Release Notes for Cisco Enterprise Network Function Virtualization Infrastructure Software, Release 3.8.x

First Published: 2018-04-20

About Cisco Enterprise NFVIS

Cisco Enterprise Network Function Virtualization Infrastructure Software (Cisco Enterprise NFVIS) is a Linux-based infrastructure software designed to help service providers and enterprises dynamically deploy virtualized network functions, such as a virtual router, firewall, and WAN acceleration, on a supported Cisco device. There is no need to add a physical device for every network function, and you can use automated provisioning and centralized management to eliminate costly truck rolls.

Cisco Enterprise NFVIS provides a Linux-based virtualization layer to the Cisco Enterprise Network Functions Virtualization (ENFV) solution.

Cisco ENFV Solution Overview

Cisco ENFV solution helps you convert your critical network functions into software, making it possible to deploy network services in minutes across dispersed locations. It provides a fully integrated platform that can run on top of a diverse network of both virtual and physical devices with the following primary components:

- Cisco Enterprise NFVIS
- VNFs
- Unified Computing System (UCS) and Enterprise Network Compute System (ENCS) hardware platforms
- Digital Network Architecture Center (DNAC)

For more details on the Cisco ENFV solution, see the Cisco Enterprise Network Functions Virtualization Solution Overview.

System Requirements

The following resources are required for a standalone Cisco Enterprise NFVIS:

- One CPU core
- 2 GB RAM
- 20 GB storage

Note More memory and disk space are required to be added to the system, depending on VM deployments.

Software Upgrade

The Cisco Enterprise NFVIS upgrade image is available as a *.nfvispkg* file. Currently, downgrade is not supported.

For more details on the software upgrade, see the Upgrading Cisco Enterprise NFVIS section in the Cisco Enterprise Network Function Virtualization Infrastructure Software Configuration Guide.

Note NFVIS 3.8.1 supports upgrade from NFVIS 3.7.1-FC2.

Note NFVIS 3.8.1 supports auto-upgrade of CIMC and BIOS for the ENCS5400 platform: After NFVIS 3.8.1 is clean installed or upgraded from version 3.7.1, it will automatically upgrade CIMC to version 3.2.4 and BIOS to version 2.5 for ENCS5400 platform.

Supported Programs and Platforms for Cisco ENFV

Supported Platforms and Firmware

The following table lists the only supported platforms and firmware for Cisco ENFV

Platform	Firmware	Version
ENCS 5406, ENCS 5408, and ENCS 5412	BIOS	2.5
	CIMC	3.2.4
	WAN Port Driver	1.63, 0x80000e2f
	LAN Port Driver	5.04 0x800027d4
ENCS 5104	BIOS	V010
	MCU	1.1
	WAN Port Driver	5.2.18-k/1.63, 0x80000f76
UCS-E160S-M3/K9	BIOS	2.5
	CIMC	3.2.4
UCS-E140S-M2/K9	BIOS	UCSES.1.5.0.7
	CIMC	3.2.4

Platform	Firmware	Version
UCS-E160D-M2/K9	BIOS	UCSED.2.5.0.5
	CIMC	3.2.4
UCS-E180D-M2/K9	BIOS	UCSED.2.5.0.5
	CIMC	3.2.4
UCS-E180D-M3/K9	BIOS	UCSEDM3_2.5
	CIMC	3.2.4
UCS-E1120D-M3/K9	BIOS	UCSEDM3_2.5
	CIMC	3.2.4
UCS-C220-M4	BIOS	3.0.3a
	CIMC	3.0(3c)
CSP-2100-X1	BIOS	3.0.3a
	CIMC	3.0(3a)

Supported Features in Cisco Enterprise NFVIS Release 3.8.1

- SNMP Trap support for switch interface status
- MSTP Support
- RMA support in ENCS 5400
- CIMC access via NFVIS hostip portforwarding in ENCS 5400
- BIOS/CIMC update from NFVIS for ENCS 5400
- NFVIS support for deleting image while download is in progress
- NFVIS support for restoring image download process after power outage or lost connectivity
- PnP FQDN Support
- Handle ISRv restart, implement host and csr-agent monitoring & restartability
- Configurable int-management-network
- Prioritize TACACS over local authentication
- Process MIB memory objects support
- Support SSH/SCP to the int management address
- use ssh force_command to support scp only via 22222 port
- Hostname enhancement
- ENCS: Portal cannot select "source bridge" for Port-Forwarding

- Support for PnP to update admin password without providing current password

Supported VMs

The following table lists supported VMs.

