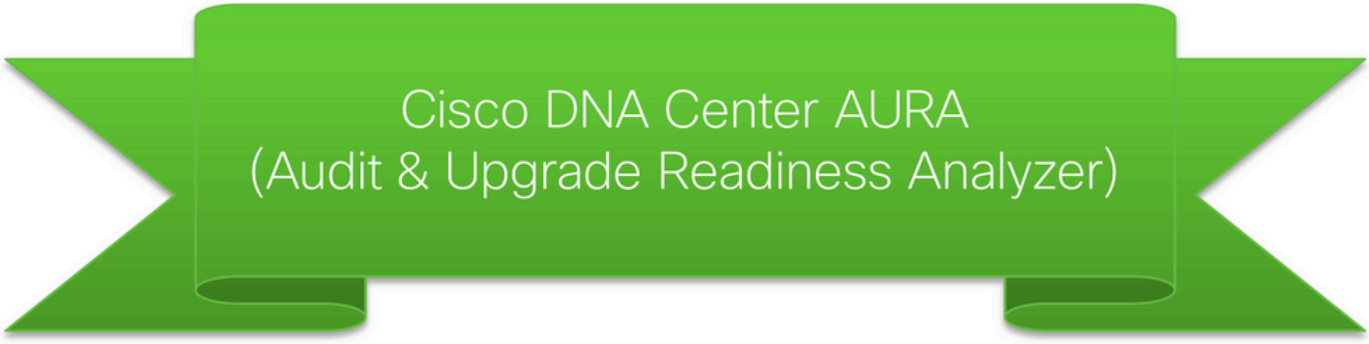
Nutzen Sie AURA für mehr Transparenz im DNA-Center

Inhalt



Einleitung

Dieses Dokument beschreibt das Befehlszeilentool Cisco DNA Center Audit and Upgrade Readiness Analyzer (AURA).

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der Cisco DNA Center-Plattform.

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

AURA führt eine Vielzahl von Integritäts-, Skalierungs- und Upgrade-Bereitschaftsprüfungen für das Cisco DNA Center und das übrige Fabric-Netzwerk durch. Die Ausführung des Tools ist äußerst einfach und erfolgt in Cisco DNA Center. Das Tool verwendet API-Aufrufe (Application Programming Interface), DB liest und zeigt Befehle (schreibgeschützte Vorgänge) und beeinträchtigt daher weder die Leistung noch das Cisco DNA Center oder die Netzwerkgeräte.

Warum ist AURA so unkompliziert und benutzerfreundlich

- Verwendet NUR vorinstallierte Bibliotheken/Software.
- Automatisch generierter PDF-Bericht.
- Einzige erforderliche Eingabe: Cisco DNA Center-Kennwörter (admin und maglev).
- Gezippte Protokolle und Berichte können automatisch auf Cisco SR hochgeladen werden (optional).

- Kopieren Sie einfach die Datei in Cisco DNA Center und führen Sie sie dort aus.
- Nicht aufdringlich - nur Datenbank (DB) liest, zeigt Befehle und API-Aufrufe an.
- Ausführungszeit - weniger als 15 Minuten für die Cisco DNA Center-Prüfungen, und die Zeit variiert für die SDA-Prüfungen (Software Defined Access) je nach Größe des Netzwerks (etwa 30 Minuten für 30 Geräte).
- Funktioniert mit den Versionen 1.2.8, 1.2.10.x, 1.2.12.x, 1.3.x und 2.x.

Bitte kontaktieren Sie uns bei Problemen oder Feedback unter dnac_sda_audit_tool@cisco.com.

AURA-Tool: Überprüfungsbereiche und Merkmale

- Cisco DNA Center Scale-Test
- Cisco DNA Center Infra. Health
- Cisco DNA Center Assurance Health
- Zustand von WLC/eWLC Assurance
- CLI-Erfassung auf SDA-Geräten
- SDA-Kontrolle und Sicherheits-Audit
- Softwarefehler, die zu Upgrade-Fehlern führen
- Prüfungen zur Upgrade-Bereitschaft
- SDA-Kompatibilitätsprüfung (Switches, Wireless Controller und Identity Services Engine (ISE) für 2.3.3.x
- Digital Network Architecture Center (DNAC)-ISE-Integrationsprüfungen
- Fabric-Gerätekonfigurationen: Erfassung und Vergleich sowie Verwendung des integrierten Vergleichstools
- Remote-Start von AURA (ab Version 1.2.0)
- AURA mit Cron planen (ab Version 1.2.0)
- Syslog-Serverintegration (ab Version 1.2.0)
- Herunterladen von Test-Images aus der Cloud (ab Version 1.5.0)

So führen Sie das Tool aus (einfache Schritte)

Schritt 1: Kopieren Sie die ausführbare AURA-Datei in Cisco DNA Center. Die neueste Version finden Sie unter https://github.com/CiscoDevNet/DNAC-AURA.

Schritt 2: Führen Sie das Tool vom Cisco DNA Center aus (falls Sie einen Cluster haben, sehen Sie sich Beispiel 5 im Abschnitt "Cisco DNA Center AURA-Optionen" an).

```
$ ./dnac_aura
```

So führen Sie das Tool aus (detaillierte Schritte)

Wenn die Cisco DNA Center-Version 2.3.3.x oder höher ist, verfügt Cisco DNA Center über eine eingeschränkte Shell, die ab Version 2.3.3.x zusätzliche Sicherheit bietet. Die Standard-Shell heißt magshell und unterstützt keine Linux-Befehle oder die Ausführung von AURA. Deaktivieren

Sie die eingeschränkte Shell, und aktivieren Sie die Bash-Shell, bevor Sie mit dem nächsten Schritt fortfahren. Deaktivierung der eingeschränkten Shell unter 2.3.3.x. Bei Version 2.3.4.x und höher kann ein Zustimmungstoken vom Cisco Technical Assistance Center (TAC) benötigt werden, um die eingeschränkte Shell zu deaktivieren.

Schritt 1: Kopieren Sie die ausführbare Datei in Cisco DNA Center.

```
dnac_aura
```

Die Datei befindet sich unter https://github.com/CiscoDevNet/DNAC-AURA. Es gibt mehrere Möglichkeiten, die Datei in Cisco DNA Center zu kopieren.

