Cisco Virtual Wide Area Application Services Configuration Guide

WAAS Software Version 6.2.x
December 11, 2018

Cisco Systems, Inc.
www.cisco.com

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

Cisco Virtual Wide Area Application Services Configuration Guide

CONTENTS

Preface

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

Audience

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

Document Organization

This guide is organized as follows:

- Chapter 1, "Introduction to Cisco vWAAS"
- Chapter 2, "Configuring Cisco vWAAS and Viewing vWAAS Components"
- Chapter 3, "Cisco vWAAS and VMware vSphere ESXi"
- Chapter 4, "Cisco vWAAS on KVM"
- Chapter 5, "Cisco vWAAS on Microsoft Hyper-V"
- Chapter 6, "Cisco vWAAS in Microsoft Azure"
- Chapter 7, "Cisco vWAAS with Akamai Connect"
- Chapter 8, "Troubleshooting Cisco vWAAS"

Document Conventions

Command descriptions use these conventions:

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

Screen examples use these conventions:

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

This document uses the following conventions:

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

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

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

Related Documentation

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

- *Cisco Wide Area Application Services Upgrade Guide*
- *Cisco Wide Area Application Services Quick Configuration Guide*
- *Cisco Wide Area Application Services Configuration Guide*
- *Cisco Wide Area Application Services Command Reference*
- *Cisco Wide Area Application Services API Reference*
- *Cisco Wide Area Application Services Monitoring Guide*
- *Cisco WAAS on Service Modules for Cisco Access Routers*

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

Obtaining Documentation and Submitting a Service Request

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

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

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

Introduction to Cisco vWAAS

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

This chapter contains the following sections:

About Cisco vWAAS

This section has the following topics:

Benefits of Cisco vWAAS

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

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

- Public cloud environments:
  - Deploy vWAAS in public clouds, with the Cisco Nexus 1000V Series, to obtain benefits similar to benefits vWAAS produces in private cloud environments.
- Cisco vWAAS is supported on a wide range of hypervisors, including Microsoft Hyper-V, RHEL KVM, KVM on CentOS, and Microsoft Azure. Each hypervisor is described in Hypervisors Supported for Cisco vWAAS.
- Cisco vWAAS runs on a wide range of platforms, described in Platforms Supported for Cisco vWAAS.

Cisco vWAAS at the Branch and the Data Center

Cisco Virtual WAAS (vWAAS) is a virtual appliance—for both enterprises and service providers—that accelerates business applications delivered from private and virtual private cloud infrastructure. Cisco vWAAS enables you to rapidly create WAN optimization services with minimal network configuration or disruption.

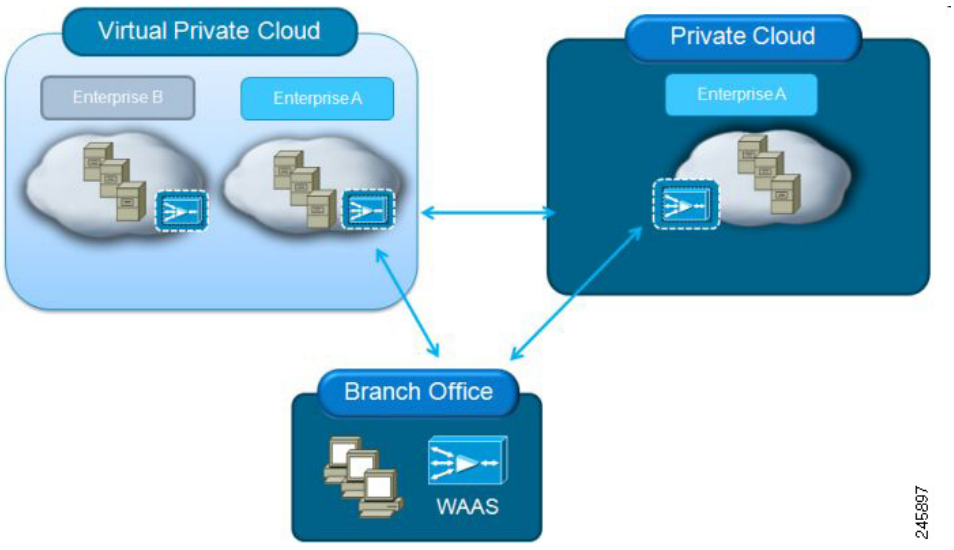
Cisco vWAAS supports WAN optimization in a cloud environment where physical WAE devices cannot usually be deployed. Virtualization also provides various benefits like elasticity, ease of maintenance, and a reduction of branch office and data center footprint.

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

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

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

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



The following hypervisors are supported for Cisco vWAAS:

- Cisco ISR-WAAS
- Cisco NFV Infrastructure Software (NFVIS)
- VMware vSphere ESXi
- Microsoft HyperV
- Red Hat Enterprise Linux Kernel-based Virtual Machine (RHEL KVM)
- KVM on CentOS
- Microsoft Azure

The following platforms are supported for Cisco vWAAS:

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

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

vWAAS Model Profiles

This section contains the following topics:

ISR Models: CPUs, Memory, Disk Storage and Supported ISR Platforms

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

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

ISR Model	CPUs	Memory	Disk Storage	Supported ISR Platform
ISR-WAAS-200 (for WAAS 5.x and 6.2.1)	1	3 GB	151 GB	ISR-4321
ISR-WAAS-200 (for WAAS 6.2.3x and 6.3.1)	1	4 GB	151 GB	ISR-4321
ISR-WAAS-750	2	4 GB	151 GB	ISR-4351, ISR-4331, ISR-4431, ISR-4451
ISR-WAAS-1300	4	6 GB	151 GB	ISR-4431, ISR-4451
ISR-WAAS-2500	6	8 GB	338 GB	ISR-4451

Note For vWAAS with WAAS Version 6.2.3x or WAAS Version 6.3.1, ISR-4321 with profile ISR-WAAS-200, ISR-WAAS RAM is increased from 3 GB to 4 GB. For this increase in ISR-WAAS RAM to be implemented, you must complete a new OVA deployment of WAAS version 6.2.3x or 6.3.1; the increase in ISR-WAAS RAM is not automatically implemented with an upgrade to WAAS 6.2.3x or 6.3.1.

vWAAS Models: CPUs, Memory and Disk Storage

Table 1-2 shows the default number of CPUs, memory capacity and disk storage for each vWAAS model.

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

vWAAS Model	CPUs	Memory	Disk Storage
vWAAS-150 (for WAAS Version 6.x)	1	3 GB	160 GB
vWAAS-200 (for WAAS Version 5.x through 6.2.1)	1	3 GB	260 GB
vWAAS-200 (for WAAS Version 6.2.3x and 6.3.1)	1	4 GB	260 GB
vWAAS-750	2	4 GB	500 GB
vWAAS-1300	2	6 GB	600 GB
vWAAS-2500	4	8 GB	750 GB
vWAAS-6000	4	11 GB	900 GB
vWAAS-12000	4	12 GB	750 GB
vWAAS-50000	8	48 GB	1500 GB

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

- When using vWAAS-150 or vWAAS-200 with the KVM hypervisor, you must increase the default memory of 3 GB to 4 GB.

Note For vWAAS with WAAS Version 6.2.3x or WAAS Version 6.3.1, ISR-4321 with profile ISR-WAAS-200, ISR-WAAS RAM is increased from 3 GB to 4 GB. For this increase in ISR-WAAS RAM to be implemented, you must complete a new OVA deployment of WAAS version 6.2.3x or 6.3.1; the increase in ISR-WAAS RAM is not automatically implemented with an upgrade to WAAS 6.2.3x or 6.3.1.

- When vWAAS-6000, 1300, 12000, or 50000 are used with Akamai Connect and when connections are more than 70% of TFO, response time will be on the higher side. Adding CPUs to these models when used with Akamai Connect may improve response time.

VMware VMFS Block Size and vWAAS Disk Size

Table 1-3 shows the VMware Virtual Machine File System (VMFS) block size and associated vWAAS maximum disk file size. For more information on VMware and vWAAS interoperability, see Table 1-12.

Table 1-3 VMware VMFS Block Size and vWAAS Maximum File Size

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

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

vWAAS Models: OVA and NPE OVA Files

Table 1-4 shows the OVA and NPE OVA file for each vWAAS model (all models are available with WAAS version 4.3.1 and later, except as noted):

Table 1-4 OVA and NPE OVA Files, by vWAAS Model

vWAAS Model	OVA Filename	NPE OVA Filename
vWAAS-150 (for WAAS Version 6.x)	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-500000-npe.ova

vWAAS Central Manager (vCM) Model Profiles

This section contains the following topics:

vCM Models: CPUs, Memory, Disk Storage and Managed Nodes

Table 1-5 shows the number of managed nodes and disk storage for each vCM model, as well as the required and recommended number of vCPUs and the required and recommended memory capacity.

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

However, as the number of managed devices on your system increases, the Central Manager service can experience intermittent restarts or flapping—device states when under resource shortage. To remedy this, please configure the recommended values for number of CPUs and memory shown in Table 1-5.

Table 1-5 vCM Models: Managed Nodes, vCPUs, Memory, and Disk Storage

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

Note If your WAAS Central Manager restarts intermittently with the following vCM models - vCM-500, vCM-1000, or vCM-2000 - it may be due to insufficient system resources. To remedy this, for these vCM models we recommend that you upgrade your system with the CPU and memory resources show in Table 1-6.

Table 1-6 Recommended CPU and Memory Upgrade for vCM-500, vCM-1000, and vCM-2000

vCM Model	Default Number of vCPUs	Recommended Number of vCPUs	Default Memory	Recommended Memory	Disk Storage (unchanged)	Managed Nodes (unchanged)
vCM-500	2	4	2 GB	5 GB	300 GB	500
vCM-1000	2	6	4 GB	8 GB	400 GB	1000
vCM-2000	4	8	8 GB	16 GB	600 GB	2000

vCM Models: OVA and NPE OVA Files

Table 1-7 shows the OVA and NPE OVA file for each vCM model (all models are available with WAAS version 4.3.1 and later, except as noted):

Table 1-7 OVA and NPE OVA Files, by vCM Model

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 WAAS and vWAAS Interoperability

Table 1-8 shows the default number of CPUs, memory capacity, disk storage and supported ISR platforms for ISR models.

Table 1-8 ISR Models: CPUs, Memory, Disk Storage and Supported ISR Platforms

ISR Model	CPUs	Memory	Disk Storage	Supported ISR Platform
ISR-WAAS-200 (for WAAS 5.x and 6.2.1)	1	3 GB	151 GB	ISR-4321
ISR-WAAS-200 (for WAAS 6.2.3x and 6.3.1)	1	4 GB	151 GB	ISR-4321
ISR-WAAS-750	2	4 GB	151 GB	ISR-4351, ISR-4331, ISR-4431, ISR-4451
ISR-WAAS-1300	4	6 GB	151 GB	ISR-4431, ISR-4451
ISR-WAAS-2500	6	8 GB	338 GB	ISR-4451

Note For vWAAS with WAAS Version 6.2.3x or WAAS Version 6.3.1, ISR-4321 with profile ISR-WAAS-200, ISR-WAAS RAM is increased from 3 GB to 4 GB. For this increase in ISR-WAAS RAM to be implemented, you must complete a new OVA deployment of WAAS version 6.2.3x or 6.3.1; the increase in ISR-WAAS RAM is not automatically implemented with an upgrade to WAAS 6.2.3x or 6.3.1.

