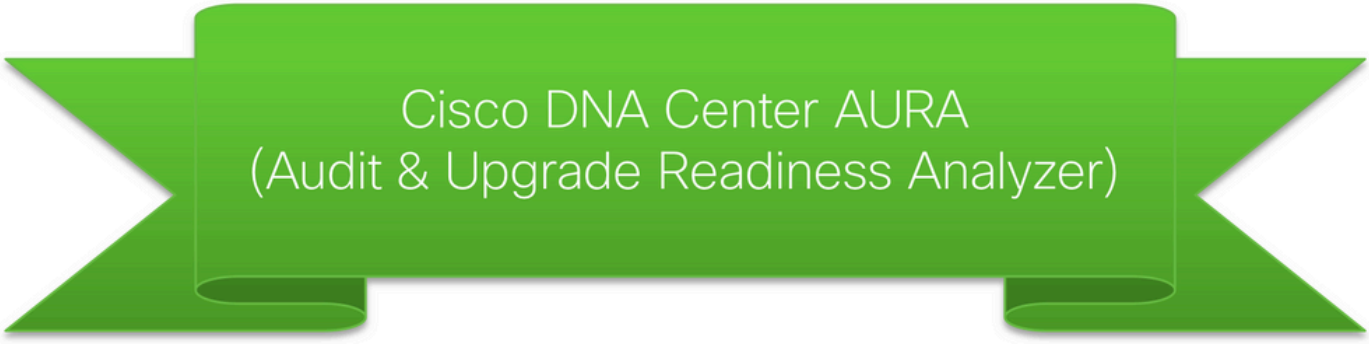
Use AURA for Enhanced Visibility into the DNA Center

Contents



Introduction

This document describes the Cisco DNA Center Audit and Upgrade Readiness Analyzer (AURA) command line tool.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on Cisco DNA Center platform.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

AURA performs a variety of health, scale and upgrade readiness checks for the Cisco DNA Center and the rest of the Fabric network. The tool is extremely simple to run and is executed on the Cisco DNA Center. The tool uses Application Programming Interface (API) calls, DB reads and show commands (read only operations) and hence, does not affect performance or cause impact to the Cisco DNA Center or the networking devices.

Why is AURA Simple and Straight Forward to Use

- Uses current pre-installed libraries/software ONLY.
- Automatically generated PDF report.
- Only Input required – Cisco DNA Center passwords (both admin & maglev).
- Zipped Logs & Report can be automatically uploaded to Cisco SR (optional).
- Simply copy the file to the Cisco DNA Center and execute the file on the Cisco DNA Center.
- Not Intrusive - only Database (DB) reads, show commands and API calls.
- Run Time - less than 15 minutes for the Cisco DNA Center checks and the time varies for the Software Defined Access (SDA) checks based on the scale of the network (about 30 minutes for 30 devices).
- Works with 1.2.8, 1.2.10.x, 1.2.12.x, 1.3.x and 2.x releases.

Please contact us at dnac_sda_audit_tool@cisco.com for any issues or feedback.

AURA Tool Check Areas / Features

- Cisco DNA Center Scale Test
- Cisco DNA Center Infra Health
- Cisco DNA Center Assurance Health
- WLC/eWLC Assurance Health
- SDA Device CLI Capture
- SDA Control & Security Audit
- Software Bugs Causing Upgrade Failures
- Upgrade Readiness Checks
- SDA Compatibility Check (Switches, Wireless Controllers and Identity Services Engine (ISE) for 2.3.3.x
- Digital Network Architecture Center (DNAC)-ISE Integration Checks
- Fabric Devices Configurations Capture and Compare and use inbuilt diff tool
- Remote Launch of AURA (from 1.2.0 release)
- Schedule AURA with cron (from 1.2.0 release)
- Syslog Server Integration (from 1.2.0 release)
- Download test images from the Cloud (from 1.5.0 release)

How to Run the Tool (Simple Steps)

Step 1. Copy the executable AURA file to the Cisco DNA Center. The latest version is present at https://github.com/CiscoDevNet/DNAC-AURA.