Option 1: Klicken Sie auf die URL und laden Sie die Datei über Ihren Browser herunter:

Kopieren Sie die Datei in Ihr Cisco DNA Center und verwenden Sie eine Dateiübertragungssoftware (vergessen Sie nicht, Secure File Transfer Protocol (SFTP) mit Port 2222 und Benutzername maglev zu verwenden).

Option 2: Kopieren Sie die Datei direkt in das Cisco DNA Center, und verwenden Sie die GIT-Befehle:

```
$ git clone https://github.com/CiscoDevNet/DNAC-AURA
```

Option 3: Wenn ein Proxy-Server eingerichtet wurde, kopieren Sie die Datei in das Cisco DNA Center, verwenden Sie GIT-Befehle und die Proxy-Server-Details:

```
$ https_proxy=https://<server>:<port> git clone https://github.com/CiscoDevNet/DNAC-AURA
```

Schritt 2: Stellen Sie sicher, dass die Datei dnac_aura ausführbar ist.

Wenn die Datei dnac_aura in das Cisco DNA Center kopiert wird, wird sie normalerweise nicht als ausführbare Datei kopiert. Führen Sie den Befehl aus, um sie ausführbar zu machen. Wenn Sie GIT verwendet haben, ist dieser Schritt nicht erforderlich.

```
$ chmod 755 dnac_aura
```

Schritt 3. (Optional) Überprüfen Sie den Hash der Datei dnac_aura, um sicherzustellen, dass die richtige Datei heruntergeladen wurde.

Um sicherzustellen, dass die richtige Datei heruntergeladen wurde, vergleichen Sie entweder den MD5- oder den SHA256-Hashwert, die am Ende dieser Seite aufgeführt sind. Jede Version von AURA kann über einen eindeutigen Satz von Hashwerten verfügen.

Option 1: MD5-Hashüberprüfung.

Verwenden Sie den Befehl md5sum (wie aufgeführt). Generieren Sie den Hash auf Ihrem Cisco DNA Center oder einem anderen Linux-System, und vergleichen Sie den Hash-Wert mit dem Wert am Ende dieser Seite.

```
$ md5sum dnac_aura
52f429dd275e357fe3282600d38ba133 dnac_aura
```

Option 2: SHA256 Hash-Verifizierung.

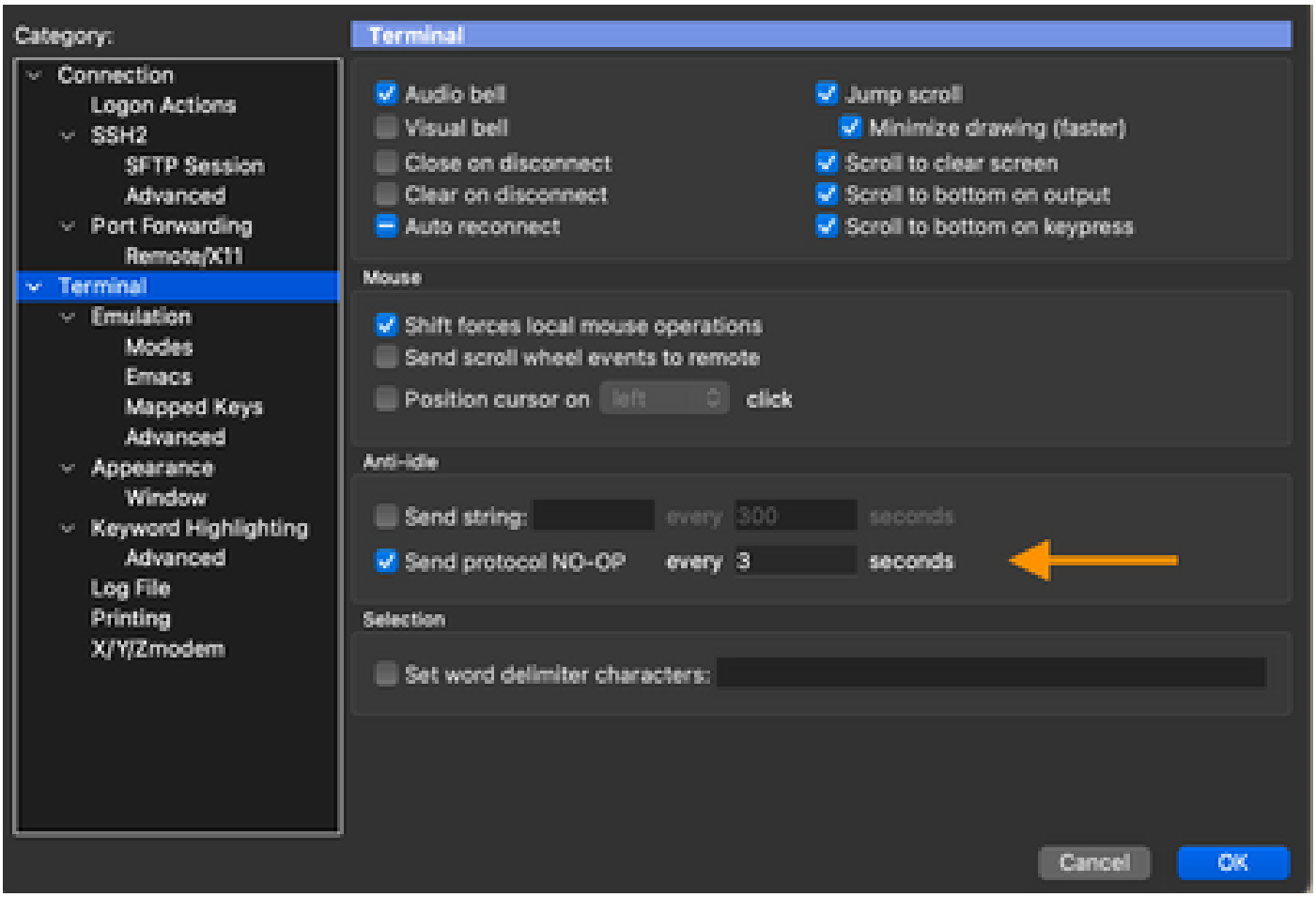
Verwenden Sie den Befehl sha256sum (wie aufgeführt). Generieren Sie den Hash auf Ihrem Cisco DNA Center oder einem anderen Linux-System, und vergleichen Sie den Hash-Wert mit dem Wert am Ende dieser Seite.

```
$ sha256sum dnac_aura
c91b6092ab4fa57adbe698a3c17f9146523bba5b0315222475aa4935662a0b6e dnac_aura
```

Schritt 4: Legen Sie ein Leerlauf-Timeout für die SSH-Sitzung fest.

