using the **Up** and **Down** options, set the boot order sequence.

Step 12 **CD/DVD Linux Virtual CD/DVD** must be the first listing in the boot order.

Step 13 To complete the boot order setup, click **Apply**.

Step 14 Launch the KVM console. You can launch the KVM console from CIMC Home page or the Remote Management area.

Step 15 *At the KVM console:*

After the KVM console is initialized, map the vWAAS bundled image through the **Server > Remote Presence > Virtual Media** tab on the KVM console.

Step 16 To load the mapped image, at the KVM Console Power tab, use the **Power Cycle System [cold boot]** option to power off and then power on the device.

Note When the server reboots, the KVM Console will automatically install the Cisco Enterpirse NFVIS from the virtual CD/DVD drive. The entire installation may take 30 minutes to one hour to complete.

Step 17 With the installation running in the background, use your laptop to connect via SSH to the CIMC default IP (192.168.1.2).

Step 18 After the installation is successful, the ENCS device reboots.

```
[  OK  ] Unmounted /mnt/sysimage/dev.
[  OK  ] Unmounted /mnt/sysimage/sys.
Unmounting /mnt/sysimage...
[  OK  ] Unmounted /mnt/sysimage.
[  OK  ] Reached target Unmount All Filesystems.
[  OK  ] Stopped target Local File Systems (Pre).
[  OK  ] Stopped Create Static Device Nodes in /dev.
Stopping Create Static Device Nodes in /dev...
[  OK  ] Stopped Remount Root and Kernel File Systems.
Stopping Remount Root and Kernel File Systems...
[  OK  ] Stopped Collect Read-Ahead Data.
Stopping Collect Read-Ahead Data...
Stopping Monitoring of LVM2 mirrors...
dmeventd or progress polling...
[  OK  ] Stopped Monitoring of LVM2 mirrors,...
ng dmeventd or progress polling.
Stopping LVM2 metadata daemon...
[  OK  ] Stopped LVM2 metadata daemon.
[  OK  ] Started Restore /rdracut Warning: Killing all remaining processes
Rebooting.

[ deviceID] Restarting system.
```

Step 19 The ENCS device boots up and displays options to install vWAAS. Depending on your ENCS model, one of the following choices is displayed:

- For ENCS 5406-W—vWAAS 200 and vWAAS-750 are displayed.
  Select one vWAAS model for ENCS 5406-W.
- For ENCS 5408-W—vWAAS-1300 is the only choice displayed.
  vWAAS-1300 is automatically selected for ENCS 5408-W.
- For ENCS 5412-W—vWAAS-2500 and vWAAS-6000-R are displayed.
  Select one model for ENCS 5412-W.

  Example:

  In the following example, a vWAAS-6000-R is selected for an ENCS 5412-W:

```
vWAAS Model
1) vWAAS-2500
2) vWAAS-6000-R
3) Quit
Please enter your choice: 2
```

Table 7-5 shows installation times by vWAAS model/number of connections:

Table 7-5 Installation Time by vWAAS Model/Number of Connections

vWAAS Model	Number of connections	NFVIS Installation Time	WAAS Installation Time	Total Installation Time
vWAAS-200	200 connections	60 minutes	15 minutes	75 minutes
vWAAS-750	750 connections	60 minutes	24 minutes	84 minutes
vWAAS-1300	1300 connections	55 minutes	28 minutes	83 minutes
vWAAS-2500	2500 connections	67 minutes	34 minutes	101 minutes
vWAAS-6000-R	6000 connections	66 minutes	38 minutes	104 minutes

Step 20 After installation is complete, the Cisco WAAS login prompt appears.

Step 21 The new OE-ENCS device will be displayed in the WAAS Central Manager **Devices** > **All Devices** listing table.

Step 22 You can view detailed information on the new OE-ENCS device by navigating to **Devices** > *DeviceName* > **Dashboard**.

CLI Commands Used with vWAAS on ENCS 5400-W

Table 7-6 shows the CLI commands used to display information about vWAAS on ENCS.

Table 7-6 CLI Commands Used with vWAAS on ENCS

Mode	Command	Description
EXEC	**copy sysreport disk**	The ENCS logs are part of the sysreport generation for debugging.
	reload	Halts the operation and performs a cold restart of the VM.
	show hardware	Displays the following information for the specified device: • Hardware Information—Manufacturer, PID, serial number, hardware version, CPU information, Memory information, and disk size. • System Information—UUID, NFVIS version, compile time, kernel version, Qemu version, LibVirt version, and OVS version.
	show inventory	Displays system inventory information, including a description of the device, and the device's PID, chassis or slot number, version number, and serial number.
	show nfvis version	Displays NFVIS and BIOS version.
	show version	Displays the version of the OE-ENCS device, as well as device ID, system restart time, system restart reason, and amount of time system has been up.
	shutdown	Powers down the ENCS host/server.
global config	**interface virtual**	The internal interface is used for communication between the NFVIS host and the WAAS guest. The IP address associated with this interface (virtual 1/0) is assigned automatically by NFVIS while booting up, and cannot be modified. **Note** The interface virtual slot/port command cannot be used to configure ENCS internal interface.

System Requirements for vWAAS on ENCS-W with Akamai Connect

Table 7-7 shows memory and disk requirements for vWAAS on ENCS-W with Akamai Connect, by vWAAS model.

Table 7-7 Memory and Disk Requirements for vWAAS on ENCS with Akamai Connect

vWAAS model, Number of ENCS Connections	Memory	Data Disk	Akamai Cache
vWAAS-200, 200 ENCS connections	3 GB	160 GB	100 GB
vWAAS-750, 750 ENCS connections	4 GB	250 GB	250 GB
vWAAS-1300, 1300 ENCS connections	6 GB	300 GB	300 GB
vWAAS-2500, 2500 ENCS connections	8 GB	400 GB	350 GB
vWAAS-6000 6000 ENCS connections	11 GB	500 GB	350 GB

Registering and Deploying vWAAS ENCS 5400-W Series

This section contains the following procedures:

Registering vWAAS on ENCS 5400-W

Before you begin, verify the following:

- The disk is already mounted.
- Gigabit Ethernet port 0/0 can be used for vWAAS management or data.
- Gigabit Ethernet port 0/1 can be used for vWAAS management or data.
- The existing LAN-net and SR-IOV will be used.

To register vWAAS on ENCS, follow these steps:

Step 1 Power on the ENCS device.

The vWAAS automatically starts up when the ENCS device is powered on.

Step 2 Using an Ethernet cable, connect your laptop to the MGMT port of the ENCS device.

Step 3 Verify that the WiFi is disabled on your laptop.

Step 4 Perform the following steps on a MAC system:

- Navigate to **Preferences > Network > Thunderbolt**.
- From the Configure IPv4 drop-down list, choose **Manually**.
- In the IP Address field, enter an IP address, for example, 192.168.1.5.
- In the Subnet Mask field, enter 255.255.255.0.
- Open the terminal and use SSH to connect to the device (192.168.1.1).

  Use **admin** for login and password credentials.

Step 5 Run the shell script (mfg.sh), which registers, installs, and checks the status of the vWAAS instance.

Step 6 Exit.

Deploying vWAAS on ENCS 5400-W

To deploy vWAAS on NFVIS on ENCS, follow these steps:

Step 1 Perform the steps shown in Registering vWAAS on ENCS 5400-W.

Step 2 Copy the vWAAS KVM tar.gz file to a directory on your laptop, for example, “/downloads.”

Step 3 Navigate to the directory that you have created.

Step 4 Start an HTTP server on your laptop to upload and register the image.

Step 5 Connect the Ethernet port of your laptop to the Management port of the Cisco ENCS device.

Step 6 Configure the laptop with static IP, for example, 192.168.1.2.

By default, the Management port on the Cisco ENCS is 192.168.1.1.

Step 7 On your laptop, start the manufacturing script from the directory you have created.

The manufacturing script performs the following actions:

a. Connect to the Cisco ENCS device.

b. The following status messages will be displayed:

```
Trying to connect to ENCS Device
NFVIS server up and running
Reconfiguring the LAN bridge.......
Reconfiguring the WAN bridge.......
Cleaning existing vWAAS instance.......
Checking disk health.......
Following vWAAS images are available:
list of images
```

c. At the **Enter the image number:** prompt, enter your image number.

d. The following status messages will be displayed:

```
Preparing for WAAS installation
Progress: ############ 100%
Installation is in progress.......
Progress: ############ 100%
Installation is completed!!!
```

Step 8 Registration and installation are complete.

Step 9 Exit.

Registering vWAAS on ENCS 5400-W with the Central Manager

You must register the vWAAS instance and/or the WAAS appliance running in accelerator mode with the WAAS Central Manager.

To register vWAAS on NFVIS on ENCS with the Central Manager, these steps:

Step 1 The Central Manager IP address is 10.78.99.142.

At the vWAAS instance or WAAS appliance that you want to register, enter the following Central Manager IP address information:

```
DC2-WAE-1(config)#central-manager address 10.78.99.142
DC2-WAE-1(config)#
DC2-WAE-1(config)#end
DC2-WAE-1#show running-config | i central
central-manager address 10.78.99.142
```

Step 2 At the vWAAS instance or WAAS appliance that you want to register, enable the Centralized Management System (CMS) service:

```
DC2-WAE-1(config)#cms enable
Registering WAAS Application Engine...
Sending  device registration request to Central Manager with address 10.78.99.142
```

```
Please wait, initializing CMS tables
Successfully initialized CMS tables
Registration complete.
Please preserve running configuration using 'copy running-config startup-config'.
Otherwise management service will not be started on reload and node will be shown
'offline' in WAAS Central Manager UI.
management services enabled
```

Step 3 In the Central Manager, navigate to **Devices > All Devices**.

- The WAAS appliance will be displayed in the Device Type column as **OE-ENCS**.

Step 4 Exit.

Adding or Removing RAID-1 for ENCS 5400-W Series

Note The RAID-1 option is available for vWAAS for WAAS Version 6.4.1a and later.

This section contains the following topics:

Note For further information on RAID and the ENCS 5400-W Series, see the *Cisco 5400 Enterprise Network Compute System Hardware Installation Guide*.

Migrating Equipment from No RAID and 1 SSD to RAID-1 and 2 SSDs

Note The RAID-1 option is available for vWAAS for WAAS Version 6.4.1a and later.

Before You Begin

- To enable RAID-1 virtual disk on ENCS, refer to Mixing Drives Types in RAID Groups for hard drive compatibility and best practice for performance. Before creating virtual disk, both drives must be in **Unconfigured Good** state. If drive is in other status, use the CIMC Web GUI or CLI and do the following:

  If disk is in JBOD state:

  a. Navigate to **Storage** tab > **Physical Drive Info** tab.

  b. In the Actions area, choose **Set State as Unconfigured Good**.

  c. Confirm that disk is in Unconfigured Good state.

  *If disk is in **Foreign Config** state:*

  a. Navigate to **Storage** tab > **Controller Info** tab.

  b. In the Actions area, choose **Clear Foreign Config**.

  c. In the Actions area, choose **Unconfigured Good**.

d. Confirm that disk is in Unconfigured Good state.

To create the virtual disk, follow these steps:

Step 1 Log in to the CIMC console.

Step 2 In the CIMC console left pane, click the **Storage** tab.

Step 3 In the CIMC console middle pane, click the **Controller Info** tab.

Step 4 In the Action area, click **Create Virtual Drive from Unused Physical Drives**.\

The Create Virtual Drive from Unused Physical Drives Wait dialog box is displayed.

Step 5 In the Create Virtual Drive from Unused Physical Drives dialog box, choose the following:

a. At the RAID Level drop-down box, choose **1**.

b. In the Create Drive Groups area:

Select physical drives for your system from the Physical Drives pane and click >> to add these to the Drive Groups pane.

c. In the Virtual Drive Properties area:

- The Virtual Drive Name field displays the automatically assigned name.
- At the Strip Size drop-down list, select the strip size (default is 64k).
- At the Write Policy drop-down list, select the Write policy (default is Write Through)
- At the Access Policy drop-down list, select the Access policy (default is Read Write).
- At the Read Policy drop-down list, select the Read policy (default is No Read Ahead).
- At the Cache Policy drop-down list, select the Cache policy (default is Direct IO)
- At the Disk Cache Policy drop-down list, select the Disk Cache policy (default is Unchanged).
- The value for the Size drop-down list automatically filled.

Step 6 Click **Create Virtual Drive**.

Migrating Equipment from RAID-1 and 2 SSDs to No RAID and 1 SSD

Note The RAID-1 option is available for vWAAS for WAAS Version 6.4.1a and later.

Before You Begin

- You must wait for the disk to be completely shut down before you physically remove the disk from the WAE. When the RAID removal process is complete, WAAS generates a disk failure alarm and trap. In addition, a syslog error message is logged.
- If the removal event occurs while the RAID array is in the rebuild process, the RAID removal process may take up to 1 minute to complete. The duration of this process depends on the size of the disk.

  If you administratively shut down the disk during the RAID rebuild process, a RAID rebuild abort alarm is generated instead.

