Durchführen einer Integritäts- und Konfigurationsprüfung für Catalyst

Inhalt

Einleitung

In diesem Dokument werden das Verfahren und die Anforderungen beschrieben, die für die automatische Integritäts- und Konfigurationsprüfung von Catalyst 9000-Plattformen gelten.

Voraussetzungen

Anforderungen

Die automatische Integritäts- und Konfigurationsprüfung wird nur für Catalyst 9000-Plattformen unterstützt, auf denen die Cisco IOS® XE Standalone-Software ausgeführt wird, und nicht für Switches, auf denen die Meraki-Software ausgeführt wird.

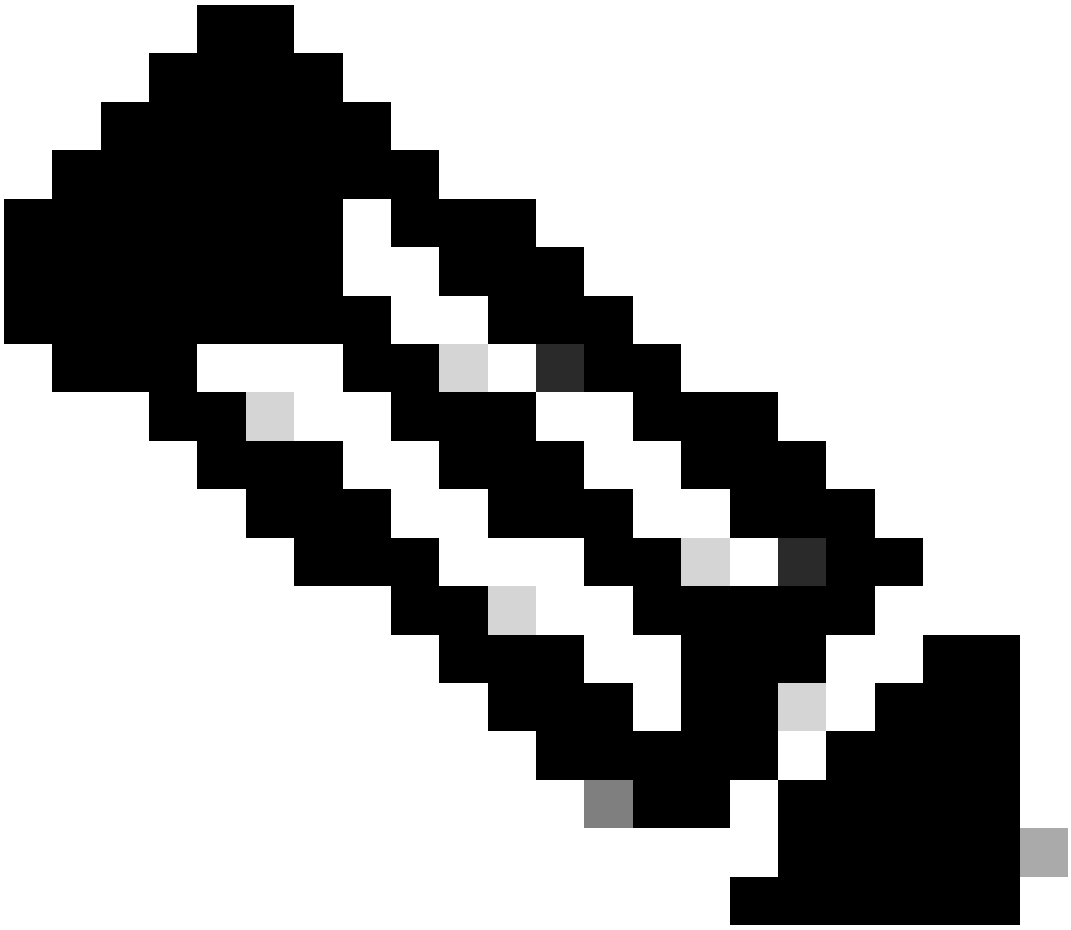
Cisco RADKit wird verwendet, um auf die Geräte zuzugreifen, auf denen die Integritätsprüfung durchgeführt wird. Eine verbundene RADKit-Instanz ist erforderlich. jhwatson@cisco.com muss ein zulässiger Benutzer sein. Lesen Sie hier die RADKit Dokumentation und Installationsanweisungen.