Spätere Versionen (2.x +, 1.3.3.8+) von Cisco DNA Center haben ein SSH-Leerlauf-Timeout. Dies kann Auswirkungen haben, wenn AURA über eine SSH-Sitzung ausgeführt wird. Stellen Sie sicher, dass die Leerlaufzeitüberschreitung eingestellt ist. Andernfalls kann das AURA-Tool abrupt beendet werden.

Hier ein Beispiel für das Festlegen eines Leerlauf-Timeouts von 3 Sekunden auf SecureCRT.



Schritt 5: Führen Sie das Tool über die Befehlszeile aus.

Wählen Sie die entsprechende Option aus, je nachdem, wo sich die Datei befindet, um die Prüfungen im Cisco DNA Center durchzuführen. (Wenn Sie Optionen verwenden, können Sie verschiedene Prüfungen ein- bzw. ausschließen.)

```
$ ./dnac_aura
```

Oder

```
$ ./DNAC-AURA/dnac_aura
```

Remote-Ausführung von AURA

Mit diesem Skript können Sie die AURA auf einem entfernten Cisco DNA Center starten. Es verwendet paramiko- und scp-Bibliotheken.

Installationsverfahren

Für die Installation wird eine virtuelle Umgebung empfohlen. Diese Leitungen können eine virtuelle python3-Umgebung erstellen, aktivieren, pip aktualisieren und die erforderlichen Bibliotheken installieren.

```
python3 -m venv env3
source env3/bin/activate
pip install --upgrade pip
pip install -r requirements.txt
```

Sitzungs-Timeout

Spätere Versionen (2.1+, 1.3.3.8+) von Cisco DNA Center haben ein SSH-Leerlauf-Timeout. Dies kann Auswirkungen haben, wenn AURA von einer SSH-Sitzung entweder direkt auf DNAC oder indirekt über das Skript run_remote oder ansible ausgeführt wird.

Die Problemumgehung ist einfach. Bei einer SSH-Verbindung kann das -o ServerAliveInterval=3-Flag Keepalives senden und die Sitzung aufrechterhalten. Dies wird in diesem Skript verwendet und kann auch für direkte ssh-Verbindung sowie ansible verwendet werden.

Skript verwenden

Das Skript erfordert drei Argumente:

- DNAC
- admin password (auch als Umgebungsvariable DNAC_ADMIN_PASS verfügbar)
- maglev password (auch als Umgebungsvariable DNAC_MAGLEV_PASS verfügbar)
- admin user (auch als Umgebungsvariable DNAC_ADMIN_USER verfügbar). Dies ist standardmäßig "admin" und muss nur geändert werden, wenn Sie eine externe Authentifizierung und einen anderen SuperUser-Namen verwenden. In vielen Fällen ist dies nicht erforderlich, ist aber als --admin-user verfügbar.

Der einfachste Weg, das Skript mit Argumenten auszuführen (siehe Abschnitt zu Umgebungsvariablen weiter unten), ist

```
./run_remote.py --dnac 1.1.1.1 --admin-pass passwd --maglev-pass passwd
```

Wenn Sie mit Shell-Umgebungsvariablen vertraut sind, kann dies weiter vereinfacht werden

```
export DNAC_ADMIN_PASS="passwd"
export DNAC_MAGLEV_PASS="passwd"
./run_remote.py --dnac 10.1.1.1
```

AURA-Optionen übergeben (—)

Um AURA-spezifische Argumente zu übergeben (z. B. -s zum Ausführen von SDA-Tests), müssen Sie Folgendes tun:

```
## note the extra --, due to a qwirk in the way argparse library works
./run_remote.py --dnac 10.1.1.1 -- -s
```

Stellen Sie sicher, dass Sie alle run_remote-Optionen wie --local-dir, all-cluster und --no-pull VOR dem „--“ einfügen

AURA-spezifische Optionen wie -n, --syslog, -d, -s müssen nach dem „--“ stehen

AURA-Ausgabe lokal speichern

Das AURA-Skript unterstützt die Option --json-summary. Dadurch wird eine JSON-Zusammenfassung der Testergebnisse sowie des Speicherorts der Berichts- und Protokolldatei in DNAC erstellt. Wenn run_remote mit der Option —local-dir ausgeliefert wird, können die Protokoll- und Berichtsdateien zurück in DNAC verschoben werden. Eine json-summary-Datei kann erstellt werden. Ein Verzeichnis für die DNAC wird erstellt.

```
/home/aradford/RUN_REMOTE/run_remote.py --dnac 10.1.1.1  --local-dir /home/aradford/RUN_REMOTE/logs
```

Nach Abschluss dieses Vorgangs kann das Verzeichnis /home/aradford/RUN_REMOTE/logs Folgendes enthalten:

```
ls RUN_REMOTE/logs/10.1.1.1
DNAC_AURA_Logs_2020-09-08_23_20_11.tar.gz
DNAC_AURA_Report_2020-09-08_23_20_11.json
DNAC_AURA_Report_2020-09-08_23_20_11.pdf
```

die json-Datei enthält:

```
cat RUN_REMOTE/logs/*/DNAC_AURA_Report_2020-09-08_23_20_11.json
{
  "json-summary": {
    "check_count": 64,
    "report-name": "/data/tmp/dnac_aura/reports/DNAC_AURA_Report_2020-09-08_23_20_11.pdf",
    "logfile-name": "/data/tmp/dnac_aura/logs/DNAC_AURA_Logs_2020-09-08_23_20_11.tar.gz",
    "ur_check_count": 19,
    "ur_error_count": 0,
```

```
    "warning_count": 5,
    "assur_warning_count": 2,
    "error_count": 5,
    "ur_warning_count": 3,
    "assur_check_count": 14,
    "assur_error_count": 0
  }
}
```

Cluster-Ausführung

Wenn Sie die Option —all-cluster verwenden, kann das Skript alle Elemente des Clusters finden und AURA auf jedem einzelnen ausführen.
Dies ist derzeit eine serielle Ausführung. Es kann mit —local-dir verwendet werden, um den Bericht, die Logdatei und die json-summary von DNAC zurück zu kopieren.

