Cisco Nexus Fabric Manager Release Notes for Administrators, Release 1.2(3)

This document describes the features, bugs, and limitations for Cisco Nexus Fabric Manager. Use this document in combination with documents listed in the "Obtaining Documentation and Submitting a Service Request" section.

Table 1 shows the online change history for this document.

Table 1. Online History Change

Date	Description
February 10, 2017	Created the Release Notes for Release 1.2(3)

Contents

Introduction

The Cisco Nexus Fabric Manager (NFM) is a product designed to simplify fabric lifecycle management requirements for users requiring easier options than switch-by-switch offerings such as CLI and element managers. The NFM provides a simple point-n-click web-based user interface to a *fabric-aware* management engine that can build and manage fabrics based on simplified user requests. The NFM bears the heavy lifting of creating, installing, and maintaining proper fabric-wide switch configurations to deliver on these simplified requests. The NFM, being fabric-aware, also understands how the fabric should operate and can monitor and take actions within the fabric throughout its lifecycle to ensure optimal fabric operation. You can focus on workflows associated with delivering business-enabling applications and leave the complexity of building and managing the fabric to the NFM.

Behind the scenes, the NFM implements a self-managed VXLAN-based topology incorporating an EVPN control plane. This choice of technology ensures a future-proofed fabric delivering service for today and tomorrow's requirements in an open manner.

Supported Platforms

- Cisco Nexus 9500 Series switches
- Cisco Nexus 9300 Series switches
- Cisco Nexus 9200 Series switches

- Cisco Nexus 2000 Series Fabric Extenders

Supported NX-OS Releases

Table 2 Supported NX-OS Releases

7.0(3)I5(2)	This release is supported.
7.0(3)I4(1), 7.0(3)I4(2), 7.0(3)I4(3), 7.0(3)I4(4), 7.0(3)I4(5)	These releases are supported.
7.0(3)I3(1)	This release is supported.
7.0(3)I2(4), 7.0(3)I2(5)	These releases are supported.
7.0(3)I2(3)	This release is supported only if the patch for CSCuy96592 is loaded. This release does not support the Nexus Fabric Manager Auto Fabric Provisioning (AFP) feature.
7.0(3)I2(2e)	This release is supported.

Limitations

The following are the known limitations for Cisco Nexus Fabric Manager:

- The NFM does not support border-spine configurations.
- The maximum number of gateways for a fabric of 20 switches or less is 50. The maximum number of gateways for a fabric greater than 20 or up to 50 is 20.
- The maximum number of leaf switches within a supported fabric is 50.
- The maximum number of host-facing interfaces within the fabric connected to devices such as physical servers, firewalls, and load balancers is 2,400. For example, a dual-homed host would count as two host-facing attachments.
- The maximum number of discovered foreign devices is 1,200. A discovered device is any foreign device that has been discovered by the NFM through either CDP or LLDP and results in a created foreign object (host or networking device) within the NFM. A device that is connected to a leaf switch (host or networking device) that does not provide CDP or LLDP information and is enabled through a manual interface role assignment (host-facing or border) does not count towards this limit.
- The maximum number of configurable broadcast domains is limited to 500.
- The maximum number of Cisco Nexus 2000 Series of fabric extenders (FEX) supported per Leaf switch is 4. FEX Fabric interfaces must be configured on the CLI, and then host interfaces are shown and can be managed within the Cisco Nexus Fabric Manager.
- The Cisco Unified Compute System B-Series (UCS) fabric interconnect module is discoverable by the NFM. However, any compute blades behind it are not represented within the NFM topology.
- After an upgrade from a 1.1 release, the allowed range of BGP autonomous system numbers are reduced from a 4-byte to a 2-byte autonomous system. During an upgrade, any AS number greater than the limit 65535 will be converted to 65535. AS numbers should be manually checked by the administrator and modified according to their preferences before using the system due to any change to the BGP AS results in a disruptive change to the fabric.

