Release Notes for Cisco Enterprise Network Function Virtualization Infrastructure Software, Releases 4.6.1, 4.6.2, 4.6.3, and 4.6.4

First Published: 2021-06-09

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 4.6.1

Feature	Description	Where Documented
Local Authentication for a Specific Group of Users	This feature allows you to create a group with specific users, who can perform only the local authentication; and don't have to authenticate externally through TACACS.	Local Authentication for a Specific Group of Users
Support for External Storage for Cisco Cloud Services Platforms	External disks are supported for Cisco Cloud Services Platforms (CSP).	Support for External Storage for Cisco Cloud Services Platforms

Feature	Description	Where Documented
Support for Replacing HTTP Basic Authentication	This feature enhances NFVIS local portal capabilities, to replace HTTP basic authentication to prevent accidental leakage of credentials.	–
Support for NFVIS Container Life Cycle Management	This features provides support for container lifecycle management. **Note** Cisco, may at its discretion, provide support (as defined by Cisco) to host container based applications for NFVIS 4.6.1. This capability is a beta feature in this release and should not be used in production because, Cisco may make changes in subsequent releases without providing any backward compatibility. The beta is provided AS-IS and without any warranty of any kind.	Support for NFVIS Container Life Cycle Management

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.

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

Resolved and Open Bugs for Cisco NFVIS Release 4.6.4

There are no defect fixes in the Cisco NFVIS Release 4.6.4.

Resolved and Open Bugs

Resolved Bugs for Cisco Enterprise Release 4.6.3

Identifier	Headline
CSCvz73973	Cisco Network Function Virtualization Infrastructure Software (NFVIS) Vulnerability
CSCvz73971	Cisco Enterprise NFV Infrastructure Software (NFVIS) XXE vulnerability
CSCvz73988	Cisco Enterprise NFV Infrastructure Software (NFVIS) Command Injection Vulnerability
CSCwc18420	VM name and hugepage migration command support
CSCwd04322	Cisco Catalyst 8000V bin upgrade to 17.9.1a from 17.6.3a cause traffic fail on iavf interface while virtio works
CSCvz74003	Cisco Enterprise NFV Infrastructure Software Improper Signature Verification Vulnerability

Resolved and Open Bugs

Resolved Bugs for Cisco Enterprise NFVIS Release 4.6.2

Bug ID	Description
CSCwa04732	Portal Packaging UI: OIB when create VM package, show "Unknown" status and no further notification.
CSCwa04530	Portal Packaging UI does not allow to specify mount point for bootstrap file.
CSCwa03312	One bulk configuration change commit may cause DPDK network creation fail lead to VM deploymnt fail.
CSCwa04779	Portal OIB: when click Download Tech Support button, no further progress/status info. Kind of stuck.
CSCwa06000	Portal Packaging UI: "invalid value for: custom-property-key" error is seen when create VM package
CSCwa39981	Portal Packaging UI: OIB when create VM package, show "ERROR" status if same image is used twice.
CSCvz29533	GUI Portal->Configuration->vManage->VM export missing include image and property option.

Resolved and Open Bugs

Resolved Bugs for Cisco Enterprise NFVIS Release 4.6.1

Bug ID	Description
CSCvy80433	ENCS orphanized vlan in switch
CSCvy83948	NFVIS 4.5.1, NTP(Private-ip)/Secure-overlay issue
CSCvy83962	NFVIS 4.5.1 Secure-overlay error state (reboot fixing issue)
CSCvy39879	First VM gets deleted if second VM name is firstVm+n
CSCvy52227	4.6. iso image registration may fail with 4.5 or 4.4 baseline due to timiming race condition
CSCvz60918	Device template push fail after ISRv comes up and online

