Get Information

- Perform Nexus Health and Configuration Check

Perform Nexus Health and Configuration Check

Updated:November 7, 2023
Document ID:217990

Contents

Introduction

This document describes the procedure and requirements to perform automatic health and configuration checks for Nexus 3000/9000 and 7000 platforms.

Prerequisites

Requirements

Automated Health and Configuration Check is supported only for the Nexus platforms that run standalone NX-OS software, and not the switches that run ACI software.

These hardware platforms are supported:

- Nexus 3000/9000 series switches that run unified NX-OS software image: 7.0(3)Ix or newer
- Nexus 7000/7700 series switches that run NX-OS software version 7.x or newer

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Health and Configuration Check Procedure

Please collect `show tech-support details` or `show tech-support` logs from the Nexus switch for which you would like to perform health and config check. The `show tech-support details` is preferred, as it provides higher value with more checks done. Please make sure the logs are captured either in .txt or .gz/.tar format. Currently the `show tech-support` or `show tech-support details` file captured in ASCII and UTF-8 text formats are supported.

Open a regular TAC Service Request at Cisco Support Case Manager with these set of keywords (Technology / Sub-Technology / Problem Code):

Tech: Data Center and Storage Networking

Sub-Tech: (choose an appropriate platform)
Nexus 3000 (N3000 series only) - Health and Config Check (AUTOMATED)
Nexus 3000 (N3100-N3600 series) - Health and Config Check (AUTOMATED)
Nexus 7000 Series Switch - Health and Config Check (AUTOMATED)

Nexus 9200 - Health and Config Check (AUTOMATED)
Nexus 9300 (Non EX/FX/R Series) - Health and Config Check (AUTOMATED)
Nexus 9300 (EX/FX/R Series) - Health and Config Check (AUTOMATED)

Nexus 9400 series switches - Health and Config Check (AUTOMATED)
Nexus 9500 (Non EX/FX/R Series) - Health and Config Check (AUTOMATED)
Nexus 9500 (EX/FX/R Series) - Health and Config Check (AUTOMATED)

Nexus 9800 series switches - Health and Config Check (AUTOMATED)

Problem Code: Health and Config Check

Once the SR opened, a Cisco Guided Workflow walks you through the steps to upload the `show tech-support details` or `show tech-support` logs.

After the required output uploaded, Cisco analyzes the logs and provides a report (in PDF format) attached to an email sent to you. The report contains a list of issues detected, relevant steps to troubleshoot the problems, and recommended actions plan.

If there are questions in regards to the health check failures reported, users are advised to open a separate service request(s) with appropriate keywords to get further expert assistance. It is strongly recommended to refer the Service Request (SR) number opened for the Automated Health and Config Check along with the report generated to expedite the investigation.

Health and Configuration Check Modules

Automated Nexus Health and Configuration Check **Version 1**, August 2022 release, performs the checks listed in the Table 1.

Table 1: Health Check Modules and Associated CLIs used by the Modules

Index	Health Check Module	Brief Description of the Module	CLI(s) Used to Perform Health Check
1.	NX-OS Release Check	Checks if the device runs a Cisco recommended NX-OS software release	`show version`

2.	Nexus EoS/EoL Product Check	Verifies if any of the components (hardware/software) has reached End-of-Life (EOL) or End-of-Sale (EOS)	`show version`
			`show module`
			`show inventory`

3.	Field Notice Check	Checks if the device is potentially affected by a known PSIRT/CVE or Field Notice.	`show version`
			`show module`
			`show inventory`
			`show running-config`
			and, any command needed to check the file against a given FN/PSIRT.

4.	NX-OS CPU Health Check	Checks the symptoms for the elevated CPU utilization. It is reported when the current/historical CPU usage is >60%.	`show processes cpu`
			`show processes cpu sort`
			`show processes cpu history`
			`show system resources`

5.	NX-OS Memory Health Check	Checks if memory usage on the device is over the system memory thresholds (default or user configured values).	`show version`
			`show processes memory`
			`show system resources`

6.	NX-OS Interfaces Check	Checks if any of the interfaces reported drops in either RX or TX direction. The module prints 5 interfaces with the highest error rates in each direction.	`show interface`
			`show interface brief`
			`show queuing`

7.	CoPP Health Check	Checks if CoPP is disabled, or incorrectly configured (for example, all CPU-bound traffic that hits default-class), or have outdated CoPP policy (for example, carried over from older releases), or >1000 drops reported in non-default classes.	`show copp status`
			`show policy-map interface control-plane`
			`show running-config`

