Durchführen einer Integritäts- und Konfigurationsprüfung für Nexus

Inhalt

Einleitung

In diesem Dokument werden das Verfahren und die Anforderungen zum Durchführen automatischer Integritäts- und Konfigurationsprüfungen für die Nexus 3000-/9000- und 7000-Plattformen beschrieben.

Voraussetzungen

Anforderungen

Die automatische Integritäts- und Konfigurationsprüfung wird nur für Nexus-Plattformen unterstützt, auf denen eigenständige NX-OS-Software ausgeführt wird, und nicht für Switches, auf denen ACI-Software ausgeführt wird.

Diese Hardwareplattformen werden unterstützt:

- Switches der Serien Nexus 3000/9000 mit einheitlichem NX-OS Software-Image: 7.0(3)Ix oder neuer
- Switches der Serien Nexus 7000/7700 mit NX-OS Software 7.x oder höher

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

Verfahren zur Integritäts- und Konfigurationsprüfung

Bitte sammeln Sie **Details zum technischen Support anzeigen** (oder) **zeigen Sie technische Support**-Protokolle vom Nexus-Switch an, für die Sie Integritäts- und Konfigurationsprüfungen durchführen möchten. **zeigen Details zum technischen Support** wird bevorzugt, da dieser einen höheren Wert bietet, wenn mehr Prüfungen durchgeführt werden. Stellen Sie sicher, dass die Protokolle entweder im TXT- oder im GZ/.tar-Format erfasst werden.

Erstellen Sie beim Cisco Support Case Manager ein regelmäßiges TAC-Serviceticket mit den folgenden Stichwörtern (Technologie/Subtechnologie/Problemcode):

Technologie: Rechenzentrums- und Speichernetzwerke

Sub-Tech: (Wählen Sie eine geeignete Plattform)
Nexus 3000 (nur Serie N3000) - Integritäts- und Konfigurationsprüfung (AUTOMATISIERT)
Nexus 3000 (Serie N3100-N3600) - Integritäts- und Konfigurationsprüfung (AUTOMATISIERT)
Switch der Serie Nexus 7000 - Integritäts- und Konfigurationsprüfung (AUTOMATISIERT)
Nexus 9200 - Integritäts- und Konfigurationsprüfung (AUTOMATISIERT)
Nexus 9300 (außer Serie EX/FX/R) - Integritäts- und Konfigurationsprüfung (AUTOMATISIERT)
Nexus 9300 (Serie EX/FX/R) - Integritäts- und Konfigurationsprüfung (AUTOMATISIERT)

Nexus Switches der Serie 9400 - Integritäts- und Konfigurationsprüfung (AUTOMATISIERT)
Nexus 9500 (außer Serie EX/FX/R) - Integritäts- und Konfigurationsprüfung (AUTOMATISIERT)
Nexus 9500 (Serie EX/FX/R) - Integritäts- und Konfigurationsprüfung (AUTOMATISIERT)

Nexus Switches der Serie 9800 - Integritäts- und Konfigurationsprüfung (AUTOMATISIERT)

Problemcode: Integritäts- und Konfigurationsprüfung

Nach dem Öffnen des Servicetickets kann ein von Cisco geführter Workflow Sie durch den Prozess führen, um die **Show Tech-Support-Details (**oder) **Show Tech-Support**-Protokolle **anzuzeigen**.

Nachdem die erforderlichen Daten hochgeladen wurden, analysiert Cisco die Protokolle und stellt einen Bericht (im PDF-Format) bereit, der einer an Sie gesendeten E-Mail beigefügt ist. Der Bericht enthält eine Liste der erkannten Probleme, relevante Schritte zur Fehlerbehebung und einen empfohlenen Aktionsplan.

Wenn Fragen zu den gemeldeten Fehlern bei der Integritätsprüfung auftreten, wird den Benutzern empfohlen, eine separate(n) Serviceanfrage(n) mit den entsprechenden Stichwörtern zu öffnen, um weitere Unterstützung von Experten zu erhalten. Es wird dringend empfohlen, die für die automatische Integritäts- und Konfigurationsprüfung geöffnete Service Request-Nummer (SR) zusammen mit dem zur Beschleunigung der Untersuchung erstellten Bericht zu verwenden.

Integritäts- und Konfigurationsprüfungsmodule

Die automatische Nexus Integritäts- und Konfigurationsprüfung **Version 1**, Version August 2022, führt die in Tabelle 1 aufgeführten Prüfungen durch.