- If using the browser Firefox, there may be an additional password prompt when logging in for the first time after a password change. This only occurs in Firefox, and once the user credentials are provided then the login process is complete.

Caveats

The open and resolved bugs for this 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.

Note: 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.

For more information about the Cisco Bug Search Tool, see the Bug Search Tool Help & FAQ.

- Known NX-OS Issues that Might Impact Cisco Nexus Fabric Manager Functionality
- Resolved Caveats - Cisco Nexus Fabric Manager, Release 1.2(3)
- Open Caveats – Cisco Nexus Fabric Manager, Release 1.2(3)

Known NX-OS Issues that Might Impact Cisco Nexus Fabric Manager Functionality

The following table describes how these NX-OS issues impact NFM. Please consult the NX-OS release notes for more details

Table 5. Cisco Nexus Fabric Manager, Release 1.2(3) – Known NX-OS Issues

Record Number	Release Note Enclosure
CSCvd10781	• **Synopsis:** When a vPC is created with native VLAN, the anycast gateway is not reachable. • **Symptoms:** Anycast gateway is not reachable and doesn't respond to pings. • **Conditions:** vPC is created with native VLAN and anycast gateway is created. • **Workarounds:** There is no known workaround.
CSCvb69890	• **Synopsis:** A Nexus 9K switch auto-provisioned using Auto Fabric Provisioning my refuse to authenticate after successful first boot. • **Symptoms:** The switch shows SearchFailed after successful provisioning using Auto Fabric Provisioning. Login at the console or authentication through NFM does not work. • **Conditions:** The switch was auto-provisioned using Auto Fabric Provisioning feature of Cisco NFM. • **Workarounds:** There is no known workaround. The only way out of this situation is to reclaim the switch using recovery mode, write erase to put the switch back into POAP mode and retry by entering a different password for the switch object inside of NFM.
CSCvb32973	• **Synopsis:** Cisco Nexus 9000 series switches become unable to save startup configuration. • **Symptoms:** Recurring faults are reported on one or more switches with the command 'copy running-config startup-config' failing with the error 'Configuration update aborted: request was aborted'. • **Conditions:** A backing for a logical gateway is created or modified, which caused the 'no ip redirects' to be issued for a SVI on a switch. As an example, this problem can be triggered by removing or changing the VRF of a logical gateway. • **Workarounds:** Manually execute the command 'no ip redirects' on the backing of the logical gateway on the switch.
CSCuz46651	• **Synopsis:** Duplicate foreign switches (FSW) would be discovered. • **Symptoms:** In the switchpool, a foreign switch (FSW) for the same switch will appear twice. • **Conditions:** If on the switch, 'ip domain-name x' is set, the system name does not match for CDP or LLDP advertisements for the switch. • **Workarounds:** Remove 'ip domain-lookup' and 'ip domain-name x' on the switch and reload it. On NFM delete the duplicate entries.

CSCvc90572	• **Synopsis:** Any configuration deployed to the switch through NX-API that contains the keyword "setup" will fail. • **Symptoms:** Configuration changes are not applied as expected. • **Conditions:** Any configuration that contains the keywork "setup" will trigger the issue. • **Workarounds:** Do not use the keyword "setup" in any configuration strings.
CSCuy96592	• **Synopsis:** Certain VRF changes may not take effect on the switch. • **Symptoms:** VRF creation does not succeed, or a VRF does not get updates after a name change. NFM reports faults on the switches related to VRF commands that report 'Requested object does not exist'. • **Conditions:** No known conditions, the failure appears to be sporadic. • **Workarounds:** No workaround, but retrying the operation using the reconcile button may help.

