



Cisco Nexus Dashboard Insights
Software Management, Release 6.5.1 -
For Cisco NDFC or Standalone NX-OS

Table of Contents

| | |
|--|---|
| New and Changed Information | 2 |
| Software Management | 3 |
| Software Management | 3 |
| View Software Management Jobs | 3 |
| Creating Software Management | 4 |
| View Active and Susceptible Bugs | 6 |
| Pre-Validation Criteria for NDFC | 6 |
| Copyright | 9 |

First Published: 2024-07-16

Americas Headquarters

Cisco Systems, Inc.

170 West Tasman Drive

San Jose, CA 95134-1706

USA

<http://www.cisco.com>

Tel: 408 526-4000

800 553-NETS (6387)

Fax: 408 527-0883

New and Changed Information

The following table provides an overview of the significant changes up to the current release. The table does not provide an exhaustive list of all changes or of the new features up to this release.

New Features and Changed Behavior in the Cisco Nexus Dashboard Insights

| Feature | Description | Release | Where Documented |
|--------------------|---|----------------|-------------------------|
| Terminology change | The term "sites" is renamed to "fabrics". | 6.5.1 | Entire document |

This document is available from your Nexus Dashboard Insights GUI as well as online at www.cisco.com. For the latest version of this document, visit [Cisco Nexus Dashboard Insights Documentation](#).

Software Management

Software Management

Before performing an upgrade there are multiple validations that need to be performed. Similarly after an upgrade process, multiple checks helps to determine the changes and the success of the upgrade procedure.

The Software Management feature suggests an upgrade path to a recommended software version and determines the potential impact of upgrade impact. It also helps with the pre-upgrade and post-upgrade validation checks.

The Software Management feature offers the following benefits:

- Assists in preparing and validating a successful upgrade of the network.
- Provides visibility on the pre-upgrade checks.
- Provides visibility on the post-upgrade checks and the status after the upgrade.
- Minimizes the impact to the production environment.
- Provides visibility if the upgrade process is a single step or multiple steps.
- Displays the bugs applicable to a specific firmware version.

In general, we recommend that you upgrade to the latest maintenance release and patch for a particular long-lived release. If you need features that were introduced after that release, you can upgrade to the latest release.

Guidelines and Limitations

Before running a post-upgrade analysis, ensure that all the nodes are already upgraded.

View Software Management Jobs

1. Navigate to **Manage > Fabric Software Management**.

Software Management

Software Management Jobs 🕒 Last week ↻ Refresh ➕ New Analysis

Filter

Job Status



| Status | Name | Fabric | Node Target Firmware | Devices | Start Time | End Time | ⚙️ |
|-------------------|------------|---------|----------------------|-----------------|--------------------------------|--------------------------------|----|
| Analysis Failed | test-demo | ndfc129 | 9.3(12) | ni-dcnm-switch1 | Feb 09 2024 09:54:49.457 AM | Feb 09 2024 09:58:33.564 AM | |
| Analysis Failed | demo1 | ndfc129 | 10.2(6)M | ni-dcnm-switch1 | Feb 09 2024 10:09:56.556 AM | Feb 09 2024 10:13:51.061 AM | |
| Analysis Complete | test-ua-sa | aci130 | 16.0(4c) | aci-switch-103 | Feb 08 2024 11:18:51.663 AM | Feb 08 2024 11:30:30.962 AM | |
| Analysis Complete | demo | aci130 | 16.0(4c) | aci-switch-103 | Feb 09 2024 10:27:15.766 AM | Feb 09 2024 10:39:17.362 AM | |

- Use the Time selector, to select the time range.
 - The Software Management page displays the job status for your fabrics based on the selected time range.
 - Use the filter bar to filter the jobs by status.
 - The Job Status donut chart displays the number of jobs along with their status.
 - In the Jobs table you view the information for the software management jobs such as status, name, fabric, node target firmware, devices, start time, end time
- Click the gear icon to configure the columns in the Jobs table.