VM	Version
Cisco ISRv	16.06.03
Cisco ASAv	9.8.2
Cisco vWAAS	6.4.1a-b-6
Cisco NGFWv	6.2.2-81
Viptela vEdge	17.2.1
ThousandEyes	1.27.4
Fortinet	5.6.2
PaloAlto	PAN-OS 8.0.5

Note Windows and Linux VMs are also supported.

Open and Resolved Bugs

The open and resolved bugs for a release are accessible through the Cisco Bug Search Tool. This web-based tool provides you with access to the Cisco bug tracking system, which maintains information about bugs and vulnerabilities in this product and other Cisco hardware and software products. Within the Cisco Bug Search Tool, each bug is given a unique identifier (ID) with a pattern of CSCxxNNNNN, where x is any letter (a-z) and N is any number (0-9). The bug IDs are frequently referenced in Cisco documentation, such as Security Advisories, Field Notices and other Cisco support documents. Technical Assistance Center (TAC) engineers or other Cisco staff can also provide you with the ID for a specific bug. The Cisco Bug Search Tool enables you to filter the bugs so that you only see those in which you are interested.

In addition to being able to search for a specific bug ID, or for all bugs in a product and release, you can filter the open and/or resolved bugs by one or more of the following criteria:

- Last modified date
- Status, such as fixed (resolved) or open
- Severity
- Support cases

You can save searches that you perform frequently. You can also bookmark the URL for a search and email the URL for those search results.

Using the Cisco Bug Search Tool

For more information about how to use the Cisco Bug Search Tool, including how to set email alerts for bugs and to save bugs and searches, see Bug Search Tool Help & FAQ.

Before You Begin

You must have a Cisco.com account to log in and access the Cisco Bug Search Tool. If you do not have one, you can register for an account.

Procedure

Step 1 In your browser, navigate to the Cisco Bug Search Tool.

Step 2 If you are redirected to a Log In page, enter your registered Cisco.com username and password and then, click Log In.

Step 3 To search for a specific bug, enter the bug ID in the Search For field and press Enter.

Step 4 To search for bugs related to a specific software release, do the following:

a) In the Product field, choose Series/Model from the drop-down list and then enter the product name in the text field. If you begin to type the product name, the Cisco Bug Search Tool provides you with a drop-down list of the top ten matches. If you do not see this product listed, continue typing to narrow the search results.

b) In the Releases field, enter the release for which you want to see bugs.

The Cisco Bug Search Tool displays a preview of the results of your search below your search criteria.

Step 5 To see more content about a specific bug, you can do the following:

- Mouse over a bug in the preview to display a pop-up with more information about that bug.
- Click on the hyperlinked bug headline to open a page with the detailed bug information.

Step 6 To restrict the results of a search, choose from one or more of the following filters:

Filter	Description
Modified Date	A predefined date range, such as last week or last six months.
Status	A specific type of bug, such as open or fixed.
Severity	The bug severity level as defined by Cisco. For definitions of the bug severity levels, see Bug Search Tool Help & FAQ .
Rating	The rating assigned to the bug by users of the Cisco Bug Search Tool .
Support Cases	Whether a support case has been opened or not.

Your search results update when you choose a filter.

