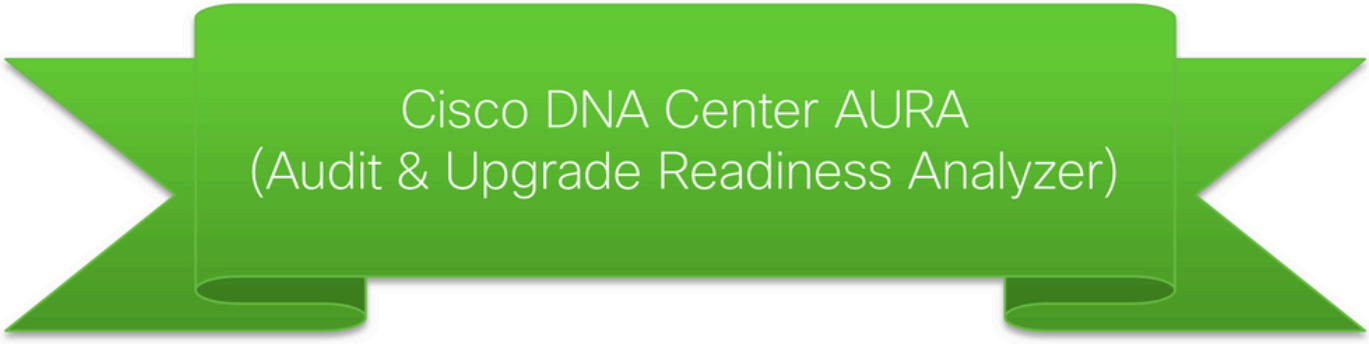
Utilizzo di AURA per una migliore visibilità nel DNA Center

Sommario



Introduzione

Questo documento descrive lo strumento da riga di comando Cisco DNA Center Audit and Upgrade Readiness Analyzer (AURA).

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Per redigere questo documento, è stata usata la piattaforma Cisco DNA Center.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

AURA esegue una serie di controlli di stato, scalabilità e idoneità all'upgrade per Cisco DNA Center e il resto della rete Fabric. Lo strumento è molto semplice da usare e viene eseguito su Cisco DNA Center. Lo strumento utilizza chiamate API (Application Programming Interface), letture DB e comandi show (operazioni di sola lettura) e pertanto non influisce sulle prestazioni né causa impatto su Cisco DNA Center o sui dispositivi di rete.

Perché AURA è così semplice da usare

- Utilizza SOLO le librerie e il software preinstallati correnti.
- Genera automaticamente il report in formato PDF.
- Richiede solo l'immissione delle password di Cisco DNA Center (admin e maglev).
- I log e i report compressi possono essere caricati automaticamente su Cisco SR (facoltativo).

- È sufficiente copiare il file su Cisco DNA Center ed eseguire il file su Cisco DNA Center.
- Non intrusivo - solo lettura di database (DB), comandi show e chiamate API.
- Tempo di esecuzione: meno di 15 minuti per i controlli di Cisco DNA Center e il tempo necessario per i controlli SDA (Software Defined Access) varia in base alla scala della rete (circa 30 minuti per 30 dispositivi).
- Funziona sulle release 1.2.8, 1.2.10.x, 1.2.12.x, 1.3.x e 2.x.

Per eventuali problemi o commenti, contattare dnac_sda_audit_tool@cisco.com.

Aree di controllo/funzionalità dello strumento AURA

- Cisco DNA Center Scale Test
- Cisco DNA Center Infra Health
- Cisco DNA Center Assurance Health
- Integrità di WLC/eWLC Assurance
- Acquisizione del dispositivo SDA dalla CLI
- Verifica del piano di controllo e del piano di sicurezza di SDA
- Bug software che causano errori di aggiornamento
- Controlli preliminari all'aggiornamento
- Verifica compatibilità SDA (Switch, Wireless Controller e Identity Services Engine (ISE)) per 2.3.3.x
- Controlli sull'integrazione Digital Network Architecture Center (DNAC)-ISE
- Configurazioni dei dispositivi fabric Acquisizione e confronto e utilizzo dello strumento diff incorporato
- Avvio di AURA da remoto (dalla release 1.2.0)
- Pianificazione di AURA con cron (dalla versione 1.2.0)
- Integrazione del server syslog (dalla release 1.2.0)
- Download delle immagini dei test dal cloud (dalla release 1.5.0)

Come eseguire lo strumento (passaggi semplici)

Passaggio 1. Copiare il file AURA eseguibile su Cisco DNA Center. Per la versione più recente, visitare il sito Web https://github.com/CiscoDevNet/DNAC-AURA.

Passaggio 2. Eseguire lo strumento da Cisco DNA Center (se si dispone di un cluster, vedere l'esempio 5 nella sezione Cisco DNA Center AURA Options).

```
$ ./dnac_aura
```

Come eseguire lo strumento (procedure dettagliate)

Se la versione di Cisco DNA Center è 2.3.3.x e successive, Cisco DNA Center dispone di una shell con restrizioni abilitata per una maggiore sicurezza a partire dalla versione 2.3.3.x. La shell predefinita è denominata magshell e non supporta alcun comando Linux o l'esecuzione di AURA.

