Release Notes for Cisco Enterprise Network Function Virtualization Infrastructure Software, Release 3.5.x

First Published: 2017-04-03

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 3.6.2 supports upgrade from NFVIS 3.5.1-FC4, NFVIS3.5.2-FC2, or NFVIS 3.6.1-FC3 to NFVIS 3.6.2-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	3.5.1-FC4
Cisco ESA	1.0.78
Application Policy Infrastructure Controller Enterprise Module (APIC-EM)	1.4.1.1159 and later
Cisco Prime Infrastructure Software	3.1.0.0.132 and later Device-Pack-10-PI3.1-94.ubf and later PI_3_1_6-1.0.14.ubf and later
Cisco Network Services Orchestrator (NSO) vBranch Core Function Pack	1.0

Supported Platforms and Firmware

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

Note The listed platforms will be installed with HUU 3.1.4 and CIMC 3.1 (4.20170327095406).

Platform	Firmware	Version
ENCS 5406, ENCS 5408, and ENCS 5412	BIOS	1.2
	CIMC	3.1(4.20170327095406)
	HUU	3.1.4
	WAN Port Driver	1.63, 0x80000e2f
	LAN Port Driver	5.04 0x800027d4 1.1256.0
	FPGA	1.5
UCS-E160S-M3/K9	BIOS	UCSEM3_1.0 (Build Date: 05/27/2016)
	CIMC	3.1 (4.20170327095406)
	HUU	3.1.4
UCS-E140S-M2/K9	BIOS	UCSES.1.5.0.5 (Build Date: 02/03/2016)
	CIMC	3.1 (4.20170327095406)
	HUU	3.1.4
UCS-E160D-M2/K9	BIOS	UCSED.2.5.0.3 (Build Date: 04/10/2015)
	CIMC	3.1 (4.20170327095406)
	HUU	3.1.4
UCS-E180D-M2/K9	BIOS	UCSED.2.5.0.3 (Build Date: 04/10/2015)
	CIMC	3.1 (4.20170327095406)
	HUU	3.1.4
UCS-C220-M4	BIOS	UCSED.2.5.0.3 (Build Date: 04/10/2015)
	CIMC	3.1 (4.20170327095406)
	HUU	3.1.4

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	16.03.03 and later 16.05.01 and later
Cisco ASAv	961 and later
Cisco vWAAS	6.3.0-b-185 and later
Cisco NGFWv	6.2.0-362 and later

Supported Features in Cisco Enterprise NFVIS Release 3.5.2

- Cisco Enterprise NFV Portal—A graphical interface that helps you configure almost all features.
- Cisco Network Plug-n-Play Support—A unified approach to provision enterprise networks comprised of Cisco routers, switches, and wireless devices with a near zero touch deployment experience.
- Managing VM Operations—Start, stop, and restart VMs as required using the Cisco Enterprise NFV Portal or REST or NETCONF APIs.
- VM Lifecycle Management—You can register VMs, deploy VMs, and create multiple flavors of a VM using APIs or the Cisco Enterprise NFVIS Portal.
- VM Network Management and Monitoring
- VM OVA Packaging—Supports deployment of VMs through uploading of OVA packages for Cisco supplied VMs, third party VMs, and for supported Windows and Linux operating systems. OVA packages must be created according to the Cisco Enterprise NFVIS packaging specification. For detailed information, see the following Cisco document:

  http://www.cisco.com/c/en/us/td/docs/routers/nfvis/user_guide/nfvis-config-guide/nfvis-user-guide_chapter_0110.html
- Service Chaining of VMs—A set of network services in the form of VMs connecting virtual networks. Cisco Enterprise NFVIS supports service chaining of two or more VMs by connecting two or more virtual networks where the VM is running in L2 bridge mode. Service chaining is also implemented by one VM configured to perform packet diversion to another VM.
- Self-signed and Third Party Certificates—You can use the default self-signed certificate or generate CM certificates.
- Single WAN IP Deployment—A single WAN IP deployment can be considered when the Cisco ENCS is preconfigured at the corporate main office with the service provider's WAN IP address, and shipped to the branch office for quick deployment.
- Switched Port Analyzer (SPAN) Session—This feature helps you analyze network traffic passing through interfaces or VLANs by using SPAN sessions.

