Collect and Analyze Data from the Cisco SD-Access Fabric

Revised: July 13, 2021

Fabric Data Collection Overview

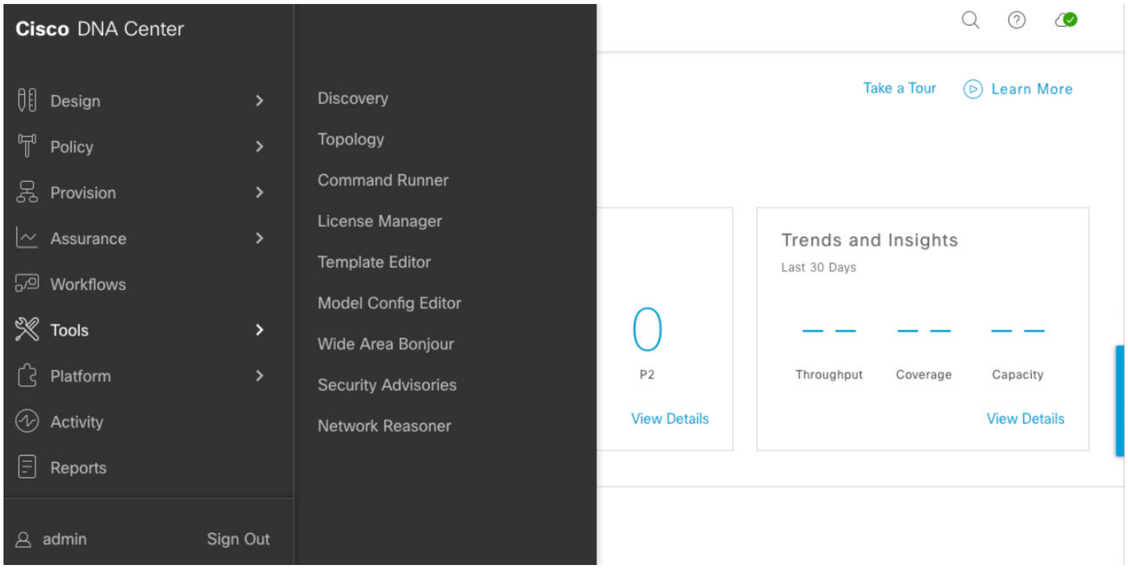
The Fabric Data Collection tool provides a simple way to collect data from the Cisco Software-Defined Access (SD-Access) fabric. The tool uses a preset list of commands to connect to all selected devices, and the tool also executes those commands to bundle the outputs. The main benefit of this approach is that large amounts of information are collected from all fabric devices almost simutaneously. If a problem occurs inside the fabric, the problem may be analyzed later for the cause and solution. Because the tool automatically collects information, it provides a snapshot of the state of the fabric at that time.

Use the Fabric Data Collection Tool

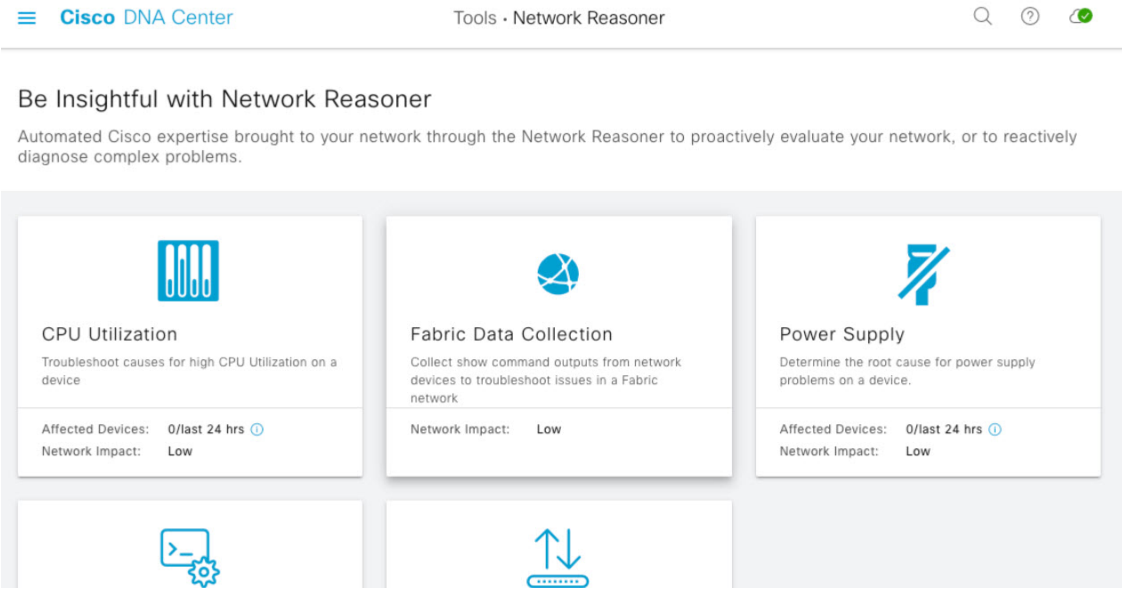
The following steps show how to use the Fabric Data Collection tool.

