



Cisco Virtual Wide Area Application Services Configuration Guide

vWAAS in WAAS Software Version 6.4.3x
June 18, 2020

Cisco Systems, Inc.
www.cisco.com

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Cisco Virtual Wide Area Application Services Configuration Guide
© 2006-2020 Cisco Systems, Inc. All rights reserved.



Audience	i
Document Organization	i
Document Conventions	ii
Related Documentation	ii
Obtaining Documentation and Submitting a Service Request	iii

CHAPTER 1

Introduction to Cisco vWAAS	1-1
About Cisco vWAAS	1-1
Benefits of Cisco vWAAS	1-3
Cisco vWAAS and Cisco WAAS Interoperability	1-4
OVA Package Files for Cisco vWAAS and Cisco vCM Models	1-4
Cisco vWAAS and Cisco vCM Model Profiles	1-5
Cisco vWAAS Models: CPUs, Memory, and Disk Storage	1-5
VMware VMFS Block Size and Cisco vWAAS Disk Size	1-6
Cisco vCM Models: Managed Nodes, vCPUs, Memory, and Disk Storage	1-6
Cisco vWAAS and Cisco vCM Sizing Guidelines for Cisco WAAS Version 6.4.3x	1-7
Cisco vCM on VMware ESXi Sizing Guidelines	1-7
Cisco vWAAS on Microsoft Hyper-V Sizing Guidelines	1-8
Cisco vCM on RHEL KVM Sizing Guidelines	1-11
Cisco vWAAS Resizing for WAAS Version 6.4.1a and Later	1-12
About Cisco vWAAS Resizing	1-13
Operating Guidelines for vWAAS Resizing	1-13
Original and Resized Cisco vWAAS Specifications for Cisco WAAS Version 6.4.1a and Later	1-13
Resizing Guidelines: Upgrading to Cisco WAAS Version 6.4.1a and Later	1-14
Resizing Guidelines: Installing Cisco WAAS 6.4.1a	1-16
Resizing Guidelines by Hypervisor for Cisco WAAS 6.4.1b and Later	1-17
DRE Disk, Object Cache, and Akamai Connect Cache Capacity	1-21
DRE Disk, Default Object Cache, and Default Akamai Connect Cache, by Cisco WAVE Model	1-21
Default and Resized DRE Disk, Object Cache, and Akamai Connect Cache Capacity, by Cisco vWAAS Model	1-22
Cisco Hardware Platforms Supported for Cisco vWAAS	1-23
Platforms Supported for Cisco vWAAS, by Hypervisor Type	1-23
Components for Deploying Cisco vWAAS, by Hypervisor Type	1-24

- Components for Managing Cisco vWAAS, by Hypervisor Type 1-25
- Cisco UCS E-Series Servers and NCEs 1-26
- Cisco Enterprise Network Computer System 5400-W Series 1-29
- Hypervisors Supported for Cisco vWAAS and Cisco vCM 1-31
 - About Hypervisors Supported for Cisco vWAAS and Cisco vCM 1-31
 - Hypervisor OVA Packages for Cisco vWAAS 1-32
- Cloud Platforms Supported for Cisco vWAAS 1-35

CHAPTER 2

Configuring Cisco vWAAS and Viewing Cisco vWAAS Components 2-1

- Configuring Cisco vWAAS 2-1
 - Configuring Cisco vWAAS Settings 2-1
 - Configuring Cisco vWAAS Traffic Interception 2-2
- Identifying a Cisco vWAAS Device 2-5
 - Identifying a Cisco vWAAS Model 2-5
 - Identifying a Cisco vWAAS Device on the Cisco WAAS Central Manager 2-5
 - Identifying a Cisco vWAAS Device with the Cisco WAAS CLI 2-6
- Cisco vWAAS System Partitions 2-6
- Operating Considerations for Cisco vWAAS and Cisco WAAS 2-7
- Cisco vWAAS with Single-Root I/O Virtualization 2-7
 - About Single-Root I/O Virtualization 2-8
 - Interoperability and Platforms Supported for Cisco vWAAS with SR-IOV 2-8
 - Upgrade and Downgrade Considerations for Cisco vWAAS with SR-IOV 2-9
 - Deploying Cisco vWAAS with SR-IOV 2-10
- Upgrade and Downgrade Guidelines for Cisco vWAAS 2-18
 - Upgrade Guidelines for Cisco vWAAS and Cisco vWAAS Nodes 2-19
 - Cisco vWAAS Upgrade and SCSI Controller Type 2-19
 - Cisco vWAAS Upgrade and Cisco vCM-100 with RHEL KVM or KVM on CentOS 2-19
 - Migrating a Physical Appliance Being Used as a Cisco WAAS Central Manager to a Cisco vCM 2-20
 - Downgrade Guidelines for Cisco vWAAS 2-21

CHAPTER 3

Cisco vWAAS on Cisco ISR-WAAS 3-1

- About Cisco ISR-WAAS 3-1
- Supported Host Platforms, Software Versions, and Disk Types 3-2
- Cisco OVA Packages for Cisco vWAAS on Cisco ISR-WAAS 3-2
- Deploying and Managing Cisco vWAAS on Cisco ISR-WAAS 3-3

CHAPTER 4

Cisco vWAAS on VMware ESXi	4-1
About Cisco vWAAS on VMware ESXi	4-1
Supported Host Platforms and Software Versions	4-1
VMware ESXi Server Datastore Memory and Disk Space for Cisco vWAAS and Cisco vCM Models	4-3
OVA Package Formats for Cisco vWAAS on VMware ESXi	4-4
OVA Package for Cisco vWAAS on VMware ESXi for Cisco WAAS Version 5.x to 6.2.x	4-4
OVA Package for Cisco vWAAS on VMware ESXi for Cisco WAAS Version 6.4.1 and Later	4-5
Installing Cisco vWAAS on VMware ESXi	4-6
Installing VMware ESXi for Cisco vWAAS in Cisco WAAS Versions 5.x to 6.2.x	4-6
Installing VMware ESXi for Cisco vWAAS for Cisco WAAS Version 6.4.1 through 6.4.3a	4-11
Installing VMware ESXi for Cisco vWAAS for Cisco WAAS Version 6.4.3b and Later	4-12
Operating Guidelines for Cisco vWAAS in WAAS Version 6.4.3 and later in VMware ESXi	4-25
Upgrade and Downgrade Guidelines for Cisco vWAAS on VMware ESXi	4-25

CHAPTER 5

Cisco vWAAS on Microsoft Hyper-V	5-1
About Cisco vWAAS on Microsoft Hyper-V	5-1
Supported Host Platforms, Software Versions, and Disk Type	5-2
Cisco vWAAS on Microsoft Hyper-V System Requirements	5-2
System Infrastructure Requirements	5-2
Hardware Virtualization Requirements	5-2
Deployment Options for Cisco vWAAS on Microsoft Hyper-V	5-3
OVA Package Formats for Cisco vWAAS on Microsoft Hyper-V	5-4
OVA Package for Cisco vWAAS on Microsoft Hyper-v in Cisco WAAS Version 6.1.x and Later	5-4
Unified OVA Package for Cisco vWAAS on Microsoft Hyper-V in Cisco WAAS Version 6.4.1 and Later	5-5
Installing Cisco vWAAS on Microsoft Hyper-V	5-6
Installing Cisco vWAAS on Microsoft Hyper-V for Cisco vWAAS in Cisco WAAS Version 5.x to 6.2.x	5-6
Installing Cisco vWAAS on Microsoft Hyper-V in Cisco WAAS Version 6.4.1 and Later	5-7
Activating and Registering Cisco vWAAS on Microsoft Hyper-V	5-8
Traffic Interception Methods for Cisco vWAAS on Microsoft Hyper-V	5-8
About Traffic Interception for Cisco vWAAS on Microsoft Hyper-V	5-9
WCCP Interception	5-9
AppNav Controller Interception	5-10
Operating Guidelines for Cisco vWAAS on Microsoft Hyper-V	5-11
Cisco vWAAS Deployments, Cisco UCS-E Upgrades, and Microsoft Windows Server Updates	5-11
Configuring NTP Settings for Cisco vWAAS on Microsoft Hyper-V	5-11
Microsoft Hyper-V High Availability Features	5-12

Configuring GPT Disk Format for Cisco vWAAS-50000 on Microsoft Hyper-V with Akamai Connect 5-14

CHAPTER 6

Cisco vWAAS on RHEL KVM, KVM on CentOS, and KVM in SUSE Linux 6-1

- About vWAAS on RHEL KVM, KVM on CentOS, and KVM in SUSE Linux 6-1
- Supported Host Platforms, Software Versions, and Disk Type 6-2
- Cisco vWAAS on RHEL KVM System Requirements 6-2
- Cisco vWAAS on RHEL KVM in Cisco WAAS Version 5.x to 6.2.x 6-3
 - TAR Archive Package for Cisco vWAAS on RHEL KVM in Cisco WAAS Version 5.x to 6.2.x 6-3
 - Installing Cisco vWAAS on RHEL KVM in Cisco WAAS Version 5.x to 6.2.x 6-5
- Cisco vWAAS on RHEL KVM in Cisco WAAS Version 6.4.1 and Later 6-8
 - Unified OVA Package for Cisco vWAAS on KVM in WAAS Version 6.4.1 and Later 6-8
 - Installing Cisco vWAAS on KVM in Cisco WAAS Version 6.4.1 and Later 6-9
- Operating Guidelines for Cisco vWAAS on RHEL KVM/KVM on CentOS 6-11
 - Interoperability Guidelines for Cisco vWAAS on KVM and KVM on CentOS 6-12
 - Traffic Interception Methods for Cisco vWAAS on RHEL KVM 6-13
- Upgrade and Downgrade Guidelines for Cisco vWAAS on RHEL KVM 6-13

CHAPTER 7

Cisco vWAAS on Cisco ENCS 5400-W Series 7-1

- Cisco vWAAS on Cisco ENCS 5400-W Series 7-1
 - About the Cisco ENCS 5400-W and ENCS 5400 Series 7-1
 - Cisco vWAAS as VM on Cisco ENCS 5400-W Series 7-2
 - Cisco ENCS 5400-W Models that Replace EOL/EOS Cisco WAVE Devices 7-2
 - Cisco ENCS 5400-W Hardware Features and Specifications 7-3
- Cisco vWAAS Bundled Image Install Procedure 7-4
- Strong Password Enforcement 7-7
- Shared LOM Support 7-8
- CLI Commands Used with Cisco vWAAS on Cisco ENCS 5400-W 7-9
- System Requirements for Cisco vWAAS on Cisco ENCS 5400-W with Akamai Connect 7-9
- Registering and Deploying Cisco vWAAS on a Cisco ENCS 5400-W Device 7-10
 - Registering Cisco vWAAS on a Cisco ENCS 5400-W Device 7-10
 - Deploying Cisco vWAAS with Cisco NFVIS on a Cisco ENCS 5400-W Device 7-11
 - Registering Cisco vWAAS on a Cisco ENCS 5400-W Device with the Cisco WAAS Central Manager 7-12
- Adding or Removing RAID-1 for Cisco ENCS 5400-W Series 7-12
 - Migrating Equipment from No RAID and One SSD to RAID-1 and Two SSDs 7-13
 - Migrating Equipment from RAID-1 and Two SSDs to No RAID and One SSD 7-14
- Fail-to-Wire on vWAAS on ENCS 5400-W 7-15
 - About Fail-to-Wire on Cisco vWAAS on Cisco ENCS 5400-W Series 7-15

Fail-to-Wire Traffic Interception Modes	7-15
Fail-to-Wire Failure Handling	7-16
CLI Commands for Port Channel and Standby Interfaces	7-16
Configuring Inline Interception for Fail-to-Wire on a Cisco ENCS 5400-W Device	7-18
Fail-to-Wire Upgrade and Downgrade Guidelines	7-19
Upgrade and Downgrade Guidelines for Cisco vWAAS on Cisco ENCS 5400-W	7-20

CHAPTER 8

Cisco vWAAS on Cisco CSP 5000-W Series	8-1
Cisco vWAAS on Cisco CSP 5000-W Series	8-1
About the Cisco CSP 5000-W Series	8-1
Cisco CSP 5000-W Models Supported for Cisco vWAAS	8-2
Cisco vWAAS on Cisco CSP 5000-W with Akamai Connect	8-2
Traffic Interception Methods	8-3
Cisco CSP 5000-W Hardware Features and Specifications	8-3
Deploying, Registering, and Configuring Cisco vWAAS on Cisco CSP 5000-W	8-4
Workflow for Deploying, Registering, and Configuring Cisco vWAAS on Cisco CSP 5000-W	8-5
Installing Cisco vWAAS on a Cisco CSP 5000-W Device	8-5
Configuring a Port Channel and Standby Interface	8-5
Registering or Deregistering a Cisco CSP 5000-W Device with the Cisco WAAS Central Manager	8-9
CLI Commands Used with Cisco vWAAS on Cisco CSP 5000-W	8-11
Upgrade and Downgrade Guidelines for Cisco vWAAS on Cisco CSP 5000-W	8-12

CHAPTER 9

Cisco vWAAS with Cisco Enterprise NFVIS	9-1
Cisco Enterprise NFVIS	9-1
Cisco vWAAS with Cisco Enterprise NFVIS	9-2
About Cisco vWAAS with Cisco Enterprise NFVIS	9-2
Operating Guidelines for Cisco vWAAS with Cisco Enterprise NFVIS	9-2
Platforms and Software Versions Supported for Cisco vWAAS with Cisco Enterprise NFVIS	9-2
Unified OVA Package for Cisco vWAAS with Cisco Enterprise NFVIS in Cisco WAAS Version 6.4.1 and Later	9-3
About the Unified OVA Package for Cisco vWAAS with Cisco Enterprise NFVIS in Cisco WAAS Version 6.4.1 and Later	9-4
Operating Guidelines for the Unified OVA Package Cisco vWAAS with Cisco Enterprise NFVIS in Cisco WAAS Version 6.4.1 and Later	9-4
Firmware Upgrade for Cisco Enterprise NFVIS	9-5
Traffic Interception for Cisco vWAAS with Cisco Enterprise NFVIS	9-6
Upgrade Guidelines for Cisco Enterprise NFVIS	9-8
Upgrading to Cisco Enterprise NFVIS 3.9.1 for Cisco WAAS Version 6.4.3	9-8

Upgrading to Cisco Enterprise NFVIS 3.10.1 for Cisco WAAS Version 6.4.3a	9-9
Upgrading to Cisco Enterprise NFVIS 3.11.1 for Cisco WAAS Version 6.4.3b	9-10

CHAPTER 10

Cisco vWAAS with Akamai Connect 10-1

About Cisco vWAAS with Akamai Connect	10-1
Supported Platforms for Cisco vWAAS with Akamai Connect	10-2
Cisco vWAAS with Akamai Connect License	10-3
Cisco vWAAS with Akamai Connect Hardware Requirements	10-3
Upgrading Cisco vWAAS Memory and Disk for Akamai Connect	10-4
Upgrading Memory and Disk for Cisco vWAAS in Cisco WAAS Version 5.4.1x Through 6.1.1x	10-4
Upgrading Memory and Disk for vWAAS in WAAS Versions Earlier than Cisco WAAS Version 5.4.1	10-5
Upgrading Memory and Disk for Cisco vWAAS-12000 with VMware ESXi	10-6
Upgrading Memory and Disk for Cisco vWAAS-12000 with Microsoft Hyper-V	10-7
Cisco vWAAS-150 with Akamai Connect	10-8
Cisco WAAS Central Manager and Cisco vWAAS-150	10-9
Akamai Connect Cache Engine on Cisco Mid-End and High-End Platforms	10-9

CHAPTER 11

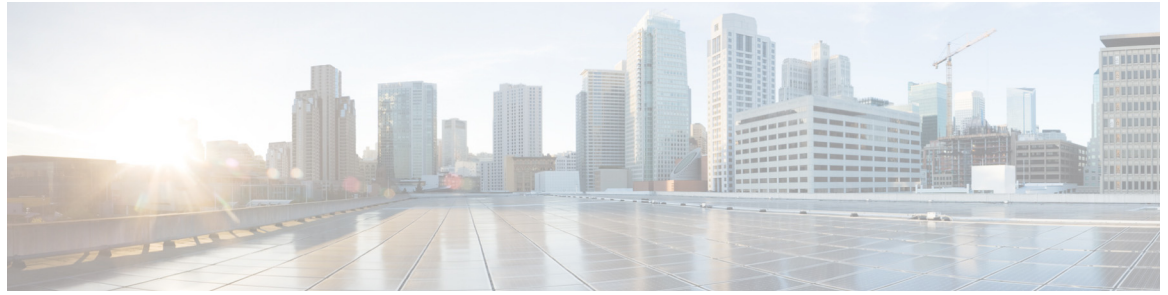
Cisco vWAAS in Cloud Computing Systems 11-1

Cisco vWAAS in Cloud Computing Systems	11-1
Cisco vWAAS in Microsoft Azure	11-1
About Cisco vWAAS in Microsoft Azure	11-2
Operating Considerations for Cisco vWAAS in Microsoft Azure	11-2
Registering the Cisco vWAAS in Microsoft Azure with the Cisco WAAS Central Manager	11-3
Deploying Cisco vWAAS in Microsoft Azure	11-4
Upgrade and Downgrade Guidelines for Cisco vWAAS in Microsoft Azure	11-9
Cisco vWAAS in OpenStack	11-9
Operating Guidelines for Cisco vWAAS in OpenStack	11-9
Upgrade and Downgrade Guidelines for Cisco vWAAS in OpenStack	11-9
Deploying Cisco vWAAS in OpenStack	11-10

CHAPTER 12

Troubleshooting Cisco vWAAS 12-1

Resolving Diskless Startup and Disk Failure	12-1
Troubleshooting Cisco vWAAS Device Registration	12-1
Verifying Cisco vWAAS Virtual Interfaces	12-2
Troubleshooting Cisco vWAAS Networking	12-3
Troubleshooting an Undersized Alarm	12-3



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, page i](#)
- [Document Organization, page i](#)
- [Document Conventions, page ii](#)
- [Related Documentation, page ii](#)
- [Obtaining Documentation and Submitting a Service Request, page iii](#)

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).

Document Organization

This guide is organized as follows:

- Chapter 1, “[Introduction to Cisco vWAAS](#)”
- Chapter 2, “[Configuring Cisco vWAAS and Viewing Cisco vWAAS Components](#)”
- Chapter 3, “[Cisco vWAAS on Cisco ISR-WAAS](#)”
- Chapter 4, “[Cisco vWAAS on VMware ESXi](#)”
- Chapter 5, “[Cisco vWAAS on Microsoft Hyper-V](#)”
- Chapter 6, “[Cisco vWAAS on RHEL KVM, KVM on CentOS, and KVM in SUSE Linux](#)”
- Chapter 7, “[Cisco vWAAS on Cisco ENCS 5400-W Series](#)”
- Chapter 8, “[Cisco vWAAS on Cisco CSP 5000-W Series](#)”
- Chapter 9, “[Cisco vWAAS with Cisco Enterprise NFVIS](#)”
- Chapter 10, “[Cisco vWAAS with Akamai Connect](#)”
- Chapter 11, “[Cisco vWAAS in Cloud Computing Systems](#)”
- Chapter 12, “[Troubleshooting Cisco vWAAS](#)”

Document Conventions

Command descriptions use these conventions:

boldface font	Commands and keywords are in boldface.
<i>italic font</i>	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.
<i>italic screen font</i>	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 WAAS software and hardware, see the following documentation:

- [Cisco Wide Area Application Services Upgrade Guide](#)
- [Cisco Wide Area Application Services Quick Configuration Guide](#)
- [Cisco Wide Area Application Services Configuration Guide](#)
- [Cisco Wide Area Application Services Command Reference](#)

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

Obtaining Documentation and Submitting a Service Request

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

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

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





Introduction to Cisco vWAAS

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

This chapter contains the following sections:

- [About Cisco vWAAS, page 1-1](#)
- [Cisco vWAAS and Cisco WAAS Interoperability, page 1-4](#)
- [OVA Package Files for Cisco vWAAS and Cisco vCM Models, page 1-4](#)
- [Cisco vWAAS and Cisco vCM Model Profiles, page 1-5](#)
- [Cisco vWAAS and Cisco vCM Sizing Guidelines for Cisco WAAS Version 6.4.3x, page 1-7](#)
- [Cisco vWAAS Resizing for WAAS Version 6.4.1a and Later, page 1-12](#)
- [DRE Disk, Object Cache, and Akamai Connect Cache Capacity, page 1-21](#)
- [Cisco Hardware Platforms Supported for Cisco vWAAS, page 1-23](#)
- [Hypervisors Supported for Cisco vWAAS and Cisco vCM, page 1-31](#)
- [Cloud Platforms Supported for Cisco vWAAS, page 1-35](#)

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, 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.

Table 1-1 shows the hypervisors supported for Cisco vWAAS. For more information on each of these hypervisors, see [Hypervisors Supported for Cisco vWAAS and Cisco vCM, page 1-31](#) and in the chapters listed in Table 1-1.

Table 1-1 Hypervisors Supported for Cisco vWAAS

Hypervisor	For More Information:
Cisco ISR-WAAS	Chapter 3, “ Cisco vWAAS on Cisco ISR-WAAS ”
VMware vSphere ESXi	Chapter 4, “ Cisco vWAAS on VMware ESXi ”
Microsoft HyperV	Chapter 5, “ Cisco vWAAS on Microsoft Hyper-V ”
RHEL KVM	Chapter 6, “ Cisco vWAAS on RHEL KVM, KVM on CentOS, and KVM in SUSE Linux ”
KVM on CentOS	Chapter 6, “ Cisco vWAAS on RHEL KVM, KVM on CentOS, and KVM in SUSE Linux ”
KVM in SUSE Linux	Chapter 6, “ Cisco vWAAS on RHEL KVM, KVM on CentOS, and KVM in SUSE Linux ”
Cisco Enterprise NFVIS	Chapter 9, “ Cisco vWAAS with Cisco Enterprise NFVIS ”

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, page 1-23](#).

- Hardware platforms
 - Cisco Unified Computing System (UCS)
 - Cisco UCS E-Series Servers
 - Cisco UCS E-Series Network Compute Engines (NCEs)
 - Cisco ISR-4000 Series
 - Cisco ENCS 5400-W Series
 - Cisco CSP 5000-W Series
- Cloud Computing Systems
 - Microsoft Azure Cloud
 - OpenStack

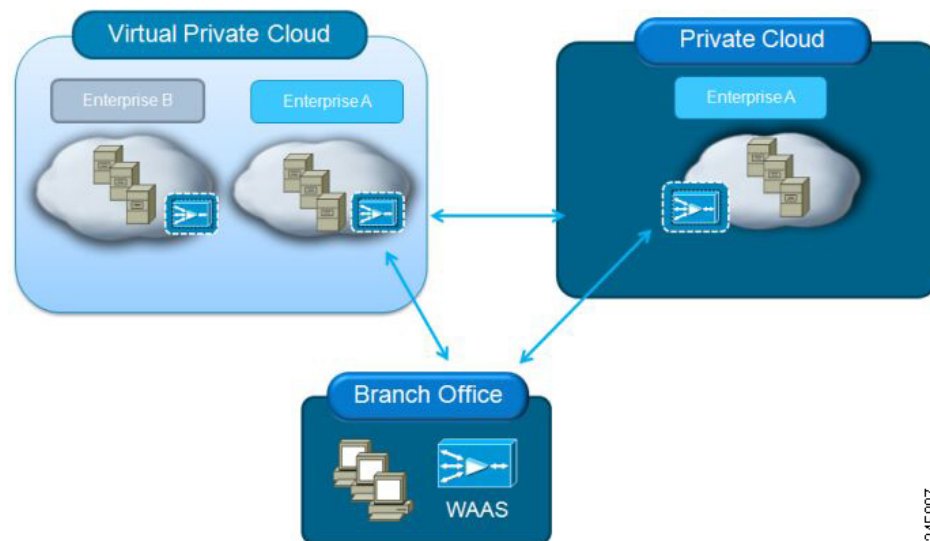
For details on the interoperability of the hypervisors and platforms supported for Cisco vWAAS, see [Table 1-20](#).

As shown in [Figure 1-1](#), you can enable Cisco vWAAS at the branch or data center or both:

- At the branch: With Cisco ENCS 5400 Series, Cisco Unified Computing System (UCS) E-Series servers and E-Series Network Compute Engines (NCEs), on either the Cisco 4000 Series ISRs or Cisco ISR G2 branch router.
- At the data center: With Cisco UCS server.

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.

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



Benefits of Cisco vWAAS

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

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

Cisco vWAAS and Cisco WAAS Interoperability

Consider the following guidelines when using Cisco vWAAS with Cisco 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 Cisco vCM Models

Table 1-2 shows the OVA and NPE OVA file for each Cisco vWAAS model:

Table 1-2 OVA Package Files for Cisco vWAAS Models

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

Table 1-3 shows the OVA and NPE OVA file for each Cisco vCM model (all the models are available with Cisco WAAS version 4.3.1 and later, except when noted otherwise):

Table 1-3 OVA Package Files for Cisco vCM Models

Cisco 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 and Cisco vCM Model Profiles

This section contains the following topics:

- [Cisco vWAAS Models: CPUs, Memory, and Disk Storage](#), page 1-5
- [VMware VMFS Block Size and Cisco vWAAS Disk Size](#), page 1-6
- [Cisco vCM Models: Managed Nodes, vCPUs, Memory, and Disk Storage](#), page 1-6

Cisco vWAAS Models: CPUs, Memory, and Disk Storage

This section contains the following topics:

- [Operating Guidelines for Cisco vWAAS CPUs, Memory and Disk Storage](#), page 1-5
- [Cisco vWAAS Memory and Disk Storage Information for Akamai Connect and Cisco ENCS 5400-W](#), page 1-5

Operating Guidelines for Cisco vWAAS 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. [Table 1-17](#) shows the resizing capability for Cisco vWAAS in Cisco WAAS Version 6.4.1a and later.
- When Cisco vWAAS-6000, 1300, 12000, or 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.

Cisco vWAAS Memory and Disk Storage Information for Akamai Connect and Cisco ENCS 5400-W

[Table 1-4](#) shows where to find additional memory and disk storage information for Akamai Connect and Cisco ENCS 5400-W, by Cisco vWAAS model.

Table 1-4 For More Information on Specific Cisco vWAAS Models

Cisco vWAAS Model	For more information:
vWAAS-150	<ul style="list-style-type: none"> • See Cisco vWAAS-150 with Akamai Connect in the chapter “Cisco vWAAS with Akamai Connect”.
vWAAS-6000-R	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • See Akamai Connect Cache Engine on Cisco Mid-End and High-End Platforms in the chapter “Cisco vWAAS with Akamai Connect”.

Cisco vWAAS Model	For more information:
vWAAS models with Akamai Connect	<ul style="list-style-type: none"> See Cisco vWAAS with Akamai Connect Hardware Requirements in the chapter “Cisco vWAAS with Akamai Connect.”
vWAAS models on Cisco ENCS 5400 Series	<ul style="list-style-type: none"> 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 Cisco vWAAS Disk Size

[Table 1-5](#) shows the VMware Virtual Machine File System (VMFS) block size and associated vWAAS maximum disk file size. For more information on VMware and Cisco vWAAS interoperability, see [Table 1-20](#).

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

VMFS Block Size	Cisco 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

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



Note

Cisco 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 [Table 1-6](#).

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

Cisco vCM Model	Managed Nodes	Required vCPUs	Recommended vCPUs	Required Memory	Recommended Memory	Disk Storage
vCM-100	100	2	2	2 GB	3 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 Cisco vCM Sizing Guidelines for Cisco WAAS Version 6.4.3x

This section contains the following topics:

- [Cisco vCM on VMware ESXi Sizing Guidelines, page 1-7](#)
- [Cisco vWAAS on Microsoft Hyper-V Sizing Guidelines, page 1-8](#)
- [Cisco vCM on RHEL KVM Sizing Guidelines, page 1-11](#)



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 topics:

- [Cisco vCM on VMware ESXi: Central Manager Mode Sizing Guidelines, page 1-7](#)
- [Cisco vCM on VMware ESXi: Virtual Hardware Requirements, page 1-8](#)
- [Cisco vCM on VMware ESXi: Hardware Requirements, page 1-8](#)

Cisco vCM on VMware ESXi: Central Manager Mode Sizing Guidelines

Table 1-7 Cisco vCM Sizing Guidelines: Central Manager Mode

vCM Model	Number of Nodes (WAAS Devices Only)	Number of Nodes (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

**Note**

In [Table 1-7](#), the **Number of Nodes (WAAS and Other Devices)** column: In cases when the WAAS Central Manager manages WAAS devices the total number of managed devices can be reduced by 20% compared to management of only WAAS devices.

Cisco vCM on VMware ESXi: Virtual Hardware Requirements

Table 1-8 Cisco vCM on VMware ESXi: Virtual Hardware Requirements

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	2	254
vCM-500N	2	4	2 GB	5 GB	2	304
vCM-1000N	2	6	4 GB	8 GB	2	404
vCM-2000N	4	8	8 GB	16 GB	2	604

Cisco vCM on VMware ESXi: Hardware Requirements

Table 1-9 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 topics:

- [Cisco vWAAS on Microsoft Hyper-V: Connections Sizing Guidelines](#), page 1-9
- [Cisco vWAAS on Microsoft Hyper-v: Bandwidth, Throughput, Disk, and Cache Sizing Guidelines](#), page 1-9
- [Cisco vWAAS on Microsoft Hyper-v: Virtual Hardware Requirements](#), page 1-11
- [Cisco vWAAS on Microsoft Hyper-v: Hardware Requirements](#), page 1-11

Cisco vWAAS on Microsoft Hyper-V: Connections Sizing Guidelines

Table 1-10 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 Encrypted MAPI (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	15,000	15,000	50,000

Consider the following guidelines for connections sizing for Cisco vWAAS on Microsoft Hyper-V, as shown in [Table 1-10](#):

- 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** columns: These connections, when used, are part of the overall connection limit for the device.
- For the **Optimized MAPI Connections** and **Optimized Encrypted MAPI (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.

Cisco vWAAS on Microsoft Hyper-v: Bandwidth, Throughput, Disk, and Cache Sizing Guidelines

Table 1-11 Cisco vWAAS on Microsoft Hyper-V 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	---

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-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 [Table 1-11](#).

- 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

Cisco vWAAS on Microsoft Hyper-v: Virtual Hardware Requirements

Table 1-12 Cisco vWAAS on 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

Cisco vWAAS on Microsoft Hyper-v: Hardware Requirements

Table 1-13 Cisco vWAAS on 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
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 topics:

- [Cisco vCM on RHEL KVM: Central Manager Mode Sizing Guidelines, page 1-12](#)
- [Cisco vCM on RHEL KVM: Virtual Hardware Requirements, page 1-12](#)
- [Cisco vCM on RHEL KVM: Hardware Requirements, page 1-12](#)

Cisco vCM on RHEL KVM: Central Manager Mode Sizing Guidelines

Table 1-14 vCM 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 [Table 1-14](#), 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.

Cisco vCM on RHEL KVM: Virtual Hardware Requirements

Table 1-15 Cisco vCM on 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 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

Cisco vCM on RHEL KVM: Hardware Requirements

Table 1-16 Cisco vCM on 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 Resizing for WAAS Version 6.4.1a and Later

This section contains the following topics:

- [About Cisco vWAAS Resizing, page 1-13](#)
- [Operating Guidelines for vWAAS Resizing, page 1-13](#)

- [Original and Resized Cisco vWAAS Specifications for Cisco WAAS Version 6.4.1a and Later, page 1-13](#)
- [Resizing Guidelines: Upgrading to Cisco WAAS Version 6.4.1a and Later, page 1-14](#)
- [Resizing Guidelines: Installing Cisco WAAS 6.4.1a, page 1-16](#)
- [Resizing Guidelines by Hypervisor for Cisco WAAS 6.4.1b and Later, page 1-17](#)

About Cisco vWAAS Resizing

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.

Therefore, we highly recommend the following actions:

- Resize CPU and memory resources, as shown in [Table 1-17](#).
- Resize the DRE object cache and Akamai Connect Cache, as shown in [Table 1-19](#).
- For optimum performance, use the SSD disk with the UCS models listed in [Table 1-17](#).

Operating Guidelines for vWAAS Resizing

Consider the following operating guidelines for 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.

Original and Resized Cisco vWAAS Specifications for Cisco WAAS Version 6.4.1a and Later

- [Table 1-17](#) shows the original and resized Cisco vWAAS CPU and memory specifications, as well as tested clock speed and minimum recommended platform.
- [Table 1-19](#) shows the default and resized DRE disk capacity, object cache capacity, and Akamai Connect cache capacity, by Cisco vWAAS model.

Table 1-17 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 Recommended Cisco Platform
vWAAS-150 (earliest supported version: Cisco 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 CPUs	1.9 GHz	8 GB	16 GB	UCS-E160S-M3
vWAAS-6000	4 CPUs	8 CPUs	2.0 GHz	11 GB	24 GB	UCS-E180D-M3
vWAAS-6000R (earliest supported version: Cisco WAAS 6.4.x)	4 CPUs	8 CPUs	2.0 GHz	11 GB	24 GB	UCS-E180D-M3
vWAAS-12000	4 CPUs	12 CPUs	2.6 GHz	12 GB	48 GB	UCS-C220 or UCS-C240
vWAAS-50000	8 CPUs	16 CPUs	2.6 GHz	48 GB	72 GB	UCS-C220 or UCS-C240
vWAAS-150000 (earliest supported version: Cisco WAAS 6.4.1a)	24 CPUs	---	3.0 Ghz	96 GB	---	UCS C220 M5 For more information, see the Cisco UCS C220 M5 Rack Server Data Sheet .

Resizing Guidelines: Upgrading to Cisco WAAS Version 6.4.1a and Later

This section contains the following procedures:

- [Upgrading to Cisco WAAS Version 6.4.1a and Later with Existing CPU and Memory, page 1-14](#)
- [Upgrading to Cisco WAAS Version 6.4.1a and Later with Resized CPU and Memory, page 1-15](#)

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

This section contains the following topics:

- [Using the Cisco WAAS CLI to Perform an Upgrade with Existing CPU Memory, page 1-14](#)
- [Using the Cisco WAAS Central Manager to Perform an Upgrade with Existing CPU and Memory, page 1-15](#)

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 Cisco WAAS Version 6.4.1a and Later with Resized CPU and Memory

This section contains the following topics:

- [Using the Cisco WAAS CLI to Perform an Upgrade with Resized CPU and Memory, page 1-15](#)
- [Using the Cisco WAAS Central Manager to Perform an Upgrade with Resized CPU and Memory, page 1-16](#)

Using the Cisco WAAS CLI to Perform an Upgrade with Resized CPU and Memory

Before you begin:

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.

To perform an upgrade with resized CPU and memory using the Cisco WAAS CLI, follow these steps:

Step 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:
 1. Open **Virtual Manager**.
 2. Choose **Virtual Machine** > **CPUs**.
 3. Choose **Virtual Machine** > **Memory**.
- To change settings in Cisco NFVIS, for the Cisco vBranch solution:
 1. Choose **VM Life Cycle** > **Image Repository** > **Profiles** and add another profile with: resized CPU, memory, and same disk size.
 2. Choose **VM Life Cycle** > **Deploy** > **VM Details** and select the resized profile created.

3. Click **Deploy**.

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

- To change settings Microsoft Azure:
 - a. Choose **Deployments > Microsoft Template Overview > Custom Deployment**,
 - b. Choose **Home > Virtual Machines > vWAAS Instance > Size**.

Step 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 an 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: Installing Cisco WAAS 6.4.1a

This section contains the following topics:

- [New Installation with Existing CPU and Memory, page 1-16](#)
- [New Installation with Resized CPU and Memory, page 1-17](#)

New Installation with Existing CPU and Memory

1. Install the Cisco vWAAS OVA with a Cisco WAAS version earlier than Cisco WAAS Version 6.4.1a, which, by default, will deploy with resized resource.
2. Upgrade to Cisco WAAS Version 6.4.1a and retain existing CPU and memory resources.