Wenn Cisco RADKit nicht verfügbar ist, steht auch eine Option zum manuellen Hochladen von Dateien zur Verfügung.

Diese Hardwareplattformen und Softwareversionen werden unterstützt:

- Catalyst 9200
- Catalyst 9300
- Catalyst 9400

- Catalyst 9500
- Catalyst 9600
- Cisco IOS® XE 17.3.1 und neuere Versionen



Anmerkung: Catalyst Switches der Serien 9500X und 9600X werden derzeit nicht unterstützt.

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

Um mit dem automatisierten Catalyst 9000-Gesundheitscheck zu beginnen, müssen Sie lediglich eine reguläre TAC-Serviceanfrage (TAC Service Request, SR) beim Cisco Support Case Manager mit den folgenden Schlüsselwörtern eröffnen (Technologie/Subtechnologie/Problemcode):

Tech: LAN-Switching

Sub-Tech: Catalyst 9000 - Health Check (automatisiert)

Problemcode: Integritäts- und Konfigurationsprüfung

Nach dem Öffnen des Servicetickets führt Sie ein Cisco Guided Workflow durch die einzelnen Schritte zum Hochladen der erforderlichen Protokolle.

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

Wenn Sie Fragen zu den gemeldeten Fehlern bei der Integritätsprüfung haben, wird empfohlen, einen separaten Serviceticket mit geeigneten Schlüsselwörtern zu öffnen, um weitere Unterstützung von Experten zu erhalten. Es wird dringend empfohlen, die ursprüngliche SR-Nummer, die für die automatische Integritäts- und Konfigurationsprüfung geöffnet wurde, zusammen mit dem erstellten Bericht zur Beschleunigung der Untersuchung zu verwenden.

Integritäts- und Konfigurationsprüfungsmodule

Die automatische Catalyst Integritäts- und Konfigurationsprüfung Version 1 führt die in Tabelle 1 aufgeführten Prüfungen durch.

Tabelle 1: Integritätsprüfungsmodule und zugehörige CLI-Befehle, die von den Modulen verwendet werden.

Index	Health Check-Modul	Kurze Beschreibung des Moduls	CLI-Befehl(e) zur Durchführung der Integritätsprüfung
1	CPU- und Speicherprüfung	Überprüft, ob die CPU- und Speichernutzung die Systemschwellenwerte überschreitet.	Plattformressourcen anzeigen
2	TCAM-Integritätsprüfung	Überprüft, ob der TCAM	show platform hardware

		über TCAM-Banken verfügt, die nahezu vollständig ausgelastet sind oder derzeit überausgelastet sind	fed switch active fwd-asic resource tcam usage*
3	Integritätsprüfung des Objektmanagers	Überprüft, ob im Objektmanager festsitzende oder ausstehende Objekte vorhanden sind.	show platform software object-manager switch active f0 statistics*
4	ASIC-Statusprüfung	Überprüft, ob ASIC-Ressourcen nahezu vollständig oder bereits vollständig genutzt werden	show platform hardware fed switch active fwd-asic resource usage*
5	Control Plane Policer-Prüfung	Überprüft, ob eine Kontrollebenen-Richtlinienwarteschlange übermäßige Dropwerte aufweist.	Zeigt den Status der aktiven QoS-Warteschlange für den hardwaregesteuerten Switch der Plattform an. Interne CPU-Überwachung*
6	Überprüfung von PSU, PoE und Lüfter	Überprüft den Umgebungsstatus von Netzteilen, Lüftern und der PoE-Fähigkeit.	Umgebung anzeigen alle
7	GOLD-Prüfung (Generic Online Diagnostic)	Prüft die Diagnoseergebnisse auf Fehler	Zeigt das Diagnoseergebnismodul mit allen Details an*
8	Selbsttest beim Einschalten	Überprüft, ob auf dem System ein POST-Fehler festgestellt wird.	show post
9	Schnittstellenintegritätsprüfung	Prüft die Schnittstellenzähler auf Fehler (CRC, Giganten, Ausgabefehler)	show interfaces
10	Fehler beim Deaktivieren der Überprüfung	Überprüft, ob derzeit Schnittstellen fehlerhaft deaktiviert sind.	show interfaces status err-disabled
11	SFP-Integritätsprüfung	Überprüft, ob optische Produkte von Drittanbietern vorhanden sind.	Inventar anzeigen
12	Prüfung der empfohlenen Version	Überprüft, ob auf dem System die aktuelle empfohlene Software	show version

