

Sammeln von Protokollen in der Cisco DNA Center Quick Start Guide

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[AURA Tool zur Durchführung von Health-, Scale- und Upgrade-Bereitschaftsprüfungen](#)

[Kategorisierung von Cisco DNA Center-Problemen](#)

[Protokolle, die bei Upgrade-Problemen gesammelt werden müssen](#)

[Zu erfassende Protokolle für Automatisierung, Gewährleistung oder SDA-/Nicht-SDA-Bereitstellungsprobleme](#)

[Protokolle, die bei GUI-Problemen erfasst werden sollen](#)

[Von Netzwerkgeräten zu erfassende Protokolle für Probleme mit Netzwerken mit softwaredefiniertem Zugriff](#)

Einleitung

In diesem Dokument werden die Schritte zur Erfassung der erforderlichen Protokolle und Befehlsausgaben von Cisco DNA Center beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Der Benutzer muss über eine Kommandozeile (Command Line Interface, CLI) mit dem Cisco DNA Center verbunden sein.
- Um sich über CLI bei Cisco DNA Center anzumelden, müssen Sie über Secure Socket Shell (SSH) eine Verbindung zur IP-Adresse Ihres Cisco DNA Centers mit Maglev als Benutzername auf Port 222 herstellen.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco DNA Center

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.

Hintergrundinformationen

Wenn Sie diese Informationen im Voraus in einem Technical Assistance Center (TAC)-Serviceticket (SR) angeben, können Sie das Problem schnell und problemlos lösen.

AURA Tool zur Durchführung von Health-, Scale- und Upgrade-Bereitschaftsprüfungen

Verwenden Sie das AURA-Tool, das auf Github verfügbar ist, um Health-, Scale- und Upgrade Readiness-Prüfungen im Cisco DNA Center durchzuführen. Das Tool kann auch die Ausgaben von den Fabric-Geräten, ISE und WLC erfassen, um mehrere Integritäts-, Kontroll- und Sicherheitsebenen sowie Assurance-basierte Prüfungen durchzuführen. Die Ausführung vor einem Upgrade ist äußerst nützlich, um ein reibungsloses und erfolgreiches Upgrade zu gewährleisten. Die regelmäßige Ausführung des Tools kann geplant werden.

Weitere Informationen finden Sie [hier](#).

Kategorisierung von Cisco DNA Center-Problemen

Bei Problemen mit den in der Problembeschreibung erwähnten Komponenten lesen Sie die entsprechenden Problemkategorien weiter unten, um die erforderlichen Informationen zu sammeln.

Problemkategorie	Problembeschreibung
Upgrade	Alle Fehler, die während der System-/Anwendungs-Upgrades festgestellt wurden.
Automatisierung	Sichern und Wiederherstellen Hohe Verfügbarkeit Managed Services Inventarisierung/Erkennung Netzwerkdesign Bereitstellung IP-Pools LAN-Automatisierung SCHWIMMEN Bereitstellung von Vorlagen NFV-Bereitstellung PNP Smart Licensing Zugriffsrichtlinie (ACA) Karten-Topologie Integrationsprobleme mit ISE, CMX, Cisco DNA-Spaces, UDN, NBAPI, NB-Benachrichtigungen usw.
Nicht-SDA-	Alle bei Nicht-SDA-Bereitstellungsabläufen beobachteten Fehler.

Bereitstellung	
Sicherheit	Analysen und Berichte Telemetrie Alle anderen Fehler, die in Assurance-Flows beobachtet wurden.
Probleme mit der Benutzeroberfläche	Es empfiehlt sich, zusätzlich zu den Informationen, die in anderen bereichsspezifischen Gruppen angefordert werden, alle in der GUI beobachteten Fehler zu erfassen.
Software-Defined Access	Alle bei den Software-Defined Access Fabric-Geräten festgestellten Fehler.

Protokolle, die bei Upgrade-Problemen gesammelt werden müssen

Schritt 1: Erfassen Sie in der CLI von Cisco DNA Center die folgenden Befehlsausgaben:

```
maglev system_updater update_info
maglev catalog settings display
maglev catalog release_channel display -V
maglev catalog settings validate
etcdctl get /maglev/config/cluster/cloud
maglev catalog system_update_package display
maglev catalog package display
```

Schritt 2: Senden Sie die Ausgabe des System-Updater-Diensts an eine Protokolldatei, und verwenden Sie diesen Befehl, und erfassen Sie die Datei im Ordner /tmp.

```
magctl service logs -r system-updater > /tmp/system-updater.log
```

Schritt 3: Sammeln Sie die RCA-Protokolle gemäß den Anweisungen in diesem [Dokument](#).

