Release Notes for Cisco Enterprise Network Function Virtualization Infrastructure Software, Release 3.7.x

First Published: 2018-01-15

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 dynamically deploy virtualized network functions, such as a virtual router, firewall, and WAN acceleration, on a supported Cisco device. There is no need to add a physical device for every network function, and you can use automated provisioning and centralized management to eliminate costly truck rolls.

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

Cisco ENFV Solution Overview

Cisco ENFV solution helps you convert your critical network functions into software, making it possible to deploy network services in minutes across dispersed locations. 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 3.7.1 supports upgrade from NFVIS 3.6.1-FC3 or 3.6.2-FC3 to 3.7.1-FC2.

Supported Programs and Platforms for Cisco ENFV

The Cisco ENCS 5400 Series and UCS E-Series platforms ship with multiple firmware binaries that are inter-dependent on the corresponding NFVIS releases. When these platforms are ordered, Cisco ships them with the right combination of software. Special care must be taken while upgrading from NFVIS 3.6.x to 3.7.x.

Please be aware of the following BIOS restrictions:

- NFVIS 3.7.1 supports all ENCS5400 BIOS versions from 1.2 through 2.4.
- Version 2.3 or above is required if you are using a hardware RAID card.
- Note that version 2.3 or above are not compatible with NFVIS 3.5.1. Upgrading to BIOS 2.3 or above on a system running NFVIS 3.5.1 may cause the install to fail and require reinstallation after downgrading the BIOS.
- To upgrade your ENCS 5400 BIOS to 2.3 or above, ensure you upgrade NFVIS to 3.6.1 or later first, before upgrading the BIOS.
- Please refer to the Supported Platforms and Firmware, on page 2section of the Release Notes 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	2.4
	CIMC	3.2.3
	WAN Port Driver	1.63, 0x80000e2f
	LAN Port Driver	5.04 0x800027d4
ENCS 5104	BIOS	V009
	MCU	1.1
	WAN Port Driver	5.2.18-k / 1.63, 0x80000f25
UCS-E160S-M3/K9	BIOS	2.4
	CIMC	3.2.3
UCS-E140S-M2/K9	BIOS	UCSES.1.5.0.6
	CIMC	3.2.3
UCS-E160D-M2/K9	BIOS	UCSED.2.5.0.4
	CIMC	3.2.3
UCS-E180D-M2/K9	BIOS	UCSED.2.5.0.4
	CIMC	3.2.3
UCS-E180D-M3/K9	BIOS	UCSEDM3_2.4
	CIMC	3.2.3
UCS-E1120D-M3/K9	BIOS	UCSEDM3_2.4
	CIMC	3.2.3
UCS-C220-M4	HUU	2.0(10b)
CSP-2100-X1	BIOS	2.0.9b
	CIMC	2.0(9e)

Supported Features in Cisco Enterprise NFVIS Release 3.7.1

- Port Channel Support
- LDPP Support
- Admin Status Support
- NFS Support
- IPv6 Support on Static and Management Interface and on PnP and NTP.

- Port 22222 and Management Interface ACL
- Image Signing and Verification
- RBAC Enhancements
- Support VM updating when VM is stopped
- Support VM start / restart when VM is in error state
- Support following image formats: tar.gz, qcow2, vmdk, img, iso
- Support registering VM image and deploying VM on NFS
- Support user configured VM management IP address
- Support VM deployment with multi-storage and multi serial / console ports.
- Allow user to specify image properties when registering image to:
    - Support registering image from source file on NFS
    - Support user configured internal management network IP address pool
    - Support Backing a VM
    - Allow to use the disk size in the profile when creating disk while deploying VM
- SNMP v3 and SNMP traps support
- Configurable Native Vlan
- Configurable disk-space threshold
- SCP enhancements: to/from NFS mount point, from log folder, IPv6 support
- Serviceability CLI:
    - New support commands for showing low-level system information (virsh, ovs, show)
    - tech-support CLI to generate log tar ball
    - Utility CLI: ping, ping-ipv6, telnet, traceroute

