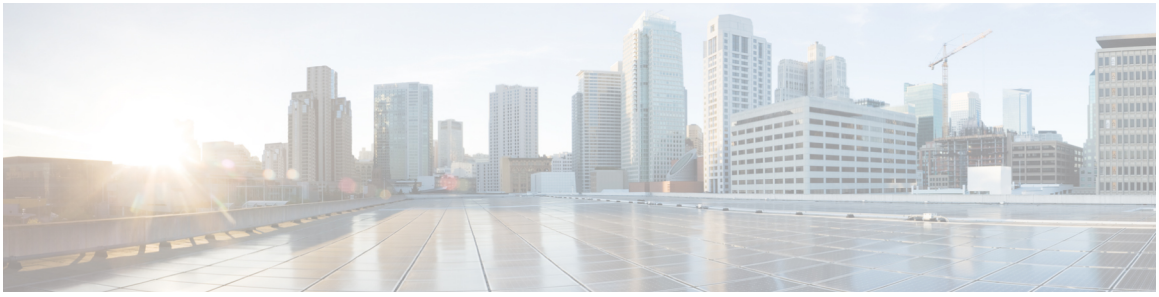
Cisco vWAAS Configuration Guide (for WAAS Version 6.4.5x)

Last Modified: 2020-09-17

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



CONTENTS

Preface

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

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 (Cisco vWAAS) in Cisco WAAS.

You should be familiar with the basic concepts and terminology used in internetworking, and understand your network topology and the protocols that the devices in your network can use. You should also have a working knowledge of the operating systems on which you are running your Cisco WAAS network, such as Microsoft Windows, Linux, or Solaris, and hypervisors used with Cisco vWAAS, such as VMware ESXi or RHEL KVM.

Document Organization

This guide is organized as follows:

Table 1:

Chapter	Chapter Title	Description
Chapter 1	Introduction to Cisco vWAAS	Overview of the Cisco 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.
Chapter 2	Configuring Cisco vWAAS and Viewing Cisco vWAAS Components	How to configure Cisco vWAAS settings, such as Cisco WAAS Central Manager address and traffic interception settings, and how to identify a vWAAS on the Cisco WAAS Central Manager or through the WAAS CLI.
Chapter 3	Cisco vWAAS on Cisco ISR-WAAS	How to use Cisco vWAAS on Cisco ISR-WAAS.
Chapter 4	Cisco vWAAS on VMware ESXi	How to use Cisco vWAAS on VMware ESXi.
Chapter 5	Cisco vWAAS on Microsoft Hyper-V	How to use Cisco vWAAS on Microsoft Hyper-V.
Chapter 6	Cisco vWAAS on RHEL KVM, KVM on CentOS, and KVM in SUSE Linux	How to use Cisco vWAAS on RHEL KVM, KVM on CentOS, and KVM in SUSE Linux.
Chapter 7	Cisco vWAAS on Cisco ENCS 5400-W Series	How to use Cisco vWAAS on the Cisco Enterprise Network Compute System 5400-W Series (Cisco ENCS 5400-W Series) appliance
Chapter 8	Cisco vWAAS on Cisco CSP 5000-W Series	How to use Cisco vWAAS on the Cisco Cloud Services Platform, 5000-W Series (Cisco CSP 5000-W Series) appliance.
Chapter 9	Cisco vWAAS with Cisco Enterprise NFVIS	How to use Cisco vWAAS with Cisco Enterprise Network Functions Virtualization Infrastructure Software (Cisco Enterprise NFVIS).
Chapter 10	Cisco vWAAS with Akamai Connect	Overview of Cisco vWAAS with Akamai Connect, and describes hardware requirements for Cisco vWAAS with Akamai Connect, including how to upgrade Cisco vWAAS memory and disk for the Akamai cache engine.
Chapter 11	Cisco vWAAS in Cloud Computing Systems	How to use Cisco vWAAS in the Microsoft Azure and OpenStack cloud computing systems.
Chapter 12	Troubleshooting Cisco vWAAS	How to identify and resolve operating issues with Cisco vWAAS, and contains the following sections

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.

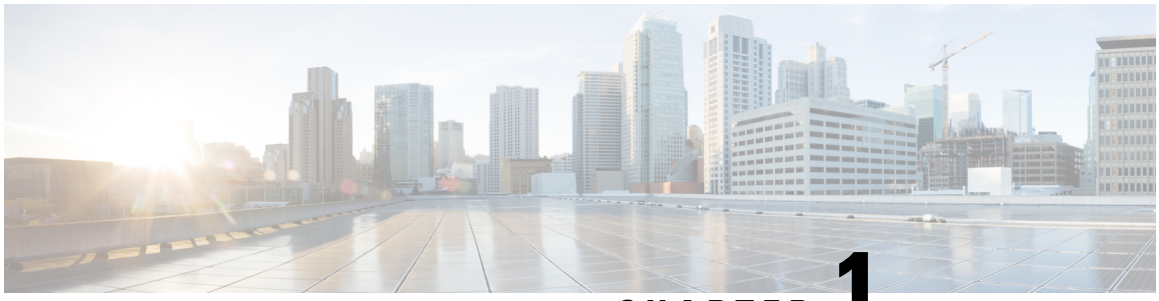
Tip Means the following information will help you solve a problem. Tips might not be troubleshooting or even an action, but could help you save time.

Related Documentation

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

- Release Note for Cisco Wide Area Application Services
- Cisco Wide Area Application Services Configuration Guide

- Cisco Wide Area Application Services Upgrade Guide
- Cisco Wide Area Application Services Command Reference
- Cisco Wide Area Application Services Quick Configuration Guide
- Cisco Wide Area Application Services API Reference
- Cisco Wide Area Application Services Monitoring Guide
- Configuring WAAS Express
- Configuring Cisco WAAS Network Modules for Cisco Access Routers
- WAAS Enhanced Network Modules
- Regulatory Compliance and Safety Information for the Cisco Wide Area Virtualization Engines
- Regulatory Compliance and Safety Information for the Cisco Content Networking Product Series



CHAPTER 1

Introduction to Cisco vWAAS

This chapter provides an overview of the Cisco Virtual Wide Area Applications Services (Cisco 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 vWAAS is a virtual appliance, for both enterprises and service providers, which 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 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 the 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.

Cisco Integrated Services Router-Cisco Wide Area Application Services (Cisco ISR-Cisco 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, or ISR-4461). In this context, **container** refers to the hypervisor that runs virtualized applications on a Cisco ISR 4000 Series router.

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

The following table shows the hypervisors supported for Cisco vWAAS. For more information on each of these hypervisors, see Hypervisors Supported for Cisco vWAAS and vCM, on page 34 in this chapter, and in the chapters listed in the following table.

Table 2: Hypervisors Supported for Cisco vWAAS

Hypervisor	For More Information:
Cisco ISR-WAAS	See the chapter "Cisco vWAAS on Cisco ISR-WAAS, on page 59."
VMware vSphere ESXi	See the chapter "Cisco vWAAS on VMware ESXi, on page 63."
Microsoft HyperV	See the chapter "Cisco vWAAS on Microsoft Hyper-V, on page 87."
RHEL KVM	See the chapter "Cisco vWAAS on RHEL KVM, KVM on CentOS, and KVM in SUSE Linux, on page 103."
KVM on CentOS	See the chapter "Cisco vWAAS on RHEL KVM, KVM on CentOS, and KVM in SUSE Linux, on page 103."
KVM in SUSE Linux	See the chapter "Cisco vWAAS on RHEL KVM, KVM on CentOS, and KVM in SUSE Linux, on page 103."
Cisco Enterprise NFVIS	See the chapter "Cisco vWAAS with Cisco Enterprise NFVIS, on page 149."

Cisco vWAAS supports WAN optimization in a cloud environment where Cisco physical WAN Automation Engine (Cisco WAE) devices cannot usually be deployed. Virtualization also provides various benefits such as 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 Cisco vWAAS.

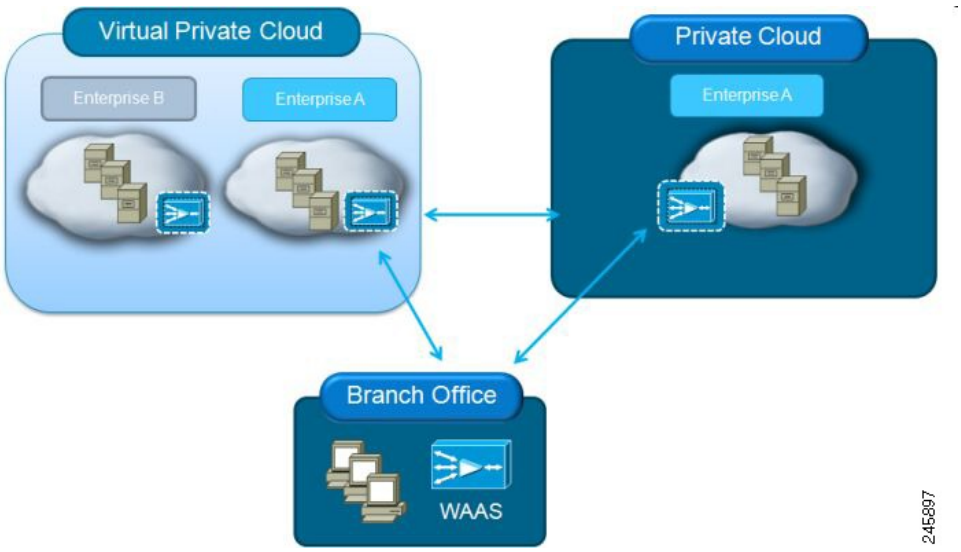
- Cisco Unified Computing System (UCS)
- Cisco UCS E-Series Servers
- Cisco UCS E-Series Network Compute Engines (NCEs)
- Cisco ISR-4000 Series
- Cisco ENCS 5400 Series
- Microsoft Azure Cloud

For details on the interoperability of the hypervisors and platforms supported for vWAAS, see Platforms Supported for Cisco vWAAS, by Hypervisor Type.

As shown in the following figure, 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.

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



Cisco 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.

Cisco vWAAS and WAAS Interoperability

Consider the following guidelines when using Cisco vWAAS with WAAS:

- **For Cisco vWAAS in Cisco WAAS Version 6.1.x and later**: The Cisco vWAAS and Cisco vCM devices require both virtual (network) interfaces to be present, but both need not be active. If only one virtual interface is active, the Cisco vWAAS and Cisco vCM devices will not be operational after power up.
- **Cisco WAAS Central Manager interoperability**: In a mixed-version Cisco WAAS network, the Cisco WAAS Central Manager must be running the latest 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 another 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.

OVA Package Files for Cisco vWAAS and vCM Models

The following table shows the OVA and NPE OVA file for each Cisco vWAAS model:

Table 3: OVA Package Files for Cisco 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

The following table shows the OVA and NPE OVA file for each Cisco vCM model (all models are available with Cisco WAAS Version 4.3.1 and later, except as noted):

Table 4: OVA Package Files for Cisco 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 vWAAS Models: CPUs, Memory, and Disk Storage

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

- When using Cisco vWAAS in Cisco WAAS Version 6.4.x or later, we recommend that you select **vWAAS Re-sized** during installation.
- When Cisco vWAAS-6000, vWAAS-1300, vWAAS-12000, or vWAAS-50000 are used with Akamai Connect and when connections are more than 70 percent of Transport Flow Optimization (TFO), the response time will be on the higher side. Adding CPUs to these models when used with Akamai Connect may improve response time.

- The following table shows where to find additional memory and disk storage information for Akamai Connect and Cisco ENCS 5400-W, by Cisco vWAAS model.

Table 5: Cisco vWAAS Memory and Disk Storage, Akamai Connect and Cisco ENCS 5400-W

Cisco vWAAS Model	For more information
vWAAS-150	• See Cisco vWAAS-150 with Akamai Connect in the chapter "Cisco vWAAS with Akamai Connect."
vWAAS-6000R	• See the chapter "Cisco vWAAS on Cisco ENCS 5400-W Series." • See *Cisco vWAAS Bundled Image Upgrade for ENCS 5400 Series, with RMA Process for Cisco EOS/EOL WAVE Devices*.
vWAAS-12000 and vWAAS-50000	• See Akamai Connect Cache Engine on Cisco Mid-End and High-End Platforms, on page 166 in the chapter "Cisco vWAAS with Akamai Connect."
vWAAS models with Akamai Connect	• See Cisco vWAAS with Akamai Connect Hardware Requirements, on page 160 in the chapter "Cisco vWAAS with Akamai Connect."
vWAAS models on Cisco ENCS 5400 Series	• See the chapter "Cisco vWAAS on Cisco ENCS 5400-W Series." • See *Cisco vWAAS Bundled Image Upgrade for ENCS 5400 Series, with RMA Process for Cisco EOS/EOL WAVE Devices*.

VMware VMFS Block Size and vWAAS Disk Size

The following table shows the VMware Virtual Machine File System (VMware VMFS) block size and associated Cisco vWAAS maximum disk file size.

Table 6: VMware VMFS Block Size and Cisco 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 Cisco vWAAS models that have a disk size that is larger than 256 GB, a VMFS block size that is larger than 1 MB is required.

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

The following table shows the number of managed nodes and disk storage for each Cisco vCM model, as well as the required and recommended number of vCPUs and the required and recommended memory capacity.

Note Cisco vCM 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 Cisco WAAS Central Manager service can experience intermittent restarts or flapping: device states when under resource shortage. To remedy this, configure the recommended values for number of CPUs and memory, as shown in the following table.

Table 7: Cisco 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

Cisco vWAAS and vCM Sizing Guidelines for Cisco WAAS Version 6.4.3x and Later

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 this section.

Cisco vCM on VMware ESXi Sizing Guidelines

This section contains the following Cisco vCM on VMware ESXi sizing guidelines tables:

The following table shows Cisco vCM on VMware ESXi sizing guidelines for Central Manager Mode.

Note In the **Number of Nodes (Cisco WAAS and Other Devices)** column in the following table: In cases when the Cisco WAAS Central Manager manages Cisco WAAS devices, the total number of managed devices can be reduced by 20% compared to management of only Cisco WAAS devices.

Table 8: Cisco vCM on VMware ESXI Sizing Guidelines: Central Manager Mode

Cisco vCM Model	Number of Nodes (Cisco WAAS Devices Only)	Number of Nodes (Cisco WAAS and Other Devices)	Number of Managed Appnav Clusters
vCM-100	100	80	25
vCM-500N	500	500	125
vCM-1000N	1000	1000	250
vCM-2000N	2000	2000	300

The following table shows Cisco vCM on VMware ESXi sizing guidelines for virtual hardware requirements.

Table 9: Cisco vCM on VMware ESXi: Virtual Hardware Requirements

Cisco vCM Model	Required Number of vCPUs	Recommended Number of vCPUs	Required Virtual Memory	Recommended Virtual Memory	Number of Virtual Disks	Virtual Disk Datastore
vCM-100	2	2	2	3	2	254
vCM-500N	2	4	2	5	2	304
vCM-1000N	2	6	4	8	2	404
vCM-2000N	4	8	8	16	2	604

The following table shows Cisco vCM on VMware ESXi sizing guidelines for hardware requirements.

Table 10: Cisco vCM on VMware ESXi: Hardware Requirements

Cisco vCM Model	Cisco Hardware	CPU Clock Speed	Disk
vCM-100	UCS C210 M2	2.6 GHz	HDD-7.2K RPM
vCM-500N	UCS C210 M2	2.6 GHz	HDD-7.2K RPM
vCM-1000N	UCS C210 M2	2.6 GHz	HDD-7.2K RPM
vCM-2000N	UCS C210 M2	2.6 GHz	HDD-7.2K RPM

Cisco vWAAS on Microsoft Hyper-V Sizing Guidelines

This section contains the following Cisco vWAAS on Microsoft Hyper-V sizing guidelines tables:

The following table shows Cisco vWAAS on Microsoft Hyper-V sizing guidelines for connections.

Table 11: Cisco vWAAS on Microsoft Hyper-V: Connections Sizing Guidelines

Cisco vWAAS Model	Optimized TCP Connections	Optimized CIFS/SMB Connections	Optimized SSL Connections	Optimized MAPI Connections	Optimized EMAPI Connections	Akamai Connect Optimized TCP Connections
vWAAS-150	150	150	150	45	45	150
vWAAS-200	200	200	200	60	60	200
vWAAS-750	750	750	750	225	225	750
vWAAS-1300	1,300	1,300	1,300	390	390	1,300
vWAAS-2500	2,500	2,500	2,500	750	750	2,500
vWAAS-6000	6,000	6,000	6,000	1,800	1,800	6,000
vWAAS-12000	12,000	12,000	12,000	3,600	3,600	12,000
vWAAS-50000	50,000	50,000	50,000	15,500	15,500	50,000

Consider the following guidelines for connections sizing for Cisco vWAAS on Microsoft Hyper-V, as shown in the above table.

- For the **Optimized TCP Connections** column: Any system will optimize up to the maximum of its capacity until overload conditions arise. During overload conditions, new connections will not be optimized. Existing connections will be optimized to the greatest degree possible by the system. Should you need scalability beyond the capacity of a single device, multiple devices can be deployed.
- For the **Optimized SSL Connections** column: These connections, when used, are part of the overall connection limit for the device.
- For the **Optimized MAPI Connections** and **Optimized EMAPI Connections** columns: MAPI/EMAPI numbers represent the number of concurrent clients.
- For the **Akamai Connect Optimized TCP Connections** column:
  - Any system will optimize up to the maximum of its capacity until overload conditions arise. During overload conditions, new connections will not be optimized.Existing connections will be optimized to the greatest degree possible by the system. Should you need scalability beyond the capacity of a single device, multiple devices can be deployed.
  - Connections per second (CPS) is approximately 20% of the TFO limit. If the CPS exceeds this some traffic will end up in pass through and not optimized.

The following table shows Cisco vWAAS on Microsoft Hyper-V sizing guidelines for bandwidth, throughput, disk, and cache sizing.

Table 12: Cisco vWAAS on Microsoft Hyper-V: Bandwidth, Throughput, Disk, and Cache Sizing Guidelines

Cisco vWAAS Model	Target WAN Bandwidth	Optimized LAN Throughput	DRE Disk Capacity	Default SMB AO Object Cache Capacity	Default Akamai Connect Cache Capacity	Akamai Connect Target WAN Bandwidth
vWAAS-150	15 Mbps	75 Mbps	52 GB	–-	80 GB	–-
vWAAS-200	20 Mbps	300 Mbps	50 GB	72 GB	100 GB	–-
vWAAS-750	50 Mbps	500 Mbps	95 GB	108 GB	250 GB	–-
vWAAS-1300	80 Mbps	500 Mbps	140 GB	108 GB	300 GB	–-
vWAAS-2500	150 Mbps	750 Mbps	230 GB	108 GB	350 GB	–-
vWAAS-6000	150 Mbps	800 Mbps	320 GB	108 GB	350 GB	–-
vWAAS-12000	310 Mbps	1,600 Mbps	450 GB	202 GB	750 GB	–-
vWAAS-50000	380 Mbps	2,000 Mbps	1,000 GB	203 GB	850 GB	–-

Consider the following guidelines for bandwidth, throughput, DRE disk, object cache, and Akamai Connect sizing for Cisco vWAAS on Microsoft Hyper-V, as shown in the above table.

- For the **Target WAN Bandwidth** column: Target WAN bandwidth is not limited in software or by any other system limit, but is rather provided as guidance for deployment sizing purposes. Target WAN bandwidth is a measure of the optimized/compressed throughput WAAS can support, this value is taken at approximately 50 to 70% compression.
- For the Optimized LAN Throughput column: Maximum LAN Throughput is the theoretical maximum throughput the WAAS device can deliver on the LAN side. This number is measured at 99% compression in a dual-sided scenario with TFO, DRE, or LZ and no WAN condition between the WAAS devices.

Note Your specific results are highly dependent on the type of traffic, compression values, WAN conditions, and how much and the type of "work" the WAAS device is doing (such as TFO, DRE, LZ, AO).

Also, if you are using an appliance with a 2- or 4-port port-channel, or a 10 G port, it is possible to scale beyond 1 Gbps of throughput. The same is true for Cisco vWAAS if you have a 10 G NIC in your ESXi or Hyper-V host, you can scale beyond 1 Gbps. Actual results depend on the use case.

- For the **Default SMB AO Object Cache Capacity** column: SMB Object cache is not available on the Cisco vWAAS-150 and 200 models in Cisco WAAS Version 6.2.1. However the space is there to be reallocated toward Akamai Connect if desired.

- For the **Default Akamai Connect Cache Capacity** column: The SMB Object Cache and Akamai Connect Cache can be modified to skew toward SMB, Akamai, or a 50/50 split. For more information, see the Cisco WAAS information on resizing Cisco vWAAS on NFVIS, see the *Cisco Wide Area Application Services Configuration Guide*.
- For the **Akamai Connect Target WAN Bandwidth** column:
  - Target WAN bandwidth is not limited in software or by any other system limit, but is rather provided as guidance for deployment sizing purposes. Target WAN bandwidth is a measure of the optimized/compressed throughput WAAS can support, this value is taken at approximately 50 - 70% compression.
  - Akamai Connect for Cisco vWAAS-1300:

    - **Hardware**: Cisco UCS-EN120S-M2/K9

    - **CPU Clock Speed**: 1.799 GHz

    - **Disk Type**: SATA and selected platform test coverage

The following table shows Cisco vWAAS on Microsoft Hyper-V sizing guidelines for virtual hardware requirements.

Table 13: Cisco vWAAS on Microsoft Hyper-V: Virtual Hardware Requirements

Cisco vWAAS Model	Number of vCPUs	Virtual Memory	Number of Virtual Disks	Virtual Disk Datastore
vWAAS-150	1	3 GB	3	168 GB
vWAAS-200	1	3 GB	4	267.2 GB
vWAAS-750	2	4 GB	4	508.2 GB
vWAAS-1300	2	6 GB	4	610.2 GB
vWAAS-2500	4	8 GB	4	762.2 GB
vWAAS-6000	4	11 GB	4	915 GB
vWAAS-12000	4	12 GB	3	766.2 GB
vWAAS-50000	8	48 GB	3	1,552 GB

The following table shows Cisco vWAAS on Microsoft Hyper-V sizing guidelines for hardware requirements.

Table 14: Cisco vWAAS on Microsoft Hyper-V: Hardware Requirements

Cisco vWAAS Model	Cisco Hardware	CPU Clock Speed	Disk	Interface
vWAAS-150	ISR-4321 and UCS-EN140N-M2/K9	1.7 GHz	SSD	1 GE
vWAAS-200	ISR-3945E and UCS-E140S-M2/K9	1.8 GHz	HDD -7.2K RPM	1 GE

Cisco vWAAS Model	Cisco Hardware	CPU Clock Speed	Disk	Interface
vWAAS-750	ISR-3945E and UCS-E140S-M2/K9	1.8 GHz	HDD -7.2K RPM	1 GE
vWAAS-1300	ISR-3945E and UCS-E140S-M2/K9	1.8 GHz	HDD -7.2K RPM	1 GE
vWAAS-2500	ISR-4451 and UCS-E140S-M2/K9	1.8 GHz	HDD -7.2K RPM	1 GE
vWAAS-6000	ISR-4451 and UCS-E140S-M2/K9	1.8 GHz	HDD -7.2K RPM	1 GE
vWAAS-12000	UCSC-C240-M3S	3.5 GHz	HDD -7.2K RPM	10 GE
vWAAS-50000	UCSC-C240-M3S	3.5 GHz	HDD -7.2K RPM	10 GE

Cisco vCM on RHEL KVM Sizing Guidelines

This section contains the following tables:

- Cisco vCM on RHEL KVM Sizing Guidelines: Central Manager Mode
- Cisco vCM on RHEL KVM Sizing Guidelines: Virtual Hardware Requirements
- Cisco vCM on RHEL KVM Sizing Guidelines: Hardware Requirements

The following table show sizing guidelines for Cisco vCM in Central Manager Mode.

Table 15: Cisco vCM on RHEL KVM Sizing Guidelines: Central Manager Mode

Cisco vCM Model	Number of Nodes (Cisco WAAS Devices Only)	Number of Nodes (Cisco WAAS and Other Devices)	Number of Managed Cisco AppNav Clusters
vCM-100	100	80	25
vCM-500N	500	500	125
vCM-1000N	1000	1000	250
vCM-2000N	2000	2000	300

Note In the above table, the **Number of Nodes (WAAS and Other Devices)** column: In cases when the Cisco WAAS Central Manager manages Cisco WAAS devices the total number of managed devices can be reduced by 20% compared to management of only Cisco WAAS devices.

The following table shows virtual hardware requirements sizing guidelines for Cisco vCM on ESXi.

Table 16: Cisco vCM on RHEL KVM Sizing Guidelines: Virtual Hardware Requirements

Cisco vCM Model	Required Number of vCPUs	Recommended Number of vCPUs	Required Virtual Memory	Recommended Virtual Memory	Number of Virtual Disks	Virtual Disk Datastore
vCM-100	2	2	2 GB	3 GB	3	250 GB
vCM-500N	2	4	2 GB	5 GB	3	300 GB
vCM-1000N	2	6	4 GB	8 GB	3	400 GB
vCM-2000N	4	8	8 GB	16 GB	3	600 GB

Table 17: Cisco vCM on RHEL KVM Sizing Guidelines: Hardware Requirements

Cisco vCM Model	Cisco Hardware	CPU Clock Speed	Disk
vCM-100	UCS C210 M2	2.6 GHz	HDD-7.2K RPM
vCM-500N	UCS C210 M2	2.6 GHz	HDD-7.2K RPM
vCM-1000N	UCS C210 M2	2.6 GHz	HDD-7.2K RPM
vCM-2000N	UCS C210 M2	2.6 GHz	HDD-7.2K RPM

Resizing for Cisco vWAAS in WAAS Version 6.4.1a to 6.4.1x

This section contains the following topics:

Cisco vWAAS Resizing Guidelines

Cisco vWAAS in Cisco WAAS Version 6.4.1a and later requires additional resources. Resizing Cisco vWAAS on the recommended platforms enables Cisco vWAAS to scale to optimized TCP connections for the associated device, and to reduce CPU and RAM utilization.

Consider the following guidelines and recommendations for Cisco vWAAS resizing:

- Only vWAAS models can be resized. Cisco ISR-WAAS and Cisco vCM cannot be resized.
- Although optional, we highly recommend that you resize CPU and memory resources for Cisco vWAAS models on all hypervisors. For Cisco vWAAS in Cisco WAAS 6.4.1b and later, options are provided during Cisco vWAAS deployment for you to select either original or resized resources.
- For Cisco vWAAS in Cisco WAAS Version 6.4.1b: You cannot deploy Cisco vWAAS-12000 or Cisco vWAAS-50000 in Microsoft Hyper-V with the original resources. For a successful deployment of Cisco vWAAS 12000 or Cisco 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 Cisco WAAS Version 6.4.1b.
- We recommend the following actions:

- Resize CPU and memory resources, as shown in the table "Resized Cisco vWAAS Specifications for Cisco WAAS Version 6.4.1a and Later" in this section.
- Resize the DRE object cache and Akamai Connect Cache, as shown in the two tables in the section DRE Disk, Object Cache, and Akamai Connect Cache Capacity, on page 20.
- For optimum performance, use the SSD disk with the UCS models listed in the table "Resized Cisco vWAAS Specifications for Cisco WAAS Version 6.4.1a and Later" in this section.

The following table shows original and resized specifications for CPU and memory, by vWAAS model, as well as the tested CPU clock speed and minimum Cisco platform model recommended for each vWAAS model. For default and resized DRE disk capacity, object cache capacity, and Akamai Connect cache capacity, by Cisco vWAAS model, see .

Table 18: Resized Cisco vWAAS Specifications for Cisco WAAS Version 6.4.1a and Later

Cisco vWAAS Model	Original CPU	Resized CPU	Tested CPU Clock Speed	Original Memory	Resized Memory	Minimum Cisco Platform
vWAAS-150 (earliest supported version: WAAS 6.1.x)	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 GB	1.9 GHz	8 GB	16 GB	UCS-E160S-M3
vWAAS-6000	4 CPUs	8 GB	2.0 GHz	11 GB	24 GB	UCS-E180D-M3
vWAAS-6000R (earliest supported version: WAAS 6.4.x)	4 CPUs	8 GB	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-50000	8 CPUs	16 CPUs	2.6 GHz	48 GB	72 GB	UCS-C220 or UCS-C240

Cisco vWAAS Model	Original CPU	Resized CPU	Tested CPU Clock Speed	Original Memory	Resized Memory	Minimum Cisco Platform
vWAAS-150000 (earliest supported version: 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.

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

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

- **Using the Cisco WAAS CLI to Perform an Upgrade with Existing CPU Memory**:

  During the upgrade, if the vCPU and memory resources are undersized, you will be prompted to resize these Cisco vWAAS parameters before the upgrade.

  You can continue the upgrade procedure and retain the existing vWAAS resources.

  Note For Cisco vWAAS in Cisco WAAS 6.4.1a only: After the upgrade, undersized-resource alarms are displayed for vCPU and memory for the vWAAS device. Use the show alarms command to display information about these undersized alarms for the vWAAS model.

- **Using the Cisco WAAS Central Manager to Perform an Upgrade with Existing CPU and Memory**:

  During the upgrade, if the vCPU and memory resources are undersized, informational note is displayed in the Upgrade window, but there will not be a prompt to resize these Cisco vWAAS parameters before the upgrade.

  You can continue the upgrade procedure and retain the existing Cisco vWAAS resources.

  Note For Cisco vWAAS in Cisco WAAS 6.4.1a only: After the upgrade, undersized-resource alarms are listed for vCPU and memory for the Cisco vWAAS device. Use the show alarms command to display information about these undersized alarms for the Cisco vWAAS model.

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

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

- **Using the Cisco WAAS CLI to perform an upgrade with resized CPU and memory**:

  During the upgrade, if the vCPU and memory resources are undersized, you will be prompted to resize these Cisco vWAAS parameters *before* the upgrade. You can then cancel the upgrade procedure, resize the specific resources, and restart the upgrade procedure.

  1. 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: Choose **Edit Settings... > Hardware**.
     - To change settings in Microsoft Hyper-V: Choose **Virtual Machine > Settings... > Hardware**.
     - To change settings in RHEL KVM/CentOS:
       a. Open **Virtual Manager**.
       b. Choose **Virtual Machine > CPUs**.
       c. Choose **Virtual Machine > Memory**.
     - To change settings in Cisco NFVIS, for the Cisco vBranch solution:
       a. Choose **VM Life Cycle > Image Repository > Profiles** and add another profile with: resized CPU, memory, and same disk size.
       b. Choose **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 for Microsoft Azure:
       a. Choose **Deployments > Microsoft Template Overview > Custom Deployment**.
       b. Choose **Home > Virtual Machines > vWAAS Instance > Size**.
  2. Restart the device. With the resized vCPU and memory, the host should have sufficient resources for a successful upgrade.

Note The resources will not change automatically in subsequent upgrades and downgrades of the system change; you must manually change resources as needed for your system.

- **Using the Cisco WAAS Central Manager to perform the upgrade with resized CPU and memory**:

  Consider these guidelines as you perform an upgrade with resized CPU and memory using the Cisco WAAS Central Manager:

  - During the upgrade, if the vCPU and memory resources are undersized, an informational note is displayed on the Upgrade window, but there will not be a prompt to resize these Cisco vWAAS parameters before the upgrade.
  - You cannot cancel the upgrade procedure, in process, from the Cisco WAAS Central Manager. In this scenario, wait until the is complete, change resources as needed, and perform the upgrade.

Note The resources will not change automatically in subsequent upgrades and downgrades of the system change; you must manually change resources as needed for your system.

Resizing Guidelines by Hypervisor for vWAAS in WAAS 6.4.1b and Later

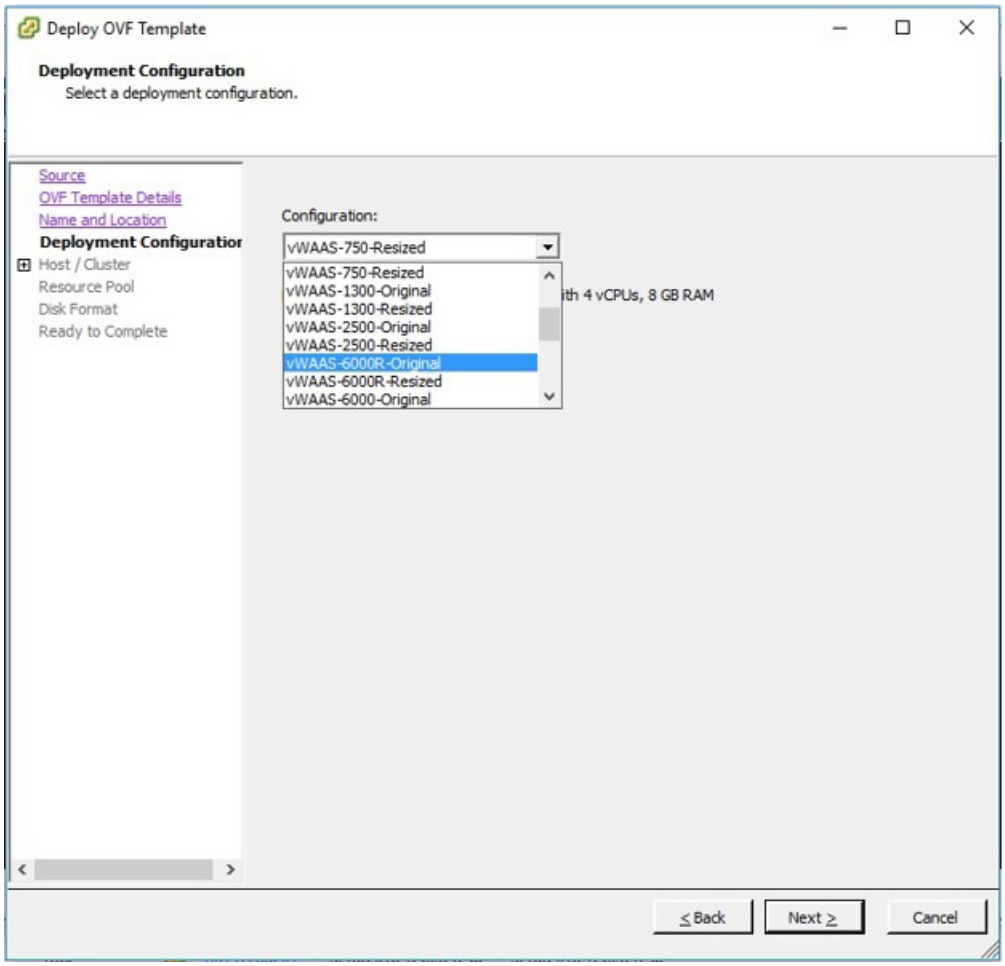
This section contains the following topics:

Resizing for Cisco vWAAS on VMware ESXi

Procedure

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

Figure 2: vSphere Client Deployment Configuration Window



Step 2 From the **Configuration** drop-down list, choose the Cisco vWAAS model for this hypervisor.

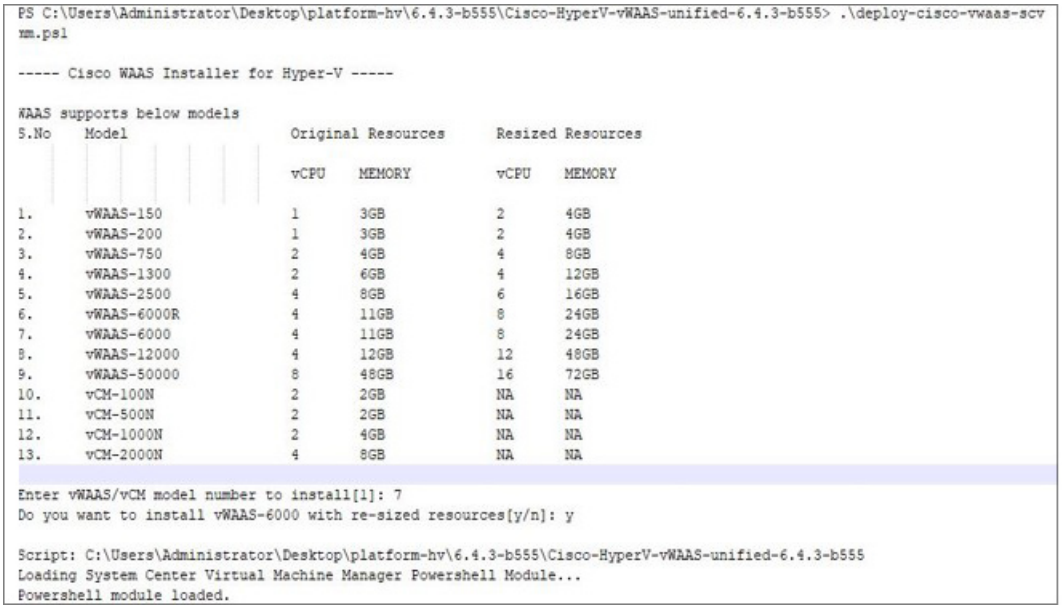
For example, if the model you want to choose is **Cisco vWAAS-6000**, you can either choose **vWAAS-6000-Original** or **vWAAS-6000-Resized**.

Resizing for Cisco vWAAS on Microsoft Hyper-V

Procedure

Step 1 Log in to the Cisco WAAS Installer for Microsoft Hyper-V, which displays a list of supported Cisco WAAS models.

Figure 3: Cisco vWAAS and Cisco vCM Resources for Cisco vWAAS on Hyper-V



Step 2 At the **Enter vWAAS/vCM model to install** prompt, enter the line number for the model that you want to install. For example, from the listing shown in the above figure, if you enter **7**, you will 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 Cisco vWAAS on RHEL CentOS or SUSE Linux

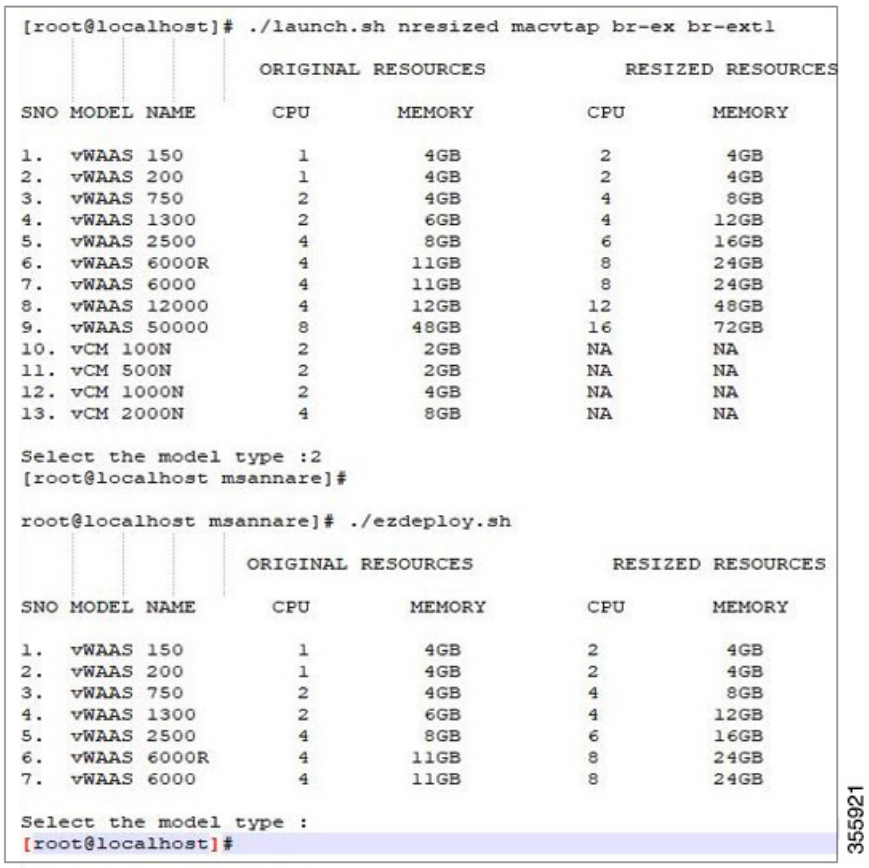
Procedure

Step 1 In the **root@localhost** window, 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 Cisco vWAAS model.