		ausgeführt wird.	
13	StackWise Virtual Health Check	Überprüft, ob SVL Best Practices implementiert sind, wenn das System im HA-Modus ausgeführt wird	StackWise-Virtual anzeigen show stackwise-virtual-Link show stackwise-virtual dual-active-detection
14	Spanning Tree-Konfigurationsprüfung	Überprüft, ob STP Best Practices implementiert sind	show spanning-tree Spanning Tree-Instanzen anzeigen Spanning-Tree-Übersicht anzeigen Spanning-Tree-Details anzeigen show spanning-tree inconsistentPorts show running-config
15	Prüfung der Sicherheitsberatung	Prüft Konfigurationen auf bekannte Sicherheitsempfehlungen	AP-Status anzeigen App-Hostingliste anzeigen avc sd-service info detailliert anzeigen Inventar anzeigen show iox-service ip nat statistik anzeigen IP-Sockets anzeigen IP SSH anzeigen show mdns-sd Zusammenfassung show module

			Redundanz zeigen Subsysteme anzeigen Show udld udp anzeigen Übersicht zur Wireless-Mobilität anzeigen show ip interface brief show run all show snmp-benutzer

* Befehle variieren je nach Switch-Modell und ob sie Teil einer StackWise- oder einer StackWise-Virtual-Konfiguration sind.

Manuelles Hochladen von Dateien

Um die Benutzerfreundlichkeit des manuellen Datei-Uploads zu optimieren, werden die erforderlichen Befehle je nach Hardwarekonfigurationstyp aufgelistet. Kopieren Sie die Befehlsliste, fügen Sie sie in eine Datei ein, und laden Sie sie hoch, wenn Sie dazu aufgefordert werden.

Catalyst 9200 Standalone oder Catalyst 9200 StackWise

Catalyst 9300 Standalone oder Catalyst 9200 StackWise

Catalyst 9500 in StackWise-Virtual

```
term exec prompt expand
show version
show running-config
show redundancy
show platform resources
show wireless mobility summary
show run all
show ap status
show snmp user
show ip ssh
show spanning-tree inconsistentports
show platform hardware fed switch active qos queue stats internal cpu policer
show app-hosting list
show ip sockets
show udld
show environment all
show avc sd-service info detailed
show iox-service
```

```
show spanning-tree detail
show spanning-tree instances
show platform hardware fed switch active fwd-asic resource utilization
show spanning-tree
show interfaces
show platform hardware fed switch active fwd-asic resource tcam utilization
show udp
show mdns-sd summary
show post
show process cpu sorted | exclude 0.00
show module
show ip interface brief
show process cpu platform sorted | exclude 0% 0% 0%
show inventory
show interfaces status err-disabled
show platform hardware fed switch active fwd-asic resource rewrite utilzation
show logging
show diagnostic result module all detail
show platform software object-manager switch active f0 statistics
show spanning-tree summary
show subsys
show ip nat statistics
```

Catalyst 9500, Standalone

```
term exec prompt expand
show version
show running-config
show module
show inventory
show iox-service
show spanning-tree instances
show run all
show platform resources
show subsys
show ip nat statistics
show udld
show interfaces
show platform hardware fed active fwd-asic resource rewrite utilzation
show spanning-tree detail
show wireless mobility summary
show platform hardware fed active fwd-asic resource tcam utilization
show snmp user
show platform hardware fed active qos queue stats internal cpu policer
show spanning-tree inconsistentports
show diagnostic result module all detail
show ip sockets
show mdns-sd summary
show ap status
show process cpu sorted | exclude 0.00
show avc sd-service info detailed
show udp
show ip ssh
show spanning-tree
show redundancy
show post
show logging
show process cpu platform sorted | exclude 0% 0% 0%
```

```
show app-hosting list
show platform software object-manager f0 statistics
show ip interface brief
show platform hardware fed active fwd-asic resource utilization
show interfaces status err-disabled
show spanning-tree summary
show environment all
```