To remove a RAID-1 disk, follow these steps:

Step 1 To manually shut down the disk, enter global configuration mode and then enter the **disk disk-name** *diskxx* **shutdown** command:

```
WAE# configure
WAE(config)# disk disk-name diskxx shutdown
```

Step 2 Wait for the disk to be completely shut down before you physically remove the disk from the WAE.

Step 3 When the RAID removal process is complete, WAAS generates a disk failure alarm and trap. In addition, a syslog error message is logged.

Note We recommend that you disable the **disk error-handling reload** option if it is enabled because it is not necessary to power down the system to remove a disk.

Upgrade/Downgrade Guidelines for vWAAS on ENCS-W

Consider the following for upgrading or downgrading a WAAS device on ENCS:

- You can use the WAAS Central Manager or the CLI to upgrade a vWAAS on ENCS-W device to WAAS Version 6.4.1x.
- You can use the Central Manager to upgrade from the device level and the device group level. To use the Central Manager to upgrade a vWAAS on ENCS-W device:
  1. Telnet to the vWAAS device.
  2. Update the Central Manager IP address.
  3. Login to the Central Manager.
- The Central Manager supports downgrade of all *applicable* device types in a device group.

  For example, if you are downgrading a device group that has a physical WAE, a virtual WAE, and an ENCS platform to a version earlier than WAAS Version 6.4.1, the Central Manager will initiate the downgrade process only for the physical and virtual WAEs, but not for the ENCS platform.
- For upgrade/downgrade guidelines for vWAAS on NFVIS, see Chapter 8, “Cisco vWAAS with Cisco Enterprise NFVIS,” section Upgrade/Downgrade Guidelines for vWAAS with NFVIS.

Cisco vWAAS with Cisco Enterprise NFVIS

This section describes vWAAS on Cisco Enterprise Network Functions Virtualization Infrastructure Software (Enterprise NFVIS). It contains the following sections:

Cisco Enterprise NFVIS

Cisco Enterprise Network Function Virtualization Infrastructure Software (NFVIS) is a Linux-based software hosting layer with embedded KVM hypervisor with CentOS Version 7.x.

Cisco Enterprise NFVIS contains the following features:

- vWAAS with Cisco Enterprise NFVIS is deployed on the Cisco ENCS 5400-W Series. For more information on the ENCS 5400-W Series, see Chapter 7, "Cisco vWAAS on Cisco ENCS 5400-W Series".
- Cisco Enterprise Network Functions Virtualization (NFV)—Extends Linux by packaging additional functions for Virtual Network Functions (VNF) that support lifecycle management, monitoring, device programmability, service chaining, and hardware acceleration.

  Cisco Enterprise NFV also provides local network management capabilities that enable you to dynamically deploy virtualized network functions such as a virtual router, firewall, WAN acceleration, on a supported Cisco device, eliminating the need to add a physical device for every network function.
- Monitoring—Monitors all parameters of the deployed vWAAS, including memory, storage, and CPU, and monitors memory, storage, and CPU utilization of the vWAAS.
- Traffic verification—Verifies traffic flows through vWAAS by monitoring the Virtualized Network Function (VNF) interface statistics.
- Add-On Capability—Ability to add vCPU, memory, and storage, to modify the networking option and add a virtual interface, to configure the virtual networking port and it to a VLAN.

vWAAS with Enterprise NFVIS

This section contains the following topics:

About vWAAS with Enterprise NFVIS

vWAAS with NFVIS enables WAAS to run vWAAS as a standalone virtual machine (VM) on the ENCS 5400-W Series platform, to provide WAN application optimization, and, optionally, application optimization with Akamai Connect.

Caution For guaranteed performance, the ENCS 5400-W Series, UCS-C Series, UCS-E Series, ENCS 5100, CSP-2100, and ISR configurations listed in the WAAS Sizing Guides and specifically noted in WAAS and vWAAS user guides and WAAS Release Notes are the only devices we recommend for use with vWAAS. Although vWAAS models may be able to operate with other Cisco or third-party hardware, successful performance and scale for those configurations is not guaranteed.

For more information about supported platforms for Cisco Enterprise NFV, see the Release Notes for Cisco Enterprise Network Function Virtualization Infrastructure Software, Release 3.9.x,

Table 8-1 shows the platforms and software versions supported for vWAAS with NFVIS.

Table 8-1 Platforms and Software Versions Supported for vWAAS with NFVIS

PID and Device Type	Minimum WAAS Version	Host Platforms	Minimum Host Version	Disk Type
• PID: OE-VWAAS-ENCS • Device Type: OE-VWAAS-ENCS	• 6.4.1	• Cisco ENCS (Enterprise Network Compute System)	• NFV FC2	• virtio
• PID: OE-VWAAS-KVM • Device Type: OE-VWAAS-KVM	• 6.2.x	• Cisco UCS-E Series	• NFV FC2	• virtio

vWAAS with NFVIS on ENCS provides the following capabilities:

- Enterprise Application Optimization—Branch to branch, and branch to data center optimization of application traffic, either within or outside of an IWAN solution. This includes traditional WAAS WAN optimization functions, as well as the deployment of other IWAN solution features that are inherent in IOS-XE platforms.
- XaaS (Everything as a Service) Optimization—For single-sided use cases in cloud deployments, where you have control of one side of the connection: branch to cloud, and data center to cloud (for backup and recovery purposes). Optimizations are applied in a unilateral fashion, without reliance on a peer.

- Service Nodes—A service node is a Cisco WAAS application accelerator that optimizes and accelerates traffic according to the optimization policies configured on the device. It can be a vWAAS instance or a Cisco ENCS appliance.

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 to diskless mode.

- vWAAS with NFVIS on ENCS is part of Cisco Intelligent WAN (IWAN)—a suite of components that brings together WAN optimization, performance routing, and security levels of leased lines and MPLS VPN services to the Internet. For more information on Cisco NFVIS and Cisco NFV, see the *Cisco Intelligent WAN - An SD-WAN Solution*.

vWAAS with NFVIS 3.7.1 System Requirements

Cisco NFVIS 3.7.1 is supported for vWAAS for WAAS Version 6.4.1x.

Table 8-2 shows Cisco Enterprise NFVIS 3.7.1 system requirements.

Table 8-2 Cisco Enterprise NFVIS 3.7.1 System Requirements

System Component	ENCS 5406-W	ENCS 5408-W	ENCS 5412-W
CPU	1	1	2
Memory	2 GB	2 GB	2 GB
Disk Space	10 GB	10 GB	10 GB

For more information on Cisco NFVIS see the *Cisco Enterprise Network Functions Virtualization (NFV) Infrastructure Software Data Sheet*.

About vWAAS with NFVIS for WAAS Version 6.2.x

For vWAAS with NFVIS for WAAS Version 6.2.x, vWAAS is deployed in a RHEL KVM hypervisor on a Cisco UCS-E Series device.

Note For vWAAS with NFVIS for WAAS Version 6.2.x, the vWAAS must run as an unmanaged VM.

To configure vWAAS as an unmanaged VM, follow these steps:

1. From the vCenter Orchestrator configuration console, navigate to **vCenter Server**.
2. For the vCenter Server instance, click Edit.

- Under Specify which strategy will be used for managing the users logins, select Share a unique session and click Apply changes.
- Restart the vCenter Orchestrator Server service.

Unified OVA Package for vWAAS with NFVIS for WAAS Version 6.4.1 and Later

For vWAAS with NFVIS for WAAS Version 6.4.x, vWAAS is deployed in a RHEL KVM hypervisor on a Cisco ENCS 5400-W Series device.

For vWAAS with NFVIS 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.

Caution For guaranteed performance, the ENCS 5400-W Series, UCS-C Series, UCS-E Series, ENCS 5100, CSP-2100, and ISR configurations listed in the WAAS Sizing Guides and specifically noted in WAAS and vWAAS user guides and WAAS Release Notes are the only devices we recommend for use with vWAAS. Although vWAAS models may be able to operate with other Cisco or third-party hardware, successful performance and scale for those configurations is not guaranteed.

For more information about supported platforms for Cisco Enterprise NFV, see the Release Notes for Cisco Enterprise Network Function Virtualization Infrastructure Software, Release 3.9.x,

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.

Traffic Interception for vWAAS with NFVIS

vWAAS with NFVIS on ENCS supports WCCP traffic interception.

The Web Cache Communication Protocol (WCCP) specifies interactions between one or more routers and one or more WAE's, to establish and maintain the transparent redirection of selected types of traffic in real time. The selected traffic is redirected to a group of WAE's with the aim of optimizing resource usage and lowering response times. A WCCP-enabled router and a WAE exchange WCCP protocol packets and negotiate membership of WCCP service groups.

For vWAAS on Cisco ENCS with WCCP, there are two Ethernet Gigabit ports that can be configured to intercept the traffic. With the Network Interception Module card and if the inline interception method is not configured, the ports can be used to intercept the WCCP traffic (configure port channel with LAN and WAN interface).

For detailed information on configuring WCCP, see Chapter 5, “Configuring Traffic Interception” in the *Cisco Wide Area Application Services Configuration Guide*.

Table 8-3 shows the CLI commands used to configure WCCP traffic interception for vWAAS with NFVIS.

Table 8-3 CLI Commands for WCCP Interception Mode

Mode	Command	Description
Global configuration	**interception method wccp**	Configures the WCCP traffic interception method.
	wccp access-list	Configures an IP access list on a WAE for inbound WCCP GRE encapsulated traffic.
	wccp flow-redirect	Redirects moved flows.
	wccp router-list	Configures a router list for WCCP Version 2.
	wccp shutdown	Sets the maximum time interval after which the WAE will perform a clean shutdown of the WCCP.
	wccp tcp-promiscuous	Configures the WCCP Version 2 TCP promiscuous mode service.
	wccp tcp-promiscuous service-pair *serviceID serviceID+1*	Configures the WCCP Version 2 TCP promiscuous mode service and specifies a pair of IDs for the WCCP service on devices configured as application accelerators.

Mode	Command	Description
EXEC	**show statistics wccp**	Displays WCCP statistics for a WAE.
	show wccp clients	Displays which WAEs are seen by which routers.
	show wccp egress	Displays the WCCP egress method—IP forwarding, generic GRE, WCCP GRE, or L2.
	show wccp flows tcp-promiscuous summary	Displays WCCP packet flows and TCP-promiscuous service information.
	show wccp masks tcp promiscuous	Displays WCCP mask assignments and TCP-promiscuous service information.
	show wccp routers [detail]	Displays details of routers seen and not seen by the specified WAE.
	show wccp services [detail]	Displays the configured WCCP services.
	show wccp statistics	Displays WCCP generic routing encapsulation packet-related information.
	show wccp status	Displays the enabled state of WCCP and the configured service IDs.

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

Upgrade/Downgrade Guidelines for vWAAS with NFVIS

This section contains the following topics:

Note For upgrade/downgrade guidelines for vWAAS on ENCS 5400-W, see Chapter 7, "Cisco vWAAS on ENCS 5400-W Device," section Upgrade/Downgrade Guidelines for vWAAS on ENCS-W.

Cisco NFVIS Downgrade Guidelines

- *For vWAAS with Cisco NFVIS 3.7.1,* you cannot downgrade a WAAS device on ENCS to a version earlier than WAAS Version 6.4.1.

  If you try to downgrade a WAAS device on ENCS to a version earlier than WAAS Version 6.4.1, the WAAS Central Manager displays the following warning message:

  Device Group has unsupported devices *ENCS-DeviceName* to the selected version. The image installation will not be applied on such devices.

  Do you still want to proceed with the downgrade?

Cisco vWAAS with Akamai Connect

This chapter provides an overview of Cisco vWAAS with Akamai Connect, and describes the hardware requirements for vWAAS with Akamai Connect, including how to upgrade vWAAS memory and disk for the Akamai Cache Engine (CE).

This chapter contains the following sections:

About Cisco vWAAS with Akamai Connect

Cisco IWAN (Intelligent WAN) --- The Akamai Connect feature integrates an HTTP object cache inside Cisco WAAS. This allows WAAS to cache any HTTP content whether it is delivered via your internal corporate network, direct from the Internet, or from Akamai's Intelligent Platform. For more information, see the "Configuring Application Acceleration" chapter, section "Akamai Connect and WAAS," of the *Cisco Wide Area Application Services Configuration Guide*.

Supported Platforms for Cisco vWAAS with Akamai Connect

Table 9-1 shows supported vWAAS models for Akamai caching up to 6,000 connections. Table 9-2 shows supported vWAAS models for Akamai caching beyond 6,000 connections, and disk and memory requirements for Akamai caching beyond 6,000 connections

Table 9-1 Supported vWAAS Models for Akamai Caching up to 6,000 Connections

Appliance	SM	vWAAS	ISR-WAAS
		vWAAS-150	ISR-G2 and ISR-G3
WAVE-294	SM-700	vWAAS-200	ISR-WAAS-750 (ISR-4451, ISR-4431, ISR-4351, ISR-4331, ISR-4321)
WAVE-594	SM-900	vWAAS-750	ISR-WAAS-1300 (ISR-4451, ISR-4431)
WAVE-694	SM-710	vWAAS-1300	ISR-WAAS-2500 (ISR-4451)
	SM-910	vWAAS-2500	
		vWAAS-6000	

Table 9-2 Supported vWAAS Models and Memory/Disk Requirements for Akamai Connect beyond 6,000 Connections

vWAAS Model	Total HTTP Object Cache Connections (K)	Cache Engine Cache Disk (GB)	Additional Resource to be Added
vWAAS-12000	12	750	6GB RAM, 750 GB disk
vWAAS-50000	50	850	850 GB disk

Note For vWAAS with WAAS Version 6.2.x, vWAAS with Akamai Connect beyond 6,000 connections is not supported for Cisco vWAAS on RHEL KVM or KVM on CentOS.