Disabilitare la shell con restrizioni e abilitare la shell Bash prima di procedere al passaggio successivo. Disabilitazione della shell con restrizioni su 2.3.3.x. Nelle versioni 2.3.4.x e successive, è possibile richiedere un token di consenso da parte di Cisco Technical Assistance Center (TAC) per disabilitare la shell con restrizioni.

Passaggio 1. Copiare il file eseguibile su Cisco DNA Center.

```
dnac_aura
```

Per la versione più recente, vedere https://github.com/CiscoDevNet/DNAC-AURA. Per copiare il file su Cisco DNA Center, sono disponibili diversi metodi.

Opzione di copia file 1. Fare clic sull'URL e scaricare il file dal browser:

Copiare il file su Cisco DNA Center e utilizzare un software di trasferimento file (non dimenticare di utilizzare il protocollo SFTP (Secure File Transfer Protocol) con porta 2222 e nome utente maglev).

Opzione di copia dei file 2. Copiare il file direttamente nel Cisco DNA Center e utilizzare i comandi GIT:

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

Opzione di copia dei file 3. Se è stato configurato un server proxy, copiare il file in Cisco DNA Center e utilizzare i comandi GIT e i dettagli del server proxy:

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

Passaggio 2. Assicurarsi che il file dnac_aura sia eseguibile.

Quando il file dnac_aura viene copiato nel Cisco DNA Center, generalmente non viene copiato come eseguibile. Eseguire il comando per renderlo eseguibile. Se è stato utilizzato GIT, questo passaggio non è necessario.

```
$ chmod 755 dnac_aura
```

Passaggio 3. (Facoltativo) Convalidare l'hash del file dnac_aura per accertarsi che sia stato scaricato il file corretto.

Per accertarsi che vengano scaricati i file corretti, confrontare i valori dell'hash MD5 o dell'hash SHA256 che sono disponibili alla fine di questo documento. Ogni versione di AURA può avere un insieme univoco di valori hash.

Opzione 1. Verifica hash MD5.

Usare il comando md5sum (come elencato). Genera l'hash sul tuo Cisco DNA Center o su qualsiasi altro sistema Linux e confronta il valore dell'hash con il valore alla fine di questa pagina.

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

Opzione 2. Verifica hash SHA256.

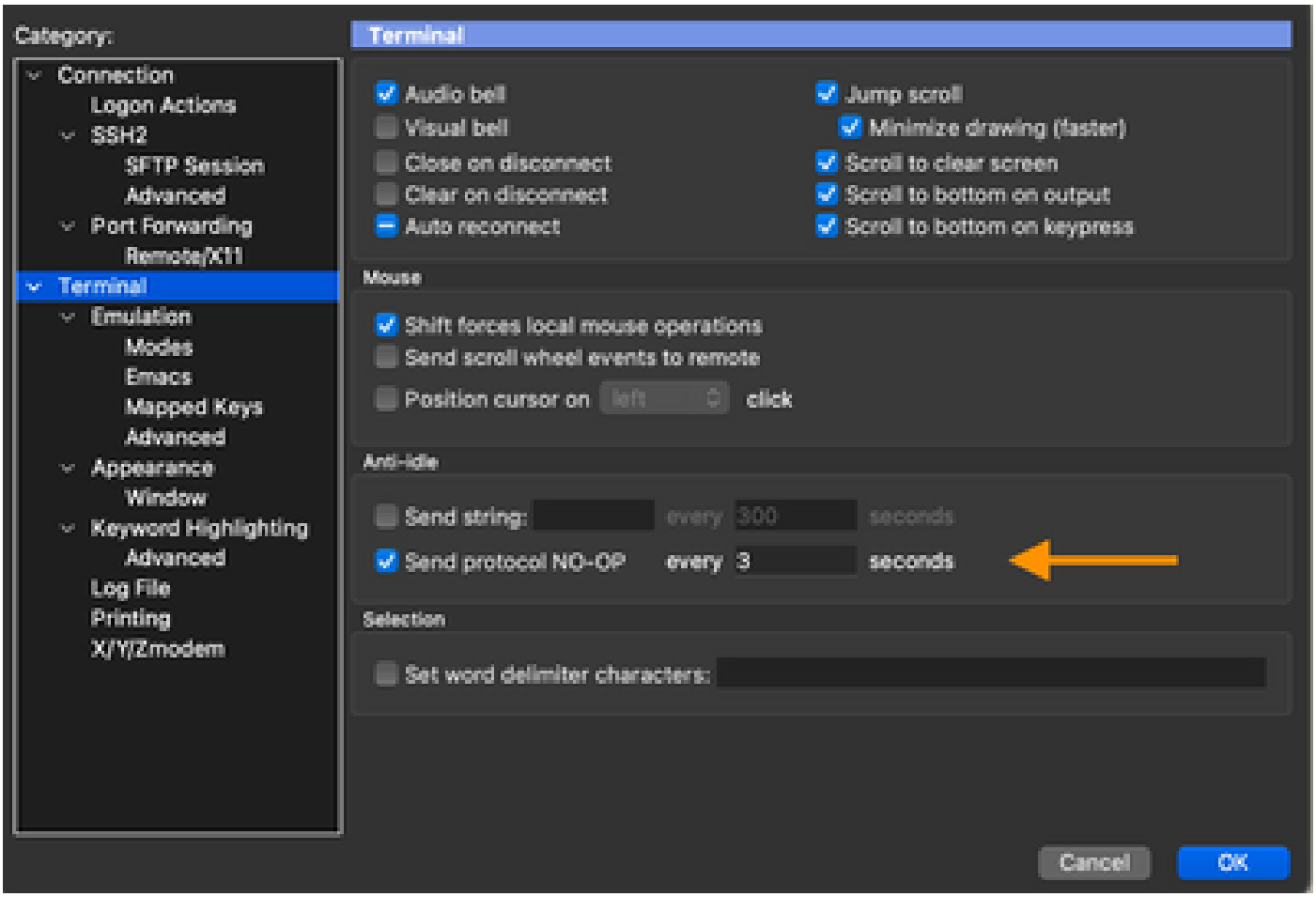
Utilizzare il comando sha256sum (come elencato). Genera l'hash sul tuo Cisco DNA Center o su qualsiasi altro sistema Linux e confronta il valore dell'hash con il valore alla fine di questa pagina.

```
$ sha256sum dnac_aura
c91b6092ab4fa57adbe698a3c17f9146523bba5b0315222475aa4935662a0b6e dnac_aura
```