Procedure

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Tools** > **Network Reasoner**.



Step 2 In the **Network Reasoner** window, there is a collection of Network Reasoner tools. In the Validated Tools area, locate the Fabric Data Collection tool.



Be Insightful with Network Reasoner

Automated Cisco expertise brought to your network through the Network Reasoner to proactively evaluate your network, or to reactively diagnose complex problems.

CPU Utilization

Troubleshoot causes for high CPU Utilization on a device

Affected Devices: 0/last 24 hrs

Network Impact: Low

Fabric Data Collection

Collect show command outputs from network devices to troubleshoot issues in a Fabric network

Network Impact: Low

Power Supply

Determine the root cause for power supply problems on a device.

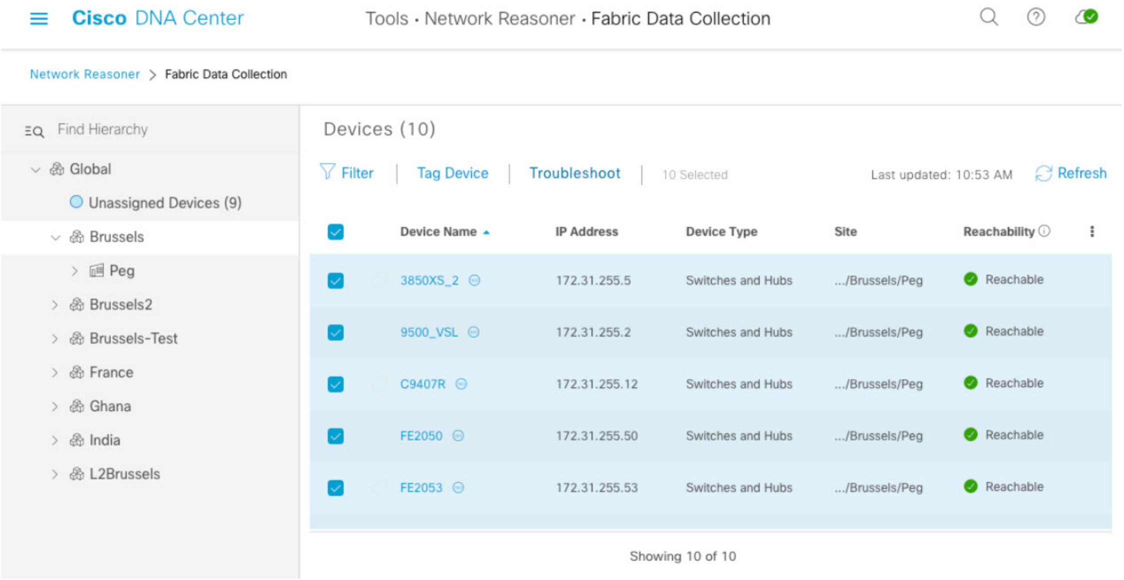
Affected Devices: 0/last 24 hrs

Network Impact: Low

Step 3 Click **Fabric Data Collection**. The **Fabric Data Collection** window appears.