Cisco vWAAS with Akamai Connect License

Cisco IWAN with Akamai Connect is an advanced license that you can add to Cisco WAAS. The license for Cisco IWAN with Akamai Connect is aligned with the number of optimized connections in each supported Cisco WAAS model.

Table 9-3 lists the standalone licenses for Cisco IWAN with Akamai Connect and vWAAS. For information on all licenses for Cisco IWAN with Akamai Connect, see the *Cisco Intelligent WAN with Akamai Connect Data Sheet*.

Note The actual number of connections for each Cisco IWAN with Akamai Connect License shown in Table 9-3 is dependent on the hardware module on which WAAS is running.

Table 9-3 Licenses for Cisco IWAN with Akamai Connect with vWAAS

Cisco IWAN with Akamai Connect License	License Description	Supported Platforms (vWAAS platforms in bolded text)
SL-1300-AKC	Akamai Connect license for up to 1300 WAAS connections	• ISR-2900/ISR-3900 and one of the following: – **vWAAS-1300 or lower (UCS-E)** • ISR-4451, ISR-4431, ISR-4351, ISR-4331: – **vWAAS-2500 or lower** • UCS server: – **vWAAS-1300 or lower** • WAVE-594
SL-2500-AKC	Akamai Connect license for up to 2500 WAAS connections	• ISR-2900/ISR-3900 and one of the following: – **vWAAS-2500 or lower (UCS-E)** • ISR-4451: – **vWAAS-2500 or lower** • UCS server: – **vWAAS-2500 or lower** • WAVE-694
SL-6000-AKC	Akamai Connect license for up to 6000 WAAS connections	• ISR-2900/ISR-3900 and one of the following: – **vWAAS-6000 or lower (UCS-E)** • UCS server: – **vWAAS-6000 or lower** • WAVE-694

Cisco vWAAS with Akamai Connect Hardware Requirements

Table 9-4 shows the hardware requirements for Cisco UCS (Unified Computing System) E-Series and ISR-WAAS (Integrated Services Router-WAAS) for vWAAS with Akamai Connect.

Note For information on hardware requirements for vWAAS with Akamai Connect on Hyper-V, see Configuring GPT Disk Format for vWAAS-50000 on Hyper-V with Akamai Connect in Chapter 5, "Cisco vWAAS on Microsoft Hyper-V".

Table 9-4 Hardware Requirements for vWAAS with Akamai Connect

Cisco vWAAS or WAAS Model	Memory Required for vWAAS with Akamai Connect	Disk Required for vWAAS with Akamai Connect
vWAAS-150	4 GB	160 GB
vWAAS-200	4 GB	260 GB
vWAAS-750	4 GB	500 GB
vWAAS-1300	6 GB	600 GB
vWAAS-2500	8 GB	750 GB
vWAAS-6000	11 GB	900 GB

Cisco vWAAS or WAAS Model	Memory Required for vWAAS with Akamai Connect	Disk Required for vWAAS with Akamai Connect
vWAAS-12000	18 GB	1500 GB
vWAAS-50000	48 GB	2350 GB
ISR-WAAS-200	2 GB	170 GB
ISR-WAAS-750	4 GB	170 GB
ISR-WAAS-1300	6 GB	170 GB
ISR-WAAS-2500	8 GB	360 GB

Note Table 9-7 shows the WAAS Mid to High End Platform Cache Engine Memory Requirements. Table 9-8 shows the WAAS Mid to High End Platform Cache Engine Cache Disk Requirements.

Upgrading vWAAS Memory and Disk for Akamai Connect

This section has the following information on upgrading upgrade memory and disk to use the Akamai Cache Engine:

- Upgrading vWAAS Memory and Disk with WAAS v5.4.1x through v6.1.1x
- Upgrading vWAAS Memory and Disk with WAAS Version Earlier than v5.4.1
- Upgrading vWAAS Memory and Disk for vWAAS-12000 with ESXi
- Upgrading vWAAS Memory and Disk for vWAAS-12000 with Hyper-V

Upgrading vWAAS Memory and Disk with WAAS v5.4.1x through v6.1.1x

If you are running vWAAS with WAAS Version 6.1.1x, the Akamai disk is added by default; you do not need to use the following upgrade memory and disk procedure to use the Akamai Connect feature with vWAAS.

Upgrading vWAAS Memory and Disk with WAAS Version Earlier than v5.4.1

If you running vWAAS with a WAAS version earlier than Version 5.4.1, and are using an ESXi version lower than Version 5.0, and want to upgrade to WAAS v5.4.1, v5.5.1, or v6.1.1, use the following update memory and disk procedure to use the Akamai Connect feature with vWAAS.

Before using this procedure, note the upgrade paths for WAAS Version 6.2.3 shown in Table 9-5. For complete upgrade instructions, see the *Release Note for Cisco Wide Area Application Services*.

Table 9-5 Upgrade Paths for WAAS Version 6.2.3

Current WAAS Version	WAAS CM Upgrade Path	WAAS Upgrade Path
5.5.3 and later	• Upgrade directly to 6.2.3	• Upgrade directly to 6.2.3
4.3.x through 5.5.1	1. Upgrade to 5.5.3, 5.5.5x (5.5.5, 5.5.5a), or 5.5.7 2. Upgrade to 6.2.3	1. Upgrade to 5.5.3 or 5.5.5x 2. Upgrade to 6.2.3

Step 1 Power off the vWAAS.

Step 2 Right-click the vWAAS and choose **Editing Settings...** .

Step 3 Choose**Add...** .

Step 4 At the **Add Hardware** dialog box, choose **Hard Disk**. Click **Next**.

Step 5 At the **Select a Disk** dialog box, choose **Create a new virtual disk**. Click **Next**.

Step 6 At the **Create a Disk** dialog box:

- At the **Capacity** dropdown lists, enter the size of the new disk.
- At **Disk Provisioning**, choose **Thick Provision Lazy Zeroed**.
- At **Location**, choose **Store with the virtual machine**.
- Click **Next**.

Step 7 At the **Advanced Options** dialog box:

- At the **Virtual Device Node** dropdown list, choose SCSI (0:2).
- At Mode, choose **Persistent**.
- Click **Next**.

Step 8 At the **Ready to Complete** dialog box, confirm the following options:

- Hardware type
- Create disk
- Disk capacity
- Disk provisioning
- Datastore
- Virtual Device Node
- Disk mode

Step 9 Click **Finish**.

Step 10 The screen displays the status message **New hard Disk (adding)**. Click **OK**.

Step 11 Wait until the **Recent Tasks** screen shows **Reconfigure Virtual machine** task as **Completed**. Power on.

Step 12 To verify the new disk, display the current hardware listing with **Virtual Machine Properties > Hardware**.

Upgrading vWAAS Memory and Disk for vWAAS-12000 with ESXi

Caution When the vWAAS-12000 model is deployed, the RAM size is 12 GB and the /local/local1 directory size is 15 GB. When you enable Akamai Connect for vWAAS, you need to increase the RAM to 18 GB. This procedure alters the calculation of the local1 directory size for the vWAAS-12000, because the expected size would be 27 GB. The mismatch between the existing size (15 GB) for the local1 directory and the expected size (27 GB) triggers an alarm.

The mismatch between RAM size and disk size can cause a serious problem during a kernel crash in the vWAAS-12000, because the vmcore file would then be larger than what could be stored in the local1 directory.

To avoid the scenario described in the above Caution note, and to safely upgrade vWAAS memory and disk for Akamai Connect for the vWAAS-12000, follow these steps:

Step 1 Power off the vWAAS VM (Virtual Manager).

Step 2 Add an additional disk of the required size for your system.

Step 3 Increase the size of the RAM.

Note To run Akamai Connect on vWAAS-12000, you must increase the size of the RAM by at least 6 GB.

Step 4 Power on the vWAAS VM.

Step 5 Check the alarms.

The filesystem_size_mism alarm will be raised:

```
Critical Alarms
-----------------------

Alarm ID                  Module/Submodule          Instance
------------------------  ------------------        ---------------

1 filesystem_size_mism    disk                      Filesystem size
```

Step 6 Use the **disk delete-data-partitions** command.

Note The **disk delete-data-partitions** command deletes cache files, including DRE cache files.

Step 7 Reload.

Note You must reload the device after using the **disk delete-data-partitions** command. The reload process automatically re-creates data partitions, and initializes the caches. This process may take several minutes.

DRE optimization will not start until the DRE cache has finished initializing.

Upgrading vWAAS Memory and Disk for vWAAS-12000 with Hyper-V

Caution When the vWAAS-12000 model is deployed, the RAM size is 12 GB and the /local/local1 directory size is 15 GB. When you enable Akamai Connect for vWAAS, you need to increase the RAM to 18 GB. This procedure alters the calculation of the local1 directory size for the vWAAS-12000, because the expected size would be 27 GB. The mismatch between the existing size (15 GB) for the local1 directory and the expected size (27 GB) triggers an alarm.

The mismatch between RAM size and disk size can cause a serious problem during a kernel crash in the vWAAS-12000, because the vmcore file would then be larger than what could be stored in the local1 directory.

To avoid the scenario described in the above Caution note, and to safely upgrade vWAAS memory and disk for Akamai Connect for the vWAAS-12000, follow these steps:

Step 1 Power off the vWAAS VM (Virtual Manager).

Step 2 Add an additional disk of the required size for your system.

Step 3 Increase the size of the RAM.

Note To run Akamai Connect on vWAAS-12000, you must increase the size of the RAM by at least 6 GB.

Step 4 Increase the size of the kdump file from 12.2 GB to 19 GB.

To enable the kernel crash dump mechanism, use the **kernel kdump enable** global configuration command. To display kernel crash dump information for the device, use the **show kdump** EXEC command.

Step 5 Power on the vWAAS VM.

Step 6 Check the alarms.

The filesystem_size_mism alarm will be raised:

```
Critical Alarms
-----------------------
```

```
Alarm ID                  Module/Submodule          Instance
------------------------  ------------------        ---------------

1 filesystem_size_mism    disk                      Filesystem size
```

Step 7 Use the **disk delete-data-partitions** command.

Note The **disk delete-data-partitions** command deletes cache files, including DRE cache files.

Step 8 Reload.

Note You must reload the device after using the **disk delete-data-partitions** command. The reload process automatically re-creates data partitions, and initializes the caches. This process may take several minutes.

DRE optimization will not start until the DRE cache has finished initializing.

Cisco vWAAS-150 with Akamai Connect

For vWAAS for WAAS Version 6.1.1 and later, vWAAS-150 on ISR-WAAS is supported for Akamai Connect (AKC). For WAAS Version 6.2.1 and later, vWAAS-150 is also supported for RHEL KVM and Microsoft Hyper-V (Chapter 5, "Cisco vWAAS on Microsoft Hyper-V").

Note Downgrading vWAAS-150 for RHEL KVM or for Microsoft Hyper-v to a version earlier than WAAS Version 6.2.1 is not supported.

Table 9-6 shows specifications for vWAAS-150.

Table 9-6 vWAAS-150 Profile

Feature	Description
Memory with Akamai Connect	4 GB
Disk with Akamai Connect	160 GB
vCPU	1 vCPU
module	Cisco UCS E-Series NCE blade (PID: UCS-EN120E-208-M2/K9), supported on Cisco ISR-G2 platform
NIM module	Cisco UCS E-Series NCE NIM blade (PID: UCS-EN140N-M2/K9), supported on Cisco ISR-G3 platform

WAAS Central Manager and Cisco vWAAS-150

For the Cisco vWAAS-150 model, the WAAS Central Manager (CM) must be WAAS Version 6.2.1 or later, but supports mixed versions of device models (Version 6.2.1 and earlier). The WAAS CM must be a higher or equal version than associated devices.

Note The vWAAS-150 model is deployed for WAAS Version 6.1.1 only, so you cannot upgrade or downgrade the vWAAS-150 from Version 6.1.1.

Akamai Connect Cache Engine on Cisco Mid- and High-End Platforms

For WAAS Version 6.2.1 and later, the Akamai Connect Cache Engine (CE) is supported for scaling beyond 6,000 connections on the following platforms:

- WAVE-7541, WAVE-7571, and WAVE-8541
- vWAAS-12000 and vWAAS 50000

Scaling for these platforms is based on memory availability, scale performance, and the particular dynamic cache-size management feature. Table 9-7 shows the connections, total memory, and cache engine memory requirements for each of these platforms. Table 9-8 shows the connections, number of disks, and cache engine disks for each of these platforms.