Figure 4: Cisco vWAAS and Cisco vCM Resources on CentOS or SUSE Linux



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

The system displays the following 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 the above figure.

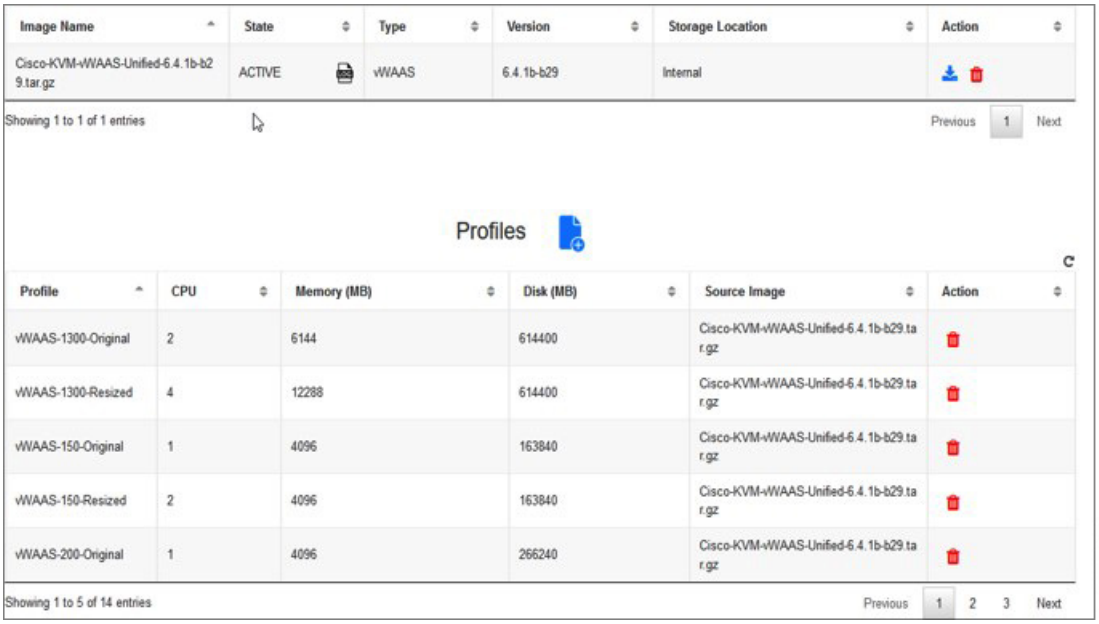
Step 5 The system deploys the selected model, with resized resources.

Resizing for Cisco vWAAS on NFVIS

Procedure

Step 1 To resize Cisco vWAAS on Cisco NFVIS, install the Cisco vWAAS OVA with Cisco WAAS Version 6.4.1b or later. The following figure shows the NFVIS profiles listing for original and resized Cisco vWAAS resources.

Figure 5: Cisco vWAAS Profiles Listing on Cisco vWAAS on NFVIS



Step 2 For more information on resizing Cisco vWAAS on NFVIS, see the *Cisco Enterprise Network Function Virtualization Infrastructure Configuration Guide*.

DRE Disk, Object Cache, and Akamai Connect Cache Capacity

The two tables in this section describe:

- The first table shows default specifications for DRE disk, object cache, and Akamai Connect cache capacity for Cisco WAVE models.
- The second table shows default and resized specifications for DRE disk, object cache, and Akamai Connect cache capacity for Cisco vWAAS models.

Table 19: DRE Disk, Default OC, and Default Akamai Connect Cache by Cisco WAVE Model

Cisco WAVE Model	DRE Disk Capacity	Default Object Cache Capacity	Default Akamai Connect Cache Capacity
WAVE 294-4G	40 GB	102 GB	59 GB

Cisco WAVE Model	DRE Disk Capacity	Default Object Cache Capacity	Default Akamai Connect Cache Capacity
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

Table 20: Default and Resized DRE, OC, and Akamai Connect Cache, by Cisco vWAAS Model

Cisco 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

Cisco Hardware Platforms Supported for Cisco vWAAS

This section contains the following topics:

Platforms Supported for Cisco vWAAS, by Hypervisor Type

For each hypervisor used with Cisco vWAAS, the following table shows the types of platforms supported for Cisco vWAAS, including minimum Cisco WAAS version, host platform, and disk type.

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

Table 21: Platforms Supported for Cisco vWAAS, by Hypervisor Type

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

Earliest Supported Cisco WAAS Version	Host Platforms	Earliest Supported Host Version	Disk Type
• 6.2.x (Cisco UCS-E Series) • 6.4.1 (Cisco ENCS 5400 Series and Cisco)	• Cisco ENCS 5400-W Series • Cisco UCS-E Series	• NFV FC2	• virtio
Hypervisor: **VMware vSphere ESXi** PID: **OE-VWAAS-ESX** and Device Type: **OE-VWAAS-ESX**			
• 5.0.3g	• Cisco UCS • Cisco UCS-E Series	• ESXi 5.0	• VMDK
Hypervisor: **Microsoft Hyper-V** PID: **OE-VWAAS-HYPERV** and Device Type: **OE-VWAAS-HYPERV**			
• 6.1.x	• Cisco UCS • Cisco UCS-E Series	• Microsoft Windows 2008 R2	• VHD
Hypervisor: **RHEL KVM** PID: **OE-VWAAS-KVM** and Device Type: **OE-VWAAS-KVM**			
• 6.2.x	• Cisco UCS • Cisco UCS-E Series	RHEL CentOS 7.1	virtio
Hypervisor: **SUSE Linux** PID: **OE-VWAAS-GEN-LINUX** and Device Type: **OE-VWAAS-GEN-LINUX**			
• 6.4.1b	• Cisco UCS • Cisco UCS-E Series	SUSE Linux Enterprise Server (SLES) 12	virtio
Hypervisor: **Microsoft Azure** PID: **OE-VWAAS-AZURE** and Device Type: **OE-VWAAS-AZURE**			
• 6.2.x	• Microsoft Azure cloud	• N/A	• VHD
Hypervisor: **OpenStack** PID: **OE-VWAAS-OPENSTACK** and Device Type: **OE-VWAAS-OPENSTACK**			
• 6.4.1b	• OpenStack cloud	• OpenStack Mitaka	• virtio

Components for Deploying Cisco vWAAS, by Hypervisor Type

For each hypervisor used with Cisco vWAAS, the following table shows the components used to deploy Cisco vWAAS, including package format, deployment tool, preconfiguration tool (if needed), and network driver.

Table 22: Components for Deploying Cisco 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
Microsoft Azure	• JSON template	• ---	• ---	• netvsc

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

Components for Managing Cisco vWAAS, by Hypervisor Type

For each hypervisor used with Cisco vWAAS, the following table shows the components used to manage Cisco vWAAS, including Cisco vCM model, Cisco vWAAS model, number of instances supported, and traffic interception method used.

Table 23: Components for Managing Cisco 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 • vWAAS-750 • vWAAS-1300 • vWAAS- 2500	• 1	• AppNav-XE

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

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

Hypervisor	vCM Models Supported	vWAAS Models Supported	Number of Instances Supported	Traffic Interception Method
OpenStack	• vCM-100 • vCM-500 • vCM-1000 • vCM-2000	• vWAAS-150 • vWAAS-200 • vWAAS-750 • vWAAS-1300 • vWAAS-2500 • vWAAS-6000 • vWAAS-12000 • vWAAS-50000	• many	• WCCP • APPNav-XE

Cisco UCS E-Series Servers and NCEs

This section contains the following topics:

Cisco vWAAS and Cisco UCS E-Series Interoperability

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

Table 24: Cisco vWAAS and UCS E-Series Interoperability

Supported Operating Systems for Cisco vWAAS	Supported Hypervisors for Cisco vWAAS	Supported Cisco ISR Routers for Cisco vWAAS	Minimum Cisco IOS -XE Version
Cisco UCS E-Series Servers			

Supported Operating Systems for Cisco vWAAS	Supported Hypervisors for Cisco vWAAS	Supported Cisco ISR Routers for Cisco vWAAS	Minimum Cisco IOS -XE Version
• Microsoft Windows Server 2008 R2, 2012, and 2012 R2 • Red Hat Enterprise Linux (RHEL) 7.1 and later • Linux (Community Enterprise Operating System) CentOS 7.1 and later	• Microsoft Hyper-V 2008 R2, 2012, and 2012 R2 • VMware vSphere ESXi 5.5 and 6.0 (vWAAS in WAAS Versions 6.4.3b and earlier) • VMware vSphere ESXi 6.7 (vWAAS in WAAS Version 6.4.3c and later) • RHEL KVM or CentOS 7.1 (vWAAS in WAAS Version 6.4.3b and earlier) • RHEL KVM or CentOS 7.2 (vWAAS in WAAS Version 6.4.3c and later)	• ISR-4331 • ISR-4351 • ISR-4451 • ISR-4461	• 3.10
Cisco UCS E-Series NCEs			

Supported Operating Systems for Cisco vWAAS	Supported Hypervisors for Cisco vWAAS	Supported Cisco ISR Routers for Cisco vWAAS	Minimum Cisco IOS -XE Version
• Microsoft Windows Server 2012 R2	• Microsoft Hyper-V 2012 R2 • VMware vSphere ESXi 5.5 and 6.0 (vWAAS in WAAS Versions 6.4.3b and earlier) • VMware vSphere ESXi 6.7 (vWAAS in WAAS Version 6.4.3c and later) • RHEL KVM or CentOS 7.1 (vWAAS in WAAS Version 6.4.3b and earlier • RHEL KVM or CentOS 7.2 (vWAAS in WAAS Version 6.4.3c and later)	• ISR-4331 • ISR-4351 • ISR-4451 • ISR-4461	• 3.10 (UCS-EN120S) • 3.15.1 (UCS-EN140N)

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

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.

For information on vCPUs, ESXi server datastore memory, and disk space by Cisco vWAAS model and vCM model, see the chapter "Cisco vWAAS on VMware ESXi."

Example 1:

A deployment of vWAAS-750 on the UCS-E140S, using VMware v6.0: Cisco UCS-E140S has a default value of 8 GB memory (which can be expanded to 48 GB).

- Cisco 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.
- You can deploy Cisco vWAAS-750 on the Cisco UCS-E140S without adding additional memory to the Cisco UCS-E140S DRAM.

Example 2:

A deployment of vWAAS-1300 on the UCS-E140S, using VMware v6.0: Cisco UCS-E140S has a default value of 8 GB DRAM, (which can be expanded to 48 GB).

- Cisco vWAAS-1300 requires 6 GB memory + VMware v6.0 requires 2 GB DRAM = 8 GB memory, which equals the memory capacity of UCS-E140S.
- To deploy Cisco vWAAS-1300 on the Cisco UCS-E140S, you must add additional memory to the Cisco UCS-E140S memory.

Note For Cisco vWAAS datastore, you can use either SAN storage or local storage on the VMware ESXi server. NAC Appliance Server (NAS) should only be used in nonproduction scenarios, such as test purposes.

The following table shows memory and disk storage capacity for Cisco UCS E-Servers NCEs.

Table 25: 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: 4 GB Maximum: 16 GB	Up to one 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 one 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

Cisco UCS E-Series Server (E) or NCE (EN)	Memory	Disk Storage
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)	N/A	One of the following mSATA SSD drives: • mSATA SSD drive: 50 GB • mSATA SSD drive: 100 GB • mSATA SSD drive: 200 GB
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: 96 GB	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-W Series

This section contains the following topics:

About the Cisco ENCS 5400 Series

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

The Cisco 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 acting as a server that addresses processing, workload, and storage challenges.

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

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

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

Cisco ENCS 5400-W Series Hardware Features and Specifications

The following table shows specifications that apply to all three Cisco ENCS 5400-W series models. For more information, see the Cisco 5400 Enterprise Network Compute System Data Sheet .

Table 26: Cisco ENCS 5400 Series Features and Specifications

Cisco ENCS 5400-W Feature/Specification	Description
Cisco vWAAS models supported	One of the following configurations: • Cisco ENCS-5406/K9 supports vWAAS 200 and vWAAS-750 • Cisco ENCS-5408/K9 supports vWAAS-1300 • Cisco ENCS-5412/K9 supports vWAAS-2500 and vWAAS-6000-R

Cisco ENCS 5400-W Feature/Specification	Description
CPU	One of the following specifications: • Cisco ENCS-5406/K9: Intel Xeon Processor D-1528 (6 core, 1.9 GHz, and 9 MB cache) • Cisco ENCS-5408/K9: Intel Xeon Processor D-1548 (8 core, 2.0 GHz, and 12 MB cache) • Cisco ENCS-5412/K9: 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: • Cisco ENCS 5406-W: 16 GB • Cisco ENCS-5408-W: 16 GB • Cisco ENCS-5412-W: 32 GB
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	lthough there are two hot-swappable HDD slots, we do not recommend HDD storage for the Cisco ENCS 5400-W Series.
SSD Storage	• No RAID and one 960 GB SSD • RAID-1 and two SSDs (960 GB SSD)

Cisco ENCS 5400-W Feature/Specification	Description
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**

  Cisco ISR-WAAS is the implementation of vWAAS running in a Cisco IOS-XE software container on a Cisco ISR4400 Series router. In this context, **container** refers to a KVM hypervisor that runs virtualized applications on the Cisco ISR-4400 Series router.

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

- **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.

- **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.

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

- **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.

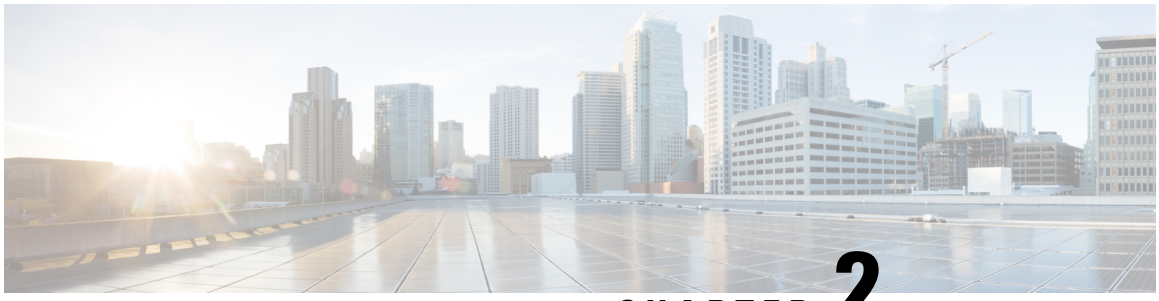
- For vWAAS on WAAS Version 5.x to 6.2.x, Cisco NFVIS is available for vWAAS running on Cisco UCS E-Series Servers.
- For vWAAS on WAAS Version 6.4.1 and later, Cisco NFVIS is available for vWAAS running on Cisco UCS E-Series Servers and the Cisco ENCS 5400 Series.

Cloud Platforms Supported for Cisco vWAAS

Cisco vWAAS supports the following cloud computing platforms:

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

For more information, see the chapter "Cisco vWAAS in Cloud Computing Platforms."



CHAPTER 2

Configuring Cisco vWAAS and Viewing vWAAS Components

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

This chapter contains the following sections:

Configuring Cisco vWAAS Settings

Before you begin

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

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

Procedure

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

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

Example:

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

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

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

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

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

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

Example:

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

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

Example:

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

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

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

Configuring Cisco vWAAS Traffic Interception

You can configure the following traffic interception methods for Cisco vWAAS.

- **WCCP**: Available for Cisco vWAAS in all Cisco WAAS versions.
- **AppNav**: Available for Cisco vWAAS in all Cisco WAAS versions

- **L2 Inline**: Available for Cisco WAAS Version 6.2.x and later, for Cisco vWAAS with RHEL KVM. The following table shows the commands for configuring and displaying information on L2 Inline interception for Cisco vWAAS.

The following table provides descriptions of each traffic interception method.

Table 27: Traffic Interception Methods for Cisco vWAAS

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

The following table shows the commands for configuring and displaying information on L2 Inline interception for Cisco vWAAS.

Table 28: CLI Commands for L2 Inline Traffic Interception

Mode	Command	Description
Global Configuration	**(config) interception-method inline**	Enables L2 inline traffic interception on Cisco vWAAS.
Interface Configuration	**(config-if) cdp**	Enables CDP (Cisco Discovery Protocol) on the interface on a Cisco WAAS device. (To globally enable the CDP interval and holdtime options, run 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 Cisco WAAS device, or negotiates an IP address from DHCP on the interface of a Cisco WAAS device.
	(config-if) ipv6	Configures the IPv6 address on the interface of a Cisco WAAS device, or negotiates an IP address from DHCP on the interface of a Cisco WAAS device.
	(config-if) load-interval	Configures the interval at which to poll the network interface for statistics.
	(config-if) shutdown	Shuts down a specific hardware interface on a Cisco WAAS device, and shuts down the inlinegroup interface to bypass the traffic, and does not optimize the traffic.
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.

Mode	Command	Description
	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 Cisco vWAAS Device

This section describes how to:

- Identify a Cisco vWAAS model.
- Identify a Cisco vWAAS device on the Cisco WAAS Central Manager.
- Identify a Cisco vWAAS device with the Cisco CLI.

To identify a Cisco vWAAS model:

As shown in the following table, a Cisco vWAAS model is determined by the number of vCPUs and the maximum number of TCP connections.

Table 29: Cisco vWAAS Models with vCPUs and Maximum TCP Connections

Cisco 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 supported version: Cisco WAAS Version 6.4.x)	4	6,000
vWAAS-12000	4	12,000
vWAAS-50000	8	50,000

Identifying a Cisco vWAAS device on the Cisco WAAS Central Manager:

There are two windows on the Cisco WAAS Central Manager that show identifying information for a Cisco vWAAS device.

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

The following table shows the displayed Cisco vWAAS device types.

Table 30: Cisco vWAAS Device Types Displayed in Cisco WAAS Central Manager

vWAAS Device	vWAAS Device Type shown in Cisco WAAS Central Manager
vWAAS on Cisco ISR-WAAS	OE-VWAAS-KVM
vWAAS on Cisco NFVIS	OE-VWAAS-KVM
vWAAS on VMware ESXi	OE-VWAAS-ESX
vWAAS on Microsoft Hyper-V	OE-VWAAS-HYPERV
vWAAS on RHEL KVM	OE-VWAAS-KVM
vWAAS on KVM on CentOS	OE-VWAAS-KVM
vWAAS on SUSE Linux	OE-VWAAS-GEN-LINUX
vWAAS in Microsoft Azure	OE-VWAAS-AZURE
vWAAS in OpenStack	OE-VWAAS-OPENSTACK

Identifying a Cisco vWAAS Device with the Cisco WAAS CLI:

The following table shows the commands used to display Cisco vWAAS device information. For more information on these commands, see the *Cisco Wide Area Application Services Command Reference*.

Table 31: CLI Commands for Cisco vWAAS Device Information

Mode	Command	Description
user-level EXEC and privileged-level EXEC	**show version**	Displays version information about the Cisco WAAS software currently running on the Cisco vWAAS device, including date and time system last started, and the length of time the system has been running since the last reboot. • (Optional) Run the **show version last** command to display version information for the last saved image. • (Optional) Run the **show version pending** command to display version information for the pending upgraded image.

Mode	Command	Description
privileged-level EXEC	**show hardware**	Displays system hardware status for the Cisco vWAAS device, including: • Startup date and time, the run time since startup, microprocessor type and speed, and a list of disk drives.
privileged-level EXEC	**show tfo detail**	Displays Transport Flow Optimization (TFO) information, including: • **State**: Registered or Not Registered • **Default Action**: Drop or Use • **Connection Limit**: The maximum TFO connections handled before new connection requests are rejected. • **Effective Limit**: The dynamic limit relating to how many connections are handled before new connection requests are rejected. • **Keepalive Timeout**: The connection keepalive timeout, in seconds.

Cisco vWAAS System Partitions

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

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

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

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

Operating Guidelines for Cisco vWAAS and Cisco WAAS

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

- For Cisco vWAAS in WAAS Version 6.1.x and later, the Cisco vWAAS and Cisco vCM devices require both virtual (network) interfaces to be present, but both need not be active. If only one virtual interface is active, the Cisco vWAAS and Cisco vCM devices will not be operational after power up. For more information, see Configuring Cisco vWAAS Settings, on page 37.
- If the virtual host was created using an OVA file of Cisco vWAAS in Cisco WAAS Version 5.0 or earlier, and you have upgraded Cisco vWAAS in Cisco WAAS, you must verify that the **SCSI Controller Type** is set to **VMware Paravirtual**. Otherwise, Cisco vWAAS 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:

  1. Power down the Cisco vWAAS.
  2. From the **VMware vCenter**, choose **vSphere Client > Edit Settings > Hardware**.
  3. Choose **SCSI controller 0**.
  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**.
  5. Click **OK**.
  6. Power up the Cisco vWAAS, in Cisco WAAS Version 6.1.x or later.

Cisco vWAAS with Single Root I/O Virtualization

This section contains the following topics:

About SR-IOV

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

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

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

The following table shows the two types of functions used with SR-IOV.

Table 32: SR-IOV Physical Functions and Virtual Functions

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

Interoperability and Platforms Supported for Cisco vWAAS with SR-IOV

This section describes the following topics:

- Cisco WAAS Central Manager and Cisco vWAAS with SR-IOV
- Platforms supported for Cisco vWAAS with SR-IOV

Cisco WAAS Central Manager and Cisco vWAAS with SR-IOV:

- Devices with SR-IOV are registered with the Cisco WAAS Central Manager in the same manner as other Cisco vWAAS devices. Run the **cms deregister** EXEC command to deregister these devices as you would for other Cisco vWAAS devices.
- The following list shows how vWAAS devices with SR-IOV are displayed on the Cisco WAAS Central Manager:
  - Cisco vWAAS with SR-IOV on VMware ESXi is displayed as **OE-VWAAS-ESX**.
  - Cisco vWAAS with SR-IOV on KVM (RHEL, CentOS or Cisco NFVIS) is displayed as **OE-VWAAS-KVM**.

Platforms supported for Cisco vWAAS with SR-IOV:

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

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

The following table shows the Cisco WAAS version and platforms supported for Cisco vWAAS with SR-IOV.

Table 33: Cisco WAAS Version and Platforms Supported for Cisco vWAAS with SR-IOV

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

Upgrade and Downgrade Guidelines for Cisco vWAAS with SR-IOV

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

- **Upgrade Guidelines**
  - The upgrade procedure for Cisco vWAAS with SR-IOV is the same as for other vWAAS devices.
- **Downgrade Guidelines**
  - Before a downgrade from Cisco vWAAS in Cisco WAAS Version 6.4.1x or 6.4.3 to an earlier version, from the host, remove those SR-IOV interfaces that do not support this functionality when operating in a Cisco WAAS version earlier than WAAS Version 6.4.1x. Downgrade of Cisco vWAAS instances with SR-IOV is blocked for unsupported WAAS versions.
  - At the device level, if you downgrade a Cisco vWAAS instance with SR-IOV to a version earlier than 6.4.1x or 6.4.3 (depending on your Cisco WAAS configuration), a warning message is displayed

at the start of the downgrade process. This warning message is displayed if the device supports SR-IOV functionality, even if the device does not use the SR-IOV interface, because downgrade of vWAAS instances with SR-IOV is blocked for unsupported Cisco WAAS versions.

- At the device group level, if you downgrade a device group that contains at least one device that supports SR-IOV functionality, a warning message is displayed at the start of the downgrade process, because downgrade of Cisco vWAAS instances with SR-IOV is blocked for unsupported Cisco WAAS versions.

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

Deploying Cisco vWAAS with SR-IOV

This section contains the following topics:

Deploying Cisco vWAAS with SR-IOV on VMware ESXi

This section contains the following topics:

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

Before you begin

Before you begin, note the VMware ESXi host requirements for Cisco vWAAS with SR-IOV on Cisco UCS C-Series:

Table 34: VMware ESXi Requirements for Cisco vWAAS with SR-IOV on Cisco UCS C-Series

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

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

Procedure

Step 1 Log in to the VMware ESXi shell.

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

Step 3 Run this command to create virtual functions:

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

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

Example 1:

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

Example 2:

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

```
[root@localhost:~]
[root@localhost:~] lspci | grep -1 intel | grep -1 'ethernet\|network'
0000:01:00.0 Network controller: Intel Corporation I350 Gigabit Network Connection (vmnic2)
0000:01:00.1 Network controller: Intel Corporation I350 Gigabit Network Connection (vmnic3)
0000:06:00.0 Network controller: Intel Corporation 82599EB 10-Gigabit SFI/SFP+ Network
Connection (vmnic0)
0000:06:00.1 Network controller: Intel Corporation 82599EB 10-Gigabit SFI/SFP+ Network
Connection (vmnic1)
0000:81:00.0 Network controller: Intel Corporation Ethernet Controller X710 for 10GbE
SFP+(vmnic4)
0000:81:00.1 Network controller: Intel Corporation Ethernet Controller X710 for 10GbE
SFP+(vmnic5)
[root@localhost:~]
[root@localhost:~] esxcli system module parameters set -m i40e -p max_vfs=5,0
[root@localhost:~]
```

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

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

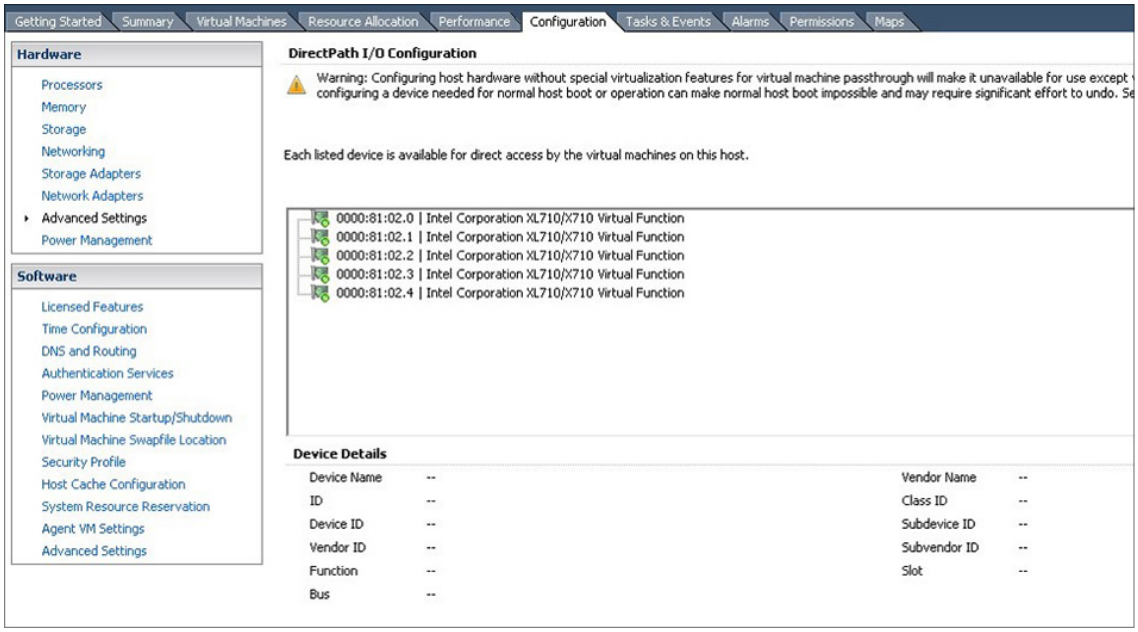
355944

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

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

- Run the VMware ESXi **lspci** command
- Choose **Host > Configuration > Hardware > Advanced Settings** to display the **VMware vSphere Client DirectPath I/O Configuration** window.

Figure 6: VMware vSphere Client DirectPath I/O Configuration Window



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

Procedure

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

Step 2 Power up the vWAAS.

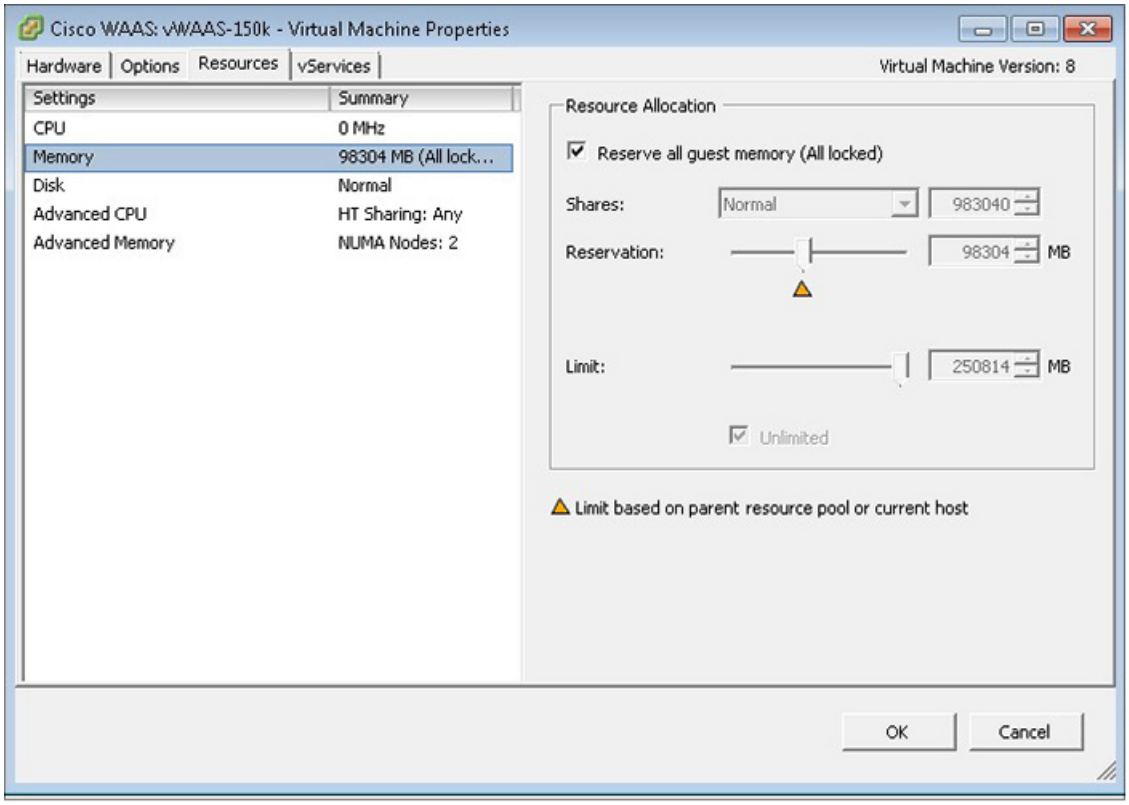
Step 3 Right-click and choose **Edit Settings**.

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

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

The **Resource Allocation** window is displayed.

Figure 7: Cisco vWAAS Resource Allocation Window



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

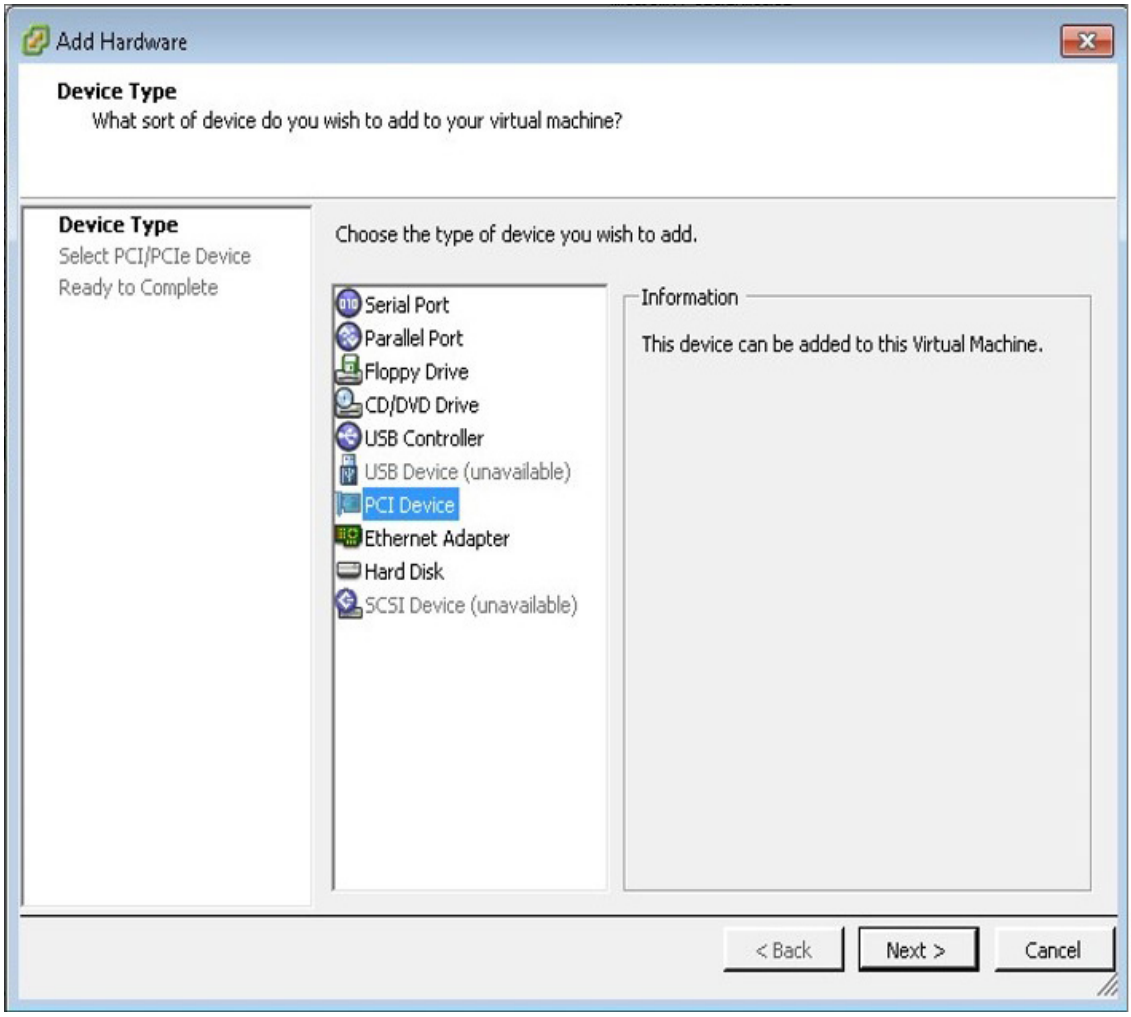
Step 7 Click **OK**.

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

Step 9 Click **Add**.

The **Device Type** window is displayed.

Figure 8: Cisco vWAAS Add Hardware > Device Type Window

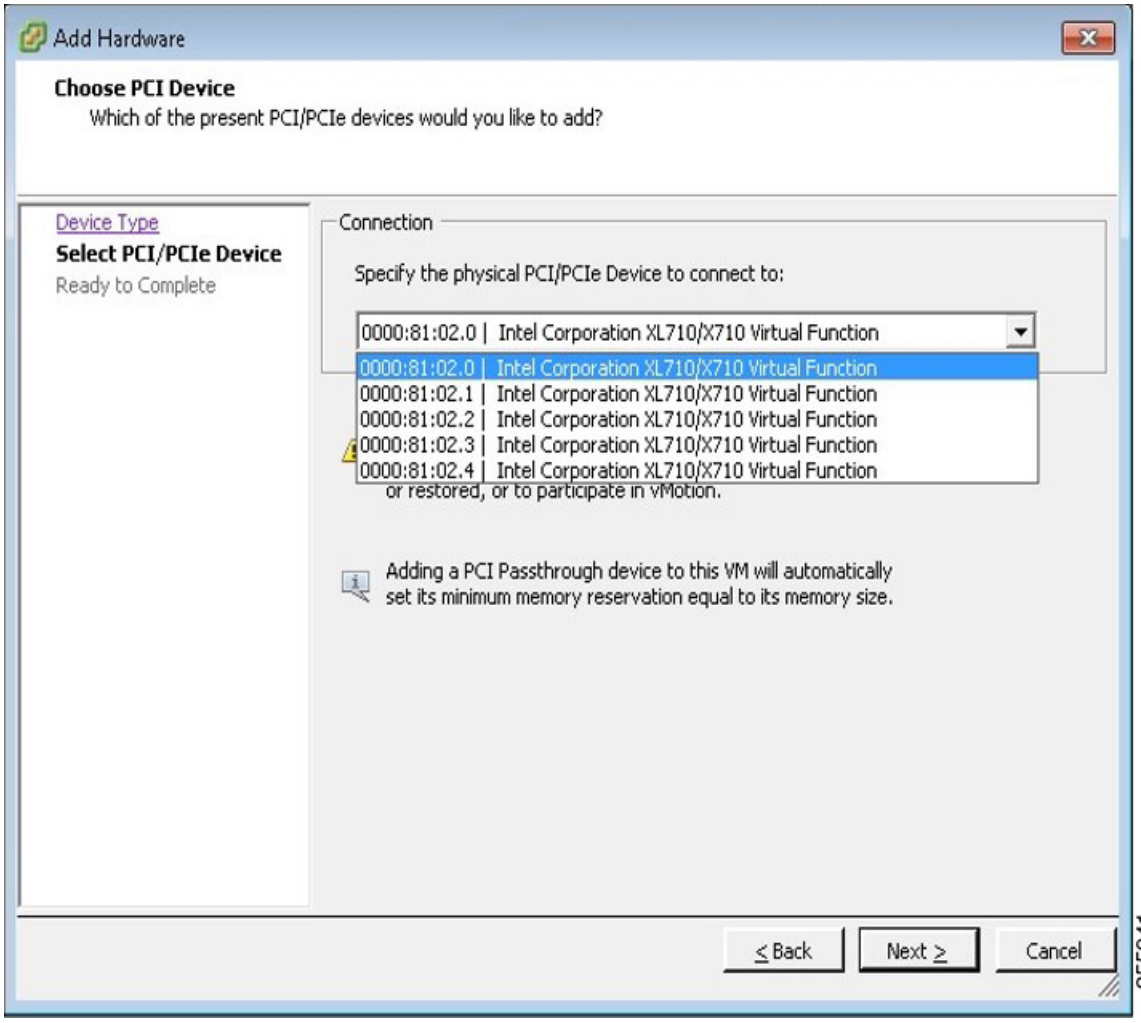


Step 10 For device type, select **PCI Device**.