Tabelle 1: Health Check-Module und zugehörige CLIs, die von den Modulen verwendet werden

Index	Health Check-Modul	Kurze Beschreibung des Moduls	CLI(s) für die Integritätsprüfung
1.	NX-OS-Versionsprüfung	Überprüft, ob auf dem Gerät eine von Cisco empfohlene NX-OS-Softwareversion ausgeführt wird.	show version
2.	Nexus EoS/EoL-Produktprüfung	Überprüft, ob eine der Komponenten (Hardware/Software) das End-of-Life (EOL) oder End-of-Sale (EOS) erreicht	show version show module Inventar anzeigen
3.	Prüfung von Problemhinweisen	Überprüft, ob das Gerät potenziell von einem bekannten PSIRT/CVE oder einer Problemhinweis-Meldung betroffen ist.	show version show module Inventar anzeigen show running-config und alle Befehle, die zum Überprüfen der Datei mit einer bestimmten FN/PSIRT erforderlich sind.
4.	Integritätsprüfung der NX-OS-CPU	Überprüft die Symptome für die erhöhte CPU-Auslastung. Es wird berichtet, wenn die aktuelle/historische CPU-Auslastung > 60 % ist.	show processes cpu show prozesse cpu sortieren Prozesse CPU-Verlauf anzeigen Systemressourcen anzeigen
5.	Integritätsprüfung des NX-OS-Arbeitsspeichers	Überprüft, ob die Speichernutzung auf dem Gerät die Schwellenwerte für den Systemspeicher (Standard- oder benutzerdefinierte Werte) überschreitet.	show version Prozessspeicher anzeigen Systemressourcen anzeigen
6.	NX-OS-Schnittstellenüberprüfung	Überprüft, ob eine der gemeldeten Schnittstellen in RX- oder TX-Richtung fällt. Das Modul druckt 5 Schnittstellen mit den höchsten Fehlerquoten in jede Richtung.	show interface Schnittstellenübersicht anzeigen Warteschlange anzeigen
7.	CoPP-Integritätsprüfung	Überprüft, ob CoPP deaktiviert oder falsch konfiguriert ist (z. B. der gesamte CPU-gebundene Datenverkehr, der die Standardklasse erreicht) oder veraltete CoPP-Richtlinien (z. B. Übertragung von älteren Versionen)	Kopiestatus anzeigen show policy-map interface control plane show running-config

		aufweist oder >1000 Verwerfungen in nicht standardmäßigen Klassen gemeldet wurden.	
8.	MTS-Statusprüfung (Inter-Process Communication)	Erkennt, ob Nachrichten für die Kommunikation zwischen Prozessen (als MTS bezeichnet) länger als 1 Tag blockiert sind.	show system internal mts buffer summary Systeminterne Details zum mts-Puffer anzeigen
9.	Integritätsprüfung des Nexus-Moduls	Überprüft, ob eines der Module (Linecard, Fabric usw.) Diagnosefehler meldet oder heruntergefahren/ausgefallen ist	Module anzeigenBestand anzeigen alle Details des Diagnoseergebnismoduls anzeigen
10.	Statusprüfung für Netzteil und Lüfter	Erkennt, ob eines der Netzteile nicht betriebsbereit ist.	show inventorshow environment <Optionen> Protokoll anzeigen show logging nvram
11.	vPC Best Practices Check	Überprüft, ob die Gerätekonfiguration den Best Practices für vPC entspricht, z. B. Peer-Router-, Peer-Switch- und Peer-Gateway-Konfigurationen.	<u>Layer-3-Peer-Router:</u> show running-config (um zu überprüfen, ob OSPF-, EIGRP- und BGP-Adjacencies gebildet wurden) <u>Peer-Gateway/Peer-Switch:</u> show running-config show spanning-tree vPC-Kurzübersicht anzeigen Schnittstellenübersicht anzeigen
12.	MTU-Prüfung	Erkennt inkonsistente MTU-Konfigurationen wie Layer 2-Schnittstellen und Layer 3-SVI haben unterschiedliche MTU-Konfigurationen, falsche MTU auf OTV-Join-Schnittstellen oder nicht aktivierte Jumbo-MTU auf Schnittstellen, wo sie benötigt wird usw.	show running-configSchnittstelle anzeigen show ip arp <Optionen> MAC-Adresstabelle anzeigen show ip route detail <Optionen> show ip eigrp neighbors

