Cisco vWAAS with Cisco Enterprise NFVIS

This chapter describes Cisco vWAAS with Cisco Enterprise Network Functions Virtualization Infrastructure Software (Cisco Enterprise NFVIS).

This chapter contains the following sections:

About Cisco vWAAS with Cisco Enterprise NFVIS

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

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

Cisco Enterprise NFVIS contains the following features:

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

  Cisco Enterprise NFV also provides local network management capabilities that enable you to dynamically deploy virtualized network functions such as a virtual router, firewall, and WAN acceleration on a supported Cisco device, eliminating the need to add a physical device for every network function.
- **Monitoring**: Monitors all the parameters of the deployed Cisco vWAAS, including memory, storage, and CPU, and monitors memory, storage, and CPU utilization of the Cisco vWAAS.
- **Traffic verification**: Verifies traffic flows through Cisco vWAAS by monitoring the VNF interface statistics.

- **Add-On Capability**: Ability to add vCPU, memory, and storage, to modify the networking option and add a virtual interface, to configure the virtual networking port and connect it to a VLAN.

Platforms Supported for Cisco vWAAS with Cisco Enterprise NFVIS

The following table shows the platforms and software versions supported for Cisco vWAAS with Cisco Enterprise NFVIS.

Table 1: Platforms and Software Versions Supported for Cisco vWAAS with Cisco NFVIS

PID and Device Type	Earliest Cisco WAAS Version Supported	Host Platforms	Earliest Host Version Supported	Disk Type
PID: OE-CSP Device Type: OE-CSP	6.4.3a	Cisco CSP 5000-W Series	Cisco Enterprise NFVIS 3.10.1	virtio
PID: OE-VWAAS-ENCS Device Type: OE-VWAAS-ENCS	6.4.1	Cisco ENCS 5400-W Series	Cisco Enterprise NFVIS 3.7.1	virtio
PID: OE-VWAAS-KVM Device Type: OE-VWAAS-KVM	6.2.x	Cisco UCS-E Series	Cisco Enterprise NFVIS 3.7.1	virtio

Cisco vWAAS with Cisco Enterprise NFVIS on Cisco ENCS 5400-W provides the following capabilities:

- **Enterprise Application Optimization**: Branch to branch, and branch to data center optimization of application traffic, either within or outside of a Cisco iWAN solution. This includes traditional WAAS WAN optimization functions, as well as the deployment of other iWAN solution features that are inherent in Cisco IOS-XE platforms.
- **Everything as a Service (XaaS) Optimization**: For single-sided use cases in cloud deployments, where you have control of one side of the connection, for example, branch to cloud, and data center to cloud (for backup and recovery purposes). Optimizations are applied in a unilateral fashion, without reliance on a peer.
- **Service Nodes**: A service node is a Cisco WAAS application accelerator that optimizes and accelerates traffic according to the optimization policies configured on the device. It can be a Cisco vWAAS instance or a Cisco ENCS 5400-W device.

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

- **Cisco vWAAS with Cisco Enterprise NFVIS on Cisco ENCS 5400-W** is part of Cisco iWAN: A suite of components that brings together WAN optimization, performance routing, and security levels of leased lines and MPLS VPN services to the Internet.

  Cisco vWAAS with Cisco Enterprise NFVIS on Cisco ENCS 5400-W is available for vWAAS in WAAS Version 6.4.1 and later.

- **Cisco vWAAS with Cisco Enterprise NFVIS on Cisco CSP 5000-W** is a Cisco open x86 hardware platform for deployment of Cisco datacenter Network Functions Virtualization (VNFs). Cisco CSP 5000-W Series contains an embedded KVM CentOS hypervisor, and enables you to monitor and manage the lifecycle of vWAAS on NFVIS.

  Cisco vWAAS with Cisco Enterprise NFVIS on Cisco CSP 5000-W is available for vWAAS in WAAS Version 6.4.3e and later.

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

This section contains the following topic:

About the Unified OVA Package for Cisco vWAAS on Cisco NFVIS

The following list highlights the features of the Unified OVA package for Cisco vWAAS with NFVIS for Cisco WAAS Version 6.4.1 and later.