Open Bugs for Cisco Enterprise NFVIS Release 4.6.1

Bug ID	Description
CSCvx74716	Mcast Traffic: admin login failure post reboot, root login is ok
CSCvx93276	LAN WAN BW Failure:Input/output rate are not consistent or as expected on nfvis c8kv lan switch port
CSCvy80292	PSU PID information is missing from nfvis command
CSCvz06226	vBranch: VM stuck at REBOOTING/STOPPING after VNF restart/stop (when "ip host" in add-on CLI)
CSCvz08350	Memory related traceback seen at boot up on CSP with 64GB and 10 pnic
CSCvz08639	nfvis SFP PID inventory on CSP,Tabei,ENCS
CSCvz09517	Out of memory (oom-killer): Stopping strobe of WDT monitoring BMC. Reset coming
CSCvz11312	SFP FTLX8571D3BCVI31 failed to come up as 10G
CSCvz16613	pnic speed duplex setting error propaation to cdb causing discrepancy
CSCvz26665	CSP5444 network accessw fail, 2 c8kv fail to Alive
CSCvz26669	traffic fail and a few show system commands are broken
CSCvz29533	GUI Portal->Configuration->VM Manage->vmExport missing includeimage and property option
CSCvz30088	Mac-address interface-config cmd on c8kv updates NFVIS SR-IOV VF, leading to mis-match of mac
CSCvz33310	Config->Host->Datastore->intdatastore or extdatastore NFVIS upgrade image registration missing

Bug ID	Description
CSCvz39381	VM deployment fail with custom network with name containing '-SRIOV-'
CSCwa14085	vBranch Single IP: VM is shut after upgrade/reload VM. For upgrade, VM rollback after start manually

Important Notes

- In NFVIS release 4.6.1, backup with GE0-1-SRIOV-3 cannot be restored on ENCS 5400. For more details, see CSCvz82738.

Software Upgrade

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

For more details on the software upgrade, see the Upgrading Cisco Enterprise NFVIS section in the https://www.cisco.com/c/en/us/td/docs/routers/nfvis/get_started/nfvis-getting-started-guide/m-upgrade-nfvis.html.

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 Programs and Platforms

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

Note Cisco NFVIS Release 4.6.3 is not supported on the ENCS 5100 series devices.

Platform	Firmware	Version
ENCS 5406, ENCS 5408, and ENCS 5412	BIOS	ENCS54_BIOS_3.00.SPA
	CIMC	CIMC_3.2.13.2
	WAN Port Driver	5.4.0-5-k CISCO
	LAN Port Driver	1.4.22.7-11-ciscocsx
UCS-E160S-M3/K9	BIOS	UCSEM3_2.10
	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_2.10
	CIMC	3.2.11.5
UCS-E1120D-M3/K9	BIOS	UCSEDM3_2.10
	CIMC	3.2.11.5
UCSC-C220-M4S	BIOS	Use HUU 4.1(2f)
	CIMC	Use HUU 4.1(2f)
UCSC-C220-M5SX	BIOS	Use HUU 4.1(3b)
	CIMC	Use HUU 4.1(3b)
CSP-5216	BIOS	Use HUU 4.1(3d)
	CIMC	Use HUU 4.1(3d)
CSP-5228	BIOS	Use HUU 4.1(3d)
	CIMC	Use HUU 4.1(3d)

Platform	Firmware	Version
CSP-5436, CSP-5456, and CSP-5444	BIOS	Use HUU 4.1(3d)
	CIMC	Use HUU 4.1(3d)
C8200-UCPE-1N8	BIOS	C8200-UCPE_1.04.103020201614
	MCU	240.52

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 4.6.1 release.

For the supported VNFs that can be orchestrated through Cisco vManage, see the Guest VNFs section in the NFVIS 4.6.1, 4.6.2 Release Notes.

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 Catalyst 8000V Edge Software	17.6.4 17.6.3a 17.6.1a 17.5.1 17.4.1b
Cisco ISRv	17.3.5 17.3.4 17.3.3 17.3.2 17.3.1a 17.2.1r

Product homepage	Software download
Cisco vEdge	20.6.4 20.6.3.1 20.6.2 20.6.1 20.4.1 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)	6.6.1-91 6.6.0-90
Cisco ASAv	9.14.2 9.14.1
WAN Optimization VNFs	
Cisco vWAAS	6.4.5a-b-50 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