3. After installation is complete, there will be undersized-resource alarms for CPU and memory for the Cisco vWAAS device. You use the **show alarms** command to display information about undersized alarms for the Cisco vWAAS model.
4. After resources are upgraded, there will not be any automatic change in resources for subsequent upgrades/downgrades of the system.

New Installation with Resized CPU and Memory

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

Resizing Guidelines by Hypervisor for Cisco WAAS 6.4.1b and Later

This section contains the following topics:

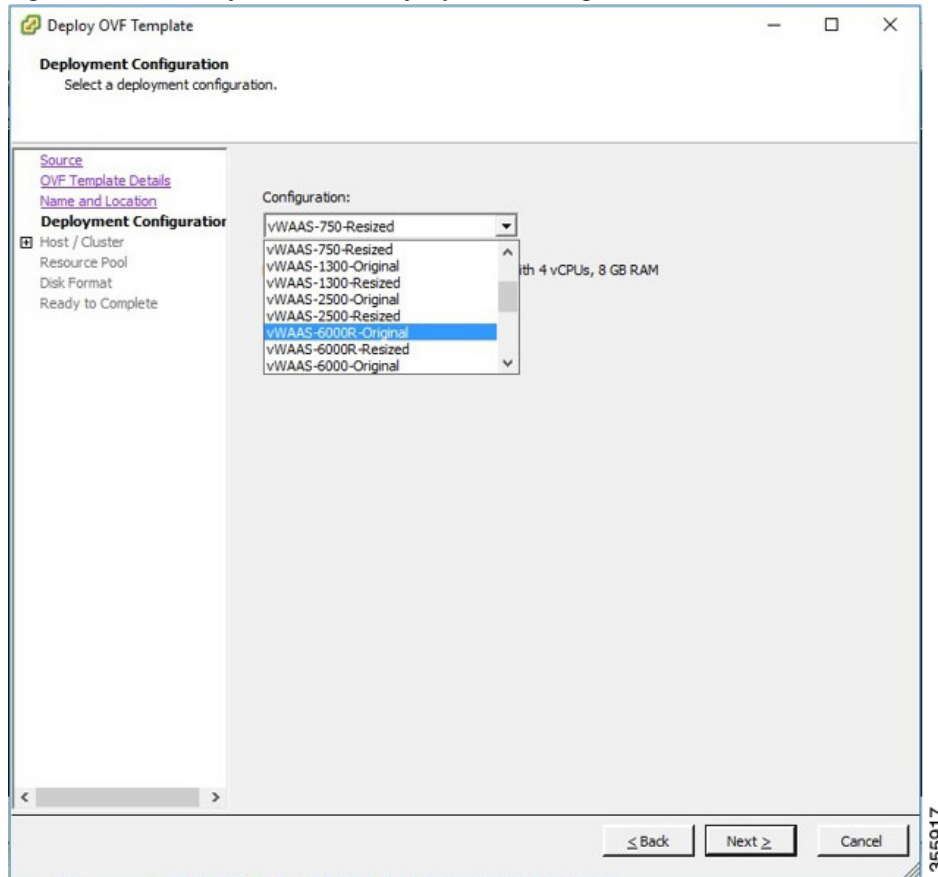
- [Resizing for Cisco vWAAS on VMware ESXi, page 1-17](#)
- [Resizing for Cisco vWAAS on Microsoft Hyper-V, page 1-18](#)
- [Resizing for Cisco vWAAS on RHEL CentOS or SUSE Linux, page 1-19](#)
- [Resizing for Cisco vWAAS on NFVIS, page 1-21](#)

Resizing for Cisco vWAAS on VMware ESXi

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

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

Figure 1-2 vSphere Client Deployment Configuration Window



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

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

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

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

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

```

PS C:\Users\Administrator\Desktop\platform-hv\6.4.3-b555\Cisco-HyperV-vWAAS-unified-6.4.3-b555> .\deploy-cisco-waas-scv
m.ps1

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

WAAS supports below models
S.No  Model                Original Resources    Resized Resources
      Model                vCPU  MEMORY             vCPU  MEMORY
-----
1.    vWAAS-150             1      3GB                 2      4GB
2.    vWAAS-200             1      3GB                 2      4GB
3.    vWAAS-750             2      4GB                 4      8GB
4.    vWAAS-1300           2      6GB                 4      12GB
5.    vWAAS-2500           4      8GB                 6      16GB
6.    vWAAS-6000R          4      11GB                8      24GB
7.    vWAAS-6000           4      11GB                8      24GB
8.    vWAAS-12000          4      12GB                12     48GB
9.    vWAAS-50000          8      48GB                16     72GB
10.   vCM-100N              2      2GB                 NA     NA
11.   vCM-500N              2      2GB                 NA     NA
12.   vCM-1000N            2      4GB                 NA     NA
13.   vCM-2000N            4      8GB                 NA     NA

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

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

```

355918

- Step 2** At the **Enter vWAAS/vCM model to install** prompt, enter the line number for the model that you want to install. For example, from the listing shown in [Figure 1-3](#), entering 7 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-b555\Cisco-HyperV-vWAAS-unified-6.4.3-b555
Loading System Center Virtual Machine Manager Powershell Module...
Powershell module loaded.

```

Resizing for Cisco vWAAS on RHEL CentOS or SUSE Linux

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

- Step 1** In the **root@localhost** window, enter the resizing launch script:
- ```
[root@localhost]# ./launch.sh nresized macvtap br-ex br-ext1
```
- Step 2** The system displays original and resized resources for each Cisco vWAAS model ([Figure 1-4](#)):

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

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

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

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

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

| SNO | MODEL | NAME  | ORIGINAL RESOURCES |        | RESIZED RESOURCES |        |
|-----|-------|-------|--------------------|--------|-------------------|--------|
|     |       |       | CPU                | MEMORY | CPU               | MEMORY |
| 1.  | vWAAS | 150   | 1                  | 4GB    | 2                 | 4GB    |
| 2.  | vWAAS | 200   | 1                  | 4GB    | 2                 | 4GB    |
| 3.  | vWAAS | 750   | 2                  | 4GB    | 4                 | 8GB    |
| 4.  | vWAAS | 1300  | 2                  | 6GB    | 4                 | 12GB   |
| 5.  | vWAAS | 2500  | 4                  | 8GB    | 6                 | 16GB   |
| 6.  | vWAAS | 6000R | 4                  | 11GB   | 8                 | 24GB   |
| 7.  | vWAAS | 6000  | 4                  | 11GB   | 8                 | 24GB   |

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

355921

**Step 3** At the **Select the model type** prompt, enter the line number of the model type for your system. For example, clicking **7** 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 [Figure 1-4](#).



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



## Resizing for Cisco vWAAS on NFVIS

To resize Cisco vWAAS on Cisco NFVIS, install the Cisco vWAAS OVA with Cisco WAAS Version 6.4.1b. [Figure 1-5](#) shows the NFVIS profiles listing for original and resized Cisco vWAAS resources.






**Figure 1-5** Cisco vWAAS Profiles Listing on Cisco vWAAS on NFVIS

| Image Name                               | State  | Type  | Version    | Storage Location | Action                                                                                                                                                                  |
|------------------------------------------|--------|-------|------------|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cisco-KVM-WAAS-Unified-6.4.1b-b29.tar.gz | ACTIVE | vWAAS | 6.4.1b-b29 | Internal         |   |

Showing 1 to 1 of 1 entries

Previous 1 Next

| Profile             | CPU | Memory (MB) | Disk (MB) | Source Image                             | Action                                                                              |
|---------------------|-----|-------------|-----------|------------------------------------------|-------------------------------------------------------------------------------------|
| vWAAS-1300-Original | 2   | 6144        | 614400    | Cisco-KVM-WAAS-Unified-6.4.1b-b29.tar.gz |  |
| vWAAS-1300-Resized  | 4   | 12288       | 614400    | Cisco-KVM-WAAS-Unified-6.4.1b-b29.tar.gz |  |
| vWAAS-150-Original  | 1   | 4096        | 163840    | Cisco-KVM-WAAS-Unified-6.4.1b-b29.tar.gz |  |
| vWAAS-150-Resized   | 2   | 4096        | 163840    | Cisco-KVM-WAAS-Unified-6.4.1b-b29.tar.gz |  |
| vWAAS-200-Original  | 1   | 4096        | 266240    | Cisco-KVM-WAAS-Unified-6.4.1b-b29.tar.gz |  |

Showing 1 to 5 of 14 entries

Previous 1 2 3 Next

For 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

This section contains the following topics:

- [DRE Disk, Default Object Cache, and Default Akamai Connect Cache, by Cisco WAVE Model, page 1-21](#)
- [Default and Resized DRE Disk, Object Cache, and Akamai Connect Cache Capacity, by Cisco vWAAS Model, page 1-22](#)

## DRE Disk, Default Object Cache, and Default Akamai Connect Cache, by Cisco WAVE Model

[Table 1-18](#) shows the DRE disk, default object cache, and default Akamai Connect cache, by Cisco WAVE model.

**Table 1-18** 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                                 |
| 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                                |

## Default and Resized DRE Disk, Object Cache, and Akamai Connect Cache Capacity, by Cisco vWAAS Model

Table 1-19 shows the default and resized DRE disk capacity, object cache capacity, and Akamai Connect cache capacity, by Cisco vWAAS model.

**Table 1-19** 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, page 1-23](#)
- [Components for Deploying Cisco vWAAS, by Hypervisor Type, page 1-24](#)
- [Components for Managing Cisco vWAAS, by Hypervisor Type, page 1-25](#)
- [Cisco UCS E-Series Servers and NCEs, page 1-26](#)
- [Cisco Enterprise Network Computer System 5400-W Series, page 1-29](#)

## Platforms Supported for Cisco vWAAS, by Hypervisor Type

For each hypervisor used with Cisco vWAAS, [Table 1-20](#) 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 1-20** *Platforms Supported for Cisco vWAAS, by Hypervisor Type*

| Hypervisor     | PID and Device Type                                                                                                      | Earliest Supported Cisco WAAS Version                                                                                              | Host Platforms                                                                                                                                                                                                                                                         | Earliest Supported Host Version                                | Disk Type                                                                      |
|----------------|--------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------|--------------------------------------------------------------------------------|
| Cisco ISR-WAAS | <ul style="list-style-type: none"> <li>• PID: <b>OE-VWAAS-KVM</b></li> <li>• Device Type: <b>ISR-WAAS</b></li> </ul>     | <ul style="list-style-type: none"> <li>• 6.4.1b (ISR-4461)</li> <li>• 5.4.1</li> <li>• 5.2.1 (ISR-4451)</li> </ul>                 | <ul style="list-style-type: none"> <li>• ISR-4461 (vWAAS-750, 1300, 2500)</li> <li>• ISR-4451 (vWAAS-750, 1300, 2500)</li> <li>• ISR-4431 (vWAAS-750, 1300)</li> <li>• ISR-4351 (vWAAS-750)</li> <li>• ISR-4331 (vWAAS-750)</li> <li>• ISR-4321 (vWAAS-200)</li> </ul> | <ul style="list-style-type: none"> <li>• IOS-XE 3.9</li> </ul> | <ul style="list-style-type: none"> <li>• ISR-SSD</li> <li>• NIM-SSD</li> </ul> |
| Cisco NFVIS    | <ul style="list-style-type: none"> <li>• PID: <b>OE-VWAAS-KVM</b></li> <li>• Device Type: <b>OE-VWAAS-KVM</b></li> </ul> | <ul style="list-style-type: none"> <li>• 6.2.x (Cisco UCS-E Series)</li> <li>• 6.4.1 (Cisco ENCS 5400 Series and Cisco)</li> </ul> | <ul style="list-style-type: none"> <li>• Cisco ENCS (Enterprise Network Compute System) 5400 Series</li> <li>• Cisco UCS-E Series</li> </ul>                                                                                                                           | <ul style="list-style-type: none"> <li>• NFV FC2</li> </ul>    | <ul style="list-style-type: none"> <li>• virtio</li> </ul>                     |

| Hypervisor          | PID and Device Type                                                                                                                  | Earliest Supported Cisco WAAS Version                      | Host Platforms                                                                                                         | Earliest Supported Host Version                                                            | Disk Type                                                  |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|------------------------------------------------------------|
| VMware vSphere ESXi | <ul style="list-style-type: none"> <li>• PID: <b>OE-VWAAS-ESX</b></li> <li>• Device Type: <b>OE-VWAAS-ESX</b></li> </ul>             | <ul style="list-style-type: none"> <li>• 5.0.3g</li> </ul> | <ul style="list-style-type: none"> <li>• Cisco UCS (Unified Computing System)</li> <li>• Cisco UCS-E Series</li> </ul> | <ul style="list-style-type: none"> <li>• ESXi 5.0</li> </ul>                               | <ul style="list-style-type: none"> <li>• VMDK</li> </ul>   |
| Microsoft Hyper-V   | <ul style="list-style-type: none"> <li>• PID: <b>OE-VWAAS-HYPERV</b></li> <li>• Device Type: <b>OE-VWAAS-HYPERV</b></li> </ul>       | <ul style="list-style-type: none"> <li>• 6.1.x</li> </ul>  | <ul style="list-style-type: none"> <li>• Cisco UCS</li> <li>• Cisco UCS-E Series</li> </ul>                            | <ul style="list-style-type: none"> <li>• Microsoft Windows 2008 R2</li> </ul>              | <ul style="list-style-type: none"> <li>• VHD</li> </ul>    |
| RHEL KVM            | <ul style="list-style-type: none"> <li>• PID: <b>OE-VWAAS-KVM</b></li> <li>• Device Type: <b>OE-VWAAS-KVM</b></li> </ul>             | <ul style="list-style-type: none"> <li>• 6.2.x</li> </ul>  | <ul style="list-style-type: none"> <li>• Cisco UCS</li> <li>• Cisco UCS-E Series</li> </ul>                            | <ul style="list-style-type: none"> <li>• RHEL CentOS 7.1</li> </ul>                        | <ul style="list-style-type: none"> <li>• virtio</li> </ul> |
| SUSE Linux          | <ul style="list-style-type: none"> <li>• PID: <b>OE-VWAAS-GEN-LINUX</b></li> <li>• Device Type: <b>OE-VWAAS-GEN-LINUX</b></li> </ul> | <ul style="list-style-type: none"> <li>• 6.4.1b</li> </ul> | <ul style="list-style-type: none"> <li>• Cisco UCS</li> <li>• Cisco UCS-E Series</li> </ul>                            | <ul style="list-style-type: none"> <li>• SUSE Linux Enterprise Server (SLES) 12</li> </ul> | <ul style="list-style-type: none"> <li>• virtio</li> </ul> |
| Microsoft Azure     | <ul style="list-style-type: none"> <li>• PID: <b>OE-VWAAS-AZURE</b></li> <li>• Device Type: <b>OE-VWAAS-AZURE</b></li> </ul>         | <ul style="list-style-type: none"> <li>• 6.2.x</li> </ul>  | <ul style="list-style-type: none"> <li>• Microsoft Azure cloud</li> </ul>                                              | <ul style="list-style-type: none"> <li>• N/A</li> </ul>                                    | <ul style="list-style-type: none"> <li>• VHD</li> </ul>    |
| OpenStack           | <ul style="list-style-type: none"> <li>• PID: <b>OE-VWAAS-OPENSTACK</b></li> <li>• Device Type: <b>OE-VWAAS-OPENSTACK</b></li> </ul> | <ul style="list-style-type: none"> <li>• 6.4.1b</li> </ul> | <ul style="list-style-type: none"> <li>• OpenStack cloud</li> </ul>                                                    | <ul style="list-style-type: none"> <li>• OpenStack Mitaka</li> </ul>                       | <ul style="list-style-type: none"> <li>• virtio</li> </ul> |

## Components for Deploying Cisco vWAAS, by Hypervisor Type

For each hypervisor used with Cisco vWAAS, [Table 1-21](#) shows the components used to deploy Cisco vWAAS, including package format, deployment tool, preconfiguration tool (if needed), and network driver.

**Table 1-21** Components for Deploying Cisco vWAAS, by Hypervisor Type

| Hypervisor          | Package Format                                          | Deployment Tool                                                                   | Preconfiguration Tool                                                     | Network Driver                                                 |
|---------------------|---------------------------------------------------------|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------|----------------------------------------------------------------|
| Cisco ISR-WAAS      | <ul style="list-style-type: none"> <li>• OVA</li> </ul> | <ul style="list-style-type: none"> <li>• Ezconfig</li> </ul>                      | <ul style="list-style-type: none"> <li>• onep</li> </ul>                  | <ul style="list-style-type: none"> <li>• virtio_net</li> </ul> |
| Cisco NFVIS         | <ul style="list-style-type: none"> <li>• TAR</li> </ul> | <ul style="list-style-type: none"> <li>• NFVIS</li> </ul>                         | <ul style="list-style-type: none"> <li>• Bootstrap Day0 config</li> </ul> | <ul style="list-style-type: none"> <li>• virtio_net</li> </ul> |
| VMware vSphere ESXi | <ul style="list-style-type: none"> <li>• OVA</li> </ul> | <ul style="list-style-type: none"> <li>• —</li> </ul>                             | <ul style="list-style-type: none"> <li>• —</li> </ul>                     | <ul style="list-style-type: none"> <li>• vmxnet3</li> </ul>    |
| Microsoft HyperV    | <ul style="list-style-type: none"> <li>• Zip</li> </ul> | <ul style="list-style-type: none"> <li>• Powershell script</li> </ul>             | <ul style="list-style-type: none"> <li>• —</li> </ul>                     | <ul style="list-style-type: none"> <li>• netvsc</li> </ul>     |
| RHEL KVM            | <ul style="list-style-type: none"> <li>• TAR</li> </ul> | <ul style="list-style-type: none"> <li>• EZdeploy</li> <li>• launch.sh</li> </ul> | <ul style="list-style-type: none"> <li>• —</li> </ul>                     | <ul style="list-style-type: none"> <li>• virtio_net</li> </ul> |

| Hypervisor      | Package Format                                                  | Deployment Tool                                                                 | Preconfiguration Tool                                 | Network Driver                                               |
|-----------------|-----------------------------------------------------------------|---------------------------------------------------------------------------------|-------------------------------------------------------|--------------------------------------------------------------|
| SUSE Linux      | <ul style="list-style-type: none"> <li>TAR</li> </ul>           | <ul style="list-style-type: none"> <li>EZdeploy</li> <li>launch.sh</li> </ul>   | <ul style="list-style-type: none"> <li>---</li> </ul> | <ul style="list-style-type: none"> <li>virtio_net</li> </ul> |
| Microsoft Azure | <ul style="list-style-type: none"> <li>JSON template</li> </ul> | <ul style="list-style-type: none"> <li>---</li> </ul>                           | <ul style="list-style-type: none"> <li>---</li> </ul> | <ul style="list-style-type: none"> <li>netvsc</li> </ul>     |
| OpenStack       | <ul style="list-style-type: none"> <li>TAR</li> </ul>           | <ul style="list-style-type: none"> <li>OpenStack portal (Horizon U1)</li> </ul> | <ul style="list-style-type: none"> <li>---</li> </ul> | <ul style="list-style-type: none"> <li>virtio_net</li> </ul> |

**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, [Table 1-22](#) 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 1-22** Components for Managing Cisco vWAAS, by Hypervisor Type

| Hypervisor          | Cisco vCM Models Supported                                                 | Cisco vWAAS Models Supported                                                                          | Number of Instances Supported                          | Traffic Interception Method                                                                                            |
|---------------------|----------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|--------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|
| Cisco ISR-WAAS      | <ul style="list-style-type: none"> <li>N/A</li> </ul>                      | <ul style="list-style-type: none"> <li>vWAAS-200, 750, 1300, 2500</li> </ul>                          | <ul style="list-style-type: none"> <li>1</li> </ul>    | <ul style="list-style-type: none"> <li>AppNav-XE</li> </ul>                                                            |
| Cisco NFVIS         | <ul style="list-style-type: none"> <li>N/A</li> </ul>                      | <ul style="list-style-type: none"> <li>vWAAS-200, 750, 1300, 2500, 6000</li> </ul>                    | <ul style="list-style-type: none"> <li>1</li> </ul>    | <ul style="list-style-type: none"> <li>WCCP</li> <li>APPNav-XE</li> <li>Inline (with WAAS v6.2.1 and later)</li> </ul> |
| VMware vSphere ESXi | <ul style="list-style-type: none"> <li>vCM-100, 500, 1000, 2000</li> </ul> | <ul style="list-style-type: none"> <li>vWAAS-150, 200, 750, 1300, 2500, 6000, 12000, 50000</li> </ul> | <ul style="list-style-type: none"> <li>many</li> </ul> | <ul style="list-style-type: none"> <li>WCCP</li> <li>APPNav-XE</li> </ul>                                              |
| Microsoft HyperV    | <ul style="list-style-type: none"> <li>vCM-100, 500, 1000, 2000</li> </ul> | <ul style="list-style-type: none"> <li>vWAAS-150, 200, 750, 1300, 2500, 6000, 12000, 50000</li> </ul> | <ul style="list-style-type: none"> <li>many</li> </ul> | <ul style="list-style-type: none"> <li>WCCP</li> <li>APPNav-XE</li> </ul>                                              |
| RHEL KVM            | <ul style="list-style-type: none"> <li>vCM-100, 500, 1000, 2000</li> </ul> | <ul style="list-style-type: none"> <li>vWAAS-150, 200, 750, 1300, 2500, 6000, 12000, 50000</li> </ul> | <ul style="list-style-type: none"> <li>many</li> </ul> | <ul style="list-style-type: none"> <li>WCCP</li> <li>APPNav-XE</li> <li>Inline (with WAAS v6.2.1 and later)</li> </ul> |
| SUSE Linux          | <ul style="list-style-type: none"> <li>vCM-100, 500, 1000, 2000</li> </ul> | <ul style="list-style-type: none"> <li>vWAAS-150, 200, 750, 1300, 2500, 6000, 12000, 50000</li> </ul> | <ul style="list-style-type: none"> <li>many</li> </ul> | <ul style="list-style-type: none"> <li>WCCP</li> <li>APPNav-XE</li> </ul>                                              |

| Hypervisor      | Cisco vCM Models Supported                                                 | Cisco vWAAS Models Supported                                                                          | Number of Instances Supported                          | Traffic Interception Method                                                                |
|-----------------|----------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|--------------------------------------------------------|--------------------------------------------------------------------------------------------|
| Microsoft Azure | <ul style="list-style-type: none"> <li>N/A</li> </ul>                      | <ul style="list-style-type: none"> <li>vWAAS-200, 750, 1300, 2500, 6000, 12000</li> </ul>             | <ul style="list-style-type: none"> <li>1</li> </ul>    | <ul style="list-style-type: none"> <li>Routed mode (with WAAS v6.2.1 and later)</li> </ul> |
| OpenStack       | <ul style="list-style-type: none"> <li>vCM-100, 500, 1000, 2000</li> </ul> | <ul style="list-style-type: none"> <li>vWAAS-150, 200, 750, 1300, 2500, 6000, 12000, 50000</li> </ul> | <ul style="list-style-type: none"> <li>many</li> </ul> | <ul style="list-style-type: none"> <li>WCCP</li> <li>APPNav-XE</li> </ul>                  |

## Cisco UCS E-Series Servers and NCEs

This section has the following topics:

- [Cisco vWAAS and Cisco UCS E-Series Interoperability, page 1-26](#)
- [Cisco vWAAS and Cisco UCS E-Series Memory Guidelines and Requirements, page 1-27](#)

### 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. [Table 1-23](#) shows the supported operating systems, hypervisors, Cisco ISR routers, and the minimum version of Cisco IOS-XE used.

**Table 1-23 Cisco vWAAS and Cisco UCS E-Series Interoperability**

| Cisco UCS E-Series   | Supported Operating Systems for vWAAS                                                                                                                                                                                                    | Supported Hypervisors for vWAAS                                                                                                                                                                                                                                                                                                                                                                                   | Supported Cisco ISR Routers for vWAAS                                                                                                               | Minimum IOS -XE Version                                                                          |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
| UCS E-Series Servers | <ul style="list-style-type: none"> <li>Microsoft Windows Server 2008 R2, 2012, and 2012 R2</li> <li>Red Hat Enterprise Linux (RHEL) 7.1 and later</li> <li>Linux CentOS (Community Enterprise Operating System) 7.1 and later</li> </ul> | <ul style="list-style-type: none"> <li>Microsoft Hyper-V 2008 R2, 2012, and 2012 R2</li> <li>VMware vSphere ESXi 5.5 and 6.0 (vWAAS in WAAS Versions 6.4.3b and earlier)</li> <li>VMware vSphere ESXi 6.7 (vWAAS in WAAS Version 6.4.3c and later)</li> <li>RHEL KVM or CentOS 7.1 (vWAAS in WAAS Version 6.4.3b and earlier)</li> <li>RHEL KVM or CentOS 7.2 (vWAAS in WAAS Version 6.4.3c and later)</li> </ul> | <ul style="list-style-type: none"> <li>ISR-4331</li> <li>ISR-4351</li> <li>ISR-4451</li> <li>ISR-4461</li> </ul>                                    | <ul style="list-style-type: none"> <li>3.10</li> </ul>                                           |
| UCS E-Series NCEs    | <ul style="list-style-type: none"> <li>Microsoft Windows Server (2012 R2)</li> <li>RHEL 7.1 and later</li> <li>Linux CentOS 7.1 and later</li> </ul>                                                                                     | <ul style="list-style-type: none"> <li>Microsoft Hyper-V 2012 R2</li> <li>VMware vSphere ESXi 5.5 and 6.0 (vWAAS in WAAS Versions 6.4.3b and earlier)</li> <li>VMware vSphere ESXi 6.7 (vWAAS in WAAS Version 6.4.3c and later)</li> <li>RHEL KVM or CentOS 7.1 (vWAAS in WAAS Version 6.4.3b and earlier)</li> <li>RHEL KVM or CentOS 7.2 (vWAAS in WAAS Version 6.4.3c and later)</li> </ul>                    | <ul style="list-style-type: none"> <li>ISR-432</li> <li>ISR-4331</li> <li>ISR-4351</li> <li>ISR-4431</li> <li>ISR-4451</li> <li>ISR-4461</li> </ul> | <ul style="list-style-type: none"> <li>3.10 (UCS-EN120S)</li> <li>3.15.1 (UCS-EN140N)</li> </ul> |

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

Table 1-24 shows memory and disk storage capacity for Cisco UCS E-Servers NCEs. When calculating memory requirements for your Cisco 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 Table 4-4 and Table 4-5 in Chapter 4, “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.

**Table 1-24 Memory and Disk Storage for Cisco UCS E-Servers NCEs**

| Cisco UCS E-Series Server (E) or NCE (EN)         | Memory                          | Disk Storage                                                                                                                                                                                                                                      |
|---------------------------------------------------|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| UCS-E140S<br>(single-wide blade)                  | Default: 8 GB<br>Maximum: 16 GB | Up to two of the following: <ul style="list-style-type: none"> <li>• 7200-RPM SATA: 1 TB</li> <li>• 10,000-RPM SAS: 900 GB</li> <li>• 10,000-RPM SAS SED: 600 GB</li> <li>• SAS SSD SLC: 200 GB</li> <li>• SAS SSD eMLC: 200 or 400 GB</li> </ul> |
| UCS-EN120S<br>(single-wide blade)                 | Default: 4 GB<br>Maximum: 16 GB | Up to two of the following: <ul style="list-style-type: none"> <li>• 7200-RPM SATA: 500 GB</li> <li>• 7200-RPM SATA: 1 TB</li> <li>• 10,000-RPM SAS: 900 GB</li> </ul>                                                                            |
| UCS-E140DP<br>(double-wide blade with PCIe cards) | Default: 8 GB<br>Maximum: 48 GB | Up to two of the following: <ul style="list-style-type: none"> <li>• 7200-RPM SATA: 1 TB</li> <li>• 10,000-RPM SAS: 900 GB</li> <li>• 10,000-RPM SAS SED: 600 GB</li> <li>• SAS SSD SLC: 200 GB</li> <li>• SAS SSD eMLC: 200 or 400 GB</li> </ul> |



| Cisco UCS E-Series Server (E) or NCE (EN)         | Memory                          | Disk Storage                                                                                                                                                                                                                                                                          |
|---------------------------------------------------|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| UCS-E140D<br>(double-wide blade)                  | Default: 8 GB<br>Maximum: 48 GB | Up to three of the following: <ul style="list-style-type: none"> <li>• 7200-RPM SATA: 1 TB</li> <li>• 10,000-RPM SAS: 900 GB</li> <li>• 10,000-RPM SAS SED: 600 GB</li> <li>• SAS SSD SLC: 200 GB</li> <li>• SAS SSD eMLC: 200 or 400 GB</li> </ul>                                   |
| UCS-EN40N<br>(Network Interface Module)           | —                               | One of the following mSATA SSD drives: <ul style="list-style-type: none"> <li>• mSATA SSD drive: 50 GB</li> <li>• mSATA SSD drive: 100 GB</li> <li>• mSATA SSD drive: 200 GB</li> </ul>                                                                                               |
| UCS-E160DP<br>(double-wide blade with PCIe cards) | Default: 8 GB<br>Maximum: 48 GB | Up to two of the following: <ul style="list-style-type: none"> <li>• 7200-RPM SATA: 1 TB</li> <li>• 10,000-RPM SAS: 900 GB</li> <li>• 10,000-RPM SAS SED: 600 GB</li> <li>• SAS SSD SLC: 200 GB</li> <li>• SAS SSD eMLC: 200 or 400 GB</li> </ul>                                     |
| UCS-E160D<br>(double-wide blade)                  | Default: 8 GB<br>Maximum: 96 GB | Up to three of the following: <ul style="list-style-type: none"> <li>• 7200-RPM SATA: 1 TB</li> <li>• 10,000-RPM SAS: 900 GB</li> <li>• 10,000-RPM SAS SED: 600 GB</li> <li>• SAS SSD SLC: 200 GB</li> <li>• SAS SSD eMLC: 200 or 400 GB</li> </ul>                                   |
| UCS-E180D<br>(double-wide blade)                  | Default: 8 GB<br>Maximum: 96GB  | Up to three of the following: <ul style="list-style-type: none"> <li>• 7200-RPM SATA: 1 TB</li> <li>• 10,000-RPM SAS: 1.8 TB</li> <li>• 10,000-RPM SAS: 900 GB</li> <li>• 10,000-RPM SAS SED: 600 GB</li> <li>• SAS SSD SLC: 200 GB</li> <li>• SAS SSD eMLC: 200 or 400 GB</li> </ul> |

## Cisco Enterprise Network Computer System 5400-W Series

This section contains the following topics:

- [About the Cisco Enterprise Network Compute System 5400-W Series, page 1-30](#)
- [Cisco ENCS 5400 Series Hardware Features and Specifications, page 1-30](#)

## About the Cisco Enterprise Network Compute System 5400-W 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 5000 Enterprise Network Compute System Data Sheet](#).

For information on vWAAS with NFVIS on the ENCS 5400-W Series, see the chapter “[Cisco vWAAS with Cisco Enterprise NFVIS](#)”.

## Cisco ENCS 5400 Series Hardware Features and Specifications

[Table 1-25](#) shows specifications that apply to all three Cisco ENCS 5400-W Series models. For further information, see the [Cisco 5000 Enterprise Network Compute System Data Sheet](#).

**Table 1-25 Cisco ENCS 5400 Series Features and Specifications**

| Cisco ENCS 5400 Feature/Specification | Description                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cisco vWAAS models supported          | One of the following configurations: <ul style="list-style-type: none"> <li>ENCS-5406/K9 supports vWAAS 200 and vWAAS-750</li> <li>ENCS-5408/K9 supports vWAAS-1300</li> <li>ENCS-5412/K9 supports vWAAS-2500 and vWAAS-6000-R</li> </ul>                                                                                                       |
| CPU                                   | One of the following specifications: <ul style="list-style-type: none"> <li>ENCS-5406/K9: Intel Xeon Processor D-1528 (6 core, 1.9 GHz, and 9 MB cache)</li> <li>ENCS-5408/K9: Intel Xeon Processor D-1548 (8 core, 2.0 GHz, and 12 MB cache)</li> <li>ENCS-5412/K9: Intel Xeon Processor D-1557 (12 core, 1.5 GHz, and 18 MB cache)</li> </ul> |
| 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                                                                                                                                                                                                                                                                                                                                |

| Cisco ENCS 5400 Feature/Specification | Description                                                                                                                                                                                                                                                   |
|---------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| WAN Ethernet port                     | Intel i350 dual port                                                                                                                                                                                                                                          |
| DIMM                                  | Two DDR4 dual in-line memory module (DIMM) slots, for ENCS models with the following capacities: <ul style="list-style-type: none"> <li>ENCS 5406-W: 16 GB</li> <li>ENCS-5408-W: 16 GB</li> <li>ENCS-5412-W: 32 GB</li> </ul>                                 |
| 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 Series.                                                                                                                                                     |
| SSD Storage                           | <ul style="list-style-type: none"> <li>No RAID and one 960 GB SSD</li> <li>RAID-1 and two SSDs (960 GB SSD)</li> </ul>                                                                                                                                        |
| Offload Capabilities                  | Optional crypto module to provide offload capabilities to optimize CPU resources such as VM-VM traffic and to maintain open software support.                                                                                                                 |

## Hypervisors Supported for Cisco vWAAS and Cisco vCM

This section contains the following topics:

- [About Hypervisors Supported for Cisco vWAAS and Cisco vCM, page 1-31](#)
- [Hypervisor OVA Packages for Cisco vWAAS, page 1-32](#)

## About Hypervisors Supported for Cisco vWAAS and Cisco vCM

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

- Cisco ISR-WAAS**

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



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

For more information, see Chapter 3, “[Cisco vWAAS on Cisco ISR-WAAS](#)”.

- **VMware ESXi**

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

For more information, see Chapter 4, “[Cisco vWAAS on VMware ESXi](#)”.

- **Microsoft Hyper-V**

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

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

Microsoft HyperV, Chapter 5, “[Cisco vWAAS on Microsoft Hyper-V](#)”.

- **RHEL KVM and KVM CentOS**

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

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




---

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

---

For more information, see Chapter 6, “[Cisco vWAAS on RHEL KVM, KVM on CentOS, and KVM in SUSE Linux](#)”.

- **Cisco Enterprise NFVIS**

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

For more information, see Chapter 9, “[Cisco vWAAS with Cisco Enterprise NFVIS](#)”.

## Hypervisor OVA Packages for Cisco vWAAS

This section contains the following topics:

- [Hypervisor OVA Package Format for Cisco vWAAS in Cisco WAAS Versions 5.x to 6.2.x, page 1-33](#)
- [Hypervisor-Wise Unified OVA Package Format for Cisco vWAAS in Cisco WAAS Version 6.4.x and Later, page 1-33](#)

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

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

For a listing of hypervisor-wise NPE and non-NPE OVA files for Cisco vWAAS or Cisco vCM, 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 1-26 shows the file formats for hypervisors supported for Cisco vWAAS and Cisco vCM, in Cisco WAAS Version 5.x to 6.2.x.

**Table 1-26** File Formats for OVA Packages for Cisco vWAAS and Cisco vCM in WAAS Versions 5.x to 6.2.x

| Cisco vWAAS or vCM | Hypervisor Support | File Format | NPE File Format | Sample Image and NPE Image Filename Formats                                                                                                    |
|--------------------|--------------------|-------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| vWAAS              | VMware ESXi        | .ova        | .ova            | Cisco-vWAAS-750-6.2.3d-b-68.ova<br>Cisco-vWAAS-750-6.2.3d-npe-b-68.ova                                                                         |
|                    | Microsoft Hyper-V  | .zip        | .zip            | Hv-Cisco-vWAAS-750-6.2.3d-b-68.zip<br>Hv-Cisco-vWAAS-750-6.2.3d-npe-b-68.zip                                                                   |
|                    | RHEL KVM           | .tar.gz     | .tar.gz         | Cisco-KVM-vWAAS-750-6.2.3d-b-68.tar.gz<br>Cisco-KVM-vWAAS-750-6.2.3d-b-68-npe.tar.gz                                                           |
| vCM                | VMware ESXi        | .ova        | .ova            | <ul style="list-style-type: none"> <li>Cisco-vCM-100N-6.2.3d-b-68.ova</li> <li>Cisco-vCM-100N-6.2.3d-npe-b-68.ova</li> </ul>                   |
|                    | Microsoft Hyper-V  | N/A         | .zip            | <ul style="list-style-type: none"> <li>Hv-Cisco-100N-6.2.3d-b-68.zip</li> <li>Hv-Cisco-100N-6.2.3d-npe-b-68.zip</li> </ul>                     |
|                    | RHEL KVM           | .tar.gz     | .tar.gz         | <ul style="list-style-type: none"> <li>Cisco-KVM-vCM-100N-6.2.3d-b-68.tar.gz</li> <li>Cisco-KVM-vCM-100N-6.2.3d-npe-b-68-npe.tar-gz</li> </ul> |

## Hypervisor-Wise Unified OVA Package Format for Cisco vWAAS in Cisco WAAS Version 6.4.x and Later

For Cisco vWAAS in Cisco WAAS Version 6.4.x and later, Cisco provides a single unified OVA package, one each for the NPE and non-NPE version of the Cisco WAAS image for all the Cisco vWAAS and Cisco vCM models for that hypervisor (Table 1-27). Each unified OVA package file provides an option to select a Cisco vWAAS or Cisco vCM model and other required parameters to launch Cisco vWAAS or Cisco vCM in Cisco WAAS in the required configuration.



### Note

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

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

**Table 1-27 Supported Unified OVA Files for Cisco vWAAS and vCM in WAAS Version 6.4.x and Later, by Hypervisor**

| Hypervisor or Appliance | Cisco Unified OVA Filename Format                                                                                                                    | Supported Cisco vWAAS Models                                                                                                                                                                                                                       | Supported Cisco vCM Models                                                                                     |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|
| Cisco ISR-WAAS          | <ul style="list-style-type: none"> <li>ISR-WAAS-6.4.3c-b-42.ova</li> <li>ISR-WAAS-6.4.3c-b-42-npe.ova</li> </ul>                                     | <ul style="list-style-type: none"> <li>vWAAS-200</li> <li>WAAS-750</li> <li>vWAAS-1300</li> <li>vWAAS-2500</li> </ul>                                                                                                                              | <ul style="list-style-type: none"> <li>N/A</li> </ul>                                                          |
| VMware ESXi             | <ul style="list-style-type: none"> <li>Cisco-WAAS-Unified-6.4.3c-b-42.tar</li> <li>Cisco-WAAS-Unified-6.4.3c-npe-b-42.tar</li> </ul>                 | <ul style="list-style-type: none"> <li>vWAAS-150</li> <li>vWAAS-200</li> <li>vWAAS-750</li> <li>vWAAS-1300</li> <li>vWAAS-2500</li> <li>vWAAS-6000</li> <li>vWAAS-6000R</li> <li>vWAAS-12000</li> <li>vWAAS-50000</li> <li>vWAAS-150000</li> </ul> | <ul style="list-style-type: none"> <li>vCM-100</li> <li>vCM-500</li> <li>vCM-1000</li> <li>vCM-2000</li> </ul> |
| Microsoft Hyper-V       | <ul style="list-style-type: none"> <li>Cisco-HyperV-vWAAS-unified-6.4.3c-b-42.tar</li> <li>Cisco-HyperV-vWAAS-unified-6.4.3c-b-42-npe.tar</li> </ul> | <ul style="list-style-type: none"> <li>vWAAS-150</li> <li>vWAAS- 200</li> <li>vWAAS-750</li> <li>vWAAS-1300</li> <li>vWAAS-2500</li> <li>vWAAS-6000</li> <li>vWAAS-6000R</li> <li>vWAAS-12000</li> <li>vWAAS-50000</li> </ul>                      | <ul style="list-style-type: none"> <li>vCM-100</li> <li>vCM-500</li> <li>vCM-1000</li> <li>vCM-2000</li> </ul> |
| KVM CentOS              | <ul style="list-style-type: none"> <li>Cisco-KVM-vWAAS-Unified-6.4.3c-b-42.tar.</li> <li>Cisco-KVM-vWAAS-Unified-6.4.3c-b-42-npe.tar</li> </ul>      | <ul style="list-style-type: none"> <li>vWAAS-150</li> <li>vWAAS- 200</li> <li>vWAAS-750</li> <li>vWAAS-1300</li> <li>vWAAS-2500</li> <li>vWAAS-6000</li> <li>vWAAS-6000R</li> <li>vWAAS-12000</li> <li>vWAAS-50000</li> </ul>                      | <ul style="list-style-type: none"> <li>vCM-100</li> <li>vCM-500</li> <li>vCM-1000</li> <li>vCM-2000</li> </ul> |

| Hypervisor or Appliance | Cisco Unified OVA Filename Format                                                                                                                                       | Supported Cisco vWAAS Models                                                                                                                                                      | Supported Cisco vCM Models                            |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------|
| Cisco ENCS 5400-W       | <ul style="list-style-type: none"> <li>Cisco_NFVIS_3.11.1-FC7_WAAS-APPLIANCE-6.4.3c-b42.iso</li> <li>Cisco_NFVIS_3.11.1-FC7_WAASNPE-APPLIANCE-6.4.3c-b42.iso</li> </ul> | <ul style="list-style-type: none"> <li>vWAAS-200</li> <li>WAAS-750</li> <li>vWAAS-1300</li> <li>vWAAS-2500</li> <li>vWAAS-6000R</li> </ul>                                        | <ul style="list-style-type: none"> <li>N/A</li> </ul> |
| Cisco NFVIS vBranch     | <ul style="list-style-type: none"> <li>Cisco-KVM-vWAAS-Unified-6.4.3c-b-42.tar</li> <li>Cisco-KVM-vWAAS-Unified-6.4.3c-b-42-npe.tar</li> </ul>                          | <ul style="list-style-type: none"> <li>vWAAS-150</li> <li>vWAAS-200</li> <li>WAAS-750</li> <li>vWAAS-1300</li> <li>vWAAS-2500</li> <li>vWAAS-6000</li> <li>vWAAS-6000R</li> </ul> | <ul style="list-style-type: none"> <li>N/A</li> </ul> |

## 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 Systems”](#).







# Configuring Cisco vWAAS and Viewing Cisco vWAAS Components

---

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

This chapter contains the following sections:

- [Configuring Cisco vWAAS, page 2-1](#)
- [Identifying a Cisco vWAAS Device, page 2-5](#)
- [Cisco vWAAS System Partitions, page 2-6](#)
- [Operating Considerations for Cisco vWAAS and Cisco WAAS, page 2-7](#)
- [Cisco vWAAS with Single-Root I/O Virtualization, page 2-7](#)
- [Upgrade and Downgrade Guidelines for Cisco vWAAS, page 2-18](#)

## Configuring Cisco vWAAS

This section contains the following topics:

- [Configuring Cisco vWAAS Settings, page 2-1](#)
- [Configuring Cisco vWAAS Traffic Interception, page 2-2](#)

## Configuring Cisco vWAAS Settings

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

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

To configure Cisco vWAAS settings, follow these steps:

---

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

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

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




---

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

---

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

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

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

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

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

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

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




---

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

---

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

---

## Configuring Cisco vWAAS Traffic Interception

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

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

**Table 2-1** Traffic Interception Methods for Cisco vWAAS



| Traffic Interception Method | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| WCCP                        | <p>Specifies interactions between one or more routers (or L3 switches) and one or more application appliances, web caches, and caches of other application protocols, to establish and maintain the transparent redirection of selected types of traffic. The selected traffic is redirected to a group of appliances. Any type of TCP traffic can be redirected.</p> <p>WCCP uses a WCCP-enabled router or L3 switch.</p> <p> <b>Note</b> You can configure WCCP-GRE or L2 Inline as the redirection method for 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.</p> <p>For more information on WCCP, see Chapter 5, “Configuring Traffic Interception” in the <i>Cisco Wide Area Application Services Configuration Guide</i>.</p>                                                |
| AppNav                      | <p>A policy and class-based traffic interception method that reduces dependency on the intercepting switch or router by distributing traffic among Cisco WAAS devices for optimization.</p> <p>For more information on AppNav, see Chapter 4, “Configuring AppNav” and Chapter 5, “Configuring Traffic Interception” in the <i>Cisco Wide Area Application Services Configuration Guide</i>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| L2 Inline                   | <p>Places the 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.</p> <p>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.</p> <p> <b>Note</b> Cisco vWAAS in Cisco WAAS Version 6.2.1 does not include fail-to-wire capability.</p> <p>For more information on configuring L2 Inline interception on the Cisco WAAS Central Manager, see Chapter 5, “Configuring Traffic Interception” in the <i>Cisco Wide Area Application Services Configuration Guide</i>.</p> |

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

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

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

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

# Identifying a Cisco vWAAS Device

This section has the following topics:

- [Identifying a Cisco vWAAS Model, page 2-5](#)
- [Identifying a Cisco vWAAS Device on the Cisco WAAS Central Manager, page 2-5](#)
- [Identifying a Cisco vWAAS Device with the Cisco WAAS CLI, page 2-6](#)

## Identifying a Cisco vWAAS Model

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

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

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

## Identifying a Cisco vWAAS Device on the Cisco WAAS Central Manager

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

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

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

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

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

## Identifying a Cisco vWAAS Device with the Cisco WAAS CLI

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

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

| Mode                                      | Command                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------------------|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| user-level EXEC and privileged-level EXEC | <b>show version</b>    | Displays version information about the WAAS software currently running on the vWAAS device, including date and time system last started, and the length of time the system has been running since the last reboot. <ul style="list-style-type: none"> <li>(Optional) Use the <b>show version last</b> command to display version information for the last saved image.</li> <li>(Optional) Use the <b>show version pending</b> command to display version information for the pending upgraded image.</li> </ul>          |
| privileged-level EXEC                     | <b>show hardware</b>   | Displays system hardware status for the vWAAS device, including: <ul style="list-style-type: none"> <li>Startup date and time, the run time since startup, microprocessor type and speed, and a list of disk drives.</li> </ul>                                                                                                                                                                                                                                                                                           |
| privileged-level EXEC                     | <b>show tfo detail</b> | Displays Transport Flow Optimization (TFO) information, including: <ul style="list-style-type: none"> <li>State: Registered or Not Registered</li> <li>Default Action: Drop or Use</li> <li>Connection Limit: The maximum TFO connections handled before new connection requests are rejected.</li> <li>Effective Limit: The dynamic limit relating to how many connections are handled before new connection requests are rejected.</li> <li>Keepalive Timeout: The connection keepalive timeout, in seconds.</li> </ul> |

## Cisco vWAAS System Partitions

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

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



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

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

## Operating Considerations for Cisco vWAAS and Cisco WAAS

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

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

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

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

## Cisco vWAAS with Single-Root I/O Virtualization

This section has the following topics:

- [About Single-Root I/O Virtualization, page 2-8](#)
- [Interoperability and Platforms Supported for Cisco vWAAS with SR-IOV, page 2-8](#)
- [Upgrade and Downgrade Considerations for Cisco vWAAS with SR-IOV, page 2-9](#)
- [Deploying Cisco vWAAS with SR-IOV, page 2-10](#)

## About Single-Root I/O Virtualization

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

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

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

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

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

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

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

This section contains the following topics:

- [Cisco WAAS Central Manager and Cisco vWAAS with SR-IOV, page 2-8](#)
- [Platforms Supported for Cisco vWAAS with SR-IOV, page 2-9](#)

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

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

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



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

## Platforms Supported for Cisco vWAAS with SR-IOV

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

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

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

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

| Ethernet Controller | Hypervisor | Earliest Cisco WAAS Version Supported | Supported Cisco vWAAS Models                                                                                                                                              |
|---------------------|------------|---------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Intel I350          | CentOS     | 6.4.1                                 | <ul style="list-style-type: none"> <li>• vWAAS-150</li> <li>• vWAAS-200</li> <li>• vWAAS-750</li> <li>• vWAAS-1300</li> <li>• vWAAS-2500</li> <li>• vWAAS-6000</li> </ul> |
| Intel X710          | NFVIS      | 6.4.1                                 | <ul style="list-style-type: none"> <li>• vWAAS-150</li> <li>• vWAAS-200</li> <li>• vWAAS-750</li> <li>• vWAAS-1300</li> <li>• vWAAS-2500</li> <li>• vWAAS-6000</li> </ul> |
|                     | CentOS     | 6.4.3                                 | <ul style="list-style-type: none"> <li>• vWAAS-12000</li> <li>• vWAAS-50000</li> </ul>                                                                                    |
|                     | ESXi       | 6.4.3                                 | <ul style="list-style-type: none"> <li>• vWAAS-12000</li> <li>• vWAAS-50000</li> <li>• vWAAS-150000</li> </ul>                                                            |

## Upgrade and Downgrade Considerations for Cisco vWAAS with SR-IOV

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

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

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

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

## Deploying Cisco vWAAS with SR-IOV

This section contains the following topics:

- [Deploying Cisco vWAAS with SR-IOV on KVM, page 2-10](#)
- [Deploying Cisco vWAAS with SR-IOV on VMware ESXi, page 2-13](#)

## 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, page 2-10](#)
- [Deploying Cisco vWAAS with SR-IOV on RHEL KVM or CentOS Using Deployment Script for Cisco UCS C-Series, page 2-11](#)
- [Deploying Cisco vWAAS with SR-IOV on RHEL KVM or CentOS Using Cisco NFVIS Portal for Cisco ENCS 5400-W Series, page 2-12](#)

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

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

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

---

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

Enable **VT-d**:

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

The command value should be greater than 0.

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

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

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

- c. For the changes to take effect, compile using `grub2-mkconfig -o /boot/grub2/grub.cfg`.
- d. Reboot the host.

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

- a. Verify the maximum number of virtual functions allowed for the specified interface.  
For example, if the SR-IOV-supported interface is `enp1s0f0`, 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 `enp1s0f0` interface, enter the following:  
`echo 7 > /sys/class/net/enp1s0f0/device/sriov_numvfs`

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

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

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

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

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