Es kann entweder eine vIP-Adresse oder eine physische Adresse angegeben werden. Das Skript kann eine Verbindung herstellen und nach allen physischen IP-Adressen im gleichen Subnetz suchen wie die IP-Adressen, die für die Verbindung verwendet werden.

Weitere Optionen

Das Skript kann auch mit der Option --no-pull ausgeführt werden. Dies stoppt den Git-Abruf, um auf die neueste Version von AURA zu aktualisieren, geht aber davon aus, dass Sie Aura in das Ausgangsverzeichnis in DNA Center kopiert haben.

AURA mit CRON

Cron ist eine Herausforderung für AURA aufgrund des Fehlens von PTY. Außerdem muss das crontab des DNA-Zentrums bearbeitet werden.

run_remote ist wahrscheinlich eine bessere Möglichkeit, AURA auszuführen, da es das PTY-Problem löst und die lokale crontab von DNA Center nicht bearbeitet werden muss. Die Ausführung in Kombination mit --local-path bedeutet, dass sich alle DNA Center-Protokolle auf einem externen Server im selben Protokoll befinden.

Hier ein Beispiel für einen crontab-Eintrag für die stündliche Ausführung von AURA auf einem DNAC. Sie müssen den Python-Interpreter explizit zur Verfügung stellen, um die virtuelle Umgebung zu übernehmen, die Paramiko- und SCP-Bibliotheken enthält.

```
00 * * * * /home/aradford/RUN_REMOTE/env3/bin/python /home/aradford/RUN_REMOTE/run_remote.py --dnac 10.
```

Dies kann durch ein Shell-Skript weitergeführt werden, um zu verhindern, dass die Anmeldeinformationen im Klartext gespeichert werden.

AURA-Optionen in Cisco DNA Center

Tabelle 1 - Überprüfung/Funktionalität der verschiedenen AURA-Optionen

	Keine Optionen (Standard)	s	-d	-o	-c
Zustandsprüfungen der DNA Center-Infrastruktur	X	X	X		
Zustandsprüfungen von DNA Center Assurance	X	X			
Zustandsprüfungen von WLC/eWLC Assurance	X	X			
Grundlegende SDA-Prüfungen (Bestandsprüfung)DNAC-ISE-Integration (nur wenn ISE integriert ist)	X	X			
SDA(Fabric Device CLI-Erfassung, Audit und Kompatibilitätsprüfung der Kontrollebene und Sicherheitsebene)		X			
Prüfung der Upgrade-Bereitschaft (einschließlich Bugs)	X	X			
DNA-Center-Skalierung (Fabric- und Nicht-Fabric-Skalierungsparameter)	X	X	X		
Erfassen Sie CLI-Ausgänge von den Fabric-Geräten, und speichern Sie diese lokal im DNA-Center - Befehl und Geräteliste, bereitgestellt über die Datei captureFile.yaml2 erfasste Dateien:.json - Command Runner Standardausgabe.log - Für Menschen lesbar				X	
Vergleich von Konfigurationen auf mehreren Geräten (basierend auf erfassten Ergebnissen und Verwendung der Option -o)					X

Befehlszeilenausgabe der AURA-Optionen

```
usage: dnac_aura [-h] [-v] [-V] [--json-summary] [-s] [-u U] [-n N] [--syslog SYSLOG] [--admin-pass ADM
```

```
[--admin-user ADMIN_USER] [--maglev-pass MAGLEV_PASS] [-d] [--sdadevcheck] [-o] [-c] [--download-test]

Select options.


optional arguments:
-h, --help show this help message and exit
-v verbose logging
-V version information
--json-summary print json-summary
-s Run additional SDA checks. To execute these checks, the tool can login to other devices in the fabri
and collect show command outputs.
-u U Upload report and logs file to the SR. Please provide SR and password in the format sr_number:sr_pa
-n N Add customer name to the PDF report on the first page (the summary page)
--syslog SYSLOG destination syslog server
--admin-pass ADMIN_PASS maglev admin password (this is the UI password for admin user)
--admin-user ADMIN_USER maglev admin user (webUI user, default is admin)
--maglev-pass MAGLEV_PASS maglev password (for sudo)
-d Perform all DNA Center Infrastructure Health checks only
--sdadevcheck to skip the SDA Device limit
-o To collect CLI outputs from the network devices via the Cisco DNA Center.
Ensure you have the captureFile.yaml in the same folder as this tool.
-c Compare configurations across multiple devices.
You can choose 2 timestamps from previous captures taken with the -o option.
PDF Report can be generated with the diffs.
--download-test To perform a download test of 3 test images of different sizes
from the DNAC Cloud Repo in AWS.
```

Beispiele für die Ausführung von AURA mit verschiedenen Optionen

Beispiel 1: Um Stark Industries als Firmennamen auszuwählen, führen Sie standardmäßige AURA-Prüfungen durch und kopieren Sie die Datei mit dem Kennwort 123kjaksdhf in SR 611111111. Der Befehl lautet:

```
$ ./dnac_aura -n "Stark Industries" -u 611111111:123kjaksdhf
```

Beispiel 2: Um sowohl Cisco DNA Center- als auch SDA-Prüfungen für den Kunden Stark Industries durchzuführen, lautet der Befehl:

```
$ ./dnac_aura -s -n "Stark Industries"
```

Beispiel 3: Verwenden Sie die Option -o, um show-Befehlsausgaben auszuführen und sie in einer Datei im Cisco DNA Center zu speichern. Das Tool kann über den Befehlsrunder von Cisco DNA Center die Ergebnisse für Sie abrufen. Der Befehl lautet:

```
$ ./dnac_aura -o
```

Um die Geräte und die Befehle, die auf diesen Geräten ausgeführt werden sollen, anzugeben, muss sich captureFile.yaml im selben Verzeichnis befinden. Das Beispiel ist in github vorhanden.

Beispiel 4: Verwenden Sie die Option -c, um laufende Konfigurationen der Catalyst Switches und/oder des eWLC zu vergleichen. Stellen Sie sicher, dass Sie zuvor die Option -o verwendet haben, um die Ausgaben der Geräte zu erfassen. Der Befehl lautet:

```
$ ./dnac_aura -c
```

Beispiel 5: Um AURA-Prüfungen für einen Cluster auszuführen, wählen Sie für einen Knoten die entsprechende Option aus der Tabelle aus. Wählen Sie für die verbleibenden beiden Knoten die Option -d aus.