Step 2. Run the tool from the Cisco DNA Center (if you have a cluster, please look at example 5 in section Cisco DNA Center AURA Options).

```
$ ./dnac_aura
```

How to Run the Tool (Detailed Steps)

If Cisco DNA Center version is 2.3.3.x and later, the Cisco DNA Center has a restricted shell enabled for added security from versions 2.3.3.x onwards. The default shell is called magshell and it does not support any Linux commands or the execution of AURA. Disable the restricted shell and enable the Bash shell before you proceed to the next step. Disabling restricted shell on 2.3.3.x. For versions 2.3.4.x and later, a consent token can be required from Cisco Technical Assistance Center (TAC) to disable the restricted shell.

Step 1. Copy the executable file to the Cisco DNA Center.

```
dnac_aura
```

The file is located at https://github.com/CiscoDevNet/DNAC-AURA and there are a few ways to copy the file to the Cisco DNA Center.

File Copy Option 1. Click the URL and download the file via your browser:

Copy the file to your Cisco DNA Center and use a file transfer software (do not forget to use Secure File Transfer Protocol (SFTP) with port 2222 & username maglev).

File Copy Option 2. Copy the file to the Cisco DNA Center directly and use GIT commands:

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

File Copy Option 3. If a proxy server is setup, then copy the file to the Cisco DNA Center and use GIT commands and the proxy server details:

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

Step 2. Ensure the file dnac_aura is executable.

When the file dnac_aura is copied to the Cisco DNA Center, it is usually not copied as executable. Run the command to make it executable. If you have used GIT, then this step is not necessary.

```
$ chmod 755 dnac_aura
```

Step 3. (Optional) Validate the hash of the file dnac_aura to ensure the right file has been downloaded.

To ensure the right file has been downloaded, compare either the MD5 hash or the SHA256 hash values which are available at the end of this page. Each version of AURA can have a unique set of hash values.

Option 1. MD5 Hash verification.

Use the command md5sum (as listed). Generate the hash on your Cisco DNA Center or any other Linux system and compare the hash value with the value at the end of this page.

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

Option 2. SHA256 Hash verification.