Consider the following guidelines when using Cisco vWAAS with WAAS:

Note For vWAAS with WAAS Version 6.2.3x or WAAS Version 6.3.1, ISR-4321 with profile ISR-WAAS-200, ISR-WAAS RAM is increased from 3 GB to 4 GB. For this increase in ISR-WAAS RAM to be implemented, you must complete a new OVA deployment of WAAS version 6.2.3x or 6.3.1; the increase in ISR-WAAS RAM is not automatically implemented with an upgrade to WAAS 6.2.3x or 6.3.1.

Note When selecting the format in the vSphere Client for the virtual machine's disks for vWAAS with VMware vSphere ESXi, you must choose the **Thick Provision Eager Zeroed** disk format for vWAAS deployment; this is the format recommended with vWAAS deployment for a clean installation.

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

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

- For vWAAS with WAAS Version 6.1.x and later, the vWAAS and vCM devices require *both* virtual (network) interfaces to be present, but both need not be active. If only one virtual interface is active, the vWAAS and vCM devices will not be operational after power up. For more information, see the *Cisco Virtual Wide Area Application Services Installation and Configuration Guide*.

- To ensure reliable throughput with the following configuration—**vWAAS on Windows Server 2012 R2 Hyper-V in Cisco UCS-E Series 160S-M3**—we recommend that you do the following:
  - Upgrade to the latest UCS-E firmware (Version 3.1.2), available on the Cisco Download Software Page for UCS E-Series Software, UCS E160S M3 Software.
  - Verify that you have installed the critical Windows Server updates, available on the Microsoft Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2 Update Rollup page. You can also obtain the standalone update package through the Microsoft Download Center by searching for **KB2887595**.

Note When upgrading vWAAS, do not upgrade more than five vWAAS nodes at the same time on a single UCS box. Upgrading more than five vWAAS nodes at the same time may cause the vWAAS devices to go offline and diskless mode.

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

  If needed, change the SCSI controller type to **VMware Paravirtual** by following these steps:

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

  For more information on setting the SCSI Controller Type and on the vWAAS VM installation procedure, see the *Cisco Virtual Wide Area Application Services Installation and Configuration Guide*.

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

When you upgrade to WAAS Version 6.2.3 from an earlier version, or downgrade from WAAS Version 6.2.3 to an earlier version, and use either the **restore factory-default** command or the **restore factory-default preserve basic-config** command, the vCM-100 may not come up due to GUID Partition Table (GPT) boot order errors.

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

To resolve this situation, follow these steps:

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

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

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

DRE Disk, Object Cache, and Akamai Connect Cache Capacity

This section contains the following topics:

- Table 1-9 shows the DRE disk capacity, default object cache capacity, and default Akamai Connect Cache capacity by WAVE model.
- Table 1-10 shows the DRE disk capacity, default object cache capacity, and default Akamai Connect Cache capacity by vWAAS model.

Table 1-9 DRE Disk, Default OC, and Default Akamai Connect Cache by WAVE Model

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

Table 1-10 shows the default DRE disk capacity, object cache capacity, and Akamai Connect cache capacity, by vWAAS model.

Table 1-10 Default DRE, OC, and Akamai Connect Cache, by vWAAS Mode

vWAAS Model	DRE Disk Capacity	Default Object Cache Capacity	Default Akamai Connect Cache Capacity
vWAAS-150	52.3 GB	52 GB	30 GB
vWAAS-200	52.23 GB	82 GB	100 GB
vWAAS-750	96.75 GB	122 GB	250 GB
vWAAS-1300	140 GB	122 GB	300 GB
vWAAS-2500	238 GB	122 GB	350 GB
vWAAS-6000	320 GB	122 GB	400 GB
vWAAS-6000R	320 GB	122 GB	350 GB
vWAAS-12000	450 GB	226 GB	750 GB
vWAAS-50000	1000 GB	227 GB	850 GB

Hypervisors Supported for Cisco vWAAS

This section has the following topics, which show the hypervisors supported for Cisco vWAAS and Virtual Central Manager (vCM).

- Cisco ISR-WAAS
- VMware vSphere ESXi
- RHEL KVM and KVM on CentOS
- Microsoft Hyper-V
- Microsoft Azure

Table 1-11 shows the file formats for hypervisors supported for vWAAS and vCM, for WAAS Version 6.x and later.

Table 1-11 File Formats for Hypervisors Supported for vWAAS and vCM

vWAAS or vCM	Hypervisor	File Format	NPE File Format	Example of Image and NPE Image Filename Formats
vWAAS	VMware ESXi	.ova	.ova	• Cisco-vWAAS-2500-6.2.1-b-11.ova • Cisco-vWAAS-2500-6.2.1-npe-b-11.ova
	Microsoft Hyper-V	.zip	.zip	• Hv-Cisco-vWAAS-750-6.2.1-b-11.zip • Hv-Cisco-vWAAS-750-6.2.1-b-11-npe.zip
	RHEL KVM	.tar.gz	.tar.gz	• Cisco-KVM-vWAAS-2500-6.2.1-b-11.tar.gz • Cisco-KVM-vWAAS-2500-6.2.1-b-11-npe-npe.tar.gz
	Microsoft Azure	N/A	N/A	• N/A
vCM	VMware ESXi	.ova	.ova	• Cisco-VCM-500N-6.2.1-b-11.ova • Cisco-VCM-500N-6.2.1-npe-b-11.ova
	Microsoft Hyper-V	N/A	.zip	• Hv-Cisco-vCM-100N-6.1.1-b-26.zip • Hv-Cisco-vCM-500N-6.1.1-b-26.zip
	RHEL KVM	.tar.gz	.tar.gz	• Cisco-KVM-vCM-500N-6.2.1-b-11.tar.gz • Cisco-KVM-vCM-500N-6.2.1-b-11-npe-npe-tar.gz
	Microsoft Azure	N/A	N/A	• N/A

Cisco ISR-WAAS

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

VMware vSphere ESXi

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

For more information, see Chapter 3, "Cisco vWAAS and VMware vSphere ESXi".

RHEL KVM and KVM on CentOS

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

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

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

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

Microsoft Hyper-V

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

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

For more information, see Chapter 5, "Cisco vWAAS on Microsoft Hyper-V".

Microsoft Azure

Microsoft Azure is a Microsoft cloud computing platform that can be used to build and host applications online, using the Microsoft Hyper-V hypervisor. Cisco vWAAS in Azure is available for vWAAS with WAAS Version 6.2.1x and later. Cisco vWAAS in Azure is also part of WAAS support for Office 365, and end-to-end solution with enterprise branch offices.

For more information, see Chapter 6, "Cisco vWAAS in Microsoft Azure".

Platforms Supported for Cisco vWAAS

Cisco vWAAS is supported on the following platforms:

- Cisco Unified Computing System (UCS)

- Cisco UCS E-Series Servers
- Cisco UCS E-Series Network Compute Engines (NCEs)
- Cisco ISR-4000 Series
- Microsoft Azure Cloud

This section contains the following topics:

Platforms Supported for vWAAS, by Hypervisor Type

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

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

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

Hypervisor	PID and Device Type	Minimum WAAS Version	Host Platforms	Minimum Host Version	Disk Type
Cisco ISR-WAAS	• PID: OE-VWAAS-KVM • Device Type: ISR-WAAS	• 5.4.1 • 5.2.1 (ISR-4451)	• ISR-4451 (vWAAS-750, 1300, 2500) • ISR-4431 (vWAAS-750, 1300) • ISR-4351 (vWAAS-750) • ISR-4331 (vWAAS-750) • ISR-4321 (vWAAS-750)	• IOS-XE 3.9	• ISR-SSD • NIM-SSD
Cisco NFVIS	• PID: OE-VWAAS-KVM • Device Type: OE-VWAAS-KVM	• 6.2x	• Cisco ENCS (Enterprise Network Compute System) • Cisco UCS-E Series	• NFV FC2	• virtio
VMware vSphere ESXi	• PID: OE-VWAAS-ESX • Device Type: OE-VWAAS-ESX	• 5.0.3g	• Cisco UCS (Unified Computing System) • Cisco UCS-E Series	• ESXi 5.0	• VMDK
Microsoft HyperV	• PID: OE-VWAAS-HYPERV • Device Type: OE-VWAAS-HYPERV	• 6.1x	• Cisco UCS • Cisco UCS-E Series	• Microsoft Windows 2008 R2	• VHD

Hypervisor	PID and Device Type	Minimum WAAS Version	Host Platforms	Minimum Host Version	Disk Type
RHEL KVM	• PID: OE-VWAAS-KVM • Device Type: OE-VWAAS-KVM	• 6.2x	• Cisco UCS • Cisco UCS-E Series	• RHEL CentOS 7.1	• virtio
Microsoft Azure	• PID: OE-VWAAS-AZURE • Device Type: OE-VWAAS-AZURE	• 6.2x	• Microsoft Azure cloud	• N/A	• VHD

Components for Deploying vWAAS, by Hypervisor Type

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

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

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

Components for Managing vWAAS, by Hypervisor Type

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

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

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

vWAAS on Cisco UCS E-Series Servers and NCEs

This section has the following topics:

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

vWAAS and Cisco UCS E-Series Interoperability

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

Table 1-15 vWAAS and UCS E-Series Interoperability

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

vWAAS and Cisco UCS E-Series Memory Guidelines and Requirements

When calculating memory requirements for your vWAAS system, include the following parameters:

- vWAAS on VMware
  - 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.
  - Table 1-16 shows memory and disk storage for Cisco UCS E-Servers/NCEs
- 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.
  - Table 1-18 shows vCPUs, ESXi server datastore memory, and disk space by vWAAS model.
  - Table 1-19 shows vCPUs, ESXi server datastore memory, and disk space by vCM model.

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

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

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

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

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

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

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

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

VMware ESXi for Cisco vWAAS and Cisco WAAS

This section contains the following topics:

VMware ESXi Versions Supported for Cisco WAAS

Table 1-17 VMware ESXi Versions Supported for Cisco WAAS

ESX version	WAAS v5.1	WAAS v5.2	WAAS v5.3	WAAS v5.4	WAAS v5.5	WAAS v6.x
ESXi 6.0 vWAAS fresh installation	x	x	x	x	x	Supported OVA
ESXi 6.0 vWAAS upgrade	x	x	x	x	x	Upgrade with .bin file

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

- VMware vCenter server and vSphere client version 4.x management software.

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

This section has the following topics:

- Table 1-18 shows ESXi server datastore memory and disk space per vWAAS model, for WAAS v4.3.1 through v5.3.5, and for WAAS v5.4.x through v6.x.
- Table 1-19 shows ESXi server datastore memory and disk space per vCM model, for WAAS v4.3.1 through v5.3.5, and for WAAS v5.4.x through v6.x.

