

Collect Logs from Cisco DNA Center Quick Start Guide

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[AURA Tool to Perform Health, Scale and Upgrade Readiness Checks](#)

[Cisco DNA Center Issue Categorization](#)

[Logs to be Collected for Upgrade Issues](#)

[Logs to be Collected for Automation, Assurance or any SDA / Non-SDA Provisioning Issues](#)

[Logs to be Collected for GUI Issues](#)

[Logs to be Collected from Network Devices for Software-Defined Access Network Issues](#)

Introduction

This document describes the steps to collect necessary logs and command outputs from Cisco DNA Center.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- It is required that the user has Command Line Interface (CLI) access to the Cisco DNA Center.
- To log into Cisco DNA Center using CLI, you must connect via Secure Socket Shell (SSH) to your Cisco DNA Center's IP address using maglev as the username on port 2222.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco DNA Center

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

Providing this information upfront in a Technical Assistance Center (TAC) Service Request (SR) helps you hit the ground running with respect to resolving your issue.

AURA Tool to Perform Health, Scale and Upgrade Readiness

Checks

Execute the AURA tool which is available on Github to perform Health, Scale and Upgrade Readiness checks on the Cisco DNA Center. The tool can also capture outputs from the fabric devices, ISE & WLC to perform multiple health, control plane, security plane, and Assurance based checks. It is extremely useful to run prior to an upgrade to ensure a smooth and successful upgrade. The tool can be scheduled to run on a regular basis.

More details available [here](#).

Cisco DNA Center Issue Categorization

For any issues faced in the components mentioned in the Issue Description, refer to the corresponding Issue Categories detailed next to collect the required information.

| Issue Category | Issue Description |
|--------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Upgrade | Any failures observed during system/application upgrade flows. |
| Automation | Backup and Restore High Availability (HA) Managed Services Inventory/Discovery Network Design Provisioning IP Pools LAN Automation SWIM Template Provisioning NFV Provisioning PNP Smart Licensing Access Policy(ACA) Maps-Topology Integration issues with ISE, CMX, Cisco DNA-Spaces, UDN, NBAPI, NB-notifications, and so on. |
| Non-SDA Provisioning | Any failures observed in Non-SDA Provisioning flows. |
| Assurance | Analytics & Reports Telemetry Any other failures observed in Assurance flows. |

| | |
|-----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| | |
| GUI Issues | This is good to collect any errors observed in the GUI in addition to the information requested in other area-specific buckets. |
| Software-Defined Access | Any failures observed across the Software-Defined Access Fabric Devices. |

Logs to be Collected for Upgrade Issues

Step 1. From the CLI of Cisco DNA Center, collect these command outputs:

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

Step 2. Send the output of the system-updater service to a log file and use this command, and collect the file from the /tmp folder.

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

Step 3. Collect the RCA logs as instructed in this [document](#).

Logs to be Collected for Automation, Assurance or any SDA / Non-SDA Provisioning Issues

Step 1. Collect the RCA logs as instructed in this [document](#).

Step 2. Run the [Cisco DNA Center AURA tool](#)

Logs to be Collected for GUI Issues

Step 1. Collect the RCA logs as instructed in this [document](#).

Step 2. Run the [Cisco DNA Center AURA tool](#)

Step 3. Collect HAR files from the web browser. Step by Step instructions for Chrome follow:

- When an error is seen in the GUI, navigate to and right-click on the page and choose **Inspect**.

Welcome, admin

Learn about new capabilities in this release on the Cisco DNA Center YouTube Channel.

Assurance Summary

Health ⓘ
Healthy as of Jun 12, 2020 3:20 PM

| | | |
|------------------------|-------------------------|-----------------------|
| 67% Network Devices | --% Wireless Clients | 100% Wired Clients |
|------------------------|-------------------------|-----------------------|

[View Details](#)

Critical Issues
Last 24 Hours

| | |
|----------|----------|
| 26 P1 | 23 P2 |
|----------|----------|

[View Details](#)