			<Optionen> show ip ospf neighbors <Optionen> show bgp <Optionen>
13.	Layer-2-Funktion: Integritätsprüfung der Konfiguration	Prüft, ob L2-Funktion aktiviert, aber nicht verwendet wird	show running-config
14.	NX-OS vPC-Kompatibilitätsprüfung	Überprüft, ob von Virtual Port-Channels (vPC) gemeldete Inkompatibilitätsfehler vom Typ 1/Typ 2 vorliegen.	show running-config show vpc <Optionen>
15.	Spanning Tree Protocol - Integritätsprüfung	Überprüft die angeschlossenen Ausgaben auf Anzeichen von Instabilitäten oder unerwarteten Zuständen des Spanning Tree Protocol. Das Modul meldet VLANs, in denen die letzten Topologieänderungen aufgetreten sind, sowie zusätzliche Informationen: Timestamp, Schnittstelle und Root-Bridge-ID. Derzeit unterstützt dieses Health Check-Modul nur RSTP; die Unterstützung für MST ist für zukünftige Versionen geplant.	Spanning-Tree-Details anzeigen show spanning-tree internal errors show spanning-tree internal event history <Optionen> show spanning-tree active Protokoll anzeigen MAC-Adresstabelle für Benachrichtigungen anzeigen mac-move show system internal <L2FM-, MTM-, L2DBG-Optionen>
16.	PortChannel-Zustandsprüfung	Erkennt, ob sich eines der konfigurierten Port-Channel-Elemente im fehlerhaften Zustand befindet: (I), (s) (D) oder (H)	Port-Channel-Übersicht anzeigen
17.	SFP-Validierung	Erkennt alle Transceiver, die den Fehler "SFP Validation Failed" (SFP-Validierung fehlgeschlagen) gemeldet haben	Schnittstellenübersicht anzeigen
18.	Integritätsprüfung der Layer-3-Funktionskonfiguration	Prüft, ob L3-Funktion aktiviert, aber nicht verwendet wird	show running-config

19.	Standard-Route über Management-VRF-Prüfung	Überprüft, ob auf dem Gerät eine Standardroute konfiguriert ist, die in Standard-VRF über Management-VRF verweist.	show running-config Abrechnungsprotokoll
20.	Prüfung auf nicht unterstütztes Multicast-Routing über vPC	Prüft auf nicht unterstützte PIM-Adjacency über vPC	show running-config show ip pim interface vrf all intern show ip pim neighbor vrf all detail
21.	OSPF-Integritätsprüfung	Prüft auf mögliche Adjacency-Probleme, die auf dem Gerät festgestellt wurden.Beispiel: • Mehrere Nachbarn an Schnittstelle erkannt, die als P2P konfiguriert ist • Router-ID nicht manuell konfiguriert oder Loopback-IP verwendet • Adjacencies nicht im FULL-Status • Adjacencies, die kürzlich den Status "FULL" erreicht haben und auf potenzielle Instabilität hinweisen	show running-config show ip interface brief vrf all show ip ospf neighbors detail vrf all private show ip ospf interface vrf all private Protokoll anzeigen
22.	EIGRP-Integritätsprüfung	Prüft auf mögliche Adjacency-Probleme, die auf dem Gerät festgestellt wurden. Beispiele: • AS-Nummer nicht konfiguriert • Keine aktiven Nachbarn erkannt • Hohe Werte von SRTT, RTO oder Q Cnt erkannt • Hohe Anzahl erkannter verworfener EIGRP-Pakete • Weniger als 15 Minuten Betriebszeit der Adjacency und deutet auf potenzielle Instabilität hin • Die Adjazenz nahm in den letzten 7 Tagen ab.	show running-config Protokoll anzeigen show ip eigrp neighbors detail vrf all show ip eigrp detail vrf all
23.	BGP-Peers - Integritätsprüfung	Überprüft die BGP-Adjacency im IDLE-Status.	show running-config show bgp vrf all zusammenfassung

24.	First-Hop Redundancy Protocol (FHRP)	Prüft auf nicht standardmäßige Timer-Konfigurationen, da diese Konfigurationen eine nicht optimale Leistung zur Folge haben können. Dieses Health Check-Modul deckt NUR das Hot-Standby Routing Protocol (HSRP) ab.	show running-config

Berichte und Hinweise

- Die Integritäts- und Konfigurationsprüfung (Health and Config Check SR) wird automatisiert und vom Virtual TAC Engineer durchgeführt.
- Der Bericht (im PDF-Format) wird in der Regel innerhalb von 24 Geschäftsstunden erstellt, nachdem alle erforderlichen Protokolle an den Serviceticket angehängt wurden.
- Der Bericht wird automatisch per E-Mail (über jhwatson@cisco.com) an alle Kontakte (primäre und sekundäre) weitergegeben, die der Serviceanfrage zugeordnet sind.
- Der Bericht wird auch der Serviceanfrage beigefügt, damit sie zu einem späteren Zeitpunkt verfügbar ist.
- Beachten Sie, dass die im Bericht aufgeführten Probleme auf den bereitgestellten Protokollen basieren und im Rahmen der Health Check-Module liegen, die zuvor in Tabelle 1 aufgeführt wurden.
- Die Liste der durchgeführten Integritäts- und Konfigurationsprüfungen ist nicht vollständig. Benutzern wird empfohlen, bei Bedarf weitere Integritätsprüfungen durchzuführen.