8.	Inter-process Communication (MTS) Health Check	Detects if there are any inter-process communication (referred as MTS) messages stuck for more than 1 day.	`show system internal mts buffer summary` `show system internal mts buffer details`
9.	Nexus Module Health Check	Checks if any of the modules (linecard, fabric, and so on) reported diagnostic failures or in powered down / failed state	`show moduleshow inventory` `show diagnostic result module all detail`

10.	PSU & FAN Health Check	Detects if any of the power supplies is not in operational state.	`show inventoryshow environment <options>` `show logging log` `show logging nvram`
11.	vPC Best Practices Check	Validates the device configuration meets vPC best practices, like peer-router, peer-switch, and peer-gateway configurations.	Layer3 Peer Router: `show running-config` (to check if OSPF, EIGRP and BGP adjacencies formed) Peer-Gateway / Peer-switch: `show running-config` `show spanning-tree` `show vpc brief` `show interface brief`
12.	MTU Check	Detects inconsistent MTU configurations, like Layer2 Interface and Layer3 SVI have mismatch MTU configs, Incorrect MTU on OTV Join Interfaces, or Jumbo MTU not enabled on interfaces where it is needed and so on.	`show running-configshow interface` `show ip arp <options>` `show mac address-table` `show ip route detail <options>` `show ip eigrp neighbors <options>` `show ip ospf neighbors <options>` `show bgp <options>`
13.	Layer2 feature Configuration Health Check	Checks if any L2 feature enabled but not used	`show running-config`
14.	NX-OS vPC Compatibility Check	Checks if type1/type 2 incompatibility errors reported of Virtual Port-Channels (vPC).	`show running-config` `show vpc <options>`
15.	Spanning Tree Protocol Health Check	Checks the attached outputs for an indication of Spanning Tree Protocol instabilities or in unexpected state. Module reports vlans where most recent topology changes occurred together with some additional information: timestamp, interface and Root bridge ID. Currently, this health check module supports only RSTP; the support for MST is planned for the future versions.	`show spanning-tree detail` `show spanning-tree internal errors` `show spanning-tree internal event-history <options>` `show spanning-tree active` `show logging log` `show mac address-table notification mac-move` `show system internal <L2FM, MTM, L2DBG options>`
16.	PortChannel Health Check	Detects if any of the configured port-channel members is in unhealthy state: (I), (s) (D) or (H)	`show port-channel summary`

17.	SFP Validation Check	Detects any transceivers which reported "SFP Validation Failed" error	`show interface brief`
18.	Layer3 Feature Configuration Health Check	Checks if any L3 feature enabled but not used	`show running-config`
19.	Default Route via Management VRF Check	Checks if the device has a default route configured in the Default vrf pointing through Management vrf.	`show running-config` `show accounting log`

20.	Unsupported Multicast Routing over vPC Check	Checks for unsupported PIM adjacency over vPC	`show running-config`
			`show ip pim interface vrf all internal`
			`show ip pim neighbor vrf all detail`

21.	OSPF Health Check	Checks for a possible adjacency issues observed on the device.For example:
		• multiple neighbors detected on interface configured as P2P
		• router ID not configured manually or that used a loopback IP
		• adjacencies not in FULL state
		• adjacencies which reached FULL state recently and indicates potential instability
			`show running-config`
			`show ip interface brief vrf all`
			`show ip ospf neighbors detail vrf all private`
			`show ip ospf interface vrf all private`
			`show logging log`

22.	EIGRP Health Check	Checks for a possible adjacency issues observed on the device. For example:
		• AS number not configured
		• No active neighbors detected
		• High Values of SRTT, RTO or Q Cnt detected
		• High number of dropped EIGRP packets detected
		• Lesser than 15 mins uptime of adjacency, and indicates potential instability
		• Adjacency went down in last 7 days
			`show running-config`
			`show logging log`
			`show ip eigrp neighbors detail vrf all`
			`show ip eigrp detail vrf all`

23.	BGP Peers Health Check	Checks for BGP adjacency in IDLE state.	`show running-config` `show bgp vrf all all summary`
24.	First-Hop Redundancy Protocol (FHRP)	Checks for the non-default timer configurations, as these configurations can result in a sub-optimal performance. This health check module covers ONLY Hot-Standby Routing Protocol (HSRP)	`show running-config`

Reports and Caveats

- The Health and Config Check SR is automated and handled by the Virtual TAC Engineer.
- The report (in PDF format) is usually generated within 24 business hours after all necessary logs attached to the SR.
- The report is automatically shared over email (sourced at jhwatson@cisco.com) with all contacts (primary as well as secondary) associated with the service request.
- The report is also attached to the Service Request to allow its availability at any later point in time.
- Be advised that the issues listed in the report are based on the logs provided and within the scope of the health check modules listed previously in Table 1.