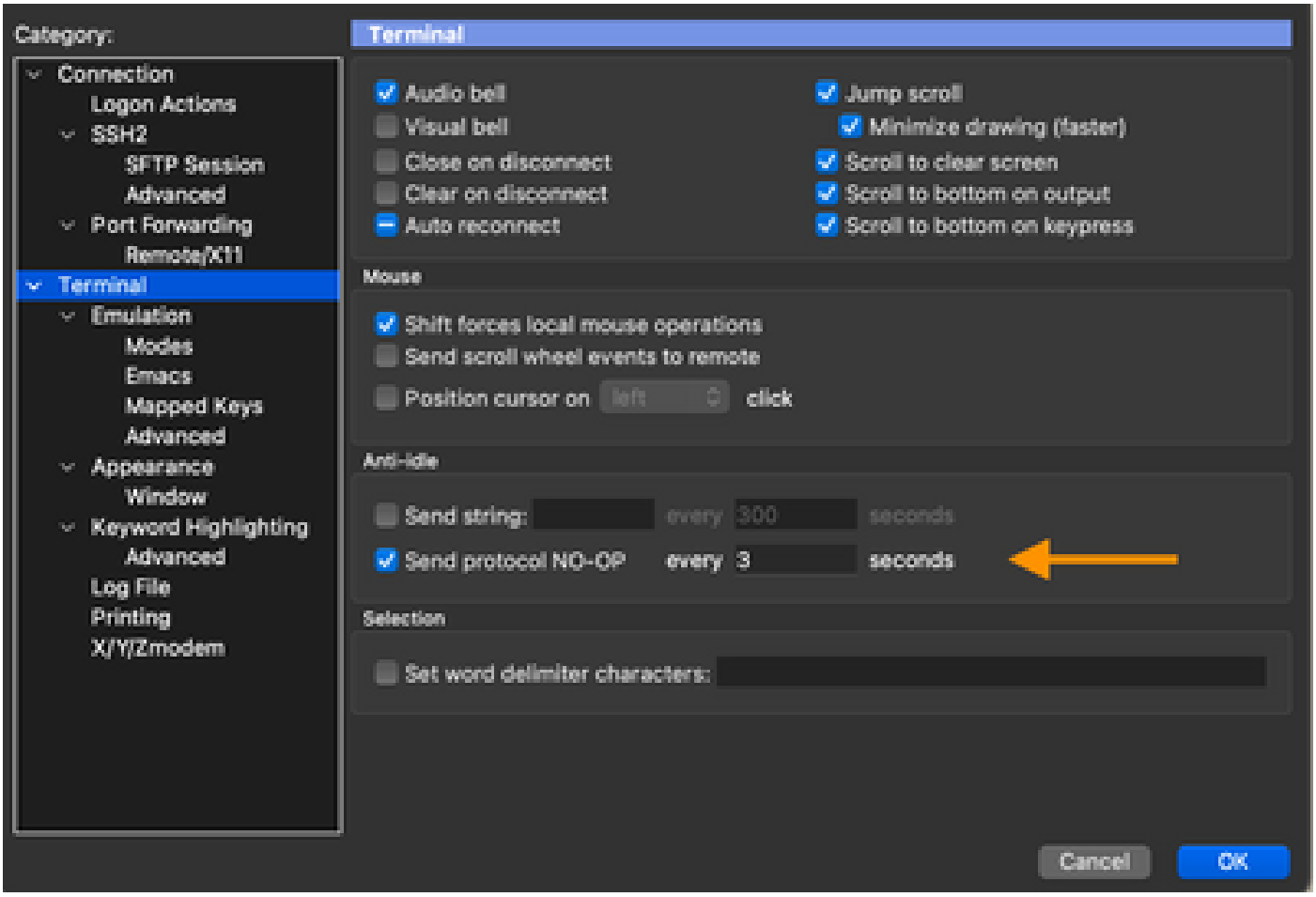
Use the command sha256sum (as listed). Generate the hash on your Cisco DNA Center or any other Linux system and compare the hash value with the value at the end of this page.

```
$ sha256sum dnac_aura
c91b6092ab4fa57adbe698a3c17f9146523bba5b0315222475aa4935662a0b6e dnac_aura
```

Step 4. Set an idle timeout for the SSH session.

Later versions (2.x+, 1.3.3.8+) of the Cisco DNA Center have an SSH idle timeout. This can impact AURA being run from an SSH session. Ensure the idle timeout is set, otherwise, the AURA tool can be abruptly terminated.

Here is an example of setting a 3 second idle timeout on SecureCRT.



Step 5. Run the tool from the Command Line.

Choose the relevant option based on where the file is located to execute the checks on the Cisco DNA Center. (When you use options, you can include/exclude various checks).

```
$ ./dnac_aura
```

or

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

Remote Execution of AURA

This script allows you to launch the AURA on a remote Cisco DNA Center. It uses paramiko and scp libraries.

Procedure to Install

To install, it is recommended that you use a virtual environment. These lines can create a python3 virtual environment, activate it, upgrade pip, and install the required libraries.

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

Session Timeout

Later versions (2.1+, 1.3.3.8+) of Cisco DNA Center have an ssh idle timeout. This can impact AURA being run from an ssh session either directly on DNAC, or indirectly via the run_remote script or ansible.

The work around is simple. For an ssh connection, the -o ServerAliveInterval=3 flag can send keepalives and maintain the session. This is used in this script, and can also be used for direct ssh connection as well as ansible.