Creating Software Management

Procedure

- Choose **Manage > Fabric Software Management > New Analysis**.
- Enter the analysis name.
- Select a fabric. Click **Next**.
- Select the firmware. Cisco recommended release and the latest firmware release are displayed.

You can also choose to skip this step.

- Click **Select Nodes**.
 - Select the nodes. Only the nodes that are required to be updated are displayed. You can only select 10 nodes at a time per analysis.
 - Click **Add**.
- Click **Create Job**. The job is displayed in the **Software Management** Dashboard.
- Click **View Update Details** to view the pre-update analysis and post update analysis for the firmware or node.

Analysis Detail

- General - This shows if the analysis status
- Firmware summary - This shows fabric, fabric firmware, fabric target firmware, selected nodes, node firmware and node target firmware
- Upgrade path for the firmware and node. The upgrade path for firmware and node is displayed separately if the firmware is selected.

Admin > Software Management > xyz
Software Management

General
Analysis In Progress

Firmware Summary
Fabric: systest_site1
Fabric firmware: 10.2(3.124) 1
Site Target Firmware: 10.2(3.124) 1
Selected Nodes: 1
Node Firmware: 10.2(3.124) 1
Node Target Firmware: 10.2(5)M

1 Nodes
Current FW 10.2(3.124)
4 Pre-Update Checks Warning
View Update Details
Target FW 10.2(5)M

Overview

This displays the update summary, the upgrade path and the list of nodes in a tabular form.

Admin > Software Management > xyz > Update Analysis
Overview Pre-Update Analysis Post-Update Delta Analysis

Update Summary
Status: 0 Nodes of 1 Updated
Nodes by Firmware: 10.2(3.124) 1
Target Software: 10.2(5)M
Analysis Last Run: Sep 13 2023 11:26:18.163 AM

1 Nodes
Current FW 10.2(3.124)
Target FW 10.2(5)M

| Node | Model | Type | Serial | Starting Firmware |
|-------------------|-----------------|------|--------------|-------------------|
| CANDID-SYS-S1-BL1 | NBK-C93180YC-FX | leaf | FDO23170P/GH | 10.2(3.124) |

10 Rows Page 1 of 1

Pre-Update Analysis

This displays details such as node status, validation results, potential affected objects, forecasted clear alerts after the upgrade, and potential release defects applicable after the upgrade. This also shows the anomaly and advisory forecast. After fixing any of the issues highlighted in the **Validation Results** area, click **Rerun Analysis**. Click the drop down button to view pre-update validation criteria and the issues detected for each criteria. See [Pre-Validation Criteria for NDFC](#).



We recommend you to run the python script again, upload the file and then run the

assurance analysis again to check if the changes had effect on the pre-upgrade validation.

Admin > Software Management > xyz > Update Analysis

Overview **Pre-Update Analysis** Post-Update Delta Analysis Rerun Analysis

Pre-Update Summary

Status: 0 Nodes of 1 Updated

Validation Results: 24 (Passed 20, Failed 4)

POTENTIAL AFFECTED OBJECTS: 0 Applications

FORECASTED CLEARED ALERTS: 0

POTENTIAL RELEASE DEFECTS: 10 (Bugs 10, P3IRTs 0)

Analysis Last Ran: Sep 13 2023 11:25:18.163 AM

Validation Results

- Devices connectivity check: No Issues found
- Module status: No Issues found
- Module exceptions: No Issues found
- Presence of core files: No Issues found
- Dual Supervisor Redundancy: No Issues found
- Port-channel members: One or more port-channel members are not up (CANDID-SYS-S1-BL1)

Anomaly Forecast

| Critical | Major | Minor | Warning |
|----------|-------|-------|---------|
| 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 |

Advisory Forecast

| Critical | Major | Minor | Warning |
|----------|-------|-------|---------|
| 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 |

Nodes

| Node | Model | Type | Serial | Starting Firmware |
|-------------------|-----------------|------|-------------|-------------------|
| CANDID-SYS-S1-BL1 | NRK-C93180VC-FX | Leaf | FD023170PGH | 10.2(3.124) |

10 Rows Page 1 of 1

Post-Update Analysis

This displays the post-update analysis details. The post-update summary displays the status of the upgrade.