```
./launch.sh check
```

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

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

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

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

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

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

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

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

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

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

**Figure 2-1 VM Deployment Process Navigation Flow**

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

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



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

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

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

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

**Step 4** Click **Next**.

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

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

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

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

**Step 7** Click **Next**.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

**Step 13** Click **Next**.

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

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

**Step 14** Click **OK**.

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

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

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

---

## Deploying Cisco vWAAS with SR-IOV on VMware ESXi

This section contains the following topics:

- [Configuring Host Settings for Cisco vWAAS with SR-IOV on VMware ESXi for Cisco UCS C-Series, page 2-14](#)
- [Configuring SR-IOV Interfaces for Cisco vWAAS on VMware ESXi on Cisco UCS-C Series, page 2-15](#)

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

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

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

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



**Note**

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

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

- Step 1** Log in to the VMware ESXi shell.
- Step 2** Run the `lspci | grep -i intel | grep -i 'ethernet\|network'` command, and note the port order of this command.
- Step 3** Run this command to create virtual functions:

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

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

Example 1:

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

Example 2:

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

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

355943

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

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

```
[root@localhost:~]# 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:~]#
```

355944

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

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

- The VMware vSphere Client **DirectPath I/O Configuration** window (Figure 2-2)  
Choose **Host > Configuration > Hardware > Advanced Settings**.
- The VMware ESXi `lspci` command

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

**DirectPath I/O Configuration**

Warning: Configuring host hardware without special virtualization features for virtual machine passthrough will make it unavailable for use except if configuring a device needed for normal host boot or operation can make normal host boot impossible and may require significant effort to undo. See the VMware Knowledge Base for more information.

Each listed device is available for direct access by the virtual machines on this host.

| Device Name                                                  | Vendor Name       |
|--------------------------------------------------------------|-------------------|
| 0000:81:02.0   Intel Corporation XL710/x710 Virtual Function | Intel Corporation |
| 0000:81:02.1   Intel Corporation XL710/x710 Virtual Function | Intel Corporation |
| 0000:81:02.2   Intel Corporation XL710/x710 Virtual Function | Intel Corporation |
| 0000:81:02.3   Intel Corporation XL710/x710 Virtual Function | Intel Corporation |
| 0000:81:02.4   Intel Corporation XL710/x710 Virtual Function | Intel Corporation |

| Device Name | ID | Device ID | Vendor ID | Function | Bus | Class ID | Subdevice ID | Subvendor ID | Slot |
|-------------|----|-----------|-----------|----------|-----|----------|--------------|--------------|------|
| --          | -- | --        | --        | --       | --  | --       | --           | --           | --   |

355945

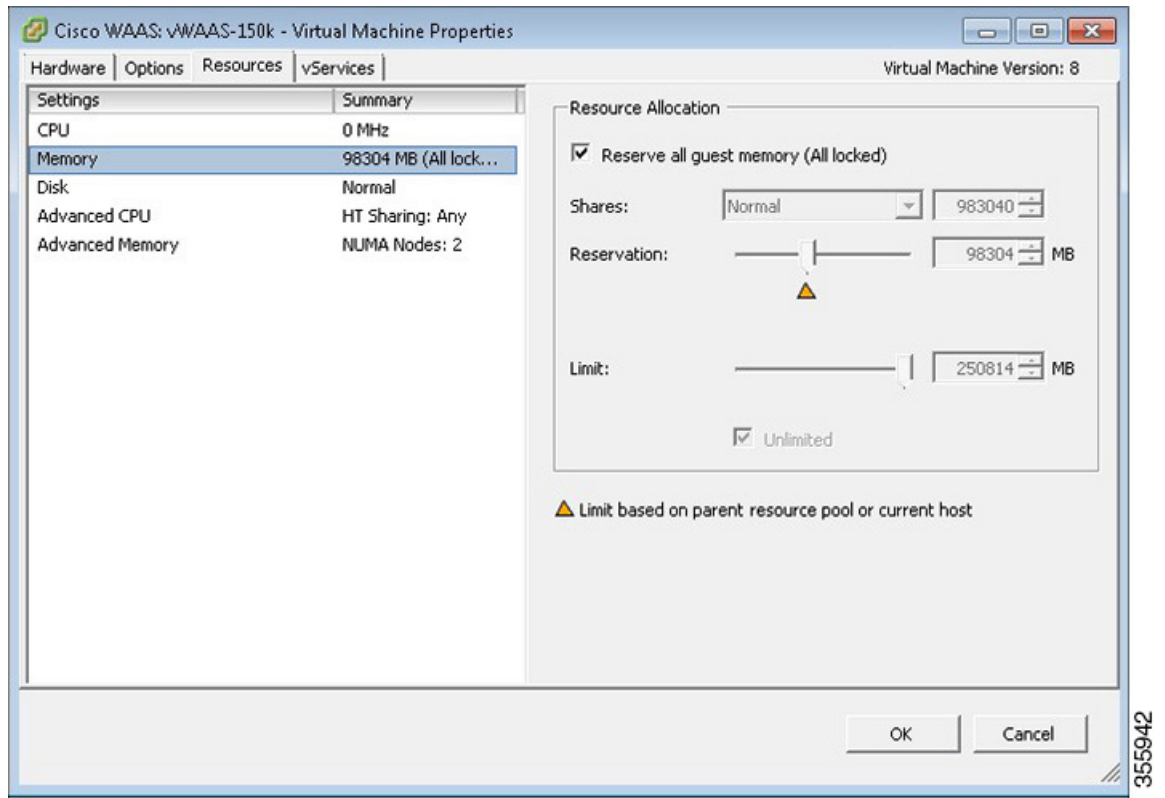
## Configuring SR-IOV Interfaces for Cisco vWAAS on VMware ESXi on Cisco UCS-C Series

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

- Step 1** After deploying the Cisco vWAAS, power down the Cisco vWAAS.
- Step 2** Power up the vWAAS.
- Step 3** Right-click and choose **Edit Settings**.
- Step 4** Click the **Virtual Machine Properties > Resources** tab.
- Step 5** At the **Settings** listing, select **Memory**.

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

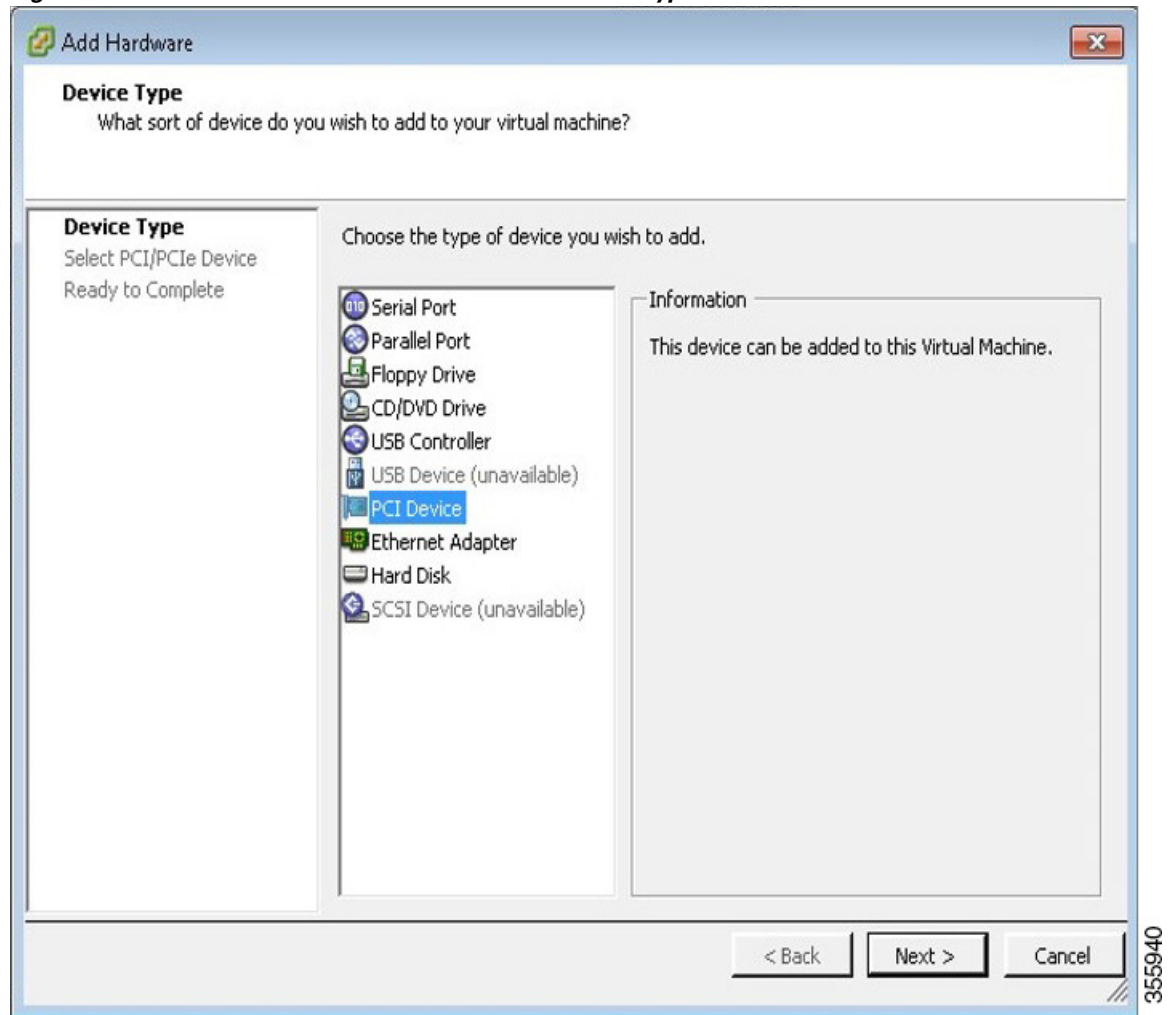
**Figure 2-3** Cisco vWAAS Resource Allocation Window



- Step 6** Click **Reserve all guest memory**.
- Step 7** Click **OK**.
- Step 8** Click the **Virtual Machine Properties > Hardware** tab.
- Step 9** Click **Add**.

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



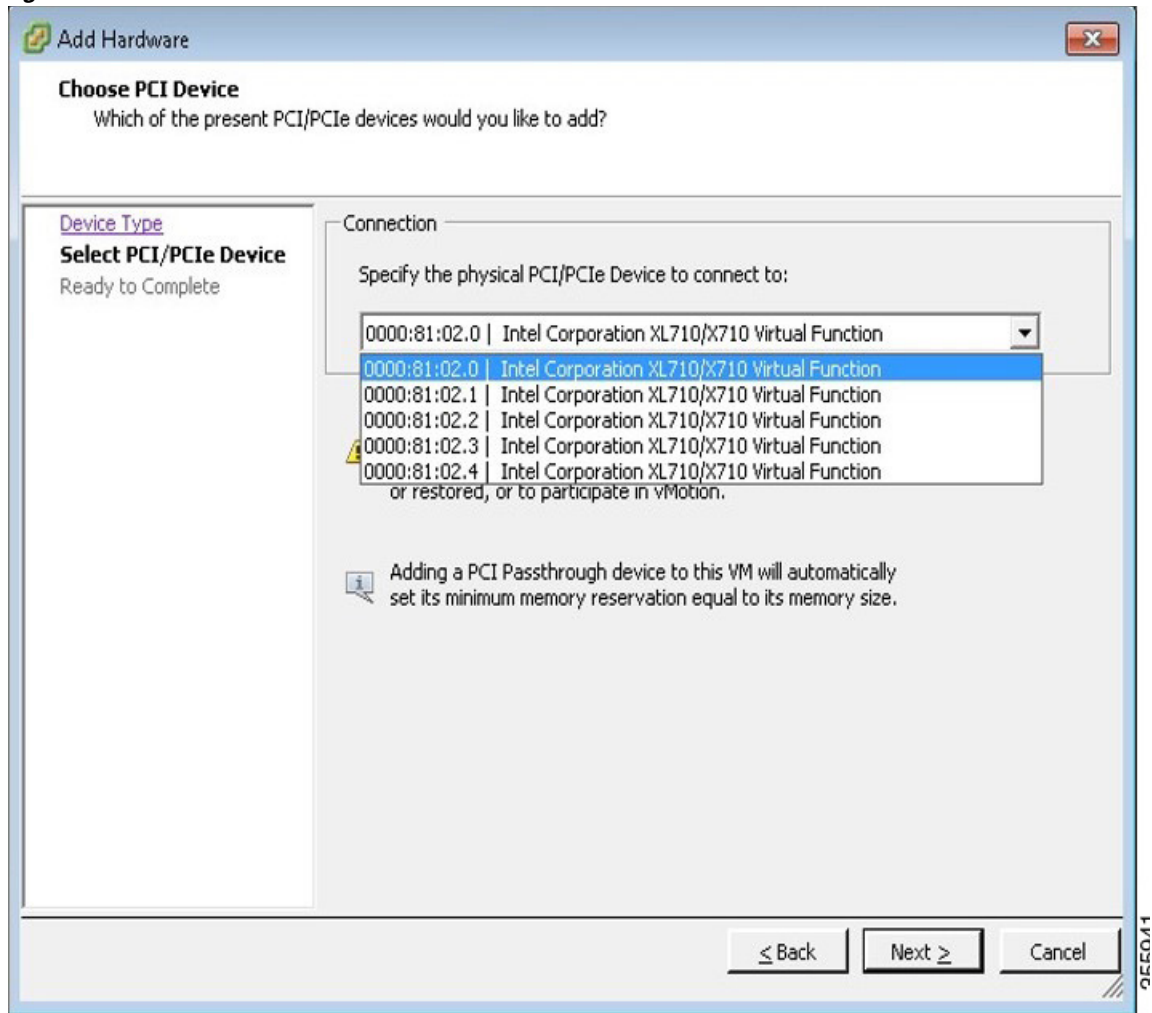
**Figure 2-4** Cisco vWAAS Add Hardware > Device Type Window

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

**Step 11** Click **Next**.

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

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



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

**Step 13** Click **Next**.

**Step 14** Click **Finish**.

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

## Upgrade and Downgrade Guidelines for Cisco vWAAS

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

- [Upgrade Guidelines for Cisco vWAAS and Cisco vWAAS Nodes](#), page 2-19
- [Cisco vWAAS Upgrade and SCSI Controller Type](#), page 2-19
- [Cisco vWAAS Upgrade and Cisco vCM-100 with RHEL KVM or KVM on CentOS](#), page 2-19
- [Migrating a Physical Appliance Being Used as a Cisco WAAS Central Manager to a Cisco vCM](#), page 2-20

- [Downgrade Guidelines for Cisco vWAAS, page 2-21](#)

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

## Upgrade Guidelines for Cisco vWAAS and Cisco vWAAS Nodes

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

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

## Cisco vWAAS Upgrade and SCSI Controller Type

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

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

- 
- Step 1** Power down the Cisco vWAAS.
  - Step 2** From the **VMware vCenter**, choose **vSphere Client > Edit Settings > Hardware**.
  - Step 3** Select **SCSI controller 0**.
  - Step 4** From the **Change Type** drop-down list, verify that the **SCSI Controller Type** is set to **VMware Paravirtual**. If this is not the case, choose **VMware Paravirtual**.
  - Step 5** Click **OK**.
  - Step 6** Power up the Cisco vWAAS in Cisco WAAS Version 5.2.1 or Cisco WAAS 6.1.x or later. (Cisco WAAS Version 6.1.x is the earliest version supported.)
- 

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

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

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

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