Use the Script

The script requires three arguments:

- dnac
- admin password (also available as an environment variable DNAC_ADMIN_PASS)
- maglev password (also available as an environment variable DNAC_MAGLEV_PASS)
- admin user (also available as an environment variable DNAC_ADMIN_USER). This defaults to "admin", and only needs to be changed if you use external auth and different superUser name. In many cases, this is not required, but is available as --admin-user

the simplest way to run the script with arguments (see later section on environment vars) is

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

If you are familiar with shell environment variables, this can be simplified further

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

Pass AURA Options (--)

To pass AURA specific arguments (for example -s to run SDA tests) you need to do this:

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

Make sure you include any run_remote options, such as --local-dir, all-cluster and --no-pull BEFORE the "--"

AURA specific options such as -n, --syslog, -d, -s need to be after the "--"

Store AURA Output Locally

AURA script supports the --json-summary option. This produces a json summary of the test results as well as the location of the report and log file on DNAC. When run_remote is supplied with the --local-dir option, the log and report files can be moved back to DNAC. A json-summary file can be created. A directory for the DNAC is created.

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

After this completes, the /home/aradford/RUN_REMOTE/logs directory can contain:

```
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
```

The json file contains:

```
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 Execution

If you use the --all-cluster option, the script can find all members of the cluster and run AURA on each one. Currently, this is a serial execution. It can be used with --local-dir to copy the report, logfile and json-summary back from DNAC.

Either a VIP or physical address can be provided. The script can connect and look for all physical IP in the same subnet as the IP used to connect.

Other Options

The script can also be run with the --no-pull option. This stops the git pull to update to the latest version of AURA, but assumes you have copied aura to the home directory on DNA Center.

AURA with CRON

Cron is a challenge for AURA due to the lack of PTY. It also requires the DNA Center crontab to be edited.

run_remote probably a better way of running AURA, as it solves the PTY issue and removes the need to edit the local DNA Center crontab. Running remotely combined with --local-path means all DNA Center logs are in the same on an external server.

Here is a sample crontab entry for running AURA on a DNAC every hour. You need to supply the python interpreter explicitly to pick up the virtual environment contain paramiko and scp libraries.

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

This can be wrapped further by a shell script to protect the credentials from being stored in plain text.

Cisco DNA Center AURA Options

Table 1 - Checks/Functionality of the Various AURA Options

	No Options (default)	-s	-d	-o	-c
DNA Center Infra Health Checks	X	X	X		
DNA Center Assurance Health Checks	X	X			
WLC/eWLC Assurance Health Checks	X	X			
Basic SDA Checks (Inventory check)DNAC-ISE Integration (only if ISE is integrated)	X	X			
SDA(Fabric Device CLI collection, Control Plane & Security		X			

Plane Audit and Compatibility Check)					
Upgrade Readiness Checks (includes bugs)	X	X			
DNA Center Scale (Fabric & Non Fabric scale parameters)	X	X	X		
Capture CLI Outputs from the fabric devices and store locally on the DNA Center - command and device list provided via file captureFile.yaml2 files captured:.json - Command Runner default output.log - Human Readable				X	
Compare configurations across multiple devices (based on outputs captured and use -o option)					X

Command Line Output of the AURA Options

```
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.
```

Examples of Running AURA with Various Options

Example 1: In order to select Stark Industries as the company name, run default AURA checks and copy the file to SR 611111111 with password 123kjaksdhf, the command is:

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

Example 2: In order to run both Cisco DNA Center and SDA checks for customer Stark Industries, the command is:

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

Example 3: In order to run show command outputs and store it in a file on the Cisco DNA Center, use the -o option. The tool can use Cisco DNA Center's command runner to fetch the outputs for you. The command is:

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

To specify the devices and the commands to run on these devices, require the captureFile.yaml to be available in the same directory. The sample is present in github.

Example 4: In order to compare running configurations of the catalyst switches and/or the eWLC, use the -c option. Please ensure you have earlier used the -o option to capture the outputs from the devices. The command is:

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

Example 5: In order to run AURA checks on a cluster, for any one node, choose the appropriate option from the table. For the remaining two nodes, choose option -d.

On any one node:

```
$ ./dnac_aura
```

On the remaining 2 nodes:

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

Example 6: In order to schedule AURA, use cron or to run AURA remotely, check out this readme file on github.

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

Example 7: In order to verify the path to the Cloud repo on AWS where the DNA Center images are stored, you can run AURA with this option. The check downloads 3 images (small - 50MB, medium - 150MB and large - 650MB) and can calculate the time to download these three files. The check can ensure that the test images are deleted and no reports are generated when you choose this option.

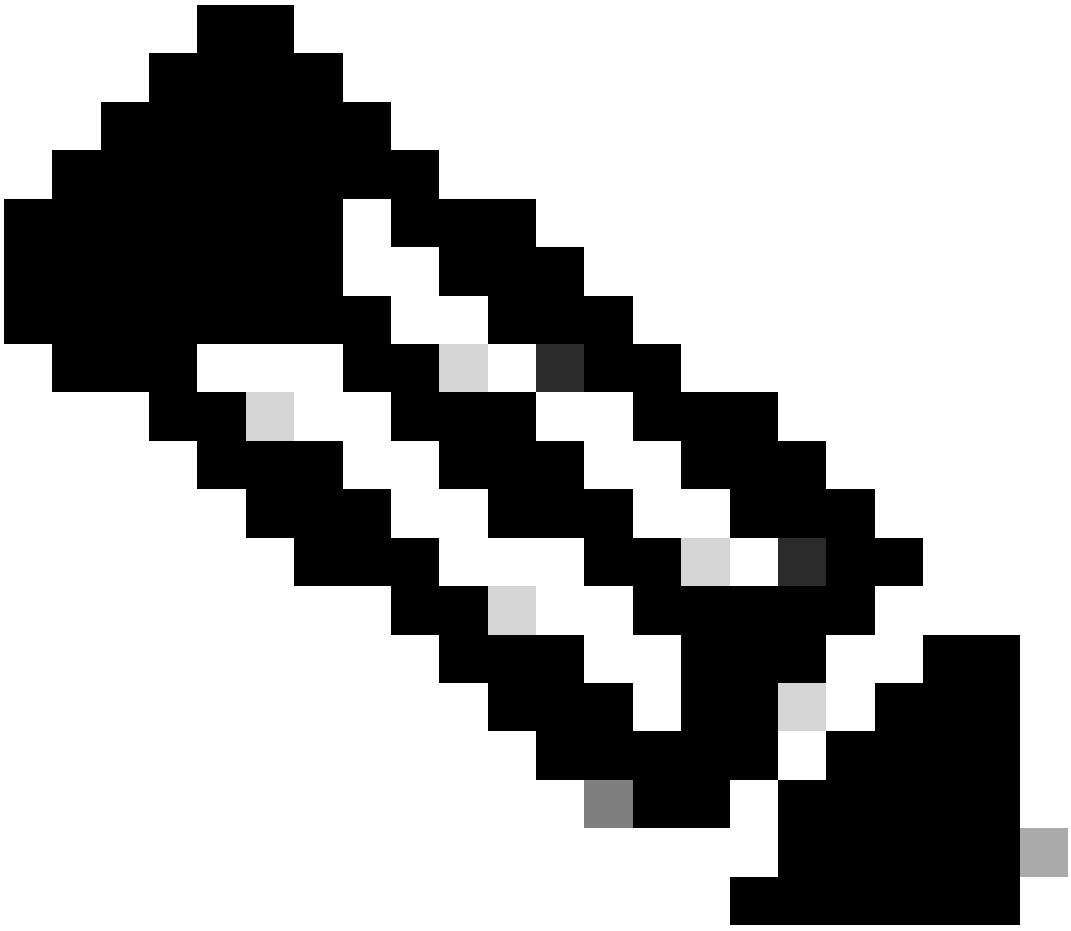
On any node:

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

Example of the check:

```
$./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

$
```

Example 7: When running AURA with the -s option, AURA can perform the control and security plane audits for a maximum of 50 fabric devices per fabric site. In order to eliminate this limit, use the --sdadevcheck option.



Note: The run time of the tool increases with the additional devices added.

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

Outputs from the Tool

When the tool starts, you are prompted for the admin username/password followed by the maglev password.