Passaggio 4. Impostare un timeout di inattività per la sessione SSH.

Le versioni successive (2.x+, 1.3.3.8+) di Cisco DNA Center hanno un timeout di inattività SSH. Ciò può influire sull'esecuzione di AURA in una sessione SSH. Assicurarsi che il timeout di inattività sia impostato, altrimenti lo strumento AURA può essere interrotto in modo improvviso.

Esempio di impostazione di un timeout di inattività a 3 secondi su SecureCRT:



Passaggio 5. Eseguire lo strumento dalla riga di comando.

Selezionare l'opzione appropriata in base alla posizione del file per eseguire i controlli su Cisco DNA Center. Quando utilizzate le opzioni, potete includere o escludere vari controlli.

```
$ ./dnac_aura
```

o

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

Esecuzione di AURA da remoto

Questo script consente di avviare l'AURA su un Cisco DNA Center remoto. usando le librerie paramiko e scp.

Procedura di installazione

Per l'installazione, si consiglia di usare un ambiente virtuale. Queste linee possono creare un ambiente virtuale Python3, attivarlo, aggiornare PIP e installare le librerie necessarie.

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

Timeout sessione

Sulle versioni successive (2.1+, 1.3.3.8+) di Cisco DNA Center è previsto un timeout di inattività ssh. Questo può influire sull'esecuzione di AURA da una sessione ssh direttamente su DNAC o indirettamente tramite lo script run_remote o Ansible.

La soluzione è semplice. Per una connessione ssh, il flag -o ServerAliveInterval=3 può inviare pacchetti keepalive e mantenere la sessione. Il flag è usato in questo script e può essere utilizzato anche per la connessione ssh diretta e Ansible.

Utilizzare lo script

Lo script richiede tre argomenti:

- dnac
- password amministratore (disponibile anche come variabile di ambiente DNAC_ADMIN_PASS)
- password maglev (disponibile anche come variabile di ambiente DNAC_MAGLEV_PASS)
- utente amministratore (disponibile anche come variabile di ambiente DNAC_ADMIN_USER). L'impostazione predefinita è "admin" e deve essere modificata solo se si utilizza l'autenticazione esterna e un nome utente privilegiato diverso. In molti casi, questo argomento non è obbligatorio, ma è disponibile come --admin-user.

Il modo più semplice per eseguire lo script con argomenti (vedere la sezione successiva sulle variabili di ambiente) è:

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

Se si conoscono le variabili di ambiente della shell, è possibile semplificare ulteriormente:

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

Passa opzioni AURA (—)

Per passare argomenti specifici AURA (ad esempio -s per eseguire test SDA) è necessario eseguire questa operazione:

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

Verificare di includere le opzioni run_remote, ad esempio --local-dir, all-cluster e --no-pull, PRIMA dei trattini "--".

Le opzioni specifiche di AURA come -n, --syslog, -d, -s, devono trovarsi dopo i trattini "--".

Archivia output AURA localmente

Lo script AURA supporta l'opzione --json-summary per generare un riepilogo json dei risultati del test, della posizione del report e del file di log su DNAC. Quando run_remote viene fornito con l'opzione —local-dir, i file di log e di report possono essere spostati nuovamente in DNAC. È possibile creare un file json-summary. Viene creata una directory per il DNAC.

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

Al termine, la directory /home/aradford/RUN_REMOTE/logs può contenere:

```
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
```

Il file json contiene:

```
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
  }
}
```

Esecuzione dei cluster

Se si utilizza l'opzione —all-cluster, lo script può trovare tutti i membri del cluster ed eseguire AURA su ciascuno di essi.
Attualmente si tratta di un'esecuzione seriale. Può essere utilizzato con —local-dir per copiare il report, il file di log e il json-summary da DNAC.

Specificare un indirizzo VIP o fisico. Lo script può connettersi e cercare tutti gli indirizzi IP fisici nella stessa subnet dell'indirizzo IP utilizzato per la connessione.

Altre opzioni

Lo script può essere eseguito anche con l'opzione --no-pull. Ciò interrompe il comando git pull per aggiornare la versione più recente di AURA, ma ne presume una copia già effettuata sulla directory home di DNA Center.