Step 11 Click **Next**.

The **Choose PCI Device** window is displayed.

Figure 9: Cisco vWAAS Add Hardware > Choose PCI Device Window



Step 12 From the **Specify the physical PCI/PCI3 Device to connect to:** drop-down list, choose the virtual function you want to connect to.

Step 13 Click **Next**.

Step 14 Click **Finish**.

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

Deploying Cisco vWAAS with SR-IOV on KVM

This section contains the following topics:

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

Before you begin

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

Procedure

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

To enable **VT-d**:

- Use the **cat /proc/cpuinfo | grep -E 'vmx|svm' | wc -l** command to verify that you have enabled VT-d.
- The command value should be greater than **0**.

Step 2 Enable **I/O MMU**:

a) In the **/etc/default/grub** file, add **intel_iommu=on** to **GRUB_CMDLINE_LINUX**.
b) After you make changes to **GRUB_CMDLINE_LINUX**, the following message is displayed:

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

c) For the changes to take effect, compile by running **grub2-mkconfig -o /boot/grub2/grub.cfg**.
d) Reboot the host.

Step 3 Enable the SR-IOV virtual functions.

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

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

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

On the **enpls0f0** interface, enter the following:

```
echo 7 > /sys/class/net/enp1s0f0/device/sriov_numvfs
```

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

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

Before you begin

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

Procedure

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

./launch.sh check

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

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

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

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

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

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

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

Procedure

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

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

VM Deployment Process Navigation Flow:

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

Consider the following guidelines for VM deployment:

- Before you enter information to begin the VM deployment process, the **VM Deployment** navigation row displays the element **1 Images** as being highlighted.
- You must specify all the parameters for the Cisco vWAAS VM during VM deployment. After the Cisco vWAAS VM is deployed, you cannot make changes to the Cisco vWAAS VM.

  To change any parameter for a deployed Cisco vWAAS VM, you must delete that Cisco vWAAS VM and deploy a new Cisco vWAAS VM.

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

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

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

Step 4 Click **Next**.

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

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

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

Step 6 To create the new profile, click **Save**.

Step 7 Click **Next**.

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

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

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

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

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

Step 9 To create the new VNIC, click **Save**.

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

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

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

- The table listing displays columns for network name, VLAN (if applicable), bridge, and port (if applicable).
- The table listing shows the available networks and bridges on the NFVIS server. Initially, the table listing shows the default networks: **lan-net** and **wan-net** and associated bridges.
- The top right corner of the table toolbar shows the selected row and the total number of rows, for example, **Selected 2 / Total 4**.
- To associate multiple VLANs with a network, separate the VLAN numbers with a comma and no space, for example, **100,200**.
- To associate multiple ports with a network, separate the port numbers with a comma and no space, for example, **1,2**.
- A network and bridge operate as one entity.

  To delete a network and bridge, click the radio button adjacent to that network and bridge row. Click **Delete**. The page automatically refreshes; there is no confirmation question. Note that you can delete only one network and bridge at a time.

Step 10 Click **Next**.

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

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

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

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

Step 13 Click **Next**.

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

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

Step 14 Click **OK**.

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

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

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

Upgrade and Downgrade Guidelines for Cisco vWAAS and vCM

This section contains the following topics:

Upgrade Guidelines for Cisco vWAAS and Cisco vWAAS Nodes

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

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

Cisco vWAAS Upgrade and SCSI Controller Type

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

Before you begin

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

Procedure

Step 1 Power down the Cisco vWAAS.

Step 2 From the **VMware vCenter**, choose **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 Cisco vWAAS in Cisco WAAS Version 5.2.1 or Cisco WAAS 6.1.x or later. Cisco WAAS Version 6.1.x is the earliest version supported.

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

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

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

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

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

  - If you upgrade the Cisco vCM device to WAAS Version 5.2.1 using the Cisco WAAS Central Manager GUI, a warning message is not displayed.

- The restore factory-default command erases the user-specified information that is stored in the flash image, including the starting configuration of the device, and also removes data from the disk, user-defined partitions, and the entire Cisco WAAS Central Manager database.

  To resolve this situation, follow these steps:

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

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

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

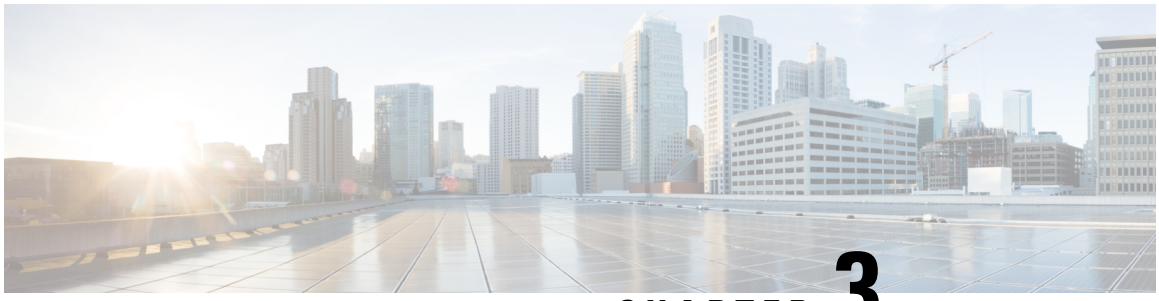
Procedure

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

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

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

Step 4 Switch over Cisco WAAS Central Manager roles so that Cisco vCM works as Primary WAAS Central Manager. For additional details, see the section "Converting a Standby Central Manager to a Primary Central Manager" in the chapter "Maintaining Your Cisco WAAS System" of the *Cisco Wide Area Application Services Configuration Guide*.



CHAPTER 3

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

Cisco ISR-WAAS is the specific implementation of Cisco vWAAS running in a Cisco IOS-XE software container on a Cisco ISR-4400 Series router. **Container** in this context refers to a KVM hypervisor that runs virtualized applications on the Cisco ISR-4400 Series router.

The following table shows the default number of CPUs, memory capacity, disk storage and supported ISR platforms for each ISR model.

Table 35: Cisco ISR Models: CPUs, Memory, Disk Storage and Supported Cisco ISR Platforms

Cisco ISR-WAAS Model	CPUs	Memory	Disk Storage	Cisco ISR Platform Supported	Earliest Cisco WAAS Version Supported
ISR-WAAS-200	1	3 GB	151 GB	ISR-4321	5.2.1
	1	4 GB	151 GB	ISR-4321	6.2.3
ISR-WAAS-750	2	4 GB	151 GB	ISR-4351 ISR-4331 ISR-4431 ISR-4451	5.2.1
	4	6 GB	151 GB	ISR-4461	6.4.1b

Cisco ISR-WAAS Model	CPUs	Memory	Disk Storage	Cisco ISR Platform Supported	Earliest Cisco WAAS Version Supported
ISR-WAAS-1300	4	6 GB	151 GB	ISR-4431 ISR-4451	5.2.1
	4	6 GB	151 GB	ISR-4461	6.4.1b
ISR-WAAS-2500	6	8 GB	338 GB	ISR-4451	5.2.1
	6	8 GB	338 GB	ISR-4461	6.4.1b

Note For Cisco vWAAS in Cisco WAAS Version 6.2.3x or later, Cisco ISR-4321 with profile ISR-WAAS-200, ISR-WAAS RAM can be 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 Cisco WAAS version 6.2.3x or later; the increase in ISR-WAAS RAM is not automatically implemented with an upgrade to Cisco WAAS Version 6.2.3x or later.

Supported Host Platforms, Software Versions, and Disk Types

The following table shows the platforms and software versions supported for Cisco vWAAS on Cisco ISR-WAAS.

Table 36: Platforms and Software Versions Supported for Cisco vWAAS on Cisco ISR-WAAS

PID and Device Type	Earliest Supported Cisco WAAS Version	Host Platforms	Earliest Supported Cisco IOS Version	Disk Type
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-750)	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 Cisco vWAAS on Cisco ISR-WAAS in the following formats:

- Cisco ISR-WAAS NPE OVA file:
  - For Cisco ISR-WAAS models 200, 750, 1300, 2500
  - File format example: **ISR-WAAS-6.4.5.75-npe.tar**
- Cisco ISR-WAAS OVA file:
  - For Cisco ISR-WAAS models 200, 750, 1300, 2500
  - File format example: **ISR-WAAS-6.4.5.75.tar**

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

Deploying and Managing vWAAS on ISR-WAAS

The following table shows the components used to deploy Cisco vWAAS on Cisco ISR-WAAS.

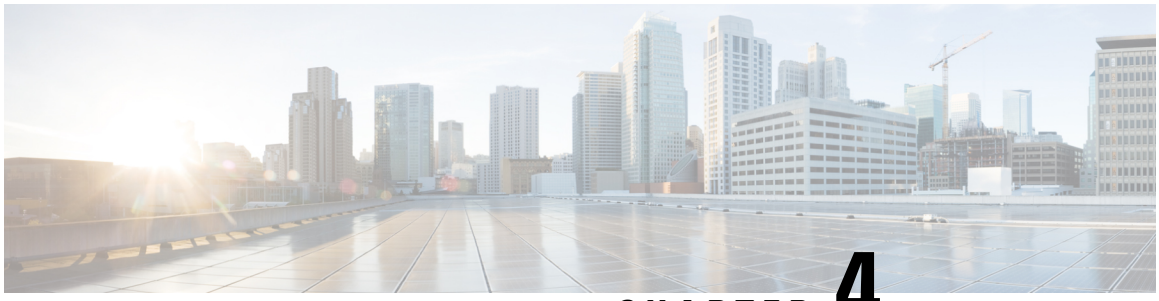
Table 37: Components for Deploying vWAAS on ISR-WAAS

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

The following table shows the components used to manage Cisco vWAAS on Cisco ISR-WAAS.

Table 38: 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



CHAPTER 4

Cisco vWAAS on VMware ESXi

This chapter describes how to use Cisco vWAAS on VMware 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 and ESXi-based environments. Cisco vWAAS on VMware ESXi is delivered as an OVA file. The Cisco Unified vWAAS OVA file helps you to deploy as an instance of a required Cisco vWAAS model.

Supported Host Platforms and Software Versions

This section contains the following tables:

- Platforms and software versions supported for Cisco vWAAS on VMware ESXi.
- Supported Cisco WAAS versions for VMware ESXi for a new Cisco vWAAS installation.
- Supported Cisco WAAS versions for VMware ESXi for a Cisco vWAAS upgrade.

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

The following table shows VMware ESXi server datastore memory and disk space per Cisco vWAAS model, for Cisco WAAS v4.3.1 through v5.3.5, and for Cisco WAAS v5.4.x through v6.x.

Table 39: vCPUs, Server Datastore Memory, and Disk Space by Cisco vWAAS Model

	For Cisco WAAS v4.3.1 through v5.3.5			For Cisco WAAS v5.4.x through v6.x		
Cisco vWAAS Model	**vCPUs**	**VMware ESXI Datastore Memory**	**Disk**	**vCPUs**	**VMware ESXI Datastore Memory**	**Disk**
vWAAS-150 (for Cisco 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

The following table shows VMware ESXi server datastore memory and disk space per Cisco vCM model, for Cisco WAAS v4.3.1 through v5.3.5, and for Cisco WAAS v5.4.x through v6.x.

Table 40: vCPUs, Server Datastore Memory, and Disk Space by Cisco vCM Model

	For Cisco WAAS v4.3.1 through v5.3.5			For Cisco WAAS v5.4.x through v6.x		
Cisco vCM Model	**vCPUs**	**VMware ESXI Datastore Memory**	**Disk**	**vCPUs**	**VMware ESXI 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

Note For Cisco WAAS resized CPU and Memory values, refer to Cisco vWAAS and vCM Sizing Guidelines for Cisco WAAS Version 6.4.3x and Later, on page 6 and Cisco vWAAS Resizing Guidelines, on page 12 in the chapter "Introduction to Cisco vWAAS."

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) Software Download page and select the WAAS software version used with your vWAAS instance.

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

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

Each unified OVA package is a preconfigured VM 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 Cisco vWAAS in Cisco WAAS in the required configuration.

The following are examples of the unified OVA and NPE OVA package filenames for Cisco vWAAS in VMware ESXi, for **vWAAS in WAAS 6.4.1 to 6.4.3x**:

- OVA: Cisco-WAAS-Unified-6.4.3c-b-42.ova
- NPE OVA: Cisco-vWAAS-Unified-6.4.3c-b-42-npe.ova

The following are examples of the unified OVA and NPE OVA package filenames for Cisco vWAAS in VMware ESXi, for **vWAAS in WAAS 6.4.5x**:

- OVA: Cisco-WAAS-Unified-6.4.5-b-69.tar
- NPE OVA: Cisco-WAAS-Unified-6.4.5-npe-b-69.tar

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, as described in Installing VMware ESXi for Cisco vWAAS in Cisco WAAS Versions 5.x to 6.2.x, on page 81 and in Installing VMware ESXi for Cisco vWAAS for Cisco WAAS Version 6.4.1 through 6.4.3a, on page 79.

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

For Cisco vWAAS on VMware ESXi in Cisco WAAS Version 5.x through 6.2.x, Cisco provides an OVA or NPE OVA package for each Cisco vWAAS connection profile and for each Cisco vCM connection profile, shown in the following two tables.

Table 41: Cisco OVA Package Format Examples for vWAAS on VMware ESXi, WAAS v5.x to 6.2.x

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

Table 42: Cisco OVA Package Format Examples for vCM in WAAS Versions earlier than Version 6.4.1

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

Installing VMware ESXi for Cisco vWAAS

This section contains the following topics:

Using VMware vCenter to Install VMware ESXi for Cisco vWAAS in WAAS v6.4.3b and Later

Before you begin

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

- Ensure that the required supporting plugins like Adobe Flash and Client Interaction Plugin are installed.
- For OVA deployments, always use **vSphere Web Client (Flash)**, because HTML5 mode does not have all the functionality supported.

Procedure

Step 1 Open the VMware vSphere Web Client with your specified vCenter IP address.

- For **VMware Version 6.5** for vWAAS in WAAS Version 6.4.3b and later, select the **Flash** method of login.
- For **VMware Version 6.7** for vWAAS in WAAS Version 6.4.3c and later, select the **Flex** method of login.

Step 2 Log in to the **VMware vCenter Single Sign-On** window.

Figure 10: VMware vCenter Single Sign-On Window

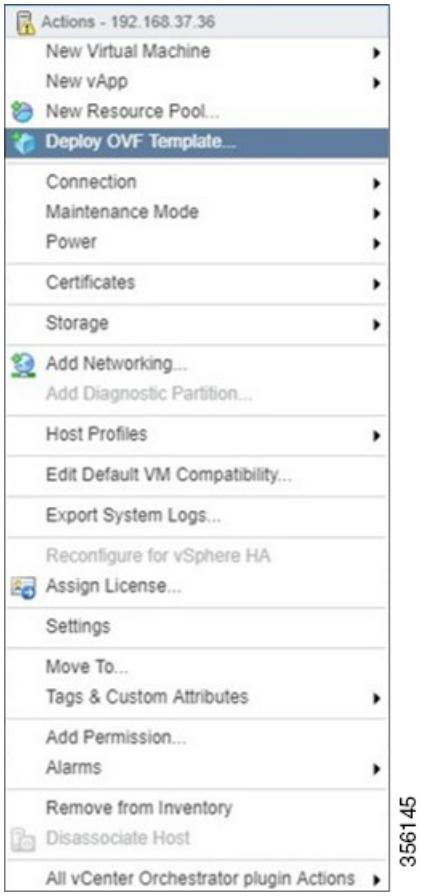
Step 3 Navigate to the required datacenter host on which the deployment will be done.

Step 4 Click the required host to highlight it, as shown in the following figure.

Figure 11: Navigator > Datacenter > Host Menu Option

Step 5 After you have highlighted the required host, right-click and select **Deploy OVF Template...**.

Figure 12: Deploy OVF Template... Menu Option

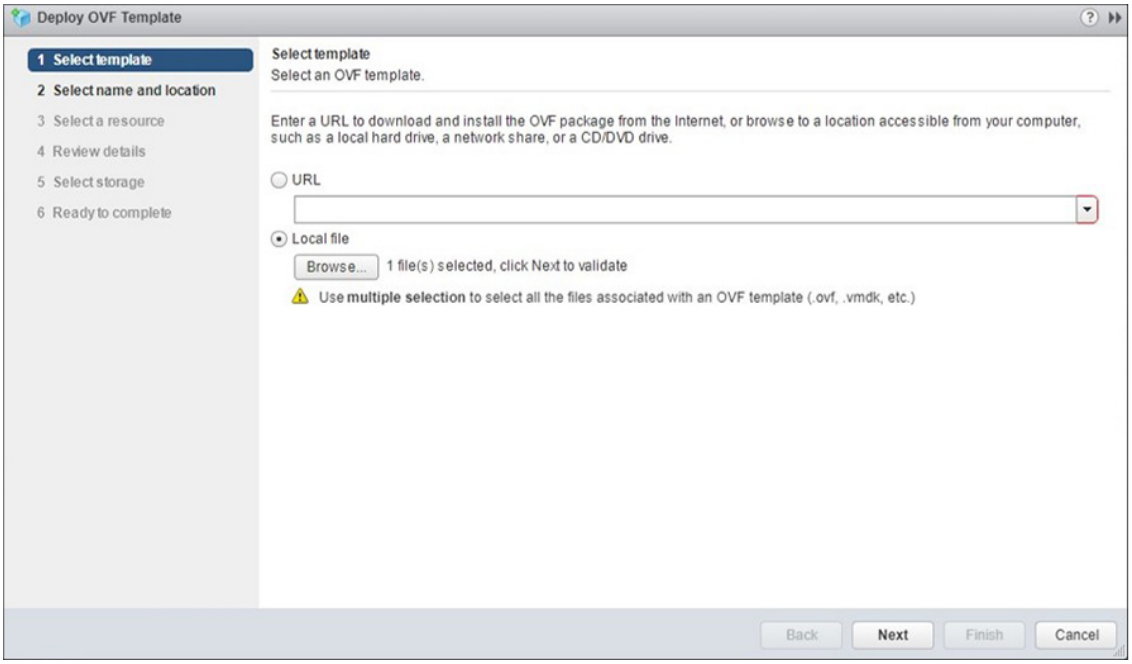


Step 6 In the **Deploy OVF Template > Select Template** window, shown below, follow these steps:

a) Enter the URL to download the OVA package or browse for the downloaded OVA file using the **Browse** button.

b) Click **Next**.

Figure 13: Deploy OVF Template > Select Template Window



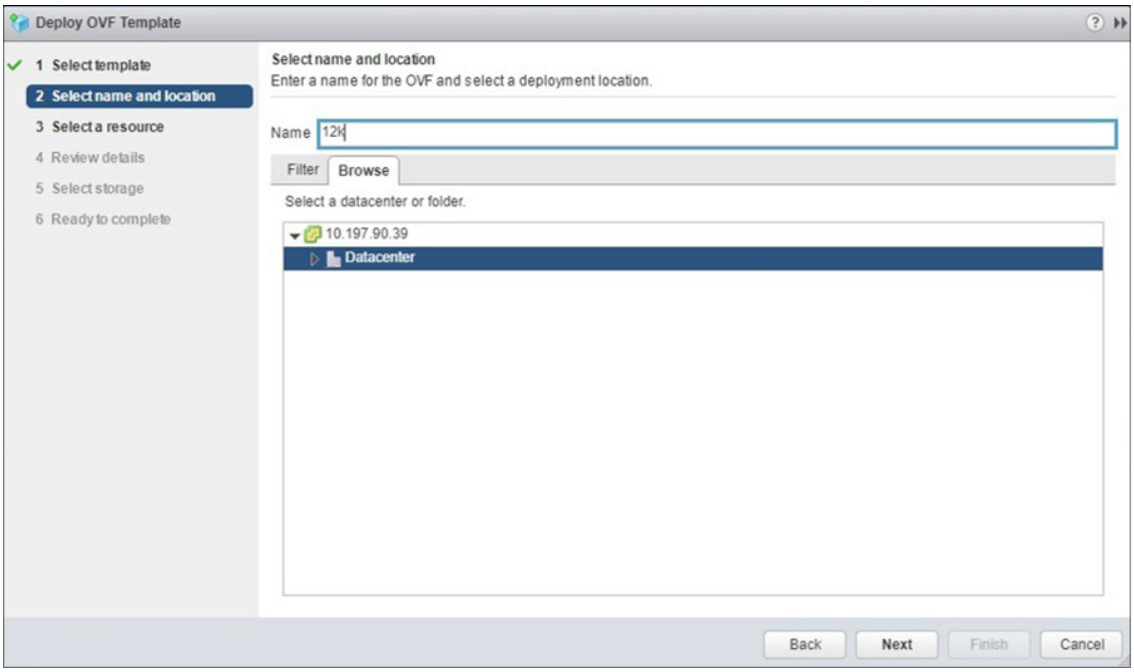
Step 7 In the **Deploy OVF Template > Select Name and Location** window, shown below, follow these steps:

a) In the **Name** field, enter the name of the Cisco vWAAS model to be deployed.

b) Click the **Browse** tab and select a datacenter or folder.

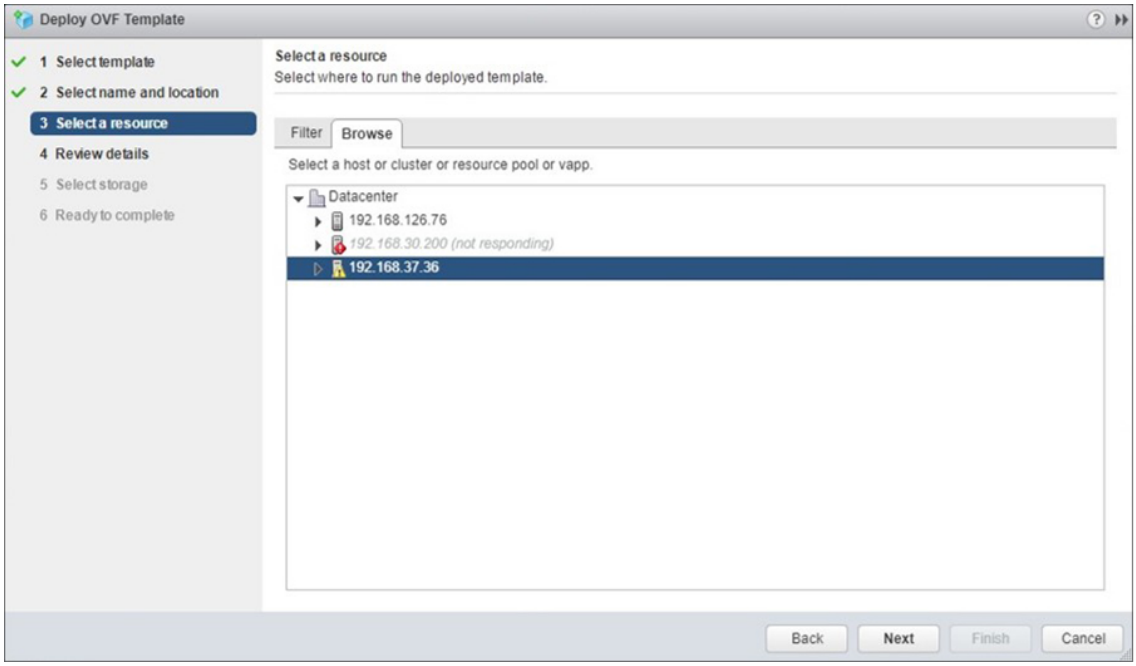
c) Click **Next**.

Figure 14: Deploy OVF Template > Select Name and Location Window



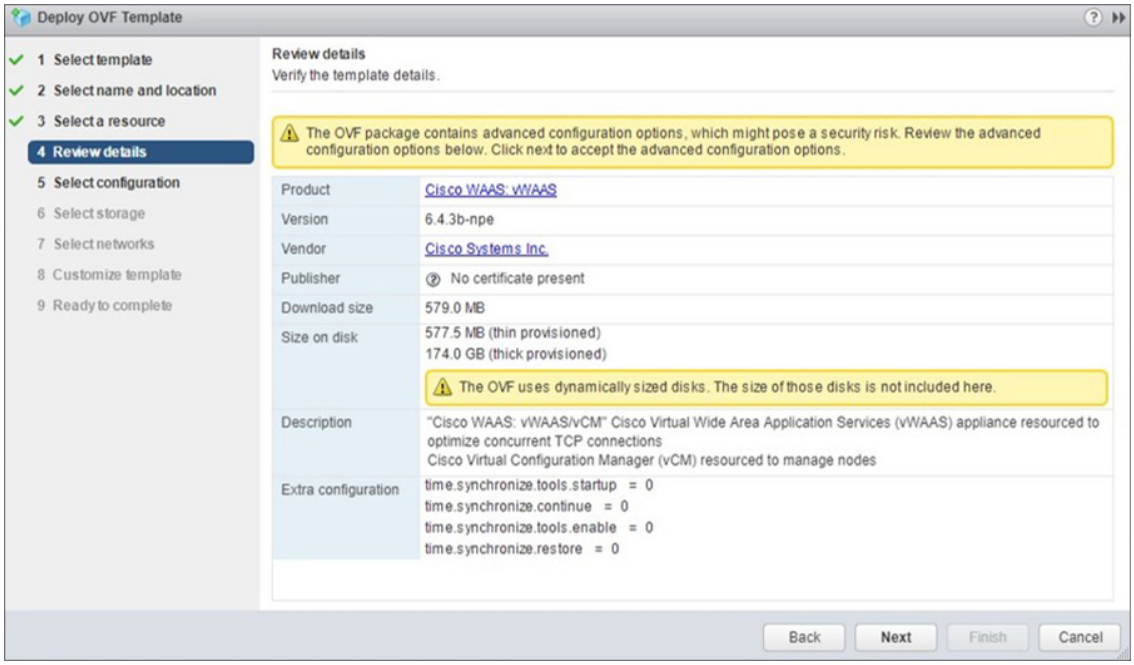
Step 8 In the **Deploy OVF Template > Select a Resource** window, select the resource (the host) where the OVA will be deployed.

Figure 15: Deploy OVF Template > Select a Resource Window



Step 9 In the **Deploy OVF Template > Review Details** window, verify that the template details are correct. The following figure shows a **Review Details** window with configuration notices and guidance messages.

Figure 16: Deploy OVF Template > Review Details Window

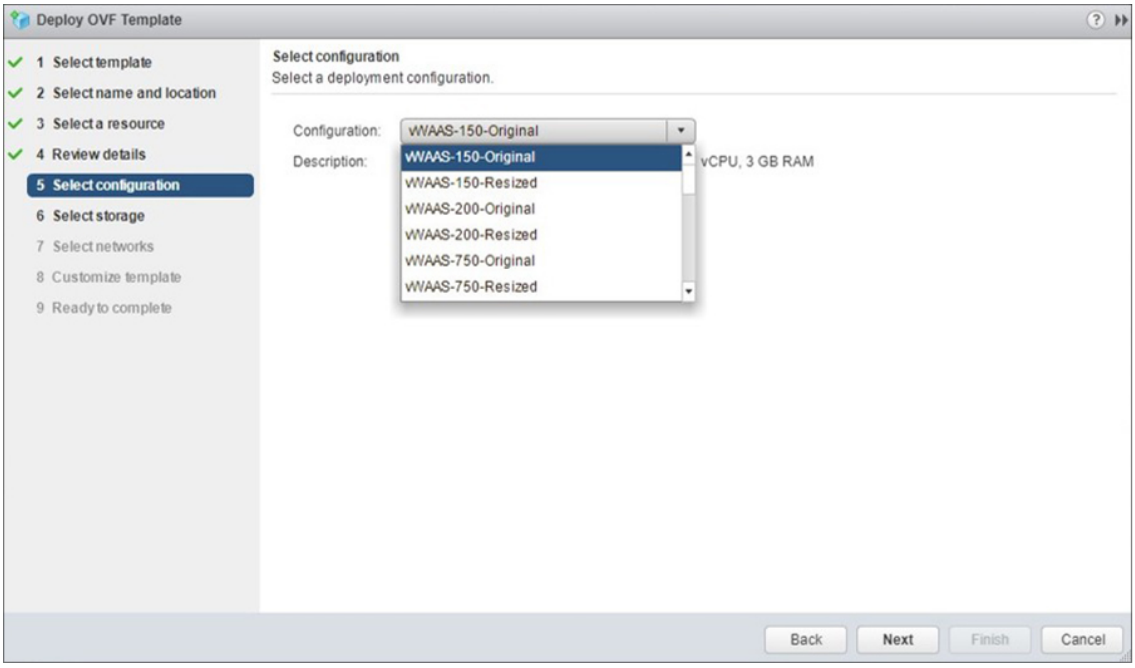


Step 10 In the **Deploy OVF Template > Select Configuration** window, shown below, follow these steps:

a) From the **Configuration** drop-down list, choose the configuration of the deployed Cisco vWAAS model.

b) Click **Next**.

Figure 17: Deploy OVF Template > Select Configuration Window



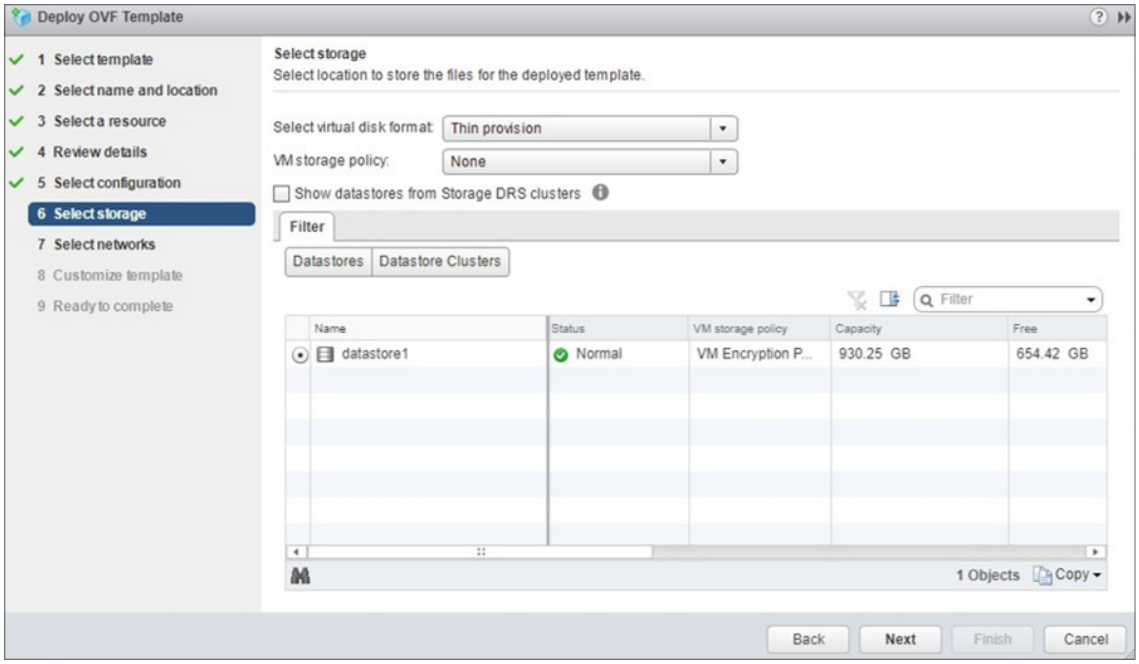
Step 11 In the **Display OVF Template > Select Storage** window, shown below, follow these steps:

a) From the **Select virtual disk format** drop-down list, select the type of storage required for your system: Thick Pro**vision Lazy Zeroed**, **Thin Provision**, or **Thick Provision Eager Zeroed**.

b) From the **VM storage policy** drop-down list, choose the VM storage policy for your system.

c) Click **Next**.

Figure 18: Deploy OVF Template > Select Storage Window

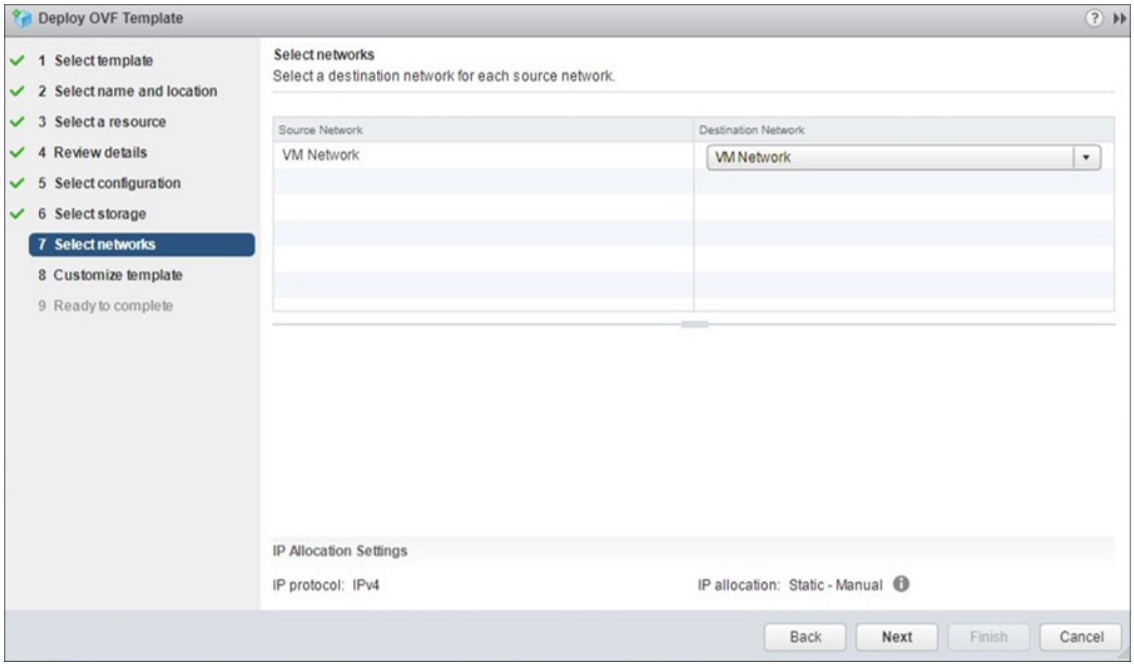


Step 12 From the **Deploy OVF Template > Select Networks** window:

a) From the **Destination Network** drop-down list, choose the appropriate VM network for your system.

b) Click **Next**.

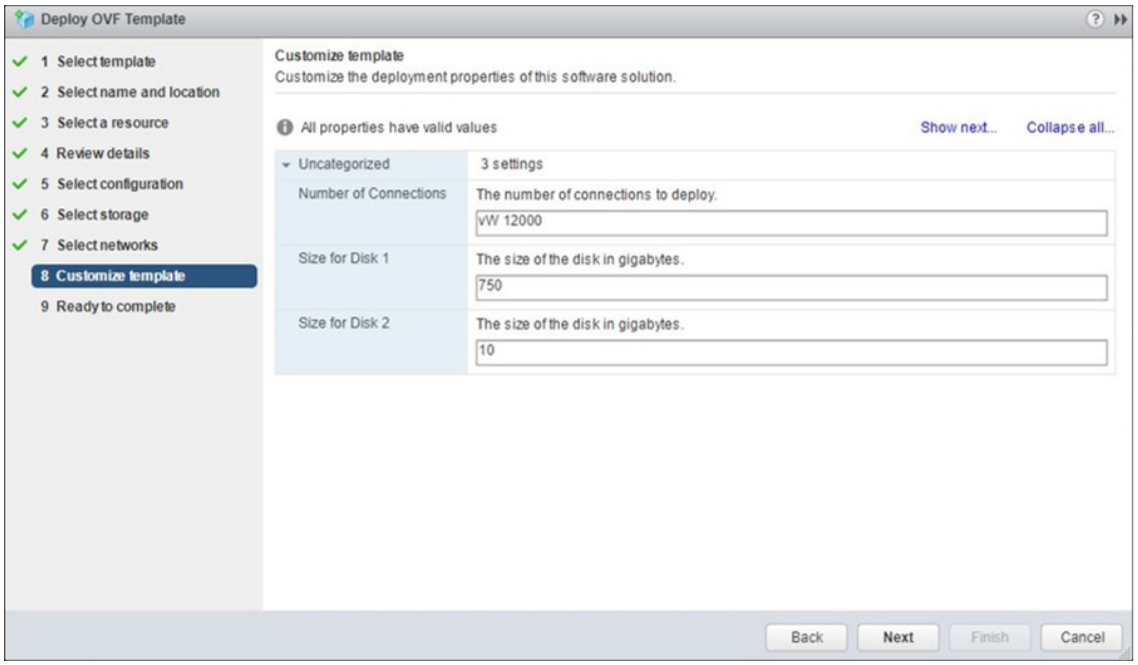
Figure 19: Deploy OVF Template > Select Networks Window



Step 13 In the **Deploy OVF Template > Customize Template** window, review the information and click **Next**.

Note Do *not* edit any values in the text boxes. Altering the values will lead to failure in deployment.