```
$ ./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_

$
```

The tool generates 2 files that are stored in /data/tmp/dnac_aura/:

- A PDF report in /data/tmp/dnac_aura/reports. The first page provides data on the DNA Center (the model, serial number, software version and IP address), the execution time of the tool and provides a summary of all the checks performed and the results. The remaining pages provide more details on the various checks, with snippets of command output and the results. Errors and warnings are color coded and easily searchable. (A report is not generated with the -o option).
- All the logs from the Cisco DNA Center and show commands from the devices are zipped into a tar.gz file.

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 Versions - Change Log

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

Checks Performed By AURA

Cisco DNA Center Health and Connectivity

#01:Check:Latest version of AURA
#02:Check:Determine Cisco DNA Center Product Type, Serial number, SW Version & Node IP
#03:Check:Determine Cisco DNA Center memberid
#04:Check:CPU Load Average
#05:Check:Disk Layout
#06:Check:Disk Partition Mounts
#07:Check:Disk Space and iNodes Utilization
#08:Check:if Glusterfs is mounted
#09:Check:for non responsive NFS mounts

#10:Check:for NFS stale file handle
#11:Check:Disk I/O throughput
#12:Check:DRAM Total Available Memory
#13:Check:DRAMs Installed in the appliance
#14:Check:Processor Cores Enabled and Status
#15:Check:Docker Status
#16:Check:Docker Proxy settings
#17:Check:Shell Environment Variables
#18:Check:Kubelet Status

#19:Check:Syslog for PLEG Errors
#20:Check:Version of Cisco DNA Center this was built from
#21:Check:Update history [this is approximate due to lack of complete data]

#22:Check:hooks applied
#23:Check:Cluster Node Reachability - nodes : [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'91.1.1.11', 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:Number of DNS servers configured in etcd on nodes (<=3)
#27:Check:Number of /etc/resolv.conf entries (<=4)
#28:Check:DNS config - /etc/network/interfaces
#29:Check:DNS Reachability - DNS : [u'8.8.8.8']
#30:Check:DNS server can resolve Cisco Connect DNA
#31:Check:NTP server Sync : ['5.6.7.8', '1.2.3.4']
#32:Check:Cluster hostname is defined
#33:Check:Default TimeZone setting on DNAC
#34:Check:interfaces for errors
#35:Check:DCBX upstream causing tx drops
#36:Check:VIP Toggle between nodes
#37:Check:check kernel logs for errors
#38:Check:Certificate Validity and Expiry
#39:Check:Expiry of truststore certificates
#40:Check:NTP Service status on the Cisco DNA Center
#41:Check:NTP Server Time Sync

#42:Check:check for Cached MTU at Intra-Cluster Interface level routes
#43:Check:Status of PMTU discovery
#44:Check:Node Display

#45:Check:Node Status
#46:Check:Node Diagnosis Report

#47:Check:Service Distribution ...
#48:Check:Appstack Status
#49:Check:Endpoint Status
#50:Check:Check Services for High Restart Counts
#51:Check:remedyctl is running
#52:Check:State of ISE states in DB
#53:Check:External authentication configured for DNAC users

#54:Check:External authentication fallback configuration
#55:Check:check Count of Scalable Groups, Contracts and Access Policies in DNAC DB

#56:Check:GBAC Migration/Sync Status

#57:Check:Glusterfs Instances
