

Mastering Troubleshooting with Cisco Catalyst Center and SD-Access

CISCO Live !

Won Je Choi
Technical Leader

Cisco Webex App

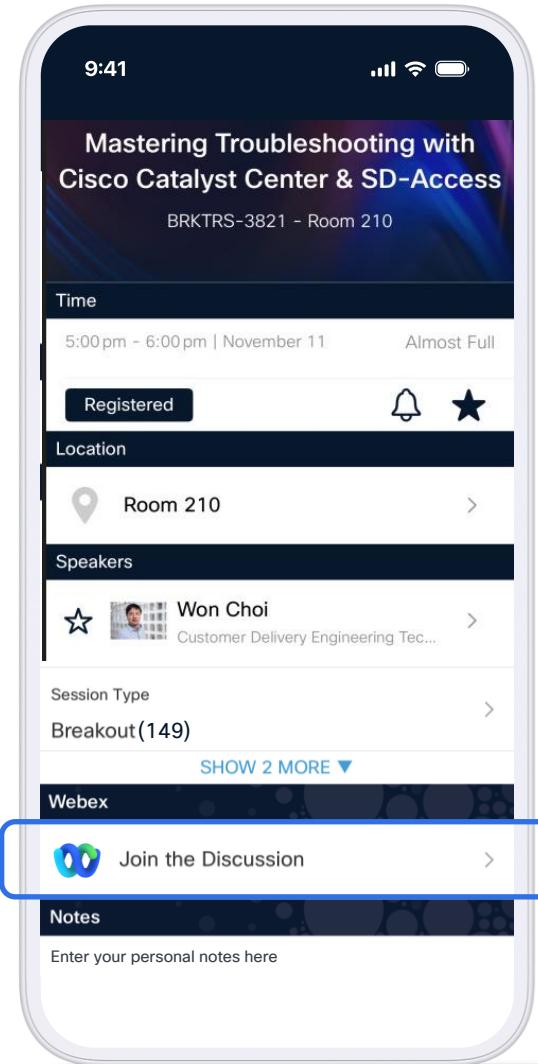
Questions?

Use Cisco Webex App to chat with the speaker after the session.

How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until 14 November 2025.





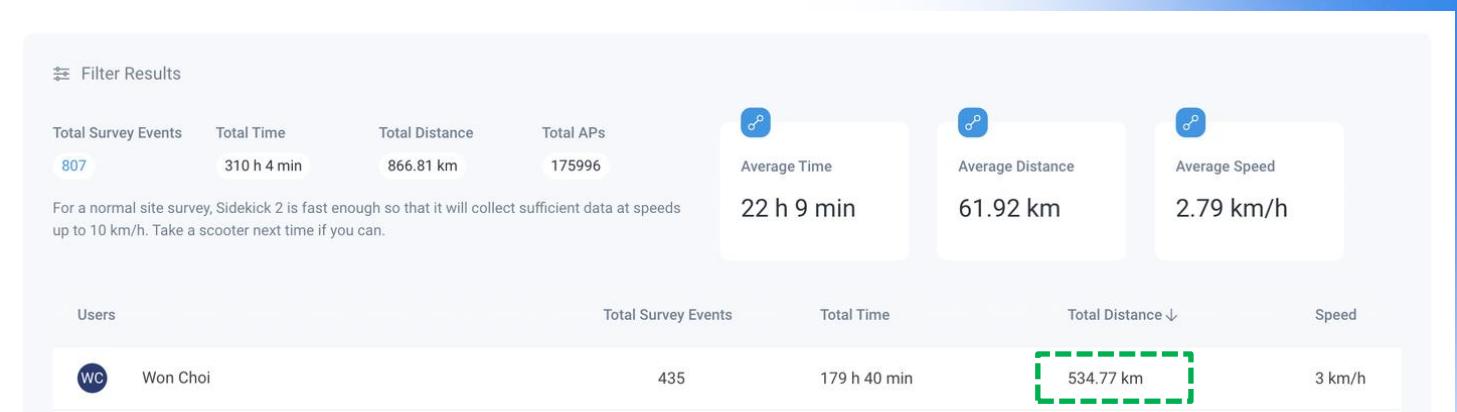
Won Je Choi

Technical Leader, Sydney TAC
CCIE #16459 (R&S)

DNAC/CatC Projects: Catalyst Center
Integration and migration for the large retail
stores in Australia and Financial institution.

