Release Notes for Cisco Enterprise Network Function Virtualization Infrastructure Software, Release 4.2.1

First Published: 2020-08-13

Last Modified: 2024-03-26

About Cisco Enterprise NFVIS

Note To achieve simplification and consistency, the Cisco SD-WAN solution has been rebranded as Cisco Catalyst SD-WAN. In addition, from Cisco IOS XE SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Release 20.12.1, the following component changes are applicable: **Cisco vManage** to **Cisco Catalyst SD-WAN Manager**, **Cisco vAnalytics** to **Cisco Catalyst SD-WAN Analytics**, **Cisco vBond** to **Cisco Catalyst SD-WAN Validator**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

Find all the information you need about this release—new features, known behavior, resolved and open bugs, and related information.

What's New

New and Enhanced Features for Cisco Enterprise NFVIS Release 4.2.1

Feature	Description	Where Documented
Enhancements to backup and restore of configurations	New commands are introduced to view the overall status of backup and restore process. Enhancements to backup file location and factory default options are introduced. Information on how to troubleshoot failure to restore NFVIS configurations is added.	Backup and Restore NFVIS and VM Configurations

Feature	Description	Where Documented
HugePage memory and CPU allocation	The system memory allocations are enhanced and all memory apart from the amount reserved for system is converted to HugePage memory.	Host System Requirements
Command for PnP certificates	A certificate can be used as a PnP root certificate through Command Line Interface (CLI).	Certificate for Static PnP discovery
Secure Operation in FIPS Mode on NFVIS	The Federal Information Processing Standards (FIPS) Publication 140-2 are publicly announced standards developed by the United States federal government for use in computer systems by non-military government agencies and government contractors.	Secure Operation in FIPS Mode on NFVIS
BIOS and CIMC password	New password restrictions and security measures are added for CIMC and BIOS.	BIOS and CIMC Password

Limitation with NFVIS Host Backup Process

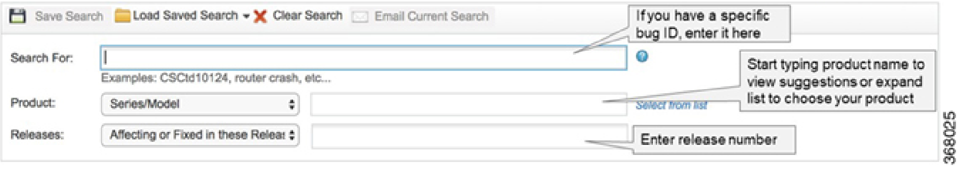
NFVIS host backup process can receive error message from Linux tar or gzip. While running hostaction backup with configuration-and-vms option, especially the components which requires longer time to copy and archive, the hostaction backup status output can show BACKUP-PARTIALLY-COMPLETED and FAILURE for the affected component. In case of discrepancy regarding the backup, delete the old backup and generate a new backup.

Resolved and Open Bugs

About the Cisco Bug Search Tool

Use the Cisco Bug Search Tool to access open and resolved bugs for a release.

The tool allows you to search for a specific bug ID, or for all bugs specific to a product and a release.



If you have a specific bug ID, enter it here

Search For:

Examples: CSCtd10124, router crash, etc...

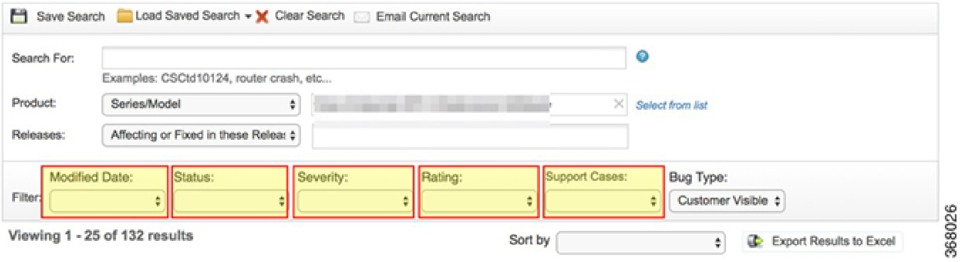
Start typing product name to view suggestions or expand list to choose your product

Product: Series/Model

Releases: Affecting or Fixed in these Releas

Enter release number

You can filter the search results by last modified date, bug status (open, resolved), severity, rating, and support cases.



Search For:

Examples: CSCtd10124, router crash, etc...

Product: Series/Model [redacted]

Releases: Affecting or Fixed in these Releas

Bug Type: Customer Visible

Viewing 1 - 25 of 132 results

Key Fixed bugs in 4.2.1

Caveat ID Number	Description
CSCvu22897	Absolute File Paths exposed on NFVIS 3.12.3-FC4
CSCvu26963	Insecure CORs Policy

Open Bugs for Cisco Enterprise NFVIS Release 4.2.1

Caveat ID Number	Description
CSCvt22539	NFVIS: factory-reset-all with VM having disk deployed on NFS
CSCvu62778	NFVIS: power cycle during host backup, files are not cleaned up
CSCvu75840	For system with more than 128Gb memory, need 8Gb free memory while upgrading to NFVIS4.2
CSCvu78025	NFVIS-ESC-LITE: vmExport process blocking other vmAction process
CSCvu81545	NFVIS: log-data name filter does not work for module vm-management
CSCvu93715	show bridge-settings cli doesnt work
CSCvu94040	custom bridge attached to sriov disabled pnic didnt migrate to dpdk
CSCvv06774	NFVIS Packaging tool doesn't work with python3
CSCvv14470	System hang after multiple iterations of upgrade and multiple iterations of reboot
CSCvv16328	Notification on /var/log critical (>=90% full) after multiple NFVIS reboots
CSCvv16664	CPU high and system is very slow and couple services keep restarting after reboot ENCS in HA topo
CSCvv16678	PnP cco redirect failure due to the 1st DNS server is unreachable and system not try the 2nd DNS one
CSCvv16807	SNMP Error=snmp_104 Unexpected value sensor_values
CSCvv19181	vBranch ZTP: Linux provision in error state. operation failed: domain 'Redhat' already exists
CSCvv19239	System restore doesnt account for deployment of low latency VM first