New hardware platform supported:

- CSP-2100-X1

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	16.06.02

VM	Version
Cisco ASAv	9.8.2
Cisco vWAAS	6.4.1-b-36 6.2.3d-b-68
Cisco NGFWv	6.2.2-81

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 3.7.1

Identifier	Description
CSCvb11894	ENCS: HDD fault LED is ON
CSCvc76820	T1/E1 NIM reboot on multicast traffic
CSCvd35503	ENCS: Ping fails with SRIOV Access VLAN
CSCve14117	Firmware update progress not automatic refresh in GUI
CSCvf38502	No SN info and PID/VID shows up in ENCS-MRAID card
CSCvf90265	Ping gateway-ipv6 fails after NFVIS reboot. User needs to specify %interface for successful pings.
CSCvf95507	IPv6 addresses assigned by DHCPv6 stateful server always shown prefix-len 64
CSCvg20043	NIM card info is not shown in CIMC 3.2.X GUI

Identifier	Description
CSCvg35963	WAN interface does not come up randomly (peer side in err-disabled mode)
CSCvg37426	NFVIS Help Videos need to be updated for NFVIS 3.7
CSCvg47257	enp5s0 interface shows up after NFVIS rpm-upgrade from 3.5.2-FC2 to 3.7.0-30
CSCvg48847	VM external-port-forwarding ssh access using NFVIS wan-br IPv6 address fails, got Permission Denied
CSCvg49502	Unexpected behavior when multiple VNICs added at once
CSCvg52417	Continuous "ixgbevf: Unable to start" msg on ENCS serial-console after rpm-upgrade 3.5 to 3.7.0-32
CSCvg56855	upgrade 3.6.2.FC3- >3.7 shows Load Time Configuration Error in porta
CSCvg58824	VM Monitoring: mgmt subnet pool assign broadcast ip to vm
CSCvg69329	Show system time only displays IPv6-NTP server, not IPv4-NTP server when both are configured
CSCvg74865	IPv6-NTP server displayed truncated (only 15 characters) in CLI show system time ntp status output
CSCvg79128	ENCS5400 MGMT link state is not retained after NFVIS reboot
CSCvg79349	ESC-LITE: Cannot boot CentOS .raw extension VM
CSCvg85945	PnP: PnP restart fails / PnP IPV6 not triggered after NFVIS upgrade from 3.6.2 FC3 to 3.7.0.
CSCvh02884	switching from static ipv6 to slaac ipv6 deletes slaac ipv6 in backend
CSCvh06198	Inconsistent OID for NFVIS
CSCvh14801	https-downloaded registered ISO/qcow2/vmdk image:not seen in GUI deploy page for further VM deploy
CSCvh18691	User lockdown when portal login with old password and keep it open and then change password in shell
CSCvh18701	application communication failure when change user password
CSCvh22081	IPv6 DHCPv6 stateful addr assign need NFVIS reboot or dhcp-renew after rpm-upgrade 3.6 - > 3.7.1-C2
CSCvh22138	NFVIS upgrade status shown as Failed though PnP Agent is running and if PnP fails to re-establish
CSCvh23596	NFVIS Upgrade Image registration status marked as Invalid when copied via USB
CSCvh23604	Files getting erased in USB with NFVIS upgrade
CSCvh23861	The dot1x authentication port will be blocked when shutdown/no shutdown it

Identifier	Description
CSCvh23870	Packet drop seen when forward the dot1x port incoming traffic
CSCvi19934	CCO software guide need clear clarified parameters/values for vmBackupAction feature in NFVIS 3.7.1

Open Caveats in Cisco Enterprise NFVIS Release 3.7.2

Identifier	Description
CSCvh49919	Intel CPU security Meltdown and Spectre bugs
CSCvh62317	DNA-C NFVIS 3.7.1 Cannot do image registration of two vnfs from remote server simultaneously
CSCvh87752	need to disable root access earlier in ks.cfg and run_filst

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 . RSS feeds are a free service.