Häufig gestellte Fragen

Frage 1: Kann ich *Details zum technischen Support* für mehrere Switches im gleichen Serviceticket hochladen, um einen Health Check-Bericht für alle Switches zu erhalten?

Antwort 1: Dies ist eine automatisierte Vorgangsbearbeitung, und die Statusprüfungen werden vom Virtual TAC Engineer durchgeführt. Die Integritätsprüfung wird nur für die ersten hochgeladenen *Details zum technischen Support durchgeführt.*

Frage 2: Kann ich mehr als eine *Show-Tech-Support-Details* für das gleiche Gerät hochladen, sagen wir, erfasst ein paar Stunden auseinander, um Health Check für beide durchgeführt?

A2: Dies ist eine automatisierte und stateless-Fallbearbeitung, die vom Virtual TAC Engineer durchgeführt wird, und die Integritäts- und Konfigurationsprüfung wird für das erste Mal durchgeführt, wenn die Datei mit den *technischen Support-Details* in den Serviceticket hochgeladen wurde, unabhängig davon, ob die hochgeladenen Dateien vom selben Switch oder von verschiedenen Switches stammen.

Frage 3: Kann ich Health Checks für Switches durchführen, deren *Tech-Support-Detaildateien* als einzelne RAR/GZ-Datei komprimiert und in den SR hochgeladen werden?

A3: Nein. Wenn mehrere *Details des technischen Supports* als einzelne rar/zip/gz-Datei hochgeladen werden, wird nur die erste Datei im Archiv für Statusprüfungen verarbeitet.

Frage 4: Ich sehe keine Überprüfung der Integrität und Konfiguration der Nexus 5000/6000-Plattformen. Wird sie zu einem späteren Zeitpunkt behandelt?

A4: Nein. Derzeit ist nicht geplant, Nexus 5000/6000-Plattformen in naher Zukunft abzudecken.

Frage 5: Was kann ich tun, wenn ich Fragen zu einem der gemeldeten Fehler bei der Integritätsprüfung habe?

A5: Öffnen Sie ein separates TAC-Serviceticket, um weitere Unterstützung zu den Ergebnissen des spezifischen Gesundheitschecks zu erhalten. Es wird dringend empfohlen, den Integritätsprüfungsbericht anzuhängen und die für die automatische Integritäts- und Konfigurationsprüfung geöffnete Serviceticketnummer (Service Request, SR) zu verwenden.

Frage 6: Kann ich denselben Serviceticket wie für die automatische Integritäts- und Konfigurationsprüfung verwenden, um die gefundenen Probleme zu beheben?

A6: Nein. Da die proaktive Integritätsprüfung automatisiert wird, öffnen Sie eine neue Serviceanfrage, um die gemeldeten Probleme zu beheben. Beachten Sie, dass der zur Integritätsprüfung geöffnete Serviceticket in 24 Stunden nach Veröffentlichung des Integritätsberichts geschlossen ist.

Frage 7: Wird die automatische Integritäts- und Konfigurationsprüfung mit der Datei *mit den Show-Details* des *technischen Supports* für den Switch durchgeführt, der ältere Versionen als die oben genannte ausführt?

A7: Die automatische Integritäts- und Konfigurationsprüfung wurde für die unten genannten Plattformen und Softwareversionen entwickelt. Bei Geräten, auf denen ältere Versionen ausgeführt werden, ist dies bestmöglich, und es gibt keine Garantie für die Richtigkeit des Berichts.

- Switches der Serie Nexus 3x00 mit einheitlichem NX-OS Software-Image: 7.0(3)Ix oder neuer
- Switches der Serien Nexus 7000/7700 mit NX-OS Software 7.x oder höher
- Switches der Serie Nexus 9x00 mit einheitlichem NX-OS Software-Image: 7.0(3)Ix oder neuer

Frage 8: Wie schließe ich den Serviceticket, der für die Integritätsprüfung geöffnet wurde?

A8: Der Serviceticket wird innerhalb von 24 Stunden nach dem Versenden des ersten Health Check-Berichts geschlossen. Der Benutzer muss keine Maßnahmen zum Schließen des Servicetickets ergreifen.

Frage 9: Wie kann ich Kommentare oder Feedback zur proaktiven Integritäts- und Konfigurationsprüfung freigeben?

A9: Bitte teilen Sie sie per E-Mail an Nexus-HealthCheck-Feedback@cisco.com

Feedback

Wir freuen uns über jede Rückmeldung zu den Funktionen dieses Tools. Wenn Sie Bemerkungen oder Vorschläge haben (z. B. zur Benutzerfreundlichkeit, zum Umfang und zur Qualität der erstellten Berichte), teilen Sie diese bitte mit uns unter Nexus-HealthCheck-Feedback@cisco.com.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.