```
WARNING: Upgrade of vCM device to 6.2.0 (or) higher version with '/sw' and
'/swstore' size less than 2GB will clear system and data partition.
```
  - If you upgrade the Cisco vCM device to WAAS Version 5.2.1 using the Cisco WAAS Central Manager GUI: A warning message is not displayed.
- The **restore factory-default** command erases the user-specified information that is stored in the flash image, including the starting configuration of the device, and also removes data from the disk, user-defined partitions, and the entire Cisco WAAS Central Manager database.

To resolve this situation, follow these steps:

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



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

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

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

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

## Downgrade Guidelines for Cisco vWAAS

Consider the following downgrade guidelines for Cisco vWAAS.

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



---

**Note**

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

---





# 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, page 3-1](#)
- [Supported Host Platforms, Software Versions, and Disk Types, page 3-2](#)
- [Cisco OVA Packages for Cisco vWAAS on Cisco ISR-WAAS, page 3-2](#)
- [Deploying and Managing Cisco vWAAS on Cisco ISR-WAAS, page 3-3](#)

## 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.

[Table 3-1](#) shows the default number of CPUs, memory capacity, disk storage, and supported Cisco ISR platforms for each Cisco ISR model.

**Table 3-1 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,<br>ISR-4331,<br>ISR-4431,<br>ISR-4451 | • 5.2.1                               |
|                      | • 4  | • 6 GB | • 151 GB     | • ISR-4461                                        | • 6.4.1b                              |
| ISR-WAAS-1300        | • 4  | • 6 GB | • 151 GB     | • ISR-4431,<br>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

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

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

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

## Cisco OVA Packages for Cisco vWAAS on Cisco ISR-WAAS

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

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

| Package Format                                     | File Format Example          |
|----------------------------------------------------|------------------------------|
| Cisco ISR WAAS (200, 750, 1300, 2500) NPE OVA file | ISR-WAAS-6.4.3c-b-42-npe.ova |
| Cisco ISR WAAS (200, 750, 1300, 2500) OVA file     | ISR-WAAS-6.4.3c-b-42.ova     |

For a listing of hypervisor OVA and NPE OVA 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.



# Deploying and Managing Cisco vWAAS on Cisco ISR-WAAS

Table 3-4 shows the components used to deploy Cisco vWAAS on Cisco ISR-WAAS.

**Table 3-4** *Components for Deploying Cisco vWAAS on Cisco ISR-WAAS*

| Package Format | Deployment Tool | Network Driver |
|----------------|-----------------|----------------|
| OVA            | Ezconfig        | virtio_net     |

Table 3-5 shows the components used to manage Cisco vWAAS on Cisco ISR-WAAS.

**Table 3-5** *Components for Managing Cisco vWAAS on Cisco ISR-WAAS*

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





## Cisco vWAAS on VMware ESXi

---

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

- [About Cisco vWAAS on VMware ESXi, page 4-1](#)
- [Supported Host Platforms and Software Versions, page 4-1](#)
- [VMware ESXi Server Datastore Memory and Disk Space for Cisco vWAAS and Cisco vCM Models, page 4-3](#)
- [OVA Package Formats for Cisco vWAAS on VMware ESXi, page 4-4](#)
- [Installing Cisco vWAAS on VMware ESXi, page 4-6](#)
- [Operating Guidelines for Cisco vWAAS in WAAS Version 6.4.3 and later in VMware ESXi, page 4-25](#)
- [Upgrade and Downgrade Guidelines for Cisco vWAAS on VMware ESXi, page 4-25](#)

### 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:

- [Table 4-1](#) shows the platforms and software versions supported for Cisco vWAAS on VMware ESXi.
- [Table 4-2](#) shows the supported Cisco WAAS versions for VMware ESXi for a new Cisco vWAAS installation.
- [Table 4-3](#) shows the supported Cisco WAAS versions for VMware ESXi for a Cisco vWAAS upgrade.

**Table 4-1 Platforms and Software Versions Supported for Cisco vWAAS on VMware ESXi**

| PID and Device Type          | Earliest Cisco WAAS Version Supported | Host Platform             | Earliest Host Version Supported                           | Disk Type |
|------------------------------|---------------------------------------|---------------------------|-----------------------------------------------------------|-----------|
| PID:<br>OE-VWAAS-ESX         | 6.4.3c                                | Cisco UCS or UCS-E Series | VMware ESXi 6.7                                           | VMDK      |
| Device Type:<br>OE-VWAAS-ESX | 6.4.3b                                | Cisco UCS or UCS-E Series | VMware ESXi 6.5 or<br>VMware ESXi 6.0<br>(for Web Client) | VMDK      |
|                              | 5.0.3g                                | Cisco UCS or UCS-E Series | VMware ESXi 6.0 or<br>VMware ESXi 5.0<br>(for vSphere)    | VMDK      |

**Note**

It is recommended to use VMware vCenter Web GUI for the deployment of Cisco vWAAS in Cisco WAAS version 6.4.3b or later.

**Table 4-2 Supported WAAS Versions for VMware ESXi for New Cisco vWAAS Installation**

| VMware ESXi Version for New vWAAS Installation | Supported Cisco WAAS Versions                                |
|------------------------------------------------|--------------------------------------------------------------|
| ESXi 6.7                                       | WAAS 6.4.3c and later                                        |
| ESXi 6.5                                       | WAAS 6.4.3b and later                                        |
| ESXi 6.0                                       | WAAS 6.1.x through 6.4.3a,<br>WAAS 6.4.3b (using Web Client) |
| ESXi 5.5                                       | WAAS 5.3,x through 6.4.3a                                    |
| ESXi 5.1                                       | WAAS 5.1.x through 6.4.3a                                    |
| ESXi 5.0                                       | WAAS 5.1.x through 6.4.3a                                    |
| ESXi 4.1                                       | WAAS 5.1.x through 5.2.x                                     |

**Table 4-3 Supported Cisco WAAS Versions for VMware ESXi for Cisco vWAAS Upgrade**

| VMware ESXi Version for Cisco vWAAS Upgrade | Supported Cisco WAAS Versions |
|---------------------------------------------|-------------------------------|
| ESXi 6.7                                    | WAAS 6.4.3c and later         |
| ESXi 6.5                                    | WAAS 6.4.3b and later         |
| ESXi 6.0                                    | WAAS 6.1.x through 6.4.3b     |
| ESXi 5.5                                    | WAAS 5.3,x through 6.4.3b     |
| ESXi 5.1                                    | WAAS 5.1.x through 6.4.3a     |
| ESXi 5.0                                    | WAAS 5.1.x through 5.5.x      |
| ESXi 4.1                                    | WAAS 5.1.x through 5.5.x      |

**Note**

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

If the I/O abort is observed:

Upgrade the RAID controller's driver to Version 6.610.19.00 or later.

If the I/O abort is still observed after the RAID controller driver upgrade:

Capture and share the following logs for further analysis:

- Guest-VM sysreport
- VMware's host diagnostic report
- RAID controller's firmware log

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

Table 4-4 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 4-4 vCPUs, Server Datastore Memory, and Disk Space by Cisco vWAAS Model**

| Cisco vWAAS Model                         | For Cisco WAAS v4.3.1 through v5.3.5 |                              |         | For Cisco WAAS v5.4.x through v6.x |                              |         |
|-------------------------------------------|--------------------------------------|------------------------------|---------|------------------------------------|------------------------------|---------|
|                                           | vCPUs                                | VMware ESXi Datastore Memory | Disk    | vCPUs                              | VMware ESXi Datastore Memory | Disk    |
| vWAAS-150<br>(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 |

Table 4-5 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 4-5** vCPUs, Server Datastore Memory, and Disk Space by Cisco vCM Model

| Cisco vCM Model | For Cisco WAAS v4.3.1 through v5.3.5 |                              |        | For Cisco WAAS v5.4.x through v6.x |                              |        |
|-----------------|--------------------------------------|------------------------------|--------|------------------------------------|------------------------------|--------|
|                 | 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 [Table 1-17](#), “Resized vWAAS CPU and Memory Specifications for Cisco WAAS Version 6.4.1a and Later,” in the chapter “[Introduction to Cisco vWAAS](#)”.

## OVA Package Formats for Cisco vWAAS on VMware ESXi

This section contains the following topics:

- [OVA Package for Cisco vWAAS on VMware ESXi for Cisco WAAS Version 5.x to 6.2.x](#), page 4-4
- [OVA Package for Cisco vWAAS on VMware ESXi for Cisco WAAS Version 6.4.1 and Later](#), page 4-5

**Note**

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

## OVA Package for Cisco vWAAS on VMware ESXi for Cisco 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 (examples shown in [Table 4-6](#)) and for each Cisco vCM connection profile (examples shown in [Table 4-7](#)).

**Table 4-6** Cisco OVA Package Format Examples for Cisco vWAAS on VMware ESXi

| Package Format                       | File Format Example                   |
|--------------------------------------|---------------------------------------|
| Cisco vWAAS 150 package file         | • Cisco-vWAAS-150-6.2.3d-b-68.ova     |
| Cisco vWAAS 150 package file for NPE | • Cisco-vWAAS-150-6.2.3d-npe-b-68.ova |
| Cisco vWAAS 200 package file         | • Cisco-vWAAS-200-6.2.3d-b-68.ova     |
| Cisco vWAAS 200 package file for NPE | • Cisco-vWAAS-200-6.2.3d-npe-b-68.ova |

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

**Table 4-7 Cisco OVA Package Formats for vCM for WAAS Versions earlier than Version 6.4.1**

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

## OVA Package for Cisco vWAAS on VMware ESXi for Cisco 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:

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

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

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

Use the VMware ESXi OVF template wizard to deploy these files, as described in [Installing VMware ESXi for Cisco vWAAS for Cisco WAAS Version 6.4.1 through 6.4.3a, page 4-11](#) and [Installing VMware ESXi for Cisco vWAAS for Cisco WAAS Version 6.4.3b and Later, page 4-12](#).

# Installing Cisco vWAAS on VMware ESXi

This section has the following topics:

- [Installing VMware ESXi for Cisco vWAAS in Cisco WAAS Versions 5.x to 6.2.x](#), page 4-6
- [Installing VMware ESXi for Cisco vWAAS for Cisco WAAS Version 6.4.1 through 6.4.3a](#), page 4-11
- [Installing VMware ESXi for Cisco vWAAS for Cisco WAAS Version 6.4.3b and Later](#), page 4-12

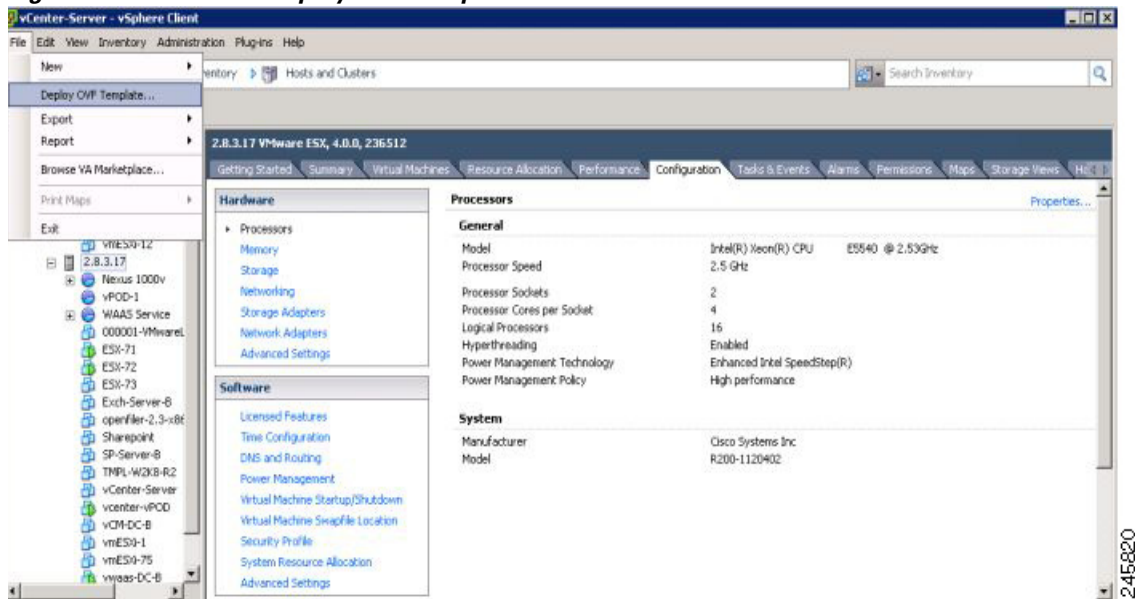
## Installing VMware ESXi for Cisco vWAAS in Cisco WAAS Versions 5.x to 6.2.x

To install the Cisco vWAAS VM with VMware vSphere ESXi, follow these steps:

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

The **Source** window appears.

**Figure 4-1** File > Deploy OVF Template



**Step 2** Click **Browse**.

The **Open** window appears.

**Step 3** Navigate to the location of the Cisco 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.

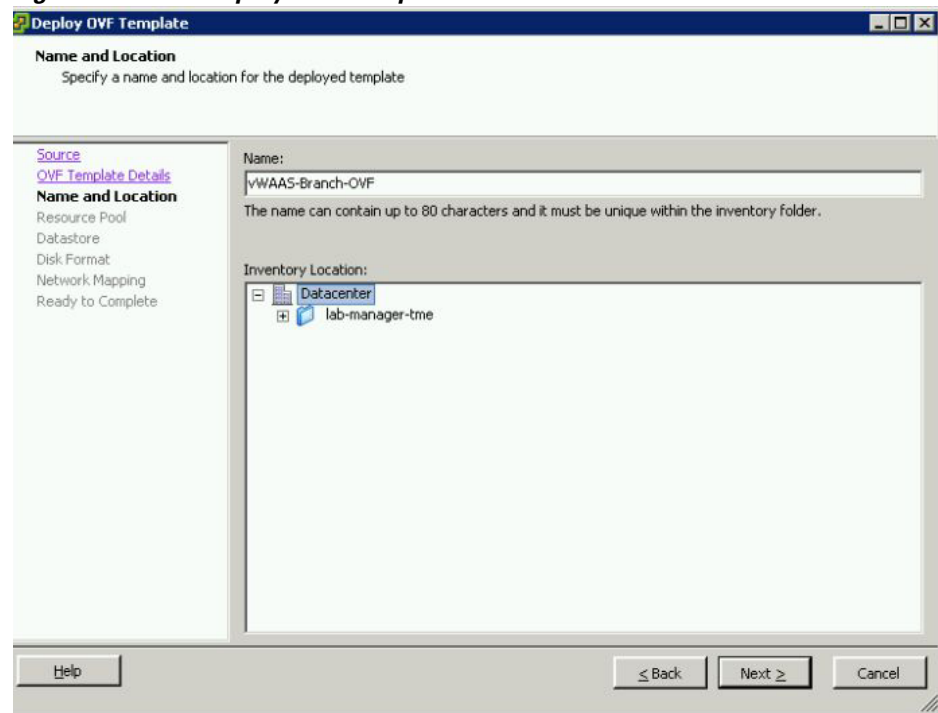
**Step 4** Click **Next** to accept the selected OVA file.

The **Name and Data Center Location** window appears (Figure 4-2).

**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).

**Figure 4-2** Deploy OVF Template > Name and Data Center Location

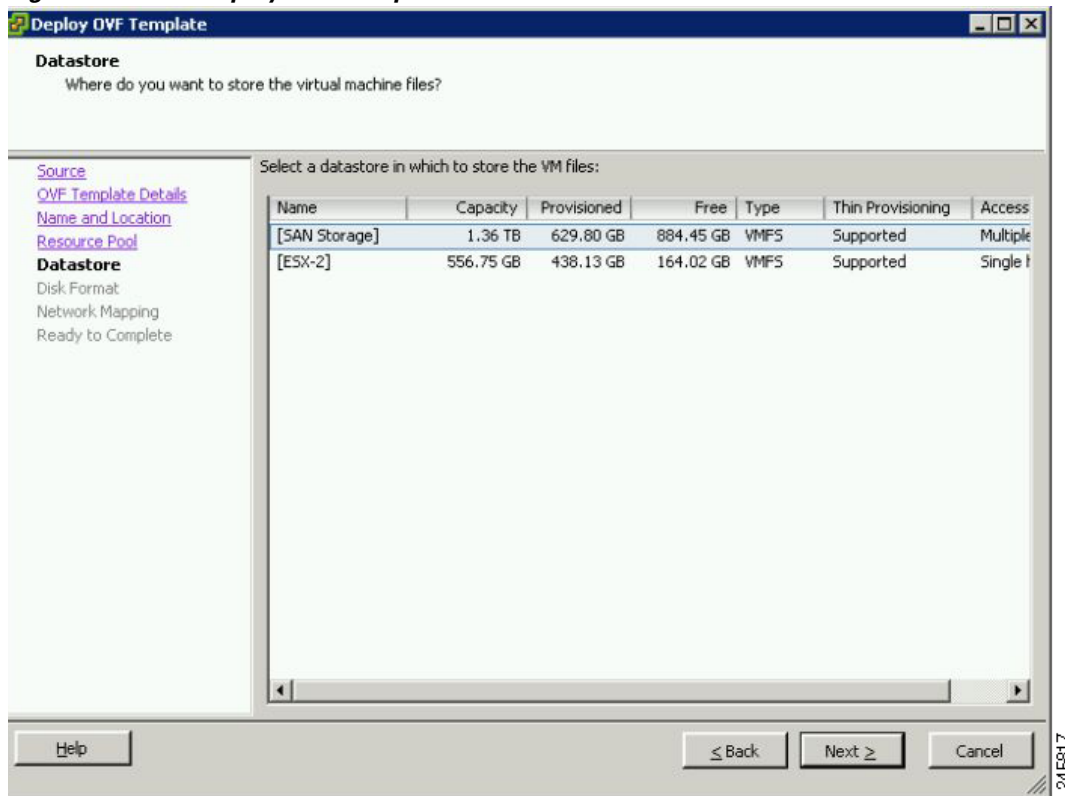


**Step 6** If configured, choose a cluster for the Cisco vWAAS VM. Otherwise, select the resource pool and then click **Next**.

The **Datastore** window appears (Figure 4-3).

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

Figure 4-3 Deploy OVF Template &gt; Datastore



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

The **Create a Disk** window appears.

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



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

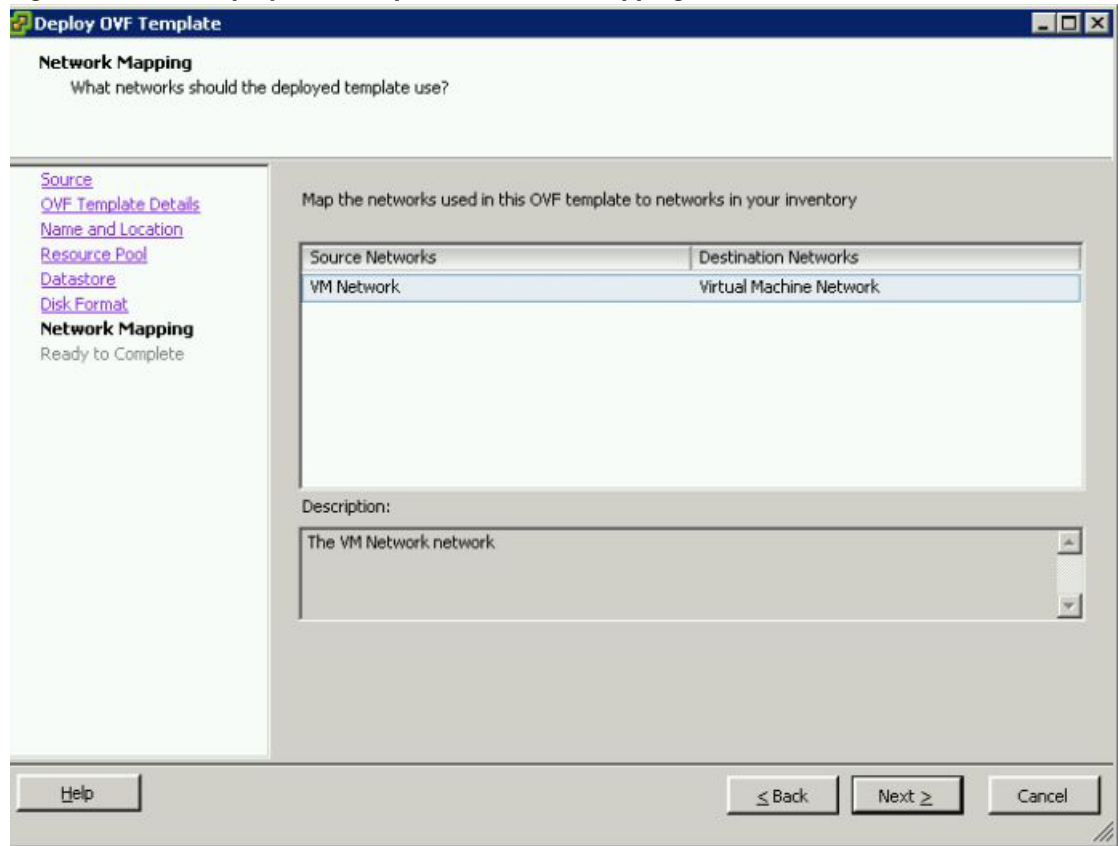
**Step 9** Click **Next**.

The **Network Mapping** window appears (Figure 4-4).

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

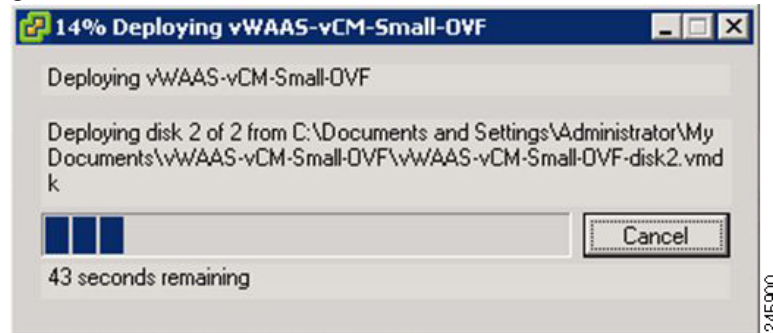
The **Ready to Complete** window appears.

Figure 4-4 Deploy OVF Template &gt; Network Mapping



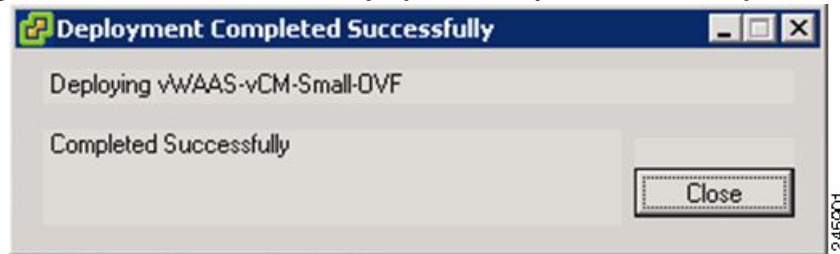
- Step 11** Click **Finish** to complete the installation.  
The **Status** window appears while the OVA file is being deployed.

Figure 4-5 Cisco vWAAS: Status Window



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

Figure 4-6 Cisco vWAAS: Deployment Completed Successfully

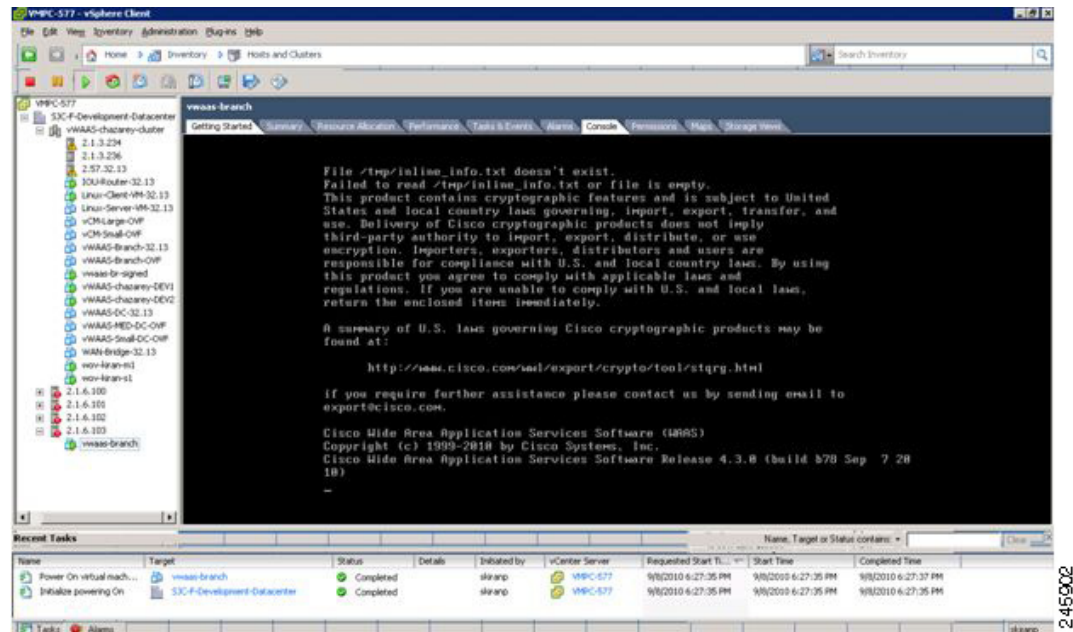


**Step 13** Click Close.

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

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

Figure 4-7 Cisco vWAAS: Console

**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 information on how to resolve this situation, see [Resolving Diskless Startup and Disk Failure](#) in the chapter “Troubleshooting Cisco vWAAS.”

For Cisco vWAAS configuration information, see the chapter “[Configuring Cisco vWAAS and Viewing Cisco vWAAS Components](#)”.

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

### Before you begin:

- As a pre-requisite, 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.

To deploy the VMware ESXi hypervisor for Cisco vWAAS, follow these steps:

---

**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 **Deploy 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 for Cisco WAAS Version 6.4.3b and Later

This section contains the following procedures:

- [Installing VMware ESXi with VMware vCenter, page 4-12](#)
- [Installing Cisco vWAAS VM with the VMware OVF Tool, page 4-23](#)

### Installing VMware ESXi with VMware vCenter



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

#### Before you begin:

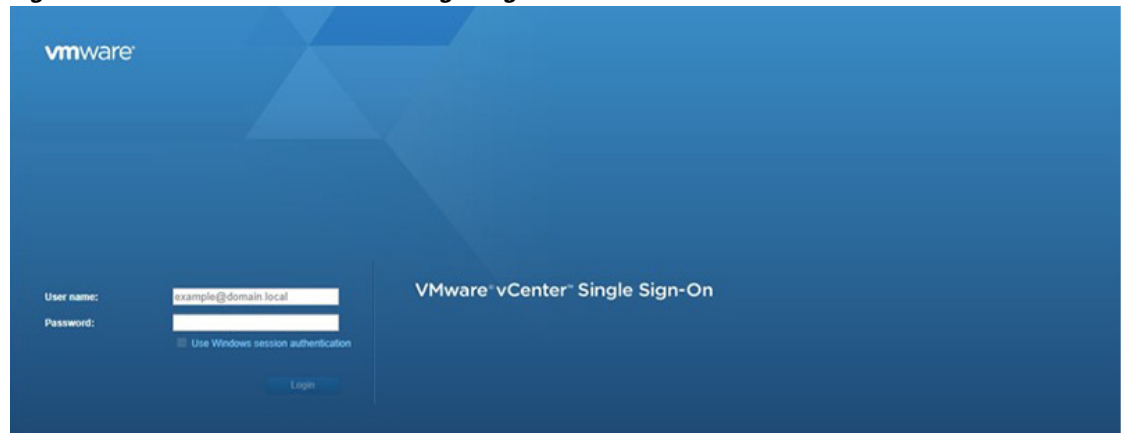
- As a pre-requisite, ensure that the required supporting plugins like Adobe Flash and Client Interaction Plugin are installed.
- For OVA deployments, always use **vSphere Web Client (Flash)**, because HTML5 mode does not have all the functionality supported.

To deploy the VMware ESXi hypervisor for Cisco vWAAS in WAAS Version 6.4.3b and later, follow these steps:

**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 4-8](#)).

**Figure 4-8 VMware vCenter Single Sign-On Window**

356143

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

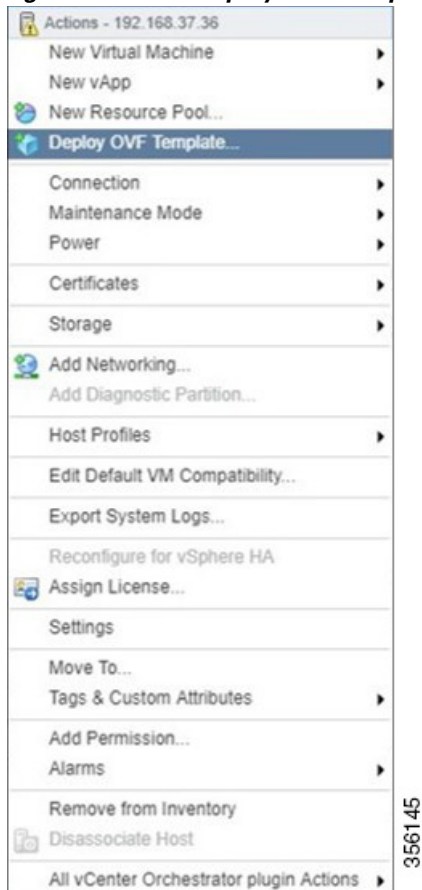
**Step 4** Click the required host to highlight it (example shown in [Figure 4-9](#)).

**Figure 4-9 Navigator > Datacenter > Host Menu Option**

356144

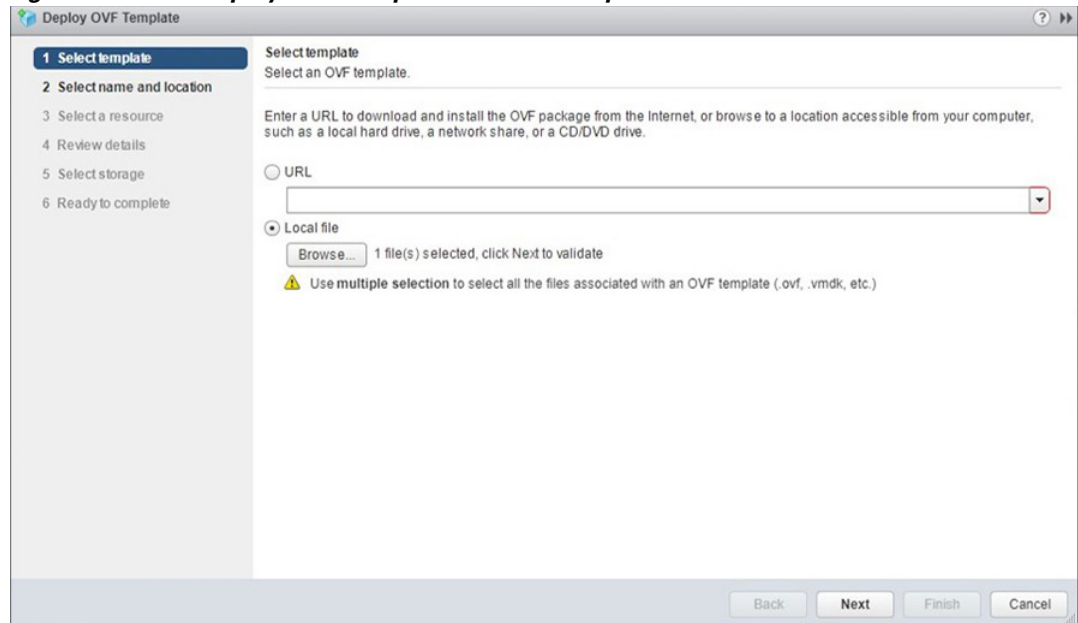
**Step 5** After you have highlighted the required host, right-click and select **Deploy OVF Template...** ([Figure 4-10](#)).

**Figure 4-10** Deploy OVF Template... Menu Option

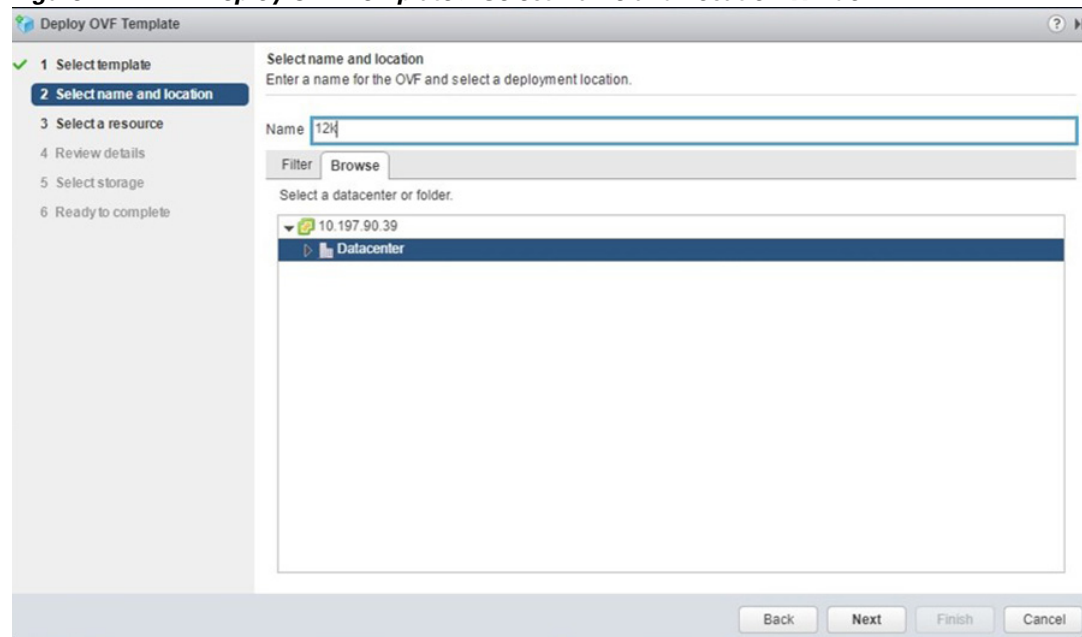


- Step 6** In the **Deploy OVF Template > Select Template** window (Figure 4-11):
- a. Enter the URL to download the OVA package or browse for the downloaded OVA file using the **Browse** button.
  - b. Click **Next**.



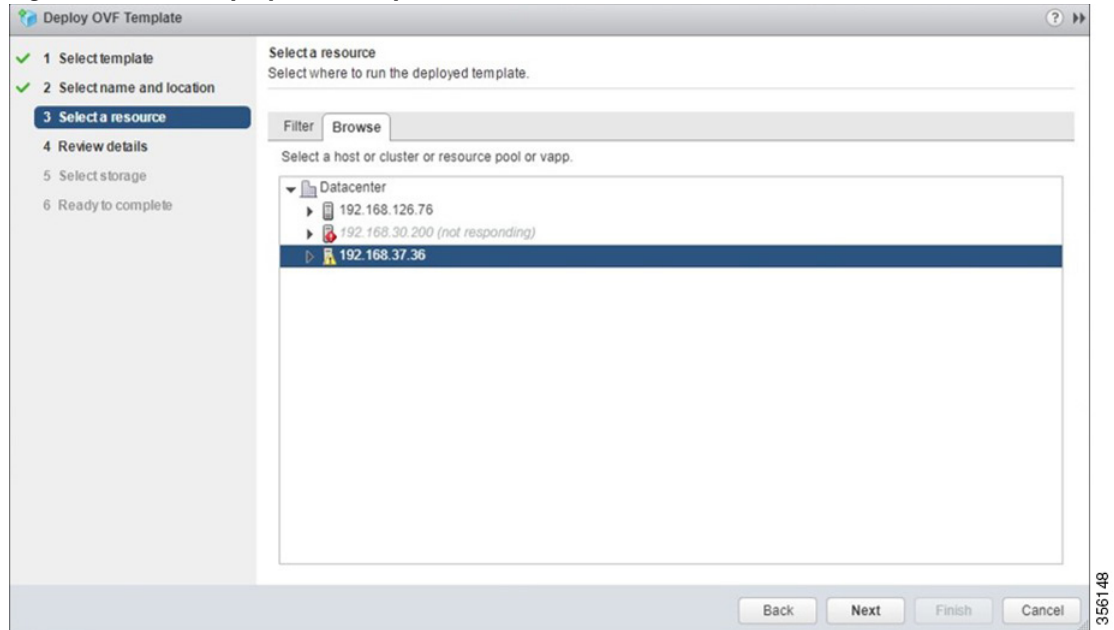
**Figure 4-11** Deploy OVF Template > Select Template Window

- Step 7** In the **Deploy OVF Template > Select Name and Location** window (Figure 4-12):
- 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 4-12** Deploy OVF Template > Select Name and Location Window

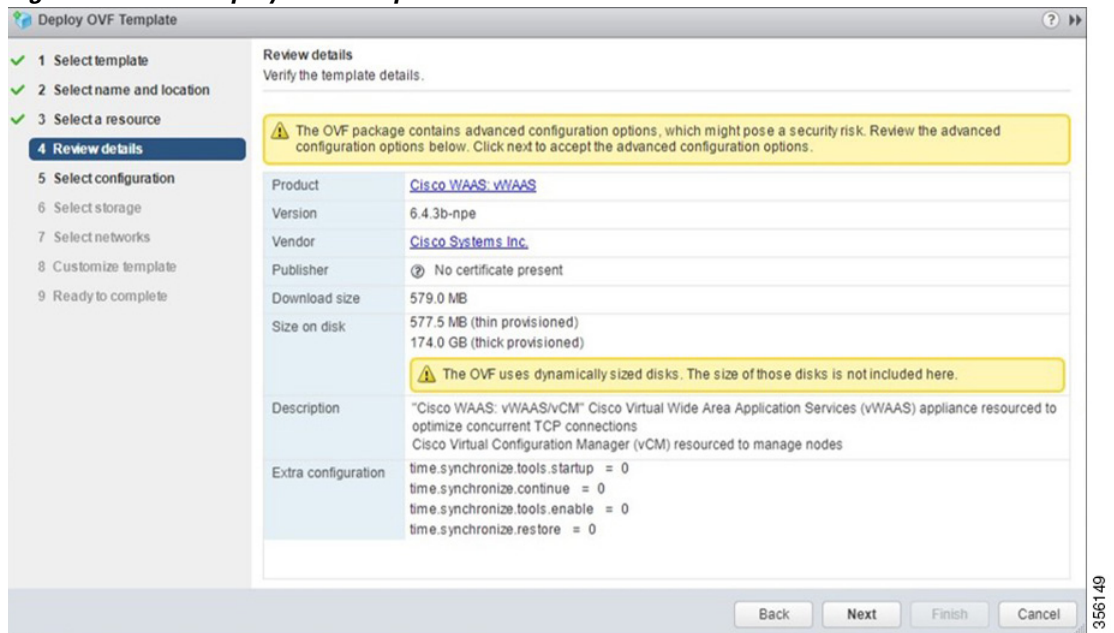
- Step 8** In the **Deploy OVF Template > Select a Resource** window (Figure 4-13), select the resource (the host) where the OVA will be deployed.

Figure 4-13 Deploy OVF Template &gt; Select a Resource Window



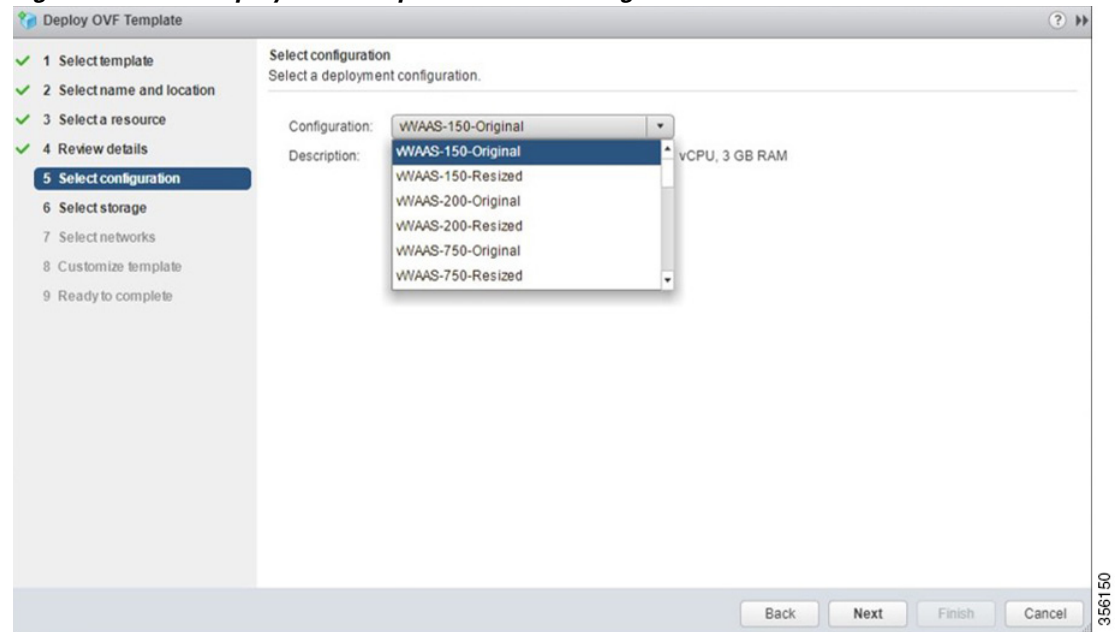
**Step 9** In the **Deploy OVF Template > Review Details** window, verify that the template details are correct. Figure 4-14 shows a **Review Details** window with configuration notices and guidance messages.

Figure 4-14 Deploy OVF Template &gt; Review Details Window



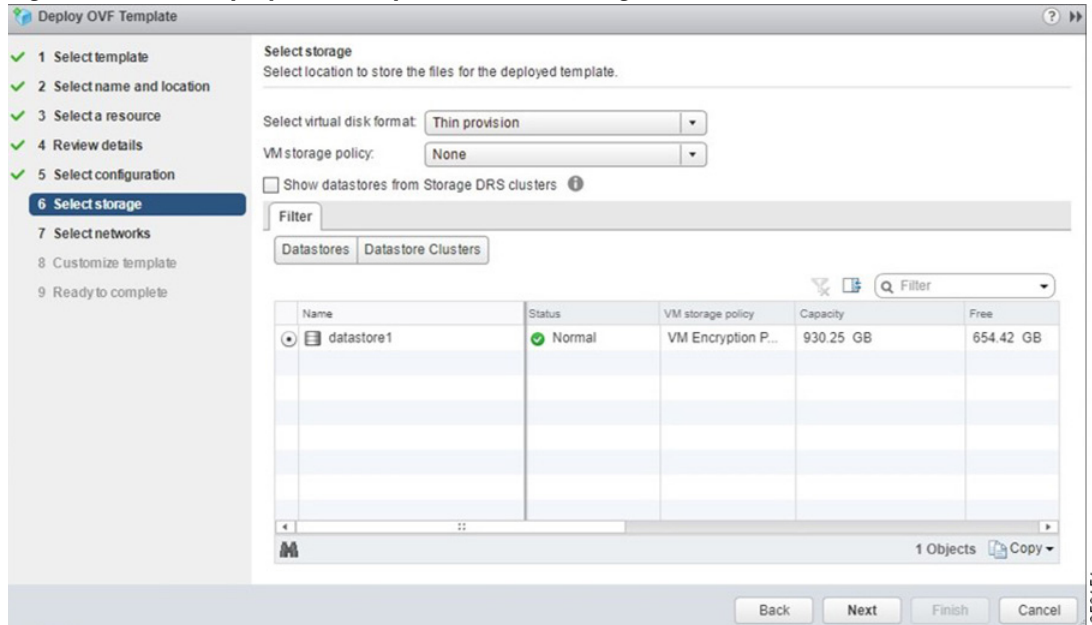
**Step 10** In the **Deploy OVF Template > Select Configuration** window (Figure 4-15):

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

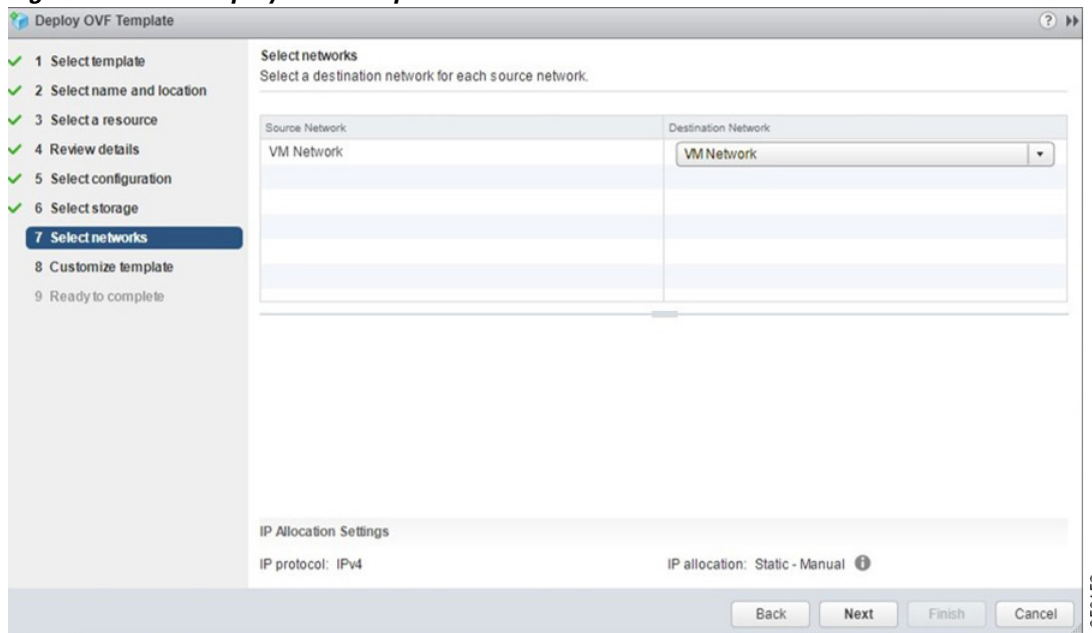
**Figure 4-15** Deploy OVF Template > Select Configuration Window

**Step 11** In the **Display OVF Template > Select Storage** window (Figure 4-16):

- a. From the **Select virtual disk format** drop-down list, select the type of storage required for your system: Thick Provision 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 4-16** Deploy OVF Template > Select Storage Window

- Step 12** From the **Deploy OVF Template > Select Networks** window (Figure 4-17):
- From the **Destination Network** drop-down list, choose the appropriate VM network for your system.
  - Click **Next**.

**Figure 4-17** Deploy OVF Template > Select Networks Window

- Step 13** In the **Deploy OVF Template > Customize Template** window (Figure 4-18), review the information and click **Next**.

**Caution**

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

**Figure 4-18** *Deploy OVF Template > Customize Template Window*

Deploy OVF Template

1 Select template  
2 Select name and location  
3 Select a resource  
4 Review details  
5 Select configuration  
6 Select storage  
7 Select networks  
8 **Customize template**  
9 Ready to complete

Customize template  
Customize the deployment properties of this software solution.

All properties have valid values [Show next...](#) [Collapse all...](#)

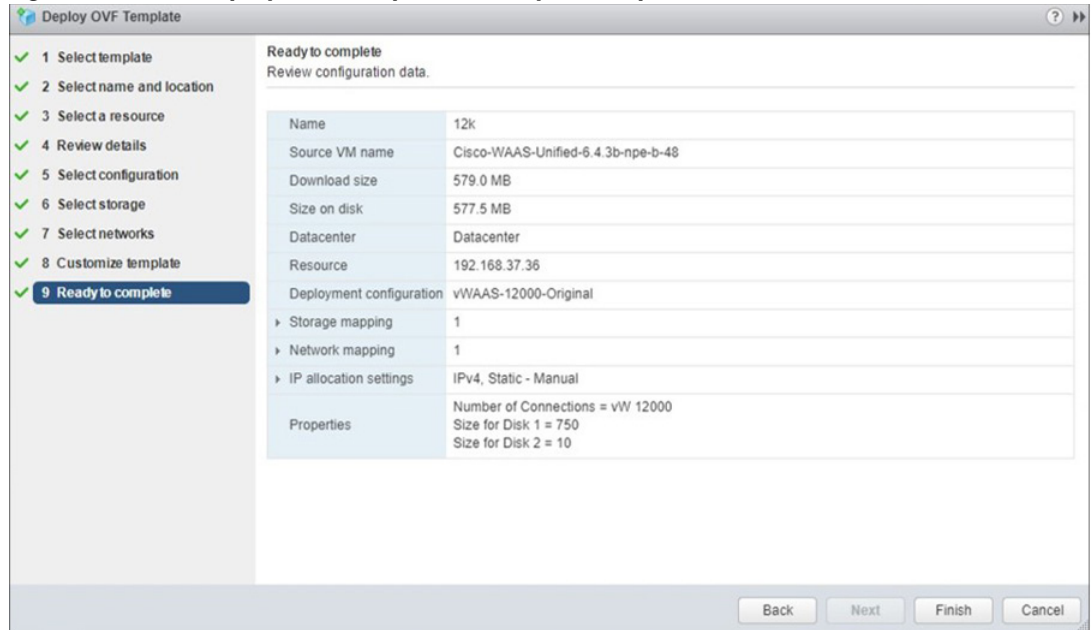
|                       |                                                                               |
|-----------------------|-------------------------------------------------------------------------------|
| Uncategorized         | 3 settings                                                                    |
| Number of Connections | The number of connections to deploy.<br><input type="text" value="vW 12000"/> |
| Size for Disk 1       | The size of the disk in gigabytes.<br><input type="text" value="750"/>        |
| Size for Disk 2       | The size of the disk in gigabytes.<br><input type="text" value="10"/>         |

Back Next Finish Cancel

356153

- Step 14** In the **Deploy OVF Template > Ready to Complete** window (Figure 4-19):
- Review and confirm configuration data, including Cisco vWAAS model name, storage mapping, network mapping, number of connections, and disk sizes.
  - Click **Next**.

Figure 4-19 Deploy OVF Template &gt; Ready to Complete Window



**Step 15** The **Recent Tasks** pane of the VMware vSphere Web Client window (Figure 4-20) displays the status of the import and deployment of the image.

Figure 4-20 VMware vSphere Web Client Recent Tasks Pane - In-Progress Status

| Task Name                 | Target        | Status    | Initiator             | Queued For | Start Time          | Completion Time     |
|---------------------------|---------------|-----------|-----------------------|------------|---------------------|---------------------|
| Deploy OVF template       | 192.168.37.36 | 0%        | VSPHERE LOCAL\...     | 22 ms      | 4/2/2019 5:14:12 PM |                     |
| Import OVF package        | 192.168.37.36 | 0%        | vsphere.local\Admi... | 115 ms     | 4/2/2019 5:11:56 PM |                     |
| Delete virtual machine    | vcm-100       | Completed | VSPHERE LOCAL\...     | 51 ms      | 4/2/2019 5:09:10 PM | 4/2/2019 5:09:10 PM |
| Power Off virtual machine | vcm-100       | Completed | VSPHERE LOCAL\...     | 8 ms       | 4/2/2019 5:09:02 PM | 4/2/2019 5:09:03 PM |
| Delete virtual machine    | 200           | Completed | VSPHERE LOCAL\...     | 11 ms      | 4/2/2019 5:07:53 PM | 4/2/2019 5:07:55 PM |

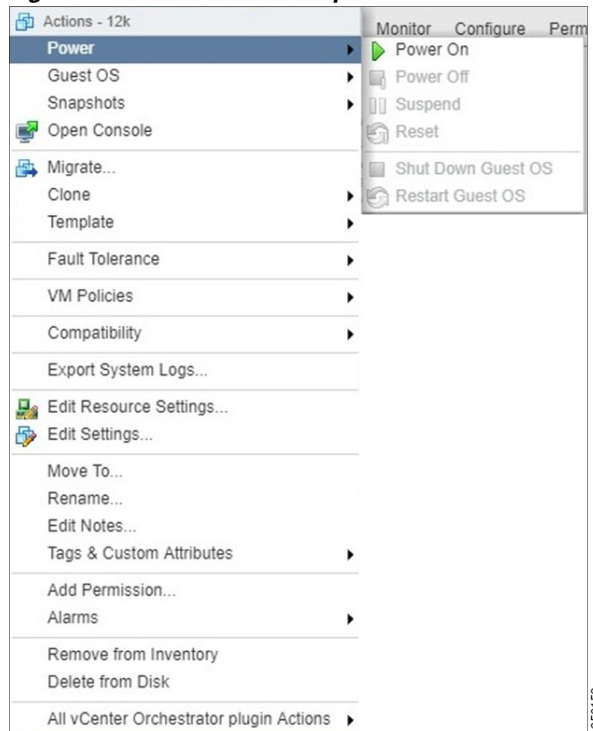
**Step 16** After deployment is complete, the **Recent Tasks** pane items show **Completed** for the deployed Cisco vWAAS image (Figure 4-21).

Figure 4-21 VMware vSphere Web Client Recent Tasks Pane - Completed Status

| Task Name                | Target        | Status    | Initiator             | Queued For | Start Time          | Completion Time     |
|--------------------------|---------------|-----------|-----------------------|------------|---------------------|---------------------|
| Power On virtual machine | Dev-150k      | Completed | VSPHERE LOCAL\...     | 11 ms      | 4/2/2019 5:15:30 PM | 4/2/2019 5:15:40 PM |
| Initialize powering On   | Datacenter    | Completed | VSPHERE LOCAL\...     | 19 ms      | 4/2/2019 5:15:30 PM | 4/2/2019 5:15:30 PM |
| Deploy OVF template      | 12k           | Completed | VSPHERE LOCAL\...     | 22 ms      | 4/2/2019 5:14:12 PM | 4/2/2019 5:17:12 PM |
| Import OVF package       | 192.168.37.36 | Completed | vsphere.local\Admi... | 115 ms     | 4/2/2019 5:11:56 PM | 4/2/2019 5:17:12 PM |
| Delete virtual machine   | vcm-100       | Completed | VSPHERE LOCAL\...     | 51 ms      | 4/2/2019 5:09:10 PM | 4/2/2019 5:09:10 PM |

**Step 17** After deployment is complete, use the **Power > Power On** menu option to power on the device (Figure 4-22).

**Figure 4-22 VMware vSphere Web Client Power > Power On Menu Option**



**Note**

Sporadically, deployment may fail due to a communication error between VMware vCenter and the VMware ESXi host. If this occurs during deployment, try 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

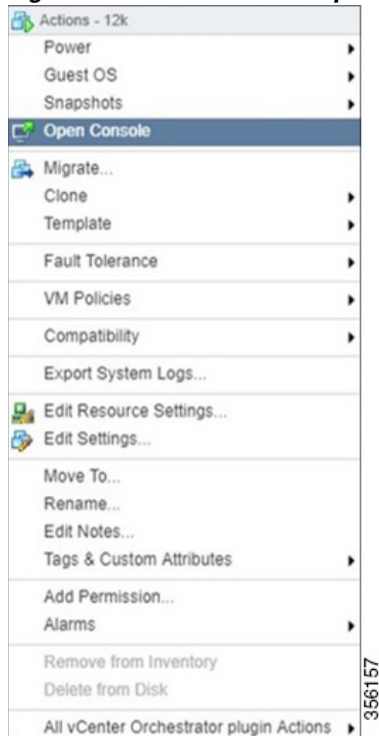
Alternatively, while deploying, choose the **Disk Type** option as **Thin Provisioning** and use the following procedure to convert the disks to **Thick Eager Zero**.

1. Wait for the deployment to complete 100%
2. Ensure the deployed VM is in **Power-Off** state. If it is not, power off the device before proceeding to the next step.
3. Navigate to the folder of the virtual disk you want to inflate.
  - a. In the vSphere Web Client, browse to the virtual machine.
  - b. Click the **Datastores** tab.  
The datastore that stores the virtual machine files is listed.
  - c. Select the datastore and click the **Browse Files** icon.  
The datastore browser displays contents of the datastore.
4. Expand the virtual machine folder and browse through the list of files. The files with extension **.vmdk** will have the virtual disk icon.
5. Right-click the **.vmdk** virtual disk file and select the **Inflate** option.

6. 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. [Figure 4-23](#) shows the **Open Console** menu option and [Figure 4-24](#) shows the device console.

**Figure 4-23** VMware vSphere Web Client Open Console Menu Option



**Figure 4-24** Device Console