Korean-Australian, Dad to 12-year-old daughter and 9-
year-old son; Home Weight Training.

Total 534Km of Ekahau Survey Distance ☺



Session Goal

Learn new techniques, tools and useful tips and tricks to further boost your troubleshooting proficiency whether you are tackling issues independently or collaborating with Cisco TAC.



Agenda

**Top 3 issues
reported by
customers
and partners.**

- 01 **Inventory use-case
(Cisco Catalyst Center)**
- 02 **Provisioning use-case
(Cisco Catalyst Center)**
- 03 **DHCP use-case
(SD-Access)**
- 04 **Additional Tool
(In Product Support Assistant
Extension)**

Introduction

Recommended Release - Cisco Catalyst Center 2.3.7.9

X

Cisco Catalyst Center

Version 2.3.7.9-70301

[Release Notes](#)

[> Packages](#)

[✓ Serial number](#)

WMP2830005D

[> Member ID](#)

© 2025 Cisco Systems Inc. All Rights Reserved.

Triaging issues using Cisco Catalyst Center Monitoring(Grafana) Tool

1. Inventory use-case

Catalyst Center: Inventory

Standard view and typical issues
(Reachability, Manageability,
Compliance)

Catalyst Center Provision / Inventory admin

Global All Routers Switches Wireless Controllers Access Points Sensors

Devices (5) Focus: Inventory Take a tour Export

Click here to apply basic or advanced filters or view recently applied filters

Tags	Device Name	IP Address	Vendor	Reachability	EoX Status	Manageability	Compliance	Site	Image Version	Last Updated
<input type="checkbox"/>	CAT9K-BORDER-01.cisco.com	172.16.0.1	Cisco	✗ Unreachable	1 alert	⚠ Managed Device Unreachable	✗ Non-Compliant	.../Krakow/KRK04	17.12.2	2 minutes ago Sync Details
<input type="checkbox"/>	CAT9K-BORDER-02.cisco.com	172.16.0.2	Cisco	✓ Reachable	1 alert	✓ Managed	✓ Compliant	.../Krakow/KRK04	17.12.2	12 hours 53 minute Sync Details
<input type="checkbox"/>	CAT9K-EDGE-01.cisco.com	172.16.0.3	Cisco	✓ Reachable	1 alert	✓ Managed	✓ Compliant	.../Krakow/KRK04	17.12.2	2 minutes ago Sync Details
<input type="checkbox"/>	CAT9K-EDGE-02.cisco.com	172.16.0.4	Cisco	⚠ Ping Reachable	1 alert	⚠ Managed SNMP Authentication Failure	✓ Compliant	.../Krakow/KRK04	17.12.2	A few seconds ago Sync Details
<input type="checkbox"/>	CAT9K-EDGE-03.cisco.com	172.16.0.5	Cisco	✓ Reachable	1 alert	✓ Managed	✓ Compliant	.../Krakow/KRK04	17.12.2	1 hour 44 minutes ago Sync Details

Catalyst Center: Inventory Troubleshooting Workflow and issue triage

1

Device Reachability



2

Manageability (Credentials)



3

Monitoring/Grafana Logs and Database Insights

- 1a) Validate reachability using “Run Commands” Tool from the Catalyst Center UI.
- 2a) Review and Validate credentials using ”Edit Device”
2b) Execute UI Inventory Re-sync operations.
2c) Execute API (force) re-sync operations.
- 3a) Check Logs and Database insights under System > System360 > Monitoring/Grafana tool.
3b) Select “Explore” to understand the query for further fine tuning.
3c) Utilise Postgres Query in Grafana to run Cisco TAC DB queries

Catalyst Center: Device Reachability

Tip #1a: Utilise the built-in Maglev “Command Runner” for Catalyst Center: Action > More > Run Commands

The screenshot illustrates the Catalyst Center interface, showing a list of devices and a Command Runner feature.