- The list of health and configuration checks performed is non-exhaustive and users are advised to perform further health checks as needed.
- For Nexus 7000 with multiple Virtual Device Context (VDC) a show tech-support details file can be needed from each VDC for best results.

FAQs

Q1: Can I upload `show tech-support details` for more than one switch in the same SR to get Health Check report for all the switches?

A1: This is an automated case handling and the health checks are performed by the Virtual TAC Engineer. The health check is done for only the first `show tech-support details` uploaded.

Q2: Can I upload more than one `s` `how tech-support details` for the same device say, captured few hours apart, to get health check done for both?

A2: This is an automated and stateless case handling performed by the Virtual TAC Engineer and the Health and Config Check is done for the first the `show tech-support details` file uploaded to the SR, irrespective of whether the files uploaded are from the same switch or different switches.

Q3: Can I get health checks done for the switches whose `show tech-support details` files compressed as a single rar/gz file and uploaded to the SR?

A3: No. if multiple `show tech-support details` are uploaded as a single rar/zip/gz file, only the first file in the archive is processed for health checks.

Q4: I do not see the health and configuration check that covers the Nexus 5000/6000 platforms. Is it covered at later point in time?

A4: No. As of now, there is no plan to cover Nexus5000/6000 platforms in near future.

Q5: What can I do if I have questions about one of the health check failures reported?

A5: Please open a separate TAC Service Request to get further assistance on the specific health check result. It is highly recommended to attach the health check report and refer the Service Request (SR) Case number opened for the automated health and config check.

Q6: Can I use the same SR opened for the Automated Health and Config Check to troubleshoot the issues found?

A6: No. As the proactive health check is automated, please open a new Service Request to troubleshoot and resolve the issues reported. Please be advised that the SR opened for health check is closed with in 24 hours after the health report published.

Q7: Does the automated health and config check run against the `show tech-support details` file for the switch that runs versions older than the one mentioned previously?

A7: The automated health and configuration check is built for the platforms and software releases mentioned below. For devices that run older versions, it is best effort and there is no guarantee on the accuracy of the report.

- Nexus 3x00 series switches that run unified NX-OS software image: 7.0(3)Ix or newer
- Nexus 7000/7700 series switches that run NX-OS software version 7.x or newer
- Nexus 9x00 series switches that run unified NX-OS software image: 7.0(3)Ix or newer

Q8: How do I close the SR opened for Health Check?

A8: The SR is closed within 24 hours after the first Health Check report is sent. No action needed from the user towards SR closure.

Q9: How do I share comments or feedback about the Proactive health and configuration Check?

A9: Please share them through email to Nexus-HealthCheck-Feedback@cisco.com

Q10. What is the recommended method to capture `show tech-support` or `show tech-support details` from a switch?

A10: It is highly recommended to capture the output of `show tech-support` or `show tech-support details` command by directing it to `bootflash:` (as shown in the next example) rather than capturing it to a log file in the terminal application (for example, SecureCRT, PuTTY). Please remember the log file captured by the terminal application could be in UTF-8-BOM format (or similar) which is NOT supported by the automated health check. The Automated Health & Config check supports file only in ASCII or UTF-8 formats.

Example CLIs to redirect the output to `bootflash:` and compress the file.

```
SwitchA# show tech-support details >> bootflash:show-tech-support-details-SwitchA-2023Jan01.txt
SwitchA# gzip bootflash:show-tech-support-details-SwitchA-2023Jan01.txt
```

Feedback

Any feedback on the operations of these tool is highly appreciated. If you have any observations or suggestions (for example, about the ease of use, scope, quality of the reports generated) please share them with us at Nexus-HealthCheck-Feedback@cisco.com.

Revision History

Revision	Publish Date	Comments
9.0	07-Nov-2023	Update
8.0	08-Jun-2023	Recertification. Informational update.
7.0	07-Jun-2023	Informational update.
5.0	09-Jan-2023	Updated.+
4.0	19-Oct-2022	Informational update
3.0	04-Sep-2022	Revision
2.0	25-Jul-2022	Initial Release
1.0	25-Jul-2022	Initial Release