Caveat ID Number	Description
CSCvv23602	NFVIS switch: vlan is not enabled properly on Portchannel when apply configuration from vManage
CSCvv25576	Restore failure followed by hostaction reboot can delete the VM.
CSCvv28644	multi upgrade->backup->fresh install->restore fail
CSCvv28736	System uses 95.6747690837% of memory, which is more than or equal to the threshold of 95
CSCvv29238	cannot scp out backup file from NFVIS when backup under /mnt/extdatastoreX
CSCvv29349	factory reset when device attached to template: NMI watchdog: BUG: soft lockup / journal i/o error
CSCvv33835	NFVIS: restore configuration-only failed on unwanted image

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 4.2.1 supports upgrade from NFVIS 4.1.x.

System Requirements

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

- For a system that has 16 or less CPU cores, one CPU core is reserved for NFVIS. For a system that has more than 16 CPU cores, 2 CPU cores are reserved for NFVIS.
- For a system that has 32 GB or less of RAM, 3 GB is reserved for NFVIS. For a system that has more than 32 GB of RAM, 4 GB is reserved for NFVIS.
- 20 GB storage.
- For NFVIS portal, the minimum supported version of browsers are:
    - Mozilla Firefox 66
    - Google Chrome 71
    - Windows 10 Edge
    - MacOS 10.15 Safari

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

Supported Programs and Platforms

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	ENCS54_BIOS_2.11.SPA
	CIMC	CIMC_3.2.10.bin
	WAN Port Driver	1.4.22.7-10-ciscocsx
	LAN Port Driver	5.4.0-3-k CISCO
ENCS 5104	BIOS	V010
	MCU	1.1
	WAN Port Driver	5.4.0-1-k, 0x80000f76
UCS-E160S-M3/K9	BIOS	UCSEM3_2.6
	CIMC	3.2(8.20190624114303)
UCS-E140S-M2/K9	BIOS	UCSES_1.5.0.8
	CIMC	3.2(8.20190624114303)
UCS-E160D-M2/K9	BIOS	UCSED_3.5.0.1
	CIMC	3.2(8.20190624114303)
UCS-E180D-M2/K9	BIOS	UCSED_3.5.0.1
	CIMC	3.2(8.20190624114303)
UCS-E180D-M3/K9	BIOS	UCSEDM3_2.6
	CIMC	3.2(8.20190624114303)
UCS-E1120D-M3/K9	BIOS	UCSEDM3_2.6
	CIMC	3.2(8.20190624114303)
UCS-C220-M4	BIOS	3.0.3a
	CIMC	3.0(3c)

Platform	Firmware	Version
CSP-2100-X1	BIOS	3.0.3a
	CIMC	3.0(3a)
UCS-C220-M5	BIOS	C220M5.3.1.3c.0.0307181404
	CIMC	3.1(3a)
CSP-5228	BIOS	C220M5.4.0.4c.0.0506190754
	CIMC	4.1(1c)
CSP-5436 and CSP- 5444 (Beta)	BIOS	Use HUU 4.1(1c)
	CIMC	Use HUU 4.1(1c)

Guest VNFs

This section provides support statements for different guest Virtual Network Functions (VNFs) that you can run on Cisco Routing virtual platforms enabled by the NFVIS 4.2.1 release.

Cisco Router VNFs

Note

- Cisco provides support for deployment and configuration of the VNF versions listed below, when deployed on Cisco Routing virtual platforms, enabled by this release of NFVIS.
- Cisco provides support on a case-by-case basis for unlisted combinations of NFVIS release + VNF version.

Product homepage	Software download
Cisco ISRv	17.3.1a 17.2.1r 16.12.4
Cisco vEdge	20.3.1 20.1.1 19.2.3

Other Cisco Owned VNFs

Note

- Limited testing is done to ensure you can create a guest VM instance using the software download image for these versions, as posted on Cisco Software download page.
- For full-support statement see the individual product release documentation.

Product homepage	Software download
Security VNFs	
Cisco NGFW (FTDv)	6.5
Cisco ASAv	9.14.1 9.12.1
WAN Optimization VNFs	
Cisco vWAAS	6.4.5-b-75 6.4.3c-b-42

Non-Cisco Vendor Owned VNFs

You can run VNFs owned by various vendors on Cisco’s NFV platforms enabled by NFVIS . Formal support for these VNFs requires a joint effort between Cisco and the VNF vendor.

Cisco offers VNF vendors a "for-fee" NFVIS 3rd-party certification program to test and certify their VNFs on Cisco’s virtualized platforms. After testing and certification is complete, the results are published on this page- Cisco Enterprise NFV Open Ecosystem and Qualified VNF Vendors.

For more specific support details about VNF versions and test compatibility matrix with NFVIS releases, see the VNF release documentation on the vendor support site.

As a NFVIS customer, if you need a unique combination of NFVIS release and a specific VNF version, you may submit your certification request to Cisco at nfv-ecosystem@cisco.com or reach out to the VNF vendor support team asking them to initiate a certification on the Cisco platform.

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