Auf einem beliebigen Knoten:

```
$ ./dnac_aura
```

Auf den verbleibenden 2 Knoten:

```
$ ./dnac_aura -d
```

Beispiel 6: Um AURA zu planen, verwenden Sie cron oder um AURA remote auszuführen, checken Sie diese Readme-Datei auf github.

https://github.com/CiscoDevNet/DNAC-AURA/tree/primary/run_remote

Beispiel 7: Um den Pfad zum Cloud-Repo auf AWS zu überprüfen, auf dem die DNA-Center-Images gespeichert sind, können Sie AURA mit dieser Option ausführen. Der Test lädt 3 Bilder herunter (klein - 50MB, mittel - 150MB und groß - 650MB) und kann die Zeit für das Herunterladen dieser drei Dateien berechnen. Durch die Überprüfung wird sichergestellt, dass die Testbilder gelöscht werden und keine Berichte generiert werden, wenn Sie diese Option auswählen.

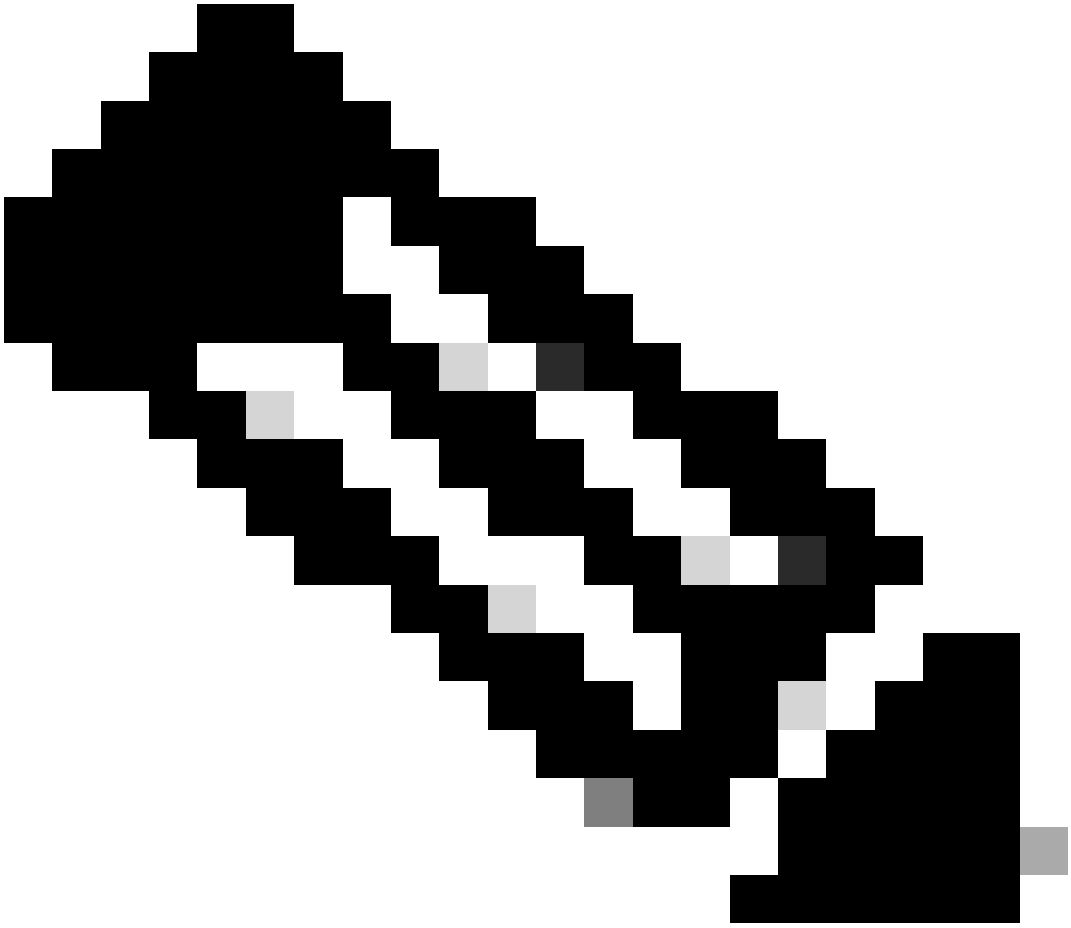
Auf einem beliebigen Knoten:

```
$./dnac_aura --download-test
```

Beispiel für die Prüfung:

```
$./dnac_aura --download-test


#####################################################
###                                               ###
###   Welcome to the Cisco DNA Center AURA Tool  ###
###              version:1.5.0                    ###
###                                               ###
#####################################################
###
### Please visit us at www.cisco.com - 'Enhanced Visibility into the Cisco DNA Center and use AURA'
###
###
### The image download test can be executed and all other checks can be skipped. ###
###

#01:Checking:Latest version of AURA
INFO:AURA is up to date
INFO:Performing login... [please provide UI admin level password]
[administration] username for 'https://kong-frontend.maglev-system.svc.cluster.local:443': admin
[administration] password for 'admin':

#02:Checking:Determine Cisco DNA Center Product Type, Serial number, SW Version & Node IP
[sudo] password for maglev:

...

#01:Checking:Download test image from the Cisco DNA Center Cloud Image Repository

INFO:This check can take up to 4 minutes to complete

INFO:Successfully downloaded a small test image of size 50MB from DNAC cloud repository in 3.4 seconds.

INFO:Successfully downloaded a medium test image of size 150MB from DNAC cloud repository in 3.2 second

INFO:Successfully downloaded a large test image of size 650MB from DNAC cloud repository in 16.2 second

$
```

Beispiel 7: Wenn AURA mit der Option -s ausgeführt wird, kann AURA die Prüfungen auf Kontroll- und Sicherheitsebene für maximal 50 Fabric-Geräte pro Fabric-Standort durchführen. Um diesen Grenzwert zu eliminieren, verwenden Sie die Option —sdadevcheck.