The Akamai Connect CE connection-handling capacity is determined by the upper limit of memory that is given to the Akamai Connect CE at startup. The Akamai Connect CE will allocate memory as needed up to the upper limit; on approaching that limit, it will push back new connections. In case of overload, the connection will be optimized by HTTP-AO, without a caching benefit.

Note For vWAAS-12000 and vWAAS-50000, HTTP object cache will scale up to the platform TFO limit. To achieve this, you must augment the platform resources (CPU, RAM, and disk) during provisioning.

For vWAAS-12000, you must allocate at least 6 GB of additional RAM.

For vWAAS-12000 and vWAAS-50000, you must allocate Cache Engine cache disk resources. Cache disk requirements are shown in Table 9-8.

Table 9-7 WAAS Mid to High End Platform Cache Engine Memory Requirements

Cisco WAAS Platform	HTTP Object Cache Connections	CPU	Total Memory	Memory Required for Cache Engine
vWAAS-12000	12 K	4	18 GB	4308 M
vWAAS-50000	50 K	8	48 GB	14136 M
WAVE-7541	18 K	2	24 GB	5802 M
WAVE-7571	60 K/ 50 K/ 40 K	2	48 GB	15360 M/ 14125 M/ 11565 M
WAVE-8541	150 K/ 125 K/1 00 K	2	96 GB	38400 M/ 32000 M/ 25600 M

Table 9-8 WAAS Mid to High End Platform Cache Engine Cache Disk Requirements

Cisco WAAS Platform	HTTP Object Cache Connections	CPU	Disk/ CE Cache Disk	Cache Engine Cache Disk
vWAAS-12000	12 K	4	750 GB	750 GB
vWAAS-50000	50 K	8	1500 GB	850 GB
WAVE-7541	18 K	2	2200 GB	708 GB
WAVE-7571	60 K/ 50 K/ 40 K	2	3100 GB	839 GB
WAVE-8541	150 K/ 125 K/100 K	2	4.1 TB	675 GB

CHAPTER 10

Cisco vWAAS in Cloud Computing Systems

This chapter contains the following sections:

Cisco vWAAS in Cloud Computing Systems

Cisco vWAAS is a cloud-ready WAN optimization solution that is fully interoperable with WAAS appliances, and can be managed by a common central manager or virtual central manager. The vWAAS cloud computing solution includes these features:

- On-demand orchestration that responds to the creation or movement of application server VMs.
- Minimal network configuration, including in a dynamic environment.
- Designed for scalability, elasticity, and multi-tenancy support.
- Designed for minimal network configuration in a dynamic environment.

Cisco vWAAS in Microsoft Azure

This section contains the following topics:

About Cisco vWAAS in Microsoft Azure

Azure is a Microsoft Cloud that provisions virtual machines (VMs) on the Microsoft Hyper-V hypervisor. vWAAS in Azure is part of WAAS support for Office 365, and is an end-to-end solution with enterprise branch offices.

- vWAAS in Azure is available for vWAAS Version 6.2.1x and later, and is supported for vWAAS-200, vWAAS-750, vWAAS-1300, vWAAS-2500, vWAAS-6000, and vWAAS-12000v.

- vWAAS in Azure is not supported for vWAAS-50000.

Table 10-1 shows the platforms supported for Cisco vWAAS in Microsoft Azure.

Table 10-1 Microsoft Azure VM Sizes for Cisco WAAS vWAAS Models

vWAAS Model	Maximum Connections	Data Disk	Minimum Azure VM Size
vWAAS-200	200	160 GB	D2_v2 (2 cores, 7GB)
vWAAS-750	750	250 GB	D2_v2 (2 cores, 7GB)
vWAAS-1300	1300	300 GB	D2_v2 (2 cores, 7GB)
vWAAS-2500	2500	400 GB	D3_v2 (4 cores, 14GB)
vWAAS-6000	6000	500 GB	D3_v2 (4 cores, 14GB)
vWAAS-12000	12000	750 GB	D3_v2 (4 cores, 14GB)

Operating Considerations for Cisco vWAAS in Microsoft Azure

This section contains the following topics:

vWAAS in Microsoft Azure and WAAS Interoperability

Note the following operating considerations for Cisco vWAAS in Microsoft Azure:

- vWAAS in Azure is available for all vWAAS models, for WAAS Version 6.2.1 and later.
- You can display and identify an Azure vWAAS device on the WAAS Central Manager or the CLI:
  - On the WAAS Central Manager, navigate to the **Manage Devices** screen. The vWAAS in Azure device type is displayed as **OE-VWAAS-AZURE**.
  - On the CLI, use either the **show version** EXEC command or the **show hardware** EXEC command. Output for both commands will include device ID, shown as **OE-VWAAS-AZURE**.
- vWAAS in Azure communicates with the WAAS Central Manager in the same ways as physical appliances communicate with the Central Manager.

  A vWAAS in Azure device is displayed on the WAAS Central Manager as AZURE-VWAAS. To display vWAAS in Azure devices, navigate to **Home > Devices > All Devices**. The Device Type column shows all WAAS and vWAAS devices.

Note For vWAAS in Azure, the supported traffic interception method is PBR (Police-Based Routing); vWAAS in Azure does not support WCCP or AppNav interception methods.

- Registering the vWAAS in Azure to the WAAS Central Manager:
  - If you register the vWAAS with the WAAS Central Manager using a private IP address, following the usual vWAAS registration process described in Configuring vWAAS Settings of Chapter 2, “Configuring and Cisco vWAAS and Viewing vWAAS Components.

– If you register the vWAAS with the WAAS Central Manager using a public IP address, you must specify the public address of the vWAAS in the WAAS Central Manager Device Activation screen (navigate to **Devices >** *device-name* **> Activation**).

Note After you have registered the vWAAS in Azure device to the WAAS Central Manager, you must configure the public IP address of the Central Manager. The vWAAS in Azure device can contact the Central Manager only by using the public IP address of the registration. To set the public IP address of the WAAS Central Manager:

1. In the WAAS Central Manager, navigate to **Home > Devices >** *Primary-CM-Device* **> Configure > Network > NatSettings**.

2. In the NAT IP field, enter the public IP address of the Central Manager.

Operating Limitations for vWAAS in Microsoft Azure

Note the following operating limitations for Cisco vWAAS in Microsoft Azure:

- vWAAS auto-registration is not supported, because Microsoft Azure uses DHCP to configure VMs with IP address and Azure fabric server IP address. There will be operational issues if you deploy a separate DHCP server for auto-registration.

  Functionality similar to auto-registration is available by providing the WAAS CM IP address during VM provisioning. The vWAAS VM will try to register with this WAAS CM during provisioning.
- Microsoft Azure does not support GRE, IPv6, or Jumbo Frames, therefore vWAAS in Azure does not support these features.

Note For vWAAS in Azure, the supported traffic interception method is PBR (Police-Based Routing); vWAAS in Azure does not support WCCP or AppNav interception methods.

- WAAS/vWAAS with Akamai Connect is not supported for vWAAS in Azure.

Upgrade/Downgrade Considerations for Cisco vWAAS in Microsoft Azure

Consider the following upgrade/downgrade guidelines for Cisco vWAAS in Microsoft Azure:

- The procedure for upgrading or downgrading vWAAS in Azure, for all vWAAS models except vWAAS-50000, is the same as for any other WAAS device.
- Downgrading a device or device group for vWAAS in Azure to a WAAS Version earlier than Version 6.2.1 is not supported.

Deploying Cisco vWAAS in Miscrosoft Azure

This section contains the following topics:

Deployment Options for Cisco vWAAS in Microsoft Azure

There are two major deployment options for Cisco vWAAS in Microsoft Azure:

- A SaaS application, such as an enterprise application where you control hosting of the application.

  In this type of deployment, both the application server and Cisco vWAAS can be put in the Azure cloud just as in a private cloud. The vWAAS is very close to the server, and tied to the server movement. In this case, the traffic flow is very similar to that in a normal enterprise data center deployment.

- A SaaS application such as Office 365, where you do not control hosting of the application

  In this type of deployment, you do not have control over the application in the cloud; you control only the vWAAS. In this case, traffic from the CSR in the branch is tunneled to the CSR in Azure, which is then redirected to the vWAAS. A Destination Network Address Translation (DNAT) is performed to get the traffic back to the CSR in the Azure cloud from the SaaS application. For more information on Office 365 and WAAS, see *Accelerate Microsoft Office 365 Shared Deployments with Cisco WAAS WAN Optimization*.

Provisioning the vWAAS VM in Microsoft Azure

Note To deploy vWAAS in Azure, you need a Microsoft Azure Pay-As-You-Go subscription. Subscription procedure and billing information are available on the Microsoft Azure website.

To provision the vWAAS VM in Microsoft Azure, follow these steps:

Step 1 Login to the Microsoft Azure portal.

Step 2 Navigate to **New > Compute > Virtual Machine > From Gallery**.

The **Create a Virtual Machine/Choose an Image** screen is displayed.

Step 3 At the **Create a Virtual Machine/Choose an Image > My Images** screen, select the vWAAS Azure image for your system.

The **Create a Virtual Machine/Virtual Machine Configuration** screen is displayed.

Step 4 In the Virtual Machine Name field, enter the name of the VM you want to create. Use only letters and numbers, up to a maximum of 15 characters.

Step 5 In the Tier field, select **Standard**.

Step 6 At the Size dropdown list, select the Azure VM size for your system. Table 10-2 shows the minimum Azure VM size for each vWAAS model available for provisioning in the Tier field.

Table 10-2 Microsoft Azure VM Sizes for Cisco WAAS vWAAS Models

vWAAS Model	Maximum Connections	Data Disk	Minimum Azure VM Size
vWAAS-200	200	160 GB	D2_v2 (2 cores, 7GB)
vWAAS-750	750	250 GB	D2_v2 (2 cores, 7GB)
vWAAS-1300	1300	300 GB	D2_v2 (2 cores, 7GB)
vWAAS-2500	2500	400 GB	D3_v2 (4 cores, 14GB)

Note Use the Microsoft Azure Tier field to select an Azure VM for the vWAAS models shown in Table 10-2. For vWAAS-6000 and vWAAS-12000, you must use the template to specify the Azure VM. For more information, see Deploying Cisco vWAAS in Miscrosoft Azure. For Azure VM sizes for vWAAS-6000 and vWAAS-12000, see Table 10-1.

Step 7 In the New User Name field, enter your user name.

Step 8 In the New Password field, enter your password.

Step 9 In the Confirm field, re-enter your password.

Step 10 (Optional) If your system uses SSH key-based authentication:

a. Check the **Upload compatible SSH key for authentication** checkbox.

b. At the Certificate field, browse for the certificate file for your system.

Step 11 (Optional) If your system requires a password, check the **Provide a password checkbox**.

Step 12 Click the right arrow at the lower right of the screen to proceed to the next screen.

The next **Create a Virtual Machine/Virtual Machine Configuration** screen is displayed.

Step 13 At the Cloud Service dropdown list, select **Create a Cloud Service**.

Step 14 In the Cloud Service DNS Name field, enter the name of the VM that you created in Step 4.

In the naming style of Azure VMs, the DNS name has **cloudapp.net** automatically appended to it.

Step 15 At the Region/Affinity Group/Virtual Network dropdown list, choose a location that is in close proximity to the resources you want to optimize, such as East US or North Europe.

The Region/Affinity Group/Virtual Network setting determines the location of the VM within the Azure cloud data centers.

Step 16 At the Storage Account dropdown list, select **Use an automatically generated storage account**.

Step 17 At the Availability Set dropdown list, choose **(None)**.

Step 18 Click the right arrow at the lower right corner of the screen to proceed to the next screen.

The **Virtual Machines/Virtual Machine Instances** screen is displayed

Step 19 By default, the **Install the VM Agent** check box is checked.

Step 20 In the Endpoints section:

a. Add an endpoint for **SSH (port 22**)

b. Add an endpoint for **HTTPS** (**port 443**)

Step 21 Click the checkmark at the lower right corner of the screen to proceed for provisioning vWAAS.

The **Virtual Machines/Virtual Machine Instances** screen is displayed, showing the newly-created VM with an initial status of *Starting (Provisioning)*.

Step 22 The process takes a few minutes before the VM status is displayed as running.

Step 23 Select the vWAAS VM.

Step 24 Attach the data disks. See Table 10-2 for data disk sizes for Azure VMs.

Step 25 Stop and then start the VM, so that it picks up the attached disks.

Your VM is ready to be deployed, with end-to-end setup.

Deploying vWAAS in Microsoft Azure

This section has the following topics:

Deploying vWAAS VM and Data Disk with the VHD Template

To deploy the vWAAS VM and data disk with the VHD template, follow these steps:

Step 1 Copy **vwaas.vhd** to the storage account using AzCopy.

The AzCopy command parameters are:

- **Source:** The local folder address on the Windows device where the VHD file is stored.
- **Dest:** The location of the container on the Azure cloud storage account.
- **Destkey:** The Azure cloud storage account key.

Step 2 Use the template to deploy the vWAAS VM.

The vWAAS VM is deployed with the data disk.

Step 3 Log in with your username and password.

Step 4 (Optional) To verify deployment details such as CMS registration and WAAS Central Manager address, see Verifying the vWAAS in Azure Deployment.