```

Keepalive problem: Node Health Mgr incorrectly marked nodemgr dead, will reregister
terPassword:
Login incorrect

UCSE-ESXI login: admin
Password:
System Initialization Finished.
UCSE-ESXI#sh ver
Cisco Wide Area Application Services Software (WAAS)
Copyright (c) 1999-2019 by Cisco Systems, Inc.
Cisco Wide Area Application Services (universal-npe-k9) Software Release 6.4.3b-
npe (build b48 Mar 29 2019)
Version: oe-vwaas-6.4.3b.48

Compiled 16:12:45 Mar 29 2019 by cnbuild

Device Id: 00:50:56:99:07:c1
System was restarted on Tue Apr 2 11:38:08 2019.
System restart reason: Power-on.
The system has been up for 10 minutes, 50 seconds.

UCSE-ESXI#_

```



## Installing Cisco vWAAS VM with the VMware OVF Tool

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.

To install the Cisco vWAAS VM with the VMware OVF Tool, follow these steps:

- 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, 200, 750, 1300, 2500, 6000, 6000R, 12000, 50000, 150000  
To deploy an original Cisco vWAAS model: Use the designation “VW\_”, for example, **VW\_6000**
    - Resized Cisco vWAAS models supported:  
vWAAS-150, 200, 750, 1300, 2500, 6000, 6000R, 12000, 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, 500, 1000, 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

---

## Operating Guidelines for Cisco vWAAS in WAAS Version 6.4.3 and later in VMware ESXi

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:
    - a. In VMware vSphere, choose the **Virtual Hardware** tab, and from the **Adapter Type** drop-down list, choose **VMXNET3**.
    - b. 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.
    - c. 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:
  - a. Power off the VM.
  - b. From the host, change the adapter type to **VMXNET3**.
  - c. Power on the VM.
  - d. To verify that the configured routers appear in the routing table output, run the **show ip route EXEC** command.

## Upgrade and Downgrade Guidelines for Cisco 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:

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





## Cisco vWAAS 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, page 5-1](#)
- [Supported Host Platforms, Software Versions, and Disk Type, page 5-2](#)
- [Cisco vWAAS on Microsoft Hyper-V System Requirements, page 5-2](#)
- [Deployment Options for Cisco vWAAS on Microsoft Hyper-V, page 5-3](#)
- [OVA Package Formats for Cisco vWAAS on Microsoft Hyper-V, page 5-4](#)
- [Installing Cisco vWAAS on Microsoft Hyper-V, page 5-6](#)
- [Activating and Registering Cisco vWAAS on Microsoft Hyper-V, page 5-8](#)
- [Traffic Interception Methods for Cisco vWAAS on Microsoft Hyper-V, page 5-8](#)
- [Operating Guidelines for Cisco vWAAS on Microsoft Hyper-V, page 5-11](#)
- [Configuring GPT Disk Format for Cisco vWAAS-50000 on Microsoft Hyper-V with Akamai Connect, page 5-14](#)

### 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

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

**Table 5-1** Platforms and Software Versions Supported for Cisco vWAAS on VMware ESXi

| PID and Device Type                                                                                          | Earliest Supported Cisco WAAS Version                  | Host Platforms                                                                          | Earliest Supported Host Version                                             | Disk Type                                             |
|--------------------------------------------------------------------------------------------------------------|--------------------------------------------------------|-----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|-------------------------------------------------------|
| <ul style="list-style-type: none"> <li>PID: OE-VWAAS-HYPERV</li> <li>Device Type: OE-VWAAS-HYPERV</li> </ul> | <ul style="list-style-type: none"> <li>6.1x</li> </ul> | <ul style="list-style-type: none"> <li>Cisco UCS</li> <li>Cisco UCS-E Series</li> </ul> | <ul style="list-style-type: none"> <li>Microsoft Windows 2008 R2</li> </ul> | <ul style="list-style-type: none"> <li>VHD</li> </ul> |

## Cisco vWAAS on Microsoft Hyper-V System Requirements

This section contains the following topics:

- [System Infrastructure Requirements, page 5-2](#)
- [Hardware Virtualization Requirements, page 5-2](#)

### System Infrastructure Requirements

Your Cisco WAAS system must have the following 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:** 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.

### Hardware Virtualization Requirements

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

- 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 Cisco vCM Models](#), page 4-3 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.

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

**Table 5-2** 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.

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

**Table 5-3 Platforms Supported for Cisco vWAAS in Microsoft Hyper-Server or Microsoft Windows Server**

| <b>Standalone Product in Microsoft Hyper-V Server</b>                                                                                                                |                                                                                          | <b>Installable Product in Windows Server</b>                                             |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|
| <b>Hyper-V Server 2008 R2</b>                                                                                                                                        | <b>Hyper-V Server 2012 or 2012 R2 or 2016</b>                                            | <b>Windows Server 2012 or 2012 R2</b>                                                    |
| 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<br>(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<br>(For Cisco WAAS Version 6.2.1 and later, supported on Cisco EHWIC and NIM.) | vWAAS-150<br>(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 Cisco vWAAS on Microsoft Hyper-V

This section contains the following topics:

- [OVA Package for Cisco vWAAS on Microsoft Hyper-v in Cisco WAAS Version 6.1.x and Later, page 5-4](#)
- [Unified OVA Package for Cisco vWAAS on Microsoft Hyper-V in Cisco WAAS Version 6.4.1 and Later, page 5-5](#)

### OVA Package for Cisco vWAAS on Microsoft Hyper-v in Cisco WAAS Version 6.1.x and Later

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 (examples shown in [Table 5-4](#)) and for each vCM connection profile (examples shown in [Table 5-5](#)).

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.

**Table 5-4 OVA Package Format Examples for Cisco vWAAS on Microsoft Hyper-V for Cisco WAAS Version 6.1.x and Later**

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

**Table 5-5 Cisco OVA Package Formats for Cisco vCM for Cisco WAAS Version 6.1.x and Later**

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

## Unified OVA Package for Cisco vWAAS on Microsoft Hyper-V in 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-6.4.1-b-33.zip
- NPE OVA: Cisco-HyperV-vWAAS-Unified-6.4.1-b-33-npe.zip

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

- SCVMM template file
- WAAS image ISO
- Virtual hard disk file for Flash
- PowerShell deployment script for SCVMM and a set of template .xml files
- PowerShell deployment script for standalone hosts and a set of template .xml files

## Installing Cisco vWAAS on Microsoft Hyper-V

This section contains the following topics:

- [Installing Cisco vWAAS on Microsoft Hyper-V for Cisco vWAAS in Cisco WAAS Version 5.x to 6.2.x, page 5-6](#)
- [Installing Cisco vWAAS on Microsoft Hyper-V in Cisco WAAS Version 6.4.1 and Later, page 5-7](#)

## Installing Cisco vWAAS on Microsoft Hyper-V for Cisco vWAAS in Cisco WAAS Version 5.x to 6.2.x

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 Cisco vWAAS on Microsoft Hyper-V, page 5-8](#).

This section contains the following topic:

- [Installing Cisco vWAAS on Microsoft Hyper-V with a VHD Template, page 5-6](#)

### Installing Cisco vWAAS on Microsoft Hyper-V with a VHD Template

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.

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

- 
- Step 1** Download the Cisco vWAAS package to the computer where the SCVMM2012 or the 2012 R2 console is installed.
  - Step 2** Unzip the Cisco vWAAS package.
  - Step 3** Log in to the SCVMM console.
  - Step 4** Launch the PowerShell window that is displayed in the SCVMM.
  - Step 5** Navigate to the PowerShell script in the uncompressed vWAAS package:  
**.\Cisco-vWAAS-model-name-6.0.0-ISO\Cisco-vWAAS-model-name-6.0.0-ISO**
  - Step 6** Run the **deploy-vwaas-model-name** PowerShell script.
  - Step 7** Follow the procedure that is requested by the deployment script.

- Step 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](#)).

- Step 9** To enter the maximum amount of memory, follow these steps:
- a. From the **SC VMM** 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.

## Installing Cisco vWAAS on Microsoft Hyper-V in Cisco WAAS Version 6.4.1 and Later

To deploy Microsoft Hyper-V in Cisco vWAAS in WAAS 6.4.1 and later, follow this step:

- Step 1** From the Cisco WAAS Installer for Hyper-V, enter the number of your Cisco vWAAS or Cisco 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.

# Activating and Registering Cisco vWAAS on Microsoft Hyper-V

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, see [Installing Cisco vWAAS on Microsoft Hyper-V, page 5-6](#).

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.

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

- 
- 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, configure WCCP interception. For more information on configuring WCCP interception, see [WCCP Interception](#). No configuration is necessary for appnav-controller interception.
- Step 3** Configure the 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, page 5-9](#)

- [WCCP Interception, page 5-9](#)
- [AppNav Controller Interception, page 5-10](#)

## 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.

## WCCP Interception

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](#).

### Before You Begin

Before you do the following procedure, you should have already configured your router for basic WCCP, as described in the [Cisco Wide Area Application Services Configuration Guide](#).

- 
- Step 1** From the 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–FE000000. The default is F00. Enter a value for the destination IP mask in the **Destination IP Mask** field. The range, in hexadecimal, is 00000000–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, check the **Enable Flow Protection** check box to keep the TCP flow intact and to avoid overwhelming the device when it comes up or is reassigned new traffic. For more information on flow redirection, see the Information about WCCP Flow Redirection on WAEs” section of the *Cisco Wide Area Application Services Configuration Guide*.
- Step 12** In the **Flow Protection Timeout** field, specify the amount of time (in seconds) for which flow protection should be enabled. The default is **0**, which means flow protection stays enabled with no timeout.
- Step 13** In the **Shutdown Delay** field, enter a maximum amount of time (in seconds) the chosen device waits to perform a clean shutdown of WCCP. The range is **0** to **86400** seconds. The default is **120** seconds.
- Step 14** From the **Failure Detection Timeout** drop-down list, choose a failure detection timeout value: **30**, **15**, or **9** seconds. The default is **30** seconds. The failure detection timeout determines the length of time the router takes to detect a WAE failure.
- Step 15** In the **Weight** field, specify the weight to be used for load balancing. The weight value range is **0** to **10000**.
- If the total of all the weight values of the WAEs in a service group is less than or equal to **100**, the weight value represents a literal percentage of the total load redirected to the device for load-balancing purposes.
  - If the total of all the weight values of the WAEs in a service group is between **101** and **10000**, the weight value is treated as a fraction of the total weight of all the active WAEs in the service group.
- Step 16** In the **Password** field, specify the password to be used for secure traffic between the WAEs within a cluster and the router for a specified service. Be sure to enable all other WAEs and routers within the cluster with the same password. Passwords must not exceed eight characters in length. Do not use the following characters: space, backwards single quote (‘), double quote (“”), pipe (|), or question mark (?)
- Step 17** Re-enter the password in the **Confirm Password** field.
- Step 18** Click **Submit** to save the settings.

## AppNav Controller Interception

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.

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

- 
- 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 has the following topics:

- [Cisco vWAAS Deployments, Cisco UCS-E Upgrades, and Microsoft Windows Server Updates, page 5-11](#)
- [Configuring NTP Settings for Cisco vWAAS on Microsoft Hyper-V, page 5-11](#)
- [Microsoft Hyper-V High Availability Features, page 5-12](#)

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



#### Caution

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](#). You can also obtain the standalone update package through the Microsoft Download Center by searching for **KB2887595**.

### Configuring NTP Settings for Cisco vWAAS on Microsoft Hyper-V

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 (SC VMM) or the Microsoft Hyper-V Manager.

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

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

From the Microsoft SC VMM:

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

From the 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**.

## Microsoft Hyper-V High Availability Features

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

- [Live Migration, page 5-12](#)
- [Network Interface Card Teaming, page 5-13](#)

### 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 workflow for initiating and completing a live migration:



- **Create a connection between hosts:** The source physical host creates a TCP connection with the destination physical host, which is used to transfer the VM configuration data to the destination physical host. A skeleton VM is set up on the destination physical host, and memory is allocated to the destination VM.
- **Copy the working set to the destination host:** The memory assigned to the migrating VM, called the working set, is copied to the destination physical host. This memory is referred to as the working set of the migrating VM. A page of memory is 4 kB in size.
- **Mark modified memory pages:** The utilized pages within the working set are copied to the destination 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.
- **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 copied 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.

---

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



---

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

---

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

## 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, page 2-7](#).

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 Cisco vWAAS-50000 on Microsoft Hyper-V with Akamai Connect

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.

To convert the Hard Disk Drive (HDD) from MBR format to GPT format, follow these steps:

- 
- Step 1** Install windows in one partition of the HDD.
- Step 2** After installation is complete, create a new volume to create a new disk partition:
- Right-click the **Windows** command prompt and then select **Run as Administrator**.
  - Enter the **diskpart** command to enter **DiskPart** command mode.  
The DISKPART prompt is displayed.
- Step 3** At the **DISKPART** prompt:
- Run the **create volume** command to create a new volume on the disk.
  - 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.
  - Run the **select disk** *disk-number* command.
  - 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](#).

---





# 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, page 6-1](#)
- [Supported Host Platforms, Software Versions, and Disk Type, page 6-2](#)
- [Cisco vWAAS on RHEL KVM System Requirements, page 6-2](#)
- [Cisco vWAAS on RHEL KVM in Cisco WAAS Version 5.x to 6.2.x, page 6-3](#)
- [Cisco vWAAS on RHEL KVM in Cisco WAAS Version 6.4.1 and Later, page 6-8](#)
- [Operating Guidelines for Cisco vWAAS on RHEL KVM/KVM on CentOS, page 6-11](#)
- [Upgrade and Downgrade Guidelines for Cisco vWAAS on RHEL KVM, page 6-13](#)

## 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

Table 6-1 shows the platforms and software versions supported for Cisco vWAAS on RHEL KVM.

**Table 6-1** Platforms and Software Versions Supported for Cisco vWAAS on RHEL KVM

| Cisco PID and Device Type                                                                                  | Earliest Cisco WAAS Version Supported                                | Cisco Host Platforms                                                            | Earliest RHEL and CentOS Host Version Supported                                                                                                                                | Disk Type                                                  |
|------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|---------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>• PID: OE-VWAAS-KVM</li> <li>• Device Type: OE-VWAAS-KVM</li> </ul> | <ul style="list-style-type: none"> <li>• 6.2x</li> </ul>             | <ul style="list-style-type: none"> <li>• UCS</li> <li>• UCS-E Series</li> </ul> | <ul style="list-style-type: none"> <li>• Red Hat Enterprise Linux (RHEL) Server 7.1</li> <li>• CentOS Linux 7.2.1511 (Core)</li> </ul>                                         | <ul style="list-style-type: none"> <li>• virtio</li> </ul> |
|                                                                                                            | <ul style="list-style-type: none"> <li>• 6.4.3d and later</li> </ul> | <ul style="list-style-type: none"> <li>• UCS</li> <li>• UCS-E Series</li> </ul> | <ul style="list-style-type: none"> <li>• RHEL Server 7.5</li> <li>• RHEL Server 7.6</li> <li>• CentOS Linux 7.5.1804 (Core)</li> <li>• CentOS Linux 7.6.1810 (Core)</li> </ul> | <ul style="list-style-type: none"> <li>• virtio</li> </ul> |

## 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 Table 10-4. While deploying RHEL KVM, Cisco vWAAS and Cisco vCM should verify that enough disk space is available in the respective partition.

**Table 6-2** Cisco vWAAS on RHEL KVM-Supported Configuration

| Feature/Component                   | Description                                                                                                                                                                            |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Platform                            | Three-disk platform of: <ul style="list-style-type: none"> <li>• 10 GB system</li> <li>• 4 GB flash</li> <li>• Data disk (customizable, depending on number of connections)</li> </ul> |
| RHEL version for Cisco vWAAS on KVM | RHEL 7.2                                                                                                                                                                               |

| Feature/Component               | Description                                                                                                                                                                                                                                                |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cisco vWAAS Memory Requirements | <ul style="list-style-type: none"> <li>vWAAS-150: 4 GB</li> <li>vWAAS-200: 4 GB</li> <li>vWAAS-750: 4 GB</li> <li>vWAAS-1300: 6 GB</li> <li>vWAAS-2500: 8 GB</li> <li>vWAAS-6000: 11 GB</li> <li>vWAAS-12000: 18 GB</li> <li>vWAAS-50000: 48 GB</li> </ul> |
| Interception Method             | Web Cache Communication Protocol (WCCP) 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, contact your Cisco account representative.                                                                                                                                                                       |
| MAC address                     | Customizable                                                                                                                                                                                                                                               |

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

This section contains the following topics:

- [TAR Archive Package for Cisco vWAAS on RHEL KVM in Cisco WAAS Version 5.x to 6.2.x, page 6-3](#)
- [Installing Cisco vWAAS on RHEL KVM in Cisco WAAS Version 5.x to 6.2.x, page 6-5](#)

### TAR Archive Package for Cisco vWAAS on RHEL KVM in Cisco 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 (examples shown in [Table 6-3](#)) and for each Cisco vCM connection profile (examples shown in [Table 6-4](#)).

[Table 6-5](#) shows the files included for deploying Cisco vWAAS on RHEL KVM, and for deploying Cisco vWAAS with Cisco Network Functions Virtualization Infrastructure Software (Cisco NFVIS). For more information on Cisco NFVIS and Cisco Network Functions Virtualization (Cisco NFV), see the [Cisco Enterprise Network Functions Virtualization Solution Overview](#). For more information on Cisco vWAAS with Cisco NFVIS, 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 6-3 OVA Package Format Examples for Cisco vWAAS on RHEL KVM in Cisco WAAS Version 5.x to 6.2.x**

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

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

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

**Table 6-5 Installation Files for Cisco vWAAS on RHEL KVM and Cisco vWAAS with Cisco NFVIS in WAAS 5.x to 6.2.x**

| Installation File                                                                                                                                                                                                                                  | RHEL KVM Installation | Cisco NFVIS Installation |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|--------------------------|
| <ul style="list-style-type: none"> <li>• <b>Cisco signature envelope file</b><br/>Verifies that this deployment is from Cisco.</li> </ul>                                                                                                          | Yes                   | Yes                      |
| <ul style="list-style-type: none"> <li>• <b>Manifest file with checksums</b></li> </ul>                                                                                                                                                            | Yes                   | Yes                      |
| <ul style="list-style-type: none"> <li>• <b>image_properties.xml</b><br/>A VM configuration template file used on the Cisco NFVIS platform.</li> </ul>                                                                                             | No                    | Yes                      |
| <ul style="list-style-type: none"> <li>• <b>package.mf</b> template file and <b>bootstrap-cfg.xml</b><br/>These two files work together on the Cisco NFVIS platform with the image_properties.xml file as Day-0 configuration template.</li> </ul> | No                    | Yes                      |
| <ul style="list-style-type: none"> <li>• <b>INSTRUCTIONS.TXT</b><br/>Describes the procedure for deploying the virtual instance and for using the launch.sh file.</li> </ul>                                                                       | Yes                   | No                       |
| <ul style="list-style-type: none"> <li>• <b>launch.sh</b> file<br/>For details on how to use this script, see <a href="#">Using the Launch Script to Deploy Cisco vWAAS on RHEL KVM in WAAS Version 5.x to 6.2.x, page 6-5</a>.</li> </ul>         | Yes                   | No                       |



| Installation File                                                                                                                                                                                                                                                                                                                                                                                                                                              | RHEL KVM Installation | Cisco NFVIS Installation |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|--------------------------|
| <ul style="list-style-type: none"> <li>• <b>vm.xml</b><br/>Configuration file needed for vWAAS deployment using virtual bridge or Open Virtual Switch (OVS) present in host mac.</li> </ul>                                                                                                                                                                                                                                                                    | Yes                   | No                       |
| <ul style="list-style-type: none"> <li>• <b>VM disk images</b><br/>A 4 GB flash disk, 10 GB system disk, and data disk (data disk size is dependent on your connection profile).</li> </ul>                                                                                                                                                                                                                                                                    | Yes                   | Yes                      |
| <ul style="list-style-type: none"> <li>• <b>ezdeploy.sh</b> file<br/>The script used to deploy Cisco vWAAS on Cisco UCS-E. For details on how to use this script, see <a href="#">Using the EzDeploy Script to Deploy Cisco vWAAS on RHEL KVM on Cisco UCS-E in WAAS Version 5.x to 6.2.x, page 6-6</a> and <a href="#">Using the EzDeploy Script to Deploy Cisco vWAAS on RHEL KVM on CentOS in Cisco WAAS Version 6.4.1 and Later, page 6-10</a>.</li> </ul> | Yes                   | No                       |

## Installing Cisco vWAAS on RHEL KVM in Cisco 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, page 6-5](#)
- [Using the EzDeploy Script to Deploy Cisco vWAAS on RHEL KVM on Cisco UCS-E in WAAS Version 5.x to 6.2.x, page 6-6](#)

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

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

- 
- Step 1** Launch the Cisco vWAAS VM. (You must have root permissions to 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, use this 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 Cisco vWAAS, run the **launch.sh** script:

- To check the prerequisite conditions, use the **/launch.sh check** command.
- To launch Cisco vWAAS using the OVS bridge, use the **./launch.sh vm-name bridge bridge1-name bridge2-name** command.
  - *bridge1-name* and *bridge2-name*: The OVS bridges already created in the host.



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

- To launch Cisco vWAAS using macvtap, use 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.

The Cisco vWAAS is launched.

- (Optional) To view Cisco vWAAS, use the VM GUI or the **virsh list** command.
- (Optional) To connect to the console, use the VM GUI or the **virsh console vm-name** command.
- (Optional) To power down Cisco vWAAS, use the **virsh destroy vm-name** command.
- (Optional) To undefine Cisco vWAAS:
  1. Use the **virsh undefine vm-name** command.
  2. 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 RHEL KVM on Cisco UCS-E in WAAS Version 5.x to 6.2.x

Use the EzDeploy script for simplified deployment of a Cisco vWAAS. Note that 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.

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

- 
- 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, use the **tar -zxvf Cisco-KVM-vWAAS-200-6.2.0.b-80.tar.gz** command.  
The contents of the tar.gz file are:
    - INSTRUCTIONS.TXT
    - Disk-0.qcow
    - Disk-1.qcow
    - Disk-2.qcow
    - vm\_tap.xml
    - vm\_macvtap.xml
    - launch.sh
    - ezdeploy.sh
    - ezdeploy.qstatus.exp
  - Step 5** Run the **ezdeploy.sh** script:
    - a. During execution of 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

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

- b. After input collection is completed, the following information is saved:
- The bootstrap configuration is saved in the **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. Therefore, you should 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 the **virsh list** command.
  - Optional: To connect to the console, use the VM GUI or the **virsh console vm-name** command.
  - Optional: To power down Cisco vWAAS, use the **virsh destroy vm-name** command.
  - Optional: To undefine Cisco vWAAS:
    1. Use the **virsh undefine vm-name** command.
    2. Remove the directory with the specified *vm-name*.

## Cisco vWAAS on RHEL KVM in Cisco 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, page 6-8](#)
- [Installing Cisco vWAAS on KVM in Cisco WAAS Version 6.4.1 and Later, page 6-9](#)

## 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-6.4.3c-b-42.tar
- NPE OVA: Cisco-KVM-vWAAS-Unified-6.4.3c-b-42-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 the **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 Open Virtual Switch (OVS) present in the host machine.

## Installing Cisco vWAAS on KVM in Cisco WAAS Version 6.4.1 and Later

This section contains the following topics:

- [Using the Launch Script to Deploy Cisco vWAAS on RHEL KVM on CentOS in Cisco WAAS Version 6.4.1 and Later, page 6-10](#)
- [Using the EzDeploy Script to Deploy Cisco vWAAS on RHEL KVM on CentOS in Cisco WAAS Version 6.4.1 and Later, page 6-10](#)



### 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 Cisco WAAS Version 6.4.1 and Later

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

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

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

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** Enter the number of the Cisco vWAAS or Cisco vCM model for your system.

After you select the Cisco vWAAS or Cisco 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 Cisco WAAS Version 6.4.1 and Later

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

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

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

**Step 2** The **Model Menu** is displayed:

```
--- Model Menu ---
```

1. vWAAS-150
2. vWAAS-200
3. vWAAS-750
4. vWAAS-1300
5. vWAAS-2500
6. vWAAS-6000R
7. vWAAS-6000

Select the model type :

- Step 3** Enter the number of the Cisco vWAAS model type for your system.
- After you select the Cisco vWAAS model type, the **EzDeploy** script completes the RHEL KVM/KVM on CentOS deployment.
- 

## Using the Unified OVA Package to Deploy Cisco vWAAS with Cisco NFVIS

To use the unified OVA package to deploy Cisco vWAAS on RHEL KVM on CentOS with Cisco NFVIS, follow these steps:

- Step 1** In the **Navigation** pane of the Cisco Enterprise NFVIS portal, choose **VM Life Cycle > Deploy**. The registered VM images are displayed in the **VM Deployment** window.
- Step 2** Select the Cisco vWAAS as the VM.
- Step 3** Drag and drop the Cisco vWAAS in the **Network Topology** area.
- After you select Cisco vWAAS as the VM, the Cisco vWAAS attributes and attribute choices are displayed in the **VM Details** pane.
- Step 4** Enter the following information in the **VM Details** pane:
- In the **VM Name** field, edit the Cisco vWAAS name for your system.
  - At the **Image** drop-down list, choose the unified OVA package for the Cisco vWAAS.
  - At the **Profile** drop-down list, choose the Cisco vWAAS connection profile for your system.
  - Other fields are automatically filled in by the system.
- Step 5** Connect the Cisco vWAAS to a specified network by dragging the pointed arrow from the Cisco vWAAS to the specified network.



**Note** During this process, the **VM Details** pane displays the Virtual Network Interface Card (vNIC) details: VM name, network name, and vNIC ID. The vNIC ID number is automatically generated; you can change this number, if needed, by using the **vNIC ID** drop-down list.

---

- Step 6** Click **Deploy**.
- The window is refreshed to display the deployment status.
- 

## Operating Guidelines for Cisco vWAAS on RHEL KVM/KVM on CentOS

This section contains the following topics:

- [Interoperability Guidelines for Cisco vWAAS on KVM and KVM on CentOS, page 6-12](#)
- [Traffic Interception Methods for Cisco vWAAS on RHEL KVM, page 6-13](#)

## 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 is available for vWAAS on 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 RHEL KVM

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

Consider the following guidelines when upgrading or downgrading your 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 WAAS Version 5.2.1 from an earlier version, or downgrade from WAAS Version 5.2.1 to an earlier version, and use either the **restore factory-default** command or the **restore factory-default preserve basic-config** command, the vCM-100 may not come up due to GUID Partition Table (GPT) boot order errors.



### Caution

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

To resolve this situation, follow these steps:

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

**Note**

---

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

---



## 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.

- [Cisco vWAAS on Cisco ENCS 5400-W Series, page 7-1](#)
- [Cisco vWAAS Bundled Image Install Procedure, page 7-4](#)
- [Strong Password Enforcement, page 7-7](#)
- [Shared LOM Support, page 7-8](#)
- [CLI Commands Used with Cisco vWAAS on Cisco ENCS 5400-W, page 7-9](#)
- [System Requirements for Cisco vWAAS on Cisco ENCS 5400-W with Akamai Connect, page 7-9](#)
- [Registering and Deploying Cisco vWAAS on a Cisco ENCS 5400-W Device, page 7-10](#)
- [Adding or Removing RAID-1 for Cisco ENCS 5400-W Series, page 7-12](#)
- [Fail-to-Wire on vWAAS on ENCS 5400-W, page 7-15](#)
- [Upgrade and Downgrade Guidelines for Cisco vWAAS on Cisco ENCS 5400-W, page 7-20](#)

### Cisco vWAAS on Cisco ENCS 5400-W Series

This section contains the following topics:

- [About the Cisco ENCS 5400-W and ENCS 5400 Series, page 7-1](#)
- [Cisco vWAAS as VM on Cisco ENCS 5400-W Series, page 7-2](#)
- [Cisco ENCS 5400-W Models that Replace EOL/EOS Cisco WAVE Devices, page 7-2](#)
- [Cisco ENCS 5400-W Hardware Features and Specifications, page 7-3](#)


### About the Cisco ENCS 5400-W and ENCS 5400 Series

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

For more information on Cisco NFVIS, see the chapter [“Cisco vWAAS with Cisco Enterprise NFVIS”](#).

[Table 7-1](#) 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 7-1** Cisco ENCS 5400 Series and ENCS 5400-W Series

Cisco ENCS Series	Description
Cisco ENCS 5400 Series	The Cisco ENCS 5400 Series: ENCS 5406, 5408, and 5412, is a line of compute appliances designed for the Cisco SD-Branch and Enterprise NFV solution.
Cisco ENCS 5400-W Series	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 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.
	 <p><b>Note</b> 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.</p>

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

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

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.

[Table 7-2](#) shows supported Cisco vWAAS models for Cisco ENCS 5406-W, 5408-W, and 5412-W.

**Table 7-2** 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](#).

[Table 7-3](#) 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 7-3 Cisco ENCS 5400-W Series Replacement 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	1300 connections
WAVE-694-16G	ENCS 5412-W	vWAAS-2500	2500 connections
WAVE-694-24G	ENCS 5412-W	vWAAS-6000-R	6000 connections

## Cisco ENCS 5400-W Hardware Features and Specifications

Table 7-4 shows 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 7-4 Cisco ENCS 5400-W Series Features and Specifications**

Cisco ENCS 5400 Feature/Specification	Description
Cisco vWAAS models supported	One of the following configurations: <ul style="list-style-type: none"> <li>ENCS 5406-W supports vWAAS 200, vWAAS-750</li> <li>ENCS 5408-W supports vWAAS-1300</li> <li>ENCS 5412-W supports vWAAS-2500, vWAAS-6000-R</li> </ul>
CPU	One of the following specifications: <ul style="list-style-type: none"> <li>ENCS 5406-W: Intel Xeon Processor D-1528 (6-core, 1.9-GHz, and 9-MB cache)</li> <li>ENCS-5408-W: Intel Xeon Processor D-1548 (8-core, 2.0-GHz, and 12-MB cache)</li> <li>ENCS-5412-W: Intel Xeon Processor D-1557 (12-core, 1.5-GHz, and 18-MB cache)</li> </ul>
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: <ul style="list-style-type: none"> <li>ENCS 5406-W: 16 GB</li> <li>ENCS 5408-W: 16 GB</li> <li>ENCS 5412-W: 32 GB</li> </ul>

Cisco ENCS 5400 Feature/Specification	Description
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.
SSD Storage	<ul style="list-style-type: none"> <li>No RAID and one 960-GB SSD</li> <li>RAID-1 and two SSDs (960-GB SSD)</li> </ul>  <p><b>Note</b> If you need to add or remove RAID-1 from your system, see <a href="#">Adding or Removing RAID-1 for Cisco ENCS 5400-W Series, page 7-12</a>. Note that the RAID-1 option is available for Cisco vWAAS in WAAS Version 6.4.1a and later.</p>
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, page 7-12](#). Note that the RAID-1 option is available for Cisco vWAAS in WAAS Version 6.4.1a and later.

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

- 
- Step 1** Copy the Cisco vWAAS bundled image file: An ISO file that contains the NFVIS 3.10.1 image (file format “Cisco\_NFVIS...”) and Cisco WAAS 6.4.3a image (file format “WAAS-APPLIANCE...”) on your laptop.
- For information on how to upgrade to Cisco NFVIS 3.10.1, see the section [Upgrading to Cisco Enterprise NFVIS 3.10.1 for Cisco WAAS Version 6.4.3a, page 9-9](#) 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**.

The default password is **password**.

**Step 6** Click **Login**.



**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**.

The CIMC home page is displayed.

**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.

**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.



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

**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:

```

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

```

Table 7-5 shows the installation times required, by Cisco vWAAS model and number of connections:

**Table 7-5** 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	1300	55 minutes	28 minutes	83 minutes
vWAAS-2500	2500	67 minutes	34 minutes	101 minutes
vWAAS-6000-R	6000	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**



# Strong Password Enforcement

Consider the following guidelines for administrator account passwords for different Cisco WAAS versions:

**For Cisco WAAS Version 6.4.3d and earlier:** Changing the password of the administrator account is *recommended but optional* after your initial login.

**For Cisco WAAS Version 6.4.3e and later:** Changing the password of the administrator account to a strong password is *required* after your initial login, regardless of device mode (Application Accelerator, Appnav or Central Manager).

The Cisco WAAS administrator account username is **admin** and the password is initially set to **default**.



**Note** For how to change the Cisco WAAS administrator account username and password, see the chapter “Creating and Managing Administrator User Accounts and Groups” in the [Cisco Wide Area Application Services Configuration Guide](#).



**Note** Strong password enforcement is applicable *only* to the Administrator account with the username **admin**.

Consider the following guidelines for strong password enforcement:

- After the Cisco WAAS administrator account password has been changed, it is pushed to the NFVIS **admin** user account as well, so that the WAAS and NFVIS admin users have the same password.



**Note** For the strong password enforcement to take effect for vWAAS on the Cisco ENCS 5400-W series or the Cisco CSP 5000-W series, you must do a fresh installation of Cisco WAAS 6.4.3e.

- At the first login after the fresh deployment of Cisco WAAS Version 6.4.3e or later, the default username and password are shown in the following list.  
You must change the username and password using the following parameters:
  - At least one lowercase character (a-z)
  - At least one uppercase character (A-Z)
  - At least one number (0-9)
  - At least one special character
  - A password length of 8 to 31 characters
- Before the device is registered to the Cisco WAAS Central Manager, the WAAS and NFVIS admin user will have the same password. After the device is registered to the Cisco WAAS Central Manager, the WAAS and NFVIS admin user will have the same password as the WAAS admin user.
- Changing the WAAS admin user password will also change the NFVIS admin user.
- If you run the **restore factory-default preserve basic-config** command or run the **restore factory-default** command, the WAAS admin user password is set to **default**, and you will be prompted again to change it to a strong password.

# Shared LOM Support

Cisco vWAAS running on ENCS 5400-W Series appliances with WAAS version 6.4.3e and later provides Shared LAN on Motherboard (Shared LOM) support.

The Shared LOM feature helps to re-use existing on-board Ethernet LAN interfaces on Cisco ENCS 5400-W series appliances by providing IP connectivity to Cisco Integrated Management Controller (CIMC) for remote management and health monitoring through SNMP and Syslog, while the same interfaces configured for traffic optimization



## Note

Shared LOM does not work when a **Port-channel** interface is configured on Cisco vWAAS running on ENCS 5400-W Series appliances

## Using the CIMC CLI to Enable Shared LOM Support

Consider the following guidelines for enabling Shared LOM support:

- Verify that the IP address used for the CIMC management and on-board interfaces belongs to the same VLAN or subnet.
- The **Enable/Disable** function of Shared LOM configuration should be executed from the CIMC Serial Console interface.
- The CIMC console supports a speed of 9600 only.

The following example configuration shows the steps to enable Shared LOM on Gig 0/1 interface.

```
ENCS 5000-W#
ENCS 5000-W# scope cimc/network
ENCS 5000-W /cimc/network # set mode shared_lom
ENCS 5000-W /cimc/network ## set interface value ge0/0 | ge0/1
ENCS 5000-W /cimc/network ## set interface ge0/1
ENCS 5000-W /cimc/network ## commit
```

Changes to the network settings are applied immediately.

You may lose connectivity to the CIMC and may have to log in again:

```
ENCS 5000-W /cimc/network #
```

## Using the CIMC CLI to Disable Shared LOM Support

The following example configuration shows the steps to disable Shared LOM:

```
ENCS 5000-W#
ENCS 5000-W# scope cimc/network
ENCS 5000-W /cimc/network # set mode dedicated
ENCS 5000-W /cimc/network ## commit
```

Changes to the network settings are applied immediately.


You may lose connectivity to the CIMC and may have to log in again.

```
ENCS 5000-W /cimc/network #
```

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

Table 7-6 shows the CLI commands used to display information about Cisco vWAAS on Cisco ENCS 5400-W Series.

**Table 7-6** CLI Commands Used with Cisco vWAAS on Cisco ENCS 5400-W Series

Mode	Command	Description
privileged-level EXEC	<b>copy sysreport disk</b>	Cisco ENCS 5400-W logs are part of the <b>sysreport</b> generation for debugging.
	<b>reload</b>	Halts the corresponding operation and performs a cold restart of the Cisco vWAAS VM.
	<b>show hardware</b>	Displays the following information for the specified device: <ul style="list-style-type: none"> <li>Hardware information: Manufacturer, PID, serial number, hardware version, CPU information, Memory information, and disk size.</li> <li>System information: UUID, NFVIS version, compile time, kernel version, QEMU version, LibVirt version, and OVS version.</li> </ul>
	<b>show inventory</b>	Displays system inventory information, including a description of the device, and the device's PID, chassis or slot number, version number, and serial number.
	<b>show nfvis version</b>	Displays Cisco NFVIS and BIOS version.
	<b>show version</b>	Displays the version of the Cisco <b>OE-ENCS</b> device, as well as device ID, system restart time, system restart reason, and amount of time for which system has been up.
	<b>shutdown</b>	Powers down the Cisco ENCS 5400-W host or server.
global config	<b>interface virtual</b>	<p>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 I/O) is assigned automatically by Cisco NFVIS while booting up, and cannot be modified.</p> <p> <b>Note</b> The <b>interface virtual slot/port</b> command cannot be used to configure the Cisco ENCS 5400-W internal interface.</p>

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

Table 7-7 shows memory and disk requirements for Cisco vWAAS on Cisco ENCS 5400-W with Akamai Connect, by Cisco vWAAS model.

**Table 7-7** *Memory and Disk Requirements for Cisco vWAAS on Cisco ENCS 5400-W with Akamai Connect*

Cisco vWAAS model, Number of Cisco ENCS 5400-W Connections	Memory	Data Disk	Akamai Cache
vWAAS-200, 200 ENCS 5400-W connections	12 GB	160 GB	100 GB
vWAAS-750, 750 ENCS 5400-W connections	12 GB	250 GB	250 GB
vWAAS-1300, 1300 ENCS 5400-W connections	12 GB	300 GB	300 GB
vWAAS-2500, 2500 ENCS 5400-W connections	8 GB	400 GB	350 GB
vWAAS-6000-R for Cisco WAAS versions earlier than Cisco WAAS Version 6.4.3e, 6000 ENCS 5400-W connections	11 GB	500 GB	350 GB
vWAAS-6000-R for Cisco WAAS versions 6.4.3e and later, 6000 ENCS 5400-W connections	11 GB	500 GB	335 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, page 7-10](#)
- [Deploying Cisco vWAAS with Cisco NFVIS on a Cisco ENCS 5400-W Device, page 7-11](#)
- [Registering Cisco vWAAS on a Cisco ENCS 5400-W Device with the Cisco WAAS Central Manager, page 7-12](#)

### 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.

To register Cisco vWAAS on Cisco ENCS 5400-W, follow these steps:

- 
- 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:
- Choose **Preferences > Network > Thunderbolt**.
  - From the **Configure IPv4** drop-down list, choose **Manually**.
  - In the **IP Address** field, enter an IP address.
  - In the **Subnet Mask** field, enter 255.255.255.0.
  - Open the terminal and use SSH to connect to the device (192.168.1.1). Use **admin** for login and password credentials.
- Step 5** Run the shell script (**mfg.sh**), which registers, installs, and checks the status of the vWAAS instance.
- Step 6** Exit the terminal.
- 

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

To deploy Cisco vWAAS with NFVIS on Cisco ENCS 5400-W, follow these steps:

- Step 1** Perform the steps described in [Registering Cisco vWAAS on a Cisco ENCS 5400-W Device, page 7-10](#).
- 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.
- Connect to the Cisco ENCS 5400-W device.  
The following status messages is 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
```
  - At the **Enter the image number:** prompt, enter your image number.  
The following status messages is 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 Cisco vWAAS on a Cisco ENCS 5400-W Device with the Cisco WAAS Central Manager

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

To register Cisco vWAAS with Cisco NFVIS on Cisco ENCS 5400-W with the Cisco WAAS Central Manager, these steps:

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

---

This section contains the following topics:

- [Migrating Equipment from No RAID and One SSD to RAID-1 and Two SSDs, page 7-13](#)
- [Migrating Equipment from RAID-1 and Two SSDs to No RAID and One SSD, page 7-14](#)

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

**Note**

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

**Before You Begin**

- 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:

- a. Click the **Storage** tab > **Physical Drive Info** tab.
- b. In the **Actions** area, choose **Set State as Unconfigured Good**.
- c. Confirm that the disk is in **Unconfigured Good** state.

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

- a. Click the **Storage** tab > **Controller Info** tab.
- b. In the **Actions** area, choose **Clear Foreign Config**.
- c. In the **Actions** area, choose **Unconfigured Good**.
- d. Confirm that the disk is in **Unconfigured Good** state.

To create the virtual disk, follow these steps:

- 
- Step 1** Log in to the CIMC console.
  - Step 2** In the CIMC console left pane, click the **Storage** tab.
  - Step 3** In the CIMC console middle pane, click the **Controller Info** tab.
  - Step 4** In the **Action** area, click **Create Virtual Drive from Unused Physical Drives**.  
The **Create Virtual Drive from Unused Physical Drives Wait** dialog box is displayed.
    - 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



### Note

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

---

### Before You Begin

- You must wait for the disk to be completely shut down before you physically remove the disk from the Cisco WAE device. After the RAID removal process is complete, 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 abort alarm is generated instead.

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

---

**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 vWAAS on ENCS 5400-W

This section contains the following topics:

- [About Fail-to-Wire on Cisco vWAAS on Cisco ENCS 5400-W Series, page 7-15](#)
- [Fail-to-Wire Traffic Interception Modes, page 7-15](#)
- [Fail-to-Wire Failure Handling, page 7-16](#)
- [CLI Commands for Port Channel and Standby Interfaces, page 7-16](#)
- [Configuring Inline Interception for Fail-to-Wire on a Cisco ENCS 5400-W Device, page 7-18](#)
- [Fail-to-Wire Upgrade and Downgrade Guidelines, page 7-19](#)

## About Fail-to-Wire on Cisco vWAAS on Cisco 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 Cisco 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 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 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

Here is how FTW handles the following 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, page 7-16](#)
- [Creating, Removing, and Showing Port Channel Interfaces, page 7-16](#)
- [Creating, Removing, and Showing Standby Interfaces, page 7-17](#)

### Show Commands Used with Port Channel and Standby Interfaces

**Table 7-8** *show Commands Used with Port Channel and Standby Interfaces*

show Command	Description
<b>show statistics f2w</b>	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.
<b>show interface InlineGroup</b>	Displays InlineGroup connection statistics and InlineGroup status, as well as the failover timeout frequency.
<b>show interface InlinePort LAN</b>	Displays InlinePort LAN connection statistics and specific port status of the InlineGroup.
<b>show interface InlinePort WAN</b>	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 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 portchannel** 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 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 Fail-to-Wire on a Cisco ENCS 5400-W Device

This section contains the following topics:

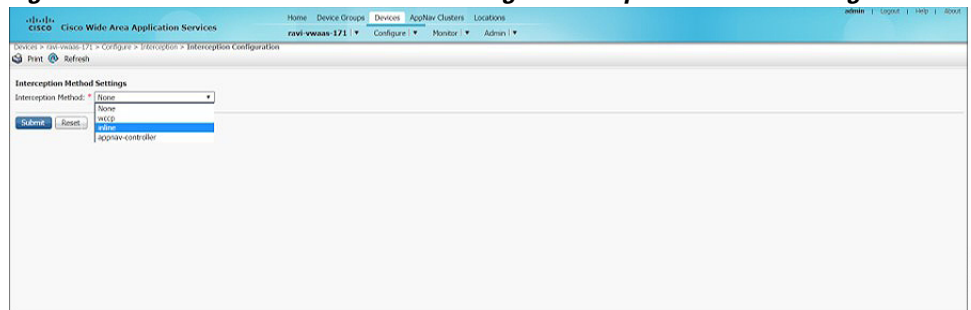
- [Configuring Inline Interception for Fail-to-Wire with the Cisco WAAS Central Manager, page 7-18](#)
- [Configuring Inline Interception for Fail-to-Wire with the Cisco WAAS CLI, page 7-19](#)

## Configuring Inline Interception for Fail-to-Wire with the Cisco WAAS Central Manager

To configure inline interception for FTW with the Cisco WAAS Central Manager, follow these steps:

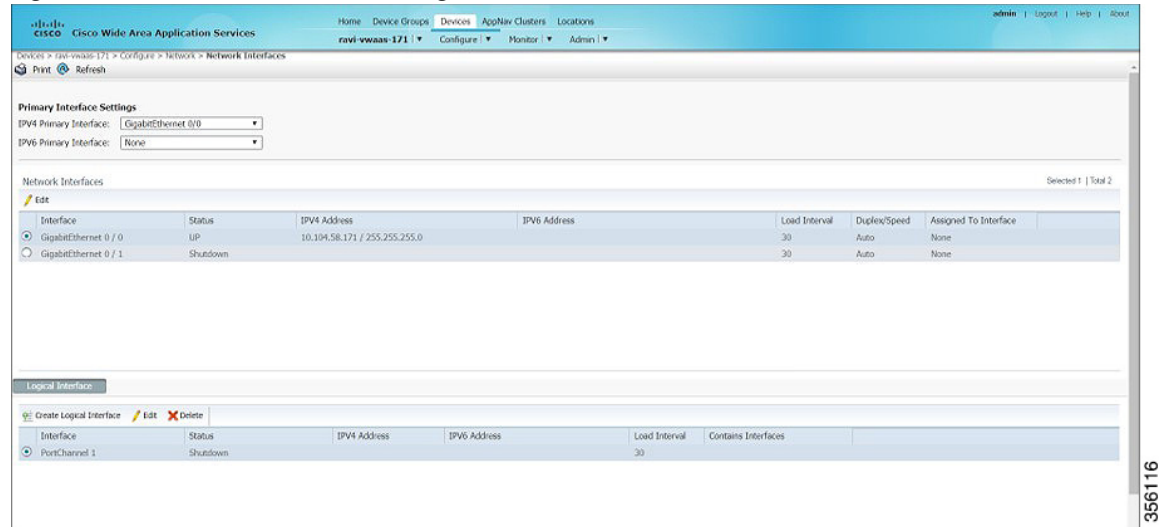
- Step 1** Choose **Devices** > *DeviceName* > **Configure** > **Interception** > **Interception Configuration** (Figure 7-1).

**Figure 7-1** Cisco WAAS Central Manager Interception Method Configuration Window



- 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 7-2).

Figure 7-2 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*.

## Configuring Inline Interception for Fail-to-Wire with the Cisco WAAS CLI

Table 7-9 shows the Cisco WAAS CLI commands used to configure inline interception for FTW on a Cisco ENCS 5400-W device.

Table 7-9 Cisco WAAS CLI Commands for Inline Interception

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

## 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 CLI to upgrade a Cisco vWAAS on a Cisco ENCS 5400-W device to the following Cisco WAAS and Cisco NFVIS versions:
  - Cisco WAAS Version 6.4.3a and Cisco NFVIS 3.10.1
  - Cisco WAAS Version 6.4.3 and Cisco NFVIS 3.9.1
  - Cisco WAAS Version 6.4.1x and Cisco NFVIS 3.71




---

**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 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 [Upgrade Guidelines for Cisco Enterprise NFVIS](#) section in the chapter “Cisco vWAAS with Cisco Enterprise NFVIS.”



## 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.

This chapter contains the following sections:

- [Cisco vWAAS on Cisco CSP 5000-W Series, page 8-1](#)
- [Cisco CSP 5000-W Hardware Features and Specifications, page 8-3](#)
- [Deploying, Registering, and Configuring Cisco vWAAS on Cisco CSP 5000-W, page 8-4](#)
- [CLI Commands Used with Cisco vWAAS on Cisco CSP 5000-W, page 8-11](#)
- [Upgrade and Downgrade Guidelines for Cisco vWAAS on Cisco CSP 5000-W, page 8-12](#)

### Cisco vWAAS on Cisco CSP 5000-W Series

This section contains the following topics:

- [About the Cisco CSP 5000-W Series, page 8-1](#)
- [Cisco CSP 5000-W Models Supported for Cisco vWAAS, page 8-2](#)
- [Cisco vWAAS on Cisco CSP 5000-W with Akamai Connect, page 8-2](#)
- [Traffic Interception Methods, page 8-3](#)

### About the Cisco CSP 5000-W Series

The Cisco Cloud Services Platform for WAAS (CSP-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.

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.

**Note**

For Cisco vWAAS in Cisco WAAS Version 6.4.3e and later, Cisco devices use the strong password enforcement feature. After initial login, you must change the default password for the Cisco WAAS administrator account, and the NFVIS administrator account for vWAAS on the ENCS 5400-W series and the CSP 5000-W series. For more information, see [Strong Password Enforcement, page 7-7](#) in the chapter “Cisco vWAAS on Cisco ENCS 5400-W Series.”

## Cisco CSP 5000-W Models Supported for Cisco vWAAS

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

These Cisco CSP 5000-W models replace three End-of-Sale and End-of-Life (EOS and EOL) Cisco WAVE models. [Table 8-1](#) 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.

**Table 8-1** Cisco CSP 5000-W and 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

For more information on the EOS and EOL Cisco WAVE models, see the [End-of-Sale and End-of-Life Announcement for the Cisco WAVE 294, 594, 694, 7541, 7571 and 8541](#).

**Note**

There is no Product Returns and Replacement (RMA) process for Cisco CSP 5000-W devices or EOS and EOL Cisco WAVE devices.

## 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:

- As shown in [Table 8-2](#), a fourth disk is required for Cisco vWAAS on Cisco CSP 5000-W with Akamai Connect caching.
- Cisco CSP 5000-W devices have fixed resources. Therefore the memory on each device remains the same with or without Akamai Connect enabled.



**Table 8-2** System Requirements for Cisco vWAAS on Cisco CSP 5000-W with Akamai Connect

Cisco CSP 5000-W Model	Supported Cisco vWAAS Model	Memory Requirement		Fourth Disk Requirement When Akamai is Enabled
		Without Akamai	Without Akamai	
CSP 5228-W	vWAAS-12000	18 GB	18 GB	750 GB
CSP 5228-W	vWAAS-50000	48 GB	48 GB	850 GB
CSP 5436-W	vWAAS-150000	96 GB	96 GB	1500 GB

## Traffic Interception Methods

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.

## Cisco CSP 5000-W Hardware Features and Specifications

[Table 8-3](#) shows the specifications for each Cisco CSP 5000-W model used with Cisco vWAAS.

Note the following details about these three Cisco CSP 5000-W models:

- 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.

Table 8-3 Specifications for Cisco CSP 5000-W Models Used with Cisco vWAAS

Cisco CSP 5228-W for Cisco vWAAS 12000							
CPU	CPU Speed	Connections	Memory	Storage	Network Interface Card	RAID	Hardware Platform
16 core	2.2 GHz	12,000	52 GB	1.5 TB	<i>PCIe Slot 1</i> —Intel X520-DA2 10-Gbps 2-port NIC (2x10-GB fiber interfaces)  <i>PCIe Slot 2</i> —Intel i350 Quad Port 1-GB Adapter	Cisco 12-G Modular RAID controller with 2-GB cache  RAID 10	Cisco UCS-220-M5
Cisco CSP 5228-W for Cisco vWAAS 50000							
CPU	CPU Speed	Connections	Memory	Storage	Network Interface Card	RAID	Hardware Platform
20 core	2.2 GHz	50,000	76 GB	2.3 TB	<i>PCIe Slot 1</i> —Intel X520-DA2 10-Gbps 2-port NIC (2x10 GB fiber interfaces)  <i>PCIe Slot 2</i> —Intel i350 Quad Port 1-GB Adapter	Cisco 12-G Modular RAID controller with 2-GB cache  RAID 10	Cisco UCS-220-M5
Cisco CSP 5436-W for Cisco vWAAS-15000							
CPU	CPU Speed	Connections	Memory	Storage	Network Interface Card	RAID	Hardware Platform
28 core	3.0 GHz	150,000	100 GB	4.5 TB	<i>PCIe Slot 1</i> —Intel X520-DA2 10-Gbps 2 port NIC (2x10-GB Fiber interfaces)  <i>PCIe Slot 4</i> —Intel i350 Quad Port 1-GB Adapter	Cisco 12-G Modular RAID controller with 2GB cache  RAID 10	Cisco UCS-240-M5

For more information on RAID configuration, see the [Cisco UCS Servers RAID Guide](#).

## 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, page 8-5](#)
- [Installing Cisco vWAAS on a Cisco CSP 5000-W Device, page 8-5](#)
- [Configuring a Port Channel and Standby Interface, page 8-5](#)

- [Registering or Deregistering a Cisco CSP 5000-W Device with the Cisco WAAS Central Manager, page 8-9](#)

## Workflow for Deploying, Registering, and Configuring Cisco vWAAS on Cisco CSP 5000-W

Task	Section or Description
1. Install the Cisco vWAAS on Cisco CSP 5000-W	• <a href="#">Installing Cisco vWAAS on a Cisco CSP 5000-W Device, page 8-5</a>
2. Register the Cisco CSP 5000-W device with the Cisco WAAS Central Manager	• <a href="#">Registering or Deregistering a Cisco CSP 5000-W Device with the Cisco WAAS Central Manager, page 8-9</a>
3. Enable Akamai Connect	• <a href="#">“Cisco vWAAS with Akamai Connect”</a> .
4. Check accelerator status	• To confirm that operational status of accelerators is <b>Running</b> , use the <b>show accelerator EXEC</b> command.
5. Configure WCCP traffic interception	• The “Configuring Traffic Interception” chapter of the <i>Cisco Wide Area Application Services Configuration Guide</i> .
6. Configure port channel support	• <a href="#">Configuring a Port Channel and Standby Interface, page 8-5</a>

## 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, perform the following tasks:

- Use the following **show** 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 a Port Channel and Standby Interface

This section contains the following topics:

- [Configuring a Port Channel Interface, page 8-6](#)
- [Configuring a Standby Interface, page 8-8](#)

## 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, use 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
```

Figure 8-1 shows an annotated output for the **show running-config interface** command:

**Figure 8-1 Cisco WAAS CLI show running-config Annotated Output**

NO-HOSTNAME#show running-config interface		
interface Virtual 1/0		
ip address 1.1.1.1 255.255.255.0		
exit		
interface Virtual 2/0	Onboard 10G	These are the
ip address 2.2.2.2 255.255.255.0	interfaces (X550)	onboard interfaces.
exit		
interface Virtual 3/0		
ip address 3.3.3.3 255.255.255.0		
exit		
interface Virtual 3/1	10G interfaces in	This card goes in PCI
ip address 4.4.4.4 255.255.255.0	PCI slot (X520)	Slot 1 for both CSP-
exit		5228 and CSP-5436
interface Virtual 4/0		
ip address 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-
interface Virtual 4/2		5436.
ip address 7.7.7.7 255.255.255.0		
exit		

356112

- 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#

```

## Configuring a Standby Interface

You can create two port channel groups and use them as the active and backup members of a standby group. 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#

```

- To configure an interface to be a standby for another interface, use the **(config-if) standby** command:

```

CSP-APPLIANCE# configure
CSP-APPLIANCE# interface standby 1
CSP-APPLIANCE(config-if)#

```

## 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, page 8-10](#)
- [Deregistering a Cisco CSP 5000-W Device, page 8-11](#)

## Registering a Cisco CSP 5000-W Device with the Cisco WAAS Central Manager

To register a Cisco WAAS device or Cisco vWAAS device with the WAAS Central Manager, follow these steps:

- 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** Use the **cms** command to register the Cisco CSP 5000-W device:

```
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** Use the **copy running-config startup-config** command to preserve the running configuration.



**Note** If you do not use 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 8-2).

**Figure 8-2 Cisco OE-CSP Displayed in the WAAS Central Manager Device Listings Window**

Device Name	Service	IP Address	Management Status	Device Status	Location	Software Version	Device Type	Max Connections	License Type	License Status	Maximal Contract
BR-CSPW-12K	Application Accelerator	2.75.2.39	Offline	Offline	BR-CSPW-12K-location	6.4.3	OE-CSP	12000	Perpetual	Enterprise	Not Active
CN	CN (Primary)	2.78.18.69	Online	Online		6.4.3	OE294	N/A	Perpetual	Enterprise	Not Supported
Dagger-4325-ISR-WAAS	Application Accelerator	2.69.89.194	Online	Online	Dagger-4325-ISR-WAAS-location	5.5.7b	ISR-WAAS	200	Perpetual	Enterprise	Not Active
DC-WAE	Application Accelerator	2.78.18.23	Online	Online	DC-WAE-location	5.5.7b	OE294	200	Perpetual	Enterprise	Not Active

- 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

To deregister a Cisco CSP 5000-W device, follow these steps.

- 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** Click **yes** to initiate the deregistering process. 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** Use the **copy running-config startup-config** command to preserve the running configuration.



**Note** If you do not use 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

Table 8-4 shows the CLI commands used with Cisco vWAAS on Cisco CSP 5000-W.

**Table 8-4** CLI Commands used with Cisco vWAAS on Cisco CSP 5000-W

Mode	Command	Description
Global Configuration	<b>(config) interface PortChannel</b>	Configures a port-channel interface.
Interface Configuration	<b>(config-if) channel-group</b>	Configures the port channel group for a network interface.
privileged-level EXEC	<b>copy sysreport disk</b>	Cisco CSP 5000-W logs will be part of the <b>sysreport</b> generation for debugging.
	<b>reload</b>	Restarts the Cisco vWAAS VM.
	<b>show hardware</b>	Validates the CPU and memory depending on the Cisco vWAAS model.
	<b>show inventory</b>	Validates the PID depending on the Cisco vWAAS model.
	<b>show running-config interface</b>	Displays a Cisco WAAS device current running configuration on the terminal,
user-level EXEC and privileged-level EXEC	<b>show tfo detail</b>	Verifies the number of TFO connections depending on the Cisco vWAAS model.
	<b>show version</b>	Verifies that the Cisco WAAS version is Cisco WAAS Version 6.4.3a or later.
privileged-level EXEC	<b>shutdown</b>	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.
  - Downgrade is not supported for Cisco vWAAS for Cisco WAAS versions earlier than Cisco WAAS 6.4.3a.
  - 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.