Devices (5) Focus: Inventory

- Global
- All

Devices (5) Focus: Inventory

Click here to apply basic or advanced filters or view recently applied filters

0 Selected Tag [+ Add Device](#) [Edit Device](#) [Delete Device](#)

Tags	Device Name	IP Address
<input type="checkbox"/>	CAT9K-BORDER-01.cisco.com	172.16.0.1
<input type="checkbox"/>	CAT9K-BORDER-02.cisco.com	172.16.0.2
<input type="checkbox"/>	CAT9K-EDGE-01.cisco.com	172.16.0.3
<input type="checkbox"/>	CAT9K-EDGE-02.cisco.com	172.16.0.4
<input type="checkbox"/>	CAT9K-EDGE-03.cisco.com	172.16.0.5

Actions [Actions](#) [More](#)

Inventory

Software Image

Provision

Telemetry

Device Replacement

Switch Refresh

Compliance

More

Run Commands

Command Runner

Learn Device Config

CTRL+E - Exports the current command history as a text file
CTRL+F - Search within the window for a keyword/phrase

Command Runner

4

\$ man
This lists the commands currently supported by command runner:
man ---- Get the list of currently supported commands

connect ---- Connect to a device using hostname or ip address. For IPv6 address, enter at least one group/hextet from the address, ex - debd:
Usage: connect <device_ip> or connect <hostname>

ping ---- Usage: ping [-LRUbfdnqrVAB] [-c count] [-i interval] [-l preload] [-p pattern] [-s packetsize] [-t ttl] [-w deadline] [-F flowlabel] [-I interface] [-M hint] [-Q tos] [-S sndbuf] [-T timestamp option] [-W timeout] [hop ...] destination

traceroute ---- Usage: traceroute ip {{ip4-address | hostname}} [size packet_size] [ttl max-ttl] [count packet_count] [timeout time_out] [source ip-address]

snmpget ---- Usage: snmpget is used to retrieve data from a remote host using its host name, authentication information and an OID. Example: snmpget -v 1 -c democisco test.net-snmp.org system.sysUpTime.0 (where, system.sysUpTime.0 = Timeticks: (586731977) 67 days, 21:48:39.77)
In the above example, test.net-snmp.org is the host name we wanted to talk to, using the SNMP community string democisco and we requested the value of the OID system.sysUpTime.0

CTRL+E - Exports the current command history as a text file
CTRL+F - Search within the window for a keyword/phrase