Deploying vWAAS VM with Template and Custom VHD from the Microsoft ARM Portal

To deploy the vWAAS VM with a template and custom VHD from the Microsoft Azure Resource Manager (ARM) portal, follow these steps:

Step 1 *Prerequisite:* Verify that the vWAAS VM is provisioned in Azure, including the creation of a storage account and a VM location in Azure specified. For more information, see Provisioning the vWAAS VM in Microsoft Azure.

Step 2 Copy **vwaas.vhd** to the storage account using Azcopy.

Step 3 Use the template to deploy the vWAAS VM.

Step 4 At the Microsoft ARM portal, navigate to **New > Template Deployment > Edit Template**.

Step 5 Copy the template <<? from which location, or ? from flash>>

Step 6 Paste the template here.

Step 7 For the parameters, enter the values for your system, such as resource group and resource group location, and whether or not to deploy the vWAAS VM in a new or existing virtual network.

Step 8 Accept the Terms and Conditions.

Step 9 Click Create.

Step 10 The vWAAS VM is deployed.

Step 11 Log in with your username and password.

Step 12 (Optional) To verify deployment details such as CMS registration and WAAS Central Manager address, see Verifying the vWAAS in Azure Deployment.

Deploying vWAAS VM Using Windows Powershell

To deploy the vWAAS VM using Windows Powershell, follow these steps:

Step 1 *Prerequisite:* Verify that the vWAAS VM is provisioned in Azure, including the creation of a storage account and a VM location in Azure specified. For more information, see Provisioning the vWAAS VM in Microsoft Azure.

Step 2 Deploy vWAAS on Microsoft Hyper-V. For information on this deployment procedure, see Chapter 5, "Cisco vWAAS on Microsoft Hyper-V".

Step 3 Run the **azure_predeploy.sh** script in Hyper-V, to set the necessary Azure parameters.

Step 4 Export the flash VHD from the Hyper-V disk location to the storage account in Azure, using AzCopy.

Step 5 Use Windows Powershell commands to specify the following parameters:

- Use the **deployName** command to specify the deployment name.
- Use the **RGName** command to specify the resource group.
- Use the **locName** command to specify the location.
- Use the **templateURI** command to specify the template file.

Step 6 Use the **New-AzureRmResourceGroup -Name $RGName -Location $locName** Powershell command to create the resource group.

Step 7 Use the **New-AzureRmResourceGroupDeployment** Powershell cmdlet to deploy vWAAS in Azure. To complete the deployment, specify values for the following parameters:

- userImageStorageAccountName
- userImageStoragContainerName
- userImageVhdName
- osType
- vmName
- adminUserName
- adminPassword

Step 8 After you enter these parameters, vWAAS in Azure is deployed. The system displays provisioning information, including deployment name, provisioning state, date/time, and mode.

Step 9 Log in with your username and password.

Step 10 (Optional) To verify deployment details such as CMS registration and WAAS Central Manager address, see Verifying the vWAAS in Azure Deployment.

Verifying the vWAAS in Azure Deployment

Table 10-3 provides a checklist for verifying the vWAAS VM deployment in Microsoft Azure.

Table 10-3 Checklist for Verifying the vWAAS in Azure Deployment

Task	Description
Viewing vWAAS in Azure vWAAS devices	• On the WAAS Central Manager, navigate to the **Manage Devices** screen. The vWAAS in Azure device type is displayed as **OE-VWAAS-AZURE**. • On the WAAS CLI, use either the **show version** EXEC command or the **show hardware** EXEC command. Output for both commands will include device ID, shown as **OE-VWAAS-AZURE**.
Viewing Boot Information and Diagnostics	On the Azure portal, navigate to **Virtual Machines > VM > Settings > Boot Diagnostics** on the Azure portal.
Verifying CMS Registration	If the Centralized Management System (CMS) is enabled, use the **show cms device status** *name* command to display status for the specified device or device group. **Note** After you have registered the vWAAS in Azure device to the WAAS Central Manager, you must configure the public IP address of the Central Manager. The vWAAS in Azure device can contact the Central Manager only by using the public IP address of the registration. To set the public IP address of the WAAS Central Manager: 1. In the WAAS Central Manager, navigate to **Home > Devices >** *Primary-CM-Device* **> Configure > Network > NatSettings**. 2. In the NAT IP field, enter the public IP address of the Central Manager.
Verifying WAAS Central Manager Address	Use the **show running-config** command to display information about all WAAS device.

Note Whenever ARP cache(s) are cleared or the vWAAS is rebooted, packets may not be forwarded to the next hop in Azure cloud. To ensure that packets are successfully forwarded, use the **ping** EXEC command to update the ARP cache table.

Cisco vWAAS in OpenStack

This section contains the following topics:

Operating Considerations for vWAAS in OpenStack

Consider the following operating guidelines for vWAAS in OpenStack:

- vWAAS in OpenStack is supported for vWAAS for WAAS Version 6.4.1b and later.
- vWAAS in OpenStack is supported for all vWAAS and vCM models that are supported on KVM on CentOS.
- On the Central Manager, vWAAS devices in OpenStack are displayed as OE-VWAAS-OPENSTACK.
- All vWAAS models for vWAAS in OpenStack are deployed with a single, unified OVA. Here are examples of the unified OVA and NPE OVA package filenames for vWAAS in OpenStack:
  - 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

Upgrade/Downgrade Guidelines for Cisco vWAAS in OpenStack

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

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

Deploying Cisco vWAAS in OpenStack

This section contains the following topics:

Guidelines for Deploying vWAAS in OpenStack

Consider the following guidelines to deploy Cisco vWAAS in OpenStack:

- vWAAS in OpenStack is deployed for vWAAS on KVM. For more information on vWAAS on KVM, see the chapter "Cisco vWAAS on RHEL KVM and KVM CentOS".

  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. 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 OpenStack is operational on a device, you can use the WAAS CM or the WAAS CLI to display the OpenStack device.

- The WAAS CM displays the following information for the device:

  The OpenStack device is displayed in the **Devices** > **All Devices** listing under Device Type as OE-VWAAS-OPENSTACK.

  The OpenStack device is displayed in the **Devices** > *device-name* > **Dashboard** as OE-VWAAS-OPENSTACK.

- 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 OpenStack

To deploy vWAAS in OpenStack, follow these steps:

Step 1 Copy the unified OVA to a directory on the host machine.

Step 2 Untar the OVA using the following command, shown below and in Figure 10-1.

```
tar -xvf Cisco-KVM-vWAAS-Unified-6.4.1b-b-11.tar.gz
```

Figure 10-1 Tar Command for vWAAS OpenStack OVA

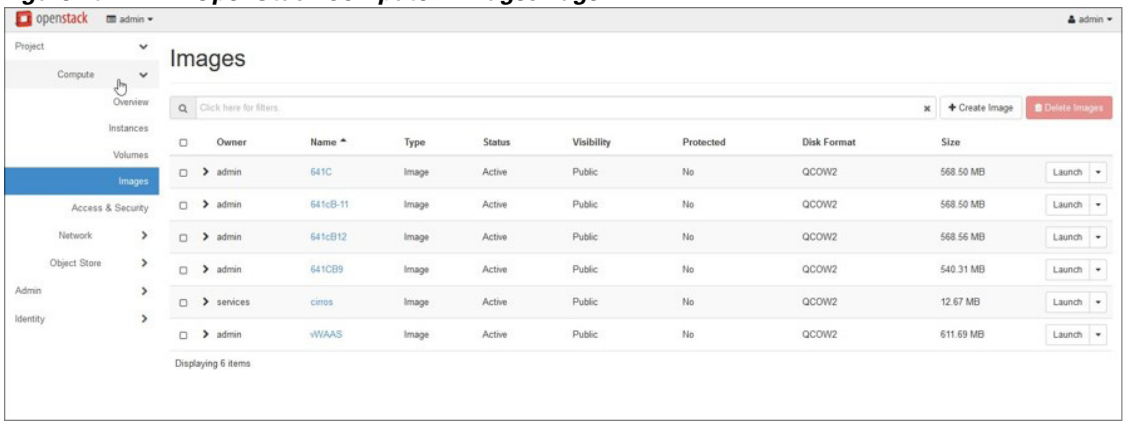
```
linux-qpaw:/home/b-11 # ls
Cisco-KVM-vWAAS-Unified-6.4.1c-b-11-npe.tar.gz  Cisco-KVM-vWAAS-Unified-6.4.1c-b-11.tar.gz
linux-qpaw:/home/b-11 # tar -xvf Cisco-KVM-vWAAS-Unified-6.4.1c-b-11.tar.gz
Disk-0.qcow2
Disk-1.qcow2
Disk-2.qcow2
launch.sh
vm.xml
ezdeploy.sh
ezdeploy_qstatus.exp
INSTRUCTIONS.TXT
OPENSTACK_INSTRUCTIONS.TXT
image_properties.xml
bootstrap-cfg.xml
akamai_disk.tar
model.txt
vwaas_install.sh
vwaas-admin-deny-config.xml
permit.xml
package.mf
```

355736

Step 3 Create the image.

From the OpenStack Admin tab, open the Compute > Images page (Figure 10-2).

Figure 10-2 OpenStack Compute > Images Page



355721

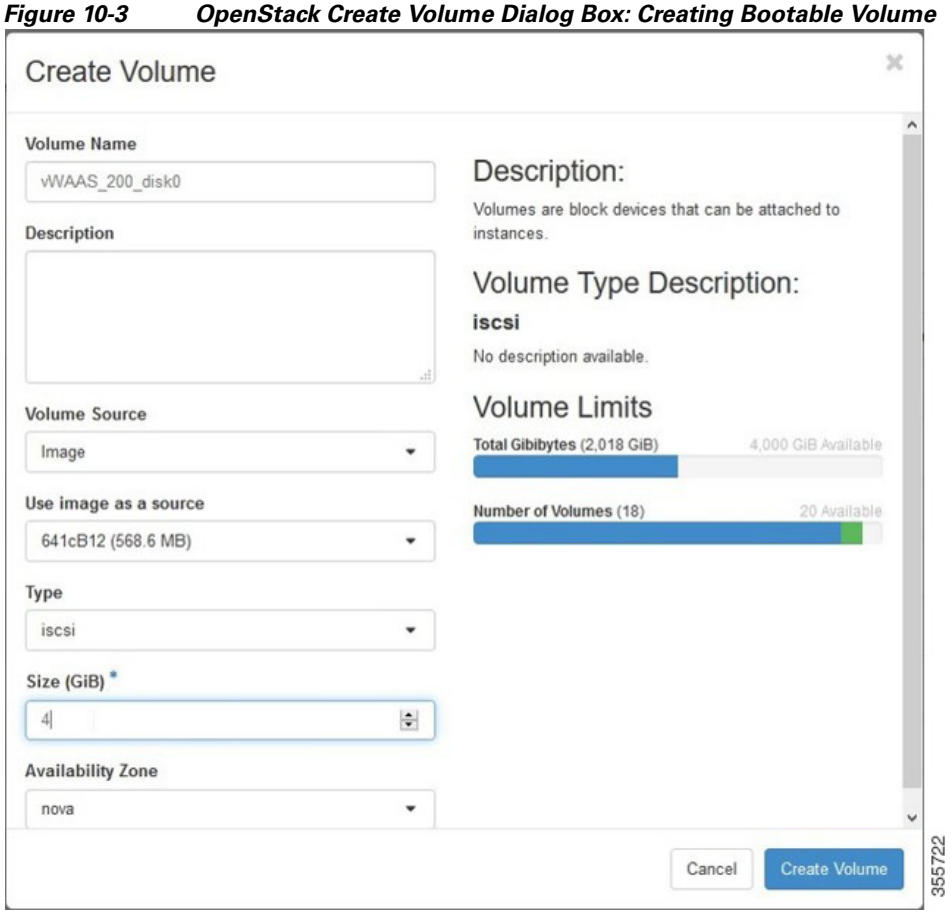
a. From the Images table listing, select the image for your system.

b. To create the image, click **Create Image**.

Step 4 Create the bootable volume.

From the OpenStack Admin tab, open the Compute > Create Volume page (Figure 10-3).

Figure 10-3 OpenStack Create Volume Dialog Box: Creating Bootable Volume



a. In the **Volume Name** field, enter the name of the vWAAS model and disk, for example, **vWAAS_200_disk0**.

b. From the **Volume Source** drop-down list, choose **Image**.

c. From the **Use image as a source** drop-down list, choose the build number for your system, for example, **641bB12 (568.6 MB)**.

d. From the **Type** drop-down list, choose **iscsi**.

e. From the **Size (GiB)** drop-down list, choose the size for this volume, for example, **4**.