#58:Check:Glusterfs NODE_NAME check
#59:Check:Glusterfs Clustering

#60:Check:Gluster Volume Heal Statistics
#61:Check:ETCD Cluster Health
#62:Check:ETCD Storage Size
#63:Check:ETCD memory utilization
#64:Check:ETCD binding to loopback(localhost/127.0.0.1
#65:Check:Postgres Cluster Status
#66:Check:Postgres size
#67:Check:MongoDB Cluster Health and Sync Status
#68:Check:Check MongoDB CPU in docker stats
#69:Check:Check MongoDB Sizes
#70:Check:Tenantintsegment overflow
#71:Check:InfluxDB Health
#72:Check:InfluxDB Memory Utilization
#73:Check:Cassandra Health
#74:Check:Cassandra status
#75:Check:Rabbitmq Cluster Health
#76:Check:Rabbitmq Cluster Status
#77:Check:Rabbitmq Queue Status
#78:Check:Rabbitmq Queues with Unacknowledged messages
#79:Check:Zookeeper Cluster Health
#80:Check:Zookeeper Cluster Status

#81:Check:Zookeeper Cluster Epoch Validation
#82:Check:Elasticsearch Cluster Status : Maglev-System
#83:Check:Elasticsearch Cluster Status : NDP
#84:Check:Sidecars listening
#85:Check:REST API (BAPI) responds
#86:Check:Backup History
#87:Check:Known issue that causes LAN Auto to fail to start

#88:Check:Critical Vulnerabilities in Apache Log4j - CVE-2021-44228 & CVE-2021-45046

Upgrade Readiness

#01:Check:Cluster Subnet Overlap with Internal Addresses
#02:Check:RCA Files Disk Usage
#03:Check:Count of Exited containers
#04:Check:Count of Non Running Pods
#05:Check:Maglev Catalog Settings
#06:Check:Catalog Release Channel Details - NO VALIDATION - ONLY INFO FOR REVIEW
#07:Check:Catalog System Update Packages - NO VALIDATION - ONLY INFO FOR REVIEW
#08:Check:Catalog Packages - NO VALIDATION - ONLY INFO FOR REVIEW
#09:Check:Parent Repository Settings
#10:Check:Proxy connect to ciscoconnectdna via:http://a.b.c.d:80
#11:Check:Check File-service for missing FileID mappings
#12:Check:Expiry of Maglev Certs
#13:Check:Expiry of registry CA cert

#14:Check:Expiry of CA Cert

#15:Check:etcd certificates

#16:Check:Check for Stale Mount Points
#17:Check:Check for Kubernetes Transient Mounts
#18:Check:Collector-ISE config has been cleaned up after a previous upgrade
#19:Check:Pending workflows
#20:Check:Backup Display to find Last Successful Backup
#21:Check:Provision fail due to invalid migration status parameter
#22:Check:Maglev Hook Installer Service status on the Cisco DNA Center

#23:Check:Download test image from the Cisco DNA Center Cloud Image Repository
#24:Check:Check if SSL Intercept is configured in the Network
#25:Check:Proxy password encoding
#26:Check:Multisite count for SDA deployment
#27:Check:DNA Center Upgrade Path to the latest patch of 2.3.3.x
#28:Check:Catalyst devices in Bundle Mode

#29:Check:Recent updates and RCA files
#30:Check:Secondary Interface Status (XL only)
#31:Check:kubectl default namespace

#32:Check:For Tiller failure due to refreshed certs

#33:Check:For sufficient space in disk partition /boot/efi
#34:Check:Fabric Devices Compatibility with DNA Center Version 2.3.3.x
#35:Check:IP Pool Migration
#36:Check:Configured AAA Servers and their Status

Cisco DNA Center Assurance

#01:Check:Assurance Partition Disk Space Usage
#02:Check:Assurance Services Status
#03:Check:Check Assurance Backend Purge Job
#04:Check:Check Assurance NDP Purge Job that cleans up Redis DB
#05:Check:Redis Out of memory
#06:Check:Assurance Pipeline status
