Release Notes for Cisco Enterprise Network Function Virtualization Infrastructure Software, Release 3.10.x

First Published: 2018-12-14

Last Modified: 2019-03-15

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:

- Atleast 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 3.10.1 supports upgrade from NFVIS 3.9.1-FC1 and NFVIS 3.9.2-FC4.

Note NFVIS 3.10.1 does not support ENCS 5100 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	2.6
	CIMC	3.2.6
	WAN Port Driver	1.63, 0x80000e2f
	LAN Port Driver	5.04 0x800027d4
UCS-E160S-M3/K9	BIOS	2.5
	CIMC	3.2.6
UCS-E140S-M2/K9	BIOS	UCSES.1.5.0.8
	CIMC	3.2.6
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

Platform	Firmware	Version
UCS-E180D-M3/K9	BIOS	2.5
	CIMC	3.2.6
UCS-E1120D-M3/K9	BIOS	2.5
	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)

Note NFVIS 3.10.1 does not support ENCS 5100 platform.

Supported Features in Cisco Enterprise NFVIS Release 3.10.1

Note Only NFVIS releases with supported features are listed in this section.

- Secure overlay and single IP configuration
- Backup and restore
- Dual WAN support
- DPDK support
- PNIC state tracking
- CSDL support

Supported VMs

The following table lists supported VMs.

VM	Version
Cisco ISRv	16.10.01a
Cisco ASAv	9.10.1
Cisco vWAAS	6.4.1c-b-57 6.4.3-b-171
Cisco NGFWv	6.2.3-83

VM	Version
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.

Limitations with NFVIS 3.10.x

TACACS Configuration

When upgrading from NFVIS 3.9.x release to 3.10.x release, if you have TACACS configured with an encrypted-shared-secret, change the key to shared-secret, upgrade to NFVIS 3.10.x release and then change back to encrypted-shared-secret key.

If you have upgraded to NFVIS 3.10.x release, ensure that the TACACS server is not reachable, so that NFVIS uses local authentication and you can login to the device and then configure the TACACS servers again.

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 and 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 and 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 3.10.1

Caveat ID Number	Description
CSCvm97077	Deployment On NFS Share Failed
CSCvn17747	nfvis 3.10.0-13 cause i2c_designware AMD0010:00: controller timed out
CSCvn32791	default-gateway is not set when wan2-br DHCP is renewed
CSCvn46461	UserID shows "Unknown" on BRIDGE_UPDATE event after NFVIS 3.10 fresh-install
CSCvn48279	Backward compatibility: PnP DNS design change between pnp agent 1.6 (NFVIS 3.9) and 1.8 (NFVIS 3.10)
CSCvn49929	NFVIS: System restore failed on multi-datastore multi-disk VM
CSCvn49929	NFVIS: System restore failed on multi-datastore multi-disk VM
CSCvn51821	NFVIS Packaging tool: global name 'xmltodict' is not defined
CSCvn52061	NFVIS: vmImportAction failed for deployment based on qcow2/vmdk image
CSCvn52061	NFVIS: vmImportAction failed for deployment based on qcow2/vmdk image
CSCvn52242	NFVIS: vmExportAction for ISO based image
CSCvn52242	NFVIS: vmExportAction for ISO based image
CSCvn54566	user create bridge or wan2-br may not show up in virsh iface-list
CSCvn57056	Some show bridge-settings subcommands are broken
CSCvn57994	Inconsistent behavior after factory-default-reset all observed on UCSC sometimes
CSCvn59965	Sometimes wan-br dhcp is disabled after clean installation when IPv6 offer is true
CSCvn60216	Application error for factory-default-reset on upgraded systems (3.5-> ... -> 3.10)
CSCvn61770	Cannot login with NFVIS new BIOS password changed
CSCvn62038	kvm : ERROR: Class:0; Subclass:50000; Operation: 1009
CSCvn66077	[hostname]ENCS hostname can not start with numeric anymore after 3.9.2/3.10.1
CSCvn66224	Login without change password when DHCP fresh install NFVIS sometimes, when doing "no" and "yes"
CSCvn67758	Error: Python cb_action error. system call failed (24): Bad file descriptor
CSCvn69411	NFVIS Packaging - nfvpt.py does not mount the bootstrap image in root location
CSCvn71548	ISRv does not recognize NIM after boot up on ENCS5400
CSCvn74856	Packet Capture does not work for DPDK ports

Resolved and Closed Bugs in NFVIS Release 3.10.2

The following table lists the resolved and closed bugs in NFVIS 3.10.2 release.

Bug ID	Summary
CSCvn71665	OIB:secure-overlay single-ip failover when vEdge is up
CSCvo00870	Add VLAN strip enable disable opcode 28 and 28 to the i40e driver
CSCvo02127	Subsystem stopped with 3.10.1-FC4 image
CSCvo05527	Upgrade from 3.10.1 to a newer version failed due to exception for UCSE/UCSC/CSP

Resolved and Closed Bugs in NFVIS Release 3.10.3

The following table lists the resolved and closed bugs in NFVIS 3.10.3 release.

Bug ID	Summary
CSCvn79261	NFVIS 3.10.1: After upgrade, user unable to login via NFVIS CLI via console
CSCvo15676	Setting source-interface as wan IP address fails for 3.10 device - Backward incompatible change

Related Documentation

- API Reference for Cisco Enterprise Network Function Virtualization Infrastructure Software
- Cisco Enterprise Network Function Virtualization Infrastructure Software Command Reference
- https://www.cisco.com/c/en/us/td/docs/routers/nfvis/release_notes/3-9-1/cisco-enterprise-nfvis-release-notes-3-9-1.html
- 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

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.

- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.