Hinweis: Die Laufzeit des Tools erhöht sich mit dem Hinzufügen weiterer Geräte.

```
$ ./dnac_aura  -s --sdadevcheck
```

Ausgaben des Tools

Wenn das Tool startet, werden Sie aufgefordert, den Benutzernamen/das Kennwort für den Administrator einzugeben, gefolgt vom maglev-Kennwort.

```
$ ./dnac_aura.py

#################################################
###                                           ###
### Welcome to the Cisco DNA Center AURA Tool    ###
###              version:1.4.6                  ###
```

```
###                                                 ###
#####################################################
###
### Please visit us at www.cisco.com - 'Enhanced Visibility into the Cisco DNA Center and use AURA'
###
###
### All Cisco DNA Center based Health,Scale,Upgrade Readiness,Assurance & SDA checks can be run ###
###
#01:Checking:Latest version of AURA
INFO:AURA is up to date

INFO:Performing maglev login...
[administration] username for 'https://kong-frontend.maglev-system.svc.cluster.local:443': admin
[administration] password for 'admin':
INFO:User 'admin' logged into 'kong-frontend.maglev-system.svc.cluster.local' successfully

#02:Checking:Determine Cisco DNA Center Product Type, Serial number, SW Version & Node IP
[sudo] password for maglev:

...



******
Cisco DNA Center AURA tool has successfully completed.
Report and Logs can be found at:
-- Cisco DNA Center AURA Report : /data/tmp/dnac_aura/reports/DNAC_AURA_Report_2021-02-25_05_27_45.pdf
-- Cisco DNA Center AURA Logs (tar.gz file) : /data/tmp/dnac_aura/logs/DNAC_AURA_Logs_2021-02-25_05_27_

$
```

Das Tool generiert zwei Dateien, die in /data/tmp/dnac_aura/ gespeichert werden:

- Einen PDF-Bericht unter /data/tmp/dnac_aura/reports. Die erste Seite enthält Daten zu DNA Center (Modell, Seriennummer, Softwareversion und IP-Adresse), die Ausführungszeit des Tools und eine Zusammenfassung aller durchgeführten Prüfungen und Ergebnisse. Auf den verbleibenden Seiten finden Sie weitere Details zu den verschiedenen Prüfungen mit Auszügen der Befehlsausgabe und den Ergebnissen. Fehler und Warnungen sind farblich gekennzeichnet und können einfach durchsucht werden. (Mit der Option -o wird kein Bericht erstellt.)
- Alle Protokolle von Cisco DNA Center und Show-Befehle der Geräte werden in eine tar.gz-Datei gepackt.

Cisco DNA Center AURA Results

Stark Industries

The Cisco DNA Center AURA (Audit & Upgrade Readiness) script performs a variety of health, scale & upgrade readiness checks across the DNA Center and the rest of the Fabric network without affecting any of the devices. This report is auto generated by the script and documents all the checks and logs performed by the script.
Thank you for running it, please reach out to dnac_sda_audit_tool@cisco.com for any feedback.

A total of 80 checks were executed on the setup, found 5 errors and 6 warnings. Please evaluate the Warnings & Errors, ensure the Errors are eliminated prior to proceeding with an upgrade.

Summary of the Results

DNA Center Device Details:

Model	Serial Number	Software Version	Node IP Address
DN2-HW-APL	ABCDE12345	1.3.3.5	10.1.1.1

Script Execution Time:

Start Time	End Time
2020-07-02_12:27:41	2020-07-02_12:33:28

DNA Center Infra Health Results:

Checks Executed	Errors Found	Warnings Found
35	4	2

DNA Center & Device Assurance Results:

Checks Executed	Errors Found	Warnings Found
6	0	1

DNA Center & Device Upgrade Readiness Results:

Checks Executed	Errors Found	Warnings Found
6	1	2

DNA Center SD-Access Health Results:

Checks Executed	Errors Found	Warnings Found
21	0	3

DNA Center Scale Limit Check Results:

Checks Executed	Errors Found	Warnings Found
18	1	0

AURA-Versionen – Änderungsprotokoll

https://github.com/CiscoDevNet/DNAC-AURA/blob/primary/ChangeLog.md

Von AURA durchgeführte Prüfungen

Cisco DNA Center - Integrität und Netzwerkanbindung

#01:Check:Neueste Version von AURA
#02:Prüfen:Cisco DNA Center-Produkttyp, Seriennummer, Softwareversion und Knoten-IP ermitteln
#03:Überprüfen:Bestimmen Sie die Cisco DNA Center-Mitgliedsnummer.
#04:Prüfen:CPU-Last durchschnittlich
#05:Überprüfen:Datenträgerlayout
#06:Überprüfen:Laufwerkpartitionsmounts
#07:Check:Festplattenspeicher und iNodes-Auslastung
#08:Überprüfen:ob Glusterfs montiert ist
#09:Überprüfen:auf nicht reagierende NFS-Mounts

#10:Überprüfen:auf veralteten NFS-Dateihandle
#11:Check:Festplatten-E/A-Durchsatz
#12:Prüfen:DRAM-Speicher gesamt
#13:Überprüfen:In der Appliance installierte DRAMs
#14:Prüfen:Prozessorkerne aktiviert und Status
#15:Überprüfen:Docker-Status
#16:Überprüfen:Docker-Proxy-Einstellungen
#17:Überprüfen:Shell-Umgebungsvariablen
#18:Überprüfen:Kubelet-Status

#19:Überprüfen:Syslog auf PLEG-Fehler
#20:Check:Version des Cisco DNA Center, aus der dieses System aufgebaut wurde
#21:Überprüfen:Aktualisierungsverlauf [dies ist ungefährer Wert, da keine vollständigen Daten vorliegen]

#22:Prüfen:Hook angewendet
#23:Prüfen:Cluster-Knoten-Erreichbarkeit - Knoten: [u'91.1.1.13', u'91.1.1.11', u'91.1.1.14']
#24:Check:Interface Reachability - all nodes : [u'99.99.99.13', u'92.1.1.1', u'91.1.1.13', u'99.99.99.11', u'92.1.1.2', u'91.1.1 1,11', u'99,99,99,14', u'92,1,1,3', u'91,1,1,14']
#25:Check:VIP Reachability - VIPs : [u'92.1.1.2', u'99.99.99.12', u'91.1.1.12']
#26:Check:Anzahl der konfigurierten DNS-Server in usw. auf Knoten (<=3)
#27:Check:Anzahl der /etc/resolv.conf-Einträge (<=4)
#28:Überprüfen:DNS-Konfiguration - /etc/network/interfaces
#29:Check:DNS Reachability - DNS : [u'8.8.8.8']
#30:DNS-Server löst Cisco Connect DNA
#31:Überprüfen:NTP-Server-Synchronisierung: ['5.6.7.8', '1.2.3.4']
#32:Überprüfen:Cluster-Hostname ist definiert
#33:Check:Standardzeitzoneneinstellung für DNAC
#34:Überprüfen:Schnittstellen auf Fehler
#35:Check:DCBX-Upstream verursacht TX-Verluste
#36:Überprüfen:VIP-Umschaltung zwischen Knoten