Catalyst 9400 Standalone und Catalyst 9600 Standalone

```
term exec prompt expand
show version
show running-config
show ip sockets
show ip interface brief
show ap status
show ip nat statistics
show diagnostic result module all detail
show ip ssh
show iox-service
show snmp user
show interfaces status err-disabled
show run all
show wireless mobility summary
show logging
show redundancy
show spanning-tree detail
show module
show mdns-sd summary
show spanning-tree
show app-hosting list
show udld
show process cpu sorted | exclude 0.00
show udp
show platform hardware fed active qos queue stats internal cpu policer
show spanning-tree instances
show platform resources
show inventory
show avc sd-service info detailed
show process cpu platform sorted | exclude 0% 0% 0%
show platform hardware fed active fwd-asic resource utilization
show post
show interfaces
show platform software object-manager f0 statistics
show platform hardware fed active fwd-asic resource rewrite utilzation
show platform hardware fed active fwd-asic resource tcam utilization
show environment all
show spanning-tree summary
show spanning-tree inconsistentports
show subsys
```

Catalyst 9400 in Stackwise-Virtual und Catalyst 9600 in Stackwise-Virtual

```
term exec prompt expand
show version
show running-config
show stackwise-virtual
show spanning-tree summary
show spanning-tree
show platform software object-manager switch active f0 statistics
show platform hardware fed switch active fwd-asic resource rewrite utilization
show inventory
show ap status
show platform hardware fed switch active fwd-asic resource tcam utilization
show avc sd-service info detailed
show run all
show udp
show interfaces status err-disabled
show subsys
show stackwise-virtual dual-active-detection
show environment all
show platform resources
show logging
show ip sockets
show stackwise-virtual link
show platform hardware fed switch active qos queue stats internal cpu policer
show platform hardware fed switch active fwd-asic resource utilization
show app-hosting list
show ip interface brief
show post
show diagnostic result switch all all detail
show process cpu sorted | exclude 0.00
show spanning-tree instances
show udld
show snmp user
show iox-service
show process cpu platform sorted | exclude 0% 0% 0%
show spanning-tree detail
show ip nat statistics
show mdns-sd summary
show wireless mobility summary
show redundancy
show module
show interfaces
show spanning-tree inconsistentports
show ip ssh
```

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 (von jhwatson@cisco.com bezogen) an alle mit dem Serviceticket verbundenen Kontakte (primäre und sekundäre) weitergegeben.
- Der Bericht wird auch dem Serviceticket hinzugefügt, damit es 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 die Befehlsausgabe manuell hochladen, anstatt Cisco RADKit zu verwenden?

Antwort 1: Ja: Wenn Cisco RADKit nicht installiert ist, steht eine Option zum manuellen Hochladen von Dateien zur Verfügung.

Frage 2: Was kann ich tun, wenn ich Fragen zu einem der gemeldeten Fehler bei der Integritätsprüfung habe?

Antwort 2: Bitte reichen Sie eine separate TAC-Serviceanfrage ein, um weitere Unterstützung für das jeweilige Ergebnis des 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 3: Kann ich denselben Serviceticket verwenden, der für die automatische Integritäts- und Konfigurationsprüfung geöffnet wurde, um die gefundenen Probleme zu beheben?

A3 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 4: Wie schließe ich das für die automatische Integritätsprüfung geöffnete Serviceticket?

Antwort 4: 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.

Feedback

Wir freuen uns über jegliches Feedback zum Betrieb dieses Tools. Falls Sie Anmerkungen oder Anregungen haben (z. B. zur Benutzerfreundlichkeit, zum Umfang, zur Qualität der erstellten Berichte), teilen Sie diese bitte mit atCatalyst-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.