- In Cisco vWAAS with Cisco Enterprise NFVIS in Cisco WAAS Version 6.4.x, Cisco vWAAS is deployed in a RHEL KVM hypervisor on a Cisco ENCS 5400-W Series device.
- In Cisco vWAAS with Cisco Enterprise NFVIS in Cisco WAAS Version 6.4.x and later, Cisco provides a single, unified OVA or NPE OVA package for each hypervisor type, which can be used with all Cisco vWAAS models for that hypervisor.
- Each unified OVA package file is a preconfigured VM image that is ready to run on a particular hypervisor. The launch script for each unified OVA package provides the model and other required parameters to launch Cisco vWAAS in Cisco WAAS in the required configuration.
- The following are examples of the unified OVA and NPE OVA package filenames for Cisco vWAAS with Cisco NFVIS:
  - Cisco-KVM-vWAAS-Unified-6.4.5-b-69.tar
  - Cisco-KVM-vWAAS-Unified-6.4.5-b-69-npe.tar
- The unified OVA package for Cisco vWAAS on RHEL KVM/KVM on CentOS contains the following files.
  - Flash disk image
  - Data system disk
  - Akamai disk

- **INSTRUCTIONS.TXT**: Describes the procedure for deploying the virtual instance and running the **launch.sh** file.
- **package.mf** template file and **bootstrap-cfg.xml**: These two files work together on the Cisco Enterprise NFVIS platform with the image_properties.xml file as day-zero configuration template.
- **ezdeploy.sh**: The script used to deploy Cisco vWAAS on Cisco UCS-E.
- **exdeploy_qstatus.exp**: The dependent file for **ezdeploy.sh** script.
- **image_properties.xml**: A VM configuration template file used on the Cisco Enterprise NFVIS platform.
- **launch.sh**: The launch script to deploy Cisco vWAAS on Linux KVM.
- **vm_macvtap.xml**: Configuration file for Cisco vWAAS deployment using host machine interfaces with the help of the mactap driver.
- **vm_tap.xml**: Configuration file for Cisco vWAAS deployment using the virtual bridge or OVS present in the host machine.

Operating Guidelines for the Unified OVA Package for Cisco vWAAS on Cisco NFVIS

The following models, highlighted in the following list and also listed in the Cisco WAAS sizing guides and specifically noted in Cisco WAAS, Cisco vWAAS user guides, and Cisco WAAS Release Notes, are the *only devices* we recommend for use with Cisco vWAAS:

- Cisco ENCS 5400-W Series
- Cisco CSP 5000-W Series
- Cisco UCS-C Series
- Cisco UCS-E Series
- Cisco ENCS 5100
- Cisco CSP-2100
- Cisco ISR configurations

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

For more information about supported platforms for Cisco Enterprise NFV, see the Release Notes for Cisco Enterprise Network Function Virtualization Infrastructure Software, Release 3.12.x.

Traffic Interception for Cisco vWAAS with Cisco NFVIS

Cisco vWAAS with Cisco Enterprise NFVIS on Cisco ENCS 5400-W supports WCCP traffic interception.

- WCCP specifies interactions between one or more routers and one or more Cisco WAEs, to establish and maintain the transparent redirection of selected types of traffic in real time. The selected traffic is redirected to a group of Cisco WAEs with the aim of optimizing resource usage and lowering response times. A WCCP-enabled router and a Cisco WAE exchange WCCP protocol packets and negotiate membership of WCCP service groups.
- For Cisco vWAAS on Cisco ENCS 5400-W with WCCP, there are two Ethernet Gigabit ports that can be configured to intercept the traffic. With the NIM card, the ports can be used to intercept the WCCP traffic (configure port channel with LAN and WAN interface) if the inline interception method is not configured.
- For more information on on configuring WCCP, see the chapter "Configuring Traffic Interception" in the *Cisco Wide Area Application Services Configuration Guide*.

The following table shows the CLI commands used to configure WCCP traffic interception for Cisco vWAAS with Cisco Enterprise NFVIS.

Table 2: Cisco WAAS CLI Commands for WCCP Interception Mode

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

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

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

Interoperabiity and Upgrade Guidelines for Cisco Enterprise NFVIS

Consider the following interoperability guidelines for Cisco Enterprise NFVIS and Cisco vWAAS:

- The following table shows the Cisco WAAS versions supported for Cisco vWAAS with Cisco Enterprise NFVIS.

Table 3: Cisco WAAS Versions Supported for Cisco Enterprise NFVIS

Cisco Enterprise NFVIS Version	Earliest Supported Cisco WAAS Version
4.12	6.4.5a
3.11.1	6.4.3b
3.10.1	6.4.3a
3.9.1	6.4.3
3.8.1	6.4.3
3.7.1	6.4.1

For more information on Cisco Enterprise NFVIS and Cisco WAAS Version interoperability, see the Cisco Wide Area Application Services Release Note for your Cisco WAAS version.

- The following models, highlighted in the following list and also listed in the Cisco WAAS sizing guides and specifically noted in Cisco WAAS, Cisco vWAAS user guides, and Cisco WAAS Release Notes, are the *only devices* we recommend for use with Cisco vWAAS:
  - Cisco ENCS 5400-W Series
  - Cisco CSP 5000-W Series
  - Cisco UCS-C Series
  - Cisco UCS-E Series
  - Cisco ISR configurations

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

For more information about supported platforms for Cisco Enterprise NFV, see the Release Notes for Cisco Enterprise Network Function Virtualization Infrastructure Software, Release 3.12.x.