### 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, [Upgrade Guidelines for Cisco Enterprise NFVIS](#) in the chapter “Cisco vWAAS with Cisco Enterprise NFVIS,



## Cisco vWAAS with Cisco Enterprise NFVIS

---

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

- [Cisco Enterprise NFVIS, page 9-1](#)
- [Cisco vWAAS with Cisco Enterprise NFVIS, page 9-2](#)
- [Unified OVA Package for Cisco vWAAS with Cisco Enterprise NFVIS in Cisco WAAS Version 6.4.1 and Later, page 9-3](#)
- [Firmware Upgrade for Cisco Enterprise NFVIS, page 9-5](#)
- [Traffic Interception for Cisco vWAAS with Cisco Enterprise NFVIS, page 9-6](#)
- [Upgrade Guidelines for Cisco Enterprise NFVIS, page 9-8](#)

### Cisco Enterprise NFVIS

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

Cisco Enterprise NFVIS contains the following features:

- Cisco vWAAS with Cisco Enterprise NFVIS is deployed on the 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 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.

# Cisco vWAAS with Cisco Enterprise NFVIS

This section contains the following topics:

- [About Cisco vWAAS with Cisco Enterprise NFVIS, page 9-2](#)
- [Operating Guidelines for Cisco vWAAS with Cisco Enterprise NFVIS, page 9-2](#)
- [Platforms and Software Versions Supported for Cisco vWAAS with Cisco Enterprise NFVIS, page 9-2](#)

## About Cisco vWAAS with Cisco Enterprise NFVIS

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.

## Operating Guidelines for Cisco vWAAS with Cisco Enterprise NFVIS

For guaranteed performance, the Cisco ENCS 5400-W Series, Cisco UCS-C Series, Cisco UCS-E Series, Cisco ENCS 5100, Cisco CSP-2100, and Cisco ISR configurations 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.

**Caution**

---

Although Cisco vWAAS models may be able to operate with other Cisco or third-party hardware, successful performance and scale for those configurations is not guaranteed.

---

For more information about supported platforms for Cisco Enterprise NFV, see the [Release Notes for Cisco Enterprise Network Function Virtualization Infrastructure Software, Release 3.11.x](#).

## Platforms and Software Versions Supported for Cisco vWAAS with Cisco Enterprise NFVIS

[Table 9-1](#) shows the platforms and software versions supported for Cisco vWAAS with Cisco Enterprise NFVIS.

**Table 9-1 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
<ul style="list-style-type: none"> <li>• PID: OE-VWAAS-ENCS</li> <li>• Device Type: OE-VWAAS-ENCS</li> </ul>	<ul style="list-style-type: none"> <li>• 6.4.1</li> </ul>	<ul style="list-style-type: none"> <li>• Cisco ENCS 5400-W Series</li> </ul>	<ul style="list-style-type: none"> <li>• Cisco Enterprise NFVIS 3.7.1</li> </ul>	<ul style="list-style-type: none"> <li>• virtio</li> </ul>
<ul style="list-style-type: none"> <li>• PID: OE-VWAAS-KVM</li> <li>• Device Type: OE-VWAAS-KVM</li> </ul>	<ul style="list-style-type: none"> <li>• 6.2.x</li> </ul>	<ul style="list-style-type: none"> <li>• Cisco UCS-E Series</li> </ul>	<ul style="list-style-type: none"> <li>• Cisco Enterprise NFVIS 3.7.1</li> </ul>	<ul style="list-style-type: none"> <li>• virtio</li> </ul>

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. For more information on Cisco Enterprise NFVIS and Cisco NFV, see the [Cisco Intelligent WAN - An SD-WAN Solution](#).

## Unified OVA Package for Cisco vWAAS with Cisco Enterprise NFVIS in Cisco WAAS Version 6.4.1 and Later

This section contains the following topics:

- [About the Unified OVA Package for Cisco vWAAS with Cisco Enterprise NFVIS in Cisco WAAS Version 6.4.1 and Later, page 9-4](#)
- [Operating Guidelines for the Unified OVA Package Cisco vWAAS with Cisco Enterprise NFVIS in Cisco WAAS Version 6.4.1 and Later, page 9-4](#)

## About the Unified OVA Package for Cisco vWAAS with Cisco Enterprise NFVIS in 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.

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

- OVA: **Cisco-KVM-vWAAS-Unified-6.4.3c-b-42.tar**
- NPE OVA: **Cisco-KVM-vWAAS-Unified-6.4.3c-b-42-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 using 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 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 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 Cisco vWAAS with Cisco Enterprise NFVIS in Cisco WAAS Version 6.4.1 and Later

The Cisco ENCS 5400-W Series, Cisco UCS-C Series, Cisco UCS-E Series, Cisco ENCS 5100, Cisco CSP-2100, and Cisco ISR configurations listed in the Cisco WAAS Sizing Guides and specifically noted in Cisco WAAS and Cisco vWAAS user guides and Cisco WAAS Release Notes are the only devices we recommend for use with Cisco vWAAS.

**Caution**

Although Cisco vWAAS models may be able to operate with other Cisco or third-party hardware, successful performance and scale for those configurations is not guaranteed.

For more information about supported platforms for Cisco Enterprise NFV, see the [Release Notes for Cisco Enterprise Network Function Virtualization Infrastructure Software](#).

## Firmware Upgrade for Cisco Enterprise NFVIS

To upgrade the Complex Programmable Logic Device (CPLD) and the Field Programmable Gate Array (FPGA) for Cisco Enterprise NFVIS to the latest version, follow these steps:

**Step 1** Ensure that your system is running the following:

- Cisco WAAS Version 6.4.3b
- Cisco Enterprise NFVIS 3.11.1

**Step 2** Download the Cisco WAAS Firmware image for ENCS-W Appliance from the [Cisco Wide Area Application Services \(WAAS\) Software 6.4.3x Download Page](#).

**Step 3** To upgrade the FPGA, use 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
```

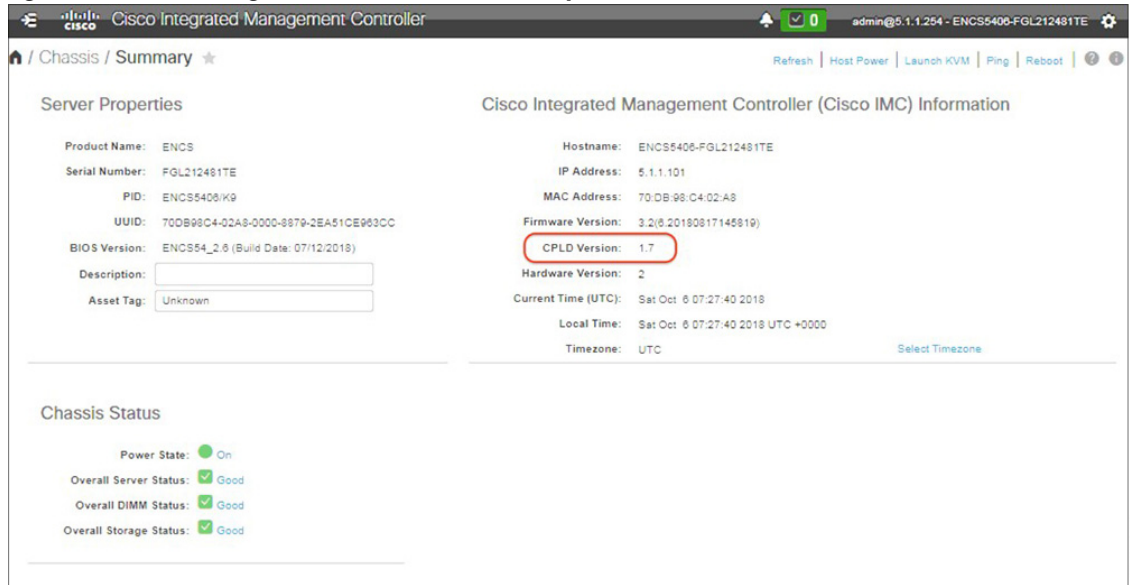


**Note** After you upgrade the firmware package, you must power-cycle the entire chassis to ensure that the FPGA takes effect.

**Step 4** To verify the CPLD and FPGA version, use the CIMC GUI or the CLI.

- To verify the CPLD and FPGA version from the CIMC GUI, choose **Chassis > Summary** ([Figure 9-1](#)).

Figure 9-1 Using the CIMC Console to Verify CPLD/FPGA Version



- To verify the CPLD and FPGA version from the CIMC CLI, use the following command:

```
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
```

## Traffic Interception for Cisco vWAAS with Cisco Enterprise 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 detailed information on configuring WCCP, see the chapter “Configuring Traffic Interception” in the [Cisco Wide Area Application Services Configuration Guide](#).

Table 9-2 shows the CLI commands used to configure WCCP traffic interception for Cisco vWAAS with Cisco Enterprise NFVIS.

**Table 9-2 CLI Commands for WCCP Interception Mode**

Mode	Command	Description
Global configuration	<b>interception method wccp</b>	Configures the WCCP traffic interception method.
	<b>wccp access-list</b>	Configures an IP access list on a WAE for inbound WCCP GRE-encapsulated traffic.
	<b>wccp flow-redirect</b>	Redirects moved flows.
	<b>wccp router-list</b>	Configures a router list for WCCP Version 2.
	<b>wccp shutdown</b>	Sets the maximum time interval after which the WAE will perform a clean shutdown of the WCCP.
	<b>wccp tcp-promiscuous</b>	Configures the WCCP Version 2 TCP promiscuous mode service.
	<b>wccp tcp-promiscuous service-pair <i>serviceID serviceID+1</i></b>	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.
user-level EXEC and privileged-level EXEC	<b>show statistics wccp</b>	Displays WCCP statistics for a WAE.
	<b>show wccp clients</b>	Displays which WAEs are seen by which routers.
	<b>show wccp egress</b>	Displays the WCCP egress method—IP forwarding, generic GRE, WCCP GRE, or L2.
	<b>show wccp flows tcp-promiscuous summary</b>	Displays WCCP packet flows and TCP-promiscuous service information.
	<b>show wccp masks tcp promiscuous</b>	Displays WCCP mask assignments and TCP-promiscuous service information.
	<b>show wccp routers [detail]</b>	Displays details of routers seen and not seen by the specified WAE.
	<b>show wccp services [detail]</b>	Displays the configured WCCP services.
	<b>show wccp statistics</b>	Displays WCCP generic routing encapsulation packet-related information.
	<b>show wccp status</b>	Displays the enabled state of WCCP and the configured service IDs.

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

# Upgrade Guidelines for Cisco Enterprise NFVIS

This section contains the following topics:

- [Upgrading to Cisco Enterprise NFVIS 3.9.1 for Cisco WAAS Version 6.4.3, page 9-8](#)
- [Upgrading to Cisco Enterprise NFVIS 3.10.1 for Cisco WAAS Version 6.4.3a, page 9-9](#)
- [Upgrading to Cisco Enterprise NFVIS 3.11.1 for Cisco WAAS Version 6.4.3b, page 9-10](#)

## Upgrading to Cisco Enterprise NFVIS 3.9.1 for Cisco WAAS Version 6.4.3

Cisco Enterprise NFVIS 3.9.1 is supported for Cisco vWAAS in Cisco WAAS Version 6.4.3.

- This section provides general guidelines. For detailed upgrade information:
  - For the full procedure to upgrade to Cisco Enterprise NFVIS 3.9.1, see the chapter [Upgrading Cisco Enterprise NFVIS](#) in the *Cisco Enterprise Network Function Virtualization Infrastructure Software Configuration Guide, Release 3.9.1*.
  - For more information on Cisco Enterprise NFVIS upgrade procedures and Cisco Enterprise NFVIS image files, see the [Cisco Enterprise NFVIS Configuration Guides Page](#)
- If you are running **nfvis-371-waas-641a** or **nfvis-371-waas-641b** on a Cisco ENCS 5400-W device, before upgrading Cisco Enterprise NFVIS, upgrade to Cisco WAAS Version 6.4.3. For more information on Cisco Enterprise NFVIS and ENCS 5400-W devices, see the section [Upgrade and Downgrade Guidelines for Cisco vWAAS on Cisco ENCS 5400-W](#) in the chapter “Cisco vWAAS on Cisco ENCS 5400-W Series,”
- [Table 9-3](#) shows the supported upgrade paths for Cisco Enterprise NFVIS 3.9.1.

**Table 9-3 Upgrade Paths for Cisco Enterprise NFVIS 3.9.1**

Current Cisco Enterprise NFVIS Version	Cisco Enterprise NFVIS Upgrade Path
3.7.1	<ol style="list-style-type: none"> <li>1. Upgrade to Cisco Enterprise NFVIS 3.8.1</li> <li>2. Upgrade to Cisco Enterprise NFVIS 3.9.1</li> </ol>
3.8.1	Upgrade directly to Cisco Enterprise NFVIS 3.9.1

- After you upgrade your system from an earlier to a later version of Cisco Enterprise NFVIS, the newly upgraded Cisco Enterprise NFVIS version automatically upgrades BIOS and CIMC for the Cisco ENCS 5400-W platform. [Table 9-4](#) shows the Cisco Enterprise NFVIS 3.9.1 automatic BIOS and CIMC upgrades for the Cisco ENCS 5400-W series.

**Table 9-4 Cisco Enterprise NFVIS 3.9.1 Automatic CIMC and BIOS Upgrades for Cisco ENCS 5400-W**

Cisco Enterprise NFVIS Upgrade	Automatic Upgrade for BIOS for Cisco ENCS 5400-W	Automatic Upgrade for CIMC for Cisco ENCS 5400-W
From Cisco Enterprise NFVIS 3.7.1 to Version 3.8.1	Upgraded to BIOS 2.5	Upgraded to CIMC 3.2.4
From Cisco Enterprise NFVIS 3.8.1 to Version 3.9.1	Upgraded to BIOS 2.6	Upgraded to CIMC 3.2.6



**Note** Each upgrade may take about 90 minutes. Do not interrupt the upgrade process.

## Upgrading to Cisco Enterprise NFVIS 3.10.1 for Cisco WAAS Version 6.4.3a

Cisco Enterprise NFVIS 3.10.1 is supported for Cisco vWAAS in Cisco WAAS Version 6.4.3a.

- This section provides general guidelines. For detailed upgrade information:
  - For the procedure to upgrade to Cisco Enterprise NFVIS 3.10.1, see the chapter [Upgrading Cisco Enterprise NFVIS](#) in the *Cisco Enterprise Network Function Virtualization Infrastructure Software Configuration Guide, Release 3.10.1*.
  - For more information on Cisco Enterprise NFVIS upgrade procedures and Cisco Enterprise NFVIS image files, see the [Cisco Enterprise NFVIS Configuration Guides Page](#).
- If you are running **nfvis-371-waas-641a** or **nfvis-371-waas-641b** on a Cisco ENCS 5400-W device: Before upgrading Cisco Enterprise NFVIS, upgrade to Cisco WAAS Version 6.4.3. For more information on Cisco Enterprise NFVIS and Cisco ENCS 5400-W devices, see the section [Upgrade and Downgrade Guidelines for Cisco vWAAS on Cisco ENCS 5400-W](#) in the chapter “Cisco vWAAS on Cisco ENCS 5400-W Series,”
- [Table 9-5](#) shows the supported upgrade paths for Cisco Enterprise NFVIS 3.10.1.

**Table 9-5 Upgrade Paths for Cisco Enterprise NFVIS 3.10.1**

Current Cisco Enterprise NFVIS Version	Cisco Enterprise NFVIS Upgrade Path
3.7.1	<ol style="list-style-type: none"> <li>1. Upgrade to Cisco Enterprise NFVIS 3.8.1</li> <li>2. Upgrade to Cisco Enterprise NFVIS 3.10.1</li> </ol>
3.8.1	Upgrade directly to Cisco Enterprise NFVIS 3.10.1
3.9.1	Upgrade directly to Cisco Enterprise NFVIS 3.10.1

- After you upgrade your system from an earlier to a later version of Cisco Enterprise NFVIS, the newly upgraded Cisco Enterprise NFVIS version automatically upgrades BIOS and CIMC for the Cisco ENCS 5400-W platform. [Table 9-6](#) shows the Cisco Enterprise NFVIS 3.10.1 automatic BIOS and CIMC upgrades for the Cisco ENCS 5400-W series.

**Table 9-6 Cisco Enterprise NFVIS 3.10.1 Automatic CIMC and BIOS Upgrades for Cisco ENCS 5400-W**

Cisco Enterprise NFVIS Upgrade	Automatic Upgrade for BIOS for Cisco ENCS 5400-W	Automatic Upgrade for CIMC for Cisco ENCS 5400-W
From Cisco Enterprise NFVIS 3.7.1 to Version 3.8.1	Upgraded to BIOS 2.5	Upgraded to CIMC 3.2.4
From Cisco Enterprise NFVIS 3.8.1 to Version 3.9.1	Upgraded to BIOS 2.6	Upgraded to CIMC 3.2.6
From Cisco Enterprise NFVIS 3.9.1 to Version 3.10.1	Upgraded to BIOS 2.6	Upgraded to CIMC 3.2.6



**Note** Each upgrade may take about 90 minutes. Do not interrupt the upgrade process.

## Upgrading to Cisco Enterprise NFVIS 3.11.1 for Cisco WAAS Version 6.4.3b

Cisco Enterprise NFVIS 3.11.1 is supported for Cisco vWAAS in Cisco WAAS Version 6.4.3b.

- This section provides general guidelines. For detailed upgrade information:
  - For the procedure to upgrade to Cisco Enterprise NFVIS 3.11.1, see the chapter “[Upgrading Cisco Enterprise NFVIS](#)” in the *Cisco Enterprise Network Function Virtualization Infrastructure Software Configuration Guide, Release 3.11.1*.
  - For more information on Cisco Enterprise NFVIS upgrade procedures and Cisco Enterprise NFVIS image files, see the [Cisco Enterprise NFVIS Configuration Guides page](#)
- If you are running **nfvis-371-waas-641a** or **nfvis-371-waas-641b** on a Cisco ENCS 5400-W device: Before upgrading Cisco Enterprise NFVIS, upgrade to Cisco WAAS Version 6.4.3. For more information on Cisco Enterprise NFVIS and Cisco ENCS 5400-W devices, see the section [Upgrade and Downgrade Guidelines for Cisco vWAAS on Cisco ENCS 5400-W](#) in the chapter “Cisco vWAAS on Cisco ENCS 5400-W Series.”
- [Table 9-7](#) shows the supported upgrade paths for Cisco Enterprise NFVIS 3.11.1.

**Table 9-7 Upgrade Paths for Cisco Enterprise NFVIS 3.11.1**

Current Cisco Enterprise NFVIS Version	Cisco Enterprise NFVIS Upgrade Path
3.7.1	<ol style="list-style-type: none"> <li>1. Upgrade to Cisco Enterprise NFVIS 3.8.1</li> <li>2. Upgrade to Cisco Enterprise NFVIS 3.10.1</li> </ol>
3.8.1	<ol style="list-style-type: none"> <li>1. Upgrade to Cisco Enterprise NFVIS 3.10.1</li> <li>2. Upgrade to Cisco Enterprise NFVIS 3.11.1</li> </ol>
3.9.1	Upgrade directly to Cisco Enterprise NFVIS 3.11.1
3.10.1	Upgrade directly to Cisco Enterprise NFVIS 3.11.1

- After you upgrade your system from an earlier to a later version of Cisco Enterprise NFVIS, the newly upgraded Cisco Enterprise NFVIS version automatically upgrades BIOS and CIMC for the Cisco ENCS 5400-W platform. [Table 9-8](#) shows the NFVIS 3.11.1 automatic BIOS and CIMC upgrades for the Cisco ENCS 5400-W series.

**Table 9-8 Cisco Enterprise NFVIS 3.11.1 Automatic CIMC and BIOS Upgrades for Cisco ENCS 5400-W**

Cisco Enterprise NFVIS Upgrade	Automatic Upgrade for BIOS for Cisco ENCS 5400-W	Automatic Upgrade for CIMC for Cisco ENCS 5400-W
From Cisco Enterprise NFVIS 3.7.1 to Version 3.8.1	Upgraded to BIOS 2.5	Upgraded to CIMC 3.2.4
From Cisco Enterprise NFVIS 3.8.1 to Version 3.9.1	Upgraded to BIOS 2.6	Upgraded to CIMC 3.2.6

<b>Cisco Enterprise NFVIS Upgrade</b>	<b>Automatic Upgrade for BIOS for Cisco ENCS 5400-W</b>	<b>Automatic Upgrade for CIMC for Cisco ENCS 5400-W</b>
From Cisco Enterprise NFVIS 3.9.1 to Version 3.10.1	Upgraded to BIOS 2.6	Upgraded to CIMC 3.2.6
From Cisco Enterprise NFVIS 3.10.1 to Version 3.11.1	Upgraded to BIOS 2.7	Upgraded to CIMC 3.2.7

**Note**

Each upgrade may take about 90 minutes. Do not interrupt the upgrade process.





## 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, page 10-1](#)
- [Supported Platforms for Cisco vWAAS with Akamai Connect, page 10-2](#)
- [Cisco vWAAS with Akamai Connect License, page 10-3](#)
- [Cisco vWAAS with Akamai Connect Hardware Requirements, page 10-3](#)
- [Upgrading Cisco vWAAS Memory and Disk for Akamai Connect, page 10-4](#)
- [Cisco vWAAS-150 with Akamai Connect, page 10-8](#)
- [Akamai Connect Cache Engine on Cisco Mid-End and High-End Platforms, page 10-9](#)

### 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

Table 10-1 shows supported platforms for Cisco vWAAS with Akamai Connect, up to 6,000 connections

**Table 10-1 Supported Cisco Devices for Akamai Caching, Up to 6,000 Connections**

Cisco vWAAS	Cisco ISR-WAAS	Cisco WAVE	Cisco SRE-SM (for Cisco vWAAS in WAAS Version 6.2.x and earlier)
vWAAS-150 (for Cisco vWAAS in Cisco WAAS Version 6.1.1 and later)	<ul style="list-style-type: none"> <li>ISR-G2</li> <li>ISR-G3</li> </ul>	<ul style="list-style-type: none"> <li>N/A</li> </ul>	<ul style="list-style-type: none"> <li>N/A</li> </ul>
vWAAS-200	<ul style="list-style-type: none"> <li>ISR-WAAS-750 (ISR-4451, ISR-4431, ISR-4351, ISR-4331, ISR-4321)</li> </ul>	<ul style="list-style-type: none"> <li>WAVE-294</li> </ul>	<ul style="list-style-type: none"> <li>SRE-SM-700</li> </ul>
vWAAS-750	<ul style="list-style-type: none"> <li>ISR-WAAS-1300 (ISR-4451, ISR-4431)</li> </ul>	<ul style="list-style-type: none"> <li>WAVE-594</li> </ul>	<ul style="list-style-type: none"> <li>SRE-SM-900</li> </ul>
vWAAS-1300	<ul style="list-style-type: none"> <li>ISR-WAAS-2500 (ISR-4451)</li> </ul>	<ul style="list-style-type: none"> <li>WAVE-694</li> </ul>	<ul style="list-style-type: none"> <li>SRE-SM-710</li> </ul>
vWAAS-2500	<ul style="list-style-type: none"> <li>N/A</li> </ul>	<ul style="list-style-type: none"> <li>N/A</li> </ul>	<ul style="list-style-type: none"> <li>SRE-SM-910</li> </ul>
vWAAS-6000	<ul style="list-style-type: none"> <li>N/A</li> </ul>	<ul style="list-style-type: none"> <li>N/A</li> </ul>	<ul style="list-style-type: none"> <li>N/A</li> </ul>

Table 10-2 shows supported platforms for Cisco vWAAS with Akamai Connect, beyond 6,000 connections

**Table 10-2 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.

Table 10-3 lists the standalone licenses for Cisco iWAN with Akamai Connect and vWAAS. For information on all licenses for Cisco iWAN with Akamai Connect, see the [Cisco Intelligent WAN with Akamai Connect Data Sheet](#).



### Note

The actual number of connections for each Cisco iWAN with Akamai Connect License shown in Table 10-3 is dependent on the hardware module on which WAAS is running.

**Table 10-3 Licenses for Cisco iWAN with Akamai Connect with vWAAS**

Cisco iWAN with Akamai Connect License	License Description	Supported Platforms (vWAAS platforms in bold font)
SL-1300-AKC	Akamai Connect license for up to 1300 Cisco WAAS connections	<ul style="list-style-type: none"> <li>ISR-2900 or ISR-3900 and one of the following:               <ul style="list-style-type: none"> <li><b>vWAAS-1300 or lower (UCS-E)</b></li> </ul> </li> <li>ISR-4451, ISR-4431, ISR-4351, or ISR-4331:               <ul style="list-style-type: none"> <li><b>vWAAS-2500 or lower</b></li> </ul> </li> <li>UCS server:               <ul style="list-style-type: none"> <li><b>vWAAS-1300 or lower</b></li> </ul> </li> <li>WAVE-594</li> </ul>
SL-2500-AKC	Akamai Connect license for up to 2500 Cisco WAAS connections	<ul style="list-style-type: none"> <li>ISR-2900 or ISR-3900 and one of the following:               <ul style="list-style-type: none"> <li><b>vWAAS-2500 or lower (UCS-E)</b></li> </ul> </li> <li>ISR-4451:               <ul style="list-style-type: none"> <li><b>vWAAS-2500 or lower</b></li> </ul> </li> <li>UCS server:               <ul style="list-style-type: none"> <li><b>vWAAS-2500 or lower</b></li> </ul> </li> <li>WAVE-694</li> </ul>
SL-6000-AKC	Akamai Connect license for up to 6000 Cisco WAAS connections	<ul style="list-style-type: none"> <li>ISR-2900/ISR-3900 and one of the following:               <ul style="list-style-type: none"> <li><b>vWAAS-6000 or lower (UCS-E)</b></li> </ul> </li> <li>UCS server:               <ul style="list-style-type: none"> <li><b>vWAAS-6000 or lower</b></li> </ul> </li> <li>WAVE-694</li> </ul>

## Cisco vWAAS with Akamai Connect Hardware Requirements

Table 10-4 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 Cisco vWAAS with Akamai Connect on Hyper-V, see [Configuring GPT Disk Format for Cisco vWAAS-50000 on Microsoft Hyper-V with Akamai Connect](#) in the chapter “Cisco vWAAS on Microsoft Hyper-V”.

**Table 10-4** Hardware Requirements for Cisco vWAAS with Akamai Connect

Cisco vWAAS or Cisco WAAS Model	Memory Required for Cisco vWAAS with Akamai Connect	Disk Required for Cisco vWAAS with Akamai Connect
vWAAS-150	4 GB	160 GB
vWAAS-200	4 GB	260 GB
vWAAS-750	4 GB	500 GB
vWAAS-1300	6 GB	600 GB
vWAAS-2500	8 GB	750 GB
vWAAS-6000	11 GB	900 GB
vWAAS-12000	18 GB	1500 GB
vWAAS-50000	48 GB	2350 GB
ISR-WAAS-200	2 GB	170 GB
ISR-WAAS-750	4 GB	170 GB
ISR-WAAS-1300	6 GB	170 GB
ISR-WAAS-2500	8 GB	360 GB

**Note**

[Table 10-7](#) shows the Cisco WAAS mid to high end platform cache engine memory requirements. [Table 10-8](#) shows the Cisco WAAS mid to high end platform cache engine cache disk requirements..

## Upgrading Cisco vWAAS Memory and Disk for Akamai Connect

This section contains the following topics:

- [Upgrading Memory and Disk for Cisco vWAAS in Cisco WAAS Version 5.4.1x Through 6.1.1x](#), page 10-4
- [Upgrading Memory and Disk for vWAAS in WAAS Versions Earlier than Cisco WAAS Version 5.4.1](#), page 10-5
- [Upgrading Memory and Disk for Cisco vWAAS-12000 with VMware ESXi](#), page 10-6
- [Upgrading Memory and Disk for Cisco vWAAS-12000 with Microsoft Hyper-V](#), page 10-7

### Upgrading Memory and Disk for Cisco vWAAS in Cisco WAAS Version 5.4.1x Through 6.1.1x

If you are running Cisco vWAAS in Cisco WAAS Version 6.1.1x, the Akamai disk is added by default.

## Upgrading Memory and Disk for vWAAS in WAAS Versions Earlier than Cisco WAAS Version 5.4.1

If you are running Cisco vWAAS in a Cisco WAAS version earlier than Cisco WAAS Version 5.4.1, and are using a VMware ESXi version earlier than VMware ESXi Version 5.0, and want to upgrade to Cisco WAAS Version 5.4.1, 5.5.1, or 6.1.1, use the following update memory and disk procedure to use the Akamai Connect feature with Cisco vWAAS.



### Note

Before using this procedure, note the upgrade paths for Cisco WAAS Version 6.2.3, as shown in [Table 10-5](#). For complete upgrade instructions, see the [Release Note for Cisco Wide Area Application Services](#).

**Table 10-5 Upgrade Paths for Cisco WAAS Version 6.2.3**

Current Cisco WAAS Version	Cisco WAAS Central Manager Upgrade Path	Cisco WAAS Upgrade Path
5.5.3 and later	Upgrade directly to 6.2.3	Upgrade directly to 6.2.3
4.3.x through 5.5.1	<ol style="list-style-type: none"> <li>Upgrade to 5.5.3, 5.5.5x (5.5.5, 5.5.5a), or 5.5.7</li> <li>Upgrade to 6.2.3</li> </ol>	<ol style="list-style-type: none"> <li>Upgrade to 5.5.3 or 5.5.5x</li> <li>Upgrade to 6.2.3</li> </ol>

- 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 **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**.

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

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

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

## Upgrading Memory and Disk for Cisco vWAAS-12000 with VMware ESXi



### Caution

When the 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 vWAAS, you need to increase the RAM to 18 GB. This procedure alters the calculation of the `local1` directory size for the vWAAS-12000 because the expected size 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 the RAM size and disk size may cause a serious problem during a kernel crash in the vWAAS-12000 because the `vmcore` file will then be larger than what can be stored in the `local1` directory.

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

**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.

- You must reload the device after using the **disk delete-data-partitions** command.  
The reload process automatically re-creates data partitions, and initializes the caches. This process may take several minutes.  
DRE optimization will not start until the DRE cache has finished initializing.

## Upgrading 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 vWAAS, increase the RAM to 18 GB.



### Caution

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 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 Caution notice, and to safely upgrade Cisco vWAAS memory and disk for Akamai Connect for the Cisco vWAAS-12000, follow these steps:

**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, increase the size of the RAM by at least 6 GB.

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

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

**Step 5** Power on the vWAAS VM.

**Step 6** Check the alarms.

The `filesystem_size_mism` alarm is 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.

- You must reload the device after using the `disk delete-data-partitions` command. The reload process automatically re-creates data partitions, and initializes the caches. This process may take several minutes. DRE optimization will not start until the DRE cache has finished initializing.

## Cisco vWAAS-150 with Akamai Connect

In Cisco vWAAS in WAAS Version 6.1.1 and later, Cisco vWAAS-150 on Cisco ISR-WAAS is supported for Akamai Connect. In vWAAS in Cisco WAAS Version 6.2.1 and later, vWAAS-150 is also supported for RHEL KVM and Microsoft Hyper-V.



**Note** 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.

Table 10-6 shows the specifications for Cisco vWAAS-150.

**Table 10-6** 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

## Cisco WAAS Central Manager and Cisco vWAAS-150

In 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.



### Note

Cisco vWAAS-150 is deployed only in Cisco WAAS Version 6.1.1. Therefore, you cannot upgrade or downgrade Cisco vWAAS-150 from Cisco WAAS Version 6.1.1.

## 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. [Table 10-7](#) shows the connections, total memory, and cache engine memory requirements for each of these platforms. [Table 10-8](#) 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 [Table 10-8](#).

**Table 10-7** Cisco WAAS Mid to High End Platform Cache Engine Memory Requirements

Cisco WAAS Platform	HTTP Object Cache Connections	CPU	Total Memory	Memory Required for Cache Engine
vWAAS-12000	12 K	4	18 GB	4308 M
vWAAS-50000	50 K	8	48 GB	14136 M
WAVE-7541	18 K	2	24 GB	5802 M
WAVE-7571	60 K/ 50 K/ 40 K	2	48 GB	15360 M 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 10-8** Cisco WAAS Mid-End to High-End Platform Cache Engine Cache Disk Requirements

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





## 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:

- [Cisco vWAAS in Cloud Computing Systems, page 11-1](#)
- [Cisco vWAAS in Microsoft Azure, page 11-1](#)
- [Cisco vWAAS in OpenStack, page 11-9](#)

### 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, page 11-2](#)
- [Operating Considerations for Cisco vWAAS in Microsoft Azure, page 11-2](#)
- [Registering the Cisco vWAAS in Microsoft Azure with the Cisco WAAS Central Manager, page 11-3](#)
- [Deploying Cisco vWAAS in Microsoft Azure, page 11-4](#)
- [Upgrade and Downgrade Guidelines for Cisco vWAAS in Microsoft Azure, page 11-9](#)

## 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.

Table 11-1 shows the platforms supported for Cisco vWAAS in Microsoft Azure.

**Table 11-1** Microsoft Azure VM Sizes for Cisco WAAS vWAAS Models

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

## Operating Considerations for Cisco vWAAS in Microsoft Azure

This section contains the following topics:

- [Cisco vWAAS in Microsoft Azure Interoperability, page 11-2](#)
- [Upgrade and Downgrade Guidelines for Cisco vWAAS in Microsoft Azure, page 11-9](#)

### Cisco vWAAS in Microsoft Azure Interoperability

Note 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

Note 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.

## Registering the 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 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 Central Manager.

## Deploying Cisco vWAAS in Microsoft Azure

This section contains the following topics:

- [Deployment Options for Cisco vWAAS in Microsoft Azure, page 11-4](#)
- [Provisioning the Cisco vWAAS VM in Microsoft Azure, page 11-4](#)
- [Deploying vWAAS in Microsoft Azure, page 11-6](#)

### 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, [Accelerate Microsoft Office 365 Shared Deployments with Cisco WAAS WAN Optimization](#).

### Provisioning the Cisco vWAAS VM in Microsoft Azure



#### Note

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.

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

- 
- 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.
  - Step 4** In the **Virtual Machine Name** field, enter the name of the VM you want to create. Use only letters and numbers, up to a maximum of 15 characters.
  - Step 5** At the **Virtual Machine Tier** pane, select **Standard**.

- Step 6** From the **Size** drop-down list, select the Azure VM size for your system. [Table 11-2](#) shows the minimum Azure VM size for each Cisco vWAAS model available for provisioning in the **Virtual Machine Tier** pane.

**Table 11-2** *Microsoft Azure VM Sizes for Cisco vWAAS Models*

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



**Note** Use the **Microsoft Azure Virtual Machine Tier** pane to select an Azure VM for the Cisco vWAAS models shown in [Table 11-2](#). For vWAAS-6000 and vWAAS-12000, you must use the template to specify the Azure VM. For more information, see [Deploying Cisco vWAAS in Microsoft Azure, page 11-4](#). For Azure VM sizes for vWAAS-6000 and vWAAS-12000, see [Table 11-1](#).

- Step 7** In the **New User Name** field, enter your user name.
- Step 8** In the **New Password** field, enter your password.
- Step 9** In the **Confirm** field, re-enter your password.
- Step 10** (Optional) If your system uses SSH key-based authentication:
- Check the **Upload compatible SSH key for authentication** checkbox.
  - From the **Certificate** field, browse for the certificate file for your system.
- Step 11** (Optional) If your system requires a password, check the **Provide a password** checkbox.
- Step 12** Click the right arrow at the lower right of the window to proceed to the next window.  
The next **Create a Virtual Machine/Virtual Machine Configuration** window is displayed.
- Step 13** From the **Cloud Service** drop-down list, choose **Create a Cloud Service**.
- Step 14** In the **Cloud Service DNS Name** field, enter the name of the VM that you created in [Step 4](#).  
When Azure VMs are being named, the DNS name has **cloudapp.net** automatically appended to it.
- Step 15** 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.
- Step 16** From the **Storage Account** drop-down list, select **Use an automatically generated storage account**.
- Step 17** From the **Availability Set** drop-down list, choose **(None)**.
- Step 18** Click the right arrow at the lower right corner of the window to proceed to the next window.  
The **Virtual Machines/Virtual Machine Instances** window is displayed
- Step 19** By default, the **Install the VM Agent** check box is checked.
- Step 20** In the **Endpoints** section:
- Add an endpoint for **SSH (port 22)**.

- Add an endpoint for **HTTPS (port 443)**.
- Step 21** 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 is displayed, showing 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**.
- Step 22** Select the Cisco vWAAS VM.
- Step 23** Attach the data disks. See [Table 11-2](#) for data disk sizes for Azure VMs.
- Step 24** 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 vWAAS in Microsoft Azure

This section has the following topics:

- [Deploying Cisco vWAAS VM and Data Disk with the VHD Template, page 11-6](#)
- [Deploying vWAAS VM with Template and Custom VHD from the Microsoft ARM Portal, page 11-6](#)
- [Deploying the Cisco vWAAS VM Using Microsoft Windows PowerShell, page 11-7](#)
- [Verifying the Cisco vWAAS in Microsoft Azure Deployment, page 11-8](#)

### Deploying Cisco vWAAS VM and Data Disk with the VHD Template

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

- 
- Step 1** Copy **vwaas.vhd** to the storage account using AzCopy.  
The AzCopy command parameters are:
- **Source:** The local folder address on the Windows device where the VHD file is stored.
  - **Dest:** The location of the container on the Azure cloud storage account.
  - **Destkey:** The Azure cloud storage account key.
- Step 2** Use the VHD template to deploy the vWAAS VM.  
The vWAAS VM is deployed with the data disk.
- Step 3** Log in with your username and password.
- Step 4** (Optional) To verify deployment details such as CMS registration and WAAS Central Manager address, see [Verifying the Cisco vWAAS in Microsoft Azure Deployment](#).
- 

### 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 Cisco vWAAS VM in Microsoft Azure](#).

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

- 
- Step 1** Copy **vwaas.vhd** to the storage account using **Azcopy**.
  - Step 2** Use the VHD template to deploy the Cisco 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](#).
- 

## Deploying the 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 Cisco vWAAS VM in Microsoft Azure](#).

To deploy the Cisco vWAAS VM using Microsoft Windows PowerShell, follow these steps:

- 
- Step 1** Deploy vWAAS on Microsoft Hyper-V. For information on this deployment procedure, see Chapter 5, “[Cisco vWAAS on Microsoft Hyper-V](#)”.
  - Step 2** Run the **azure\_predeploy.sh** script in Hyper-V, to set the necessary Azure parameters.
  - Step 3** Export the flash VHD from the Microsoft Hyper-V disk location to the storage account in Microsoft Azure, using **AzCopy**.
  - Step 4** Use Microsoft Windows PowerShell commands to specify the following parameters:
    - Use the **deployName** command to specify the deployment name.
    - Use the **RGName** command to specify the resource group.
    - Use the **locName** command to specify the location.
    - Use the **templateURI** command to specify the template file.
  - Step 5** Run the **New-AzureRmResourceGroup -Name \$RGName -Location \$locName** PowerShell command to create the resource group.
  - Step 6** Run the **New-AzureRmResourceGroupDeployment** PowerShell cmdlet to deploy Cisco vWAAS in Azure. To complete the deployment, specify values for the following parameters:
    - **userImageStorageAccountName**
    - **userImageStorageContainerName**

- userImageVhdName
- osType
- vmName
- adminUserName
- adminPassword

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 7** Log in with your username and password.

**Step 8** (Optional) To verify deployment details such as CMS registration and Cisco WAAS Central Manager address, see [Verifying the Cisco vWAAS in Microsoft Azure Deployment](#).

## Verifying the Cisco vWAAS in Microsoft Azure Deployment

[Table 11-3](#) provides a checklist for verifying the Cisco vWAAS VM deployment in Microsoft Azure.

**Table 11-3 Checklist for Verifying the Cisco vWAAS in Microsoft Azure Deployment**

Task	Description
Viewing vWAAS in Azure devices	<ul style="list-style-type: none"> <li>• From the Cisco WAAS Central Manager, choose <b>Manage Devices</b>. The vWAAS in Azure device type is displayed as <b>OE-VWAAS-AZURE</b>.</li> <li>• From the Cisco WAAS CLI, run either the <b>show version EXEC</b> command or the <b>show hardware EXEC</b> command. Output for both commands will include device ID, displayed as <b>OE-VWAAS-AZURE</b>.</li> </ul>
Viewing Boot Information and Diagnostics	On the Microsoft Azure portal, choose <b>Virtual Machines &gt; VM &gt; Settings &gt; Boot Diagnostics</b> .
Verifying CMS Registration	<ul style="list-style-type: none"> <li>• If the Centralized Management System (CMS) is enabled, use the <b>show cms device status name</b> command to display status for the specified device or device group.</li> <li>• 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: <ul style="list-style-type: none"> <li>– In the Cisco WAAS Central Manager, choose <b>Home &gt; Devices &gt; Primary-CM-Device &gt; Configure &gt; Network &gt; NatSettings</b>.</li> <li>– In the <b>NAT IP</b> field, enter the public IP address of the Central Manager.</li> </ul> </li> </ul>
Verifying Cisco WAAS Central Manager Address	Run the <b>show running-config</b> command to display information about all Cisco WAAS device.



**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, page 11-9](#)
- [Upgrade and Downgrade Guidelines for Cisco vWAAS in OpenStack, page 11-9](#)
- [Deploying Cisco vWAAS in OpenStack, page 11-10](#)

## 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-6.4.3c-b-42.tar.gz
  - NPE OVA: Cisco-KVM-vWAAS-Unified-6.4.3c-b-42-npe.tar.gz
- 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.

## 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.

## Deploying Cisco vWAAS in OpenStack

This section contains the following topics:

- [Guidelines for Deploying vWAAS in OpenStack, page 11-10](#)
- [Procedure for Deploying vWAAS in OpenStack, page 11-10](#)

## Guidelines for Deploying vWAAS in OpenStack

Consider the following guidelines to deploy Cisco vWAAS in OpenStack:

- vWAAS in OpenStack is deployed for vWAAS on KVM. For more information on vWAAS on KVM, see the chapter [“Cisco vWAAS on RHEL KVM, 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-6.4.3c-b-42.tar.
- NPE OVA: Cisco-KVM-vWAAS-Unified-6.4.3c-b-42-npe.tar

For more information about this unified OVA package, see the section [Unified OVA Package for Cisco vWAAS on KVM in WAAS Version 6.4.1 and Later](#).

- After vWAAS in OpenStack is operational on a device, you can use the WAAS CM or the WAAS CLI to display the OpenStack device.
  - The 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 vWAAS in OpenStack

To deploy vWAAS in OpenStack, follow these steps:

- 
- Step 1** Copy the unified OVA to a directory on the host machine.
- Step 2** Untar the OVA using the following command, as shown in [Figure 11-1](#)).
- ```
tar -xvf Cisco-KVM-vWAAS-Unified-6.4.1b-b-11.tar.gz
```

Figure 11-1 Tar Command for vWAAS OpenStack OVA

