Release Notes for Cisco Enterprise Network Function Virtualization Infrastructure Software, Release 3.9.x

First Published: 2018-08-23

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 to design, deploy and manage network services. Cisco Enterprise NFVIS helps dynamically deploy virtualized network functions, such as a virtual router, firewall, and WAN acceleration, on a supported Cisco device. You do not always require a physical device for every network function. Automated provisioning and centralized management also eliminates costly truck rolls.

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

Cisco ENFV Solution Overview

The Cisco ENFV solution helps convert your critical network functions into a software which can deploy network services across dispersed locations in minutes. 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 3.9.1 supports upgrade from NFVIS 3.8.1-FC3.

Note NFVIS 3.9.1 supports auto-upgrade of CIMC and BIOS for the ENCS 5400 platform. After NFVIS 3.9.1 is clean installed or upgraded from version 3.8.1, it automatically upgrades CIMC to version 3.2.6 and BIOS to version 2.6 for ENCS5400 platform. Allow at least 1.5 hours and do not interrupt the install or upgrade process.

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	2.6
	CIMC	3.2.6
	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	2.6
	CIMC	3.2.6
UCS-E140S-M2/K9	BIOS	UCSES.1.5.0.8
	CIMC	3.2.6

Platform	Firmware	Version
UCS-E160D-M2/K9	BIOS	UCSED.2.5.0.6
	CIMC	3.2.6
UCS-E180D-M2/K9	BIOS	UCSED.2.5.0.6
	CIMC	3.2.6
UCS-E180D-M3/K9	BIOS	2.6
	CIMC	3.2.6
UCS-E1120D-M3/K9	BIOS	2.6
	CIMC	3.2.6
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 3.9.1

- Enforce role base access control on
  - logging level configuration
  - reboot or shutdown of NFVIS action
  - file-copy
- Usage and leak of encypted password
- Overlapping of users management
- ENCS 5400 Secure Boot
- NFVIS Admin Password Recovery
- Hostaction reboot notification
- VM identification
- Ability to enable/disable VM monitoring
- Image registration for external data-store
- ENCS 5400 Switch LLDP

Supported VMs

The following table lists supported VMs.

VM	Version
Cisco ISRv	16.09.01a
Cisco ASAv	9.8.2
Cisco vWAAS	6.4.1a-b-6
Cisco NGFWv	6.2.2-81
Viptela vEdge	17.2.1
ThousandEyes	Agent 1.27.4
Fortinet	Fortigate 5.6.2
PaloAlto	PAN-OS 8.0.5
InfoVista	Ipanema VNF vipe_kvm v9.1.6.6
CTERA	6.0.4

Note Windows and Linux VMs are also supported.

TACACS Authentication Limitation with NFVIS 3.9.1

For NFVIS 3.9.1 release, web based TACACS authentication does not work. For TACACS Authentication feature to work, use the TACACS configuration commands or create local users.

For more information and updates on this feature, refer CSCvm39621.

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 3.9.1

Identifier	Description
CSCvg75023	Two registered upgrade-packages allowed to be applied and scheduled in Portal but 2nd apply fails.
CSCvi44811	Portal Deploy page only lists wan-br (MGMT is missing) for available source_bridge option
CSCvj75800	Need to block all accesses after issued operations related to shutdown
CSCvj77017	Error message during BMC bootup /etc/rc.d/S20bios_secure_vars_setup.sh: line 111: [: missing `]'
CSCvj83561	Add user showed notification error in portal without submitting new use
CSCvk17586	show platform-detail should list all the disks with their sizes
CSCvm01630	automatic firmware upgrade with secureboot failed
CSCvm04919	MGMT IP address becomes 0.0.0.0 after NFVIS reboot when it is in admin down state
CSCvm09561	NFVIS: wrong SNMP value for system fan sensor value
CSCvm09698	Application error while changing RBAC user role and ConfD is locked intermittently
CSCvm09839	False RED notification for upgrade package registration
CSCvm39621	NFVIS 3.9.1 - GUI Login Fails with Tacacs

Resolved and Closed Bugs in NFVIS Release 3.9.2

The following table lists the resolved and closed bugs in NFVIS 3.9.2 release.

Bug ID	Summary
CSCvj49499	NFVIS - TACACS Secret encryption
CSCvm39621	NFVIS 3.9.1 - GUI Login Fails with Tacacs
CSCvm72028	Remove G0/0 from wan-br attached to ISRv then update it with G0/0-SRIOV crash reboot the nfvis
CSCvm74018	Local user access is enabled after upgrading from 3.8.1-FC3 w/ TACACS/RADIUS authentication **Note** This fix works works only for upgrade from 3.8.1->3.9.1->3.9.2.
CSCvm82768	Enable NFVIS console access authenticate through ConfD

Bug ID	Summary
CSCvm95019	change shared-secret to aes type

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 What's New in Cisco Product Documentation RSS feed. RSS feeds are a free service.