AURA con CRON

Il funzionamento di AURA con Cron può comportare dei problemi a causa della mancanza di Phyton. Richiede inoltre la modifica del crontab di DNA Center.

run_remote è probabilmente il modo migliore per eseguire AURA, in quanto risolve il problema della mancanza di Phyton ed elimina la necessità di modificare il crontab di DNA Center locale. L'esecuzione da remoto in combinazione con --local-path permette di avere tutti log di DNA Center uguali su un server esterno.

Ecco una voce crontab di esempio per eseguire AURA su un DNAC con frequenza oraria. È necessario fornire l'interprete python in modo esplicito per selezionare l'ambiente virtuale che contiene le librerie paramiko e scp.

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

Ciò può essere ulteriormente integrato con uno script della shell per impedire che le credenziali vengano archiviate in testo normale.

Opzioni AURA di Cisco DNA Center

Tabella 1 - Controlli/funzionalità delle varie opzioni AURA

	Nessuna opzione (impostazione predefinita)	-s	-d	-o	-c
Controlli di integrità dell'infrastruttura di DNA Center	X	X	X		
Controlli di integrità di DNA Center Assurance	X	X			
Controlli di integrità di WLC/eWLC Assurance	X	X			
Controlli SDA di base (controllo dell'inventario)Integrazione DNAC-ISE (solo se ISE è integrato)	X	X			
SDA (Fabric Device CLI collection, Control Plane & Security Plane Audit and Compatibility Check)		X			
Controlli preparazione aggiornamento (include i bug)	X	X			
Scalabilità di DNA Center (parametri di scalabilità nel fabric e fuori dal fabric)	X	X	X		
Acquisire gli output CLI dai dispositivi fabric e archiviarli localmente in DNA Center - elenco di comandi e dispositivi forniti tramite file captureFile.yaml2 file catturati:.json - output predefinito del programma di esecuzione dei comandi.log - leggibile dall'utente				X	
Confronto delle configurazioni tra più dispositivi (in base agli output acquisiti e all'opzione -o)					X

Output delle opzioni AURA sulla riga di comando

```
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_p
-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.
```

Esempi di comandi AURA con varie opzioni

Esempio 1: per selezionare Stark Industries come nome della società, eseguire i controlli AURA predefiniti e copiare il file nella SR 61111111 con password 123kjaksdhf, il comando è:

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

Esempio 2: per eseguire i controlli di Cisco DNA Center e SDA per il cliente Stark Industries, il comando è:

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

Esempio 3: per eseguire i risultati del comando show e memorizzarli in un file sul Cisco DNA Center, usare l'opzione -o. Lo strumento può utilizzare il router dei comandi di Cisco DNA Center per recuperare automaticamente gli output. Il comando è:

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

Per specificare i dispositivi e i relativi comandi, captureFile.yaml deve essere presente nella stessa directory. L'esempio è presente in github.

Esempio 4: per confrontare le configurazioni in esecuzione degli switch Catalyst e/o del WLC, usare l'opzione -c. Accertarsi di aver utilizzato in precedenza l'opzione -o per acquisire gli output dai dispositivi. Il comando è:

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

Esempio 5: per eseguire i controlli AURA su un cluster, per ogni nodo, scegliere l'opzione appropriata dalla tabella. Per i restanti due nodi, scegliere l'opzione -d.

Su un nodo qualsiasi:

```
$ ./dnac_aura
```

Sui restanti 2 nodi:

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

Esempio 6: per pianificare AURA, utilizzare cron o per eseguire AURA in remoto, estrarre il file Leggimi su github.

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

Esempio 7: per verificare il percorso del repository Cloud su AWS in cui sono archiviate le immagini del DNA Center, è possibile eseguire AURA con questa opzione. Il controllo scarica 3 immagini (piccole - 50 MB, medie - 150 MB e grandi - 650 MB) e può calcolare il tempo per scaricare questi tre file. Se si seleziona questa opzione, le immagini di prova verranno eliminate e non verrà generato alcun report.

Su qualsiasi nodo:

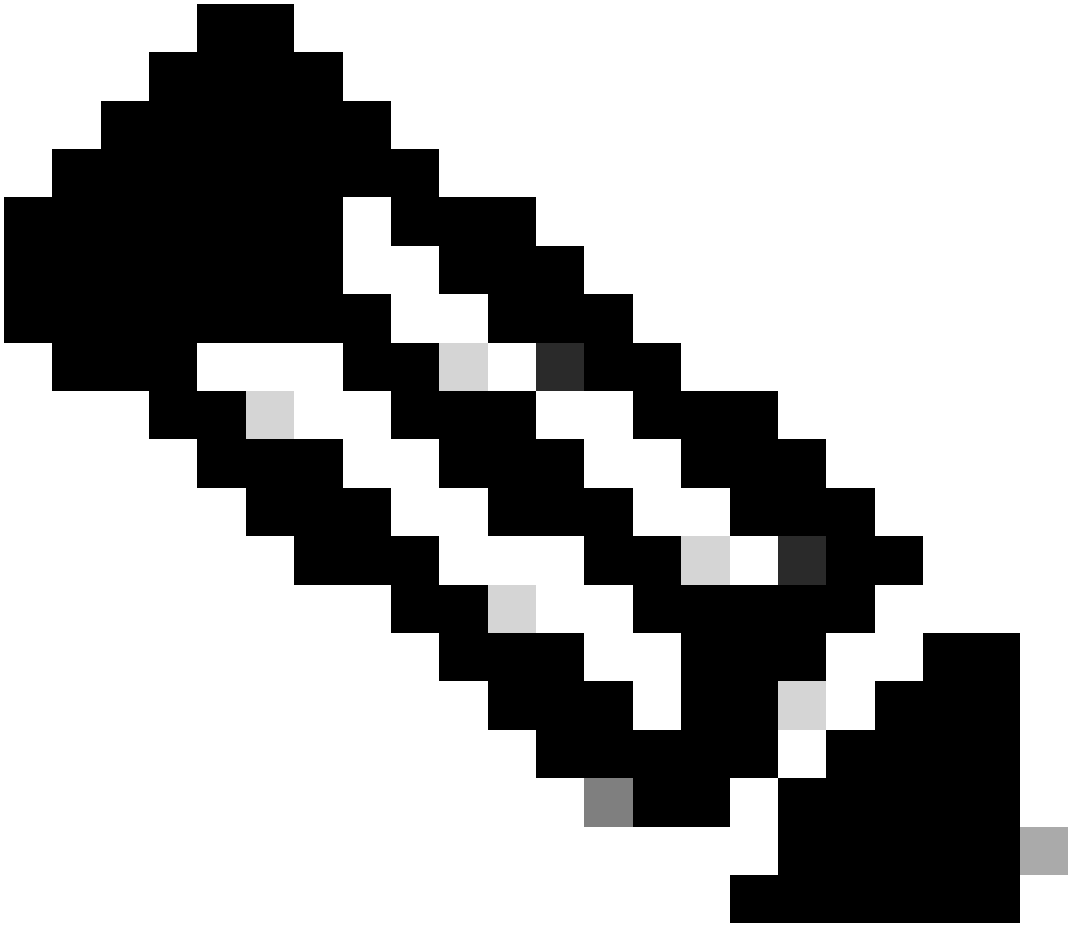
```
$./dnac_aura --download-test
```

Esempio del controllo:

```
$./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

$
```

Esempio 7: quando si utilizza AURA con l'opzione -s, AURA può eseguire gli audit del control plane e della sicurezza per un massimo di 50 dispositivi fabric per sito di fabric. Per eliminare questo limite, utilizzare l'opzione —sdadevcheck.



Nota: il tempo di esecuzione dello strumento aumenta con l'aggiunta di altre periferiche.

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

Output dello strumento

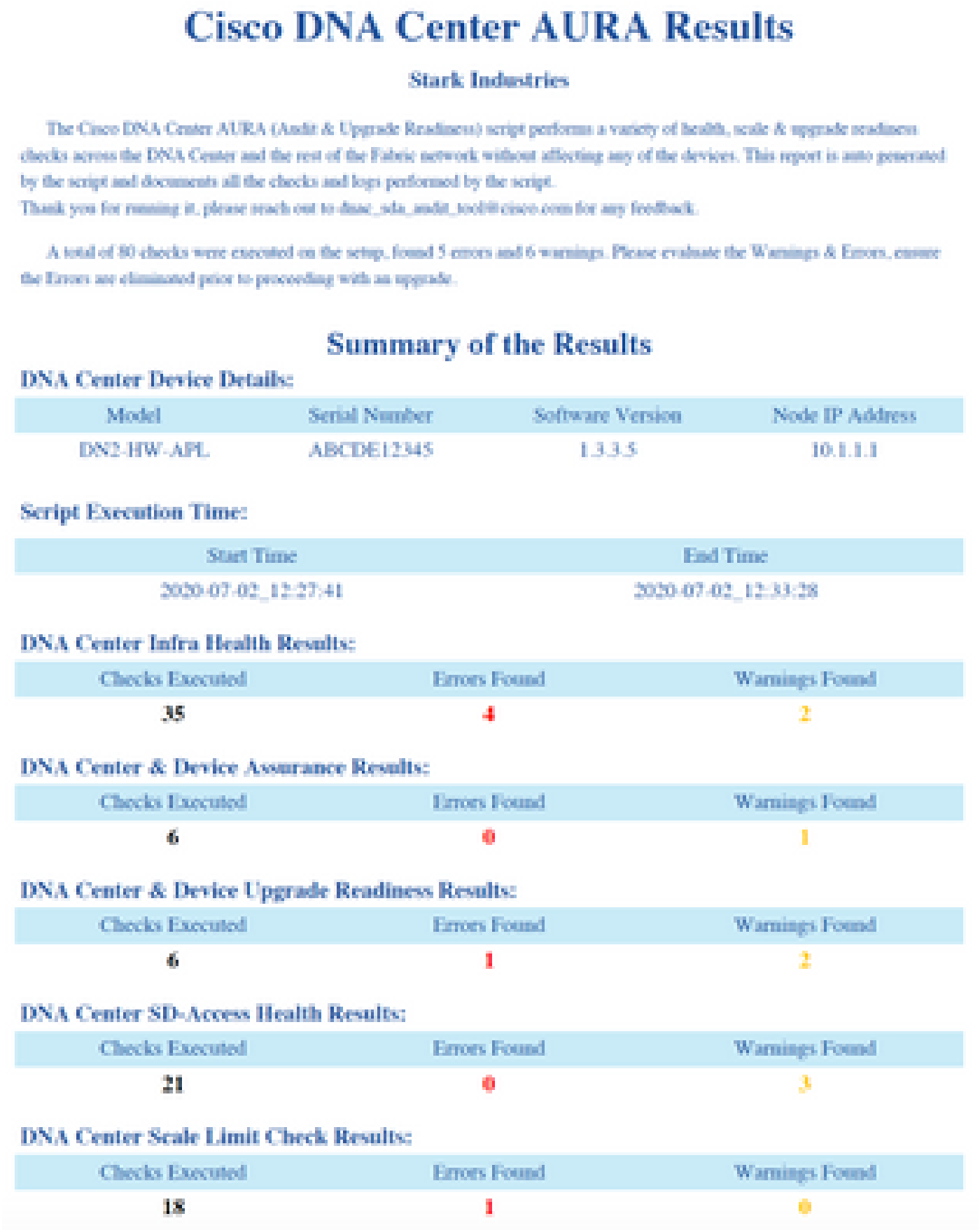
All'avvio dello strumento, viene richiesto di immettere il nome utente/la password dell'amministratore seguito dalla password maglev.

```
$ ./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_

$
```