Table 1-18 vCPUs, ESXi Server Datastore Memory, and Disk Space by vWAAS Model

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

Table 1-19 vCPUs, ESXi Server Datastore Memory, and Disk Space by vCM Model

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

Cisco vWAAS and WAAS Interoperability

Consider the following guidelines when using Cisco vWAAS with WAAS:

- *For vWAAS with WAAS Version 6.1.x and later*—The vWAAS and vCM devices require *both* virtual (network) interfaces to be present, but both need not be active. If only one virtual interface is active, the vWAAS and vCM devices will not be operational after power up
- *Cisco WAAS Central Manager interoperability*—In a mixed version Cisco WAAS network, the Central Manager must be running the highest version of the Cisco WAAS software, and associated Cisco WAAS devices must be running Version 5.1.x or later.
- *Cisco WAAS system interoperability*—Cisco WAAS Version 6.2.3 is not supported running in a mixed version Cisco WAAS network in which any Cisco WAAS device is running a software version earlier than Version 5.1.x. Directly upgrading a device from a version earlier than Version 5.5.3 to 6.2.3 is not supported.

Configuring Cisco vWAAS and Viewing vWAAS Components

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

This chapter contains the following sections:

Configuring vWAAS

This section contains the following topics:

Configuring vWAAS Settings

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

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

To configure vWAAS settings, follow these steps:

Step 1 In the vSphere Client, choose the **Console** tab and log in to the vWAAS console.

The username is **admin**, and password is **default**.

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

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

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

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

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

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

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

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

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

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

Note vWAAS registration with the Central Manager is mandatory before traffic can be optimized.

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

Configuring vWAAS Traffic Interception

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

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

Table 2-1 Traffic Interception Methods for vWAAS

Traffic Interception Method	Description
WCCP	Specifies interactions between one or more routers (or L3 switches) and one or more application appliances, web caches, and caches of other application protocols, to establish and maintain the transparent redirection of selected types of traffic. The selected traffic is redirected to a group of appliances. Any type of TCP traffic can be redirected. WCCP uses a WCCP-enabled router or L3 switch. **Note** You can configure WCCP-GRE or L2 Inline as the redirection method for vWAAS running on a UCS-E inside a Cisco ISR G2, where the UCS-E interface is configured as IP unnumbered in IOS. For more information on WCCP, see Chapter 5, "Configuring Traffic Interception" in the *Cisco Wide Area Application Services Configuration Guide*.
AppNav	A policy and class-based traffic interception method that reduces dependency on the intercepting switch or router by distributing traffic among WAAS devices for optimization. For more information on AppNav, see Chapter 4, "Configuring AppNav" and Chapter 5, "Configuring Traffic Interception" in the *Cisco Wide Area Application Services Configuration Guide*.
L2 Inline	Places the vWAAS in the data path between WAN and LAN, with an interface facing each segment to inspect and optimize the traffic as needed. For L2 Inline, traffic is forwarded directly without being sent back to the router. The vWAAS interfaces, with virtual NICs, appear as virtual interfaces in the WAAS CM for the running configuration. By default, the NICs supporting Inline mode do not appear in the running configuration when L2 Inline interception is not enabled. **Note** L2 Inline interception is available for vWAAS for RHEL KVM, for WAAS Version 6.2.1 and later. For vWAAS, L2 Inline interception does not include fail-to-wire capability. For more information on configuring L2 Inline interception on the WAAS CM, see Chapter 5, "Configuring Traffic Interception" in the *Cisco Wide Area Application Services Configuration Guide*. Table 2-2 shows the commands for configuring and displaying information on L2 Inline interception for vWAAS.

Table 2-2 CLI Commands for L2 Inline Traffic Interception

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

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

Identifying a vWAAS Device

This section has the following topics:

- Identifying a vWAAS Model

Identifying a vWAAS Model

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

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

vWAAS Model	Number of vCPUs	Maximum Number of TCP Connections
vWAAS-150	1	200
vWAAS-200	1	200
vWAAS-750	2	750
vWAAS-1300	2	1300
vWAAS-2500	4	2500
vWAAS-6000	4	6000
vWAAS-12000	4	12000
vWAAS-50000	8	50000

Identifying a vWAAS Device on the Central Manager

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

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

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

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

Identifying a vWAAS Device with the WAAS CLI

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

Table 2-5 CLI Commands for vWAAS Device Information

CLI EXEC Command	Description
show version	Displays version information about the WAAS software currently running on the vWAAS device, including date and time system last started, and the length of time the system has been running since the last reboot. • (Optional) Use **show version last** to display version information for the last saved image. • (Optional) Use **show version pending** to display version information for the pending upgraded image.
show hardware	Displays system hardware status for the vWAAS device, including: • startup date and time, the run time since startup, microprocessor type and speed, and a list of disk drives.
show tfo detail	Displays TCP Fast Open (TFO) information, including: • State—Registered or Not Registered • Default Action—Drop or Use • Connection Limit—The maximum TFO connections handled before new connection requests are rejected. • Effective Limit—The dynamic limit relating to how many connections are handled before new connection requests are rejected. • Keepalive Timeout—The connection keepalive timeout, in seconds.

vWAAS System Partitions

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

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

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

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

Operating Considerations for vWAAS and WAAS

Consider the following guidelines when using Cisco vWAAS with WAAS:

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

  If needed, change the SCSI controller type to VMware Paravirtual by following these steps:

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

vWAAS Upgrade and Downgrade Considerations

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

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

- vWAAS Upgrade and vWAAS Nodes
- vWAAS Upgrade and SCSI Controller Type
- vWAAS Upgrade and vCM-100 with RHEL KVM or KVM on CentOS
- Migrating a Physical Appliance Being Used as a WAAS CM a vCM
- vWAAS Downgrade Considerations

vWAAS Upgrade and vWAAS Nodes

When upgrading vWAAS, do not upgrade more than five vWAAS nodes at the same time on a single UCS box. Upgrading more than five vWAAS nodes at the same time may cause the vWAAS devices to go offline and to diskless mode.

vWAAS Upgrade and SCSI Controller Type

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

If needed, change the SCSI controller type to **VMware Paravirtual** by following these steps:

Step 1 Power down the vWAAS.

Step 2 From the VMware vCenter, navigate to **vSphere Client > Edit Settings > Hardware**.

Step 3 Choose **SCSI controller 0**.

Step 4 From the Change Type drop-down list, verify that the SCSI Controller Type is set to **VMware Paravirtual**. If this is not the case, choose **VMware Paravirtual**.

Step 5 Click **OK**.

Step 6 Power up the vWAAS, with WAAS Version 6.2.3, or WAAS 6.1.x or later. WAAS Version 6.1.x is the minimum version used.

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

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

- vCM-100 has default memory size of 2 GB
- vCM-100 uses the RHEL KVM or KVM on CentOS hypervisor
- You use the **restore factory-default** command or the **restore factory-default preserve basic-config** command

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

If you upgrade the vCM device to WAAS Version 6.2.3 via the console, a warning message similar to the following will be displayed:

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

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

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

To resolve this situation, follow these steps:

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

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

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

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

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

Step 1 Introduce vCM as the Standby Central Manager by registering it to the Primary Central Manager.

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

Step 3 Ensure that the Primary CM and Standby CM updates are working.

Step 4 Switch over CM roles so that vCM works as Primary CM. For additional details please refer to "*Converting a Standby Central Manager to a Primary Central Manager*" section of the WAAS Configuration Guide.

vWAAS Downgrade Considerations

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

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

Cisco vWAAS and VMware vSphere ESXi

This chapter describes how to install the VMware vSphere ESXi hypervisor for vWAAS, and contains the following section:

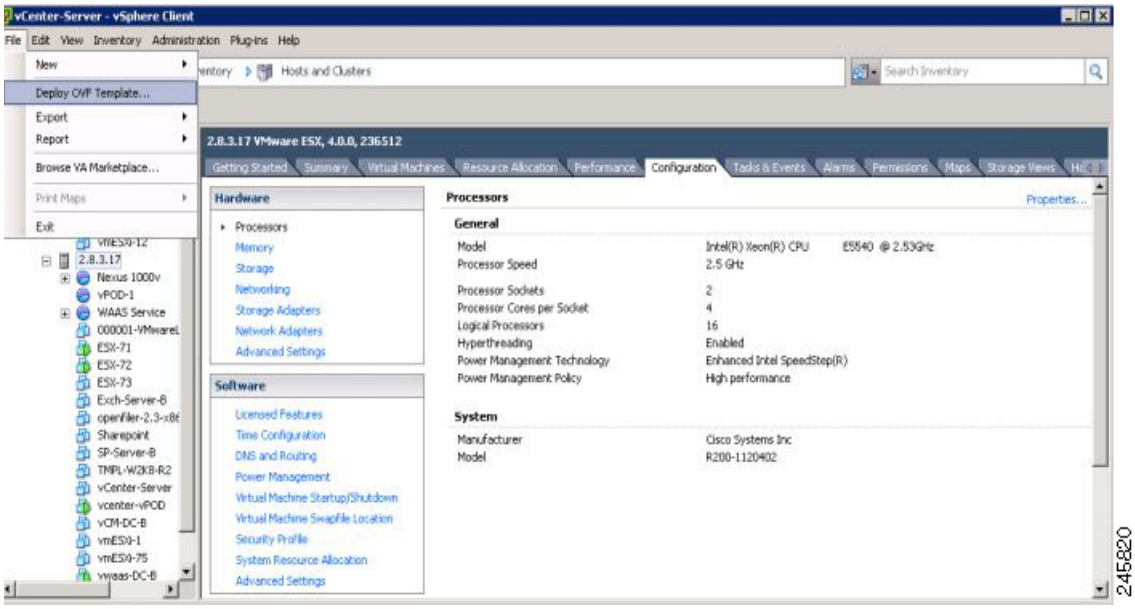
Installing Cisco vWAAS with VMware vSphere ESXi

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

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

The Source window appears.

Figure 3-1 vWAAS—Deploy OVF Template



Step 2 Click **Browse**.

The Open window appears.

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

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

  If needed, change the SCSI controller type to **VMware Paravirtual** by following these steps:

  a. Power down the vWAAS.

  b. From the VMware vCenter, navigate to **vSphere Client > Edit Settings > Hardware**.

  c. Choose **SCSI controller 0**.

  d. From the Change Type drop-down list, verify that the SCSI Controller Type is set to **VMware Paravirtual**. If this is not the case, choose **VMware Paravirtual**.

  e. Click **OK**.

  f. Power up the vWAAS, with WAAS Version 6.1.x or later.