\$

1 alert Managed Compliant .../Krakow/KRK04 17.12.2 12 minutes ago Sync Details

2 Managed Compliant .../Krakow/KRK04 17.12.2 3 minutes ago Sync Details

3 Managed

4

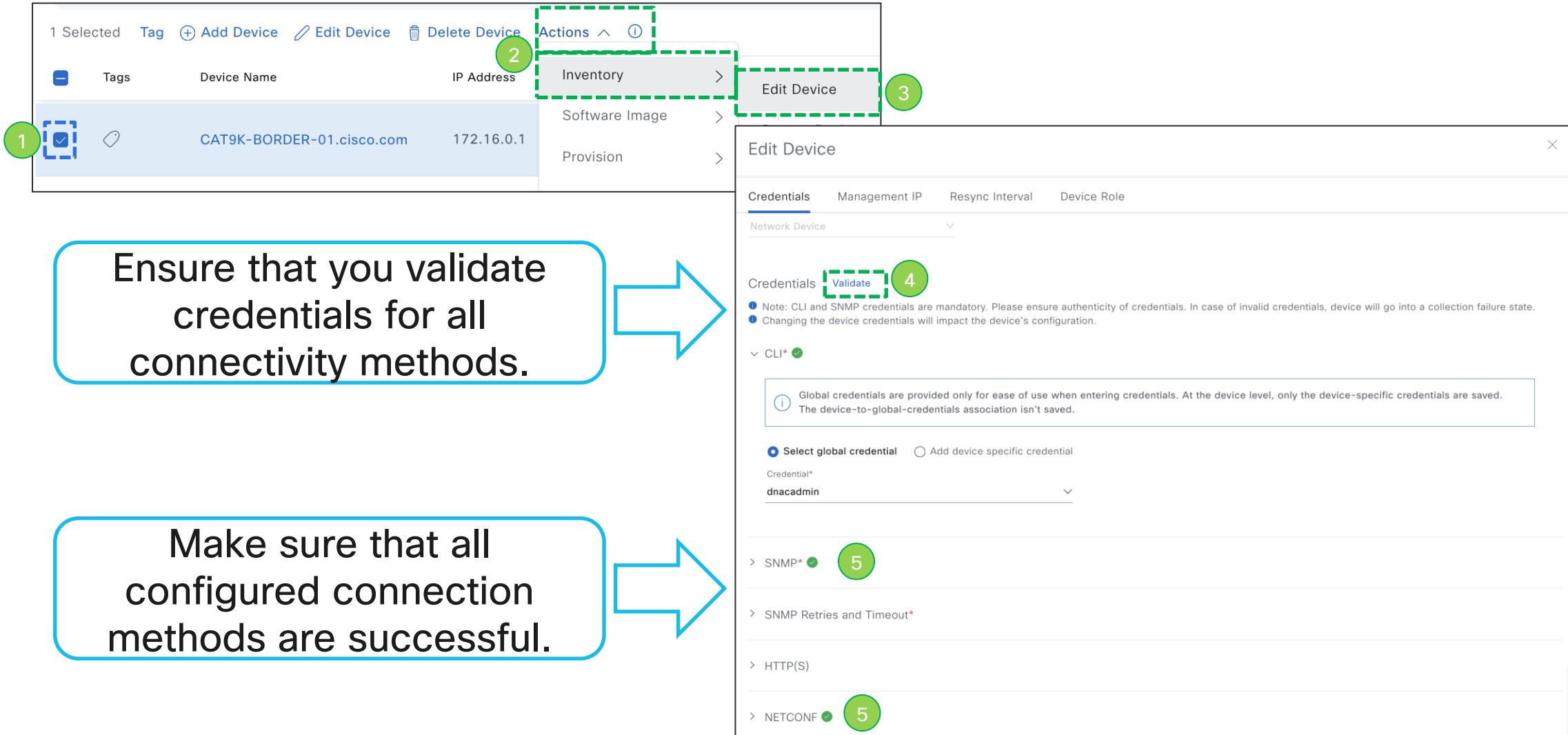
Basic checks (Maglev CLI) are available directly from Catalyst Center

Ping, Traceroute, SNMP, connect

Basic checks (Maglev CLI) are available directly from Catalyst Center UI:
Ping, Traceroute, SNMP, connect