#07:Check:Device health score summary
#08:Check:Client health score summary

#09:Check:WLC correct telemetry API call
#10:Check:Cisco IOS® XE WLC Telemetry Connection Status Check
#11:Check:Cisco IOS XE WLC Netconf Yang Datastore Check
#12:Check:Cisco IOS XE WLC sdn-network-infra-iwan Trustpoint & Certificates
#13:Check:Cisco IOS XE WLC DNAC-CA Trustpoint & Certificate
#14:Check:Cisco IOS XE WLC Device Network Assurance Status
#15:Check:AIREOS WLC Telemetry Connection Status Check
#16:Check:AIREOS WLC Telemetry Certificate Check

SD-Access Health

#01:Check:Fabric device reachability inventory status
#02:Check:Fabric inventory collection
#03:Check:SDA:Cisco DNA Center & ISE integration status
#04:Check:Verify the SSH connectivity between Cisco DNA Center and Cisco ISE
#05:Check:Cisco ISE Nodes Memory Usage
#06:Check:Cisco ISE Nodes Disks Usage
#07:Check:Status of the Cisco ISE processes

#08:Check:Determine the SGTs & SGACLs via API on the Primary ISE Node

#09:Check:SDA:Capturing Commands from the Borders/CPs/Edges
#10:Check:SDA:Software version and platform type count
#11:Check:SDA:Fabric devices CPU Utilization Check
#12:Check:SDA:Fabric devices Memory Utilization Check
#13:Check:SDA:Verify the number of LISP Sessions on the Fabric devices
#14:Check:SDA:Check the LISP IPv4 EID Table size on all Fabric devices
#15:Check:SDA:Check the LISP IPv4 MAP Cache Table size on the Borders
#16:Check:SDA:Check the ISIS Sessions state for the Fabric devices
#17:Check:SDA: Ensure the Fabric devices have more than one ISIS Session - Redundancy check
#18:Check:SDA:Borders Only:IPv4 BGP Sessions
#19:Check:SDA:Borders Only:VPNv4 BGP Sessions
#20:Check:SDA:AAA Server connectivity from the devices
#21:Check:SDA:CTS PACS downloaded to the devices
#22:Check:SDA:CTS SGTs downloaded to the devices

#23:Check:SDA:eWLC CPU Utilization Check
#24:Check:SDA:eWLC Memory Utilization Check
#25:Check:eWLC Fabric AP Check
#26:Check:eWLC Fabric WLAN Check

Cisco DNA Center Scale

#01:Check:Scale : Number of Sites
#02:Check:Scale : Number of Access Control Policies
#03:Check:Scale : Number of Access Contracts
#04:Check:Scale : Total number of devices (switch, router, wireless controller)
#05:Check:Scale : Number of Fabric Domains
#06:Check:Scale : Number of Fabric Sites
#07:Check:Scale : Number of Group SGTs
#08:Check:Scale : Number of IP SuperPools
#09:Check:Scale : Number of ISE connections
#10:Check:Scale : Max number of AAA (Radius)
#11:Check:Scale : Number of SSIDs

#12:Check:Scale : Number of Virtual Networks per site
#13:Check:Scale : Number of Wireless Access Points
#14:Check:Scale : Number of Wireless LAN Controllers
#15:Check:Scale : Number of Wireless Sensors

#16:Check:Scale : Number of Fabric Devices per Site
#17:Check:Scale : Number of Fabric Borders per Site
#18:Check:Scale : Number of Fabric Control Plane Nodes per Site

Hash Values for the dnac_aura File

AURA Version	MD5 Hash	SHA256 Hash
1.5.9	52f429dd275e357fe3282600d38ba133	c91b6092ab4fa57adbe698a3c17f9146523bba5b0315222475aa49356
1.6.0	e01328f5e0e4e5f5c977c5a14f4a1e14	4f8115d1f2f480efcdb0260cc5a9abb8a067f3cbac2c293a2615cb62b6
1.6.8	f291e3e694fadb2af722726337f31af5	fb7c125910d77c8087add419b937a893174fb30649427ad578df75d63

Troubleshoot

If you face any issues, reach out at dnac_sda_audit_tool@cisco.com with the PDF report and TAR log files.