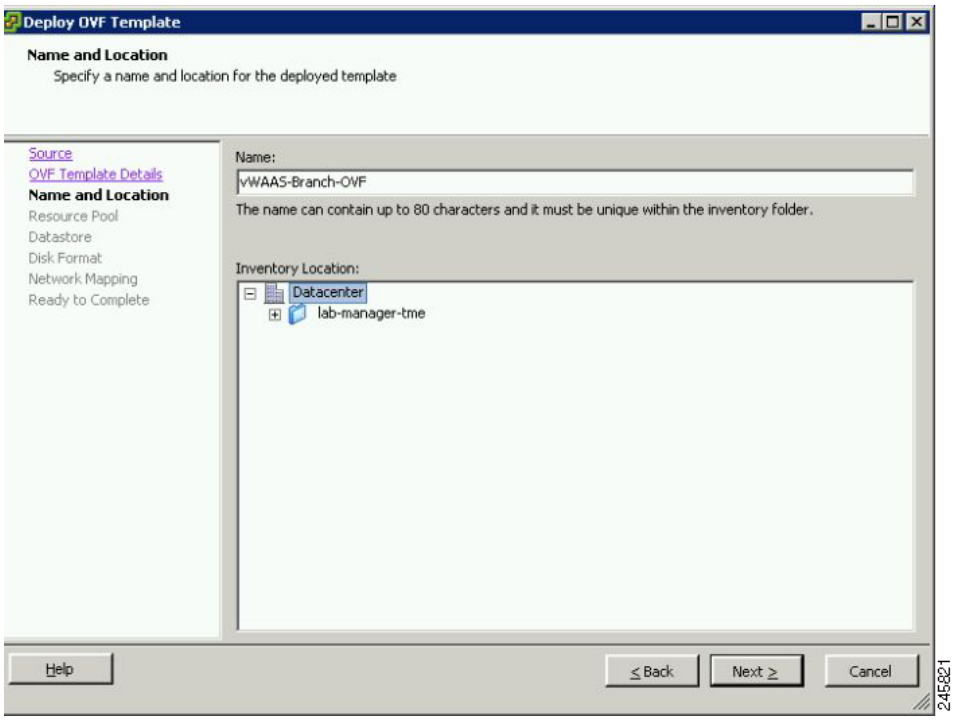
Step 4 Click **Next** to accept the selected OVA file.

The Name and Location window appears.

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

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

Figure 3-2 vWAAS—Name and Data Center Location

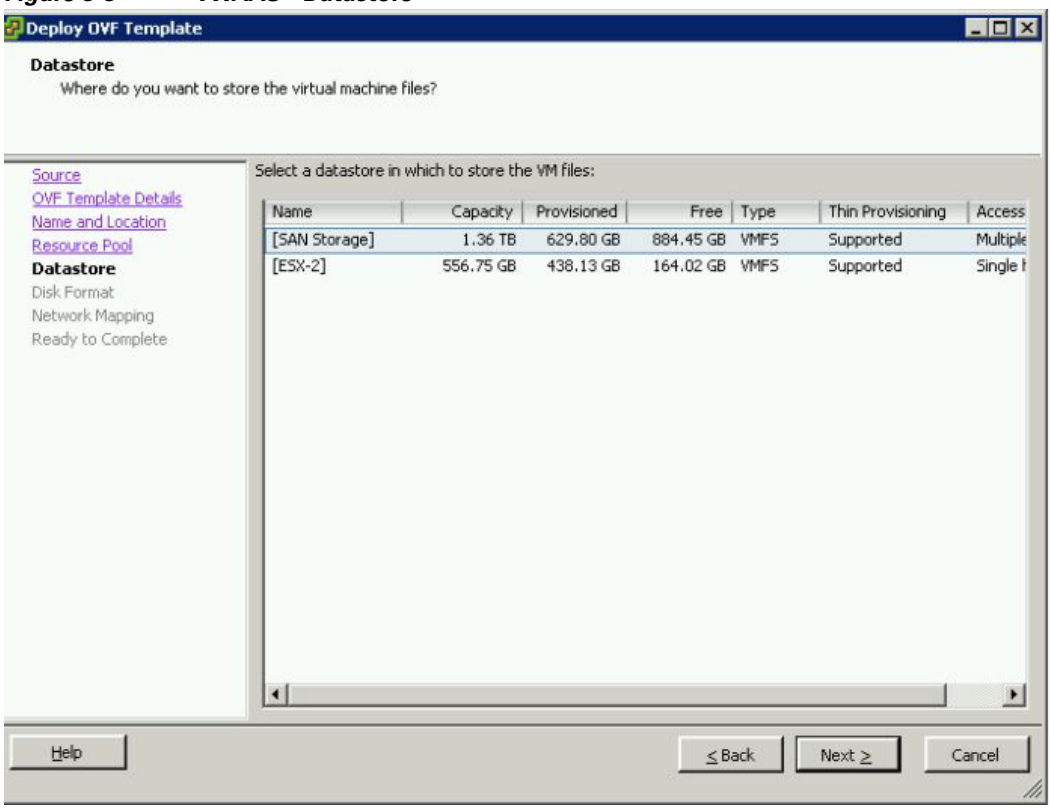


Step 6 If configured, choose a cluster for the vWAAS VM or, if configured, choose the resource pool and then click **Next**.

The Datastore window appears.

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

Figure 3-3 vWAAS - Datastore



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

The Create a Disk window appears.

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

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

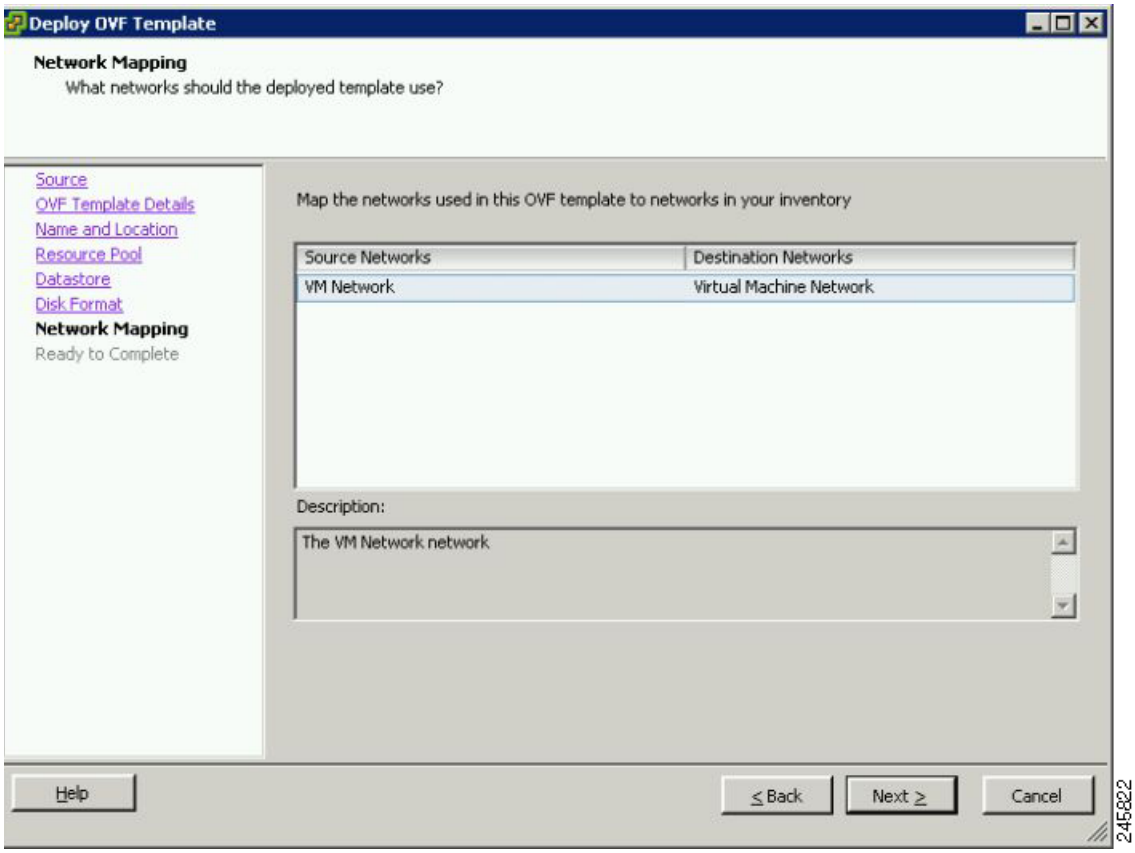
Step 9 Click **Next**.

The Network Mapping window appears.

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

The Ready to Complete window appears.

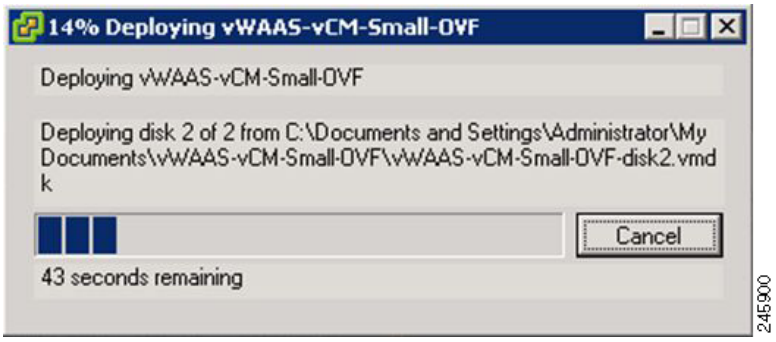
Figure 3-4 vWAAS—Network Mapping



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

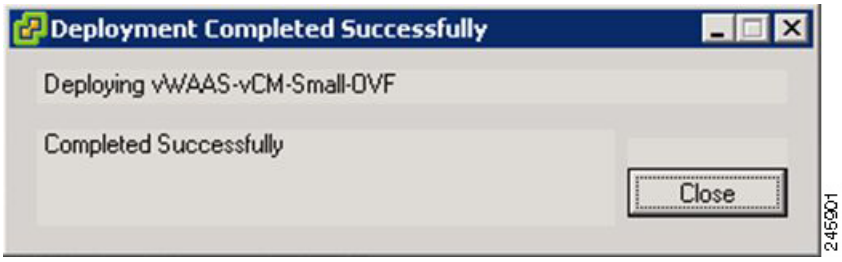
The status window appears while the OVA file is being deployed.

Figure 3-5 vWAAS—Status Window



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

Figure 3-6 vWAAS—Completed

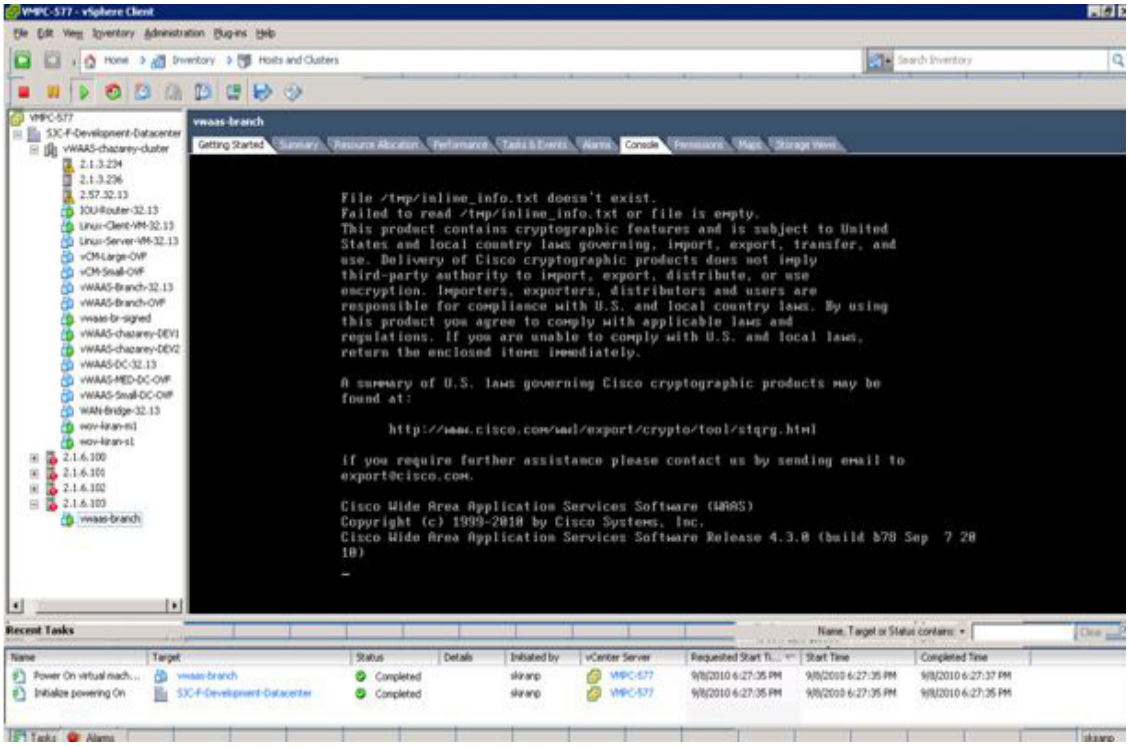


Step 13 Click **Close**.