```

linux-qpaw:/home/b-11 # ls
Cisco-KVM-vWAAS-Unified-6.4.1c-b-11-npe.tar.gz  Cisco-KVM-vWAAS-Unified-6.4.1c-b-11.tar.gz
linux-qpaw:/home/b-11 # tar -xvf Cisco-KVM-vWAAS-Unified-6.4.1c-b-11.tar.gz
Disk-0.qcow2
Disk-1.qcow2
Disk-2.qcow2
launch.sh
vm.xml
ezdeploy.sh
ezdeploy.qstatus.exp
INSTRUCTIONS.TXT
OPENSTACK_INSTRUCTIONS.TXT
image_properties.xml
bootstrap-cfg.xml
akamai_disk.tar
model.txt
vwaas_install.sh
vwaas-admin-deny-config.xml
permit.xml
package.mf

```

355736

Step 3 Create the image.

- a. Click the **OpenStack Admin** tab and choose the **Compute > Images** window (Figure 11-2).

Figure 11-2 OpenStack Compute > Images Page

| Owner | Name | Type | Status | Visibility | Protected | Disk Format | Size |
|----------|----------|-------|--------|------------|-----------|-------------|-----------|
| admin | 641C | Image | Active | Public | No | QCOW2 | 568.50 MB |
| admin | 641CB-11 | Image | Active | Public | No | QCOW2 | 568.50 MB |
| admin | 641CB12 | Image | Active | Public | No | QCOW2 | 568.56 MB |
| admin | 641CB9 | Image | Active | Public | No | QCOW2 | 540.31 MB |
| services | ciros | Image | Active | Public | No | QCOW2 | 12.67 MB |
| admin | vWAAS | Image | Active | Public | No | QCOW2 | 611.69 MB |

355721

- 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 11-3).

Figure 11-3 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**.

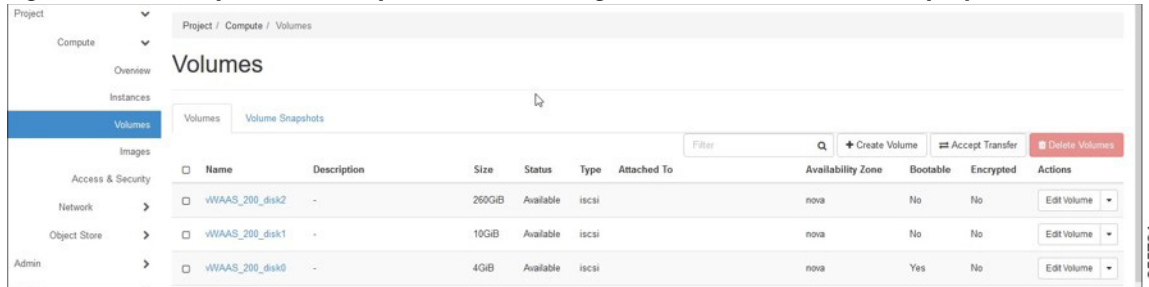
Step 5 Create nonbootable volumes.

- a. Click the **OpenStack Admin** tab and choose **Compute > Create Volume** (Figure 11-4).

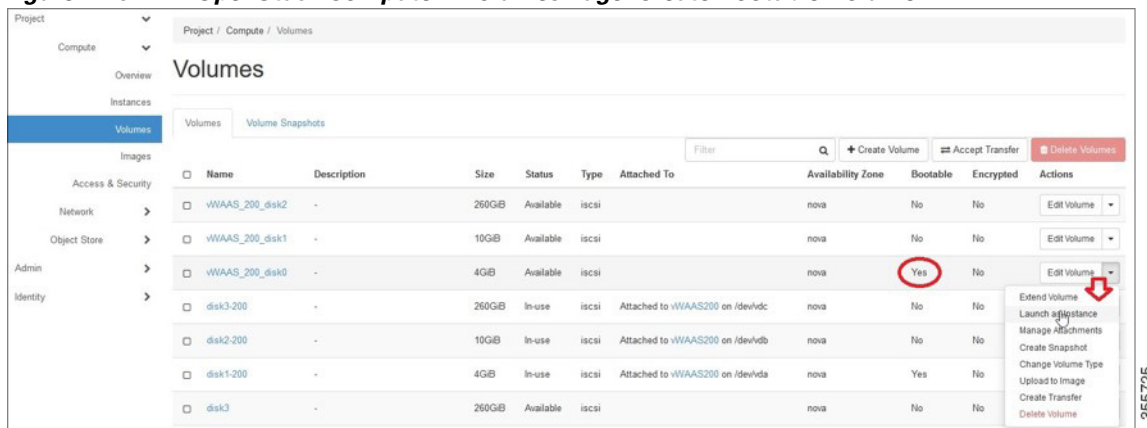
Figure 11-4 OpenStack Create Volume Dialog Box: Creating Nonbootable Volumes

- 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 11-5):

Figure 11-5 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 11-6).

Figure 11-6 OpenStack Compute > Volumes Page: Create Bootable Volume

- b. Launch the instance.
- c. Click the **OpenStack Admin** tab and choose **Compute > Instances > Launch Instance** (Figure 11-7).

Figure 11-7 OpenStack Launch Instance > Details Page

Launch Instance

Please provide the initial hostname for the instance, the availability zone where it will be deployed, and the instance count. Increase the Count to create multiple instances with the same settings.

Instance Name *
vWAAS-200

Availability Zone
nova

Count *
1

Total Instances (10 Max)
50%

- 4 Current Usage
- 1 Added
- 5 Remaining

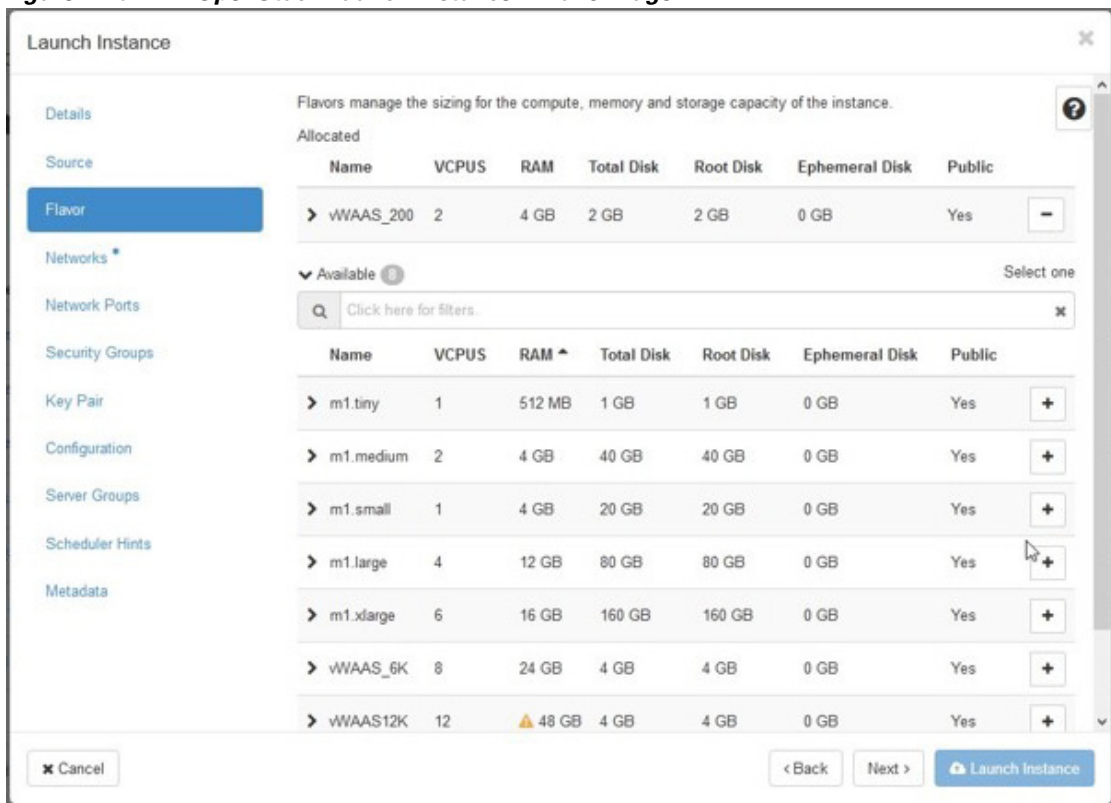
Cancel Back Next Launch Instance

355726

- In the **Instance Name** field, enter the name of the Cisco vWAAS model, for example, **vWAAS-200**.
- From the **Availability** drop-down list, choose **nova**.
- From the **Count** drop-down list, choose **1**.
- Click **Launch Instance**.

Step 7 Specify the flavor suitable for the selected Cisco vWAAS model. As noted on the OpenStack page (Figure 11-8), 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 11-8).

Figure 11-8 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 11-9).

Figure 11-9 OpenStack Launch Instance > Networks Page

Launch Instance

Details

Source

Flavor

Networks

Network Ports

Security Groups

Key Pair

Configuration

Server Groups

Scheduler Hints

Metadata

Networks provide the communication channels for instances in the cloud.

▼ Allocated ² Select networks from those listed below.

| | Network | Subnets Associated | Shared | Admin State | Status | |
|---|---------------|--------------------|--------|-------------|--------|---|
| 1 | vWAAS_Public | vWAAS_ext | Yes | Up | Active | - |
| 2 | vwaas_private | vWAAS_int | Yes | Up | Active | - |

▼ Available ¹ Select at least one network

Click here for filters.

| Network ^ | Subnets Associated | Shared | Admin State | Status | |
|---------------|----------------------------|--------|-------------|--------|---|
| vWAAS_Network | vwaas_priv
Ipv6-Private | Yes | Up | Active | + |

Cancel < Back Next > Launch Instance

355728

Step 9 Select the configuration drive to send model parameters.

Click the **OpenStack Admin** tab and choose **Compute > Instances > Launch Instance > Configuration** (Figure 11-10).

Figure 11-10 OpenStack Launch Instance > Configuration Page

Launch Instance

Details

Source

Flavor

Networks

Network Ports

Security Groups

Key Pair

Configuration

Server Groups

Scheduler Hints

Metadata

You can customize your instance after it has launched using the options available here. "Customization Script" is analogous to "User Data" in other systems.

Customization Script

Script size: 0 bytes of 16.00 KB

Load script from a file

Browse... No file selected.

Disk Partition

Automatic

Configuration Drive

Cancel

< Back

Next >

Launch Instance

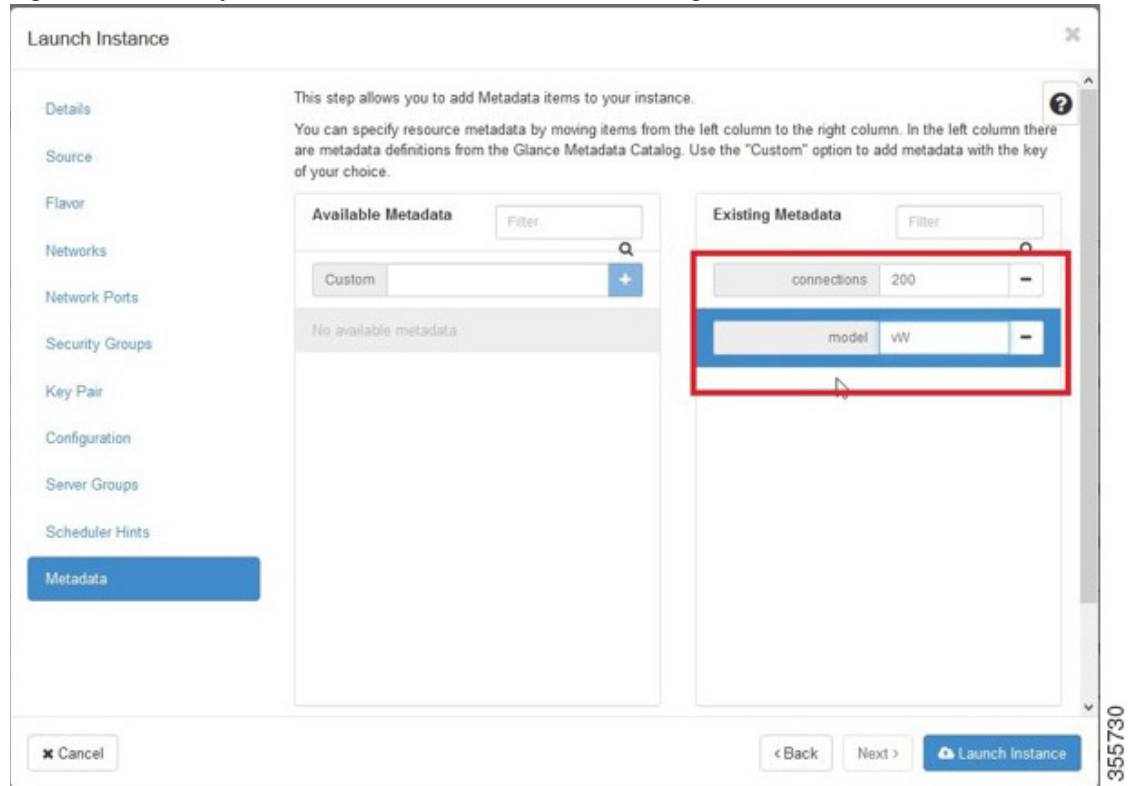
355729

- From the **Disk Partition** drop-down list, choose **Automatic**.
- Check the **Configuration Drive** check box.
- Click **Launch Instance**.

Step 10 Provide model and connection information to deploy vWAAS in OpenStack metadata.

Click the **OpenStack Admin** tab and choose **Compute > Instances > Launch Instance > Metadata** (Figure 11-11).

Figure 11-11 OpenStack Launch Instance > Metadata Page

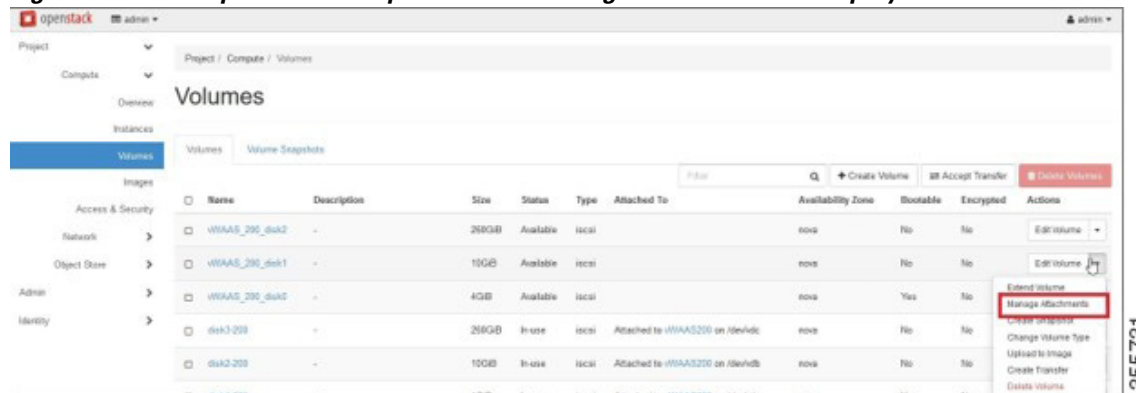


- Specify resource metadata by selecting and moving items from the **Available Metadata** column into the **Existing Metadata** column.

Step 11 Attach disks to the deployed instance.

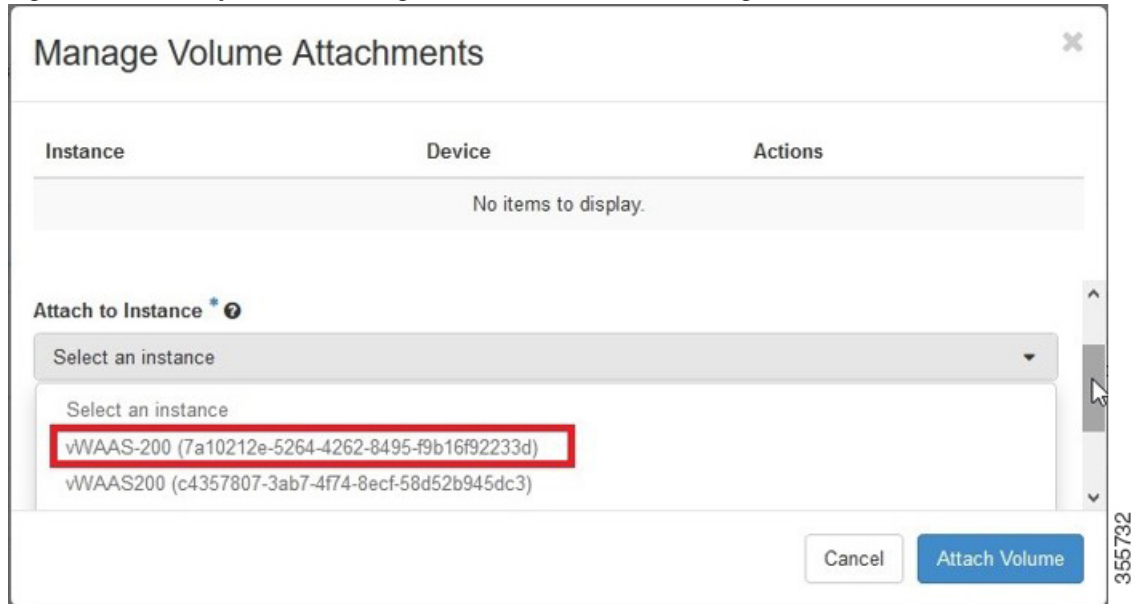
Click the **OpenStack Admin** tab and choose **Compute > Volumes** (Figure 11-12).

Figure 11-12 OpenStack Compute > Volumes Page: Attach disks to deployed instance



- From the **Edit Volume** drop-down list, choose **Manage Attachments**. The **Manage Volume Attachments** dialog box appears (Figure 11-13).

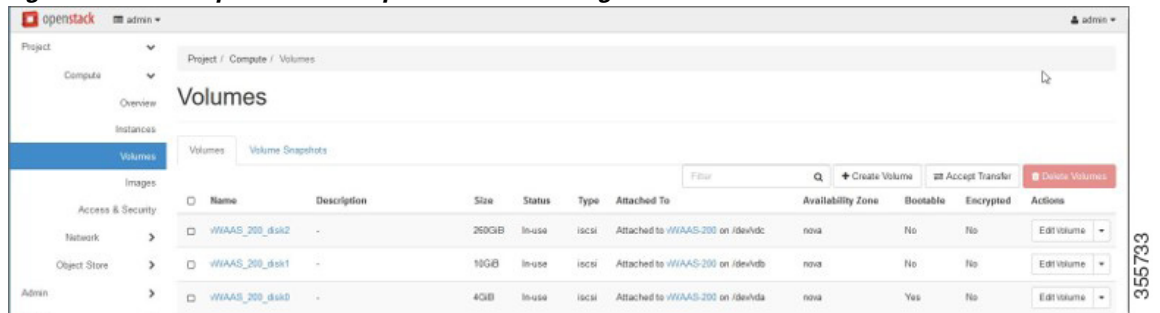
Figure 11-13 OpenStack Manage Volume Attachments Dialog Box



- b. From the **Select an instance** drop-down list, choose the instance to attach to the disk.
- c. Click **Attach Volume**.

Step 12 After attaching the disks, the **Compute > Volumes** window displays the attached disks (Figure 11-14).

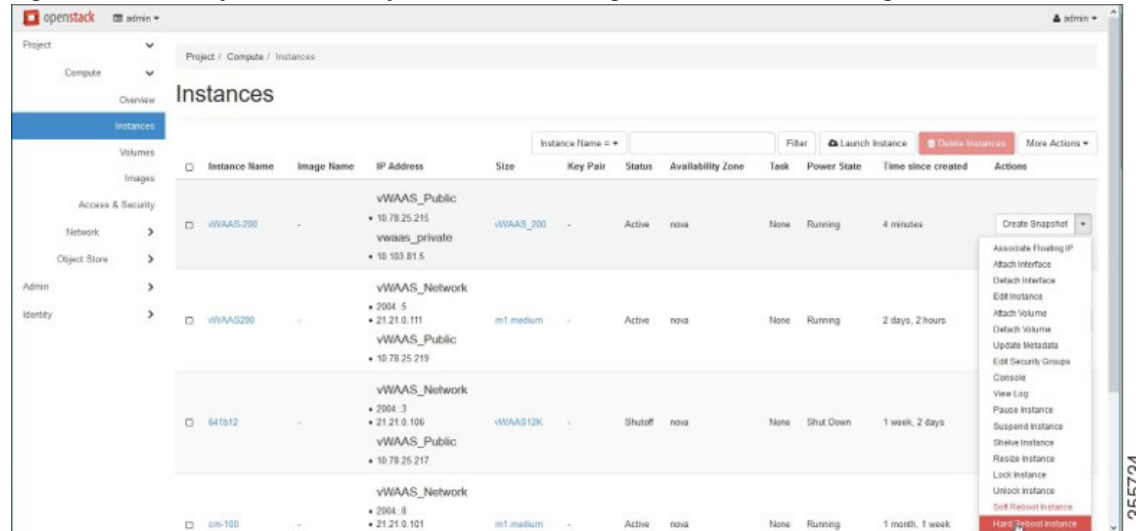
Figure 11-14 OpenStack Compute > Volumes Page: List of attached disks



Step 13 Reboot the system (hard reboot).

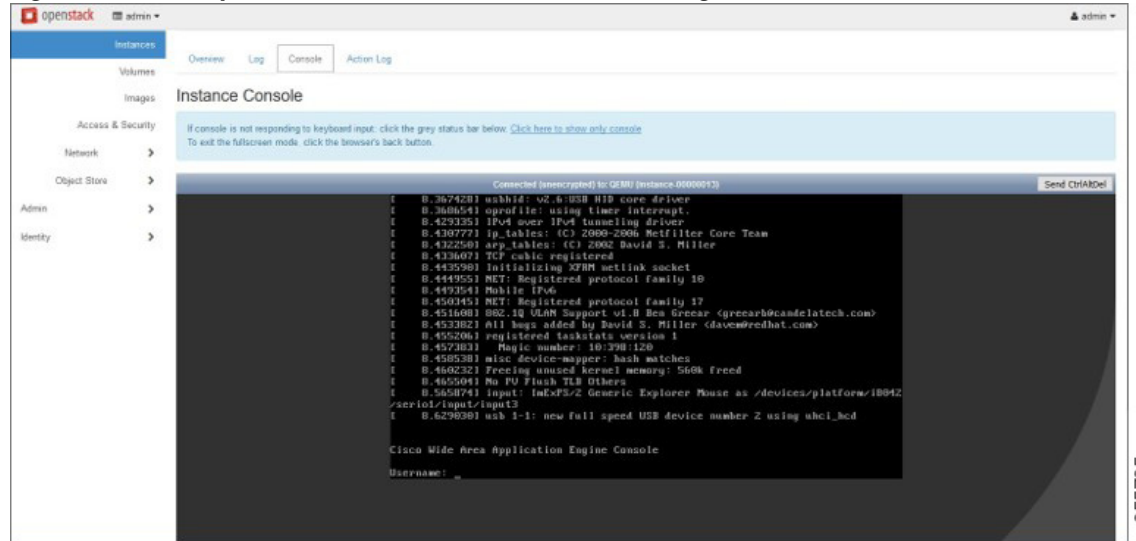
- a. After the system is rebooted, choose **Compute > Instances**.
- b. From the **Create Snapshot** drop-down list, choose **Hard Reboot Instance**.
- c. The **Compute > Instances** window displays the attached disks (Figure 11-15).

Figure 11-15 OpenStack Compute > Instances Page: Attached disks listing



Step 14 From the Instances > Instance Console page, connect to the console to work on vWAAS (Figure 11-16).

Figure 11-16 OpenStack Instances > Instance Console Page





Troubleshooting Cisco vWAAS

This chapter describes how to identify and resolve operating issues with Cisco vWAAS, and contains the following sections:

- [Resolving Diskless Startup and Disk Failure, page 12-1](#)
- [Troubleshooting Cisco vWAAS Device Registration, page 12-1](#)
- [Verifying Cisco vWAAS Virtual Interfaces, page 12-2](#)
- [Troubleshooting Cisco vWAAS Networking, page 12-3](#)
- [Troubleshooting an Undersized Alarm, page 12-3](#)

Resolving Diskless Startup and Disk Failure

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`.

To recover from this failure, follow these steps:

Step 1 Re-enable the disk:

```
vwaas# config
vwaas(config)# no disk disk-name disk00 shutdown force
vwaas(config)# exit
```

Step 2 Reload Cisco vWAAS:

```
vwaas# reload
```

Troubleshooting Cisco vWAAS Device Registration

You must register each 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** ([Figure 12-1](#)) is displayed when you use the **show alarms** command.

Figure 12-1 Display for show alarms Command: Not Registered Alarm

```
vWAAS# show alarms

Critical alarms:
-----
None

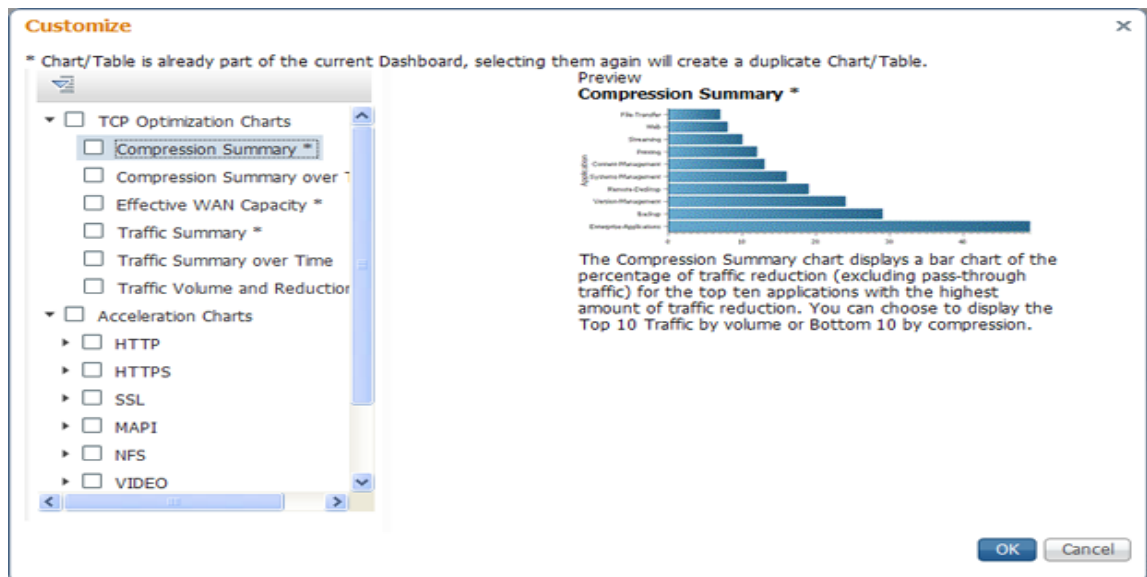
Major alarms:
-----
      Alarm ID      Module/Submodule      Instance
-----
      1 not registered      vwaas/model      vwaas/model <----- Not registered alarm
      . . .

Minor alarms:
-----
None
```

Verifying 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 > Configure > Network > Network Interfaces** to display the window shown in [Figure 12-2](#).

Figure 12-2 Network Interfaces for Device Window

For the Cisco WAAS CLI, use the **show running-config interface** command to display the virtual interfaces. For additional details on the virtual interfaces, use the **show interface virtual 1/0** command or the **show interface virtual 2/0** command.

Troubleshooting Cisco vWAAS Networking

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.

To use the VMware vSphere Client to trace Cisco vWAAS connectivity from the device page, follow these steps:

-
- Step 1** Identify which network label the network adapter is connected to.
 - Step 2** Determine the virtual switch that this network is connected to.
 - Step 3** Determine the physical NIC that is a member of this virtual switch.
 - Step 4** Verify that the configuration is correct.
 - Step 5** Verify that the virtual switch settings are correctly configured to reach the network.
 - Step 6** Verify the configured IP address, netmask, default gateway, and primary interface. For more information on these parameters, see [Verifying Cisco vWAAS Virtual Interfaces, page 12-2](#).
 - 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. [Figure 12-3](#) shows an example of this.

Figure 12-3 Sample Output for **show alarms** Command: Undersized Alarm

```
vWAAS# show alarms



Critical alarms:
-----
None

Major alarms:
-----
      Alarm ID           Module/Submodule           Instance
-----
      1 undersized       vwaas/model                memory      <----- Undersized alarm
      . . .

Minor alarms:
-----
None
```

[Table 12-1](#) describes the fields in the **show alarms** command output.

Table 12-1 *Field Descriptions for show alarms Command*

| Field | Description |
|------------------|--|
| Critical Alarms | <p>Critical alarms affect the existing traffic through the Cisco WAE and are considered fatal. The Cisco WAE cannot recover and continue to process traffic.</p> <p> Note Cisco WAAS and Cisco vWAAS provide three levels of alarms: critical, major, and minor. For more information on alarms and the show alarms command, see Cisco Wide Area Application Services Command Reference.</p> |
| Major Alarms | <p>Major alarms indicate a major service (such as the cache service) has been damaged or lost. Urgent action is necessary to restore this service. However, other node components are fully functional and the existing service should be minimally impacted.</p> <p> Note Cisco WAAS and Cisco vWAAS provide three levels of alarms: critical, major, and minor. For more information on alarms and the show alarms command, see Cisco Wide Area Application Services Command Reference.</p> |
| Alarm ID | Type of event that caused the alarm. |
| Module/Submodule | The software module affected. |
| Instance | The object that this alarm is associated with. As shown in Figure 12-3 , the instance for this alarm is <i>memory</i> . The Instance field does not have predefined values; each Instance value is application specific. |

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.