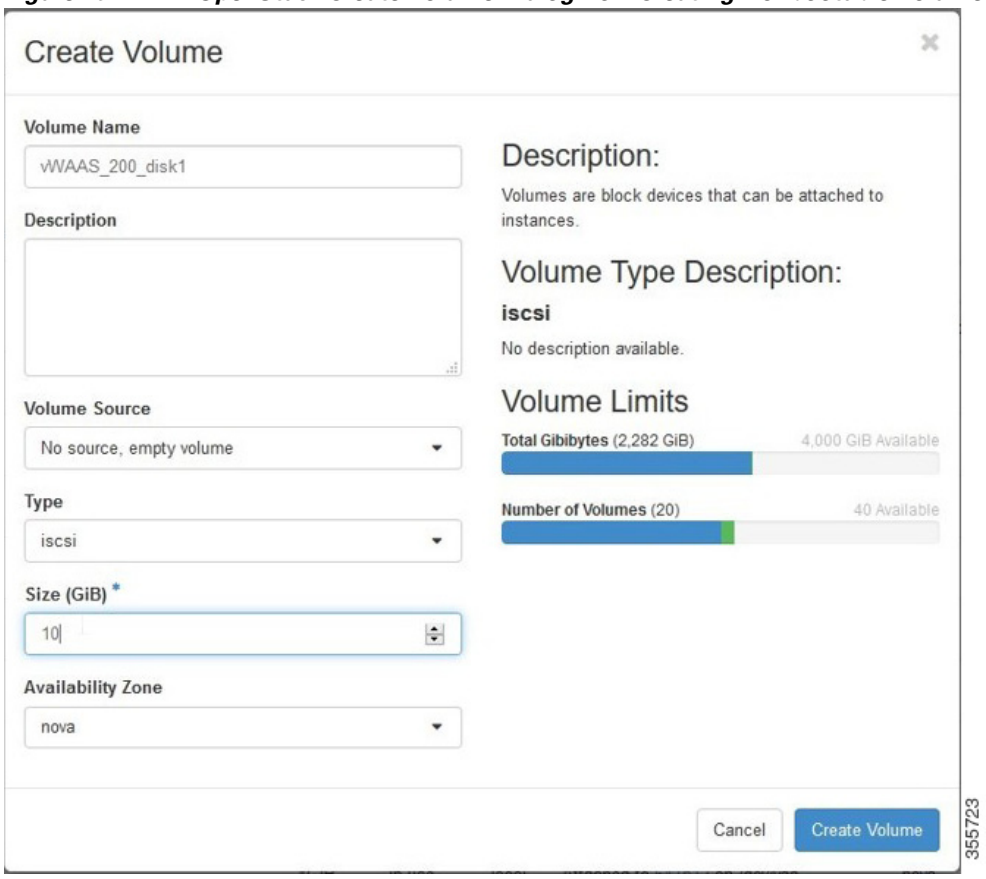
f. From the **Availability** drop-down list, choose **nova**.

g. Click **Create Volume**.

Step 5 Create nonbootable volumes.

From the OpenStack Admin tab, open the Compute > Create Volume page (Figure 10-4).

Figure 10-4 OpenStack Create Volume Dialog Box: Creating Nonbootable Volumes



a. In the **Volume Name** field, enter the name of the vWAAS model and disk, for example, **vWAAS_200_disk1**.

b. From the **Volume Source** drop-down list, choose **No source, empty volume**.

c. From the **Type** drop-down list, choose **iscsi**.

d. From the **Size (GiB)** drop-down list, choose the size for this volume, for example, **10**.

e. From the **Availability** drop-down list, choose **nova**.

f. Click **Create Volume**.

Step 6 On the OpenStack Compute > Volumes page, create all volumes related to your deployed model (Figure 10-5).

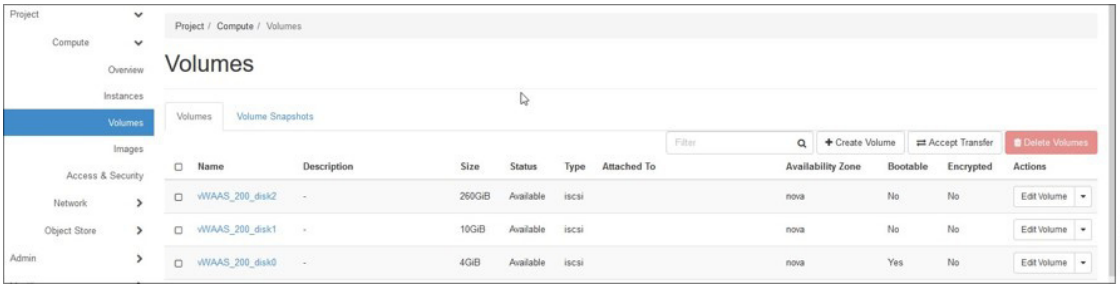
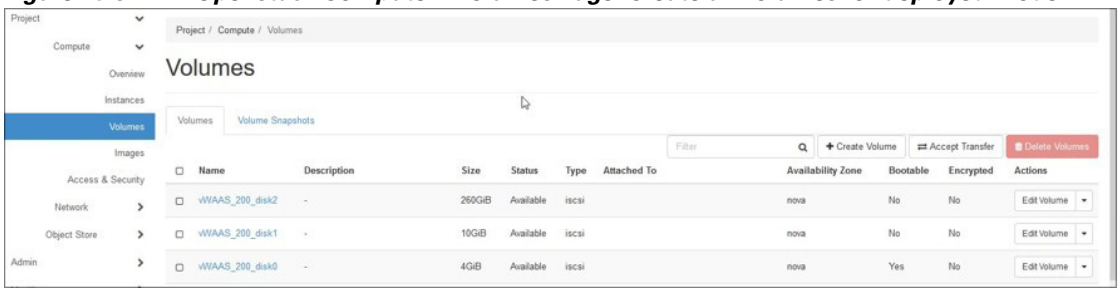
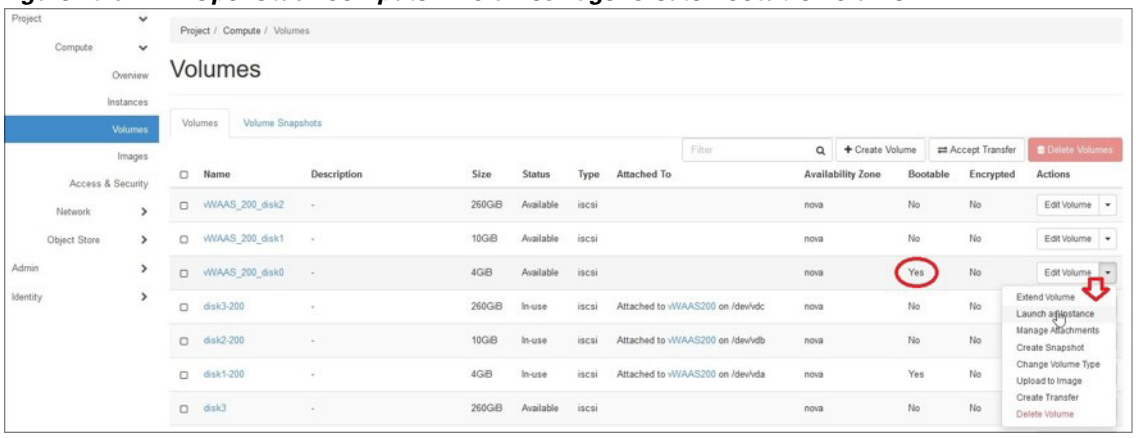


Figure 10-5 Openstack Compute > Volumes Page: Create all volumes for deployed model



On the OpenStack Compute > Volumes page, create an instance with a bootable volume (Figure 10-6).

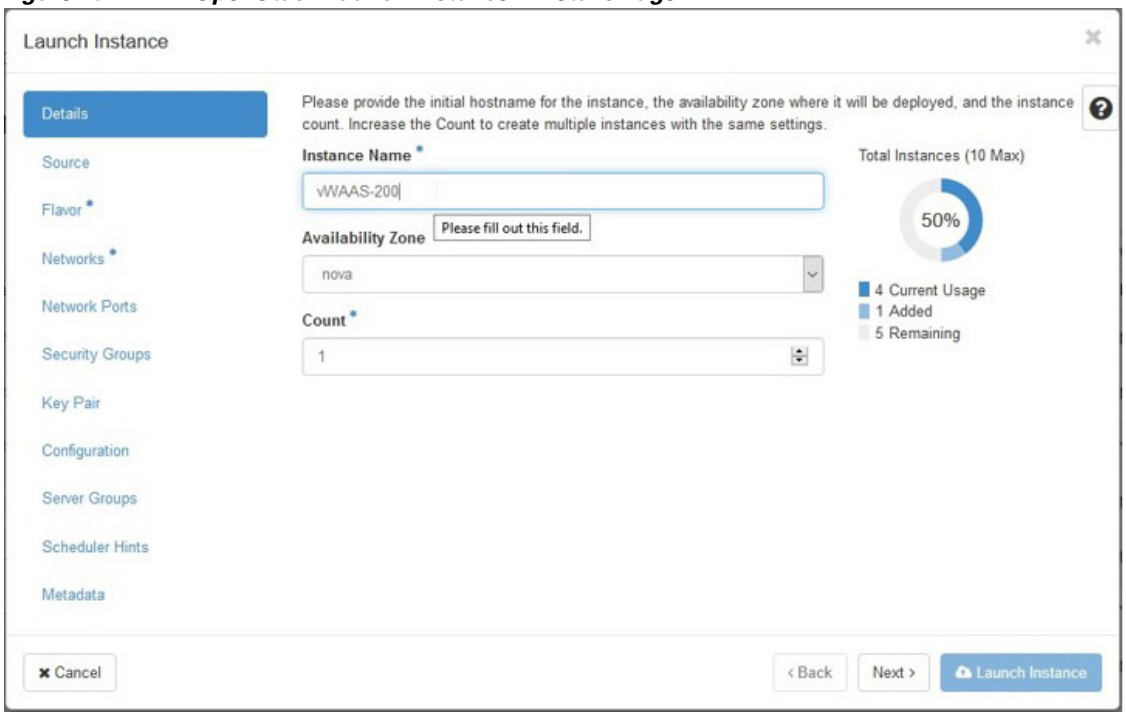
Figure 10-6 OpenStack Compute > Volumes Page: Create Bootable Volume



Step 7 Launch the instance.

From the OpenStack Admin tab, open the Compute > Instances > Launch Instance page (Figure 10-7).

Figure 10-7 OpenStack Launch Instance > Details Page



a. In the **Instance Name** field, enter the name of the vWAAS model, for example, **vWAAS-200**.

b. From the **Availability** drop-down list, choose **nova**.

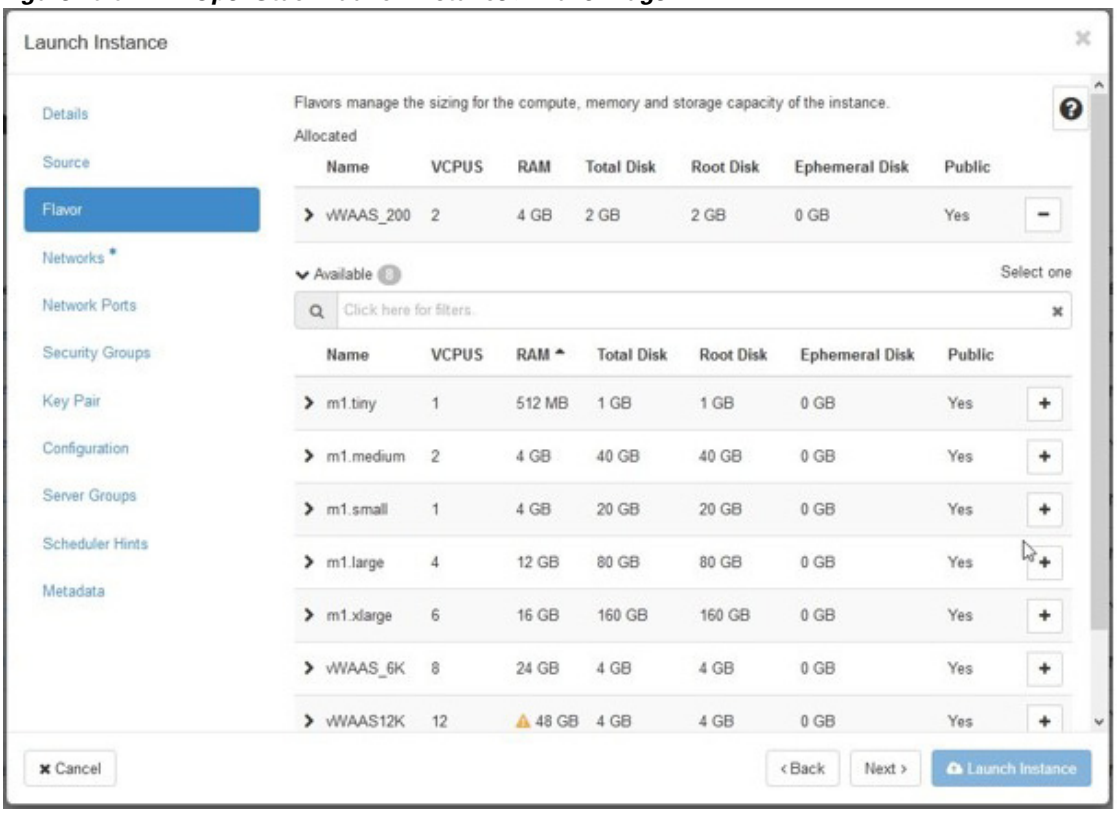
c. From the **Count** drop-down list, choose **1**.

d. Click **Launch Instance**.