Figure 20: Deploy OVF Template > Customize Template Window

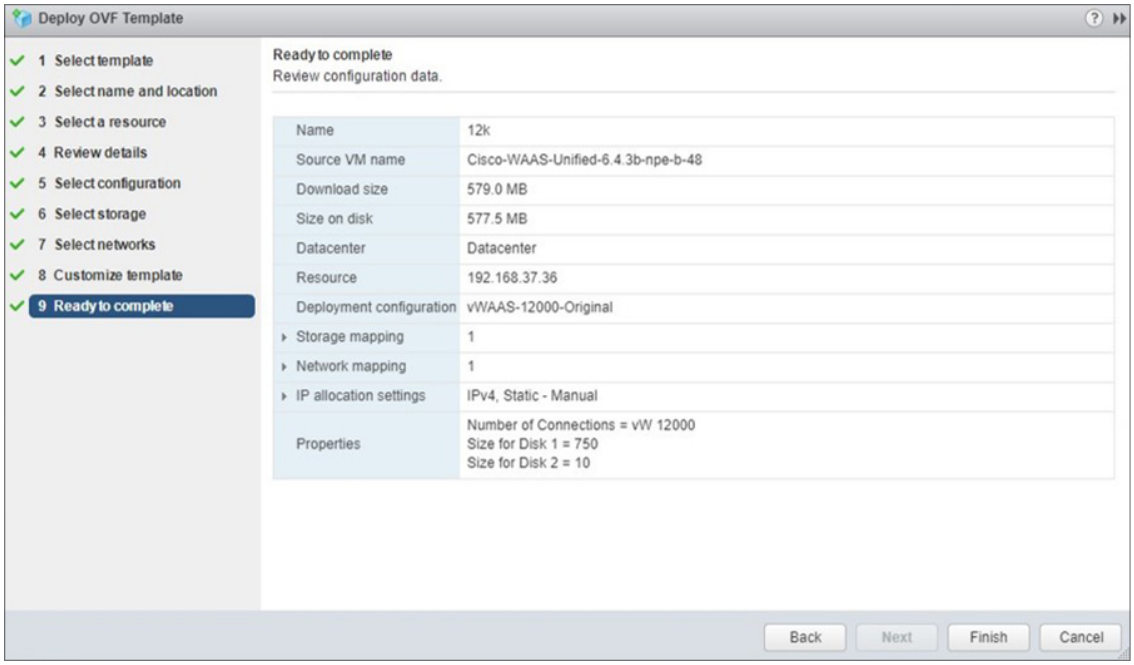


Step 14 In the **Deploy OVF Template > Ready to Complete** window, shown below, follow these steps:

a) Review and confirm configuration data, including Cisco vWAAS model name, storage mapping, network mapping, number of connections, and disk sizes.

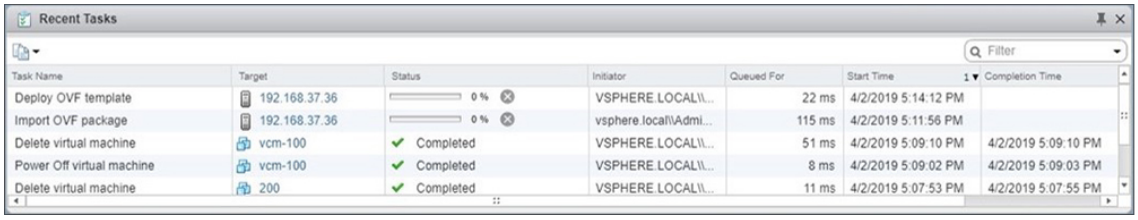
b) Click **Next**.

Figure 21: Deploy OVF Template > Ready to Complete Window



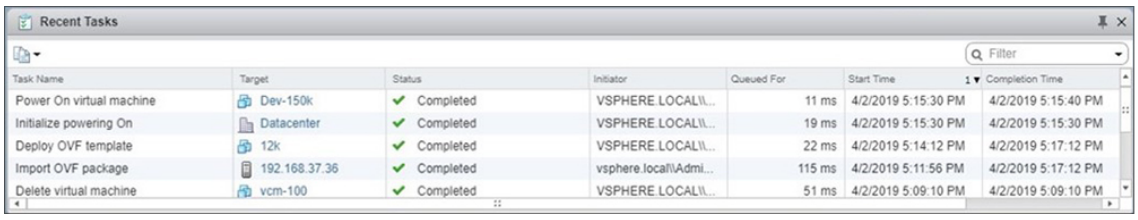
Step 15 The **Recent Tasks** pane of the **VMware vSphere Web Client** window displays the status of the import and deployment of the image.

Figure 22: VMware vSphere Web Client Recent Tasks Pane - In-Progress Status



Step 16 After deployment is complete, the **Recent Tasks** pane items show **Completed** for the deployed Cisco vWAAS image.

Figure 23: VMware vSphere Web Client Recent Tasks Pane - Completed Status



Step 17 After deployment is complete, use the **Power > Power On** menu option to power on the device.

Sporadically, deployment may fail due to a communication error between VMware vCenter and the VMware ESXi host. If this occurs during deployment, try one of the following steps and then deploy the OVA again.

- Increase the timeout value as 120 or higher in the **config.vpxd.heartbeat.notrespondingtimeout** field.

  Or

- While deploying, choose the **Disk Type** option as Thin Provisioning and use the following procedure to convert the disks to **Thick Eager Zero**.

  a. Wait for the deployment to complete 100%.

  b. Ensure the deployed VM is in Power-Off state. If it is not, power off the device before proceeding to the next step.

  c. Navigate to the folder of the virtual disk you want to inflate.

  - In the **vSphere Web Client**, browse to the virtual machine.
  - Click the **Datastores** tab.

    The datastore that stores the virtual machine files is listed.

  - Select the datastore and click the **Browse Files** icon.

    The datastore browser displays contents of the datastore.

  d. Expand the virtual machine folder and browse through the list of files. The files with extension **.vmdk** will have the virtual disk icon.

  e. Right-click the **.vmdk** virtual disk file and select the **Inflate** option.

  f. Repeat the above step for all the **.vmdk** files in the deployed VM.

Step 18 Use the **Open Console** menu option to open the device console. The following two figures show the **Open Console** menu option and the **Device Console**.

Figure 24: VMware vSphere Web Client Open Console Menu Option

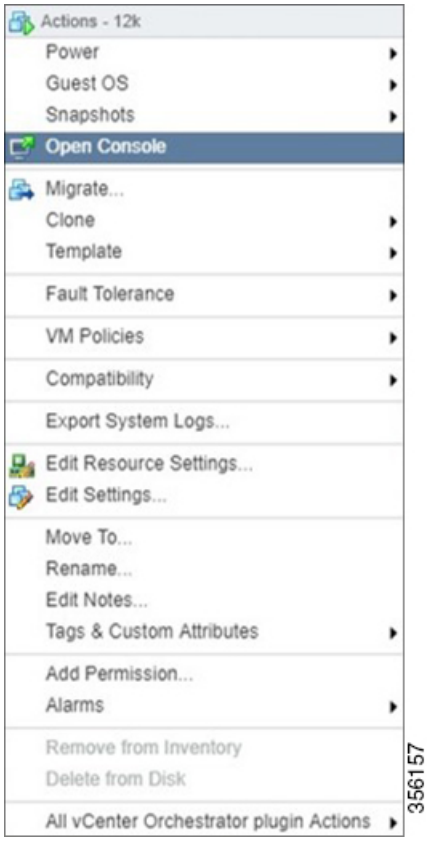
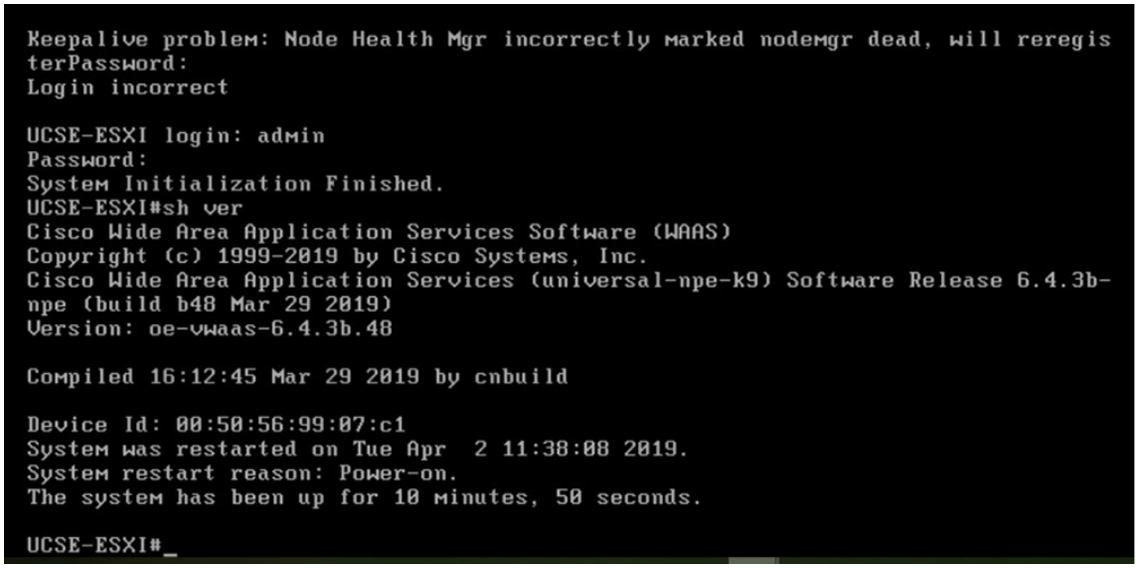


Figure 25: Device Console



Using VMware OVF Tool to Install VMware ESXi for Cisco vWAAS in WAAS v6.4.3b and Later

Before you begin

The VMware OVF Tool is a command-line utility that allows you to deploy a required Cisco vWAAS model using Cisco vWAAS Unified OVA package file.

Note The procedure for installing the Cisco vWAAS VM with the VMware OVF tool is available for Cisco vWAAS in VMware ESXi Version 6.5 only.

Procedure

Step 1 Identify the **-deploymentOption** of the vWAAS model you want to deploy.

- The supported original and resized Cisco vWAAS models are:
  - Original Cisco vWAAS models supported:

    vWAAS-150

    vWAAS-200

    vWAAS-750

    vWAAS-1300

    vWAAS-2500

    vWAAS-6000

    vWAAS-6000R

    vWAAS-12000

    vWAAS-50000

    vWAAS-150000

    To deploy an original Cisco vWAAS model: Use the designation **VW_**, for example, **VW_6000**.
  - Resized Cisco vWAAS models supported:

    vWAAS-150

    vWAAS-200

    vWAAS-750

    vWAAS-1300

    vWAAS-2500

    vWAAS-6000

    vWAAS-6000R

vWAAS-12000

vWAAS-50000

To deploy a resized vWAAS model: Use the designation **_Res**, for example, **VW_6000_Res**.

- The supported original Cisco vCM models are:

  vCM-100

  vCM-500

  vCM-1000

  vCM-2000

  To deploy an original vCM model: Use the designation **VC_**, for example, **VC_500**.

Step 2 Download the Cisco vWAAS Unified OVA to your host.

Step 3 To deploy the Cisco vWAAS Unified OVA, in the VMware OVF Tool, use the following CLI commands:

```
> ovftool \
--allowExtraConfig \
--diskMode=eagerZeroedThick \
--datastore=<your-datastore-to-deploy> \
--deploymentOption=<selected vWAAS-model> \
--powerOn \
--name=<name-of-the-vm> \
<path-to-downloaded/<downloaded-ova-file> \
'vi://<vCenter-login>:<vCenter-Passwd>@<vCenter-server-ip>/?ip=<ESXi-Host-IP>'
```

Example:

```
> ovftool \
--allowExtraConfig \
--diskMode=eagerZeroedThick \
--datastore=NewDatastore \
--deploymentOption=VW_150 \
--powerOn \
--name=vWAAS \
/home/ovftool/Cisco-WAAS-Unified-6.4.3b-b-52.ova \
'vi://administrator@vsphere.local:vSpherePasswd@1.1.1.1/?ip=2.2.2.2'
Opening OVA source: /home/ovftool/Cisco-WAAS-Unified-6.4.3b-b-52.ova
The manifest validates
Opening VI target: vi://administrator%40vsphere.local@1.1.1.1:443/
Deploying to VI: vi://administrator%40vsphere.local@1.1.1.1:443/
Transfer Completed
Powering on VM: vWAAS
Task Completed
Completed successfully
```

Installing VMware ESXi for Cisco vWAAS for Cisco WAAS Version 6.4.1 through 6.4.3a

Before you begin

- Ensure that the required supporting plugins like Adobe Flash and Client Interaction Plugin are installed.

- For OVA deployments, always use vSphere Web Client (Flash) or vSphere Web Client (Flex), because HTML5 mode does not have all the functionality supported.

Procedure

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

Step 2 From the **Configuration** drop-down list, choose the Cisco vWAAS model for this hypervisor.

Note When you choose a Cisco vWAAS model, that model's profile is displayed. For example, if you choose vWAAS-150, the vSphere Client displays a configuration such as 1 vCPU, 3 GB RAM.

Step 3 Click **Next**.

Step 4 In the **Deploy OVF Template** window, choose **Source** to select the source location for the deployed template.

Step 5 From the **Deploy from a file or URL** drop-down list, click **Browse...**.

The **Name and Location** window is displayed.

Step 6 Enter a unique name for the deployed template, and select a location for the deployed template.

a) In the **Name** field, enter a unique name for the deployed template. The template name can contain up to 80 alphanumeric characters.
b) In the **Inventory Location** listing, select a folder location.

Step 7 Click **Next**.

Step 8 In the **Deploy OVF Template** window, select **Deployment Configuration**.

Step 9 From the **Configuration** drop-down list, choose the Cisco vWAAS model for your system.

Note When you select a Cisco vWAAS model, the window displays configuration information. For example, if you select vWAAs-200, the window will display a description such as **Deploy a vWAAS-200 connection profile with 1 vCPU, 3 GB RAM**.

Step 10 Click **Next**.

Step 11 In the Dep**loy OVF Template** window, select **Disk Format**.

Step 12 In the **Datastore:** field, enter the datastore name.

Step 13 For provisioning, choose one of the following virtual disk format types:

- **Thick Provision Lazy Zero**: The entire space specified for virtual disk files is allocated when the virtual disk is created. The old data on the physical device is not erased when the disk is created, but zeroed out on demand, as needed, from the VM.
- **Thick Provision Eager Zero**: The entire space specified for virtual disk files is allocated when the virtual disk is created. Old data is erased when the disk is created. The thick provision eager zero option also supports VMware fault tolerance for high availability.

Note The **Thin Provision** option is not available for Cisco vWAAS with VMware ESXi.

Step 14 Click **Next**.

The VMware ESXi hypervisor is created for the specified Cisco vWAAS model.

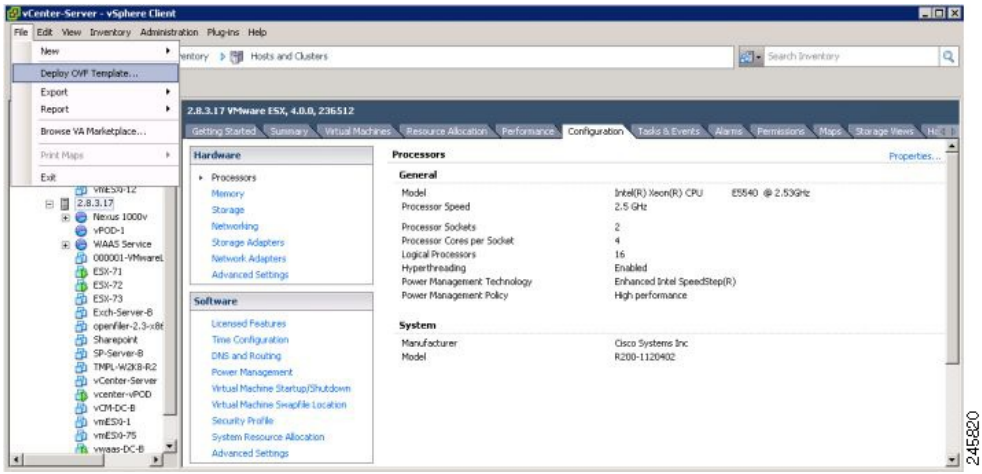
Installing VMware ESXi for Cisco vWAAS in Cisco WAAS Versions 5.x to 6.2.x

Procedure

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

The **Source** window appears.

Figure 26: File > 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**.

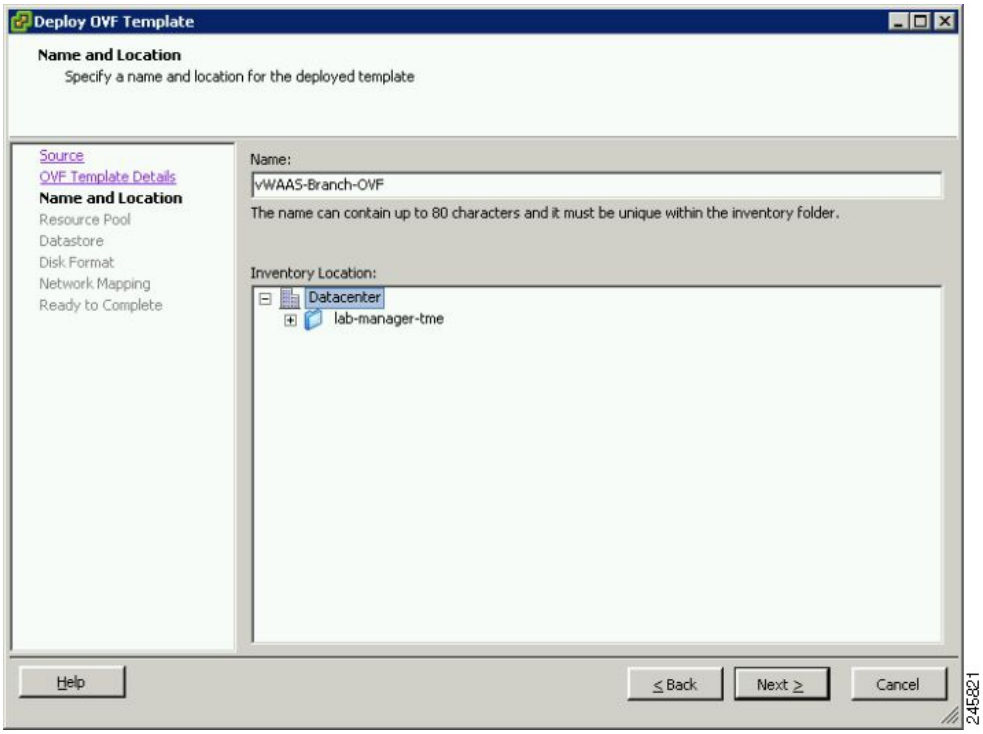
- If the virtual host was created using an OVA of Cisco vWAAS in Cisco WAAS Version 5.1.x or later, proceed to **Step 4**.
- If the virtual host was created using an OVA file of Cisco vWAAS in Cisco WAAS Version 5.0 or earlier, and you have upgraded Cisco vWAAS from inside Cisco WAAS, you must verify that the **SCSI Controller Type** is set to **VMware Paravirtual**. Otherwise, Cisco vWAAS will boot with no disk available, and will fail to load the specified configuration.
- If needed, change the **SCSI Controller Type** to **VMware Paravirtual** by following these steps:

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

Step 4 To accept the selected OVA file, click **Next**.

The **Name and Data Center Location** window appears.

Figure 27: Deploy OVF Template > Name and Data Center Location



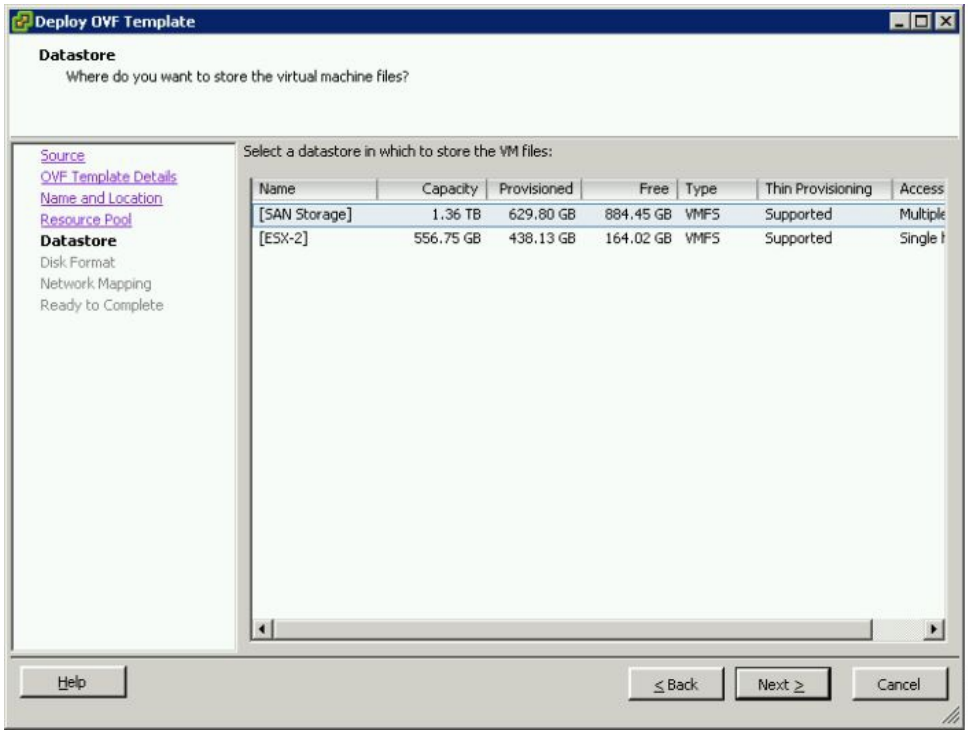
Step 5 Enter a name for the Cisco vWAAS VM, choose the appropriate data center, and then click **Next**.

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 (if this window appears, skip to **Step 7**).

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

The **Datastore** window appears.

Figure 28: Deploy OVF Template > Datastore



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

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.

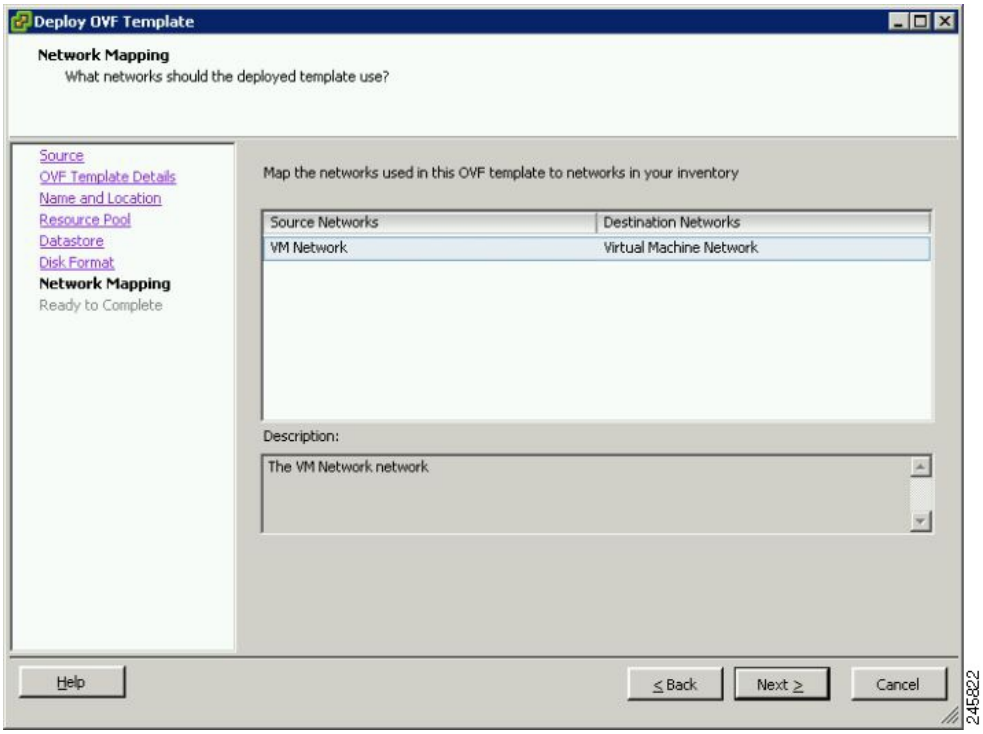
Step 8 The **Disk Provisioning** section has three disk format options: **Thick Provision Lazy Zeroed**, **Thick Provision Eager Zeroed**, and **Thin Provision**. Select **Thick Provision Eager Zeroed**.

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

Step 9 Click **Next**.

The **Network Mapping** window appears.

Figure 29: Deploy OVF Template > Network Mapping



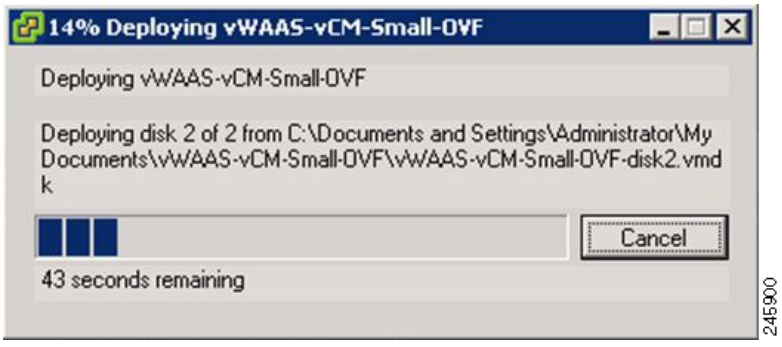
Step 10 Choose the network mapping provided by VMware ESXi and click **Next**. You have the option to change this later if necessary.

The **Ready to Complete** window appears.

Step 11 To complete the installation, click **Finish**.

The **Status** window appears while the OVA file is being deployed.

Figure 30: Cisco vWAAS: Status Window



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

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 Cisco vWAAS finishes booting, click the **Console** tab to view bootup messages.

Note Under rare conditions, the Cisco 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 more information, see the chapter "Troubleshooting Cisco vWAAS."

For more information on Cisco vWAAS configuration, see the chapter "Configuring Cisco vWAAS and Viewing Cisco vWAAS Components."

Operating Guidelines for VMware ESXi in Cisco vWAAS in WAAS v6.4.3 and Later

Consider the following guidelines for Cisco vWAAS in WAAS Version 6.4.3x and VMware ESXi 6.0 or later.

- To ensure that configured routers are displayed in the routing table output, after deployment is completed, and the Cisco vWAAS-200 is configured with IP address and default gateway:
  1. In VMware vSphere, choose the **Virtual Hardware** tab, and from the **Adapter Type** drop-down list, choose the **VMXNET3**.
  2. If the adapter type is set to any other option, such as Flexible or e1000, the configured routers will *not* appear in the routing table output.
  3. To verify that the configured routers appear in the routing table output, run the **show ip route** EXEC command.
- If you had already configured the Cisco vWAAS with a different adapter:
  1. Power off the VM.
  2. From the host, change the adapter type to VMXNET3.
  3. Power on the VM.
  4. To verify that the configured routers appear in the routing table output, run the **show ip route** EXEC command.

Upgrade and Downgrade Guidelines for vWAAS on VMware ESXi

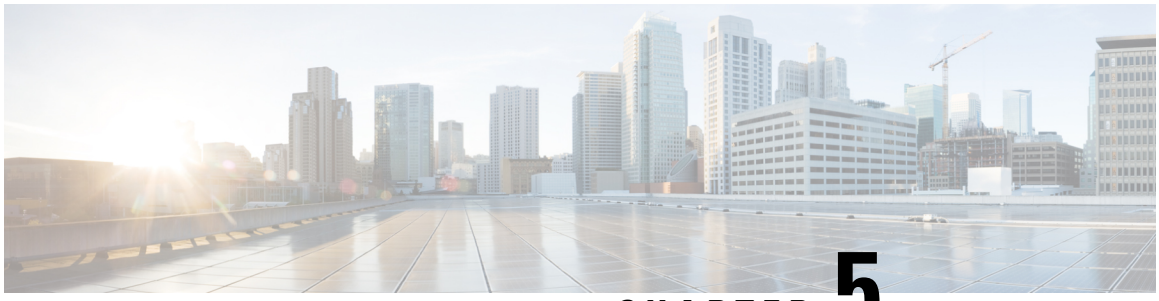
Consider the following guidelines when upgrading or downgrading your Cisco WAAS system with Cisco vWAAS on VMware ESXi:

- When upgrading Cisco vWAAS, do not upgrade more than five vWAAS nodes at the same time on a single Cisco UCS device. 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 Cisco vWAAS in Cisco WAAS Version 5.0 or earlier, and you have upgraded Cisco vWAAS within Cisco WAAS, you must verify that the SCSI Controller Type is set to VMware Paravirtual. Otherwise, the Cisco vWAAS will boot with no disk available and will fail to load the specified configuration.

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

  1. Power down the Cisco vWAAS.
  2. From the VMware vCenter, choose **vSphere Client > Edit Settings > Hardware**.
  3. Choose **SCSI controller 0**.
  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**.
  5. Click **OK**.
  6. Power up the Cisco vWAAS in Cisco WAAS Version 6.1.x or later.



CHAPTER 5

Cisco vWAAS on Microsoft Hyper-V

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

About Cisco vWAAS on Microsoft Hyper-V

Microsoft Hyper-V, available for Cisco vWAAS in 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, Cisco 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.

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

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

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

Supported Host Platforms, Software Versions, and Disk Type

The following table shows the platforms and software versions supported for Cisco vWAAS on Microsoft Hyper-V.

Table 43: Platforms and Software Versions Supported for Cisco vWAAS on Microsoft Hyper-V

PID and Device Type	Earliest Supported Cisco WAAS Version	Host Platforms	Earliest Supported Host Version	Disk Type
PID: **OE-VWAAS-HYPERV** Device Type: **OE-VWAAS-HYPERV**	6.1.x	Cisco UCS Cisco UCS-E Series	Microsoft Windows 2008 R2	VHD

System Requirements for Cisco vWAAS on Microsoft Hyper-V

This section describes the infrastructure requirements and the hardware virtualization requirements needed to deploy Cisco vWAAS on Microsoft Hyper-V.

The following list shows the infrastructure requirements needed to deploy Cisco vWAAS on Microsoft Hyper-V:

- **Microsoft Hyper-V Hypervisor**: The 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 VMs 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.
- **Microsoft System Center Virtual Machine Manager (SCVMM)**: Microsoft's virtual machine support center for Windows-based systems. SCVMM upholds Microsoft's focus on efficiency with features to help administrators consolidate multiple physical servers within a central virtualized environment.
- **PowerShell**: PowerShell is a task-based command-line shell and scripting language built on .NET. PowerShell helps system administrators and power-users rapidly automate tasks that manage operating systems (Linux, macOS, and Windows) and processes. Power Shell commands let you manage computers from the command line.

The following list shows the hardware virtualization requirements for CPU, disk, CD-ROM, and Flash needed to deploy Cisco vWAAS on Microsoft Hyper-V.

- **CPU**: Cisco vWAAS on Hyper-V supports 2, 4, and 8 CPU configurations. Cisco vWAAS on Microsoft Hyper-V requires a minimum CPU limit.

Note A Cisco vWAAS VM with different CPU configurations works, but is not recommended.

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

Deployment Options for Cisco vWAAS on Microsoft Hyper-V

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

- Cisco vWAAS on Microsoft Hyper-V as installable product in the Windows server: Windows Server 2008 R2, Windows Server 2012 or Windows Server 2012 R2.
- Cisco vWAAS on Microsoft Hyper-V as standalone role in the Hyper-V server: Used with Microsoft Hyper-V Server 2012 R2 or Microsoft Hyper-V Server 2016.

The following table shows Microsoft Hyper-V servers and Microsoft System Center Virtual Machine Manager (SCVMM) support for Cisco vWAAS.

Table 44: Cisco vWAAS Support for Microsoft Hyper-V Servers and SCVMM

Microsoft Hyper-V Server	Microsoft SCVMM	Cisco 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
Microsoft Hyper-V Server 2016	–-	Yes

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

The following table shows platforms supported for Cisco vWAAS and Cisco vCM on Microsoft Hyper-V, deployed as a standalone or installable product.

Table 45: 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 or 2016**	**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
vCM-2000	vCM-2000	vCM-2000
vWAAS-150 (For Cisco WAAS Version 6.2.1 and later, supported on Cisco Enhanced High-Speed WAN Interfaced Card (EHWIC) and Cisco Network Interfaced Module (NIM.))	vWAAS-150 (For Cisco WAAS Version 6.2.1 and later, supported on Cisco EHWIC and NIM.)	vWAAS-150 (For Cisco 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:

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

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

Each unified OVA package is a preconfigured VM image that is ready to run on a particular hypervisor.The PowerShell deployment script for each unified ova package file provides the model and other required parameters to launch Cisco vWAAS in WAAS in the required configuration.

The following are examples of the unified OVA and NPE OVA package files' filenames for Microsoft Hyper-V:

- OVA: Cisco-HyperV-vWAAS-unified-6.4.5-b-69.tar
- NPE OVA: Cisco-HyperV-vWAAS-unified-6.4.5-b-69-npe.tar

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

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

For Cisco vWAAS on Microsoft Hyper-V in Cisco WAAS Version 6.1.x and later, Cisco provides an OVA or NPE OVA package for each Cisco vWAAS connection profile and for each vCM connection profile.

The Cisco OVA package for Cisco 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.

The following list shows OVA package format and examples for Cisco vWAAS on Microsoft Hyper-V for Cisco WAAS Version 6.1.x through 6.2.x:

Table 46: OVA Package Format Examples for Cisco vWAAS on Microsoft Hyper-V in Cisco WAAS Version 6.1.x through 6.2.x

Package Format	File Format Example
1. Cisco Hyper-V 150 package file 2. Cisco Hyper-V 150 package file for NPE	1. Hv-Cisco-vWAAS-150-6.2.3d-b-68.zip 2. Hv-Cisco-vWAAS-150-6.2.3d-npe-b-68.zip
1. Cisco Hyper-V 200 package file 2. Cisco Hyper-V 200 package file for NPE	1. Hv-Cisco-vWAAS-200-6.2.3d-b-68.zip 2. Hv-Cisco-vWAAS-200-6.2.3d-npe-b-68.zip
1. Cisco Hyper-V 750 package file 2. Cisco Hyper-V 750 package file for NPE	1. Hv-Cisco-vWAAS-750-6.2.3d-b-68.zip 2. Hv-Cisco-vWAAS-750-6.2.3d-npe-b-68.zip
1. Cisco Hyper-V 1300 package file 2. Cisco Hyper-V 1300 package file for NPE	1. Hv-Cisco-vWAAS-1300-6.2.3d-b-68.zip 2. Hv-Cisco-vWAAS-1300-6.2.3d-npe-b-68.zip
1. Cisco Hyper-V 2500 package file 2. Cisco Hyper-V 2500 package file for NPE	1. Hv-Cisco-vWAAS-2500-6.2.3d-b-68.zip 2. Hv-Cisco-vWAAS-2500-6.2.3d-npe-b-68.zip

The following table shows Cisco OVA package formats and file format examples for Cisco vCM in Cisco WAAS Version 6.1.x through 6.2.x.

Table 47: Cisco OVA Package Formats for Cisco vCM in Cisco WAAS Version 6.1.x through 6.2.x

Package Format	File Format Example
1. Cisco Hyper-V 100N package file 2. Cisco Hyper-V 100N package file for NPE	1. Hv-Cisco-100N-6.2.3d-b-68.zip 2. Hv-Cisco-100N-6.2.3d-npe-b-68.zip

Installing Cisco vWAAS on Microsoft Hyper-V

This section describes how to install Cisco vWAAS on Microsoft Hyper-V, for vWAAS in Cisco WAAS Version 6.4.1 and later, and for vWAAS in Cisco WAAS Version 5.x to 6.2.x.