#37:Überprüfen:Kernelprotokolle auf Fehler überprüfen
#38:Überprüfen:Gültigkeit und Ablauf von Zertifikaten
#39:Überprüfen:Ablauf von Zertifikaten für Truststore
#40:Überprüfung:NTP-Servicestatus im Cisco DNA Center
#41:Überprüfen:NTP-Serverzeitsynchronisierung

#42:Überprüfen:auf Routen auf Intra-Cluster-Schnittstellenebene nach gepufferter MTU
#43:Überprüfen:Status der PMTU-Erkennung
#44:Überprüfen:Knotenanzeige
#45:Überprüfen:Knotenstatus
#46:Überprüfen:Knotendiagnosebericht

#47:Prüfen:Servicebereitstellung ...
#48:Überprüfen:Appstack-Status
#49:Überprüfen:Endgerätestatus
#50:Überprüfen Sie Ihre Services auf hohe Neustartzahlen.
#51:Überprüfen:remedyctl wird ausgeführt
#52:Überprüfung:Status der ISE in DB
#53:Check:Externe Authentifizierung für DNAC-Benutzer konfiguriert

#54:Check:Konfiguration des externen Authentifizierungs-Fallbacks
#55:Check:Anzahl der skalierbaren Gruppen, Verträge und Zugriffsrichtlinien in DNAC DB überprüfen

#56:Überprüfen:GBAC-Migrations-/Synchronisierungsstatus

#57:Überprüfen:Glusterfs-Instanzen
#58:Überprüfen:Glusterfs NODE_NAME-Prüfung
#59:Überprüfen:Glusterfs Clustering

#60:Überprüfen:Gluster Volumen Heilung Statistik
#61:Überprüfen:ETCD-Cluster-Zustand
#62:Überprüfen:ETCD-Speichergröße
#63:Überprüfen:ETCD-Speichernutzung
#64:Check:ETCD-Bindung an Loopback(localhost/127.0.0.1
#65:Überprüfen:Status des Postgres-Clusters
#66:Überprüfen:Größe von Postgres
#67:Überprüfen:MongoDB Cluster-Integrität und Synchronisierungsstatus
#68:Prüfen:MongoDB CPU in Dockerstatistiken
#69:Prüfen:MongoDB Größen
#70:Überprüfen:TenantSegment-Überlauf
#71:Prüfen:InfluxDB Health
#72:Check:InfluxDB Speichernutzung
#73:Überprüfen:Cassandra Gesundheit
#74:Überprüfen:Status der Cassandra
#75:Überprüfen:Rabbitmq Cluster-Integrität
#76:Überprüfen:RabbitMQ-Cluster-Status

#77:Überprüfen:RabbitMQ-Warteschlangenstatus
#78:Überprüfen:Rabbitmq-Warteschlangen mit nicht bestätigten Nachrichten
#79:Überprüfen:Zookeeper Cluster-Integrität
#80:Überprüfen:Zookeeper-Cluster-Status

#81:Überprüfen:Zookeeper Cluster Epoch-Validierung
#82:Überprüfen:ElasticSearch-Cluster-Status: Maglev-System
#83:Check:ElasticSearch-Cluster-Status: NDP
#84:Sidecars lauschen
#85:Check:REST API (BAPI) antwortet
#86:Überprüfen:Sicherungsverlauf
#87:Check:Bekanntes Problem, das dazu führt, dass LAN Auto nicht gestartet wird

#88:Check:Kritische Schwachstellen in Apache Log4j - CVE-2021-44228 & CVE-2021-45046

Upgrade-Bereitschaft

#01:Überprüfen:Cluster-Subnetz-Überlappung mit internen Adressen
#02:Überprüfen:RCA-Dateien Datenträgerverwendung
#03:Check:Anzahl der abgelaufenen Container
#04:Überprüfen:Anzahl nicht ausgeführter Pods
#05:Überprüfen:Maglev-Katalogeinstellungen
#06:Prüfen:Details zum Katalog-Release Channel - KEINE VALIDIERUNG - NUR INFORMATIONEN ZUR ÜBERPRÜFUNG
#07:Überprüfen:Katalog-Systemaktualisierungspakete - KEINE VALIDIERUNG - NUR INFORMATIONEN ZUR ÜBERPRÜFUNG
#08:Überprüfen:Katalogpakete - KEINE VALIDIERUNG - NUR INFORMATIONEN ZUR ÜBERPRÜFUNG
#09:Überprüfen:Einstellungen für übergeordnetes Repository
#10:Überprüfen:Proxy-Verbindung mit CiscoConnectdna über:http://a.b.c.d:80
#11:Überprüfen:Dateidienst auf fehlende Datei-ID-Zuordnungen überprüfen
#12:Überprüfen:Ablauf von Maglev-Zertifikaten
#13:Überprüfen:Ablauf des Zertifizierungsstellenzertifikats der Registrierung

#14:Check:Ablauf des Zertifizierungsstellenzertifikats

#15:Check:etc. Zertifikate

#16:Auf veraltete Mount-Punkte prüfen
#17:Check:Check für Kubernetes Transient Mounts
#18:Überprüfen:Die Collector-ISE-Konfiguration wurde nach einem vorherigen Upgrade bereinigt
#19:Überprüfen:Ausstehende Workflows
#20:Überprüfen:Backup-Anzeige für letzte erfolgreiche Sicherung
#21:Check:Bereitstellung aufgrund ungültiger Migrationsstatusparameter fehlgeschlagen
#22:Überprüfung:Status des Maglev Hook Installer-Service im Cisco DNA Center

#23:Check:Testbild aus dem Cisco DNA Center Cloud Image Repository herunterladen
#24:Überprüfen:SSL Intercept im Netzwerk konfiguriert

#25:Überprüfen:Proxy-Passwortcodierung
#26:Überprüfung:Anzahl der mehrere Standorte für SDA-Bereitstellung
#27:Überprüfen:Upgrade-Pfad für DNA Center auf den neuesten Patch von 2.3.3.x
#28:Überprüfen:Catalyst-Geräte im Paketmodus