Step 8 Specify the flavor suitable for the selected vWAAS model. As noted on the OpenStack page (Figure 10-8), flavors manage the sizing for the compute, memory, and storage capacity of the instance.

From the OpenStack Admin tab, open the Compute > Instances > Launch Instance > Flavor page (Figure 10-8).

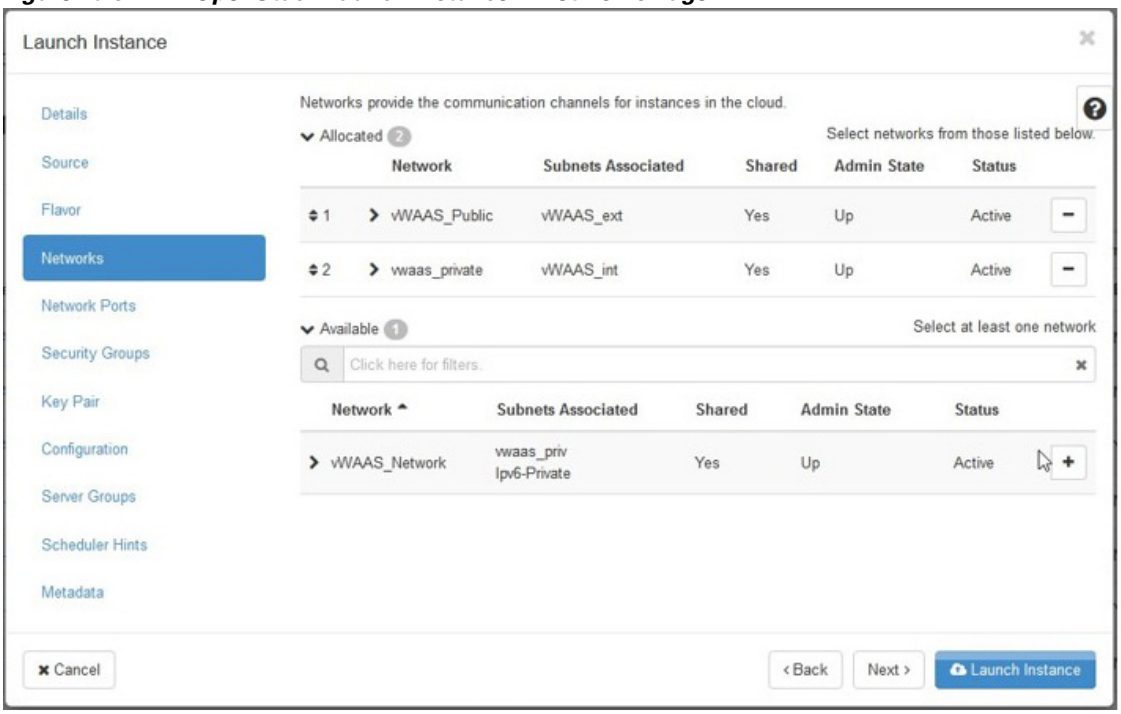
Figure 10-8 OpenStack Launch Instance > Flavor Page



Step 9 Select the networks for the vWAAS.

From the OpenStack Admin tab, open the Compute > Instances > Launch Instance > Networks page (Figure 10-9).

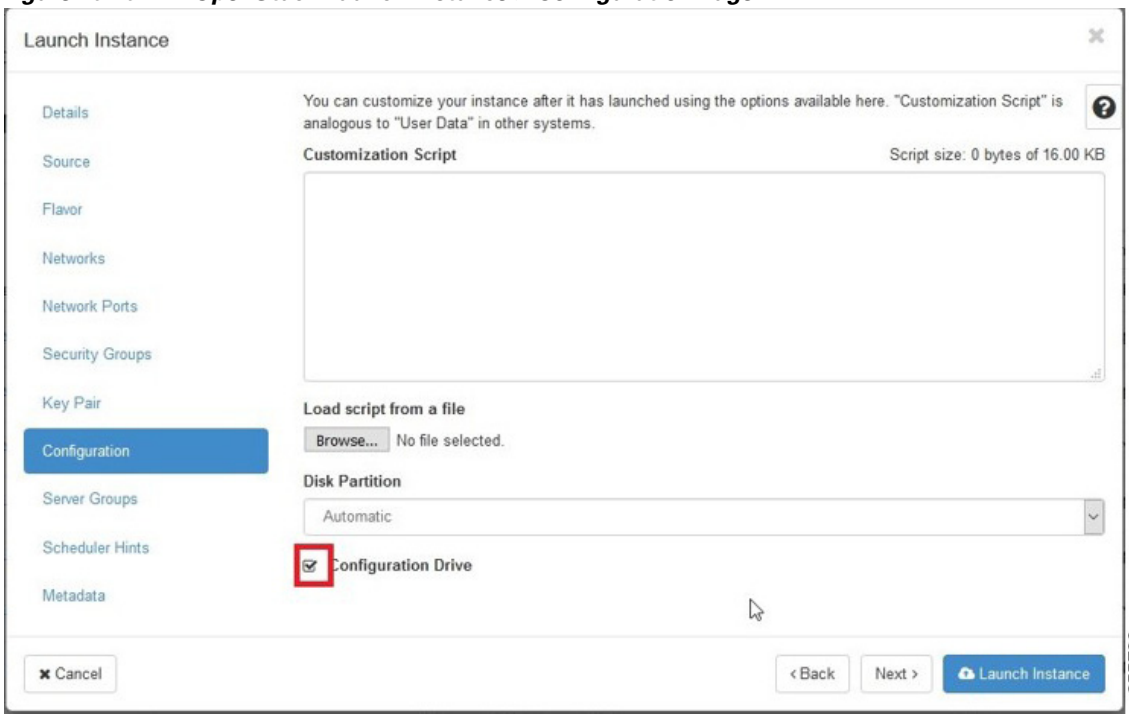
Figure 10-9 OpenStack Launch Instance > Networks Page



Step 10 Select the configuration drive to send model parameters.

From the OpenStack Admin tab, open the Compute > Instances > Launch Instance > Configuration page (Figure 10-10).

Figure 10-10 OpenStack Launch Instance > Configuration Page



a. From the **Disk Partition** drop-down list, choose **Automatic**.

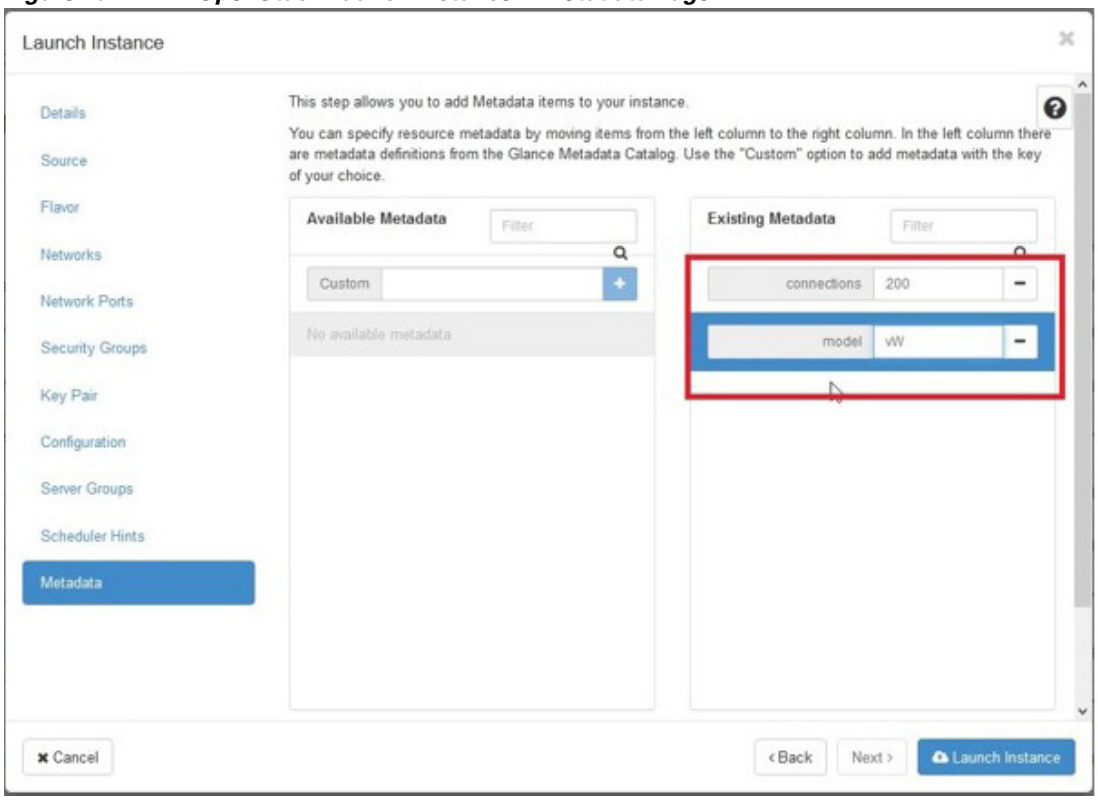
b. Check the **Configuration Drive** check box.

c. Click **Launch Instance**.

Step 11 Provide model and connection information to deploy vWAAS in OpenStack metadata.

From the OpenStack Admin tab, open the Compute > Instances > Launch Instance > Metadata page (Figure 10-11).

Figure 10-11 OpenStack Launch Instance > Metadata Page

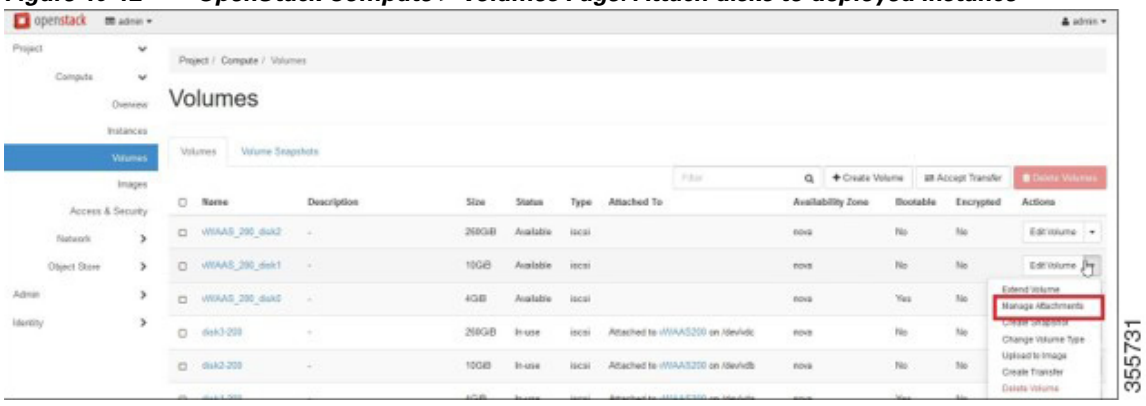


a. Specify resource metadata by selecting and moving items from the Available Metadata column into the Existing Metadata column.

Step 12 Attach disks to the deployed instance.

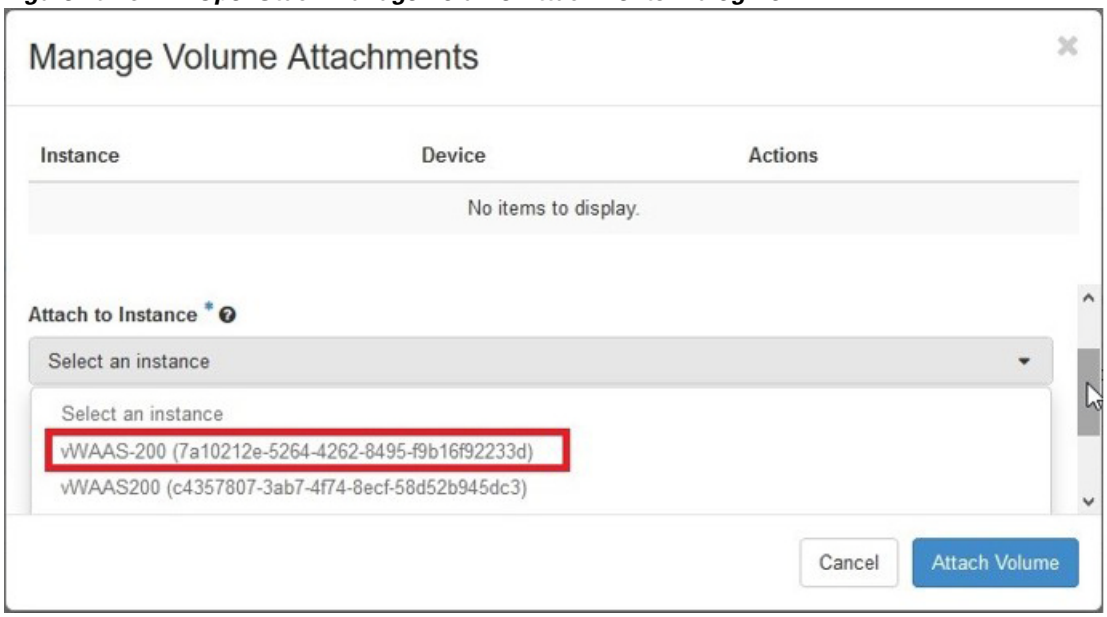
From the OpenStack Admin tab, open the Compute > Volumes page (Figure 10-12).