- To install Cisco vWAAS on Microsoft Hyper-V for WAAS Version 6.4.1 and later:
  - From the **Cisco WAAS Installer for Hyper-V**, as shown below, enter the number of your Cisco 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 [ ]:
```

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

- To install Cisco vWAAS on Microsoft Hyper-V for Cisco vWAAS in Cisco WAAS Version 5.x to 6.2.x with a VHD template:

  Cisco vWAAS on Microsoft 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 preconfigured and preinstalled Cisco vWAAS images to Microsoft 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.

  There are seven VHD templates available for Cisco vWAAS, and four VHD templates available for Cisco vCM. You can import a pre-configured, model-based VHD file for your deployment. For more information on installing Microsoft Hyper-V with a VHD template, contact your Cisco account representative.

  1. Download the Cisco vWAAS package to the computer where the SCVMM2012 or the 2012 R2 console is installed.
  2. Unzip the Cisco vWAAS package.
  3. Log in to the SCVMM console.
  4. Launch the PowerShell window that is displayed in the SCVMM.
  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
  6. Run the **deploy-vwaas-model-name** PowerShell script.
  7. Run the **deploy-vwaas-model-name** PowerShell script.
  8. If your deployment uses a Cisco vWAAS-12000 or Cisco vWAAS-50000 model, you must enter a maximum amount of memory in Non-Uniform Memory Access (NUMA) 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 Cisco vWAAS in Microsoft Hyper-V (as shown in Step 1 through Step 7).
  9. To enter the maximum amount of memory, follow these steps:
     a. From the **SCVMM console**, choose **Hardware > Processor > NUMA**.

        The **NUMA Configuration** window is displayed.

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

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

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

Activating and Registering vWAAS on Hyper-V

Before you begin

You can manage Cisco vWAAS on Microsoft Hyper-V through the Cisco WAAS Central Manager. Cisco vWAAS on Microsoft Hyper-V supports all the functionalities that are supported by Cisco WAAS devices.

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

When a Hyper-V vWAAS VM is started on the Microsoft Hyper-V, it boots up and prompts you to enter basic boot configuration information, including configuring a Microsoft Hyper-V interface and Cisco WAAS Central Manager IP address.

Procedure

Step 1 Configure the IP address or gateway on the Cisco vWAAS interface. Also configure *name-server*, *domain-name*, and any other static routes, as required.

Step 2 (Optional) If necessary, choose and configure WCCP interception. For more information on configuring WCCP interception, see Choosing WCCP Interception. No configuration is necessary for appnav-controller interception.

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

Step 4 Hyper-V vWAAS connects with the Cisco WAAS Central Manager 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 where a Cisco vWAAS cannot not successfully register with the Cisco WAAS Central Manager:

- If Hyper-V vWAAS cannot register with the Cisco WAAS Central Manager, 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 Cisco WAAS Central Manager, but lose connectivity due to a shutdown or power off. If it remains functional, Cisco vWAAS will continue to optimize the connections in the offline state.
- If you deregister the Hyper-V vWAAS (with the **cms deregister** EXEC command), the Hyper-V vWAAS is removed from service.

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

- The Hyper-V device is displayed under 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 Cisco vWAAS on Microsoft Hyper-V

This section has the following topics:

About Traffic Interception for Cisco vWAAS on Microsoft Hyper-V

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

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

Choosing WCCP Interception

Before you begin

WCCP interception, WCCP GRE, and WCCP L2 are supported for all Cisco vWAAS on Microsoft Hyper-V deployments.

To select WCCP as the interception method for a Cisco 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*.

Procedure

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

Step 2 Choose **Configure** > **Interception** > **Interception Configuration**.

The **Interception Configuration** window appears.

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

Step 4 To enable WCCP on the device, in the **WCCP Settings** area, 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 click **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.

Step 8 (Optional) In the **WCCP Assignment Settings for Load Balancing** area, 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** to **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** to **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:** and select either **Service ID1** or **Service ID2**.

  After you check a source IP, the complementary destination IP address is automatically selected.

Step 9 In the **WCCP Redirect and Egress Settings** area, 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**.

Step 11 In the **Advanced WCCP Settings** area:

a) 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*.

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

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

d) 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 the router takes to detect a WAE failure.

e) 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.

f) 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 (?)

In the **Confirm Password** field, re-enter the password.

Step 12 To save the settings, click **Submit**.

Choosing AppNav Interception

Before you begin

AppNav interception is supported for all Cisco vWAAS on Microsoft Hyper-V deployments, and works the same way as it does in the current ESXi vWAAS models.

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

Procedure

Step 1 From the Cisco 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 the vWAAS device.

Step 4 Click **Submit**.

Operating Guidelines for Cisco vWAAS on Microsoft Hyper-V

This section contains the following topics:

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

Note Multiple deployments of Cisco vWAAS on the same Hyper-V host *in parallel* may cause unexpected results, due to availability of free space when creating Virtual Hard Disks (VHDs). We recommend that you do *not* deploy multiple Cisco vWAAS on Microsoft Hyper-V in parallel, unless you have verified that you have enough free disk space required for the respective Cisco 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 Cisco UCS-E firmware (Version 3.1.2) that is available on the Cisco Download Software Page for UCS E-Series Software, UCS E160S M3 Software.
- Verify that you have installed the critical Microsoft Windows Server updates that is available on the Microsoft Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2 Update Rollup page.

Configuring NTP Settings for Cisco vWAAS on Microsoft Hyper-V

Before you begin

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

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

Procedure

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

From the Microsoft SCVMM:

a) Select **vWAAS VM**.
b) Choose **Settings > Management > Integration Services**.
c) Verify that the **Time synchronization** option is unchecked.
d) Click **OK**.

From the Microsoft 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**.

Cisco vWAAS on Microsoft Hyper-V High Availability Features

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

Live Migration

Microsoft Hyper-V live migration moves the running VMs with no impact on VM availability to the user. It does this by precopying the memory of the migrating VMs to the destination physical host. The administrator, or the script, that initiates the live migration decides 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 that 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 general workflow for initiating and completing a live migration:

1. **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.
2. **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.
3. **Mark modified memory pages**: The utilized pages within the working set are copied to the destination Microsoft Hyper-V physical host. In addition to copying the working set to the destination physical host, Microsoft 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, Microsoft Hyper-V tracks and marks them as modified.
4. **Copy modified memory pages**: During live migration, Microsoft 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 for this stage of live migration.

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 in order to allow all the memory pages to be transferred to the destination physical host.

5. **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.

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

Network Interface Card Teaming

The failure of an individual Microsoft Hyper-V port or virtual network adapter can cause a loss of connectivity for a VM. To prevent this, multiple virtual network adapter are used in a Network Interface Card (NIC) 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 Load Balancing Failover (LBFO).

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. For more information about Cisco vWAAS with SR-IOV, see Cisco vWAAS with Single Root I/O Virtualization.

NIC teaming then works in one of two ways:

- Each VM 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 VM can have a virtual function from one network adapter and a nonvirtual 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

Before you begin

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

- 4-GB Flash
- 48-GB Kdump
- 1500 GB
- 850 GB for disk (for Akamai Connect)

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

Procedure

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) Run 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.

The **DISKPART** prompt is displayed.

Step 3 At the **DISKPART** prompt:

a) Run the **create volume** command to create a new volume on the disk.
b) Run 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.

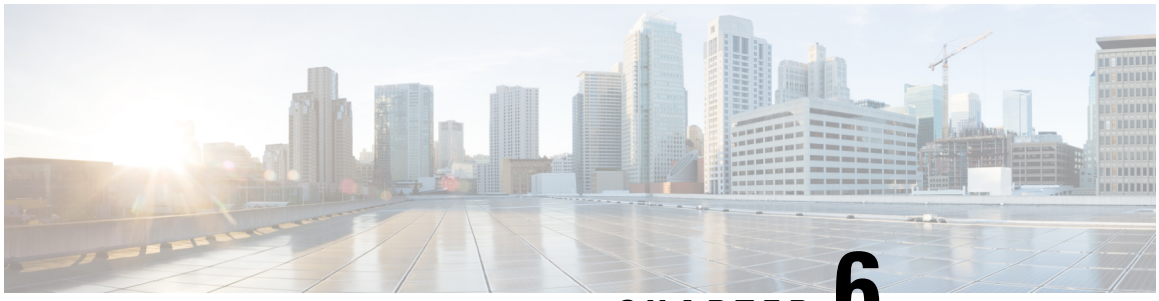
Note the disk number of the disk for which you want to convert formats.

c) Run the **select disk** *disk-number* command.
d) Run the **clean** command to specify that all sectors on the disk are set to zero.

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

e) Run the **convert gpt** command to convert the disk format to GPT format.

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*.



CHAPTER 6

Cisco vWAAS on RHEL KVM, KVM on CentOS, and KVM in SUSE Linux

This chapter describes how to use Cisco vWAAS on RHEL KVM, KVM on CentOS, and KVM in SUSE Linux, and contains the following sections:

About vWAAS on RHEL KVM, KVM on CentOS, and KVM in SUSE Linux

Cisco vWAAS on RHEL KVM is a virtual WAAS appliance that runs on a KVM Hypervisor. The Cisco vWAAS on RHEL KVM solution extends the capabilities of Cisco ISR-WAAS and Cisco vWAAS running on the Cisco UCS-E Series and the Cisco Enterprise Network Compute System (Cisco ENCS) 5400-W Series.

Consider the following interoperability guidelines for Cisco vWAAS on the KVM hypervisor platforms:

- **Cisco vWAAS on RHEL KVM**: Supported for Cisco vWAAS in WAAS Version 6.2.x 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 (Cisco NFVIS). The Cisco NFVIS portal is used to select the tar.gz file to deploy vWAAS.

- **Cisco vWAAS on KVM on CentOS**: Supported for Cisco vWAAS in WAAS version 6.2.3b and later.
- **Cisco vWAAS on KVM in SUSE Linux**: Supported for all Cisco vWAAS and Cisco vCM models that are supported on KVM on CentOS, for Cisco vWAAS in Cisco WAAS Version 6.4.1b and later.

Supported Host Platforms, Software Versions, and Disk Type

The following table shows the platforms and software versions supported for Cisco vWAAS on RHEL KVM, for the PID **OE-VWAAS-KVM** and the device type: **OE-VWAAS-KVM**.

Table 48: Platforms and Software Versions Supported for Cisco vWAAS on RHEL KVM

Earliest Cisco WAAS Version Supported	Cisco Host Platforms	Earliest RHEL and CentOS Host Version Supported	Disk Type
6.2x	• UCS • UCS E-Series	• RHEL Server 7.1 • CentOS Linux 7.2.1511 (Core)	• virtio
6.4.3d	• UCS • UCS E-Series	• RHEL Server 7.5 • RHEL Server 7.6 • CentOS Linux 7.5.1804 (Core) • CentOS Linux 7.6.1810 (Core)	• virtio

Cisco vWAAS on RHEL KVM System Requirements

Cisco 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 Cisco vWAAS on RHEL KVM, and, where applicable, highlights the customizable features.

Note Data disk size varies according to the model shown in the following table. While deploying RHEL KVM, Cisco vWAAS and Cisco vCM should verify that enough disk space is available in the respective partition.

Table 49: Cisco vWAAS on RHEL KVM Supported Configuration

Feature or Component	Description
Platform	Three-disk platform of: • 10 GB system • 4 GB flash • Data disk (customizable, depending on number of connections)
RHEL version for vWAAS on KVM	RHEL 7.2

Feature or Component	Description
Cisco vWAAS 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 Cisco Appnav
Device Emulation	Cisco vWAAS on RHEL KVM uses Quick Emulator-KVM (QEMU-KVM).
Management	Cisco WAAS Central Manager and serial console
Licensing	For information on Cisco vWAAS licensing, contract your Cisco account representative.
MAC address	Customizable

Cisco vWAAS on RHEL KVM in WAAS Version 6.4.1 and Later

This section contains the following topics:

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

For Cisco vWAAS on RHEL KVM in Cisco 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 Cisco vWAAS models for that hypervisor.

Each unified OVA package file is a preconfigured VM 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.

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

- OVA: Cisco-KVM-vWAAS-Unified-6.4.5-b-69.tar
- NPE OVA: Cisco-KVM-vWAAS-Unified-6.4.5-b-69-npe.tar

The unified OVA package for vWAAS on RHEL KVM and 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.xml A 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 Cisco vWAAS on KVM in WAAS Version 6.4.1 and Later

This section contains the following topics:

Note For how to install Cisco vWAAS with Cisco NFVIS on the Cisco ENCS 5400-W 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 Cisco vWAAS on RHEL KVM on CentOS in WAAS Version 6.4.1 and Later
- Using the EzDeploy Script to Deploy Cisco vWAAS on RHEL KVM on CentOS in WAAS Version 6.4.1 and Later

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

Procedure

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

Example:

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

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

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

Before you begin

Use the EzDeploy script (**ezdeploy.sh**) to deploy Cisco vWAAS or vCM on RHEL KVM on CentOS, for vWAAS models up to 6,000 connections.

Procedure

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

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

The **Model Menu** is displayed:

Step 2 After you select the vWAAS model type, the EzDeploy script completes the RHEL KVM/KVM on CentOS deployment.

Cisco vWAAS on RHEL KVM in WAAS Version 5.x to 6.2.x

This section contains the following topics:

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

For Cisco vWAAS on RHEL KVM in Cisco WAAS Version 5.x through 6.2.x, Cisco provides a TAR archive or No Payload Encryption (NPE) TAR archive package for each Cisco vWAAS connection profile and for each Cisco vCM connection profile.

The table shows the files included for deploying Cisco vWAAS on RHEL KVM, and for deploying Cisco vWAAS with Cisco Network Functions Virtualization Infrastructure Software (Cisco NFVIS). For more information, see the Cisco Network Function Virtualization Infrastructure Software Getting Started Guide and see the chapter "Cisco vWAAS with Cisco Enterprise NFVIS."

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

Table 50: OVA Package Format Examples for Cisco vWAAS on RHEL KVM in WAAS Version 5.x to 6.2.x

Package Format	File Format Example
1. Cisco KVM 150 package file 2. Cisco KVM 150 package file for NPE	1. Cisco-KVM-vWAAS-150-6.2.3d-b-68.tar.gz 2. Cisco-KVM-vWAAS-150-6.2.3d-b-68-npe.tar.gz
1. Cisco KVM 200 package file 2. Cisco KVM 200 package file for NPE	1. Cisco-KVM-vWAAS-200-6.2.3d-b-68.tar.gz 2. Cisco-KVM-vWAAS-200-6.2.3d-b-68-npe.tar.gz
1. Cisco KVM 750 package file 2. Cisco KVM 750 package file for NPE	1. Cisco-KVM-vWAAS-750-6.2.3d-b-68.tar.gz 2. Cisco-KVM-vWAAS-750-6.2.3d-b-68-npe.tar.gz
1. Cisco KVM 1300 package file 2. Cisco KVM 1300 package file for NPE	1. Cisco-KVM-vWAAS-1300-6.2.3d-b-68.tar.gz 2. Cisco-KVM-vWAAS-1300-6.2.3d-b-68-npe.tar.gz
1. Cisco KVM 2500 package file 2. Cisco KVM 2500 package file for NPE	1. Cisco-KVM-vWAAS-2500-6.2.3d-b-68.tar.gz 2. Cisco-KVM-vWAAS-2500-6.2.3d-b-68-npe.tar.gz
1. Cisco KVM 6000 package file 2. Cisco KVM 6000 package file for NPE	1. Cisco-KVM-vWAAS-6000-6.2.3d-b-68.tar.gz 2. Cisco-KVM-vWAAS-6000-6.2.3d-b-68-npe.tar.gz

Table 51: OVA Package Format for Cisco vCM in WAAS Version 5.x to 6.2.x

Package Format	File Format Example
1. Cisco KVM 100N package file 2. Cisco KVM 100N package file for NPE	1. Cisco-KVN-vCN-100N-6.2.3d-npe-b-68.tar-gz 2. Cisco-KVN-vCN-100N-6.2.3d-npe-b-68-npe.tar-gz

Table 52: Installation Files for Cisco vWAAS on RHEL KVM and Cisco vWAAS with Cisco NFVIS in 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.	Yes	Yes
• **Manifest file with checksums**	Yes	Yes
• **image_properties.xml** A VM configuration template file used on the Cisco NFVIS platform.	No	Yes
• **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.	No	Yes
• **INSTRUCTIONS.TXT** Describes the procedure for deploying the virtual instance and for using the **launch.sh** file.	Yes	No
• **launch.sh file** For more information, see Using the Launch Script to Deploy Cisco vWAAS on RHEL KVM in WAAS Version 5.x to 6.2.x, on page 110.	Yes	No
• **vm.xml** Configuration file needed for Cisco vWAAS deployment using virtual bridge or Open Virtual Switch (OVS) present in host mac.	Yes	No
• **VM disk images** A 4 GB flash disk, 10 GB system disk, and data disk (data disk size is dependent on your connection profile).	Yes	Yes
• ezdeploy.sh file The script used to deploy Cisco vWAAS on UCS-E. For more information, see Using the EzDeploy Script to Deploy Cisco vWAAS on KVM on UCS-E in WAAS Version 5.x to 6.2.x, on page 111 and Using the EzDeploy Script to Deploy Cisco vWAAS on RHEL KVM on CentOS in WAAS Version 6.4.1 and Later, on page 107.	Yes	No

Installing Cisco vWAAS on KVM in WAAS Version 5.x to 6.2.x

This section contains the following topics:

Using the Launch Script to Deploy Cisco vWAAS on RHEL KVM in WAAS Version 5.x to 6.2.x

Procedure

Step 1 Launch the Cisco 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 the Cisco vWAAS, run the **launch.sh** script:

- To check the prerequisite conditions, run the **./launch.sh check** command.
- To launch Cisco vWAAS using the OVS bridge, run 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 are in working state.

- To launch Cisco vWAAS using macvtap, run the **./launch.sh vm-name macvtap** *interface1-name interface2-name* command.
  - *vm-name*: The specified name of the Cisco vWAAS VM.

- *interface1-name* and *interface2-name*: The specified Ethernet interfaces of the host machine.

Step 6 The Cisco vWAAS is launched

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

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

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

Step 10 To undefine the Cisco vWAAS:

a) Run the **virsh undefine** *vm-name* command.

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

Note If you want to create another Cisco vWAAS of the same model, repeat this procedure. 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 Cisco vWAAS on KVM on UCS-E in WAAS Version 5.x to 6.2.x

Before you begin

Use the EzDeploy script (**ezdeploy.sh**) for simplified deployment of a Cisco vWAAS.

Note The EzDeploy script is not used for the Cisco vCM.

The following are the prerequisites for launching the EzDeploy script:

- To launch the Cisco 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 Cisco WAAS Central Manager registration status)
- Verify the following:
  - There is sufficient disk and RAM memory to deploy another Cisco vWAAS.
  - Compatibility of software versions.
  - Availability and readiness of network connectivity.

Note Because EzDeploy leverages the **launch.sh** script to launch a Cisco 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.

Procedure

Step 1 Launch the Cisco 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, run 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 the **ezdeploy.sh**, you are prompted for bootstrap configuration parameters:

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

  If you have not provided the Cisco vWAAS' bootstrap configuration: the name is set as the name of the guest KVM to be created. not the Cisco vWAAS' host name.

  If you have provided the vWAAS' bootstrap configuration: the Cisco vWAAS' host name is set and used in both instances.

- Cisco vWAAS local IP address and mask
- Default GW IP address: An address on the ISR-4000 series RP that is reachable by the Cisco vWAAS and has external network connectivity
- IP address of the Cisco WAAS Central Manager with which the Cisco vWAAS will register
- One NTP server address, without authentication. If you want to have authentication or multiple NTP servers, use the Cisco WAAS Central Manager to configure these after the Cisco vWAAS is powered up.

- (Optional) DNS server address

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

- The bootstrap configuration is saved in the **bootstrap-cfg.xml** file in the directory created for this KVM.
- The execution log and error log of the script are saved in the **ezdeploy-log.txt** file in the directory created for this KVM.
- For the Cisco 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 the EzDeploy script is run, the Cisco vWAAS is fully up and running. Registration with the specified Cisco WAAS Central Manager and the NTP server are automatically started after installation of their corresponding CLIs.

- (Optional) To view Cisco vWAAS, use the VM GUI or run the **virsh list** command.
- (Optional) To connect to the console, use the VM GUI or run the **virsh console** *vm-name* command.
- (Optional) To power down Cisco vWAAS, run the **virsh destroy** *vm-name* command.
- (Optional) To undefine the Cisco vWAAS:

d) To undefine the vWAAS:

1.Run the **virsh undefine** *vm-name* command.

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

Operating Guidelines for Cisco vWAAS on KVM and KVM on CentOS

This section contains the following topics:

Interoperability Guidelines for Cisco vWAAS on KVM and KVM on CentOS

Consider the following interoperability guidelines for Cisco vWAAS on KVM:

Interoperability guidelines for Cisco WAAS versions and Cisco vWAAS on KVM:

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

Interoperability guidelines for OVS and vWAAS on KVM:

- The Cisco Discovery Protocol (CDP) is not supported for Open Virtual Switch (OVS) on RHEL KVM on CentOS, therefore the show cdp command cannot be used for Cisco vWAAS on RHEL KVM on CentOS.
- For Cisco vWAAS in WAAS Version 6.2.3x and later, there is inline Cisco vWAAS support for the OVS switch, with additional settings in Cisco vWAAS.

  To configure inline Cisco vWAAS support for the OVS switch:

  1. Install CentOS 7.2 on UCS-C240.
  2. Configure OVS switch on the KVM host.
  3. Deploy the KVM vWAAS OVAs with the OVS switch on KVM host.
  4. Power off the Cisco vWAAS.
  5. Add two additional interfaces.
  6. Using the virt-manager, map the bridge ID in Cisco vWAAS:

     ```
     [root@localhost kvm]# virsh edit vwaas-name
     ```

     The domain vWAAS XML configuration is changed.
  7. Using the virt-manager, edit the virtual type:

     ```
     virtualport type='openvswitch'/
     ```
  8. Example:

     ```
     <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 Cisco 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 Cisco vWAAS on RHEL KVM, you must disable Generic Receive Offload (GRO) on the Cisco UCS NIC. Run the **ethtool -K** *nic_interface_name* **gro off** command on the KVM host to disable GRO, for example: **ethtool -K enp3sof2 gro off**. If you do not disable GRO, traffic is not recognized, and packets are discarded.

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

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

Upgrade and Downgrade Guidelines for Cisco vWAAS on KVM

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

- Cisco vWAAS on KVM is used in Cisco WAAS Version 6.2.1 and later. You cannot downgrade Cisco vWAAS on KVM or vCM on KVM devices to a version earlier than Cisco WAAS Version 6.2.1.
- When upgrading Cisco vWAAS, do not upgrade more than five Cisco vWAAS nodes at the same time on a single Cisco UCS device. Upgrading more than five Cisco vWAAS nodes at the same time may cause the Cisco vWAAS devices to go offline and diskless mode.
- For a Cisco vCM-100 model used with the RHEL KVM or KVM on CentOS hypervisor, with the default memory size of 2 GB:

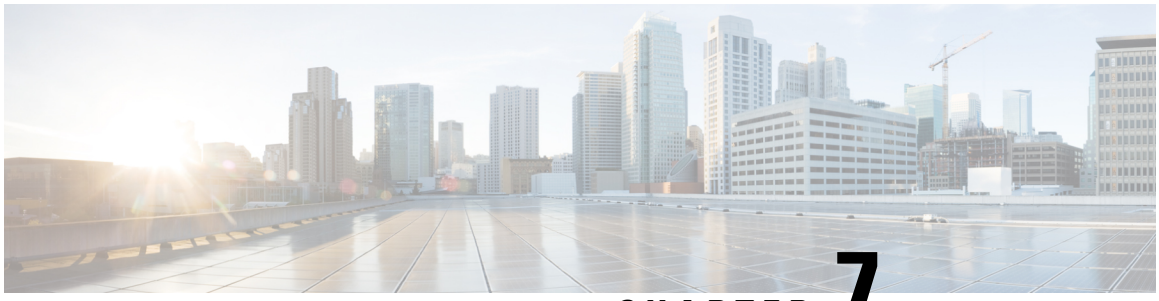
  When you upgrade to Cisco WAAS Version 5.2.1 from an earlier version, or downgrade from Cisco WAAS Version 5.2.1 to an earlier version, and run either the **restore factory-default** command or run the **restore factory-default preserve basic-config** command, the vCM-100 may not come up due to GUID Partition Table (GPT) boot order errors.

  Note 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.

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

  To resolve this situation, follow these steps:

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



CHAPTER 7

Cisco vWAAS on Cisco ENCS 5400-W Series

This chapter describes Cisco vWAAS on the Cisco Enterprise Network Compute System 5400-W Series (Cisco ENCS 5400-W Series) appliance, and contains the following sections:

About the Cisco ENCS 5400-W Series

The Cisco Enterprise Network Compute Series (Cisco ENCS) is used to host the Cisco Enterprise Network Functions Virtualization (Cisco Enterprise NFV) solution. Cisco ENCS is also used to deploy the Cisco NFV Infrastructure Software (Cisco NFVIS), and Cisco and third-party VNFs on Cisco Enterprise NFV. For more information on Cisco NFVIS, see the chapter "Cisco vWAAS with Cisco Enterprise NFVIS."

The following table describes how the Cisco ENCS 5400 Series and the Cisco ENCS 5400-W Series (used with vWAAS) are used with Cisco Enterprise NFV. For more information, see the Cisco 5400 Enterprise Network Compute System Data Sheet.

Table 53: Cisco ENCS 5400 Series and Cisco ENCS 5400-W Series

Cisco ENCS Series	Description
Cisco ENCS 5400 Series	Cisco ENCS-5406, Cisco ENCS-5408, and Cisco ENCS-5412, is a line of compute appliances designed for the Cisco SD-Branch and Enterprise NFV solution.

Cisco ENCS Series	Description
Cisco ENCS 5400-W Series	Cisco ENCS 5406-W, Cisco ENCS 5408-W, and Cisco ENCS 5412-W, is an x86 hybrid platform is designed for the Cisco Enterprise NFV solution, for branch deployment and for hosting Cisco 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** Cisco vWAAS is designed to run in appliance mode or as a Virtualized Network Function (VNF) in three Cisco ENCS 5400-W series models: Cisco ENCS 5406-W, Cisco ENCS 5408-W, Cisco ENCS 5412-W, and three Cisco PIDs: ENCS 5406-K9, ENCS 5408-K9, ENCS 5412-K9.

Cisco vWAAS as VM on Cisco ENCS 5400-W Series:

- For Cisco 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.
- Cisco vWAAS with Cisco Enterprise NFVIS runs on Cisco ENCS 5400-W Series, which is a Cisco x86 hardware platform for branch deployment for routing and hosted applications.
- The following table shows supported Cisco vWAAS models for Cisco ENCS 5406-W, Cisco ENCS 5408-W, and Cisco ENCS 5412-W.

Table 54: Supported Cisco vWAAS Models for Cisco ENCS 5400-W Series

Cisco ENCS-W Model	Processor	CPUs	RAM	Supported Cisco 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

Cisco ENCS 5400-W Models that Replace EOL/EOS Cisco 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.

The following table shows the Cisco ENCS 5400-W Series models that replace the EOS/EOL WAVE models, and the supported Cisco vWAAS models for each Cisco ENCS 5400-W model.

Table 55: Cisco ENCS 5400-W Series Replacment Models for Cisco WAVE Devices

EOS/EOL Cisco WAVE Model	Cisco ENCS 5400-W Model to Replace WAVE Model	Supported Cisco vWAAS Models for Cisco ENCS 5400-W	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	1,300 connections
WAVE-694-16G	ENCS 5412-W	vWAAS-2500	2,500 connections
WAVE-694-24G	ENCS 5412-W	vWAAS-6000-R	6,000 connections

Cisco ENCS 5400-W Hardware Features and Specifications

The following table shows the features and specifications that apply to all three Cisco 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 56: Cisco ENCS 5400-W Series Features and Specifications

Cisco ENCS 5400 Feature/Specification	Description
Cisco vWAAS models supported	One of the following configurations: • Cisco ENCS 5406-W supports vWAAS-200, vWAAS-750 • Cisco ENCS 5408-W supports vWAAS-1300 • Cisco ENCS 5412-W supports vWAAS-2500, vWAAS-6000-R

Cisco ENCS 5400 Feature/Specification	Description
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
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 1 G 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.

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

Cisco vWAAS Bundled Image Install Procedure

Before you begin

- Verify that the specified Cisco ENCS 5400-W Series chassis (Cisco ENCS 5406-W, Cisco 5408-W, or Cisco 5412-W) is already installed and powered up. For information on how to install a Cisco 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 Cisco ENCS 5400-W Series, on page 127. Note that the RAID-1 option is available for Cisco vWAAS in WAAS Version 6.4.1a and later.

Procedure

Step 1 Copy the Cisco vWAAS bundled image file: An ISO file that contains the Cisco NFVIS 3.x.x image (file format “Cisco_NFVIS...”) and the Cisco WAAS 6.x image for your system (file format “WAAS-APPLIANCE...”) on your laptop.

For information on how to upgrade to the Cisco NFVIS 3.x.x version for your system, see Interoperabiity and Upgrade Guidelines for Cisco Enterprise NFVIS, on page 154 in the chapter "Cisco vWAAS with Cisco Enterprise NFVIS."

Step 2 Connect your laptop’s Ethernet port to the Cisco 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 Cisco ENCS-W 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.

The default user name is **admin** and the default password is **password**.

Step 6 Click **Login**.

The **CIMC home page** is displayed.

Note The **Change Password** dialog box appears only when you log in to the CIMC console for the first time. Change the password as needed and click **Save**.

Step 7 In the CIMC home page, choose **Home > Compute > BIOS > Configure Boot Order**.

The **Configure Boot Order** dialog box appears.

Step 8 From the **Device Type** drop-down list, choose **CD/DVD Linux Virtual CD/DVD**. Click **Add**.

Step 9 From the **Device Type** drop-down list, choose **HDD**. Click **Add**.

Step 10 Using the **Up** and **Down** options, set the boot order sequence.

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

Step 11 To complete the boot order setup, click **Apply**.

Step 12 Launch the **KVM console**. You can launch the KVM console from the **CIMC home page** or the **Remote Management** area.

Step 13 In the KVM console, after the KVM console is initialized, map the Cisco vWAAS bundled image by choosing **Server > Remote Presence > Virtual Media** tab on the KVM console.

Step 14 To load the mapped image, use the **Power Cycle System [cold boot]** option under the **KVM Console Power** tab to power off and then power on the device.

Step 15 With the installation running in the background, use your laptop to connect to the CIMC default IP address.

After the installation is successful, the Cisco ENCS-W 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.
```

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

- For Cisco ENCS 5406-W: vWAAS 200 and vWAAS-750 are displayed.

Select one Cisco vWAAS model for Cisco ENCS 5406-W.

- For Cisco ENCS 5408-W: vWAAS-1300 is the only choice displayed.

  Cisco vWAAS-1300 is automatically selected for Cisco ENCS 5408-W.

- For Cisco ENCS 5412-W: vWAAS-2500 and vWAAS-6000-R are displayed.

  Select one model for Cisco ENCS 5412-W.

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

Example:

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

The following table shows the installation times required, by Cisco vWAAS model and number of connections:

Table 57: Installation Times Required, by Cisco vWAAS Model and Number of Connections

Cisco vWAAS Model	Number of Connections	Minimum Cisco NFVIS Installation Time	Minimum Cisco WAAS Installation Time	Minimum Total Installation Time
vWAAS-200	200	60 minutes	15 minutes	75 minutes
vWAAS-750	750	60 minutes	24 minutes	84 minutes
vWAAS-1300	1,300	55 minutes	28 minutes	83 minutes
vWAAS-2500	2,500	67 minutes	34 minutes	101 minutes
vWAAS-6000-R	6,000	66 minutes	38 minutes	104 minutes

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

The new Cisco **OE-ENCS** device is displayed in the Cisco WAAS Central Manager **Devices > All Devices** listing table.

You can view detailed information on the new Cisco OE-ENCS device by choosing **Devices > DeviceName > Dashboard**.

CLI Commands Used with Cisco vWAAS on Cisco ENCS 5400-W

The following table shows the CLI commands used to display information about Cisco vWAAS on Cisco ENCS 5400-W Series.

Table 58: CLI Commands Used with Cisco vWAAS on Cisco ENCS 5400-W Series

Mode	Command	Description
privileged-level EXEC	**copy sysreport disk**	Cisco ENCS 5400-W logs are part of the sysreport generation for debugging.
	reload	Halts the corresponding operation and performs a cold restart of the Cisco vWAAS 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 Cisco NFVIS and BIOS version.
	show version	Displays the version of the Cisco OE-ENCS device, as well as device ID, system restart time, system restart reason, and amount of time for which system has been up.
	shutdown	Powers down the Cisco ENCS 5400-W host or server.
global configuration	**interface virtual**	The internal interface is used for communication between the Cisco NFVIS host and the Cisco WAAS guest. The IP address associated with this interface (virtual 1/0) is assigned automatically by Cisco NFVIS while booting up, and cannot be modified. **Note** The **interface virtual** *slot/port* command cannot be used to configure the Cisco ENCS 5400-W internal interface.

Cisco vWAAS on ENCS 5400-W with Akamai Connect System Requirements

The following table shows memory and disk requirements for Cisco vWAAS on ENCS 5400-W with Akamai Connect, by Cisco vWAAS model

Table 59: Memory and Disk Requirements for Cisco vWAAS on Cisco ENCS 5400-W with Akamai Connect

Cisco vWAAS Model	Cisco ENCS 5400-W Connections	Memory	Data Disk	Akamai Cache
vWAAS-200	200	3 GB	160 GB	100 GB
vWAAS-750	750	4 GB	250 GB	250 GB
vWAAS-1300	1,300	6 GB	300 GB	300 GB
vWAAS-2500	2,500	8 GB	400 GB	350 GB
vWAAS-6000	6,000	11 GB	500 GB	350 GB

Registering and Deploying Cisco vWAAS on a Cisco ENCS 5400-W Device

This section contains the following procedures:

Registering Cisco vWAAS on a Cisco ENCS 5400-W Device

Before you begin

Verify the following:

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

Procedure

Step 1 Power on the Cisco ENCS 5400-W device.

The Cisco vWAAS automatically starts up when the Cisco ENCS 5400-W device is powered on.

Step 2 Using an Ethernet cable, connect your laptop to the MGMT port of the Cisco ENCS 5400-W device.

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

Step 4 Perform the following steps on a MAC system:

a) Choose **Preferences** > **Network** > **Thunderbolt**.
b) From the **Configure IPv4** drop-down list, choose **Manually**.
c) In the **IP Address** field, enter an IP address.
d) In the **Subnet Mask** field, enter **255.255.255.0**.
e) 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 the terminal.

Deploying Cisco vWAAS with Cisco NFVIS on a Cisco ENCS 5400-W Device

Procedure

Step 1 Perform the steps described in Registering Cisco vWAAS on a Cisco ENCS 5400-W Device, on page 125.

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 5400-W device.

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

By default, the Management port on the Cisco ENCS 5400-W device is 192.168.1.1.

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

a) Connect to the Cisco ENCS 5400-W device.

The following status messages are 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
```

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

The following status messages are 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 the device.

Registering the Cisco vWAAS ENCS 5400-W Device with the Cisco WAAS Central Manager

Before you begin

You must register the Cisco vWAAS instance or the Cisco WAAS appliance running in **Accelerator** mode with the Cisco WAAS Central Manager.

Procedure

Step 1 At the Cisco vWAAS instance or the Cisco WAAS appliance that you want to register, enter the following Cisco WAAS Central Manager IP address information:

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

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

```
DC2-WAE-1(config)# cms enable
Registering WAAS Application Engine...
Sending device registration request to Central Manager with address xx.x.xx.xxx
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 Cisco WAAS Central Manager, choose **Devices** > **All Devices**.

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

Step 4 Exit the device.

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

Note Online Insertion Removal (OIR) is not supported on ENCS 5400-W appliances. We recommend that you do not remove or replace the external SSD drives while the ENCS 5400-W appliance is up and running.

This section contains the following topics:

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

Migrating Equipment from No RAID and One SSD to RAID-1 and Two SSDs

Before you begin

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

Consider the following guidelines for mixing drive types in the RAID group:

- SAS + HDD + SATA HDD: Allowed.
- SAS + SSD + SATA SSD: Allowed.
- HDD + SSD: Not allowed.

Consider these best practices for mixing drive types in the RAID group:

- Use either all SAS or all SATA drives in a RAID group.
- Use the same capacity for each drive in the RAID group.
- Never mix HDDs and SSDs in the same RAID group.

Before creating the virtual disk, both drives must be in **Unconfigured Good** state. If a drive is in other status, use the CIMC Web GUI or Cisco WAAS CLI and do the following:

- If disk is in **JBOD** state:
  1. Click the **Storage** tab > **Physical Drive** Info tab.
  2. In the **Actions** area, choose Set Sta**te as Unconfigured Good**.
  3. Confirm that the disk is in **Unconfigured Good** state.
- If disk is in **Foreign Config** state:
  1. Click the **Storage** tab > **Controller** Info tab.
  2. In the **Actions** area, choose **Clear Foreign Config**.
  3. In the **Actions** area, choose **Unconfigured Good**.
  4. Confirm that the disk is in **Unconfigured Good** state.

Procedure

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.

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.

The value for the **Size** drop-down list automatically filled.

1. From the Strip Size drop-down list, choose the strip size (default is 64k).
2. From the **Write Policy** drop-down list, choose the **Write** policy (default is **Write Through**).
3. From the **Access Policy** drop-down list, choose the **Access** policy (default is **Read Write**).
4. From the **Read Policy** drop-down list, choose the **Read** policy (default is **No Read Ahead**).
5. From the **Cache Policy** drop-down list, choose the **Cache** policy (default is **Direct IO**).
6. From the **Disk Cache Policy** drop-down list, choose the **Disk Cache** policy (default is **Unchanged**).

Step 5 Click **Create Virtual Drive**.

Migrating Equipment from RAID-1 and Two SSDs to No RAID and One SSD

Before you begin

Note Online Insertion Removal (OIR) is not supported on ENCS 5400-W appliances. We recommend that you do *not* remove or replace the external SSD drives while the ENCS 5400-W appliance is up and running.

- You must wait for the disk to be completely shut down before you physically remove the disk from the Cisco WAE device. After the RAID removal process is complete, Cisco WAAS generates a disk failure alarm and trap. In addition, a syslog error message is displayed.
- 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 cancel alarm is generated instead.

Procedure

Step 1 To manually shut down the disk, run the **disk disk-name** *diskxx* **shutdown** global configuration 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 Cisco WAE device.

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

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.

Fail-to-Wire on Cisco vWAAS on ENCS 5400-W Series

This section contains the following topics:

About Fail-to-Wire on Cisco vWAAS on ENCS 5400-W Series

Fail-to-Wire (FTW) is a physical layer (Layer 1) bypass that allows interface port pairs to go into bypass mode: so that the hardware forwards packets between these port pairs without software intervention. FTW provides network connectivity when there are software or hardware failures.

The following are the operating guidelines for FTW on Cisco vWAAS on ENCS 5400-W:

- FTW is available for Cisco vWAAS in Cisco WAAS Version 6.4.3 and later.
- Hardware bypass is supported for a fixed set of ports. For example, you can pair Port 1 with Port 2, or Port 3 with Port 4, but you cannot pair Port 1 with Port 4.
- Configuring a standby and port channel in an on-board interface is supported; configuring standby over port channel in an on-board interface is not supported.
- Configuring a standby, port channel, and standby over port channel in an FTW interface is supported.

Fail-to-Wire Traffic Interception Modes

FTW uses two traffic interception modes: inline interception and WCCP.

Inline interception for FTW uses the following operating modes:

- **Interception Mode**: The NIM ports are in interception mode. Two inline groups are created for the four-port NIM card in Cisco vWAAS. The NIM card ports will use fail-to-wire after a failover timeout.
- **Bypass Mode**: You can shut down the inline group, putting the corresponding pair of ports in bypass mode. In bypass mode, traffic coming into Port 0 is redirected to Port 1, and traffic coming into Port 1 is redirected to Port 0.
- **Bypass All Mode**: If the system reloads or if the software experiences an unexpected event, all the inline groups can be put in bypass mode; no Ethernet connection can be established between the devices.

WCCP traffic interception for FTW uses the following operating mode:

- **Standalone Mode**: Each port in the NIM can be used separately. Cisco WAAS can use this mode to enable WCCP interception. The ports of the NIM card do not use fail-to-wire in this mode, and the watchdog timer remains disabled.

Fail-to-Wire Failure Handling

The following list shows how FTW handles different system failure scenarios:

- **Disk issue**: NFVIS detects the disk issue and puts the NIM into bypass mode.
- **NFVIS unexpected event**: FTW detects that the Cisco vWAAS keepalive messages have stopped, and FTW puts the NIM to pass-through FTW.
- **WAAS reload**: The Cisco vWAAS puts the FTW card into FTW mode immediately.
- **WAASnet restarts or experiences an unexpected event**: The FTW NIM card on the vWAAS goes into FTW mode immediately. After the WAASnet datapath is restored, the vWAAS returns the FTW ports to inline mode.

CLI Commands for Port Channel and Standby Interfaces

This section contains the following topics:

Show Commands Used with Port Channel and Standby Interfaces

The following table highlights the **show** commands used with port channel and standby interfaces.

Table 60: show Commands Used with Port Channel and Standby Interfaces

show Command	Description
show statistics f2w	Displays InlineGroup status, including the amount of time, in seconds, since the last keepalive was received, and how many bypass alarms have been received or cleared.
show interface InlineGroup	Displays InlineGroup connection statistics and InlineGroup status, as well as the failover timeout frequency.
show interface InlinePort LAN	Displays InlinePort LAN connection statistics and specific port status of the InlineGroup.
show interface InlinePort WAN	Displays InlinePort WAN connection statistics and specific port status of the InlineGroup.

Creating, Removing, and Showing Port Channel Interfaces

The following example shows how to create a port channel with the **interface portchannel** global configuration command:

```
vWAAS# configure
vWAAS(config)# interface portchannel 1
vWAAS(config-if)# ip address 10.10.10.10 255.0.0.0
vWAAS(config-if)# exit
```

The following example shows how to remove a port channel with the **no interface portchannel** global configuration command:

```
vWAAS# configure
vWAAS(config)# interface portchannel 1
vWAAS(config-if)# ip address 10.10.10.10 255.0.0.0
vWAAS(config-if)# exit
vWAAS(config-if)# no interface portchannel 1
```

Note The **interface port channel** and **no interface port channel** global configuration commands will be saved across reloads if you run the **copy running-config startup-config** command or run the **write-mem** command.