Zu erfassende Protokolle für Automatisierung, Gewährleistung oder SDA-/Nicht-SDA-Bereitstellungsprobleme

Schritt 1: Sammeln Sie die RCA-Protokolle gemäß den Anweisungen in diesem [Dokument](#).

Schritt 2: Ausführen des [Cisco DNA Center AURA-Tools](#)

Protokolle, die bei GUI-Problemen erfasst werden sollen

Schritt 1: Sammeln Sie die RCA-Protokolle gemäß den Anweisungen in diesem [Dokument](#).

Schritt 2: Ausführen des [Cisco DNA Center AURA-Tools](#)

Schritt 3: Sammeln Sie HAR-Dateien vom Webbrowser. Schritt für Schritt Anleitungen für Chrome folgen:

- Wenn in der GUI ein Fehler angezeigt wird, navigieren Sie zur Seite, klicken mit der rechten Maustaste darauf, und wählen Sie **Inspizieren**.

The screenshot shows the Cisco DNA Center Assurance Summary dashboard. The 'Health' section displays three metrics: Network Devices at 67%, Wireless Clients at --%, and Wired Clients at 100%. The 'Critical Issues' section shows 26 P1 and 23 P2 issues. A context menu is open over the 'Sites' section, with 'Inspect' highlighted. The 'Sites' section shows 5 sites, with 1 Unclaimed, 5 Unprovisioned, and 2 Unreachable. The 'Application' section shows 0 applications.

- Inspect öffnet die Entwicklertools auf der rechten Seite. Navigieren Sie zur Registerkarte "**Netzwerk**", und klicken Sie darauf:

The screenshot displays the Cisco DNA Center interface. At the top, it says "Cisco DNA Center" and "Welcome, admin". Below this is a banner for new capabilities. The main content is divided into two sections: "Assurance Summary" and "Network Snapshot".

Assurance Summary

- Health**: Healthy as of Jun 12, 2020 3:20 PM. Shows 67% for Network Devices, 100% for Wireless Clients, and 100% for Wired Clients. A "View Details" link is present.
- Critical Issues**: Last 24 Hours. Shows 26 P1 and 23 P2 issues. A "View Details" link is present.
- Trends and Insights**: Last 7 Days. Shows two dashed lines for Throughput and Coverage. A "View Details" link is present.

Network Snapshot

- Sites**: As of Jun 12, 2020 3:22 PM. Shows 5 sites, 0 DNS Servers, and 0 NTP Servers. An "Add Sites" link is present.
- Network Devices**: As of Jun 12, 2020 3:22 PM. Shows 10 devices, 1 Unclaimed, 5 Unprovisioned, and 2 Unreachable. A "Find New Devices" link is present.
- Application Policies**: As of Jun 12, 2020 3:29 PM. Shows 0 policies. An "Add Policies" link is present.

The screenshot shows the Chrome DevTools Network tab. The "Network" tab is selected, and a list of network requests is visible. A red circle highlights the "Download" icon (a downward-pointing arrow) next to a request. Below the network requests, the "Console" tab is open, showing "What's New X" and "Highlights from the Chrome 83 update".

- Klicken Sie auf den **Download-Pfeil** (HAR exportieren) wie folgt:

The screenshot displays the Cisco DNA Center interface. The main dashboard includes sections for Assurance Summary (Health, Critical Issues, Trends and Insights) and Network Snapshot (Sites, Network Devices, Application Policies). On the right, the Chrome DevTools Network tab is open, showing a list of blocked requests with columns for Name, Status, and Type.

- **Speichern Sie** die HAR-Datei lokal, und laden Sie sie auf Ihre TAC-Serviceanfrage hoch.

Von Netzwerkgeräten zu erfassende Protokolle für Probleme mit Netzwerken mit softwaredefiniertem Zugriff

Schritt 1: Erfassung (über Cisco DNA Center Command Runner / oder direkt über die Geräte-CLI) aller Control-Nodes, Border-Nodes sowie betroffener Ränder für eine bestimmte Software-Defined Access Fabric-Site:

Anschlusslänge 0

show tech-support

Show Tech-Support Fabric

Anzeigen von technischen Support-Listen

show tech-support cef

show tech-support isis

show tech-support platform

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.