#29:Überprüfen:Aktuelle Updates und RCA-Dateien
#30:Check:Status der sekundären Schnittstelle (nur XL)
#31:Check:kubectl-Standardnamespace

#32:Überprüfen:Tiller-Fehler aufgrund aktualisierter Zertifikate

#33:Überprüfen:Für ausreichend Speicherplatz auf der Datenträgerpartition /boot/efi
#34:Überprüfung:Kompatibilität von Fabric-Geräten mit DNA Center Version 2.3.3.x
#35:Überprüfung:IP-Pool-Migration
#36:Check:Konfigurierte AAA-Server und deren Status

Cisco DNA Center Assurance

#01:Überprüfen:Sicherstellen der Partitionsspeicherplatznutzung
#02:Überprüfen:Status von Assurance Services
#03:Überprüfen:Sicherungskopie des Löschauftrags prüfen
#04:Überprüfen:Sicherung prüfen NDP-Löschauftrag, der Redis DB bereinigt
#05:Check:Redis Nicht genügend Arbeitsspeicher
#06:Überprüfen:Status der Assurance-Pipeline
#07:Überprüfen:Bewertung des Gerätestatus
#08:Überprüfen:Zusammenfassung der Client-Integritätsbewertung
#09:Überprüfen:WLC korrekte Telemetrie-API-Aufruf
#10:Überprüfen:Cisco IOS® XE WLC Telemetrie-Verbindungsstatus prüfen
#11:Überprüfen:Cisco IOS XE WLC NetConf Yang-Datenspeicherprüfung
#12:Überprüfen:Cisco IOS XE WLC sdn-network-infra-iwan Vertrauenspunkt und Zertifikate
#13:Überprüfen:Cisco IOS XE WLC DNAC-CA-Vertrauenspunkt und -Zertifikat
#14:Überprüfen:Cisco IOS XE WLC Device Network Assurance-Status
#15:Prüfen:AIREOS WLC Telemetrie-Verbindungsstatus prüfen
#16:Überprüfen:AIREOS WLC Telemetrie-Zertifikatsprüfung

SD-Access-Zustand

#01:Überprüfen:Bestandsstatus der Erreichbarkeit von Fabric-Geräten
#02:Überprüfen:Fabric-Bestandserfassung
#03:Check:SDA:Cisco DNA Center und ISE - Integrationsstatus
#04:Überprüfung:SSH-Verbindung zwischen Cisco DNA Center und Cisco ISE
#05:Überprüfung:Speicherauslastung der Cisco ISE-Knoten
#06:Überprüfung:Nutzung von Festplatten durch Cisco ISE-Knoten
#07:Überprüfen:Status der Cisco ISE-Prozesse

#08:Prüfen:SGTs und SGACLs über API am primären ISE-Knoten ermitteln

#09:Check:SDA:Befehle von Rändern/KPs/Kanten erfassen
#10:Check:SDA:Anzahl der Softwareversionen und Plattformtypen
#11:Check:SDA:Prüfung der CPU-Auslastung von Fabric-Geräten
#12:Check:SDA:Fabric-Geräte Speicherauslastungsprüfung
#13:Check:SDA:Überprüfen der Anzahl von LISP-Sitzungen auf den Fabric-Geräten
#14:Check:SDA:Größe der LISP IPv4 EID-Tabelle auf allen Fabric-Geräten überprüfen
#15:Check:SDA:Größe der LISP IPv4 MAP-Cache-Tabelle an den Grenzen überprüfen
#16:Check:SDA:Überprüfung des ISIS-Sitzungsstatus für die Fabric-Geräte
#17:Check:SDA: Vergewissern Sie sich, dass die Fabric-Geräte über mehr als eine ISIS-Sitzung verfügen - Redundanzprüfung
#18:Check:SDA:Borders Only:IPv4 BGP-Sitzungen
#19:Check:SDA:Borders Only:VPNv4 BGP-Sitzungen
#20:Check:SDA:AAA Serververbindung von Geräten
#21:Check:SDA:CTS PACS auf die Geräte heruntergeladen
#22:Check:SDA:CTS SGTs auf die Geräte heruntergeladen

#23:Check:SDA:eWLC CPU Utilization Check
#24:Check:SDA:eWLC-Speicherauslastungsprüfung
#25:Check:eWLC Fabric AP-Prüfung
#26:Check:eWLC Fabric WLAN-Check

Cisco DNA Center-Skalierung

#01:Check:Skalierung: Anzahl der Standorte
#02:Check:Scale: Anzahl der Zugriffskontrollrichtlinien
#03:Check:Skalierung: Anzahl der Zugriffsverträge
#04:Prüfen:Skalierung : Gesamtzahl der Geräte (Switch, Router, Wireless Controller)
#05:Check:Skalierung: Anzahl der Fabric-Domänen
#06:Check:Skalierung: Anzahl der Fabric-Standorte
#07:Check:Scale: Anzahl der Gruppen-SGTs
#08:Check:Scale: Anzahl der IP-SuperPools
#09:Prüfen:Skalierung : Anzahl der ISE-Verbindungen
#10:Check:Scale: Max. Anzahl von AAA (Radius)
#11:Check:Scale: Anzahl der SSIDs
#12:Check:Scale: Anzahl der virtuellen Netzwerke pro Standort
#13:Prüfen:Skalierung: Anzahl der Wireless Access Points
#14:Prüfen:Skalierung: Anzahl der Wireless LAN-Controller
#15:Prüfen:Skalierung: Anzahl der Wireless-Sensoren

#16:Check:Scale: Anzahl der Fabric-Geräte pro Standort
#17:Check:Skalierung: Anzahl der Fabric-Grenzen pro Standort
#18:Check:Scale: Anzahl der Fabric Control Plane-Knoten pro Standort

Hashwerte für die Datei dnac_aura

AURA-Version	MD5-Hash	SHA256-Hash

1.5.9	52f429dd275e357fe3282600d38ba133	c91b6092ab4fa57adbe698a3c17f9146523bba5b0315222
1.6.0	e01328f5e0e4e5f5c977c5a14f4a1e14	4f8115d1f2f480efcdb0260cc5a9abb8a067f3cbac2c293a2
1.6.8	f291e3e694fadb2af722726337f31af5	fb7c125910d77c8087add419b937a893174fb30649427ad

---

Fehlerbehebung

Wenden Sie sich bei Problemen mit dem PDF-Bericht und den TAR-Protokolldateien an dnac_sda_audit_tool@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.