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

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

Figure 3-7 vWAAS—Console



Note Under rare conditions, the vWAAS VM may boot into diskless mode if other VMs on the host VM server do not release control of system resources or the physical disks become unresponsive. For information on how to resolve this situation, see Resolving Diskless Startup and Disk Failure in Chapter 8, "Troubleshooting Cisco vWAAS."

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

Cisco vWAAS on KVM

This chapter contains the following sections:

About Cisco vWAAS on KVM

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

Consider the following about Cisco vWAAS on RHEL KVM:

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

Note The CDP protocol is not supported for Open Virtual Switch (OVS) on RHEL KVM on CentOS, therefore the **show cdp** command cannot be used for vWAAS on RHEL KVM on CentOS.

- The network and disk paravirtualized drivers are common to ISR-WAAS. For more information on resource allocation for vWAAS and vCM models, see ESXi Server Datastore Memory and Disk Space for vWAAS and vCM Models in Chapter 1, “Introduction to Cisco vWAAS.”

Note All general vWAAS features are supported, but some features specific to ISR-WAAS, such as ONE-P integration, are not supported.

- Resource configurations (vCPU, memory, disk) use the profiles from vWAAS that support number of connections of vWAAS models 150, 200, 750, 1300, 2500, 6000, 12000, and 50000, and that support number of managed nodes of vCM models 100, 500, 1000, and 2000. vWAAS-150 supported on Cisco EHWIC (Enhanced High-Speed WAN Interface Card) and NIM modules.
- For vWAAS with WAAS Version 6.2.3x and later, there is inline vWAAS support for the OVS switch, with additional settings in vWAAS. For example

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

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

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

   ```
   virtualport type='openvswitch'/
   ```
8. Sample output:

```
<interface type='bridge'>
      <mac address='52:54:00:ea:3f:7b'/>
      <source bridge='br2'/>
      <virtualport type='openvswitch'/>
      <model type='virtio'/>
     <address type='pci' domain='0x0000' bus='0x00' slot='0x08' function='0x0'/>
    </interface>
<interface type='bridge'>
      <mac address='52:54:00:7f:7c:99'/>
      <source bridge='br3'/>
      <virtualport type='openvswitch'/>
      <model type='virtio'/>
     <address type='pci' domain='0x0000' bus='0x00' slot='0x0a' function='0x0'/>
    </interface>
```

System Requirements for vWAAS on KVM

vWAAS on RHEL KVM has a predefined configuration with specific requirements for CPU and memory. However, there are some features that are customizable. Table 4-1 shows the supported configuration for vWAAS on RHEL KVM, and, where applicable, highlights the customizable features.

Note Data disk size will vary according to the model shown in Table 7-4, "Hardware Requirements for vWAAS with Akamai Connect". While deploying RHEL KVM, Cisco vWAAS/vCM needs to verify that enough disk space is available in the respective partition.

Table 4-1 vWAAS on RHEL KVM Supported Configuration

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

Installing Cisco vWAAS on KVM

This section contains the following topics:

Cisco vWAAS on KVM Installation Files

Cisco vWAAS on RHEL KVM is deployed as a tar archive (tar.gz). Table 4-2 shows the files included for deploying Cisco vWAAS on RHEL KVM, and for deploying Cisco vWAAS on NFVIS (Network Function Virtualization Infrastructure Software). For more information on Cisco NFVIS and Cisco NFV (Network Function Virtualization), see the *Cisco Enterprise Network Functions Virtualization Solution Overview*.

Table 4-2 Installation Files for RHEL KVM and NFVIS Deployments

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

Using the Launch Script to Deploy vWAAS on KVM

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

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

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

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

Step 4 To extract the **tar.gz** gzip file, use the **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 To launch vWAAS, run the **launch.sh** script:

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

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

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

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

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

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

Step 6 The vWAAS is launched

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

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

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

Step 10 To undefine the vWAAS:

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

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

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

Using the EzDeploy Script to Deploy vWAAS on KVM on UCS-E

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

The following are prerequisites for launching the EzDeploy script:

- To launch the vWAAS VM, you must have root permission.
- The following software and utility packages must be installed before using the EzDeploy script:
  - QEMU
  - Libvirt

  - Genisoimage
  - Expect script (required only if you choose to run EzDeploy's capability for auto-monitoring WAAS CM registration status)
- Verify the following:
  - There is enough disk and RAM memory to deploy another vWAAS.
  - Compatibility of software versions.
  - Availability and readiness of network connectivity.

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

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

Step 1 Launch the vWAAS VM.

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

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

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

The contents of the tar.gz file are:

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

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

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

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

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

    If you provide the vWAAS' bootstrap configuration, vWAAS' host name is set and used in both instances.
  - vWAAS' local IP address and mask
  - Default GW IP address: an address on the ISR-4000 series RP reachable by the vWAAS and having external network connectivity
  - IP address of the WAAS CM with which the vWAAS will register

- One NTP server address, without authentication. If you want to have authentication or multiple NTP servers, use the WAAS CM to configure these after the vWAAS is powered up.
- (Optional) DNS server address

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

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

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

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

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

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

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

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

g. To undefine the vWAAS:

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

Traffic Interception Guidelines for vWAAS on KVM

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

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

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

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

Downgrade Consideration for vWAAS on KVM

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

vWAAS in Cisco Enterprise NFV

This section has the following topics:

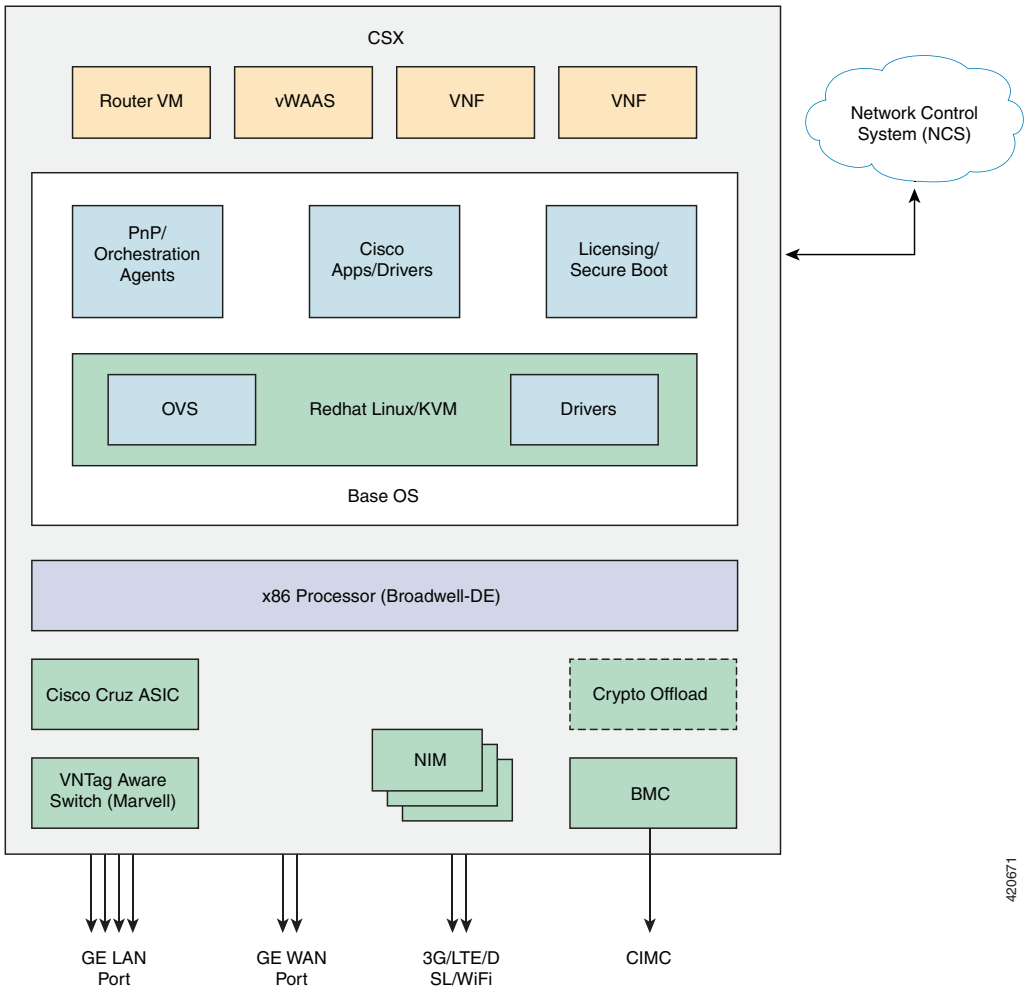
About vWAAS in Cisco Enterprise NFV

Cisco Enterprise Network Functions Virtualization (NFV) converts your critical network functions into software, making it possible to deploy services in minutes, and to create multiple virtual branch offices at once. Cisco Enterprise NFV also reduces your number of network appliances, decreases management complexity, and shrinks real estate requirements.

vWAAS in the Cisco Enterprise NFV (Network Functions Virtualization) solution offers enterprise customers the ability to virtualize the WAN optimization solution on top of x86 host platforms, USC E-Series server module the Cisco 4000 Series Integrated Services Routers (ISR), or on the Cisco ENCS Series.

As shown in Figure 4-1, vWAAS operates as a Virtual Network Function (VNF) within the Cisco Enterprise NFV.

Figure 4-1 vWAAS as VNF in Cisco Enterprise NFV



Operating Considerations for vWAAS in Cisco Enterprise NFV

Consider the following for vWAAS in Cisco Enterprise NFV:

- vWAAS must run on the NFV operating system based on Linux CentOS 7.2 or 7.3, depending on Cisco NFVIS version used.
- As part of Day 0 configuration, vWAAS supports configuration drive for Day 0 configuration, and supports specifying device IP, IP default gateway, Central Manager IP address, hostname, and NTP addresses.
- vWAAS supports WCCP and AppNav-XE traffic interception methods.
- vWAAS supports all existing vWAAS functionality per WAAS Version 6.2.1 and later.
- All vWAAS models are supported for Cisco Enterprise NFV, provided enough resources are available to deploy.
- vCM models are not supported for Cisco Enterprise NFV.