Figure 10-12 OpenStack Compute > Volumes Page: Attach disks to deployed instance



a. From the **Edit Volume** drop-down list, choose **Manage Attachments**. The Manage Volume Attachments dialog box appears (Figure 10-13).

Figure 10-13 OpenStack Manage Volume Attachments Dialog Box

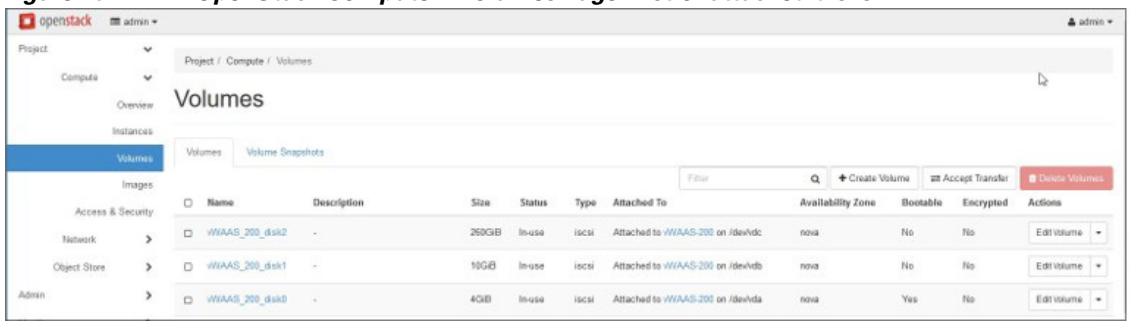


b. From the **Select an instance** drop-down list, choose the instance to attach to the disk.

c. Click **Attach Volume**.

Step 13 After attaching the disks, the Compute > Volumes page displays the attached disks (Figure 10-14).

Figure 10-14 OpenStack Compute > Volumes Page: List of attached disks



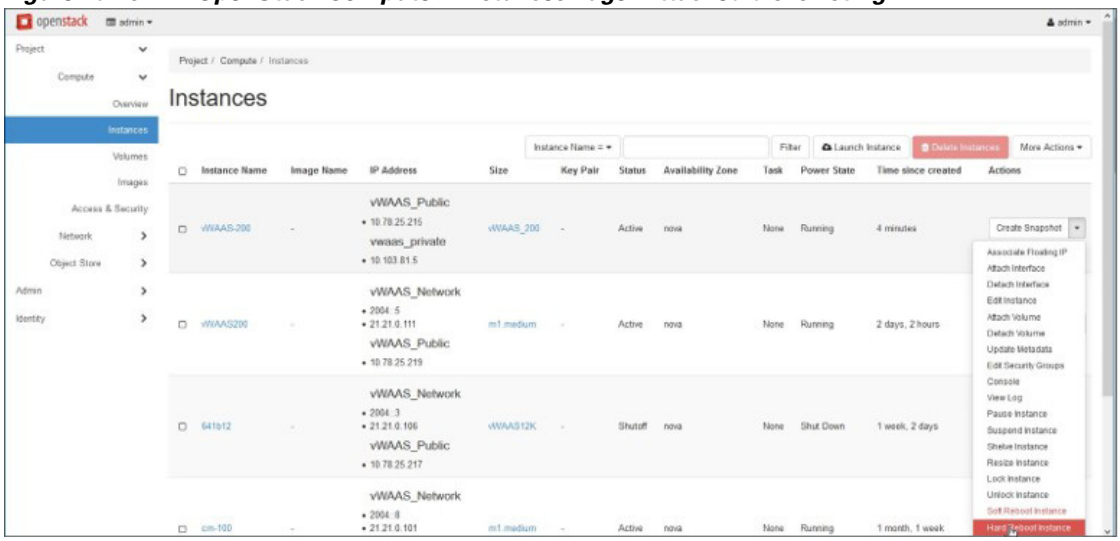
Step 14 Reboot the system (hard reboot).

a. After the system is rebooted, navigate to the Compute > Instances page.

b. From the **Create Snapshot** drop-down list, choose **Hard Reboot Instance**.

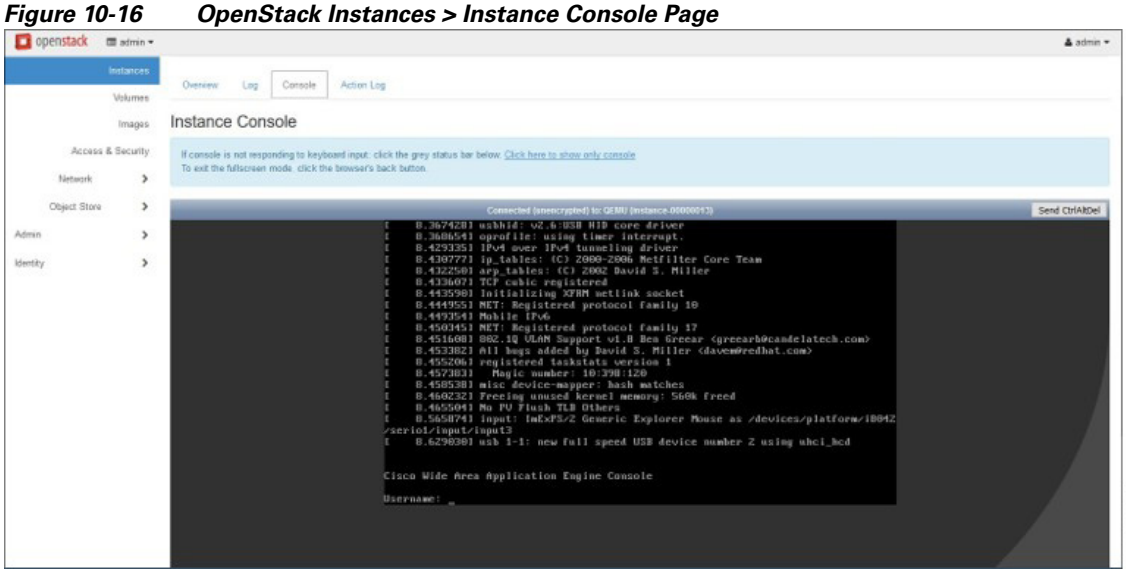
c. The Compute > Instances page displays the attached disks (Figure 10-15).

Figure 10-15 OpenStack Compute > Instances Page: Attached disks listing



Step 15 From the Instances > Instance Console page, connect to the console to work on vWAAS (Figure 10-16).

Figure 10-16 OpenStack Instances > Instance Console Page



Troubleshooting Cisco vWAAS

This chapter describes how to identify and resolve operating issues with Cisco vWAAS.

This chapter contains the following sections:

Resolving Diskless Startup and Disk Failure

Under rare conditions, the vWAAS VM may boot into diskless mode if other VMs on the host VM server do not release control of system resources or the physical disks become unresponsive. The vWAAS device raises a **disk_failure** critical alarm for disk01 and the **show disk details** EXEC command shows disk01 as Not used until replaced.

To recover from this failure, follow these steps:

Step 1 Re-enable the disk.

```
vwaas# config
vwaas(config)# no disk disk-name disk00 shutdown force
vwaas(config)# exit
```

Step 2 Reload vWAAS.

```
vwaas# reload
```

Troubleshooting vWAAS Device Registration

You must register each vWAAS device with the WAAS CM. If a vWAAS device is not registered with the WAAS CM, the **Not registered alarm** is displayed when you use the **show alarms** command.

Figure 11-1 Display for show alarms Command: Not Registered Alarm

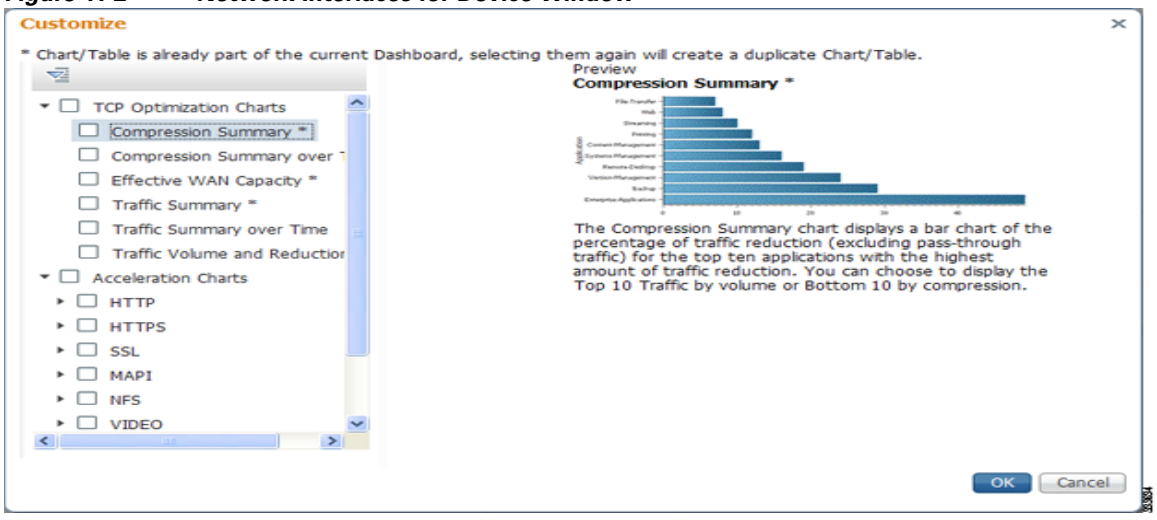
```
vWAAS# show alarms

Critical alarms:
----------------
None

Major alarms:
-------------
        Alarm ID          Module/Submodule        Instance
     -----------------    -----------------    --------------
     1 not registered       vwaas/model          vwaas/model   <----- Not registered alarm
. . .

Minor alarms:
-------------
None
```

Verifying vWAAS Virtual Interfaces

Two virtual interfaces are available on vWAAS devices, the WAAS CM and the CLI:

To show vWAAS virtual interfaces on the WAAS CM, choose ***Device*** **> Configure > Network > Network Interfaces** to display the screen shown in Figure 11-2.

Figure 11-2 Network Interfaces for Device Window



For the CLI, use the **show running-config interface** command to display the virtual interfaces. For additional details on the virtual interfaces, use the **show interface virtual 1/0** command or the **show interface virtual 2/0** command.

Troubleshooting vWAAS Networking

If you see no connections on the vWAAS device, use VMware VSphere Client to view the networking configuration and to check if the vWAAS device is connected to the correct vSwitch.

To use the VSphere Client to trace vWAAS connectivity from the device page, follow these steps:

Step 1 Identify which network label the network adapter is connected to.

Step 2 Determine the virtual switch that this network is connected to.

Step 3 Determine the physical NIC that is a member of this virtual switch.

Step 4 Verify that the configuration is correct.

Step 5 Verify that the virtual switch settings are correctly configured to reach the network.

Step 6 Verify the following on the vWAAS device: configured IP address, netmask, default gateway, and primary interface. For more information on these parameters, see Verifying vWAAS Virtual Interfaces.

Step 7 From the vWAAS device, ping the default gateway and WAAS CM to verify that they are reachable.

Troubleshooting Undersized Alarm

If the proper memory and hard disk resources are not allocated to the vWAAS device, the Undersized alarm is displayed when you use the **show alarms** command. Figure 11-3 shows sample output for the **show alarms** command for the Undersized alarm.

Figure 11-3 Sample Output for show alarms Command: Undersized Alarm

```
vWAAS# show alarms

Critical alarms:
----------------
None

Major alarms:
-------------
       Alarm ID          Module/Submodule        Instance
     -------------       ----------------      --------------
     1 undersized          vwaas/model           memory         <----- Undersized alarm
. . .

Minor alarms:
-------------
None
```

Table 11-1 describes the fields in the **show alarms** command output.

Table 11-1 Field Descriptions for the show alarms Command

Field	Description
Critical Alarms	Critical alarms affect the existing traffic through the WAE and are considered fatal (the WAE cannot recover and continue to process traffic. **Note** WAAS and vWAAS provide three levels of alarms: critical, major, and minor. For more information on alarms and the **show alarms** command, see the *Cisco Wide Area Application Services Command Reference*.
Major Alarms	Major alarms indicate a major service (such as the cache service) has been damaged or lost. Urgent action is necessary to restore this service. However, other node components are fully functional and the existing service should be minimally impacted. **Note** WAAS and vWAAS provide three levels of alarms: critical, major, and minor. For more information on alarms and the **show alarms** command, see the *Cisco Wide Area Application Services Command Reference*.
Alarm ID	Type of event that caused the alarm.
Module/Submodule	The software module affected.
Instance	The object that this alarm is associated with. As shown in Figure 11-3, the instance for this alarm is *memory*. The Instance field does not have predefined values; each Instance value is application specific.

You will not see this alarm if you are using valid OVA files to deploy vWAAS. If the alarm shown in x is displayed, delete the vWAAS VM and redeploy the vWAAS VM using a valid OVA file.