Step 4 In the left pane, choose a location site and choose the devices to use for the tool.

Step 5 After you choose the site and devices, the tool activates. Click **Troubleshoot**.



Devices (10)

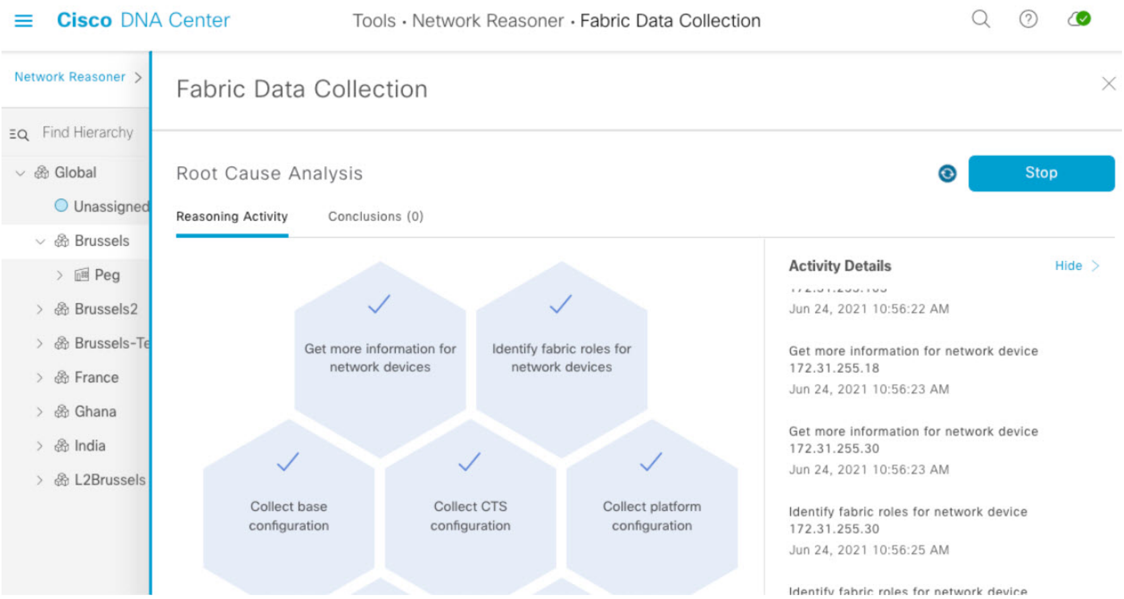
10 Selected

Last updated: 10:53 AM

☑	Device Name	IP Address	Device Type	Site	Reachability
☑	3850XS_2	172.31.255.5	Switches and Hubs	.../Brussels/Peg	✓ Reachable
☑	9500_VSL	172.31.255.2	Switches and Hubs	.../Brussels/Peg	✓ Reachable
☑	C9407R	172.31.255.12	Switches and Hubs	.../Brussels/Peg	✓ Reachable
☑	FE2050	172.31.255.50	Switches and Hubs	.../Brussels/Peg	✓ Reachable
☑	FE2053	172.31.255.53	Switches and Hubs	.../Brussels/Peg	✓ Reachable

Showing 10 of 10

Step 6 During tool activity, the tool determines the types of devices and the roles of devices in the fabric. With this information, the tool assesses which commands are being executed and which commands are not being executed on the devices. This performance allows devices to only execute commands relevant to the roles of the devices.