Cisco Enterprise NFV Features

This section describes the following Cisco Enterprise NFV features:

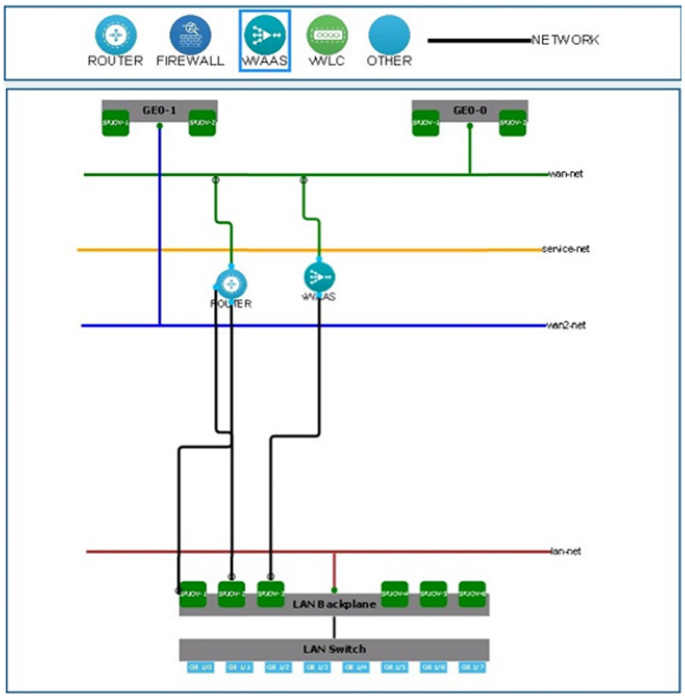
- Enterprise NFV Hosting Platforms and Host OS
- Enterprise NFV VNFs and Applications
- Enterprise NFV Service Chaining
- Enterprise NFV Orchestration and Management

Enterprise NFV Hosting Platforms and Host OS

This section describes features of the hosting platform and host operating system (OS) provided by Cisco Enterprise NFV.

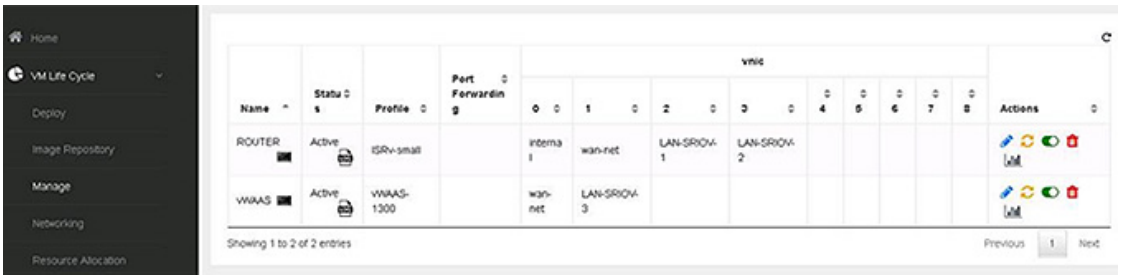
- Figure 4-2 shows a typical deployment of vWAAS in Cisco Enterprise NFV.

Figure 4-2 Typical Deployment of vWAAS in Cisco Enterprise NFV



- Use the NFVIS portal to log in to vWAAS on NFVIS. Navigate to VM Life Cycle > Manage > vWAAS Instance. Figure 4-3 shows the menu options and vWAAS instance.

Figure 4-3 vWAAS on NFVIS Login Path and vWAAS Instance



- Hosting Platforms—The Cisco Enterprise NFV hosting platform provides the hardware resources to run virtualized network functions and applications. Supported hosting platforms include:
  - Standard x86 server such as the UCS C-Series
  - ISR-4000 Series router with integrated UCS E-Series module
  - ENCS platform
- Host Operating System (OS)—Network Functions Virtualization Infrastructure Software (NFVIS) delivers the host OS functionality. NFVIS builds on top of a KVM Linux environment, with added plug-and-play (including device authentication), local GUI, and VNF and application life-cycle management capabilities.

  For a complete description of the Cisco Enterprise NFV Hardware and NFVIS requirements, see the *Cisco Enterprise Network Function Virtualization Infrastructure Software Configuration Guide*.

Note MacVTAP for VM-VM traffic is not supported for Cisco Enterprise NFV.

Enterprise NFV VNFs and Applications

With Cisco Enterprise NFV, there are two types of functions that can be virtualized in the branch, VNFs—such as routing, firewall, NAT, caching, WAN optimization, and applications—such as printer servers and LDAP servers.

Support for VNFs and applications also includes support for third-party (non-Cisco) networking functions and applications, so that even a multi-vendor branch environment that is based applications from different vendors can be simplified by consolidating these functions in software on a single x86 host platform.

Enterprise NFV Service Chaining

Service chaining, also known as service function chaining, orchestrates flows through several virtual switches in the host system. Rather than executing multiple features onto a packet flow in one functional block, the features are chained and successively applied to the packet flow. This allows for more granular services, and for easier functional configuration and management, fostering a multi-vendor VNF environment.

For service chaining on Cisco Enterprise NFV, the following features are also supported:

- Traffic Interception—Layer 2 or Layer 3 packet interception by WCCP or AppNav
- Bridged Service Chaining—VLAN or Ethernet support for bridged service chaining

Enterprise NFV Orchestration and Management

You can manage and orchestrate the Cisco Enterprise NFV solution with the Enterprise Services Automation (ESA). The ESA upon APIC-EM and Prime Infrastructure. Orchestration takes on the task of onboarding a new functionality into the branch, whether or not the branch is being activated from scratch.

There are two types of management for Cisco Enterprise NFV:

- vWAAS as a VNF running on NFVIS
- WAAS management as an optimizer

Any VNF or application onboarded onto an Enterprise NFV solution interfaces with the host at different levels, including the following:

- Physical—CPU, memory, storage
- OS—Linux version, file formats
- Network Interface—packet drivers, Layer 2 frame formats, Layer 3 packet formats
- Management—management interfaces, failure detection and reporting, statistics reporting

The orchestration and management feature also addresses Day 1 configuration and Day 2 ongoing management.

Table 4-3 shows the drivers supported for Cisco Enterprise NFV, and Table 4-4 shows the interfaces supported.

Table 4-3 Drivers Supported for Cisco Enterprise NFV

Driver Support	Description
Supported drivers	• NFVIS—VirtIO • CSP 2100—VirtIO and e1000
Driver version	• Must work under QEMU and Libvirt
Virtio	Must be compatible with QEMU or Libvirt.
Intel NICs	ENCS—Intel XL710; i350 (WAN for ENCS) UCS—Intel i350, Broadcom 5709
SR-IOV support for WAN-connected VNFs	UCS—Intel VF Drivers: IGBVF ENCS—Intel VF Drivers: IGBVF
SR-IOV support for ENCS (for VM-VM hardware offload)	Intel VF Drivers: i40evf
PCIe Pass-through support for WAN-connected VNFs	UCS—Intel VF Drivers: IGB ENCS—Intel VF Drivers: IGB
(Optional) Support for NICs	• UCS—Intel i350, Broadcom 5709, Cisco eNIC • ENCS—Intel XL710; i350 (WAN for ENCS) • CSP 2100—Intel i350, Intel X520, Intel XL710

Driver Support	Description
(Optional) For WAN-connected VMs	• SR-IOV – UCS—Intel i350, Broadcom 5709, Cisco eNIC – ENCS—Intel VF Drivers: IGBVF – CSP 2100—Intel VF Drivers: IGBVF, i40evf • PCIe-Pass Through support – UCS—Intel i350, Broadcom 5709, Cisco eNIC – ENCS—Intel VF Drivers: IGBVF – CSP 2100— •
(Optional) For VM-VM hardware offload	• SR-IOV – UCS—N/A – ENCS—Intel VF Drivers: i40evf – CSP 2100—Intel VF Drivers: IGBVF, i40evf

Table 4-4 Interfaces Supported for Cisco Enterprise NFV

Interface Support	Description
Maximum number of vNIC adapters per VNF (excluding Management)	NFVIS: 8 CSP 2100: 10
Minimum number of vNIC adapters per VNF	1
Maximum number of MAC addresses per VNF	256
Maximum number of VLANs	64
Layer 2 Ethernet Frames accepted	UCS • OVS: Any frame supported by OVS • SR-IOV—Any supported frame format ENCS • OVS: Any frame supported by OVS • SR-IOV—Any supported frame format ENCS • OVS: Any frame supported by OVS • SR-IOV—Any supported frame format

Interface Support	Description
Support for Ethernet Frame sizes greater than 1518 B	UCS • OVS—Allowed • SR-IOV—Allowed ENCS • OVS—Allowed • SR-IOV—Allowed **Note** VMs and applications must support path MTU discovery for frame sizes greater than 1518 B.
Number of IP Addresses (without management)	64*4
Data Plane Development Kit (DPDK) support	UCS—Allowed ENCS—Allowed CSP 2100—Not allowed

Cisco Enterprise NFV Licensing

Consider the following guidelines for Cisco Enterprise NFV licensing:

- For Cisco VNFs, the licensing model we recommend is Smart-Licensing. To streamline deployment, we recommend that VNFs support licensing configuration via Day-0 bootstrapping.
- VMs are independently licensed. NFVIS generates each VM with a Unique Universal ID (UUID).

Cisco vWAAS on Microsoft Hyper-V

This chapter describes how to install and use Cisco vWAAS on the Microsoft Hyper-V hypervisor.

This chapter contains the following sections:

About Cisco vWAAS on Microsoft Hyper-V

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

Hyper-V is a hypervisor-based server-virtualization product that improves utilization, consolidates server workloads, and reduces costs. To achieve this, vWAAS on Hyper-V uses hardware virtualization to enable multiple operating systems to run on a single host, and allows the operating systems to share the same underlying physical hardware.

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

vWAAS on Hyper-V Deployments

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

- Standalone role in the Hyper-V server—Hyper-V Server 2012 or Hyper-V Server 2012 R2
- In installable product in the Windows server—Windows Server 2008 R2, Windows Server 2012 or Windows Server 2012 R2.

This section contains the following topics:

Operating Guidelines for vWAAS on Hyper-V

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

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

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

Platforms Supported for vWAAS on Hyper-V

This section shows the platforms supported for vWAAS on Microsoft Hyper-V:

- Table 5-1 shows vWAAS support for the Microsoft Hyper-V servers and SCVMM (System Center Virtual Machine Manager).
- Table 5-2 shows platforms supported for vWAAS on Microsoft Hyper-V, deployed as a standalone or installable product.