Lo strumento genera 2 file che sono memorizzati in /data/tmp/dnac_aura/:

- Un report in formato pdf in /data/tmp/dnac_aura/reports. La prima pagina fornisce i dati su DNA Center (modello, numero di serie, versione software e indirizzo IP), il tempo di esecuzione dello strumento e un riepilogo di tutti i controlli eseguiti e i risultati. Le pagine rimanenti forniscono ulteriori dettagli sui vari controlli, con frammenti di codice dell'output del comando e i risultati. Errori e avvertenze sono codificati a colori e sono facilmente ricercabili. Non viene generato un report con l'opzione -o.
- Tutti i log di Cisco DNA Center e i comandi show dei dispositivi vengono compressi in un file tar.gz.



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

Versioni AURA - Log delle modifiche

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

Controlli eseguiti da AURA

Integrità e connettività di Cisco DNA Center

#01:Controllo:Versione più recente di AURA
#02:Controllo:Determinazione del tipo di prodotto, del numero di serie, della versione del software e dell'IP del nodo Cisco DNA Center
#03:Verifica:determinazione dell'ID membro di Cisco DNA Center
#04:Verifica:Carico medio CPU
#05:Controllo:Layout disco
#06:Controllo:Montaggi Partizione Disco
#07:Verifica:utilizzo dello spazio su disco e dei nodi
#08:Verificare:se Glusterfs è montato
#09:Controllo:per montaggi NFS non reattivi

#10:Controllo:per NFS handle di file non aggiornati
#11:Controllo:Throughput di I/O su disco
#12:Controllo:Memoria totale disponibile nella memoria DRAM
#13:Controllo:DRAM installate nell'accessorio
#14:Controllo:core del processore abilitati e stato
#15:Controllo:Stato Docker
#16:Controllo:impostazioni proxy Docker
#17:Check:Variabili di ambiente shell
#18:Controllo:Stato Kubelet

#19:Controllo:Syslog per errori PLEG
#20:Controllo:Versione di Cisco DNA Center da cui è stato costruito
#21:Check:Update history [approssimativo per mancanza di dati completi]

#22:Controllo:hook applicati
#23:Check:Cluster Node Reachability - nodi: [u'91.1.1.13', u'91.1.1.11', u'91.1.1.14']
#24:Check:Interface Reachability - tutti i nodi : [u'99.99.99.13', u'92.1.1.1', u'91.1.13', u'99.99.99.11', u'92.1.1.2', u'91.1.11', u'99.99.99.14', u'92.1.1.3', u'91.1 1,14"]
#25:Controllo:raggiungibilità VIP - VIP: [u'92.1.1.2', u'99.99.99.12', u'91.1.1.12']
#26:Controllo: numero di server DNS configurati in etcd nei nodi (<=3)
#27:Controllo:numero di voci /etc/resolv.conf (<=4)
#28:Check:DNS config - /etc/network/interfaces
#29:Controllo:Raggiungibilità DNS - DNS: [u'8.8.8.8']
#30:Controllo:il server DNS può risolvere Cisco Connect DNA
#31:Controllo: sincronizzazione server NTP: ['5.6.7.8', '1.2.3.4']
#32:Check:nome host del cluster definito
#33:Check:Impostazione predefinita di TimeZone su DNAC
#34:Verifica:errori nelle interfacce
#35:Controllo:DCBX a monte che causa le perdite di tx
#36:Controllo:alternanza tra nodi VIP
#37:Controllo:verifica errori nei registri del kernel

#38:Controllo:Validità e scadenza del certificato
#39:Verifica:scadenza dei certificati truststore
#40:Controllo:stato del servizio NTP su Cisco DNA Center
#41:Controllo:sincronizzazione ora server NTP

#42:Controllo: verifica dell'MTU memorizzata nella cache per le route a livello di interfaccia intra-cluster
#43:Controllo:stato rilevamento PMTU
#44:Controllo:Visualizzazione Nodo
#45:Controllo:stato nodo
#46:Controllo:Rapporto di diagnosi nodo