- vBranch High Availability—This solution uses the Hot Standby Router Protocol (HSRP), a default gateway redundancy, which allows the network to recover from the failure of the device acting as the default gateway for the LAN side end points.
- Resetting Factory Default
- Event Notifications—Cisco Enterprise NFVIS generates event notifications for key events. A NETCONF client can subscribe to these notifications for monitoring the progress of configuration activation and the status change of the system and VMs.
- Packet Capture Support—This feature helps to capture all packets being transmitted and received over physical and virtual network interface controllers (physical port and vNIC) for analysis.

Limitations and Restrictions

- The Cisco Enterprise NFVIS portal cannot be used to configure the switch firmware version running on the Cisco 5400 ENCS. The Cisco ENCS switch can be configured using the switch CLIs or APIs.
- The current switch firmware version in Cisco Enterprise NFVIS 3.5.1 running on the Cisco 5400 ENCS requires to run the **commit** command for each switch CLI to avoid configuration inconsistency between the host and the switch device.

```
nfvis# config terminal
Entering configuration mode terminal
nfvis(config)# switch
nfvis(config-switch)# vlan 100
nfvis(config-switch-vlan)# commit
Commit complete.
nfvis(config-switch-vlan)# exit
nfvis(config-switch)# interface vlan 100
nfvis(config-switch-if)# ip address 192.168.1.1 255.255.255.0
nfvis(config-switch-if)# commit
Commit complete.
nfvis(config-switch-if)# end
```

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 3.5.1

Identifier	Description
CSCve05205	vWLC is not supported in Cisco Enterprise NFVIS Release 3.5.1.
CSCvd07840	Users can hit Ctrl + D, and log into the system without changing the default admin password.
CSCvd09013	The SPAN monitor session configuration fails after the Cisco Enterprise NFVIS reboot.
CSCvd35544	Portal: vWAAS VM thick provision shall not be deployed on ENCS internal disk.
CSCvd46091	PnP: DHCP /DNS Discovery fails when ENCS is accessed through MGMT port.
CSCvd92441	vWAAS VM remains on Ext-HDD after NFVIS fresh-installation if vWAAS not undeployed before install.
CSCvd56432	A vNIC edit or swap operation reboots the VM without any warning.
CSCvd66160	Rebooting Cisco Enterprise NFVIS Release 3.5.1 cannot bring up the system.
CSCvd66538	An internal server error occurs when adding a network to a virtual machine.
CSCvd68358	The **show system-monitoring vnf disk stats** command output shows empty quotes for the **1min vnf disk** option.
CSCvd70575	The VM packaging tool (nfvpt.py) in interactive mode does not accept more than one qcow2 image.
CSCvd74535	The login attempt might fail during the first minute or so after the Cisco Enterprise NFVIS reboot.
CSCvd78934	The **Factory Reset All** option from the portal does not clear CLI history.
CSCvd82114	The SFP media type sometimes shows incorrect media type.
CSCvd82208	Sometimes PnP discovery fails after the BIOS/CIMC upgrade on the Cisco 5400 ENCS.
CSCvd82278	Traceback is observed with the **show vm_lifecycle deployments all** command.
CSCvd83948	The used disk space is marked as free in the **VM Disk Allocation** tab on the Resource Allocation page.
CSCvd86530	The **sshfingerprint** command does not return expected results.
CSCvd56745	Upgrade: Portal should timeout as soon as "upgrade now" is clicked and confirmed for upgrade.
CSCvd74602	rbac application timeout is seen and does not function when we have two wrong change role
CSCvc95151	User of Portal should not be allowed to login with Tacas+ pwd if same user exists in Tacas+ server

CSCvd59126	Tacacs Admin user is not able to edit the User roles of other users
CSCve59448	VNF unresponsive after NFVIS reboot
CSCvd66160	NFVIS: Reboot NFVIS cannot bring up the system - dracut-initqueue timeout
CSCvd77124	ENCS boot with ext-hdd
CSCvc48407	Operational API get deployment information for SRIOV interface show model virtio
CSCvc91183	Portal: image download action is not working
CSCvd49343	Get deployments API return partial data after 30 seconds after delete VM
CSCvd68894	Deploy ISRv intermittent fail: day0 is not applied
CSCvd83948	Resource Allocation page VM Disk Allocation tag does not count used disk space
CSCvd83984	Portal: Switch to Home page show memory as 0.00% even the number below is correct
CSCvd98541	Factory reset with all-except-images-connectivity option, the volumes is not cleaned
CSCvd78951	Factory reset warning message should mention vm and external datastore as well

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.