Table 5-1 vWAAS Support for Microsoft Hyper-V Servers and SCVMM

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

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

Table 5-2 Platforms Supported for vWAAS on Microsoft Hyper-V, as a Standalone or Installable Product

Standalone Product in Hyper-V Server		*Installable Product in Windows Server*
Hyper-V Server 2008 R2	**Hyper-V Server 20012 or 2012 R2**	**Windows Server 2012 or 2012 R2**
UCS E-Series and UCS servers	UCS E-Series and UCS servers	UCS E-Series and UCS servers
vCM-100	vCM-100	vCM-100
vCM-500	vCM-500	vCM-500
vCM-1000	vCM-1000	vCM-1000
vCM-2000	vCM-2000	vCM-2000
vWAAS-150 (For WAAS Version 6.2.1 and later, supported on Cisco EHWIC and NIM.)	vWAAS-150 (For WAAS Version 6.2.1 and later, supported on Cisco EHWIC and NIM.)	vWAAS-150 (For WAAS Version 6.2.1 and later, supported on Cisco EHWIC and NIM.)
vWAAS-200	vWAAS-200	vWAAS-200
vWAAS-750	vWAAS-750	vWAAS-750
vWAAS-1300	vWAAS-1300	vWAAS-1300
vWAAS-2500	vWAAS-2500	vWAAS-2500
vWAAS-6000	vWAAS-6000	vWAAS-6000
vWAAS-12000	vWAAS-12000	vWAAS-12000
	vWAAS-50000	vWAAS-50000

Interoperability Support

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

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

vWAAS on Hyper-V Requirements

This section contains the following topics:

System Infrastructure Requirements

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

- Microsoft Hyper-V Hypervisor—Hypervisor enables multiple operating systems to run on a single host. vWAAS runs as a guest on any host running Hyper-V 2008 R2 or greater.

- Hyper-V Virtual Switch—The Hyper-V Virtual Switch is a software-based Layer 2 switch that connects virtual machines to both virtual networks and the physical network. It provides policy enforcement for security, isolation, and service levels, and includes features for tenant isolation, traffic shaping, simplified troubleshooting, and protection against malicious virtual machines.

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

Hardware Virtualization

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

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

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

- Disk sizes for vWAAS on Hyper-V— Disk sizes for vWAAS on Hyper-V are the same as those for ESXi, for each model. For more information on disk sizes for WAAS versions up to v6.x, see Table 1-18, "vCPUs, ESXi Server Datastore Memory, and Disk Space by vWAAS Model".
- CD-ROM—vWAAS on Hyper-V supports standard ISO image file for its CD-ROM device.
- Flash—Unlike physical WAAS devices, vWAAS on Hyper-V does not have access to a separate flash device. Instead, vWAAS flash is installed on the first hard disk, and also uses this first disk for booting. A separate larger disk hosts the DRE/CIFS caches, etc. Other flash functionalities are supported as in ESXi.

Installing vWAAS on Hyper-V

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

This section contains the following topic:

- Installing vWAAS on Hyper-V with a VHD Template
- Configuring GPT Disk Format for vWAAS-50000 on Hyper-V with Akamai Connect

Installing vWAAS on Hyper-V with a VHD Template

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

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

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

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

Step 2 Unzip the vWAAS package.

Step 3 Login to the SCVMM console.

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

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

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

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

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

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

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

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

b. The NUMA Configuration screen is displayed.

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

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

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

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

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

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

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

Step 1 Install windows in one partition of the HDD.

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

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

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

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

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

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

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

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

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

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

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

Activating and Registering vWAAS on Hyper-V

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

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

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

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

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

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

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

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

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

- If Hyper-V vWAAS cannot register with the WAAS CM, it generates an alarm and does not optimize connections. Contact Cisco Technical Support (TAC) if you need assistance to resolve this situation.

- Hyper-V vWAAS may register successfully with the WAAS CM, but lose connectivity due to a shutdown or power off. If it remains functional, vWAAS will continue to optimize connections in the offline state.
- If you de-register the Hyper-V vWAAS (with the **cms deregister** EXEC command), it is removed from service.

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

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

Operating Considerations for vWAAS on Hyper-V

This section has the following topics:

Configuring NTP Settings for vWAAS on Hyper-V

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

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

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

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

From the SC VMM:

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

From the Hyper-V Manager:

a. Select **vWAAS VM**.

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

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

d. Click **OK**.

Traffic Interception Methods for vWAAS on Hyper-V

This section has the following topics:

About Traffic Interception for vWAAS on Hyper-V

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

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

WCCP Interception

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

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

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

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

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

Interception Method Settings area

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

WCCP Settings area

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

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

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

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

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

WCCP Assignment Settings for Load Balancing area

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

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

WCCP Redirect and Egress Settings area

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

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

Advanced WCCP Settings area

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

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

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

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

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

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

Step 16 In the **Password** field, specify the password to be used for secure traffic between the WAEs within a cluster and the router for a specified service. Be sure to enable all other WAEs and routers within the cluster with the same password. Passwords must not exceed eight characters in length. Do not use the

following characters: space, backwards single quote (‘), double quote (“”), pipe (|), or question mark (?).

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

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

AppNav Controller Interception

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

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

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

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

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

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

Step 4 Click **Submit**.

Hyper-V High Availability Features

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

- Live Migration
- NIC Teaming

Live Migration

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

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

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

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

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

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

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

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

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

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

NIC Teaming

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

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

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

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

Cisco vWAAS in Microsoft Azure

This chapter describes how to provision, deploy, and verify Cisco vWAAS in Microsoft Azure.

This chapter contains the following sections:

About Cisco vWAAS in Microsoft Azure

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

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

This section contains the following topics:

Platforms Supported for Cisco vWAAS in Microsoft Azure

The following platforms are supported for Cisco vWAAS in Microsoft Azure:

- vWAAS in Azure is available for vWAAS Version 6.2.1x and later, and is supported for vWAAS-200, vWAAS-750, vWAAS-1300, vWAAS-2500, vWAAS-6000, and vWAAS-12000v.
- vWAAS in Azure is not currently supported for vWAAS-50000.

Table 6-1 Microsoft Azure VM Sizes for Cisco WAAS vWAAS Models

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

Operating Considerations for Cisco vWAAS in Microsoft Azure

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

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

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

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

- Registering the vWAAS in Azure to the WAAS Central Manager:
  - If you register the vWAAS with the WAAS Central Manager using a private IP address, following the usual vWAAS registration process described in Configuring vWAAS Settings of Chapter 2, “Configuring and Cisco vWAAS and Viewing vWAAS Components.
  - If you register the vWAAS with the WAAS Central Manager using a public IP address, you must specify the public address of the vWAAS in the WAAS Central Manager Device Activation screen (navigate to **Devices >** *device-name* **> Activation**).

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

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

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

Operating Limitations for Cisco vWAAS in Microsoft Azure

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

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

  Functionality similar to auto-registration is available by providing the WAAS CM IP address during VM provisioning. The vWAAS VM will try to register with this WAAS CM during provisioning.

- Microsoft Azure does not support GRE, IPv6, or Jumbo Frames, therefore vWAAS in Azure does not support these features.

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

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

Upgrade/Downgrade Considerations for Cisco vWAAS in Microsoft Azure

Note the following upgrade/downgrade considerations for Cisco vWAAS in Microsoft Azure:

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

Deployment Options for Cisco vWAAS in Miscrosoft Azure

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

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

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

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

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

Provisioning the vWAAS VM in Microsoft Azure

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

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

Step 1 Login to the Microsoft Azure portal.

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

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

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

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

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

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

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

Table 6-2 Microsoft Azure VM Sizes for Cisco WAAS vWAAS Models

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

Note Use the Microsoft Azure Tier field to select an Azure VM for the vWAAS models shown in Table 6-2. For vWAAS-6000 and vWAAS-12000, you must use the template to specify the Azure VM. For more information, see Deploying vWAAS in Microsoft Azure. For Azure VM sizes for vWAAS-6000 and vWAAS-12000, see Table 6-1.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Step 20 In the Endpoints section:

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

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

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

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

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

Step 23 Select the vWAAS VM.

Step 24 Attach the data disks. See Table 6-2 for data disk sizes for Azure VMs.

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

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

Deploying vWAAS in Microsoft Azure

This section has the following topics:

Deploying vWAAS VM and Data Disk with the VHD Template

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

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

The AzCopy command parameters are:

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

Step 2 Use the template to deploy the vWAAS VM.

The vWAAS VM is deployed with the data disk.

Step 3 Log in with your username and password.

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

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

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

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

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

Step 3 Use the template to deploy the vWAAS VM.

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

Step 5 Paste the template here.

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.

Step 9 The vWAAS VM is deployed.

Step 10 Log in with your username and password.

Step 11 (Optional) To verify deployment details such as CMS registration and WAAS Central Manager address, see Verifying the vWAAS in Azure Deployment.

Deploying vWAAS VM Using Windows Powershell

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

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

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

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

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

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

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

Step 6 Use the **New-AzureRmResourceGroup -Name $RGName -Location $locName** Powershell command to create the resource group.

Step 7 Use the **New-AzureRmResourceGroupDeployment** Powershell cmdlet to deploy vWAAS in Azure. To complete the deployment, specify values for the following parameters:

- userImageStorageAccountName
- userImageStoragContainerName
- userImageVhdName
- osType
- vmName
- adminUserName
- adminPassword

Step 8 After you enter these parameters, vWAAS in Azure is deployed. The system displays provisioning information, including deployment name, provisioning state, date/time, and mode.

Step 9 Log in with your username and password.

Step 10 (Optional) To verify deployment details such as CMS registration and WAAS Central Manager address, see Verifying the vWAAS in Azure Deployment.

Verifying the vWAAS in Azure Deployment

Table 6-3 provides a checklist for verifying the vWAAS VM deployment in Microsoft Azure.

Table 6-3 Checklist for Verifying the vWAAS in Azure Deployment

Task	Description
Viewing vWAAS in Azure vWAAS devices	• On the WAAS Central Manager, navigate to the **Manage Devices** screen. The vWAAS in Azure device type is displayed as **OE-VWAAS-AZURE**. • On the WAAS CLI, use either the **show version** EXEC command or the **show hardware** EXEC command. Output for both commands will include device ID, shown as **OE-VWAAS-AZURE**.
Viewing Boot Information and Diagnostics	On the Azure portal, navigate to **Virtual Machines > VM > Settings > Boot Diagnostics** on the Azure portal.
Verifying CMS Registration	If the Centralized Management System (CMS) is enabled, use the **show cms device status** *name* command to display status for the specified device or device group. **Note** After you have registered the vWAAS in Azure device to the WAAS Central Manager, you must configure the public IP address of the Central Manager. The vWAAS in Azure device can contact the Central Manager only by using the public IP address of the registration. To set the public IP address of the WAAS Central Manager: 1. In the WAAS Central Manager, navigate to **Home > Devices >** *Primary-CM-Device* **> Configure > Network > NatSettings**. 2. In the NAT IP field, enter the public IP address of the Central Manager.
Verifying WAAS Central Manager Address	Use the **show running-config** command to display information about all WAAS device.

Note Whenever ARP cache(s) are cleared or the vWAAS is rebooted, packets may not be forwarded to the next hop in Azure cloud. To ensure that packets are successfully forwarded, use the **ping** EXEC command to update the ARP cache table.