#47:Controllo:Distribuzione servizi...
#48:Controllo:Stato Appstack
#49:Controllo:Stato dell'endpoint
#50:Controllare i servizi per un numero elevato di riavvii
#51:Check:remedyctl è in esecuzione
#52:Controllo:stato degli stati ISE nel database
#53:Controllo: autenticazione esterna configurata per gli utenti DNAC

#54:Controllo:configurazione fallback autenticazione esterna
#55:Verifica:conteggio di gruppi scalabili, contratti e criteri di accesso nel database DNAC

#56:Controllo:stato migrazione/sincronizzazione GBAC

#57:Controllo:Istanze Di Glusterfs
#58:Controllo:Controllo NODE_NAME Glusterfs
#59:Controllo:Clustering Glusterfs

#60:Controllo:Statistiche di guarigione del volume Gluster
#61:Controllo:Integrità cluster ETCD
#62:Controllare:Dimensioni archiviazione ETCD
#63:Controllo:utilizzo della memoria ETCD
#64:Controllo:binding ETCD a loopback(localhost/127.0.0.1)
#65:Verifica:Stato cluster Postgres
#66:Controllo:dimensioni postgres
#67:Controllo: stato sincronizzazione e integrità cluster MongoDB
#68:Controllare la CPU MongoDB negli stati del docker
#69:Controllo:verifica delle dimensioni di MongoDB
#70:Controllo:Overflow Tenantintsegment
#71:Controllo:integrità InfluxDB
#72:Controllo:utilizzo memoria InfluxDB
#73:Controllo:Cassandra Health
#74:Controllo:stato Cassandra
#75:Check:Rabbitmq Integrità cluster
#76:Controllo:Stato cluster Rabbitmq
#77:Controllo:Stato coda Rabbitmq

#78:Check:Code Rabbitmq con messaggi non riconosciuti
#79:Controllo:Integrità cluster Zookeeper
#80:Controllo:Stato Cluster Zookeeper

#81:Check:Convalida periodo cluster Zookeeper
#82:Check:Elasticsearch Cluster Status : Maglev-System
#83:Check:Elasticsearch Cluster Status : NDP
#84:Controllo:Ascolto sidecar
#85:Check:BAPI (REST API) risponde
#86:Controllo:Cronologia backup
#87:Verifica:problema noto che causa il mancato avvio di LAN Auto

#88:Controllo:vulnerabilità critiche in Apache Log4j - CVE-2021-44228 e CVE-2021-45046

Preparazione all'aggiornamento

#01:Verifica:Sovrapposizione subnet cluster con indirizzi interni
#02:Controllo:Uso disco file RCA
#03:Controllo:conteggio dei contenitori usciti
#04:Controllo:numero di piedini non in esecuzione
#05:Controllo:Impostazioni Catalogo Maglev
#06:Controllo: dettagli canale rilascio catalogo - NESSUNA CONVALIDA - SOLO INFORMAZIONI PER LA REVISIONE
#07:Controllo: Pacchetti di aggiornamento del sistema catalogo - NESSUNA CONVALIDA - SOLO INFORMAZIONI PER LA REVISIONE
#08:Controllo:Pacchetti catalogo - NESSUNA CONVALIDA - SOLO INFORMAZIONI PER LA REVISIONE
#09:Controllo:Impostazioni repository padre
#10:Controllo:Connessione proxy a ciscoconnectdna tramite:http://a.b.c.d:80
#11:Controllo:Verifica mapping FileID mancanti nel servizio File
#12:Controllo:Scadenza dei certificati Maglev
#13:Controllo: scadenza del certificato CA del Registro di sistema

#14:Controllo:Scadenza del certificato CA

#15:Controllo:certificati etcd

#16:Controllo:verifica della presenza di punti di montaggio obsoleti
#17:Controllo:verifica della presenza di montaggi transitori Kubernetes
#18:Controllo:la configurazione di Collector-ISE è stata pulita dopo un aggiornamento precedente
#19:Controllo:flussi di lavoro in sospeso
#20:Selezionare:Schermo di backup per trovare l'ultimo backup riuscito
#21:Check:Provisioning non riuscito a causa di un parametro di stato della migrazione non valido
#22:Controllo:stato del servizio Maglev Hook Installer su Cisco DNA Center

#23:Controllo:Download dell'immagine di test dal repository dell'immagine cloud di Cisco DNA Center
#24:Controllare:verificare se SSL Intercept è configurato nella rete

#25:Controllo:codifica password proxy
#26:Controllo:conteggio multisito per distribuzione SDA
#27:Controllo:Percorso di aggiornamento di DNA Center all'ultima patch della versione 2.3.3.x
#28:Controllo:dispositivi Catalyst in modalità Bundle

#29:Controllo:Aggiornamenti recenti e file RCA
#30:Check:Secondary Interface Status (solo XL)
#31:Check:spazio dei nomi predefinito kubectl

#32:Controllo:errori della barra di scorrimento a causa di certificati aggiornati

#33:Controllare:Per uno spazio sufficiente nella partizione del disco /boot/efi
#34:Controllo:Compatibilità dei dispositivi fabric con DNA Center versione 2.3.3.x
#35:Controllo:migrazione pool IP
#36:Controllo:Server AAA configurati e relativo stato

