Release Notes for Cisco Enterprise Network Function Virtualization Infrastructure Software, Release 3.6.x

First Published: 2017-08-30

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 accelerator on supported Cisco devices. Such virtualized deployments of VNFs also leads to device consolidation. You no longer need separate devices. 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)

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 3.6.1 supports upgrade from NFVIS 3.5.1-FC4 or NFVIS 3.5.2-FC2 to NFVIS 3.6.1-FC3.

Supported Programs and Platforms for Cisco ENFV

The following are the only supported programs and platforms for Cisco ENFV and any other program or platform will not be supported.

Supported Programs

The following table lists only the supported programs for Cisco ENFV

Programs	Release Version
Cisco Enterprise NFVIS	3.6.1-FC3
Cisco ESA	1.0.78
Application Policy Infrastructure Controller Enterprise Module (APIC-EM)	1.5.0.1368 + pnp-app-1.5.1.35
Cisco Prime Infrastructure Software	3.2.0.0.258
Cisco Network Services Orchestrator (NSO) vBranch Core Function Pack	1.0.2

The Cisco ENCS 5000 Series and UCS E-Series platforms ship with multiple firmware binaries that are inter-dependent on the corresponding NFVIS 3.5 and 3.6 releases. When these platforms are ordered, Cisco ships them with the right combination of software. Special care must be taken while upgrading from NFVIS 3.5.x to 3.6.x.

Please be aware of the following BIOS restrictions:

- NFVIS 3.6.1 supports all ENCS5400 BIOS versions from 1.2 through 2.3.
- Version 2.3 is required if you are using a hardware RAID card.
- Note that version 2.3 is not compatible with NFVIS 3.5.1. Upgrading to this BIOS on a system running NFVIS 3.5.1 may cause the install to fail and require reinstallation after downgrading the BIOS.
- To upgrade your ENCS5400 BIOS to 2.3, ensure you upgrade NFVIS to 3.6.1 or later first, before upgrading the BIOS.
- Please refer to the Supported Platforms and Firmware section of the Release Notes (link) and ensure your platform has the supported BIOS, CIMC, and other firmware versions applied.

Note If a newer HUU is applied on older NFVIS versions, the system may not boot up. To recover from this situation, downgrade the BIOS to the older version, or reinstall NFVIS. The latter will result in user data loss.

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	2.3
	CIMC	3.1.5
	WAN Port Driver	1.63, 0x80000e2f
	LAN Port Driver	5.04 0x800027d4 1.1256.0
UCS-E160S-M3/K9	BIOS	UCSEM3_2.3
	CIMC	3.1.4
	HUU	3.1.4
UCS-E140S-M2/K9	BIOS	UCSES.1.5.0.6
	CIMC	3.1.4
	HUU	3.1.4
UCS-E160D-M2/K9	BIOS	UCSED.2.5.0.4
	CIMC	3.1.4
	HUU	3.1.4
UCS-E180D-M2/K9	BIOS	UCSED.2.5.0.4
	CIMC	3.1.4
	HUU	3.1.4
UCS-E180D-M3/K9	BIOS	UCSEDM3_2.3
	CIMC	3.2.1
UCS-E1120D-M3/K9	BIOS	UCSEDM3_2.3
	CIMC	3.2.1
UCS-C220-M4	HUU	2.0(10b)

Supported Features in Cisco Enterprise NFVIS Release 3.6.1

- Syslog Support
- SNMP Support
- RADIUS Support
- Switch Portal Support
- VM Image Packaging
- Secondary IP and Source Interface
- SCP CLI command to allow SCP to and from intdatastore, extdatastore, and USB
- Hardware RAID for ENCS 5400
- Hot add vnic on the fly

New hardware platforms supported:

- UCS-E180D-M3/K9
- UCS-E1120D-M3/K9

Supported Cisco VMs

The following table lists supported Cisco VMs.



Note Third party VMs and Windows and Linux operating systems are also supported.

VM	Version
Cisco ISRv	16.06.01
Cisco ASAv	961
Cisco vWAAS	6.2.3d-b-33
Cisco NGFWv	6.2.0-362

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.

Filter	Description
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 3.6.1

Identifier	Description
CSCvc76820	T1/E1 NIM reboot on multicast traffic.
CSCvc98118	ENCS: Traffic fails when EVC is configured on IGBVF interface.
CSCve26607	ENCS: ISRv Deployment fails due to IFLA_VF_INFO in netlink response error again
CSCvb11894	ENCS: HDD fault LED is ON
CSCvd49343	Get deployments API return partial data after 30 seconds after delete VM
CSCve07179	After asav vm restart, it can not ping peer.
CSCve84852	Unable to specify exact upgrade package to be registered when multiple scp'ed packages exist
CSCve97178	SNMP SysOID Description for ENCS is incorrect
CSCvf25430	NFVIS: SRIOV network name and IP address shown incorrectly in "show vm_lifecycle .." CLI
CSCvf50314	VM Type Other and Version string not show after ISRv image registered active with TAR.GZ extension
CSCvf53263	Portal: Deployments with networks and VMs can cause REST Error for the VMs
CSCva50907	ENCS:Untagged Traffic fails when Subinterface is on the same intf
CSCvd09013	SPAN: Out-port and in-port are missing in show system mirrors after NFVIS reboot
CSCvd92441	vWAAS VM remains on Ext-HDD after NFVIS fresh-installation if vWAAS not undeployed before install
CSCvf41875	ENCS does not work properly when M.2 is moved from one ENCS to another ENCS
CSCvf56307	NFVIS: Application Communication failure with WAN DHCP Renew API
CSCvf38502	No SN info shows up in ENCS-MRAID card