Open Caveats in Cisco Enterprise NFVIS Release 3.8.1

Identifier	Description
CSCvf56170	ENCS5104: call trace during reboot
CSCvg21488	ENCS: ISRv fails to come up due to IFLA_VF_INFO in netlink response error after system reboot
CSCvg35963	WAN interface does not come up randomly (peer side in err-disabled mode)
CSCvg37347	SPAN: Incorrect packets statistics for vlan-vlan and vlan-vnic cases
CSCvg64844	Kernel panic - not syncing: VFS: Unable to mount root fs on unknown-block(2,0)
CSCvg74770	UCSE/UCSC/ENCS installation failures due to "Pane is dead" issue
CSCvg79128	ENCS5400 MGMT link state is not retained after NFVIS reboot
CSCvh22487	CSP: Factory-default-reset results in application error for NFVIS RPM upgrade case
CSCvh70527	Audit information should be cleared after factory-default-reset all and manufacturing
CSCvh89540	show platform agent-stats config with all options but output only shows info for 1st option in CLI
CSCvh91523	kvm failure with single ip access for CIMC via NFVIS portforwarding
CSCvh97384	remote http download unified vWAAS image becomes ERROR after NFVIS reboots
CSCvi02028	ENCS5400 Unable to power on server after upgrade CIMC then power outage
CSCvi19934	CCO software guide need clear clarified parameters/values for vmBackupAction feature in NFVIS 3.7.1
CSCvi45062	Getting "Internal error: Restarting CLI..." after NFVIS reboot sometimes
CSCvi57135	ENCS5100: show nfv_mode shows Error. Mode cannot be found
CSCvi58773	nfvis portal does not accept FQDN name in format of "173-36-197-104.cisco.com"
CSCvi66766	configuration database is locked
CSCvi69344	Error messages seen during server reboot with BIOS 2.5
CSCvi71536	Subsystem sysHealthChk stopped/started occurs ; traceback @ provider.py observed in nfvis_config.log
CSCvi80296	SELinux:failure in sel_netport_sid_slow(), unable determine network port label in 3.8.1RC1 install
CSCvi81021	OIB: ENCS5400: need to show message to user if the upgrade process needs to upgrade BIOS/CIM
CSCvi81143	Incorrect NFVIS platform version (3.7.1) shown in /var/log/pnp/pnp.log on unit with 3.8.1-RC1 image

Identifier	Description
CSCvi84887	3 NFVIS reboots observed during 3.7-3.8 rpm-upgrade with CIMC/BIOS auto-upgrade on ENCS5400 platform
CSCvi86481	vWAAS image remains in IMAGE_CREATING_STATE for hours after https download resume from NFVIS reboot
CSCvi90484	it takes ~30 sec to delete https-downloading vWAAS and WinISO images while image-dowload in progress
CSCvi91715	microcode: CPU0 sig=0x50663, pf=0x10, revision=0x700000c after upgrade package applied
CSCvi92062	Portal VM deploy fail w/ ACTIVE https-download VMDK,qcow2:Cant read property backingVol of undefined
CSCvi94263	ENCS5104 upgrade intermittently cause MCU error
CSCvi94332	SUDI failure due to os2bmc DOWN intermittently after fresh install 3.8.1
CSCvi94357	rbac Not OK after traffic stopped resulting in no portal access
CSCvi94379	multicast traffic degradation with 3.8RC2
CSCvj01113	traceback observed during upgrade
CSCvj03184	systemd-journald[571]: File /var/log/journal/b3fb/user-1000.journal corrupted or uncleanly shut down
CSCvj07612	ENCS5104 portforwarg disable

Related Documentation

- API Reference for Cisco Enterprise Network Function Virtualization Infrastructure Software
- Cisco Enterprise Network Function Virtualization Infrastructure Software Command Reference
- Release Notes for Cisco Enterprise Network Function Virtualization Infrastructure Software, Release 3.5.1
- Cisco 5400 Enterprise Network Compute System Hardware Installation Guide
- Cisco 5400 Enterprise Network Compute System Data Sheet
- Getting Started Guide for Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine
- Cisco UCS C220 M4 Server Installation and Service Guide
- Configuration Guide for Cisco Network Plug and Play on Cisco APIC-EM

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the . RSS feeds are a free service.