Cisco DNA Center Assurance

#01:Controllo:Utilizzo spazio su disco della partizione Assurance
#02:Check:Stato di Assurance Services
#03:Controllo:Processo di rimozione back-end Assurance
#04:Controllo: verifica della sicurezza del processo di rimozione NDP che pulisce il database Redis
#05:Controllo:memoria insufficiente per Redis
#06:Check:stato Assurance Pipeline
#07:Controllo:Riepilogo punteggio integrità dispositivo
#08:Controllo:Riepilogo punteggio integrità client
#09:Controllo:chiamata API di telemetria corretta WLC
#10:Controllo:Controllo stato connessione di telemetria WLC Cisco IOS® XE
#11:Controllo:Cisco IOS XE WLC Netconf Yang Datastore Controllo
#12:Controllo:Cisco IOS XE WLC sdn-network-infra-iwan Trustpoint e certificati
#13:Controllo:Trustpoint e certificato Cisco IOS XE WLC DNAC-CA
#14:Controllo:stato di Cisco IOS XE WLC Device Network Assurance
#15:Controllo:Controllo stato connessione di telemetria WLC AIREOS
#16:Controllo:Controllo certificato di telemetria WLC AIREOS

Integrità di SD-Access

#01:Controllo:stato inventario raggiungibilità dispositivo fabric
#02:Controllo:Raccolta inventari fabric
#03:Controllo:SDA:Cisco DNA Center e stato di integrazione ISE
#04:Controllo:Verifica della connettività SSH tra Cisco DNA Center e Cisco ISE
#05:Controllo:utilizzo memoria nodi Cisco ISE
#06:Controllo:utilizzo dei dischi Cisco ISE Nodes
#07:Controllo:stato dei processi Cisco ISE

#08:Controllo:Determinazione di SGT e SGACL tramite API sul nodo ISE primario

#09:Controllo:SDA:acquisizione di comandi da bordi/CCP/Spigoli
#10:Controllo:SDA:Numero versioni software e tipi di piattaforma
#11:Controllo:SDA:Controllo utilizzo CPU dispositivi fabric
#12:Controllo:SDA:Controllo utilizzo memoria dispositivi fabric
#13:Check:SDA:Verifica del numero di sessioni LISP sui dispositivi fabric
#14:Controllo:SDA:Controllo delle dimensioni della tabella LISP IPv4 EID su tutti i dispositivi fabric
#15:Check:SDA:Check the LISP IPv4 MAP Cache Table size on the Borders (Controllo:SDA: verifica le dimensioni della tabella della cache delle mappe IPv4 LISP sui bordi)
#16:Controllo:SDA:Controllo dello stato delle sessioni ISIS per i dispositivi fabric
#17:Controllo:SDA: verifica che i dispositivi fabric abbiano più di una sessione ISIS - controllo di ridondanza
#18:Controllo:SDA:Solo bordi:Sessioni BGP IPv4
#19:Controllo:SDA:Solo bordi:Sessioni BGP VPNv4
#20:Controllo:SDA:Connettività server AAA dai dispositivi
#21:Controllo:SDA:CTS PACS scaricato nei dispositivi
#22:Controllo:SDA:CTS SGT scaricati nei dispositivi

#23:Controllo:SDA:Controllo utilizzo CPU WLC
#24:Controllo:SDA:Controllo utilizzo memoria WLC
#25:Controllo:Controllo punto di accesso fabric WLC
#26:Controllo:Controllo WLC Fabric WLAN

Cisco DNA Center Scale

#01:Controllo:Scala: numero di siti
#02:Check:Scale: numero di criteri di controllo di accesso
#03:Controllo:Scala: numero di contratti di accesso
#04:Controllo:Scala: numero totale di dispositivi (switch, router, controller wireless)
#05:Check:Scale: numero di domini fabric
#06:Controllo:Scala: numero di siti dell'infrastruttura
#07:Check:Scale: numero di SGT di gruppo
#08:Check:Scale: numero di SuperPool IP
#09:Check:Scale: numero di connessioni ISE
#10:Controllo:Scala : numero massimo di AAA (raggio)
#11:Controllo:Scala: numero di SSID
#12:Controllo:Scala: numero di reti virtuali per sito
#13:Controllo:Scala: numero di punti di accesso wireless
#14:Controllo:Scala: numero di controller LAN wireless
#15:Controllo:Scala: numero di sensori wireless

#16:Controllo:Scala: numero di dispositivi fabric per sito
#17:Controllo:Scala: numero di bordi dell'infrastruttura per sito
#18:Check:Scale: numero di nodi del piano di controllo dell'infrastruttura per sito

Valori hash del file dnac_aura

Versione	Hash MD5	Hash SHA256

AURA		
1.5.9	52f429dd275e357fe3282600d38ba133	c91b6092ab4fa57adbe698a3c17f9146523bba5b031522
1.6.0	e01328f5e0e4e5f5c977c5a14f4a1e14	4f8115d1f2f480efcdb0260cc5a9abb8a067f3cbac2c293a
1.6.8	f291e3e694fadb2af722726337f31af5	fb7c125910d77c8087add419b937a893174fb30649427a

---

Risoluzione dei problemi

In caso di problemi, consultare il sito dnac_sda_audit_tool@cisco.com con il report in formato PDF e i file di registro TAR.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).