CSCvf63269	After on the vnic edit on the fly changes - LAN-SRIOV sub interface ping fails after Reboot of ISRv
CSCvf53023	NFVIS: HOT ADD two vnic's on ISRv at the same time fails to add one interface.
CSCvf60826	ISRv VM shows VM_MONITOR_UNSET_STATE when tried to add Vnics on the fly.
CSCve87966	ENCS: Missing network information in deployment operational data
CSCve92084	ENCS: Could not modify ISRv SRIOV interface back and forth in same physical interface
CSCvf62427	Notification info is remained after "factory-default-reset manufacturing/all"
CSCvf63553	$$TS: lose communication with switch_daemon due to "no callpoint"
CSCvg00670	ENCS: NIM is not recognized by ISRv after nfvis reboot intermittently

Open Caveats in Cisco Enterprise NFVIS Release 3.6.2

Identifier	Description
CSCva50907	ENCS:Untagged Traffic fails when Subinterface is on the same intf
CSCvb11894	ENCS: HDD fault LED is ON
CSCvc76820	T1/E1 NIM reboot on multicast traffic.
CSCvc98118	ENCS: Traffic fails when EVC is configured on IGBVF interface.
CSCvd09013	SPAN: Out-port and in-port are missing in show system mirrors after NFVIS reboot
CSCvd49343	Get deployments API return partial data after 30 seconds after delete VM
CSCvd92441	vWAAS VM remains on Ext-HDD after NFVIS fresh-installation if vWAAS not undeployed before install
CSCve07179	After asav vm restart, it can not ping peer.
CSCve16389	ENCS5104: Incorrect SFP LED behaviors
CSCve26607	ENCS: ISRv Deployment fails due to IFLA_VF_INFO in netlink response error again
CSCve84852	Unable to specify exact upgrade package to be registered when multiple scp'ed packages exist
CSCve87966	ENCS: Missing network information in deployment operational data
CSCve92084	ENCS: Could not modify ISRv SRIOV interface back and forth in same physical interface
CSCve97178	SNMP SysOID Description for ENCS is incorrect
CSCvf18544	ENCS5104: M.2 slot LED is off
CSCvf25430	NFVIS: SRIOV network name and IP address shown incorrectly in "show vm_lifecycle .." CLI

Identifier	Description
CSCvf38502	No SN info shows up in ENCS-MRAID card
CSCvf41875	ENCS does not work properly when M.2 is moved from one ENCS to another ENCS
CSCvf50314	VM Type Other and Version string not show after ISRv image registered active with TAR.GZ extension
CSCvf53023	NFVIS: HOT ADD two vnic's on ISRv at the same time fails to add one interface.
CSCvf53263	Portal: Deployments with networks and VMs can cause REST Error for the VMs
CSCvf56170	ENCS5104: call trace during reboot
CSCvf56307	NFVIS: Application Communication failure with WAN DHCP Renew API
CSCvf60826	ISRv VM shows VM_MONITOR_UNSET_STATE when tried to add Vnics on the fly.
CSCvf62178	OIB: modify boot menu to be more user friendly/readable
CSCvf62427	Notification info is remained after "factory-default-reset manufacturing/all"
CSCvf63269	After on the vnic edit on the fly changes - LAN-SRIOV sub interface ping fails after Reboot of ISRv
CSCvf63553	$$TS: lose communication with switch_daemon due to "no callpoint"
CSCvg00641	Portal: Notifications for create network can sometimes take a long time to generate > 10 seconds
CSCvg00670	ENCS: NIM is not recognized by ISRv after nfvis reboot intermittently
CSCvg02216	ENCS5104-400/K9: CRITICAL (>80% full) disk-usage issue for vWAAS-200

Open Caveats in Cisco Enterprise NFVIS Release 3.6.3

Identifier	Description
CSCve76776	Need to expose more libvirt options to vm packaging
CSCvg16037	Unable to ssh from nfvis shell to ISRv - Host key verification failed and can not clear key
CSCvg31207	Cherry picked changes from master branch to esc-lite_FC2
CSCvg31301	Cherry Pick of CLI changed from master to NFVIS-3.6.1-throttle
CSCvg71460	reverting CSCve76776 just for BT
CSCvg71556	Configure vnic/vnet txqueuelen to 4000
CSCvg73466	Emulator Pin not enabled after NFVIS upgrade 3.6.1 FC3 to 3.6.1-984
CSCvh70392	Portal not coming up. vbmd NOT OK
CSCvh79756	cannot build nfvis

Related Documentation

- Cisco Network Function Virtualization Infrastructure Software Getting Started Guide
- API Reference for Cisco Enterprise Network Function Virtualization Infrastructure Software
- Cisco Enterprise Network Function Virtualization Infrastructure Software Configuration Guide, Release 4.x
- Cisco Enterprise Network Function Virtualization Infrastructure Software Command Reference
- Release Notes for Cisco NFV SD-Branch features in Cisco vManage Release 20.12.x
- Design and Deployment Guide of Cisco NFVIS SD-Branch using Cisco SD-WAN Manager
- Cisco Catalyst 8200 Series Edge uCPE Data Sheet
- Cisco Cloud Services Platform 5000 Series Data Sheet
- Cisco 5400 Enterprise Network Compute System Hardware Installation Guide
- Cisco 5400 Enterprise Network Compute System Data Sheet
- Configuration Guide for Cisco Network Plug and Play on Cisco APIC-EM, Release 1.5.x
- Cisco SD-WAN Controller Compatibility Matrix and Recommended Computing Resources, Cisco SD-WAN Release 20.12.x

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business results 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 DevNet.
- 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.

© 2017 Cisco Systems, Inc. All rights reserved.