Consider the following upgrade guidelines for Cisco Enterprise NFVIS and Cisco vWAAS:

- You cannot upgrade to Cisco Enterprise NFVIS Version 4.12 from an earlier version; you must do a new installation of Cisco Enterprise NFVIS 4.12.
- For detailed upgrade information for Cisco Enterprise NFVIS versions 3.9.1 through 3.11.1, see the *Cisco Enterprise Network Function Virtualization Insfrastructure Software Configuration Guide* for your Cisco Enterprise NFVIS version.
- Each upgrade may take about 90 minutes. Do not interrupt the upgrade process.

Upgrading the Firmware for Cisco Enterprise NFVIS

Before you begin

This procedure is used to upgrade the Complex Programmable Logic Device (CPLD) and the Field Programmable Gate Array (FPGA) for Cisco Enterprise NFVIS to the latest version.

Procedure

Step 1 Ensure that your system is running the following:

- Cisco WAAS Version 6.4.3b or later
- Cisco Enterprise NFVIS 3.11.1 or later

Step 2 Download the Cisco WAAS Firmware image for ENCS-W Appliance from the Cisco Wide Area Application Services (WAAS) Software Download Page.

Step 3 To upgrade the FPGA, run the **nfvis scp fw-upgrade** command:

```
ENCS-W# nfvis scp fw-upgrade server-IP RemoteFileDirectory RemoteFileName
```

Example:

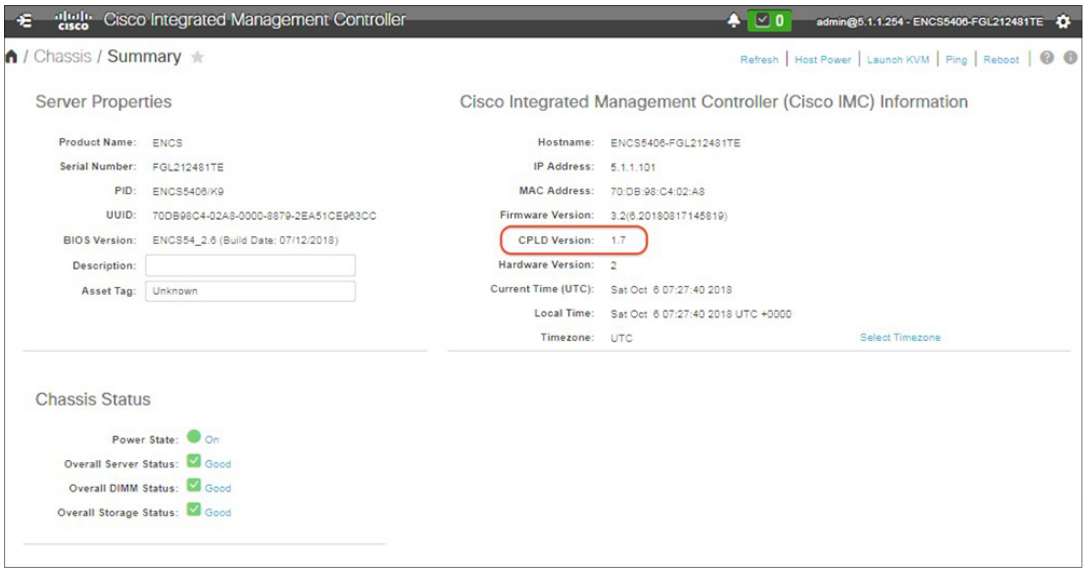
```
ENCS-W# nfvis scp fw-upgrade 172.19.156.179 ./ Cisco_ENCS_firmware-3.11.1.fwpkg
```

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

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

- To verify the CPLD and FPGA version from the CIMC GUI, choose **Chassis > Summary**.

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



- To verify the CPLD and FPGA version from the CIMC CLI, run the following commands:

```
ENCS-W# scope cimc
ENCS-W# /cimc # show firmware detail
Firmware Image Information:
Update Stage: NONE
Update Progress: 0%
Current FW Version: 3.2(6.20180817145819)
FW Image 1 Version: 3.2(6.20180817145819)
FW Image 1 State: RUNNING ACTIVATED
FW Image 2 Version: 3.2(3.20171215104530)
FW Image 2 State: BACKUP INACTIVATED
Boot-loader Version: 3.2(6.20180817145819).36
CPLD Version: 1.7
Hardware Version: 2
```