The following example shows a show running config command for a port channel interface:

```
interface PortChannel 1
ip address 10.10.10.10 255.0.0.0
exit
!
interface Virtual 1/0
channel-group 1
exit
interface Virtual 2/0
channel-group 1
exit
```

Creating, Removing, and Showing Standby Interfaces

The following example shows how to create a standby interface with the **interface standby** global configuration command:

```
ENCS-APPLIANCE# configure
ENCS-APPLIANCE(config)# interface standby 1
ENCS-APPLIANCE(config-if)# ip address 10.10.10.10 255.0.0.0
ENCS-APPLIANCE(config-if)# exit
```

The following example shows how to remove a standby interface with the **no interface standby** global configuration command:

```
ENCS-APPLIANCE# configure
ENCS-APPLIANCE(config)# interface standby 1
ENCS-APPLIANCE(config-if)# ip address 10.10.10.10 255.0.0.0
ENCS-APPLIANCE(config-if)# exit
ENCS-APPLIANCE(config-if)# no interface standby 1
```

Note The **interface standby** and **no interface standby** global configuration commands are saved across reloads if you run the **copy running-config startup-config** command or run the **write-mem** command.

The following example shows a **show running config** command for a standby interface:

```
interface Standby 1
 ip address <addr> <netmask>
 exit
!
interface Virtual 1/0
 standby 1 primary
 exit
interface Virtual 2/0
```

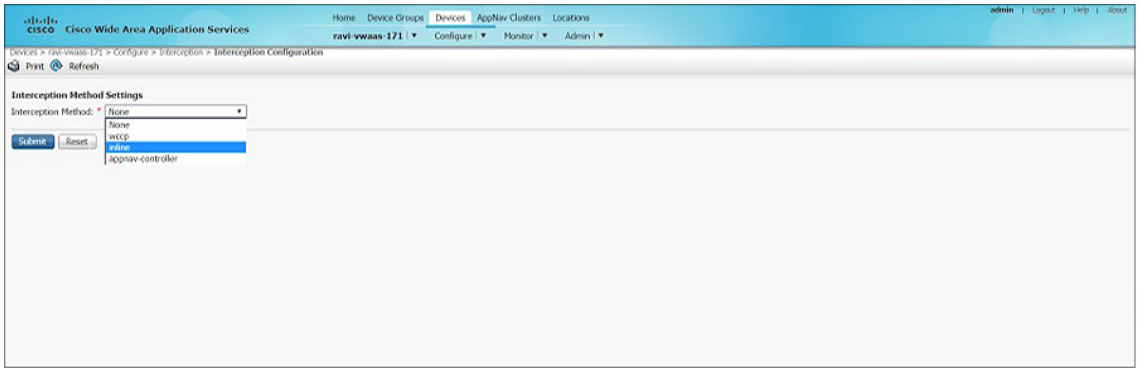
```
standby 1
exit
```

Configuring Inline Interception for FTW on a Cisco ENCS 5400-W Device

Procedure

Step 1 To configure inline interception for FTW with the Cisco WAAS Central Manager, choose **Devices** > **DeviceName** > **Configure** > **Interception** > **Interception Configuration**.

Figure 31: Cisco WAAS Central Manager Interception Method Configuration Window



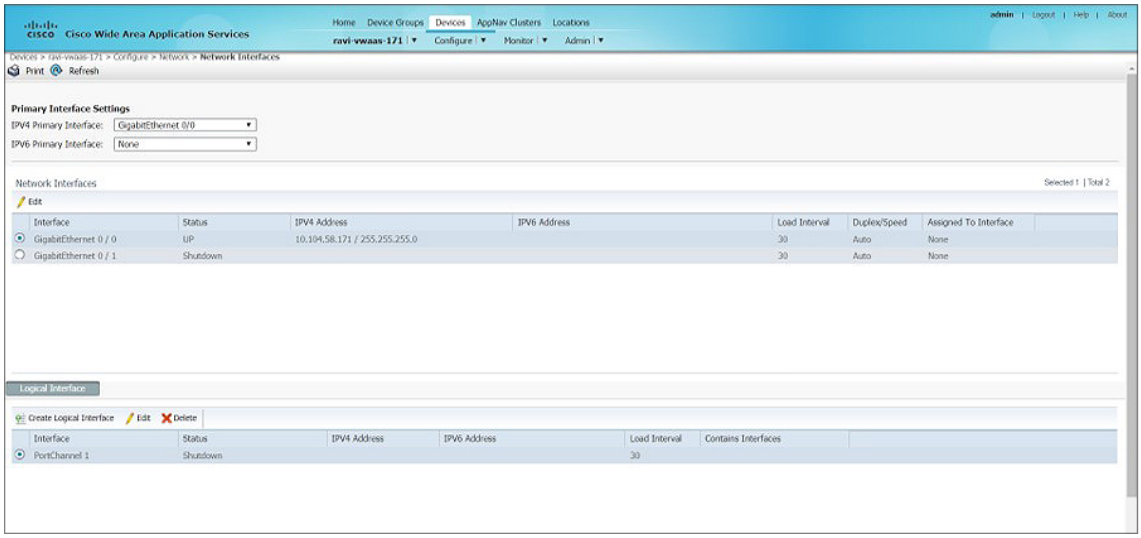
Note To configure inline interception with the Cisco WAAS CLI, see the optional Step 7.

Step 2 At the **Interception Method** drop-down list, choose **Inline**.

Step 3 Click **Submit**.

Step 4 Choose **Devices** > **DeviceName** > **Configure** > **Network** > **Network Interfaces**.

Figure 32: WAAS Central Manager Network Interfaces Window



Step 5 In the **Primary Interface Settings** area, from the **IPv4 Primary Interface** drop-down list, choose the interface that should be the primary interface.

Step 6 From the **IPv6 Primary Interface** drop-down list, choose **None**.

For information on the **Network Interface** table listing or the **Logical Interface** table listing, see the "Configuring Network Interfaces" section in the "Configuring Network Settings" chapter of the *Cisco Wide Area Application Services Configuration Guide*.

Step 7 (Optional) To configure inline interception for FTW on a Cisco ENCS 5400-W device, use the commands shown in the following table.

Table 61: Cisco WAAS CLI Commands for Inline Interception

Mode	Command	Description
Global Configuration	**(config) inline failover timeout {1 | 3 | 5 | 25}**	Configures the failover timeout for the inline interfaces. Valid values are **1**, **3**, **5**, or **25 seconds**. The default value is **3**.
	(config) interception-method inline	Enables inline traffic interception.
	(config) interface InlineGroup *slot/groupnumber*	Configures an inline group interface.
EXEC	**show interface inlinegroup** *slot/groupnumber*	Displays the inline group information and the slot and inline group number for the selected interface.

Fail-to-Wire Upgrade and Downgrade Guidelines

Consider the following guidelines for upgrading or downgrading a Cisco WAAS device with FTW:

- FTW is not supported for Cisco vWAAS in Cisco WAAS versions earlier than WAAS 6.4.3.
- In a mixed version Cisco WAAS network with FTW, the Cisco WAAS Central Manager must be running Cisco WAAS Version 6.4.3 or later.

Upgrade and Downgrade Guidelines for Cisco vWAAS on Cisco ENCS 5400-W

Consider the following for upgrading or downgrading a Cisco vWAAS device on Cisco ENCS 5400-W:

- You can use the Cisco WAAS Central Manager or the Cisco WAAS CLI to upgrade a Cisco vWAAS on a Cisco ENCS 5400-W device to Cisco WAAS and Cisco NFVIS versions shown in the following table:

Table 62: Cisco WAAS and NFVIS Versions for Cisco ENCS 5400-W

Cisco WAAS Version	Supported Cisco NFVIS Version
6.4.5a	4.12
6.4.5	3.11.1
6.4.3e	4.12
6.4.3d	3.11.1
6.4.3c	3.10.1
6.4.3b	3.10.1
6.4.3a	3.10.1
6.4.3	3.9.1
6.4.1x	3.7.1

Note If you are running nfvis-371-waas-641a or nfvis-371-waas-641b on a Cisco ENCS 5400-W device, before upgrading Cisco NFVIS, upgrade to Cisco WAAS Version 6.4.3.

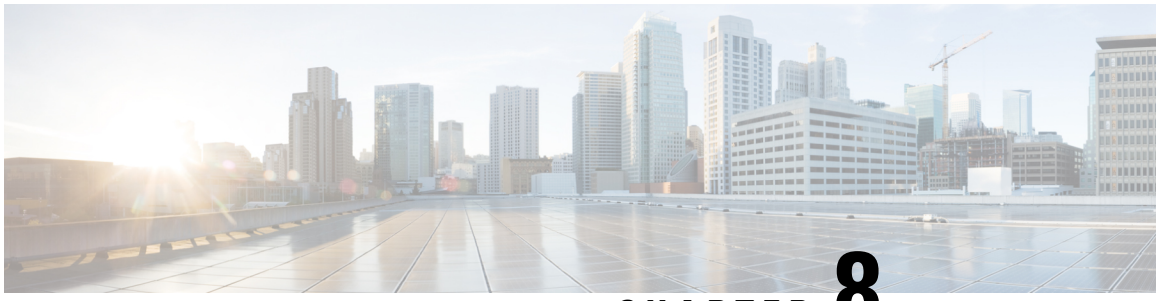
- You can use the Cisco WAAS Central Manager to upgrade from the device level and the device group level. To use the Cisco WAAS Central Manager to upgrade a Cisco vWAAS on a Cisco ENCS 5400-W device:

  1. Use Telnet to reach the Cisco vWAAS device.
  2. Update the Cisco WAAS Central Manager's IP address.
  3. Log in to the Cisco WAAS Central Manager.

- The Cisco WAAS 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 Cisco WAE, a virtual Cisco WAE, and a Cisco ENCS 5400-W platform to a Cisco WAAS version earlier than Cisco WAAS Version 6.4.1, the Cisco WAAS Central Manager initiates the downgrade process only for the physical and virtual Cisco WAEs, but not for the Cisco ENCS 5400-W platform.

- For upgrade and downgrade guidelines for Cisco vWAAS with Cisco NFVIS, see the chapter "Cisco vWAAS with Cisco Enterprise NFVIS."



CHAPTER 8

Cisco vWAAS on Cisco CSP 5000-W Series

This chapter describes Cisco vWAAS on the Cisco Cloud Services Platform, 5000-W Series (Cisco CSP 5000-W Series) appliance, and contains the following sections:

About the Cisco CSP 5000-W Series

The Cisco Cloud Services Platform 5000 Series for WAAS (Cisco CSP 5000-W Series) is a Cisco open x86 hardware platform for deployment of Cisco datacenter Network Functions Virtualization (VNFs), and provides the following features:

- Cisco CSP 5000-W Series contains an embedded KVM CentOS hypervisor, and enables you to monitor and manage the lifecycle of vWAAS on NFVIS.
- The Cisco CSP 5000-W Series enables you to quickly deploy any Cisco network virtual service through a simple, built-in, native GUI, Cisco WAAS CLI, or Representational State Transfer (REST) API.
- Cisco vWAAS on the Cisco CSP 5000-W platform supports off-path deployment for WCCP and Cisco AppNav traffic interception. However, the Cisco AppNav I/O Module (Cisco AppNav IOM) is not supported on the Cisco CSP 5000-W platform.
- Three Cisco CSP 5000-W Models are supported for Cisco vWAAS
  - Cisco CSP 5228-W (12,000 connections): For Cisco vWAAS-12000
  - Cisco CSP 5228-W (50,000 connections): For Cisco vWAAS-50000
  - Cisco CSP 5436-W (150,000 connections): For Cisco vWAAS-150000

Table 63: Cisco CSP 5000-W: Replaced and Supported Models

Cisco CSP 5000-W Model	Connections	EOS/EOL Cisco WAVE Model Replaced	Supported Cisco vWAAS Model
CSP 5228-W	12,000	WAVE-7541	vWAAS-12000
CSP 5228-W	50,000	WAVE-7571	vWAAS-50000
CSP 5436-W	150,000	WAVE-8541	vWAAS-150000

These Cisco CSP 5000-W models replace three End-of-Sale and End-of-Life (EOS and EOL) Cisco WAVE models. The following table shows the corresponding Cisco CSP 5000-W and EOS and EOL Cisco WAVE models, the supported Cisco vWAAS models, and the Cisco UCS model used with CSP 5000-W.

For more information, see the End-of-Sale and End-of-Life Announcement for the Cisco WAVE 294, 594, 694, 7541, 7571 and 8541.

Cisco CSP 5000-W Hardware Features and Specifications

Consider the following guidelines for using the Cisco CSP 5000-W Series:

- The dedicated management port on the device is used for CIMC connectivity.
- The first port on the four-port 1-G (I350) card is used for Cisco NFVIS management.
- We recommend that you use CSP-SFPs (Intel) to connect the Intel X520-DA2 10-Gbps ports on both sides of end-to-end connections.

The following list shows the specifications for each Cisco CSP 5000-W model used with Cisco vWAAS.

- Specifications for Cisco CSP 5228-W for Cisco vWAAS 12000:
  - **CPU**: 16 core
  - **CPU speed**: 2.2. GHz
  - **Connections**: 12,000
  - **Memory**: 52 GB
  - **Storage**: 1.5 TB
  - **Network Interface Card** and **RAID**:
    - **PCIe Slot 1**: Intel X520-DA2 10-Gbps 2-port NIC (2x10-GB fiber interfaces)

      RAID:
    - **PCIe Slot 2**: Intel i350 Quad Port 1-GB Adapter
  - **RAID**: Cisco 12-G Modular RAID controller with 2-GB cache, RAID 10
  - **Hardware Platform**: Cisco UCS-220-M5

- Specifications for Cisco CSP 5228-W for Cisco vWAAS 50000:
  - **CPU**: 20 core
  - **CPU speed**: 2.2 GHZ
  - **Connections**: 50,000
  - **Memory**: 76 GB
  - **Storage**: 2.3 TB
  - **Network Interface Card**:
    - **PCIe Slot 1**: Intel X520-DA2 10-Gbps 2-port NIC (2x10-GB fiber interfaces)
    - **PCIe Slot 2**: Intel i350 Quad Port 1-GB Adapter
  - **RAID**: Cisco 12-G Modular RAID controller with 2-GB cache, RAID 10
  - **Hardware Platform**: Cisco UCS-220-M5
- Specifications for Cisco CSP 5436-W for Cisco vWAAS-150000:
  - **CPU**: 28 core
  - **CPU speed**: 3.0 GHz
  - **Connections**: 150,000
  - **Memory**: 100 GB
  - **Storage**: 4.5 TB
  - **Network Interface Card**:
    - **PCIe Slot 1**: Intel X520-DA2 10-Gbps 2-port NIC (2x10-GB fiber interfaces)
    - **PCIe Slot 2**: Intel i350 Quad Port 1-GB Adapter
  - **RAID**: Cisco 12-G Modular RAID controller with 2GB cache, RAID 10
  - **Hardware Platform**: Cisco UCS-240-M5

For more information on RAID configuration, see the Cisco UCS Servers RAID Guide.

Cisco vWAAS on Cisco CSP 5000-W with Akamai Connect

Consider the following guidelines for Cisco vWAAS on Cisco CSP 5000-W with Akamai Connect:

- Cisco CSP 5000-W devices have fixed resources. Therefore the memory on each device remains the same with or without Akamai Connect enabled.
- As shown in the following table, a fourth disk is required for Cisco vWAAS on Cisco CSP 5000-W with Akamai Connect.

Table 64: System Requirements for Cisco vWAAS on Cisco CSP 5000-W with Akamai Connect

Cisco CSP 5000-W Model	Supported Cisco vWAAS Model	Memory Requirement without Akamai Connect	Fourth Disk Required When Akamai Connect is Enabled
CSP 5228-W	vWAAS-12000	18 GB	750 GB
CSP 5228-W	vWAAS-50000	48 GB	850 GB
CSP 5436-W	vWAAS-150000	96 GB	1500 GB

For more information, see the chapter "Cisco vWAAS with Akamai Connect."

Deploying, Registering, and Configuring Cisco vWAAS on Cisco CSP 5000-W

This section contains the following topics:

Workflow for Deploying, Registering, and Configuring Cisco vWAAS on Cisco CSP 5000-W

The following table shows the workflow for deploying, registering, and configuring Cisco vWAAS on Cisco CSP 5000-W.

Table 65: Workflow for Deploy, Registering, and Configuring Cisco vWAAS on Cisco CSP 5000-W

Task	Description or Section
1. Install the Cisco vWAAS on Cisco CSP 5000-W.	Installing Cisco vWAAS on a Cisco CSP 5000-W Device, on page 140.
2. Register the Cisco CSP 5000-W device with the Cisco WAAS Central Manager.	Registering or Deregistering a Cisco CSP 5000-W Device with the Cisco WAAS Central Manager, on page 145
3. Enable Akamai Connect.	Cisco vWAAS with Akamai Connect, on page 157
4. Check Accelerator status.	To confirm that the operational status of accelerators is **Running**, run the **show accelerator** EXEC command.
5. Configure WCCP traffic interception.	The "Configuring Traffic Interception" chapter of the Cisco Wide Area Application Services Configuration Guide for your Cisco WAAS version.

Installing Cisco vWAAS on a Cisco CSP 5000-W Device

Cisco CSP 5000-W is a bundled solution and is shipped with a pre-installed image.

To install any of the three supported Cisco vWAAS models on the supported Cisco CSP 5000-W device, run the following **show** EXEC commands to verify that all hardware details for the CSP 5000-W device are displayed correctly.

- **show version**: Verifies that the Cisco WAAS version is Version 6.4.3a or later.
- **show tfo detail**: Verifies the number of Transport Flow Optimization (TFO) connections depending on the Cisco vWAAS model.
- **show hardware**: Validates the CPU and memory depending on the Cisco vWAAS model.
- **show inventory**: Validates the PID depending on the Cisco vWAAS model.

Configuring Port Channel and Standby Interfaces

This section contains the following topics:

Configuring a Port Channel Interface

Consider the following guidelines for configuring a port channel interface:

- To provide increased bandwidth and redundancy, a port channel bundles individual interfaces within these NIC modules:
  - **Virtual 1/0** and **2/0**: 10 G Ethernet interface
  - **Virtual 3/0** and **3/1**: 10 G fiber interface

    For fiber connectivity, Intel SFP+ is required for connecting the Intel X520-DA2 10-Gbps two-port NIC (2x10-GB Fiber interfaces).
  - **Virtual 4/0**, **4/1**, and **4/2**: 1 G Ethernet interface
- Port channeling load balances traffic across physical interfaces. The port channel stays operational as long as at least one physical interface within the port channel is operational.
- You create a port channel by bundling compatible interfaces. You can configure and run either static port channels or ports channels running the Link Aggregation Control Protocol (LACP). Standby provides aggregation of several physical links into a logical one, but only for the purpose of furnishing fault-tolerance.
- The following CLI commands are used in the context of port channels:
  - To create a port channel:

```
CSP-APPLIANCE#config
CSP-APPLIANCE(config)#interface portchannel 1
CSP-APPLIANCE(config-if)#ip address <addr> <mask>
CSP-APPLIANCE(config-if)#exit
```

  - To remove a port channel:

```
CSP-APPLIANCE#config
CSP-APPLIANCE(config)#interface portchannel 1
CSP-APPLIANCE(config-if)#no ip address <addr> <mask>
CSP-APPLIANCE(config-if)#exit
CSP-APPLIANCE(config)#no interface portchannel 1
```

- To configure a port channel group for a network interface, run the **(config-if) channel-group** command:

```
CSP-APPLIANCE(config)#interface GigabitEthernet 1/0
CSP-APPLIANCE(config-if)#channel-group 1
```

- To show the running configuration:

```
interface PortChannel 1
  ip address <addr> <netmask>
  exit
!
interface Virtual 4/0
  channel-group 1
  exit
interface Virtual 4/1
  channel-group 1
  exit
interface Virtual 4/2
  channel-group 1
  exit
```

The following figure shows annotated output for the **show running-config interface** command:

```
NO-HOSTNAME# show running-config interface
interface Virtual 1/0
ip address 1.1.1.1 255.255.255.0
exit                                  Onboard 10G          These are the
interface Virtual 2/0                 interfaces (X550)    onboard interfaces.
ip address 2.2.2.2 255.255.255.0
exit
interface Virtual 3/0                 10G interfaces in    This card goes in PCI
ip address 3.3.3.3 255.255.255.0      PCI slot (X250)      Slot 1 for both CSP-
exit                                                       5228 and CSP-5436
interface Virtual 3/1
ip address 4.4.4.4 255.255.255.0
exit
interface Virtual 4/0
ip address 5.5.5.5.5 255.255.255.0
exit
interface Virtual 4/1                 3 * 1G interfaces    This card goes in Slot
ip address 6.6.6.6. 255.255.255.0     (I350)               2 for CSP-5228
exit                                                       and Slot 4 for CSP-5436.
interface Virtual 4/2
ip address 7.7.7.7 255.255.255.0
```

- To show port channel or standby interface statistics:

```
CSP-5228#sh interface standby 1
Interface Standby 1 (2 member interface(s)):
Virtual 3/0 (active) (primary) (in use)
Virtual 3/2 (active)
---------------------
Ethernet Address                : 52:54:00:42:4f:a6
Internet Address                : 2.93.82.20
Netmask                         : 255.255.255.240
IPv6 Enabled                    : No
Admin State                     : Up
Operation State                 : Running
Maximum Transfer Unit Size      : 1500
Input Errors                    : 0
Input Packets Dropped           : 0
Packets Received                : 94939473
Output Errors                   : 0
Output Packets Dropped          : 0
```

```
Load Interval                    : 30
Input Throughput                 : 0 bits/sec, 0 packets/sec
Output Throughput                : 0 bits/sec, 0 packets/sec
Packets Sent                     : 93430587
Interception Statistics
CSP-5228#
CSP-5228#sh interface portChannel 1
Interface PortChannel 1 (3 member interface(s)):
Virtual 3/0 (active)
Virtual 3/1 (active)
Virtual 3/2 (active)
---------------------
Ethernet Address                 : 52:54:00:42:4f:aa
Internet Address                 : 22.22.22.2
Netmask                          : 255.255.255.0
IPv6 Enabled : No
Admin State : Up
Operation State : Down
Maximum Transfer Unit Size       : 1500
Input Errors                     : 0
Input Packets Dropped            : 0
Packets Received                 : 21568
Output Errors                    : 0
Output Packets Dropped           : 0
Load Interval                    : 30
Input Throughput                 : 2290669644 bits/sec, 159 packets/sec
Output Throughput                : 2290649224 bits/sec, 0 packets/sec
Packets Sent                     : 41
CSP-5228#
```

- To configure an interface to be a standby for another interface, run the **(config-if) standby** command:

```
CSP-APPLIANCE#configure
CSP-APPLIANCE#interface standby 1
CSP-APPLIANCE(config-if)#
```

Configuring a Standby Interface

You can create two port channel groups and use them as the active and backup members of a standby group. Consider the following guidelines for configuring a standby interface:

- The standby interface has two modes:
  - **Active-backup mode**: Implements the standby interface and provides fault tolerance. Only one server interface in the bond is active. A different server interface becomes active only if the active server interface fails.
  - **SRC-DST-IP-PORT mode**: Provides load balancing and fault tolerance. In this mode, all the frames between the same source and the same destination use the same link.
- The following CLI commands are used in the context of a standby interface:
  - To create a standby interface:

```
CSP-APPLIANCE#config
CSP-APPLIANCE(config)#interface Standby 1
CSP-APPLIANCE(config-if)#ip address <addr> <mask>
CSP-APPLIANCE(config-if)#exit
```

  - To remove a standby interface:

```
CSP-APPLIANCE#config
CSP-APPLIANCE(config)#interface Standby 1
CSP-APPLIANCE(config-if)#no ip address <addr> <mask>
CSP-APPLIANCE(config-if)#exit
CSP-APPLIANCE(config)#no interface Standby 1
```

- To show the running configuration:

```
interface Standby 1
  ip address <addr> <netmask>
  exit
!
interface Virtual 1/0
  standby 1 primary
  exit
interface Virtual 2/0
  standby 1
  exit
```

- To show port channel or standby interface statistics:

```
CSP-5228#sh interface standby 1
Interface Standby 1 (2 member interface(s)):
Virtual 3/0 (active) (primary) (in use)
Virtual 3/2 (active)
---------------------
Ethernet Address               : 52:54:00:42:4f:a6
Internet Address               : 2.93.82.20
Netmask                        : 255.255.255.240
IPv6 Enabled                   : No
Admin State                    : Up
Operation State                : Running
Maximum Transfer Unit Size     : 1500
Input Errors                   : 0
Input Packets Dropped          : 0
Packets Received               : 94939473
Output Errors                  : 0
Output Packets Dropped         : 0
Load Interval                  : 30
Input Throughput               : 0 bits/sec, 0 packets/sec
Output Throughput              : 0 bits/sec, 0 packets/sec
Packets Sent                   : 93430587
Interception Statistics
CSP-5228#
CSP-5228#sh interface portChannel 1
Interface PortChannel 1 (3 member interface(s)):
Virtual 3/0 (active)
Virtual 3/1 (active)
Virtual 3/2 (active)
---------------------
Ethernet Address               : 52:54:00:42:4f:aa
Internet Address               : 22.22.22.2
Netmask                        : 255.255.255.0
IPv6 Enabled                   : No
Admin State                    : Up
Operation State                : Down
Maximum Transfer Unit Size     : 1500
Input Errors                   : 0
Input Packets Dropped          : 0
Packets Received               : 21568
Output Errors                  : 0
Output Packets Dropped         : 0
Load Interval                  : 30
Input Throughput              : 2290669644 bits/sec, 159 packets/sec
Output Throughput             : 2290649224 bits/sec, 0 packets/sec
```

```
Packets Sent                    : 41
CSP-5228#
```

Registering or Deregistering a Cisco CSP 5000-W Device with the Cisco WAAS Central Manager

This section contains the following topics:

Registering or Deregistering a Cisco CSP 5000-W Device with the Cisco WAAS Central Manager

This section contains the following topics:

Registering a Cisco CSP 5000-W Device with the Cisco WAAS Central Manager

Procedure

Step 1 At the Cisco datacenter CSP 5000-W CLI, enter the Cisco WAAS Central Manager IP address, for example: 10.78.99.141:

```
DC-CSP-WAE(config)#central-manager address 10.78.99.141
DC-CSP-WAE(config)#
DC-CSP-WAE(config)#end
DC-CSP-WAE#show running-config | i central central-manager address 10.78.99.141
```

Note The IP address configured in the Cisco NFVIS management port cannot be accessed from the Cisco WAAS Central Manager.

Step 2 To register the Cisco CSP 5000-W device, run the **cms** command :

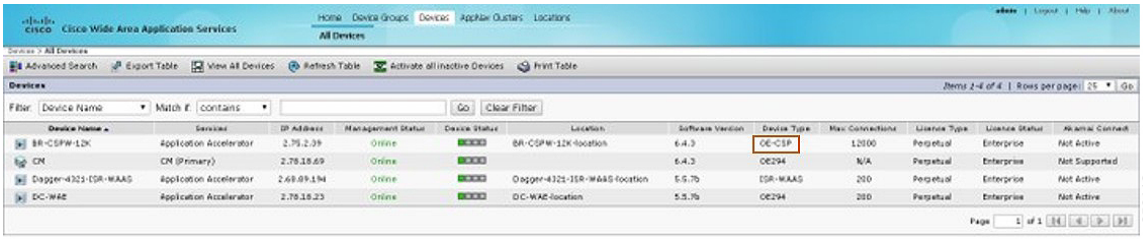
```
DC-CSP-WAE(config)#cms enable
Registering WAAS Application Engine...
Sending device registration request to Central Manager with address 10.78.99.141
Please wait, initializing CMS tables
Successfully initialized CMS tables
Registration complete.
```

Step 3 To preserve the running configuration, run the **copy running-config startup-config** command.

Note If you do not run the **copy running-config startup-config** command, the management service will not be started on reload, and the Cisco WAAS Central Manager will show the node as **Offline**.

Step 4 After the device is registered, it is displayed in the Cisco WAAS Central Manager as **OE-CSP**.

Figure 33: Cisco OE-CSP Displayed in the WAAS Central Manager Device Listings Window



Step 5 To view the Cisco CSP 5000-W device in the dashboard, choose **Devices** > *device-name* > **Dashboard**.

The **Device Dashboard** window is displayed. Information displayed for the device includes device model, IP address, interception method, and device-specific charts.

Step 6 You can also use the Cisco CSP 5000-W CLI to view device information:

```
DC-CSP-WAE#show cms info
Device registration information :
Device Id                              = 1769435
Device registered as                   = WAAS Application Engine
Current WAAS Central Manager           = 10.78.99.142
Registered with WAAS Central Manager   = 10.78.99.142
Status                                 = Online
Time of last config-sync               = Fri Jun 3 14:41:26 2018
CMS services information :
Service cms_ce is running
```

Deregistering a Cisco CSP 5000-W Device

Procedure

Step 1 At the Cisco datacenter CSP 5000-W CLI, use the cms deregister command to deregister the device:

```
DC-CSP-WAE#cms deregister

Deregistering WAE device from Central Manager will result in loss of data on encrypted
file systems.

If secure store is initialized and open, clear secure store.

If encrypted MAPI is enabled, windows-domain encryption-service identities will be
disabled. The passwords must be re-entered again the next time the WAE joins
a central manager.

Do you really want to continue (yes|no) [no]?yes
```

Step 2 To initiate the deregistering process, click **yes**. The system displays the following status messages:

```
Disabling management service.
management services are already disabled.
Sending de-registration request to CM
SSMGR RETURNING: 7 (Success)
Removing cms database tables.
Re-initializing SSL managed store and restarting SSL accelerator.
```

```
Deregistration complete. Save current cli configuration using 'copy running-config
startup-config' command because CMS service has been disabled.
```

Step 3 To preserve the running configuration, run the **copy running-config startup-config** command.

Note If you do not run the **copy running-config startup-config** command, the management service will not be started on reload, and the Cisco WAAS Central Manager will show the node as **Offline**.

CLI Commands Used with Cisco vWAAS on Cisco CSP 5000-W

The following table shows the CLI commands used with Cisco vWAAS on Cisco CSP 5000-W.

Table 66: CLI Commands used with Cisco vWAAS on Cisco CSP 5000-W

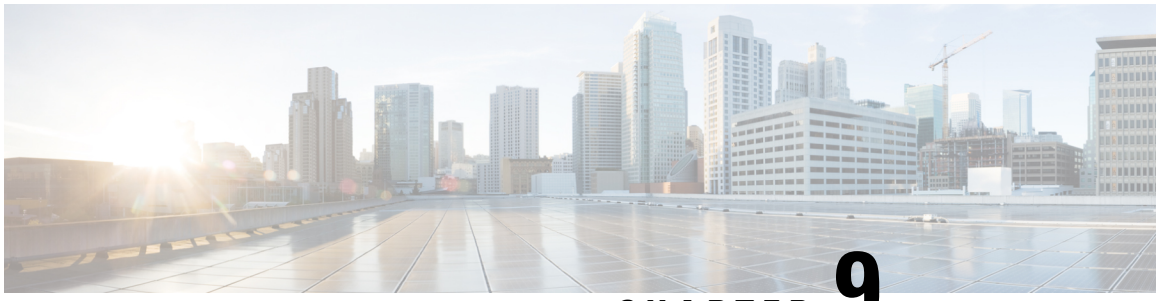
Mode	Command	Description
Global Configuration	**(config) interface PortChannel**	Configures a port-channel interface.
Interface Configuration	**(config-if) channel-group**	Configures the port channel group for a network interface.
privileged-level EXEC	**copy sysreport disk**	Cisco CSP 5000-W logs will be part of the **sysreport** generation for debugging.
	reload	Restarts the Cisco vWAAS VM.
	show hardware	Validates the CPU and memory depending on the Cisco vWAAS model.
	show inventory	Validates the PID depending on the Cisco vWAAS model.
	show running-config interface	Displays a Cisco WAAS device current running configuration on the terminal.
	show tfo detail	Verifies the number of TFO connections depending on the Cisco vWAAS model.
user-level EXEC and privileged-level EXEC	**show version**	Verifies that the Cisco WAAS version is Cisco WAAS Version 6.4.3a or later.
privileged-level EXEC	**shutdown**	Powers off the Cisco CSP 5000-W device.

Upgrade and Downgrade Guidelines for Cisco vWAAS on Cisco CSP 5000-W

Consider the following upgrade and downgrade guidelines for Cisco vWAAS on Cisco CSP 5000-W:

- Upgrade is supported for the Cisco vWAAS bundled image in Cisco WAAS Version 6.4.3a and later, and the associated Cisco NFVIS version used with Cisco WAAS.
- When there is more than one device type present at the Device Group level, the Cisco WAAS Central Manager supports upgrade and downgrade that is supported for each device type.
- Downgrade is not supported for Cisco vWAAS for Cisco WAAS versions earlier than Cisco WAAS 6.4.3a.

Note Cisco CSP 5000-W devices run with specific Cisco vWAAS and Cisco NFVIS versions. We recommend that you upgrade Cisco vWAAS and Cisco NFVIS together; do not upgrade each of these separately. For more information, see "Upgrade Guideliknes for Cisco Enterprise NFVIS" in the chapter “Cisco vWAAS with Cisco Enterprise NFVIS."



CHAPTER 9

Cisco vWAAS with Cisco Enterprise NFVIS

This chapter describes Cisco vWAAS with Cisco Enterprise Network Functions Virtualization Infrastructure Software (Cisco Enterprise NFVIS).

This chapter contains the following sections:

About Cisco vWAAS with Cisco Enterprise NFVIS

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

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

Cisco Enterprise NFVIS contains the following features:

- **Cisco ENCS 5400-W Series**: Cisco vWAAS with Cisco Enterprise NFVIS is deployed on the Cisco Enterprise Network Compute System (Cisco ENCS 5400-W) Series. For more information on the ENCS 5400-W Series, see the chapter "Cisco vWAAS on Cisco ENCS 5400-W Series."
- **Cisco Enterprise NFV**: 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, and WAN acceleration on a supported Cisco device, eliminating the need to add a physical device for every network function.
- **Monitoring**: Monitors all the parameters of the deployed Cisco vWAAS, including memory, storage, and CPU, and monitors memory, storage, and CPU utilization of the Cisco vWAAS.
- **Traffic verification**: Verifies traffic flows through Cisco vWAAS by monitoring the 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 connect it to a VLAN.

Platforms Supported for Cisco vWAAS with Cisco Enterprise NFVIS

The following table shows the platforms and software versions supported for Cisco vWAAS with Cisco Enterprise NFVIS.

Table 67: Platforms and Software Versions Supported for Cisco vWAAS with Cisco NFVIS

PID and Device Type	Earliest Cisco WAAS Version Supported	Host Platforms	Earliest Host Version Supported	Disk Type
PID: OE-CSP Device Type: OE-CSP	6.4.3a	Cisco CSP 5000-W Series	Cisco Enterprise NFVIS 3.10.1	virtio
PID: OE-VWAAS-ENCS Device Type: OE-VWAAS-ENCS	6.4.1	Cisco ENCS 5400-W Series	Cisco Enterprise NFVIS 3.7.1	virtio
PID: OE-VWAAS-KVM Device Type: OE-VWAAS-KVM	6.2.x	Cisco UCS-E Series	Cisco Enterprise NFVIS 3.7.1	virtio

Cisco vWAAS with Cisco Enterprise NFVIS on Cisco ENCS 5400-W provides the following capabilities:

- **Enterprise Application Optimization**: Branch to branch, and branch to data center optimization of application traffic, either within or outside of a Cisco iWAN solution. This includes traditional WAAS WAN optimization functions, as well as the deployment of other iWAN solution features that are inherent in Cisco IOS-XE platforms.
- **Everything as a Service (XaaS) Optimization**: For single-sided use cases in cloud deployments, where you have control of one side of the connection, for example, 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 Cisco vWAAS instance or a Cisco ENCS 5400-W device.

Note When upgrading Cisco vWAAS, do not upgrade more than five Cisco vWAAS nodes at the same time on a single Cisco UCS device. Doing this may cause the Cisco vWAAS devices to go offline and into diskless mode.

- **Cisco vWAAS with Cisco Enterprise NFVIS on Cisco ENCS 5400-W** is part of Cisco 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.

  Cisco vWAAS with Cisco Enterprise NFVIS on Cisco ENCS 5400-W is available for vWAAS in WAAS Version 6.4.1 and later.

- **Cisco vWAAS with Cisco Enterprise NFVIS on Cisco CSP 5000-W** is a Cisco open x86 hardware platform for deployment of Cisco datacenter Network Functions Virtualization (VNFs). Cisco CSP 5000-W Series contains an embedded KVM CentOS hypervisor, and enables you to monitor and manage the lifecycle of vWAAS on NFVIS.

  Cisco vWAAS with Cisco Enterprise NFVIS on Cisco CSP 5000-W is available for vWAAS in WAAS Version 6.4.3e and later.

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

This section contains the following topic:

About the Unified OVA Package for Cisco vWAAS on Cisco NFVIS

The following list highlights the features of the Unified OVA package for Cisco vWAAS with NFVIS for Cisco WAAS Version 6.4.1 and later.

- In Cisco vWAAS with Cisco Enterprise NFVIS in Cisco WAAS Version 6.4.x, Cisco vWAAS is deployed in a RHEL KVM hypervisor on a Cisco ENCS 5400-W Series device.
- In Cisco vWAAS with Cisco Enterprise NFVIS in Cisco 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 Cisco vWAAS models for that hypervisor.
- Each unified OVA package file is a preconfigured VM 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 Cisco vWAAS in Cisco WAAS in the required configuration.
- The following are examples of the unified OVA and NPE OVA package filenames for Cisco vWAAS with Cisco NFVIS:
  - Cisco-KVM-vWAAS-Unified-6.4.5-b-69.tar
  - Cisco-KVM-vWAAS-Unified-6.4.5-b-69-npe.tar
- The unified OVA package for Cisco 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 running the **launch.sh** file.
- **package.mf** template file and **bootstrap-cfg.xml**: These two files work together on the Cisco Enterprise NFVIS platform with the image_properties.xml file as day-zero configuration template.
- **ezdeploy.sh**: The script used to deploy Cisco vWAAS on Cisco UCS-E.
- **exdeploy_qstatus.exp**: The dependent file for **ezdeploy.sh** script.
- **image_properties.xml**: A VM configuration template file used on the Cisco Enterprise NFVIS platform.
- **launch.sh**: The launch script to deploy Cisco vWAAS on Linux KVM.
- **vm_macvtap.xml**: Configuration file for Cisco vWAAS deployment using host machine interfaces with the help of the mactap driver.
- **vm_tap.xml**: Configuration file for Cisco vWAAS deployment using the virtual bridge or OVS present in the host machine.