Note: If using the Nexus C93108YC or C93108TC-EX fixed switches or the N9K-X9732C-EX line card for the Nexus 9500 modular switch , an extra command is required before switches are to be managed by the NFM. The following command must be entered on each switch at the CLI, followed by a switch reboot, and cannot be automated by the Nexus Fabric Manager.

```
switch# system routing template-vxlan-scale
```

To verify this command has been properly applied to applicable switches and a reboot has been preformed, run the following command on the switch CLI:

```
switch# show system routing mode
Configured System Routing Mode: Vxlan Scale
Applied System Routing Mode: Vxlan Scale
```

"Configured" indicates the command has been applied, and "Applied" indicates the reboot has occurred.

Resolved Caveats – Cisco Nexus Fabric Manager Release 1.2(3)

The following table lists the Resolved Caveats in Cisco Nexus Fabric Manager, Release 1.2(3). Click the Record Number to access the Bug Search Tool and see additional information about the bug.

To see the most up-to-date list of Resolved Caveats, go to:

https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=286305124&rls=1.2(3)&sb=fr&bt=custV

Table 6. Cisco Nexus Fabric Manager, Release 1.2(3) – Resolved Caveats

Record Number	Bug Headline
CSCvc34672	Collected postgreSQL vulnerabilities
CSCvc77000	NFM neighbor purge fails with Internal Server Error
CSCvc80775	NFM overwhelming NXOS nginx with 'show interface counters detailed all'
CSCvc71838	Physical port in Border role does not disable BPDU guard on switch config
CSCvc36365	The topology tab does not load in some cases
CSCvc12747	Vulnerable version of apache in use
CSCvc12763	Vulnerable version of bind in use
CSCvc12766	Vulnerable version of binutils in use
CSCvc12782	Vulnerable version of c-ares in use
CSCvc12785	Vulnerable version of commons-collections in use
CSCvc12786	Vulnerable version of commons-fileupload in use
CSCvc12789	Vulnerable version of cpio in use
CSCvc12790	Vulnerable version of cracklib in use
CSCvc12792	Vulnerable version of curl in use

CSCvc12798	Vulnerable version of expat in use
CSCvc12803	Vulnerable version of fontconfig in use
CSCvc12812	Vulnerable version of fuse in use
CSCvc12813	Vulnerable version of giflib in use
CSCvc12824	Vulnerable version of glibc in use
CSCvc12831	Vulnerable version of gnutls in use
CSCvc12836	Vulnerable version of groovy in use
CSCvc12839	Vulnerable version of hibernate-validator in use
CSCvc12845	Vulnerable version of jbcrypt in use
CSCvc12849	Vulnerable version of jre in use
CSCvc12854	Vulnerable version of kerberos in use
CSCvc12857	Vulnerable version of lcms in use
CSCvc12859	Vulnerable version of libgcrypt in use
CSCvc12864	Vulnerable version of libidn in use
CSCvc12866	Vulnerable version of libndp in use
CSCvc12867	Vulnerable version of libssh2 in use
CSCvc12869	Vulnerable version of libtasn1 in use
CSCvc12875	Vulnerable version of libuv in use
CSCvc12878	Vulnerable version of libvirt in use
CSCvc12883	Vulnerable version of libxml2 in use
CSCvc12886	Vulnerable version of libxslt in use
CSCvc12894	Vulnerable version of linux_kernel in use
CSCvc12899	Vulnerable version of nettle in use
CSCvc12902	Vulnerable version of netty in use
CSCvc12905	Vulnerable version of nodejs in use
CSCvc12909	Vulnerable version of nss in use
CSCvc12910	Vulnerable version of ntp in use
CSCvc12914	Vulnerable version of openssh in use
CSCvc12920	Vulnerable version of openssl in use
CSCvc12922	Vulnerable version of pcre in use
CSCvc12933	Vulnerable version of qemu in use
CSCvc12940	Vulnerable version of spring_framework in use
CSCvc12949	Vulnerable version of sqlite3 in use
CSCvc12951	Vulnerable version of systemd in use
CSCvc12956	Vulnerable version of tomcat in use
CSCvc12959	Vulnerable version of v8 in use
CSCvc12961	Vulnerable version of wget in use
CSCvc12965	Vulnerable version of xalan in use
CSCvc12967	Vulnerable version of xen in use

Open Caveats – Cisco Nexus Fabric Manager Release 1.2(3)

The following table lists descriptions of open bugs in Cisco Nexus Fabric Manager, Release 1.2(3). You can use the record number to search the Cisco Bug Search Tool for details about the bug.