Jun 24, 2021 10:56:22 AM

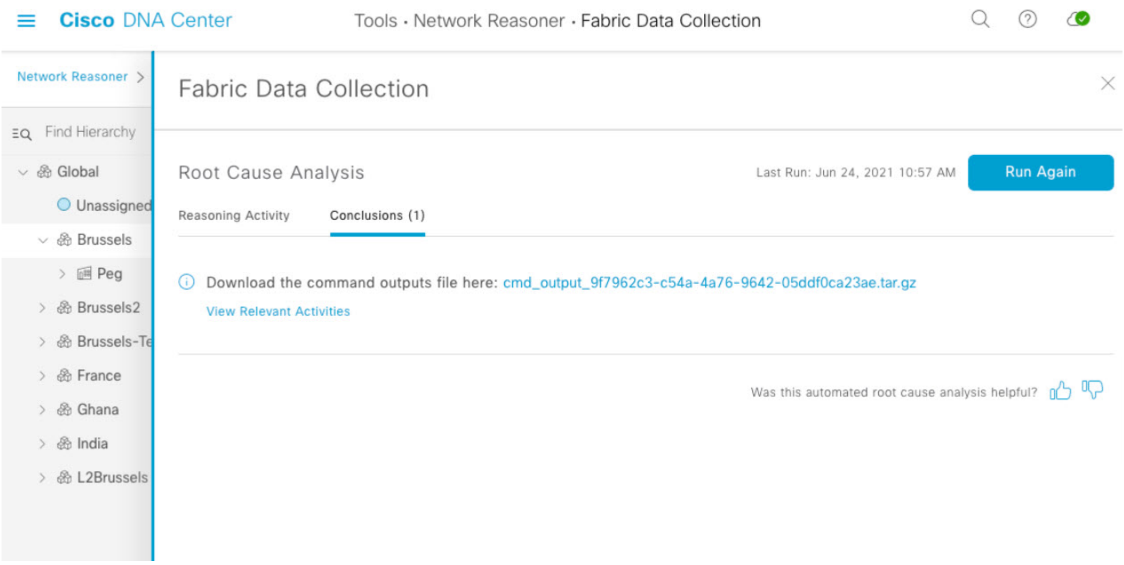
Get more information for network device 172.31.255.18
Jun 24, 2021 10:56:23 AM

Get more information for network device 172.31.255.30
Jun 24, 2021 10:56:23 AM

Identify fabric roles for network device 172.31.255.30
Jun 24, 2021 10:56:25 AM

Identify fabric roles for network device

Step 7 After the tool finishes collecting the outputs, you can find the results under the **Conclusions** tab. In the **Fabric Data Collection** window, under the Root Cause Analysis area, click the **Conclusions** tab. The other Network Reasoner tools provide the analysis of data received from the Fabric Data Collection tool. In the **Conclusions** tab, download the bundle file.



Download the command outputs file here: cmd_output_9f7962c3-c54a-4a76-9642-05ddf0ca23ae.tar.gz

Was this automated root cause analysis helpful?

Step 8 In the **Conclusions** tab, click the filename and download the file, which contains all the outputs that were collected.

Step 9 You can retrieve the bundle through various methods, such as by using the **tar** command. When the bundle files are retrieved, the **tar** command shows various .txt files that correspond to the hostnames of devices the tool ran on. These text files contain the executed commands and the outputs. These text files are normal text files.

```
########-M-K4K6:cmd_bundle ########$ tar -xzvf cmd_output_9f7962c3-c54a-4a76-9642-05ddf0ca23ae.tar.gz

x FE9200-02.txt
```

```
x FE2053.txt
x FE9404_1.txt
x FE9200-30.txt
x 9500_VSL.txt
x FE2050.txt
x 3850XS_2.txt
x FE9200-28.txt
x C9407R.txt
########-M-K4K6:cmd_bundle ########$ ls
3850XS_2.txt           FE9200-02.txt
9500_VSL.txt           FE9200-28.txt
C9407R.txt             FE9200-30.txt
FE2050.txt             FE9404_1.txt
FE2053.txt             cmd_output_9f7962c3-c54a-4a76-9642-05ddf0ca23ae.tar.gz
```

Analyze the Bundle

Inside the bundle file of every device is a text file with all the commands, which are viewable with any text editor. The commands are executed on all devices almost simutaneously. This quick process allows you to compare outputs on various devices. For example, the list map-cache on an edge device may be compared against the information from the control plane node. Because the bundle file includes information that spans across multiple features, it is able to analyze the SD-Access fabric at the time the bundle was taken. This includes information such as the Locator/ID Separation Protocol (LISP) tables, IP routing tables, authentication information, Cisco Trusted Security (CTS) information, device configurations, and various platform commands.