Operating Guidelines for the Unified OVA Package for Cisco vWAAS on Cisco NFVIS

The following models, highlighted in the following list and also listed in the Cisco WAAS sizing guides and specifically noted in Cisco WAAS, Cisco vWAAS user guides, and Cisco WAAS Release Notes, are the *only devices* we recommend for use with Cisco vWAAS:

- Cisco ENCS 5400-W Series
- Cisco CSP 5000-W Series
- Cisco UCS-C Series
- Cisco UCS-E Series
- Cisco ENCS 5100
- Cisco CSP-2100
- Cisco ISR configurations

Note Although Cisco vWAAS models may be able to operate with other Cisco or third-party hardware, successful performance and scale for those configurations are 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 3.12.x.

Traffic Interception for Cisco vWAAS with Cisco NFVIS

Cisco vWAAS with Cisco Enterprise NFVIS on Cisco ENCS 5400-W supports WCCP traffic interception.

- WCCP specifies interactions between one or more routers and one or more Cisco WAEs, to establish and maintain the transparent redirection of selected types of traffic in real time. The selected traffic is redirected to a group of Cisco WAEs with the aim of optimizing resource usage and lowering response times. A WCCP-enabled router and a Cisco WAE exchange WCCP protocol packets and negotiate membership of WCCP service groups.
- For Cisco vWAAS on Cisco ENCS 5400-W with WCCP, there are two Ethernet Gigabit ports that can be configured to intercept the traffic. With the NIM card, the ports can be used to intercept the WCCP traffic (configure port channel with LAN and WAN interface) if the inline interception method is not configured.
- For more information on on configuring WCCP, see the chapter "Configuring Traffic Interception" in the *Cisco Wide Area Application Services Configuration Guide*.

The following table shows the CLI commands used to configure WCCP traffic interception for Cisco vWAAS with Cisco Enterprise NFVIS.

Table 68: Cisco WAAS 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*.

Interoperabiity and Upgrade Guidelines for Cisco Enterprise NFVIS

Consider the following interoperability guidelines for Cisco Enterprise NFVIS and Cisco vWAAS:

- The following table shows the Cisco WAAS versions supported for Cisco vWAAS with Cisco Enterprise NFVIS.

Table 69: Cisco WAAS Versions Supported for Cisco Enterprise NFVIS

Cisco Enterprise NFVIS Version	Earliest Supported Cisco WAAS Version
4.12	6.4.5a
3.11.1	6.4.3b
3.10.1	6.4.3a
3.9.1	6.4.3
3.8.1	6.4.3
3.7.1	6.4.1

For more information on Cisco Enterprise NFVIS and Cisco WAAS Version interoperability, see the Cisco Wide Area Application Services Release Note for your Cisco WAAS version.

- The following models, highlighted in the following list and also listed in the Cisco WAAS sizing guides and specifically noted in Cisco WAAS, Cisco vWAAS user guides, and Cisco WAAS Release Notes, are the *only devices* we recommend for use with Cisco vWAAS:
  - Cisco ENCS 5400-W Series
  - Cisco CSP 5000-W Series
  - Cisco UCS-C Series
  - Cisco UCS-E Series
  - Cisco ISR configurations

Note Although Cisco vWAAS models may be able to operate with other Cisco or third-party hardware, successful performance and scale for those configurations are 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 3.12.x.

Consider the following upgrade guidelines for Cisco Enterprise NFVIS and Cisco vWAAS:

- You cannot upgrade to Cisco Enterprise NFVIS Version 4.12 from an earlier version; you must do a new installation of Cisco Enterprise NFVIS 4.12.
- For detailed upgrade information for Cisco Enterprise NFVIS versions 3.9.1 through 3.11.1, see the *Cisco Enterprise Network Function Virtualization Insfrastructure Software Configuration Guide* for your Cisco Enterprise NFVIS version.
- Each upgrade may take about 90 minutes. Do not interrupt the upgrade process.

Upgrading the Firmware for Cisco Enterprise NFVIS

Before you begin

This procedure is used to upgrade the Complex Programmable Logic Device (CPLD) and the Field Programmable Gate Array (FPGA) for Cisco Enterprise NFVIS to the latest version.

Procedure

Step 1 Ensure that your system is running the following:

- Cisco WAAS Version 6.4.3b or later
- Cisco Enterprise NFVIS 3.11.1 or later

Step 2 Download the Cisco WAAS Firmware image for ENCS-W Appliance from the Cisco Wide Area Application Services (WAAS) Software Download Page.

Step 3 To upgrade the FPGA, run the **nfvis scp fw-upgrade** command:

```
ENCS-W# nfvis scp fw-upgrade server-IP RemoteFileDirectory RemoteFileName
```

Example:

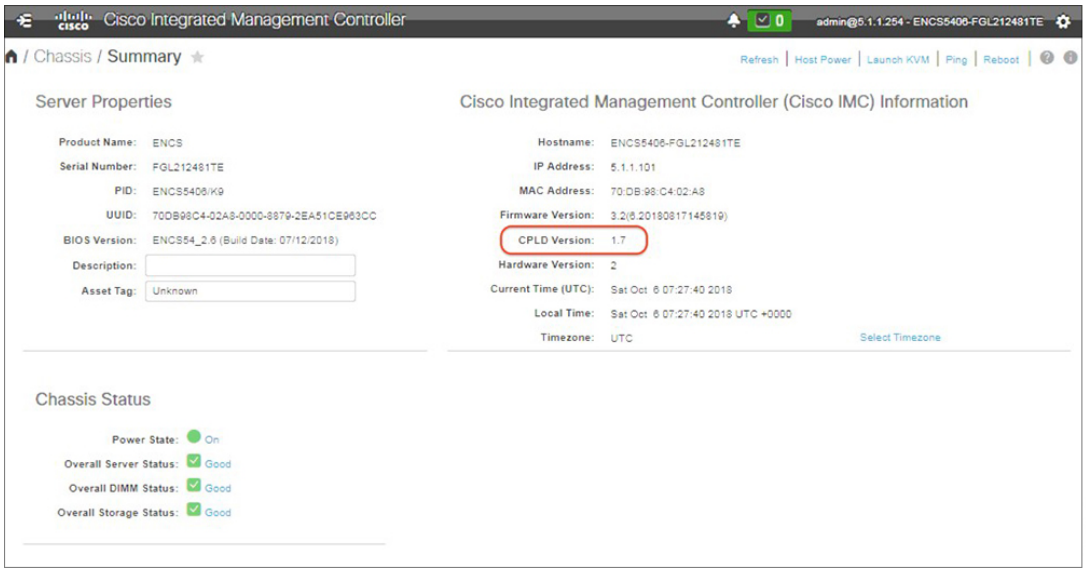
```
ENCS-W# nfvis scp fw-upgrade 172.19.156.179 ./ Cisco_ENCS_firmware-3.11.1.fwpkg
```

Note After you upgrade the firmware package, you must power-cycle the entire chassis to ensure that the FPGA takes effect.

Step 4 To verify the CPLD and FPGA version, use either the CIMC GUI or the CLI.

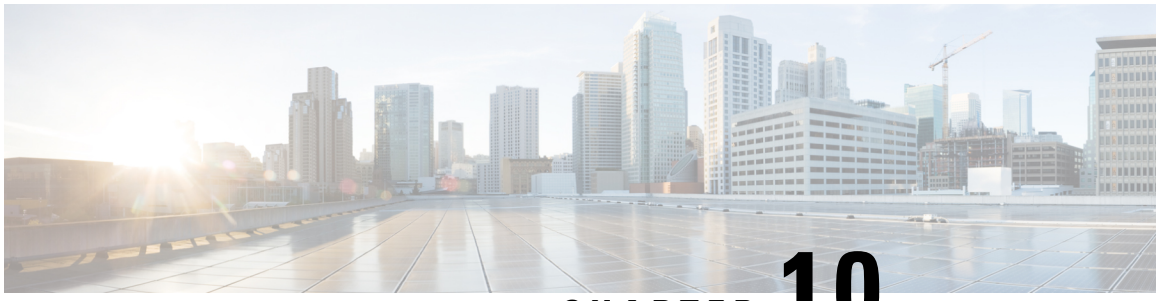
- To verify the CPLD and FPGA version from the CIMC GUI, choose **Chassis > Summary**.

Figure 34: Using the CIMC Console to Verify CPLD/FPGA Version



- To verify the CPLD and FPGA version from the CIMC CLI, run the following commands:

```
ENCS-W# scope cimc
ENCS-W# /cimc # show firmware detail
Firmware Image Information:
Update Stage: NONE
Update Progress: 0%
Current FW Version: 3.2(6.20180817145819)
FW Image 1 Version: 3.2(6.20180817145819)
FW Image 1 State: RUNNING ACTIVATED
FW Image 2 Version: 3.2(3.20171215104530)
FW Image 2 State: BACKUP INACTIVATED
Boot-loader Version: 3.2(6.20180817145819).36
CPLD Version: 1.7
Hardware Version: 2
```



CHAPTER 10

Cisco vWAAS with Akamai Connect

This chapter provides an overview of Cisco vWAAS with Akamai Connect, and describes the hardware requirements for Cisco vWAAS with Akamai Connect, including how to upgrade Cisco vWAAS memory and disk for the Akamai cache engine.

This chapter contains the following sections:

About Cisco vWAAS with Akamai Connect

Akamai Connect is the HTTP/S object cache component added to Cisco WAAS, integrated into the existing WAAS software stack and leveraged via the HTTP Application Optimizer.

- Cisco WAAS with Akamai Connect helps to reduce latency for HTTP/S traffic for business and web applications, and can improve performance for many applications, including Point of Sale (POS), HD video, digital signage, and in-store order processing.
- Cisco WAAS with Akamai Connect provides significant and measurable WAN data offload, and is compatible with existing WAAS functions such as DRE (deduplication), LZ (compression), TFO (Transport Flow Optimization), and SSL acceleration (secure/encrypted) for first and second pass acceleration.
- For more information on Cisco WAAS with Akamai Connect, see the chapter "Configuring Cisco WAAS with Akamai Connect" in the *Cisco Wide Area Application Services Configuration Guide*.

Cisco vWAAS in Cisco WAAS with Akamai Connect is an integrated solution that combines WAN optimization and intelligent object caching to accelerate HTTP/S applications, video, and content.

Cisco vWAAS in Cisco WAAS with Akamai Connect helps reduce latency for HTTP/HTTPS traffic for business and web applications, and can improve performance for many applications, including Point of Sale (POS), HD video, digital signage, and in-store order processing. It provides significant and measurable WAN

data offload, and is compatible with existing Cisco WAAS functions such as DRE, LZ, TFO, and SSL acceleration for first and second pass acceleration.

For more information, see the "Configuring Application Acceleration" chapter of the *Cisco Wide Area Application Services Configuration Guide*.

Supported Platforms for Cisco vWAAS with Akamai Connect

The following table shows supported platforms for Cisco vWAAS with Akamai Connect, up to 6,000 connections.

Table 70: Supported Cisco Devices for Akamai Caching, Up to 6,000 Connections

Cisco vWAAS	Cisco ISR-WAAS	Cisco WAVE	Cisco SRE-SM (for WAAS Version 6.2.x and earlier)
vWAAS-150 (for Cisco WAAS Version 6.1.1 and later)	• ISR-G2 • ISR-G3	• N/A	• N/A
vWAAS-200	• ISR-WAAS-750 • ISR-4451 • ISR-4431 • ISR-4351 • ISR-4331 • ISR-4321	• WAVE-294	• SRE-SM-700
vWAAS-750	• ISR-WAAS-1300 • ISR-4451 • ISR-4431	• WAVE-594	• SRE-SM-900
vWAAS-1300	• ISR-WAAS-2500 • ISR-4451	• WAVE-694	• SRE-SM-710
vWAAS-2500	• N/A	• N/A	• SRE-SM-910
vWAAS-6000	• N/A	• N/A	• N/A

The following table shows supported platforms for Cisco vWAAS with Akamai Connect, beyond 6,000 connections

Table 71: Supported Cisco vWAAS Models for Akamai Caching, Beyond 6,000 Connections

Cisco vWAAS Model	Total HTTP Object Cache Connections	Cache Engine Cache Disk	Additional Resource to be Added
vWAAS-12000	12,000	750 GB	6 GB RAM, 750 GB disk
vWAAS-50000	50,000	850 GB	850 GB disk

Note In Cisco vWAAS in WAAS Version 6.2.x, Cisco 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.

The following table 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 the following table is dependent on the hardware module on which Cisco WAAS is running.

Table 72: 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 1,300 WAAS connections	• ISR-2900 or ISR-3900 and one of the following: vWAAS-1300 or lower (UCS-E) • ISR-4451, ISR-4431, ISR-4351, or ISR-4331: vWAAS-2500 or lower • UCS server: vWAAS-1300 or lower • WAVE-594

Cisco IWAN with Akamai Connect License	License Description	Supported Platforms(vWAAS platforms in bolded text)
SL-2500-AKC	Akamai Connect license for up to 2,500 WAAS connections	• ISR-2900 or 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 6,000 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

The following table shows the hardware requirements for Cisco UCS E-Series and CIsco ISR-WAAS for Cisco 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, on page 100 in the chapter "Cisco vWAAS on Microsoft Hyper-V."

Table 73: 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

Cisco vWAAS or WAAS Model	Memory Required for vWAAS with Akamai Connect	Disk Required for vWAAS with Akamai Connect
vWAAS-6000	11 GB	900 GB
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

For more information on cache engine memory requirements and cache engine disk requirements, see Akamai Connect Cache Engine on Cisco Mid-End and High-End Platforms, on page 166.

Upgrading vWAAS Memory and Disk for Akamai Connect

This section contains the following sections:

Upgrading Memory and Disk for Earlier Versions of Cisco vWAAS with Akamai Connect

Before you begin

Note The following procedure is for Cisco WAAS systems running a Cisco WAAS version earlier than Cisco WAAS Version 6.1.1. If Cisco vWAAS in Cisco WAAS Version 6.1.1 or later is running on your Cisco WAAS system, the Akamai disk is added by default, and you do not need to use the following installation procedure.

If you are running Cisco vWAAS in an early Cisco WAAS version with the following parameters, and want to upgrade to Cisco WAAS Version 5.4.1, 5.5.1, or 6.1.1, use the update memory and disk procedure to as described in the Cisco Wide Area Application Services Release Note for the specified Cisco WAAS version.

- A Cisco WAAS version earlier than Cisco WAAS Version 5.4.1
- A VMware ESXi version earlier than VMware ESXi Version 5.0

Procedure

Step 1 Power off the Cisco vWAAS.

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

Step 3 Click **Add...**.

Step 4 In the **Add Hardware** dialog box, select **Hard Disk** and click **Next**.

Step 5 In the **Select a Disk** dialog box, select **Create a new virtual disk** and click **Next**.

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

- From the **Capacity** drop-down list, choose the size of the new disk.
- From the **Disk Provisioning** drop-down list, choose **Thick Provision Lazy Zeroed**.
- From the **Location** drop-down list, choose **Store with the virtual machine**.
- Click **Next**.

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

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

Step 8 In 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**.

The window displays the status message **New hard Disk (adding)**.

Step 10 Click **OK**.

Step 11 Wait until the **Recent Tasks** window displays the **Reconfigure Virtual** machine task as **Completed**, and then power on the Cisco vWAAS.

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

Upgrading vWAAS Memory and Disk for Cisco vWAAS-12000 with VMware ESXi

Before you begin

When the Cisco vWAAS-12000 is deployed, the RAM size is 12 GB and the **/local/local1** directory size is 15 GB. When you enable Akamai Connect for Cisco vWAAS, increase the RAM to 18 GB.

Note This procedure alters the calculation of the **local1** directory size for the vWAAS-12000 because the expected size is 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 may cause a serious problem during a kernel crash in the Cisco vWAAS-12000, because the **vmcore** file will then be larger than what could be stored in the local1 directory.

To avoid the scenario described in the above Note, and to safely upgrade vWAAS memory and disk for Akamai Connect for the Cisco vWAAS-12000, use the following procedure:

Procedure

Step 1 Power off the Cisco vWAAS VM.

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 Cisco vWAAS-12000, increase the size of the RAM by at least 6 GB.

Step 4 Power on the Cisco vWAAS VM.

Step 5 Check the alarms.

The **filesystem_size_mism** alarm is raised:

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

Alarm ID                 Module/Submodule          Instance
-----------------------  ------------------        ---------------
1 filesystem_size_mism   disk                      Filesystem size
```

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

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

Step 7 Reload the device.

- After running the **disk delete-data-partitions** command, you must reload the device.

  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 Cisco vWAAS-12000 with Microsoft Hyper-V

Before you begin

When the Cisco vWAAS-12000 is deployed, the RAM size is 12 GB and the **/local/local1** directory size is 15 GB. When you enable Akamai Connect for Cisco vWAAS, increase the RAM to 18 GB.

Note This procedure alters the calculation of the **local1** directory size for the vWAAS-12000 because the expected size is 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 may cause a serious problem during a kernel crash in the Cisco vWAAS-12000, because the **vmcore** file will then be larger than what could be stored in the local1 directory.

To avoid the scenario described in the above Note, and to safely upgrade vWAAS memory and disk for Akamai Connect for the Cisco vWAAS-12000, use the following procedure:

Procedure

Step 1 Power off the vWAAS VM.

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 least6 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 Cisco 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 Run the **disk delete-data-partitions** command.

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

Step 8 Reload the device.

- After running the **disk delete-data-partitions** command, you must reload the device.

  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

Consider the following guidelines for Cisco vWAAS-150 with Akamai Connect:

- For Cisco vWAAS in WAAS Version 6.1.1 and later, Cisco vWAAS-150 on Cisco ISR-WAAS is supported for Akamai Connect. For Cisco vWAAS in WAAS Version 6.2.1 and later, vWAAS-150 is also supported for RHEL KVM and Microsoft Hyper-V.

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

- For the Cisco vWAAS-150 model, the Cisco WAAS Central Manager *must* be Cisco WAAS Version 6.2.1 or later, but the mixed versions of device models (Cisco WAAS Version 6.2.1 and earlier) are also supported. The Cisco WAAS Central Manager must be a version that is equal to or later than the associated devices.

  Cisco vWAAS-150 is deployed *only* in Cisco WAAS Version 6.1.1 and later. Therefore, you cannot upgrade or downgrade Cisco vWAAS-150 from Cisco WAAS Version 6.1.1.

The following table shows specifications for vWAAS-150.

Table 74: Cisco 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

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

In Cisco WAAS Version 6.2.1 and later, the Akamai Connect Cache Engine is supported for scaling beyond 6,000 Cisco vWAAS connections on the following platforms:

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

Scaling for these platforms is based on memory availability, scale performance, and the particular dynamic cache size management feature. The table "Cisco WAAS Mid to High End Platform Cache Engine Memory Requirements" shows the connections, total memory, and cache engine memory requirements for each of these platforms. The table "Cisco WAAS Mid to High End Platform Cache Engine Cache Disk Requirements" shows the connections, number of disks, and cache engine disks for each of these platforms.

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

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

- For vWAAS-12000, allocate at least 6 GB of additional RAM.
- For vWAAS-12000 and vWAAS-50000, allocate cache engine cache disk resources. Cache disk requirements are shown in the table "Cisco WAAS Mid to High End Platform Cache Engine Cache Disk Requirements".

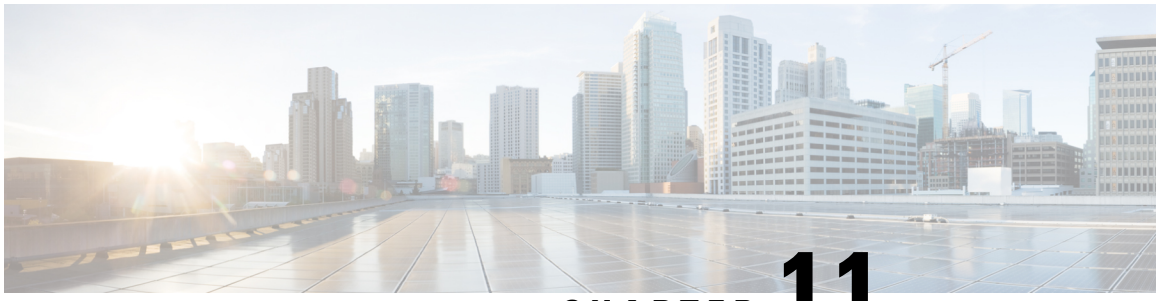
Table 75: Cisco WAAS Mid to High End Platform Cache Engine Memory Requirements

Cisco WAAS Platform	HTTP Object Cache Connections	CPU	Total Memory	Memory Required forCache 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 or 14125 M or 11565 M
WAVE-8541	150 K/ 125 K/1 00 K	2	96 GB	38400 M or 32000 M or 25600 M

Table 76: Cisco 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

Cisco WAAS Platform	HTTP Object Cache Connections	CPU	Disk/ CE Cache Disk	Cache Engine Cache Disk
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 11

Cisco vWAAS in Cloud Computing Systems

This chapter describes the operation of Cisco vWAAS in the Microsoft Azure and OpenStack cloud computing systems.

This chapter contains the following sections:

About Cisco vWAAS in Cloud Computing Systems

Cisco vWAAS is a cloud-ready WAN optimization solution that is fully interoperable with Cisco WAAS appliances, and can be managed by a common Cisco WAAS Central Manager or Cisco vCM. The Cisco 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 multitenancy 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

Microsoft Azure provisions VMs on the Microsoft Hyper-V hypervisor. Cisco vWAAS in Microsoft Azure is part of Cisco WAAS support for Microsoft Office 365, and is an end-to-end solution for enterprise branch offices.

- Cisco vWAAS in Microsoft Azure is available for Cisco vWAAS in Cisco WAAS Version 6.2.1x and later.

- Cisco vWAAS in Microsoft Azure is supported for Cisco vWAAS-200, vWAAS-750, vWAAS-1300, vWAAS-2500, vWAAS-6000, and vWAAS-12000.
- Cisco vWAAS in Microsoft Azure is not supported for Cisco vWAAS-50000.

The following table shows the platforms supported for Cisco vWAAS in Microsoft Azure.

Table 77: 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 Guidelines for Cisco vWAAS in Microsoft Azure

This section describes operating guidelines, interoperability guidelines, and operating limitations for Cisco vWAAS in Microsoft

Cisco vWAAS in Microsoft Azure interoperability:

Consider the following interoperability guidelines for Cisco vWAAS in Microsoft Azure:

- Cisco vWAAS in Microsoft Azure is available for specified vWAAS models in Cisco WAAS Version 6.2.1 and later.
- You can display and identify vWAAS in Azure device on the Cisco WAAS Central Manager or the Cisco WAAS CLI:
  - On the Cisco WAAS Central Manager, choose **Manage Devices**. The vWAAS in Azure device type is displayed as **OE-VWAAS-AZURE**.
  - On the Cisco WAAS CLI, run either the **show version** EXEC command or the **show hardware** EXEC command. Output for both commands includes the device ID, shown as **OE-VWAAS-AZURE**.
- Cisco vWAAS in Microsoft Azure communicates with the Cisco WAAS Central Manager in the same way as physical appliances communicate with the Cisco WAAS Central Manager.
- To display vWAAS in Azure devices, choose **Home > Devices > All Devices**. The **Device Type** column shows all WAAS and vWAAS devices. A vWAAS in Azure device is displayed as **OE-VWAAS-AZURE**.

Note For Cisco vWAAS in Microsoft Azure, the supported traffic interception method is PBR; Cisco vWAAS in Microsoft Azure does not support WCCP or AppNav interception methods.

Operating limitations for Cisco vWAAS in Microsoft Azure:

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

- Cisco 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 Cisco WAAS Central Manager IP address during Cisco vWAAS VM provisioning. The Cisco vWAAS VM will try to register with this Cisco WAAS Central Manager during provisioning.

- Microsoft Azure does not support GRE, IPv6, or Jumbo Frames. Therefore Cisco vWAAS in Microsoft Azure does not support these features.

Note For Cisco vWAAS in Microsoft Azure, the supported traffic interception method is PBR; Cisco vWAAS in Microsoft Azure does not support WCCP or AppNav interception methods.

- Cisco WAAS and Cisco vWAAS with Akamai Connect are not supported for Cisco vWAAS in Microsoft Azure.

Upgrade and downgrade guidelines for Cisco vWAAS in Microsoft Azure:

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

- The procedure for upgrading or downgrading Cisco vWAAS in Microsoft Azure, for all Cisco vWAAS models except Cisco vWAAS-50000, is the same as that for other Cisco WAAS devices. For more information, see *Cisco Wide Area Application Services Configuration Guide*.
- Downgrading a device or device group for Cisco vWAAS in Microsoft Azure to a version earlier than Cisco WAAS Version 6.2.1 is not supported.

Registering Cisco vWAAS in Microsoft Azure with the Cisco WAAS Central Manager

Consider the following guidelines for registering the Cisco vWAAS in Microsoft Azure with the Cisco WAAS Central Manager:

- If you register the Cisco vWAAS in Microsoft Azure with the WAAS Central Manager using a private IP address, follow the Cisco vWAAS registration process described in Configuring Cisco vWAAS Settings of the chapter “Configuring Cisco vWAAS and Viewing vWAAS Components.

- If you register the Cisco vWAAS in Microsoft Azure with the Cisco WAAS Central Manager using a public IP address, you must specify the public address of the Cisco vWAAS in the Cisco WAAS Central Manager Device Activation window (choose Devices > device-name > Activation).

  After you register the Cisco vWAAS in Microsoft Azure device with the Cisco WAAS Central Manager, you must configure the public IP address of the Cisco WAAS Central Manager. The Cisco vWAAS in Microsoft Azure device can contact the Cisco WAAS Central Manager only by using the public IP address of the registration. To set the public IP address of the WAAS Central Manager:

  1. From the Cisco WAAS Central Manager, choose **Home > Devices > Primary-CM-Device > Configure > Network > NatSettings**.
  2. In the **NAT IP** field, enter the public IP address of the Cisco WAAS Central Manager.

Deploying Cisco vWAAS in Microsoft Azure

This section has 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 the hosting of the application.

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

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

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

Provisioning the vWAAS VM in Microsoft Azure

Before you begin

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

Procedure

Step 1 Login to the Microsoft Azure portal.

Step 2 Choose **New > Compute > Virtual Machine > From Gallery**.

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

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

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

a) 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.
b) At the **Virtual Machine Tier** pane, select **Standard**.
c) From the **Size** drop-down list, select the Azure VM size for your system. The following table shows the minimum Azure VM size for each Cisco vWAAS model available for provisioning in the **Virtual Machine Tier** pane.

Table 78: 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 Virutal Machine Tier** pane to select an Azure VM for the Cisco vWAAS models shown in the above table. For vWAAS-6000 and vWAAS-12000, you must use the template to specify the Azure VM. For more information, see the table in About Cisco vWAAS in Microsoft Azure.

d) In the **New User Name** field, enter your user name.
e) In the **New Password** field, enter your password.
f) In the **Confirm** field, re-enter your password.
g) (Optional) If your system uses SSH key-based authentication:
   - Check the **Upload compatible SSH key for authentication** checkbox.
   - From the **Certificate** field, browse for the certificate file for your system.
h) (Optional) If your system requires a password, check the **Provide a password checkbox**.
i) Click the right arrow at the lower right of the window to proceed to the next window.

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

Step 4 At the next **Create a Virtual Machine/Virtual Machine Configuration** window:

a) From the **Cloud Service** drop-down list, choose **Create a Cloud Service**.
b) In the **Cloud Service DNS Name** field, enter the name of the VM that you created in **Step 3a**.

When Azure VMs are being named, the DNS name has **cloudapp.net** automatically appended to it.

c) From the **Region/Affinity Group/Virtual Network** drop-down list, choose a location that is in close proximity to the resources you want to optimize, such as East U.S. or North Europe.

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

d) From the **Storage Account** drop-down list, select **Use an automatically generated storage account**.
e) From the **Availability Set** drop-down list, choose **(None)**.
f) Click the right arrow at the lower right of the window to proceed to the next window.

The **Virtual Machines/Virtual Machine Instances** window is displayed.

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

Step 5 At the **Virtual Machines/Virtual Machine Instances** window:

a) In the **Endpoints** section:

- Add an endpoint for **SSH (port 22)**.
- Add an endpoint for **HTTPS (port 443)**.

b) Click the check mark at the lower right corner of the window to proceed for provisioning Cisco vWAAS.

The **Virtual Machines/Virtual Machine Instances** window now shows the newly-created VM with an initial status of **Starting (Provisioning)**.

The process takes a few minutes before the VM status is displayed as **Running**.

c) Select the Cisco vWAAS VM.
d) Attach the data disks. For data disk sizes for Azure VMs, see the table in About Cisco vWAAS in Microsoft Azure..
e) Stop and then restart the VM, so that it picks up the attached disks.

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

Deploying Cisco vWAAS VM and Data Disk with the VHD Template

Procedure

Step 1 Using **AzCopy**, copy **vwaas.vhd** to the storage account.

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 VHD template to deploy the Cisco vWAAS VM.

The Cisco 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 the Cisco WAAS Central Manager address, see Verifying the Cisco vWAAS in Microsoft Azure Deployment, on page 176.

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

Before you begin

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

Procedure

Step 1 Using **Azcopy**, copy **vwaas.vhd** to the storage account.

Step 2 Use the template to deploy the vWAAS VM.

Step 3 At the Microsoft ARM portal, choose **New** > **Template Deployment** > **Edit Template**.

Step 4 Copy the template.

Step 5 Paste the template in the **Templates** window.

Step 6 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 7 Accept the **Terms and Conditions**.

Step 8 Click **Create**.

The Cisco vWAAS VM is deployed.

Step 9 Log in with your username and password.

Step 10 (Optional) To verify deployment details such as CMS registration and Cisco WAAS Central Manager address, see Verifying the Cisco vWAAS in Microsoft Azure Deployment, on page 176.

Deploying Cisco vWAAS VM Using Microsoft Windows Powershell

Before you begin

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

Procedure

Step 1 Deploy Cisco vWAAS on Microsoft Hyper-V. For information on this deployment procedure, see the chapter "Cisco vWAAS on Microsoft Hyper-V, on page 87."

Step 2 To set the necessary Azure parameters, run the **azure_predeploy.sh** script in Hyper-V.

Step 3 Export the flash VHD from the Microsoft Hyper-V disk location to the storage account in Microsoft Azure, using AzCopy.

Step 4 Run the Microsoft Windows Powershell commands to specify the following parameters:

- To specify the deployment name, run the **deployName** command.
- To specify the resource group, run the **RGName** command.
- To specify the location, run the **locName** command.
- To specifiy the template file, run the **templateURL** command.

Step 5 To to create the resource group, run the **New-AzureRmResourceGroup -Name $RGName -Location $locName** Powershell command.

Step 6 To deploy Cisco vWAAS in Microsoft Azure, run the **New-AzureRmResourceGroupDeployment** Powershell cmdlet. To complete the deployment, specify values for the following parameters:

- userImageStorageAccountName
- userImageStoragContainerName
- userImageVhdName
- osType
- vmName
- adminUserName
- adminPassword

Step 7 After you enter these parameters, Cisco vWAAS in Microsoft Azure is deployed. The system displays provisioning information including deployment name, provisioning state, date/time, and mode.

Step 8 Log in with your username and password.

Step 9 (Optional) To verify deployment details such as CMS registration and Cisco WAAS Central Manager address, see .Verifying the Cisco vWAAS in Microsoft Azure Deployment, on page 176

Verifying the Cisco vWAAS in Microsoft Azure Deployment

The following table provides a checklist for verifying the Cisco vWAAS VM deployment in Microsoft Azure.

Table 79: Checklist for Verifying the Cisco vWAAS in Azure Deployment

Task	Description
Viewing vWAAS in Azure vWAAS devices	• From the Cisco WAAS Central Manager, choose Manage Devices. The vWAAS in Azure device type is displayed as **OE-VWAAS-AZURE**. • From the Cisco WAAS CLI, run either the **show version** EXEC command or the **show hardware** EXEC command. Output for both commands will include device ID, displayed as **OE-VWAAS-AZURE**.

Task	Description
Viewing Boot Information and Diagnostics	On the Microsoft Azure portal, choose **Virtual Machines > VM > Settings > Boot Diagnostics**.

Verifying CMS Registration	• If the Centralized Management System (CMS) is enabled, run the **show cms device status** *name* command to display status for the specified device or device group.
	• After you have registered the vWAAS in Azure device to the Cisco WAAS Central Manager, you must configure the public IP address of the Central Manager. The vWAAS in Azure device can contact the Cisco WAAS Central Manager only by using the public IP address of the registration. To set the public IP address of the Cisco WAAS Central Manager:
	  • In the Cisco WAAS Central Manager, choose **Home > Devices > Primary-CM-Device > Configure > Network > NatSettings**.
	  • In the **NAT IP** field, enter the public IP address of the Cisco WAAS Central Manager.

Verifying Cisco WAAS Central Manager Address	To dipslay inforamtion about all Cisco WAAS devices, run the **show running-config** command.

Note Whenever ARP caches are cleared or the Cisco vWAAS is rebooted, packets may not be forwarded to the next hop in Microsoft Azure cloud. To ensure that packets are successfully forwarded, use the ping EXEC command to update the ARP cache table.

Upgrade and Downgrade Guidelines for Cisco vWAAS in Microsoft Azure

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

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

Cisco vWAAS in OpenStack

This section contains the following topics:

Operating Guidelines for Cisco vWAAS in Openstack

Consider the following operating guidelines for Cisco vWAAS in OpenStack:

- Cisco vWAAS in OpenStack is supported for Cisco vWAAS in WAAS Version 6.4.1b and later.
- Cisco vWAAS in OpenStack is supported for all Cisco vWAAS and Cisco vCM models that are supported on RHEL KVM on CentOS.
- On the Cisco WAAS Central Manager, Cisco vWAAS devices in OpenStack are displayed as **OE-VWAAS-OPENSTACK**.
- All Cisco vWAAS models for Cisco vWAAS in OpenStack are deployed with a single, unified OVA. The following are examples of the unified OVA and NPE OVA package filenames for Cisco vWAAS in OpenStack:
  - OVA: Cisco-KVM-vWAAS-Unified-6.4.5-b-69.tar
  - NPE OVA: Cisco-KVM-vWAAS-Unified-6.4.5-b-69-npe.tar
- When you deploy the OpenStack host, it uses the default vWAAS disk size. Modify the disk size, as needed, for your configuration requirements.
- For OpenStack deployment, the Generic Receive Offload (GRO) setting on the host NIC card must be enabled.

Deploying Cisco vWAAS in OpenStack

This section contains the following topics:

Guidelines for Deploying Cisco vWAAS in OpenStack

Consider the following guidelines to deploy Cisco vWAAS in OpenStack:

- Cisco vWAAS in OpenStack is deployed for vWAAS on KVM. For more information on Cisco vWAAS on KVM, see the chapter "Cisco vWAAS on RHEL KVM, KVM on CentOS, and KVM in SUSE Linux."

  For Cisco vWAAS on KVM in Cisco 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 Cisco vWAAS models for that hypervisor. Here are some examples of the unified OVA and NPE OVA package filenames for vWAAS on KVM:
  - OVA: Cisco-KVM-vWAAS-Unified-6.4.5-b-69.tar
  - NPE OVA: Cisco-KVM-vWAAS-Unified-6.4.5-b-69-npe.tar

  For more information about this unified OVA package, see Unified OVA Package for Cisco vWAAS on KVM in WAAS Version 6.4.1 and Later, on page 105 in the chapter "Cisco vWAAS on RHEL KVM, KVM on CentOS, and KVM in SUSE Linux."
- After Cisco vWAAS in OpenStack is operational on a device, you can use the Cisco WAAS Central Manager or the Cisco WAAS CLI to display the OpenStack device.
  - The Cisco WAAS Central Manager 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**.

- Run 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 Cisco vWAAS in OpenStack

Procedure

Step 1 Copy the unified OVA to a directory on the host machine.

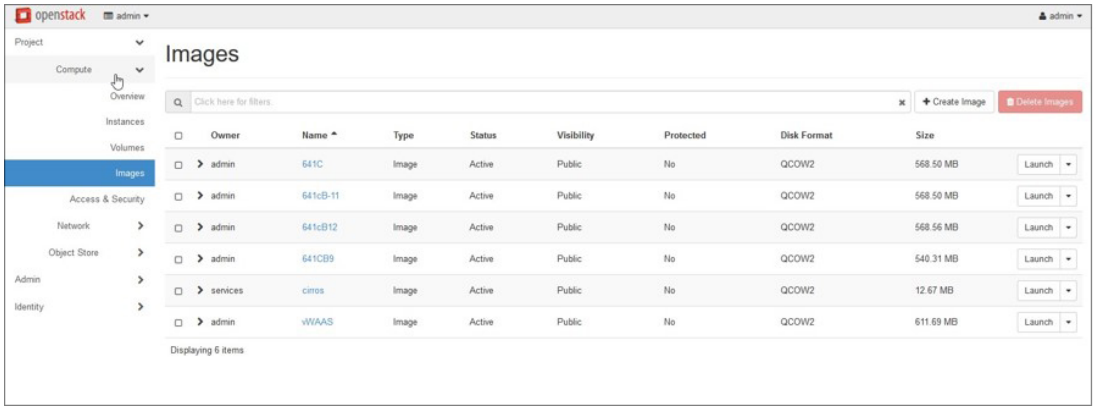
Step 2 Untar the OVA using the following command:

tar -xvf Cisco-KVM-vWAAS-Unified-6.4.5-b-69.tar.gz

Step 3 Create the image.

a) Click the **OpenStack** Admin tab and choose the **Compute** > **Images** window.

Figure 35: OpenStack Compute > Images Page



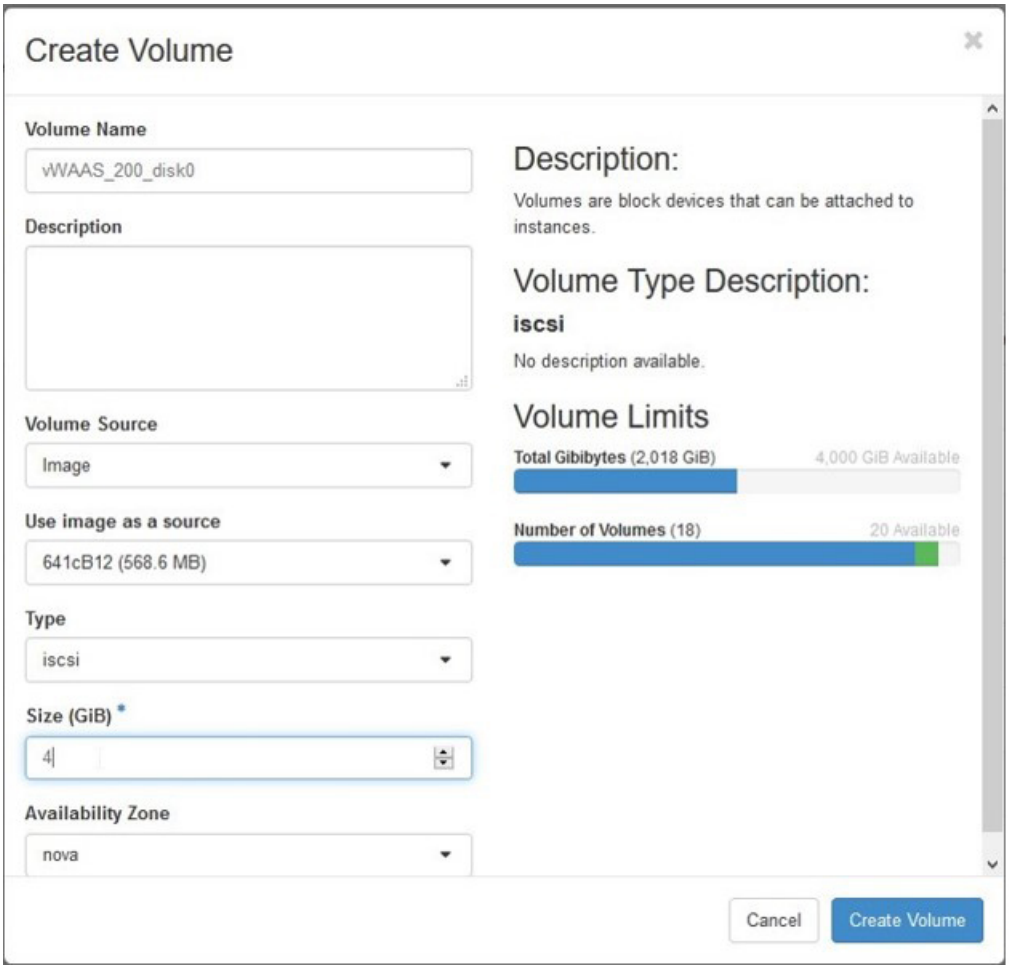
b) From the **Images** table, choose the image for your system.

c) To create the image, click **Create Image**.

Step 4 Create the bootable volume.

a) Click the **OpenStack Admin** tab and choose **Compute** > **Create Volume**.

Figure 36: OpenStack Create Volume Dialog Box: Creating Bootable Volume

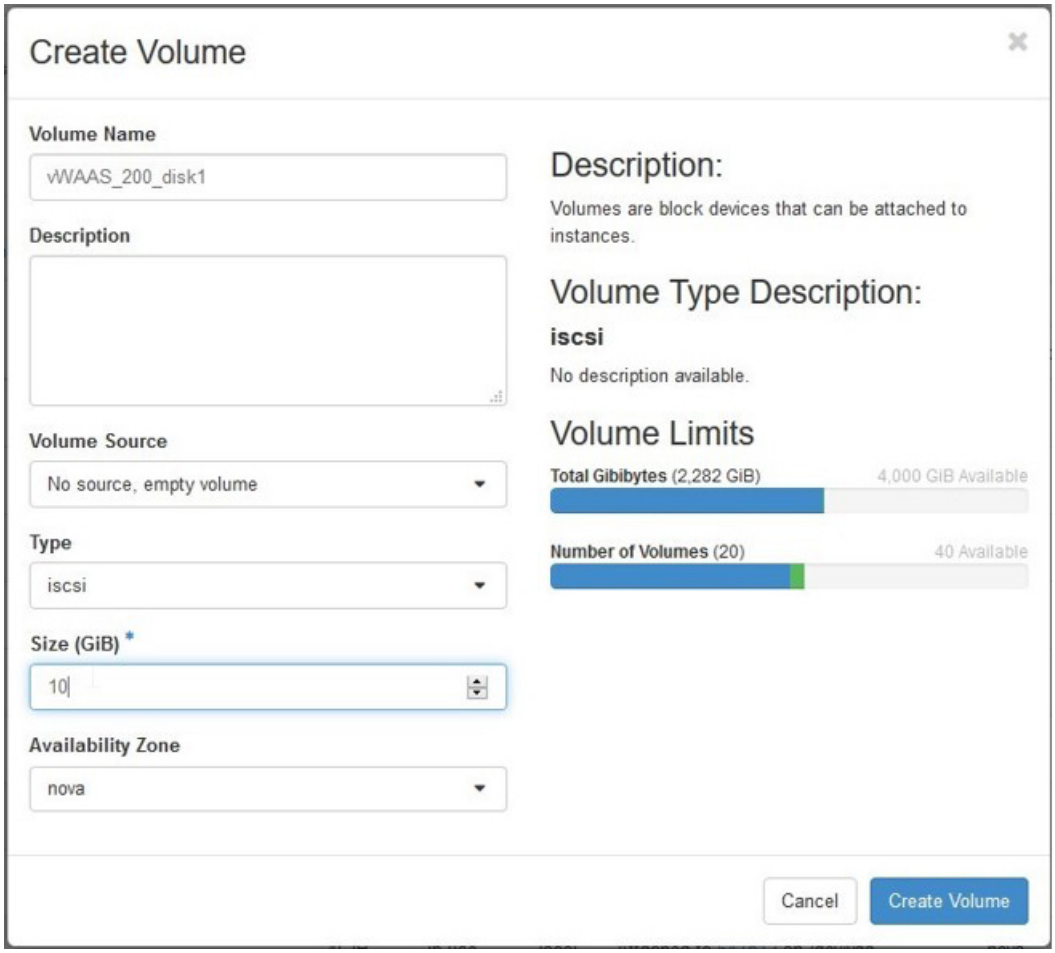


b) In the **Volume Name** field, enter the name of the Cisco vWAAS model and disk, for example, **vWAAS_200_disk0**.
c) From the **Volume Source** drop-down list, choose **Image**.
d) From the **Use image as a source** drop-down list, choose the build number for your system.
e) From the **Type** drop-down list, choose **iscsi**.
f) From the **Size (GiB)** drop-down list, choose the size for this volume, for example, **4**.
g) From the **Availability** drop-down list, choose nova.
h) Click **Create Volume**.

Step 5 Create nonbootable volumes.

a) Click the **OpenStack Admin** tab and choose **Compute** > **Create Volume**.

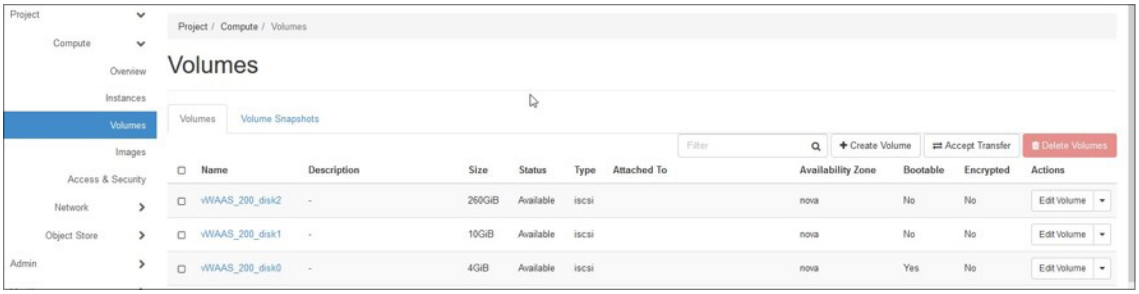
Figure 37: OpenStack Create Volume Dialog Box: Creating Nonbootable Volumes



b) In the **Volume Name** field, enter the name of the Cisco vWAAS model and disk, for example, **vWAAS_200_disk1**.
c) From the **Volume Source** drop-down list, choose **No source, empty volume**.
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, **10**.
f) From the **Availability** drop-down list, choose **nova**.
g) Click **Create Volume**.

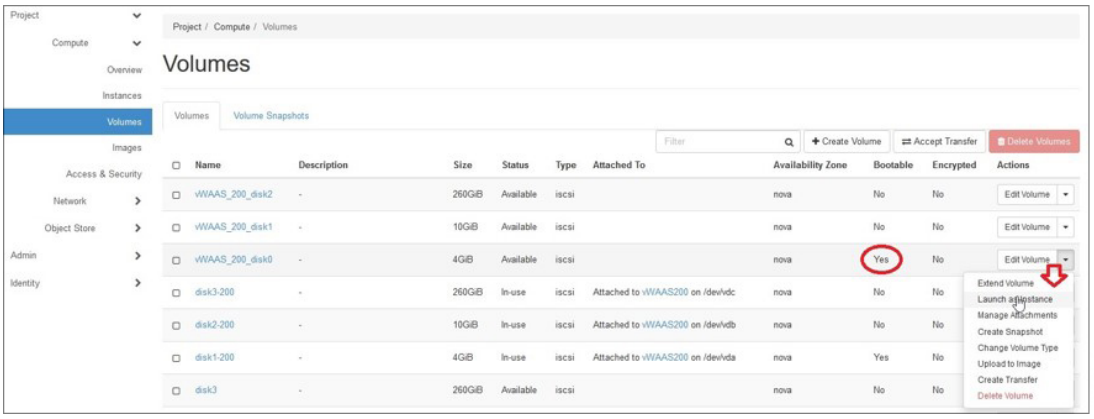
Step 6 In the **OpenStack Compute > Volumes** window, create all the volumes related to your deployed model.

Figure 38: Openstack Compute > Volumes Page: Create all Volumes for Deployed Model



a) In the **OpenStack Compute > Volumes** page, create an instance with a bootable volume.

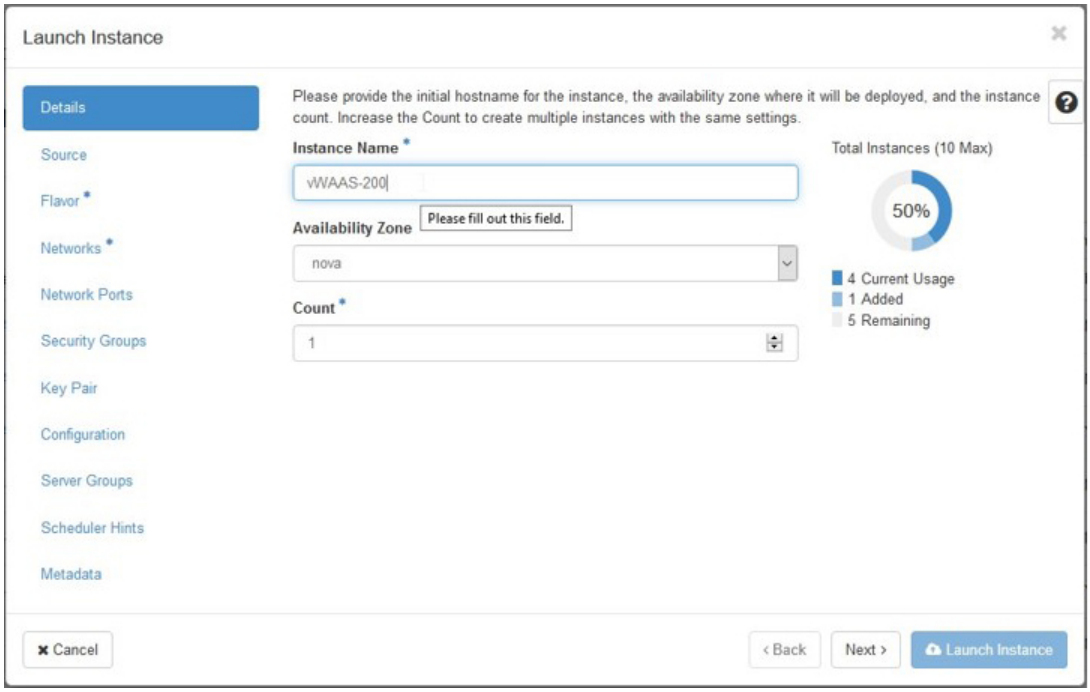
Figure 39: OpenStack Compute > Volumes Page: Create Bootable Volume



b) Launch the instance.

c) Click the **OpenStack Admin** tab and choose **Compute > Instances > Launch Instance**.

Figure 40: OpenStack Launch Instance > Details Page

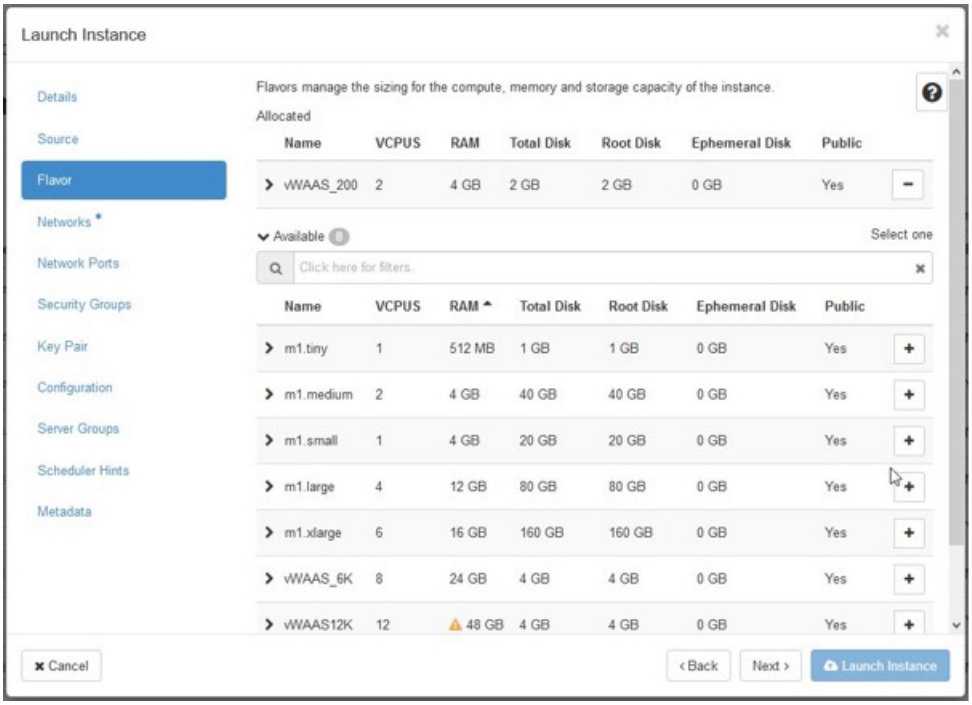


d) In the **Instance Name** field, enter the name of the Cisco vWAAS model, for example, **vWAAS-200**.
e) From the **Availability** drop-down list, choose **nova**.
f) From the **Count** drop-down list, choose **1**.
g) Click **Launch Instance**.

Step 7 Specify the flavor suitable for the selected Cisco vWAAS model. As noted on the **OpenStack** page, flavors manage the sizing for the compute, memory, and storage capacity of the instance.

Click the **OpenStack Admin** tab and choose **Compute > Instances > Launch Instance > Flavor**.

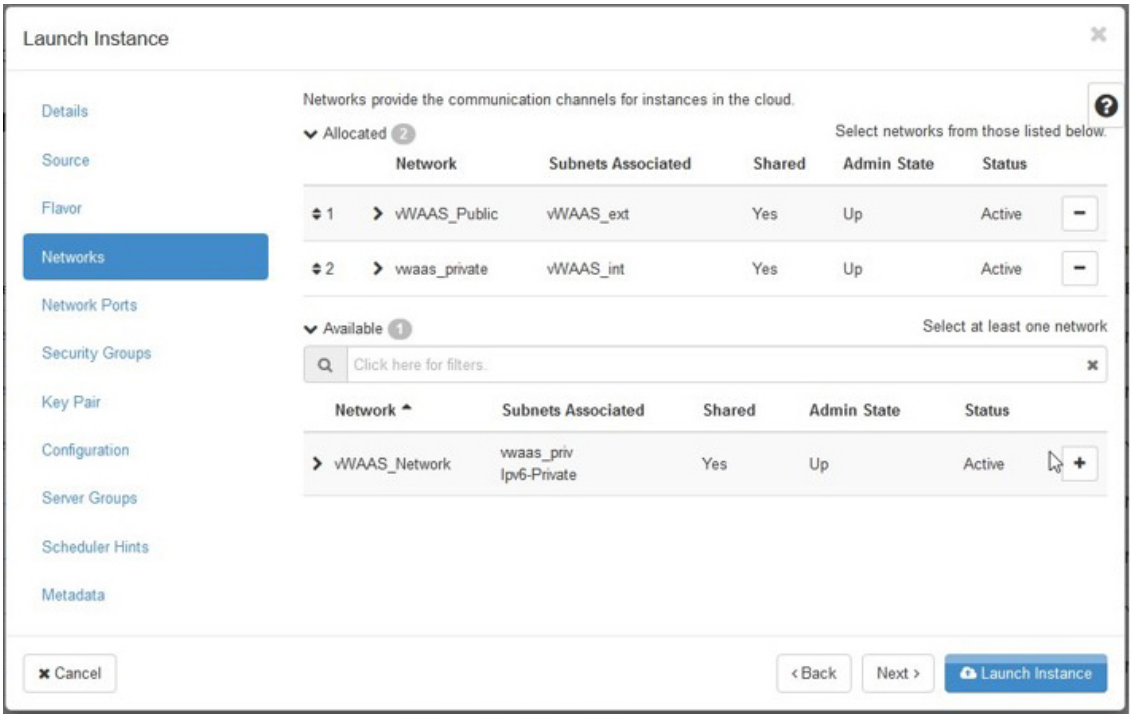
Figure 41: OpenStack Launch Instance > Flavor Page



Step 8 Select the networks for the vWAAS.

Click the **OpenStack Admin** tab and choose **Compute > Instances > Launch Instance > Networks**.

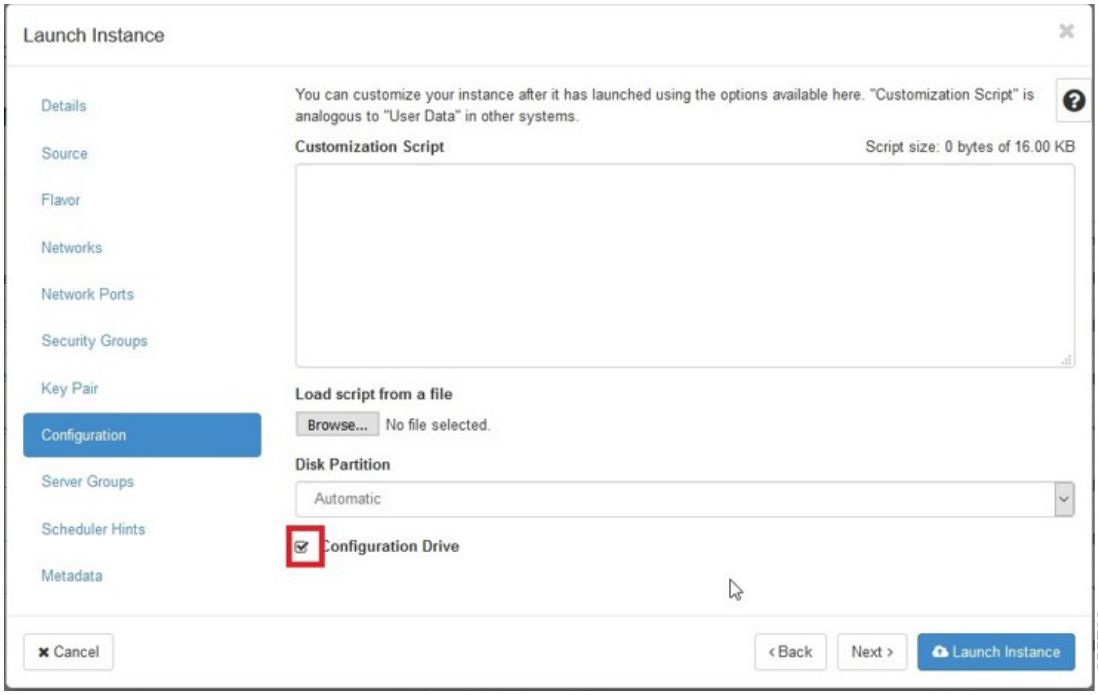
Figure 42: OpenStack Launch Instance > Networks Page



Step 9 Select the configuration drive to send model parameters.

a) Click the **OpenStack Admin** tab and choose **Compute > Instances > Launch Instance > Configuration**.

Figure 43: OpenStack Launch Instance > Configuration Page



b) From the **Disk Partition** drop-down list, choose **Automatic**.

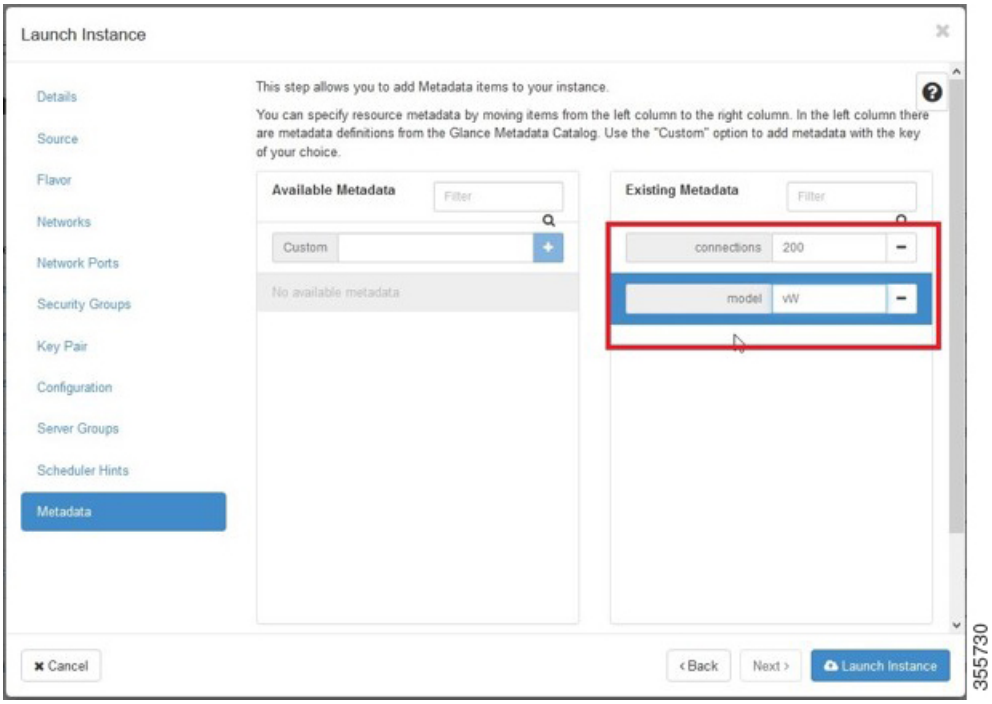
c) Check the **Configuration Drive** check box.

d) Click **Launch Instance**.

Step 10 Provide model and connection information to deploy vWAAS in OpenStack metadata.

a) Click the **OpenStack Admin** tab and choose **Compute > Instances > Launch Instance > Metadata**.

Figure 44: OpenStack Launch Instance > Metadata Page

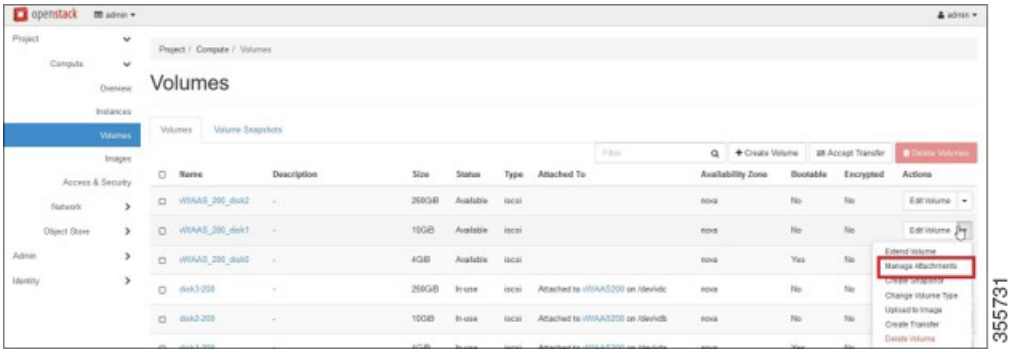


b) Specify resource metadata by selecting and moving items from the **Available Metadata** column into the **Existing Metadata** column.

Step 11 Attach disks to the deployed instance.

a) Click the **OpenStack Admin** tab and choose **Compute** > **Volumes**.

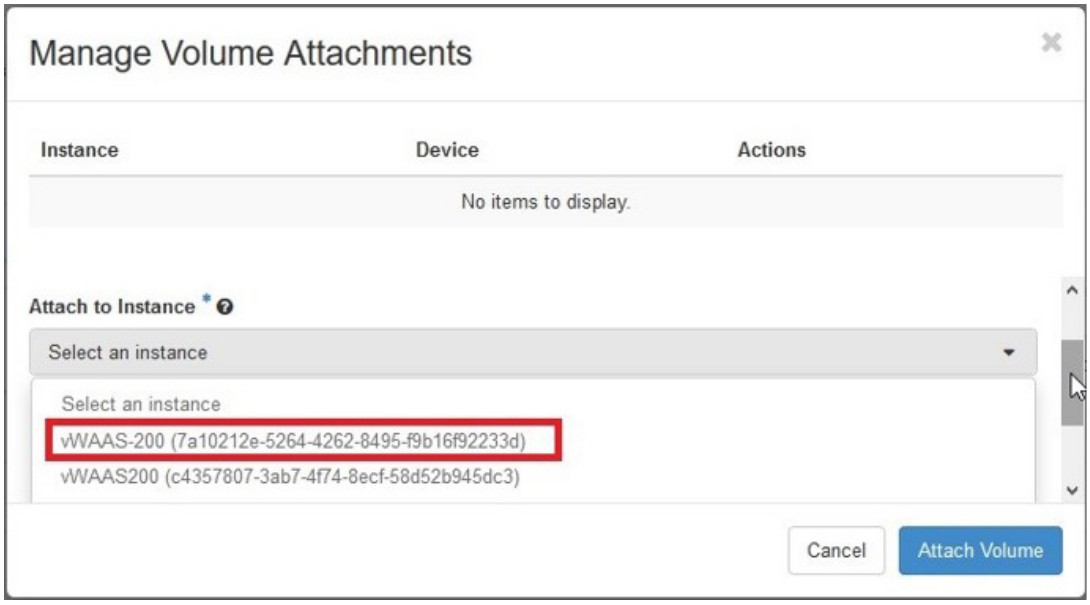
Figure 45: OpenStack Compute > Volumes Page: Attach disks to deployed instance



b) From the **Edit Volume** drop-down list, choose **Manage Attachments**.

The **Manage Volume Attachments** dialog box appears.

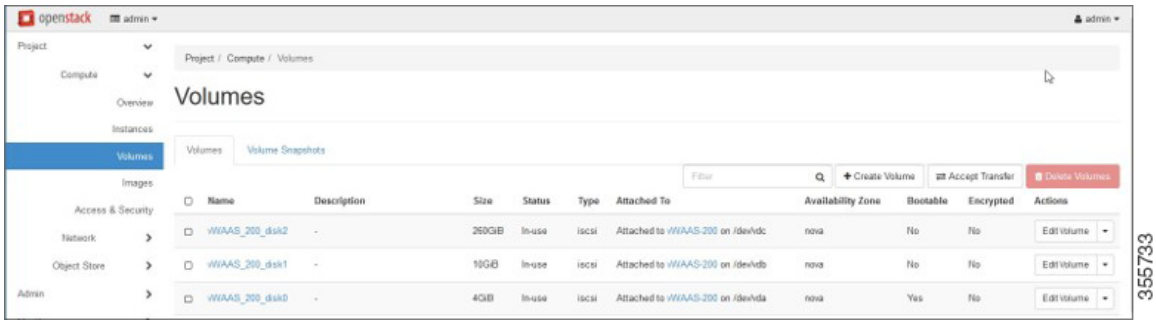
Figure 46: OpenStack Manage Volume Attachments Dialog Box



c) From the **Select an instance** drop-down list, choose the instance to attach to the disk.
d) Click **Attach Volume**.

Step 12 After attaching the disks, the **Compute > Volumes** window displays the attached disks.

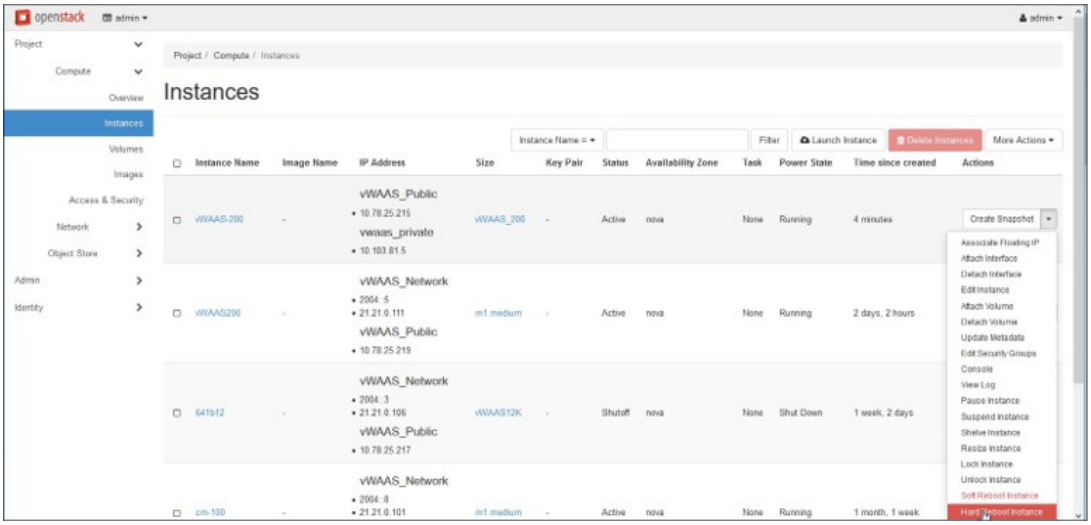
Figure 47: OpenStack Compute > Volumes Page: List of attached disks



Step 13 Reboot the system (hard reboot).

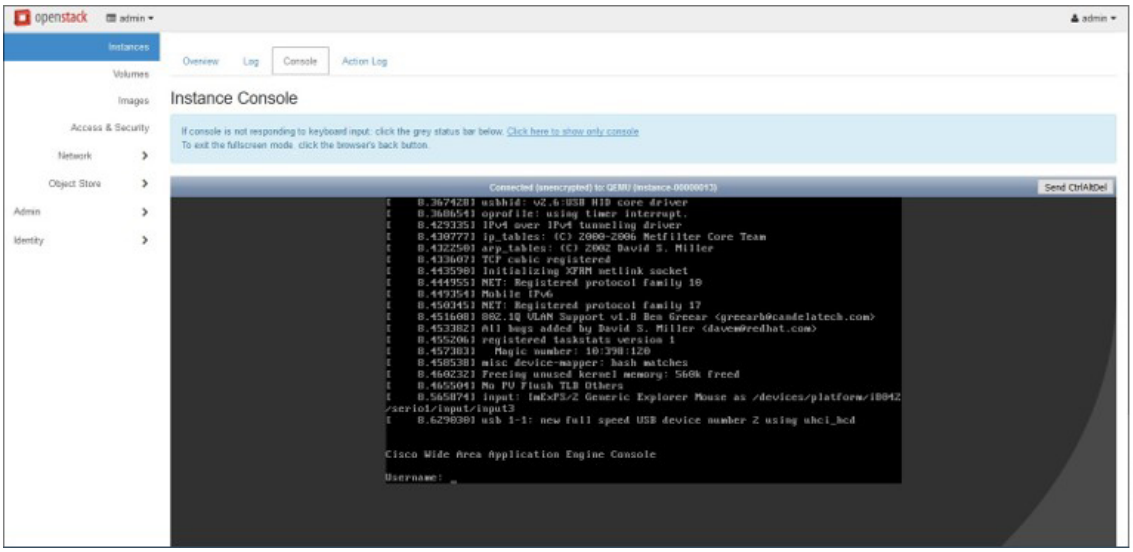
a) After the system is rebooted, choose **Compute > Instances**.
b) From the **Create Snapshot** drop-down list, choose **Hard Reboot Instance**.
c) The **Compute > Instances** window displays the attached disks.

Figure 48: OpenStack Compute > Instances Page: Attached disks listing



Step 14 From the **Instances** > **Instance Console** page, connect to the console to work on Cisco vWAAS.

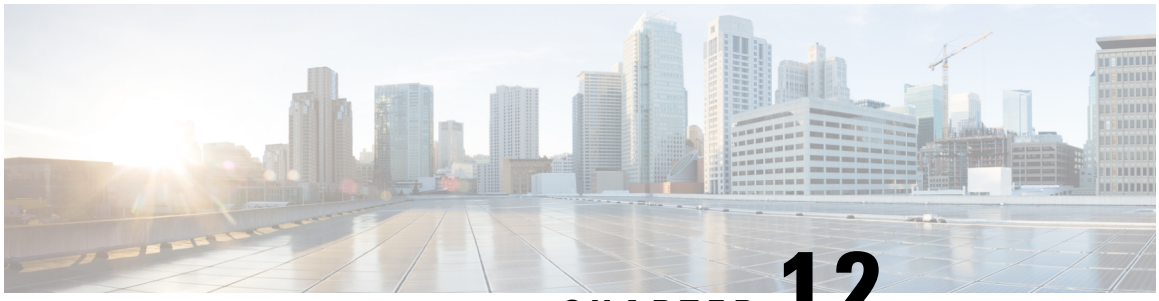
Figure 49: OpenStack Instances > Instance Console Page



Upgrade and Downgrade Guidelines for Cisco vWAAS in OpenStack

Consider the following upgrade and 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 Cisco WAAS version earlier than Version 6.4.1b is not supported.



CHAPTER 12

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

Before you begin

Under rare conditions, the Cisco 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 Cisco vWAAS device raises a **disk_failure** critical alarm for disk01 and the **show disk details** EXEC command shows disk01 as **Not used until replaced**.

Procedure

Step 1 Re-enable the disk.

Example:

```
vwaas# config
vwaas(config)# no disk disk-name disk00 shutdown force
vwaas(config)# exit
```

Step 2 Reload Cisco vWAAS.

Example:

```
vwaas# reload
```

Troubleshooting Cisco vWAAS Device Registration

You must register each Cisco vWAAS device with the Cisco WAAS Central Manager. If a Cisco vWAAS device is not registered with the Cisco WAAS Central Manager, the **Not registered alarm** is displayed when you use the **show alarms** command.

The following figure shows the output for the **show alarms** command, displaying one alarm not registered.

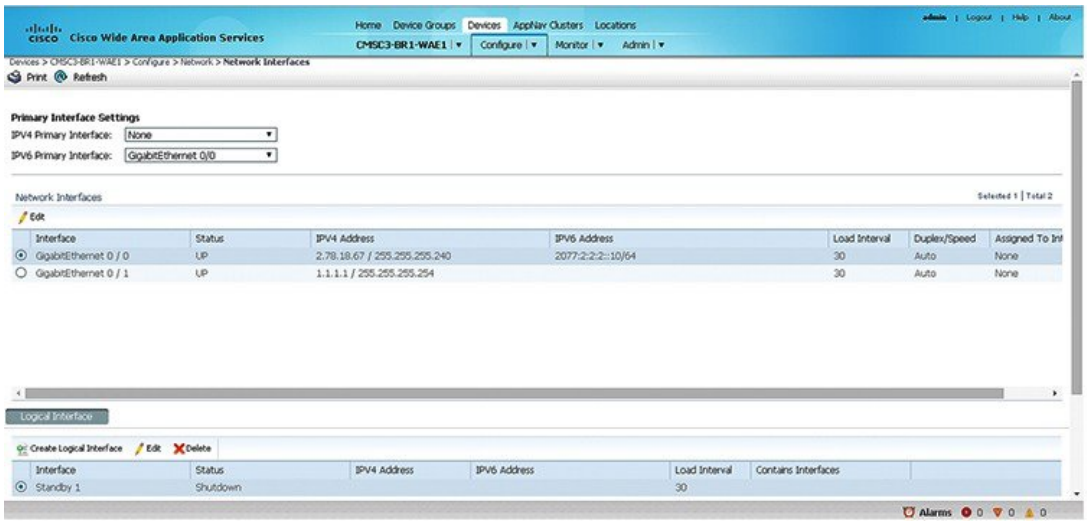
```
vWAAS# show alarms
Critical alarms:
---------------
None

Major alarms:          Module/Submodule     Instance
---------------        ----------------     -----------
Alarm ID               vwaas/model          vwaas/model     <----- Undersized alarm
1 not registered
. . .
Minor alarms:
---------------
None
```

Verifying Cisco vWAAS Virtual Interfaces

Two virtual interfaces are available on Cisco vWAAS devices, the Cisco WAAS Central Manager and the Cisco WAAS CLI.

- To display Cisco vWAAS virtual interfaces on the Cisco WAAS Central Manager, choose **Device >** *DeviceName* **> Configure > Network > Network Interfaces**. The **Network Interfaces** window appears.

Figure 50: Network Interfaces Window



To display the Cisco vWAAS virtual interfaces on the Cisco WAAS CLI, run the **show running-config interface** EXEC command. For additional details on the virtual interfaces, run the **show interface virtual 1/0** EXEC command or the **show interface virtual 2/0** EXEC command.

Troubleshooting Cisco vWAAS Networking

Before you begin

If you see no connections on the Cisco vWAAS device, use VMware VSphere Client to view the networking configuration and to check if the Cisco vWAAS device is connected to the correct vSwitch.

Procedure

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 Cisco vWAAS device: configured IP address, netmask, default gateway, and primary interface. For more information on these parameters, see Configuring Cisco vWAAS Settings, on page 37 in the chapter "Configuring Cisco vWAAS and Viewing Cisco vWAAS Components."

Step 7 From the Cisco vWAAS device, ping the default gateway and the Cisco WAAS Central Manager to verify that they are reachable.

Troubleshooting an Undersized Alarm

If the appropriate memory and hard disk resources are not allocated to the Cisco vWAAS device, the Undersized alarm is displayed when you run the show alarms command. The following figure show an example of this.

```
vWAAS# show alarms
Critical alarms:
----------------
None

Major alarms:       Module/Submodule     Instance
---------------     ----------------     -----------
Alarm ID            vwaas/model          memory      <----- Undersized alarm
1 undersized
. . .
Minor alarms:
----------------
None
```

Cisco WAAS and Cisco vWAAS provide three levels of alarms: **critical**, **major**, and **minor**. For more information on alarms and on the **show alarms** Exec command, see the *Cisco Wide Area Application Services Command Reference*.

The following table describes the fields displayed in the **show alarms** EXEC command output.

Table 80: 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. Critial alarms affect existing traffic through the WAE and are considered fatal: the WAE cannot recover and continue to process traffic.
Major Alarms	Major alarms indicate a major service (for example, 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.
Minor Alarms	Minor alarms indicate that a condition that will not affect a service has occurred, but that corrective action is required to prevent a serious fault from occurring.
Alarm ID	Type of event that caused the alarm.
Module/Submodule	The software module affected.
Instance	The object that this alarm is associated with, for example, memory. The **Instance** field does not have predefined values; each **Instance** value is application-specific.

Note You will not see the **Undersized** alarm if you are using valid OVA files to deploy Cisco vWAAS. If you see the **Undersized** alarm, delete the Cisco vWAAS VM and redeploy it using a valid OVA file.