To see the most up-to-date list of Open Caveats, go to:

https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=286305124&rls=1.2(3)&sb=afr&bt=custV

Table 7. Cisco Nexus Fabric Manager, Release 1.2(3) – Open Caveats

Record Number	Bug Headline
CSCuz30047	A fault is created for a switch with "lldp receive" CLI failure
CSCuz26004	Applying a filter expression sometimes gives unexpected results
CSCvc91287	Cannot remove user override on profiled property in some cases when multi-editing
CSCuz25993	CLI window sometimes doesn't display all lines of output
CSCvc34652	Collected libvirt-java vulnerabilities
CSCvc37539	Commas are not supported in VRF description field.
CSCuz27969	Conflicting foreign device briefly appears
CSCvc91241	Fault indication disappears after changing membership state
CSCuz22019	Interface operational MAC address no longer gets updated
CSCuz26003	Interfaces filtered on role "unknown" but tiles show different text
CSCvb46572	Logical port channel with interfaces from two switches may not have member interfaces operational
CSCuz46218	NFM cannot resolve "CLI execution" faults
CSCuz27973	Port channels get rebuilt on monitored to managed mode transition
CSCuz25989	Switchpool available VLANs becomes 0 after editing switchpool settings
CSCvb56260	Switchpool MTU change causes some members of a vPC to become inactive
CSCuz27989	The fault "neighborMismatch" is flooded at times
CSCux43004	Transitioning unconfigured switch to managed may cause some port channels to be improperly deployed
CSCux43296	Updating object memberships seems to show an object being created
CSCuz22020	User is allowed to set the same IP address on the same VRF on different interfaces
CSCvc12748	Vulnerable version of axis in use
CSCvc12778	Vulnerable version of bzip2 in use
CSCvc12788	Vulnerable version of commons-httpclient in use
CSCvc12795	Vulnerable version of cyrus-sasl in use
CSCvc92187	Vulnerable version of glibc in use (glibc 2.24 follow up)
CSCvc12842	Vulnerable version of httpcomponents-client in use

Related Documentation

Related documentation for the Cisco Nexus Fabric Manager:

Cisco Nexus Fabric Manager

http://www.cisco.com/c/en/us/support/cloud-systems-management/nexus-fabric-manager/tsd-products-support-series-home.html

Cisco Nexus 9000 Series NX-OS Fundamentals Configuration Guide, Release 7.x

http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/7-x/fundamentals/configuration/guide/b_Cisco_Nexus_9000_Series_NX-OS_Fundamentals_Configuration_Guide_7x.html

Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide, Release 7.x

http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/7-x/interfaces/configuration/guide/b_Cisco_Nexus_9000_Series_NX-OS_Interfaces_Configuration_Guide_7x.html

Cisco Nexus 9000 Series NX-OS System Management Configuration Guide, Release 7.x

http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/7-x/system_management/configuration/guide/b_Cisco_Nexus_9000_Series_NX-OS_System_Management_Configuration_Guide_7x.html

Cisco Nexus 9000 Series NX-OS VXLAN Configuration Guide, Release 7.x

http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/7-x/vxlan/configuration/guide/b_Cisco_Nexus_9000_Series_NX-OS_VXLAN_Configuration_Guide_7x.html

Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to cnfm-docfeedback@cisco.com. We appreciate your feedback.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2015-2016 Cisco Systems, Inc. All rights reserved.