Trends and
Last 7 Days

Through

Network Snapshot

Sites
As of Jun 12, 2020 3:22 PM

5

DNS Servers
NTP Servers

Unclaimed: 1
Unprovisioned: 5
Unreachable: 2

[Find New Devices](#)

| | |
|----------------------|-----------------|
| Back | Alt+Left Arrow |
| Forward | Alt+Right Arrow |
| Reload | Ctrl+R |
| Save as... | Ctrl+S |
| Print... | Ctrl+P |
| Cast... | |
| Translate to English | |
| View page source | Ctrl+U |
| View frame source | |
| Reload frame | |
| Inspect | Ctrl+Shift+I |

- Inspect opens the Developer Tools on the right side of the page. Navigate to and click the **Network** tab, as shown:

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

Assurance Summary

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

Network Snapshot

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

The screenshot shows the Chrome DevTools Network tab. The "Network" tab is selected, and a download arrow icon is visible in the top right corner of the network list. The console shows "What's New X" and "Highlights from the Chrome 83 update".

- Click the **download arrow** (Export HAR) as shown:

The screenshot displays the Cisco DNA Center interface. The top navigation bar includes the Cisco DNA Center logo and search icons. The main content area is divided into several sections:

- Welcome, admin**: A banner with a "Take a Tour" button and a link to the Cisco DNA Center YouTube Channel.
- Assurance Summary**: A section with three cards:
 - Health**: Shows a health status of 67% (Network Devices), 100% (Wireless Clients), and 100% (Wired Clients). It is noted as "Healthy as of Jun 12, 2020 3:20 PM".
 - Critical Issues**: Shows 26 P1 and 23 P2 issues. It is noted as "Last 24 Hours".
 - Trends and Insights**: Shows trends for Throughput and Coverage over the last 7 days.
- Network Snapshot**: A section with three cards:
 - Sites**: Shows 5 sites. It is noted as "As of Jun 12, 2020 3:32 PM".
 - Network Devices**: Shows 10 devices. It is noted as "As of Jun 12, 2020 3:32 PM".
 - Application Policies**: Shows 0 policies. It is noted as "As of Jun 12, 2020 3:33 PM".

On the right side, the Chrome DevTools Network tab is open, displaying a list of blocked requests. The table below shows the details of these requests:

| Name | Status | Type |
|------------------------------------------|--------|------|
| count?reachabilityStatus=Unreachable&... | 200 | xhr |
| count?isNetworkDevice=true&aggregate... | 200 | xhr |
| details?__preventCache=1591993966753 | 200 | xhr |
| details?__preventCache=1591993971758 | 200 | xhr |
| details?__preventCache=1591993976775 | 200 | xhr |
| details?__preventCache=1591993981754 | 200 | xhr |
| details?__preventCache=1591993986742 | 200 | xhr |
| TauthSource=internal&limits=1&usern... | 200 | xhr |
| details?__preventCache=1591993991754 | 200 | xhr |
| application/miniDashboardFilter=true | 200 | xhr |
| details?__preventCache=1591993996752 | 200 | xhr |
| details?__preventCache=1591994001756 | 200 | xhr |
| details?__preventCache=1591994006775 | 200 | xhr |
| details?__preventCache=1591994011765 | 200 | xhr |
| details?__preventCache=1591994016739 | 200 | xhr |
| details?__preventCache=1591994021326 | 200 | xhr |
| application/miniDashboardFilter=true | 200 | xhr |
| details?__preventCache=1591994026328 | 200 | xhr |
| details?__preventCache=1591994031353 | 200 | xhr |
| TauthSource=internal&limits=1&usern... | 200 | xhr |
| details?__preventCache=1591994036363 | 200 | xhr |
| details?__preventCache=1591994041339 | 200 | xhr |
| details?__preventCache=1591994046337 | 200 | xhr |

- **Save** the HAR file locally, and be sure to upload it to your TAC Service Request.

Logs to be Collected from Network Devices for Software-Defined Access Network Issues

Step 1. Collect (via Cisco DNA Center Command Runner / or directly from device CLI) from all control-nodes, border-nodes, as well as affected edges for given Software-Defined Access fabric site:

```
terminal length 0
```

```
show tech-support
```

```
show tech-support fabric
```

```
show tech-support lisp
```

```
show tech-support cef
```

```
show tech-support isis
```

```
show tech-support platform
```