Cisco vWAAS with Akamai Connect

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

This chapter contains the following sections:

About Cisco vWAAS with Akamai Connect

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

Supported Platforms for Cisco vWAAS with Akamai Connect

Table 7-1 shows supported vWAAS models for Akamai caching up to 6,000 connections. Table 7-2 shows supported vWAAS models for Akamai caching beyond 6,000 connections, and disk and memory requirements for Akamai caching beyond 6,000 connections

Table 7-1 Supported vWAAS Models for Akamai Caching up to 6,000 Connections

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

Table 7-2 Supported vWAAS Models and Memory/Disk Requirements for Akamai Connect beyond 6,000 Connections

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

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

Cisco vWAAS with Akamai Connect License

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

Table 7-3 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 7-3 is dependent on the hardware module on which WAAS is running.

Table 7-3 Licenses for Cisco IWAN with Akamai Connect with vWAAS

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

Cisco vWAAS with Akamai Connect Hardware Requirements

Table 7-4 shows the hardware requirements for Cisco UCS (Unified Computing System) E-Series and ISR-WAAS (Integrated Services Router-WAAS) for vWAAS with Akamai Connect.

Note For information on hardware requirements for vWAAS with Akamai Connect on Hyper-V, see Configuring GPT Disk Format for vWAAS-50000 on Hyper-V with Akamai Connect.

Table 7-4 Hardware Requirements for vWAAS with Akamai Connect

Cisco vWAAS or WAAS Model	Memory Required for vWAAS with Akamai Connect	Disk Required for vWAAS with Akamai Connect
vWAAS-150	4 GB	160 GB
vWAAS-200	4 GB	260 GB
vWAAS-750	4 GB	500 GB
vWAAS-1300	6 GB	600 GB
vWAAS-2500	8 GB	750 GB
vWAAS-6000	11 GB	900 GB
vWAAS-12000	18 GB	1500 GB

Cisco vWAAS or WAAS Model	Memory Required for vWAAS with Akamai Connect	Disk Required for vWAAS with Akamai Connect
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 7-7 shows the WAAS Mid to High End Platform Cache Engine Memory Requirements. Table 7-8 shows the WAAS Mid to High End Platform Cache Engine Cache Disk Requirements.

Upgrading vWAAS Memory and Disk for Akamai Connect

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

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

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

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

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

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

Before using this procedure, note the upgrade paths for WAAS Version 6.2.3 shown in Table 7-5. For complete upgrade instructions, see the *Release Note for Cisco Wide Area Application Services*.

Table 7-5 Upgrade Paths for WAAS Version 6.2.3

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

Step 1 Power off the vWAAS.

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

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

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

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

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

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

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

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

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

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

Step 9 Click **Finish**.

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

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

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

Upgrading vWAAS Memory and Disk for vWAAS-12000 with ESXi

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

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

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

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

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

Step 3 Increase the size of the RAM.

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

Step 4 Power on the vWAAS VM.

Step 5 Check the alarms.

The filesystem_size_mism alarm will be raised:

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

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

1 filesystem_size_mism    disk                      Filesystem size
```

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

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

Step 7 Reload.

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

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

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

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

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

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

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

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

Step 3 Increase the size of the RAM.

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

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

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

Step 5 Power on the vWAAS VM.

Step 6 Check the alarms.

The filesystem_size_mism alarm will be raised:

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

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

1 filesystem_size_mism    disk                      Filesystem size
```

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

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

Step 8 Reload.

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

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

Cisco vWAAS-150 with Akamai Connect

For WAAS Version 6.1.1 and later, vWAAS-150 on ISR-WAAS is supported for Akamai Connect (AKC). For WAAS Version 6.2.1 and later, vWAAS-150 is also supported for RHEL KVM (Chapter 4, Cisco vWAAS on KVM) and Microsoft Hyper-V (Chapter 5, "Cisco vWAAS on Microsoft Hyper-V").

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

Table 7-6 displays the profile of the vWAAS-150.

Table 7-6 vWAAS-150 Profile

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

WAAS Central Manager and Cisco vWAAS-150

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

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

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

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

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

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

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

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

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

For vWAAS-12000 and vWAAS-50000, you must allocate Cache Engine cache disk resources. Cache disk requirements are shown in Table 7-8.

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

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

Table 7-8 WAAS Mid to High End Platform Cache Engine Cache Disk Requirements

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

Troubleshooting Cisco vWAAS

This chapter describes how to identify and resolve operating issues with Cisco vWAAS.

This chapter contains the following sections:

Resolving Diskless Startup and Disk Failure

Under rare conditions, the vWAAS VM may boot into diskless mode if other VMs on the host VM server do not release control of system resources or the physical disks become unresponsive. The vWAAS device raises a **disk_failure** critical alarm for disk01 and the **show disk details** EXEC command shows disk01 as Not used until replaced.

To recover from this failure, follow these steps:

Step 1 Re-enable the disk.

```
vwaas# config
vwaas(config)# no disk disk-name disk00 shutdown force
vwaas(config)# exit
```

Step 2 Reload vWAAS.

```
vwaas# reload
```

Troubleshooting vWAAS Device Registration

You must register each vWAAS device with the WAAS CM. If a vWAAS device is not registered with the WAAS CM, the **`Not registered alarm`** is displayed when you use the **show alarms** command.

Figure 8-1 Display for show alarms Command: Not Registered Alarm

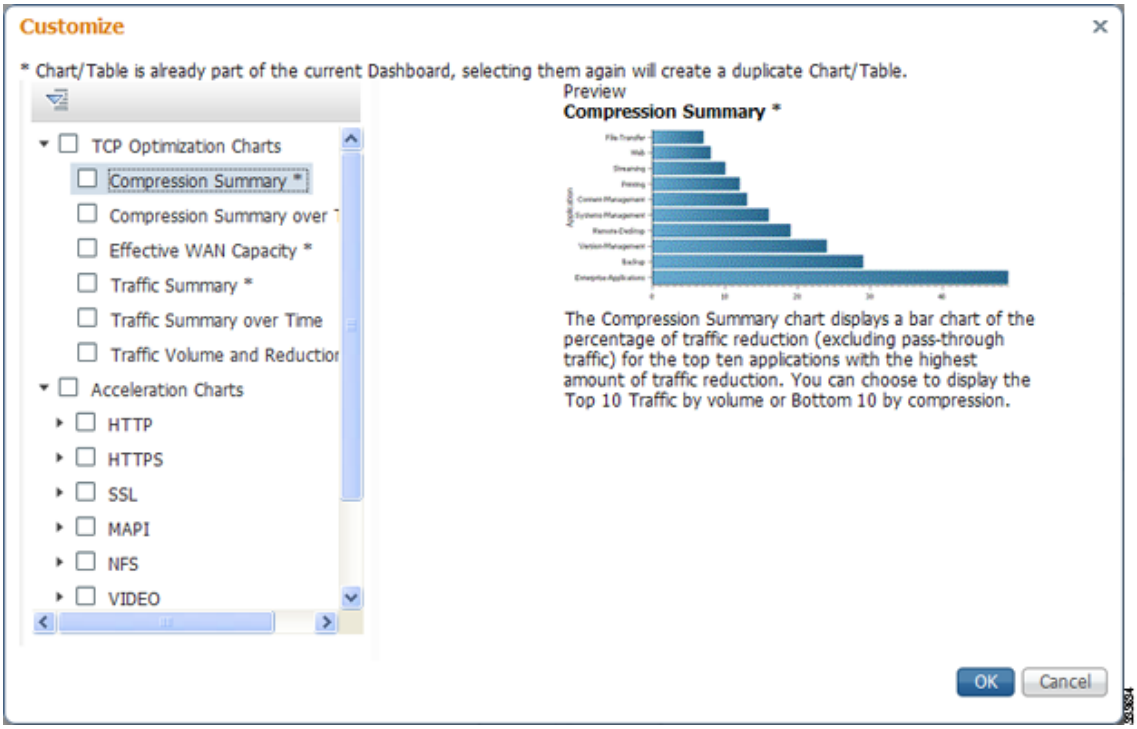
```
vWAAS# show alarms

Critical alarms:
----------------
None

Major alarms:
-------------
        Alarm ID          Module/Submodule        Instance
     -----------------    -----------------    --------------
     1 not registered       vwaas/model          vwaas/model   <----- Not registered alarm
. . .

Minor alarms:
-------------
None
```

Verifying vWAAS Virtual Interfaces

Two virtual interfaces are available on vWAAS devices, the WAAS CM and the CLI:

To show vWAAS virtual interfaces on the WAAS CM, choose ***Device*** **> Configure > Network > Network Interfaces** to display the screen shown in Figure 8-2.

Figure 8-2 Network Interfaces for Device Window



For the CLI, use the **show running-config interface** command to display the virtual interfaces. For additional details on the virtual interfaces, use the **show interface virtual 1/0** command or the **show interface virtual 2/0** command.

Troubleshooting vWAAS Networking

If you see no connections on the vWAAS device, use VMware VSphere Client to view the networking configuration and to check if the vWAAS device is connected to the correct vSwitch.

To use the VSphere Client to trace vWAAS connectivity from the device page, follow these steps:

Step 1 Identify which network label the network adapter is connected to.

Step 2 Determine the virtual switch that this network is connected to.

Step 3 Determine the physical NIC that is a member of this virtual switch.

Step 4 Verify that the configuration is correct.

Step 5 Verify that the virtual switch settings are correctly configured to reach the network.

Step 6 Verify the following on the vWAAS device: configured IP address, netmask, default gateway, and primary interface. For more information on these parameters, see Verifying vWAAS Virtual Interfaces.

Step 7 From the vWAAS device, ping the default gateway and WAAS CM to verify that they are reachable.

Troubleshooting Undersized Alarm

If the proper memory and hard disk resources are not allocated to the vWAAS device, the Undersized alarm is displayed when you use the **show alarms** command. Figure 8-3 shows sample output for the **show alarms** command for the Undersized alarm.

Figure 8-3 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 8-1 describes the fields in the **show alarms** command output.

Table 8-1 Field Descriptions for the show alarms Command

Field	Description
Critical Alarms	Critical alarms affect the existing traffic through the WAE and are considered fatal (the WAE cannot recover and continue to process traffic. **Note** WAAS and vWAAS provide three levels of alarms: critical, major, and minor. For more information on alarms and the **show alarms** command, see *Cisco Wide Area Application Services Command Reference*.
Major Alarms	Major alarms indicate a major service (such as the cache service) has been damaged or lost. Urgent action is necessary to restore this service. However, other node components are fully functional and the existing service should be minimally impacted. **Note** WAAS and vWAAS provide three levels of alarms: critical, major, and minor. For more information on alarms and the **show alarms** command, see *Cisco Wide Area Application Services Command Reference*.
Alarm ID	Type of event that caused the alarm.
Module/Submodule	The software module affected.
Instance	The object that this alarm is associated with. As shown in Figure 8-3, the instance for this alarm is *memory*. The Instance field does not have predefined values; each Instance value is application specific.

You will not see this alarm if you are using valid OVA files to deploy vWAAS. If the alarm shown in x is displayed, delete the vWAAS VM and redeploy the vWAAS VM using a valid OVA file.