- Click **Health Delta** to view the difference in the anomalies between the pre-upgrade and post-upgrade analysis.
- Click **Operational Delta** to view the difference in the operational resources between the pre-upgrade and post-upgrade analysis.
- Click **Rerun Analysis**.

View Active and Susceptible Bugs



Ensure that Bug Scan is enabled for all fabrics.

1. Navigate to **Manage > Fabric Software Management**.
2. In the Software Management Jobs table click an analysis.

In the Firmware Summary area, hover on the Node Target Firmware and click **View Bugs** to view the active and susceptible bugs for that particular software version on that fabric. See [Bug Scan](#).

3. From the Actions dropdown menu click **Run Bug Scan** to run an on-demand Bug Scan.

Pre-Validation Criteria for NDFC

| Pre-Validation Criteria | Description | Release |
|--|--|----------------|
| Could not connect to devices | This validation checks if all devices are connected. | 6.0.1 |
| Check if modules are in ok/active/standby state | This validation checks if all modules are online. | 6.0.1 |
| Found exception log messages in module | This validation checks for non-user initiated resets. | 6.0.1 |
| Found core files on devices | This validation checks for core files. | 6.0.1 |
| Found active supervisor without HA standby | This validation checks the redundancy status on dual supervisor systems. | 6.0.1 |
| One or more port-channel members are not up | This validation checks if all port-channel members are in Up state. | 6.0.1 |
| Found non user-initiated system resets | This validation checks if system reset is due to reasons other than user-initiated. | 6.0.1 |
| Found non user-initiated module resets | This validation checks if module reset is due to reasons other than user-initiated. | 6.0.1 |
| Found modules not in ok state and without backup power | This validation checks if all modules are in ok state and if backup power present. | 6.0.1 |
| Found FAILURE/ABORT/INCOMPLETE/ErrorDisabled in module | This validation checks for FAILURE/ABORT/INCOMPLETE/ErrorDisabled results in any module. | 6.0.1 |
| Found vPC status is not in Up state | This validation checks if vPC status is in Up state. | 6.0.1 |
| Found vPC sticky bit is false | This validation checks if vPC sticky bit is false. | 6.0.1 |
| Found vPC role is not secondary | This validation checks if vPC role is secondary. | 6.0.1 |
| Found OSPF is in FULL FULL/DR state | This validation checks for OSPF interfaces and process uptime stability (12 hours). | 6.0.1 |
| Found BGP session are not in Up state | This validation checks for BGP neighbors up time stability (12 hours). | 6.0.1 |

| Pre-Validation Criteria | Description | Release |
|--|--|----------------|
| Found HSRP MGO state is not Active/Standby | This validation checks if HSRP MGO state is Active/Standby. | 6.0.1 |
| Found ARPs are in Incomplete state | This validation checks if ARPs are in Incomplete state. | 6.0.1 |
| Not enough free space to continue | This validation checks if bootflash free space is greater than threshold of 5GB. | 6.0.1 |
| Found filesystems with usage higher than 85% | This validation checks if all filesystems usage is equal to or below 85%. | 6.0.1 |
| Found console register bits are not RTS or DTR or DSR | This validation checks if console register bits are RTS or DTR or DSR. | 6.0.1 |
| Found Severity 1, 2 or 3 messages | This validation checks for Severity 1, 2 or 3 messages. | 6.0.1 |
| ISSU impact check was disruptive | This validation checks if ISSU is disruptive or non-disruptive. | 6.0.1 |
| All spines are selected in same upgrade group or no redundant spine available for some nodes | This validation checks if spine nodes are upgraded with at least two separate groups to avoid traffic loss. | 6.0.2 |
| Endpoint network redundancy | This validation checks if nodes have non-redundant connected endpoints to avoid traffic loss during the reboot of nodes. | 6.0.2 |

Copyright

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

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: <http://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)

© 2017–2024 Cisco Systems, Inc. All rights reserved.