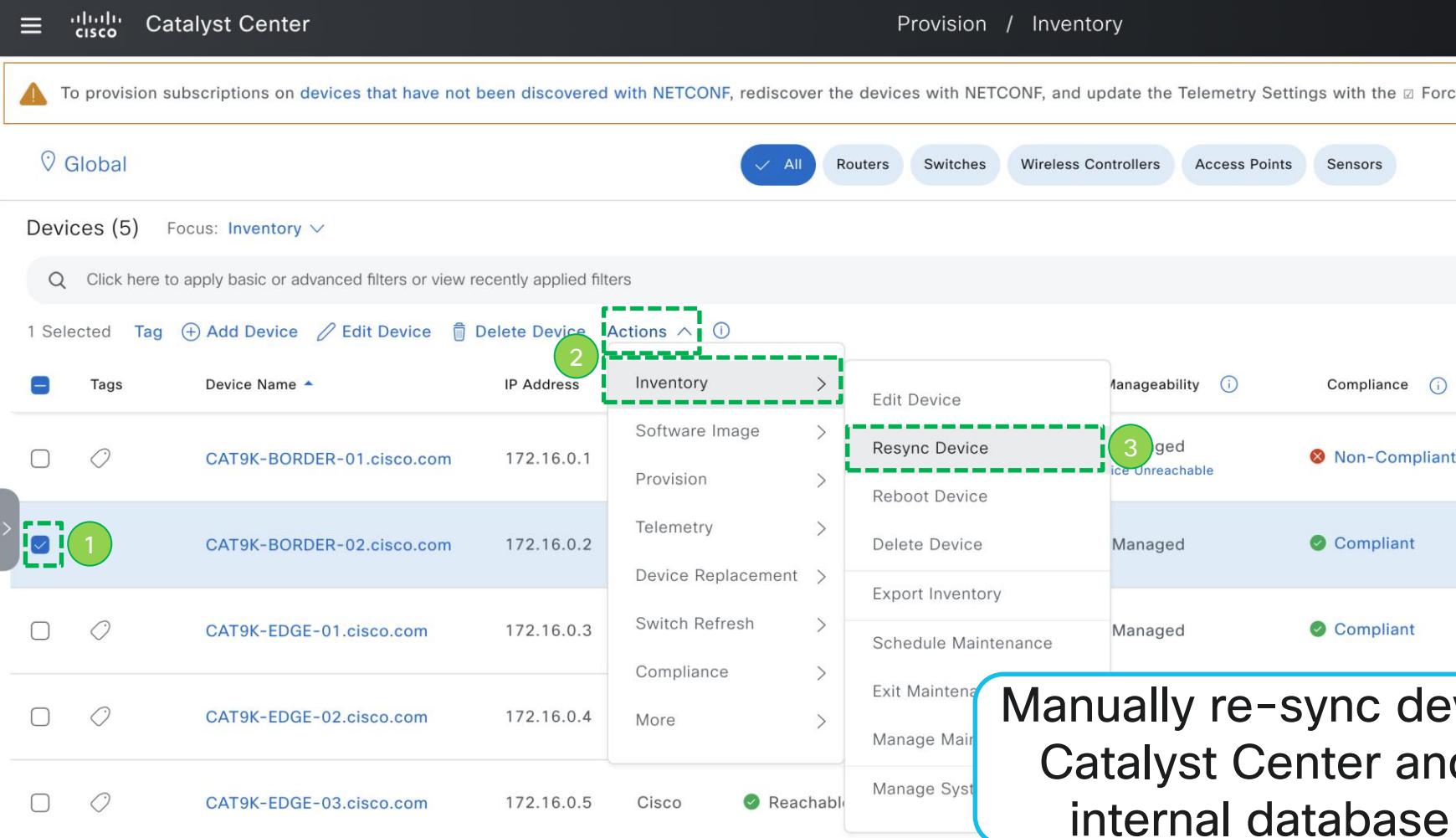
Catalyst Center: Manageability

Tip #2a: Validate (and correct) credentials: Actions > Inventory > Edit Devices



Catalyst Center: Manageability

Tip #2b: Re-sync device to get the latest details: Actions > Inventory > Resync Device



The screenshot shows the Catalyst Center interface with the following details:

- Header:** Catalyst Center, Provision / Inventory
- Alert:** To provision subscriptions on devices that have not been discovered with NETCONF, rediscover the devices with NETCONF, and update the Telemetry Settings with the Force
- Filter:** Global, Focus: Inventory
- Devices:** Devices (5) - CAT9K-BORDER-01.cisco.com, CAT9K-BORDER-02.cisco.com, CAT9K-EDGE-01.cisco.com, CAT9K-EDGE-02.cisco.com, CAT9K-EDGE-03.cisco.com
- Actions Menu:** A context menu is open for the selected device (CAT9K-BORDER-02.cisco.com). The menu is organized into sections: Inventory, Provision, Telemetry, Device Replacement, Compliance, and More. The 'Inventory' section is highlighted with a green dashed box and a green circle with the number 2. The 'Resync Device' option under the 'Inventory' section is highlighted with a green dashed box and a green circle with the number 3.
- Device Details:** The selected device (CAT9K-BORDER-02.cisco.com) is shown with the following details:
 - Tags: None
 - Device Name: CAT9K-BORDER-02.cisco.com
 - IP Address: 172.16.0.2
 - Manageability: Managed (green checkmark)
 - Compliance: Non-Compliant (red X)
- Callout:** A blue callout box with a rounded corner contains the text: "Manually re-sync device to update Catalyst Center and repopulate internal database structures."