There are two methods of analyzing the bundle:

- Use manual analysis and compare various tables.
- Use tools, such as the SDA_Digger tool, to analyze the bundle file. This tool detects and alerts on specific events and inconsistencies. Additionally, it provides an overview of what is found during the analysis.

The following example shows SDA_Digger tool output:

```
########-M-K4K6: #########$ python3 SDA_Digger.py -b ~/cmd_bundle
Session Analysis: CP session to 3850XS_2 not present on FE9200-02
Session Analysis: CP session to 3850XS_2 not present on FE9404_1
Session Analysis: Checked LISP sessions on 8 nodes towards 2 CP nodes. Found 8 sessions, missing 2, failures
0
LISP Database Analysis: d037.4544.5f3e/48 : In LISP database on FE2050(172.31.255.50) CP node: 9500_VSL reports
 RLOC 10.48.91.173
LISP Database Analysis: d037.4544.5f3e/48 : In LISP database on FE2050(172.31.255.50) CP node: 9500_VSL reports
 RLOC 10.48.91.173
LISP Database Analysis: Number of EID checked 91, failed 1
LISP Database Analysis: Number of Local EID 29
LISP Database Analysis: Number of Devices checked 8
Map Cache Analysis : Device:FE9200-28 reporting 4099:172.28.253.1/32 with RLOC 172.31.255.2 in map-cache entry
 not present on CP nodes. Expires in 23:49:05, Uptime: 1w3d,
Map Cache Analysis : Device:FE9200-02 reporting 4099:172.28.253.1/32 with RLOC 172.31.255.2 in map-cache entry
 not present on CP nodes. Expires in 04:56:04, Uptime: 1w1d,
Map Cache Analysis : Device:9500_VSL reporting 4099:172.27.0.0/24 with RLOC 172.31.255.201 in map-cache entry
 not present on CP nodes. Expires in 05:28:49, Uptime: 1d18h,
Map Cache Analysis : Device:FE9404_1 reporting 4099:172.28.253.1/32 with RLOC 172.31.255.2 in map-cache entry
 not present on CP nodes. Expires in 23:50:19, Uptime: 1w3d,
Map Cache Analysis : Device:FE2053 reporting 4099:172.28.253.1/32 with RLOC 172.31.255.2 in map-cache entry
not present on CP nodes. Expires in 07:52:07, Uptime: 6d16h,
Map Cache Analysis : Device:FE2050 reporting 4099:172.28.253.1/32 with RLOC 172.31.255.2 in map-cache entry
not present on CP nodes. Expires in 06:12:07, Uptime: 1w0d,
Map Cache Analysis : Device:C9407R reporting 4099:172.28.253.1/32 with RLOC 172.31.255.2 in map-cache entry
```

```
not present on CP nodes. Expires in 23:50:09, Uptime: 1w3d,
Map Cache Analysis : Device:FE9200-30 reporting 4099:172.28.253.1/32 with RLOC 172.31.255.2 in map-cache entry
 not present on CP nodes. Expires in 00:00:00, Uptime: 00:00:00,
Map Cache Analysis : Found 149 entries, verified 22 entry on 8 devices with 8 failures
MTU Analysis: System MTU in fabric 9100, configured on 7 devices, misconfigured on 0 devices
Device-tracking analysis: Verified 7 edge devices with SVI info, 32 success, 0 mismatches 0 info missing
Reachability Analysis: Fabric Devices with full (/32) reachabily 8, devices without full reachability 0, not
checked 0
CTS Analysis: verified CTS on 9 nodes, 0 failures found
SVI Analysis: Device FE2050 has inconsistent Interface Vlan configuration with all other edge devices
SVI Analysis: Analyzed Interface Vlan config on 7 , found inconsistency on 1
```

The SDA_Digger tool discussed in this tech note is publically available and downloadable from https://github.com/michelpe/SDA_Digger.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.