Catalyst Center: Manageability – Device re-sync progress

The screenshot shows the Catalyst Center interface with the following details:

- Header:** Catalyst Center, Provision / Inventory, admin
- Global Filter:** Global, All (selected), Routers, Switches, Wireless Controllers, Access Points, Sensors
- Devices (5):** Focus: Inventory
- Actions:** Take a tour, Export, Settings
- Table Headers:** Tags, Device Name, IP Address, Vendor, Reachability, EoX Status, Manageability, Compliance, Site, Image Version, Last Updated
- Device Data:**
 - CAT9K-BORDER-01.cisco.com: IP 172.16.0.1, Cisco, Unreachable, 1 alert, Managed, Non-Compliant, Sync Details (37 minutes ago)
 - CAT9K-BORDER-02.cisco.com: IP 172.16.0.2, Cisco, Pending Sync (2 pending), Managed, Compliant, Sync Details (13 hours 40 minutes ago)
 - CAT9K-EDGE-01.cisco.com: IP 172.16.0.3, Cisco, Pending Sync (1 pending), Managed, Compliant, Sync Details (42 minutes ago)
 - CAT9K-EDGE-02.cisco.com: IP 172.16.0.4, Cisco, Pending Sync (1 pending), Managed, Syncing..., Compliant, Sync Details (22 minutes ago)
 - CAT9K-EDGE-03.cisco.com: IP 172.16.0.5, Cisco, Pending Sync (1 pending), Managed, Compliant, Sync Details (2 hours 31 minutes ago)

A callout box highlights the second device (CAT9K-BORDER-02.cisco.com) with the text: "Check re-sync status to get high-level information about its progress." The box also shows the "Resync request(s) pending in queue" status and the "Ongoing Sync Details" for the device.

Catalyst Center: Manageability

Tip #2c: Force re-sync device (available only via API; might be requested by Cisco TAC): Developer Toolkit > Sync Devices API

The screenshot shows the Catalyst Center interface with the Developer Toolkit selected. A callout box highlights the 'Sync Devices' API endpoint with the following text:

Force re-sync to assign sync task to a high priority thread.

Key elements highlighted with green boxes and numbered circles:

- 1: Platform menu (dashed box)
- 2: Developer Toolkit menu (dashed box)
- 3: Search bar with 'sync device' (dashed box)
- 4: Sync Devices API endpoint (dashed box)

Other visible text and elements:

- Platform / Developer Toolkit
- Runtime Dashboard
- capabilities and try them out for yourself
- or test different APIs in your network environment to build,...
- Know Your Network
- Devices
- Method: PUT
- Name: Sync Devices
- Description: Synchronizes the device (default) then the sync v... If forceSync param is true, the sync task will be run on a high priority thread if available. The progress of the sync task can be seen in the child task of each device.

Catalyst Center: Manageability - force re-sync via API

Sync Devices

PUT

<https://10.62.149.204/dna/intent/api/v1/network-device-sync>

Synchronizes the devices. If forceSync param is false (default) then the sync would run in normal priority thread. If forceSync param is true then the sync would run in high priority thread if available, else the sync will fail. Result can be seen in the child task of each device

[Cisco DevNet API Guide](#)

Parameter 1

Request Body

Responses

Code Preview

Request Headers

Name

Content-Type

Request Query

List of id's in the format ["DeviceId1", "DeviceId2"]

Schema

Sample

```
1: [  
2:   "string"  
3: ]
```

Name	Description	DataType	Required	Default Value
2 forceSync	forceSync	boolean	No	false

Note: forceSync API requires internal device ID to run (not the IP address, hostname, or UUID). The simplest way to obtain it is through Grafana (refer to the next slides).

Catalyst Center: Manageability - force re-sync via API

Try 'Sync Devices'

Method: **PUT** Public URL :<https://10.62.149.204/dna/intent/api/v1/network-device-sync>

PARAMETERS

HEADERS

Content-Type* [i](#)

QUERY PARAMETERS

Unselect All
 forceSync
true

REQUEST BODY

2  Device ID

Rese

Run

Response Headers Status Code: 202

```
1 3 "response": {  
2     "taskId": "01942678-e9a9-76ff-9cea-65fa48a976eb",  
3     "url": "/api/v1/task/01942678-e9a9-76ff-9cea-65fa48a976eb"  
4   },  
5   "version": "1.0"  
6 }
```

Details (taskId/url) of the asynchronous re-sync task that has been created for re-sync

Catalyst Center: Manageability - force re-sync via API

Try 'Get task details by ID' 1

Method: GET Public URL :https://10.62.149.204/dna/intent/api/v1/tasks/01942678-e9a9-76ff-9cea-65fa48a976eb/detail

PARAMETERS

PATH PARAMETERS 2

01942678-e9a9-76ff-9c

Response Headers Status Code: 200

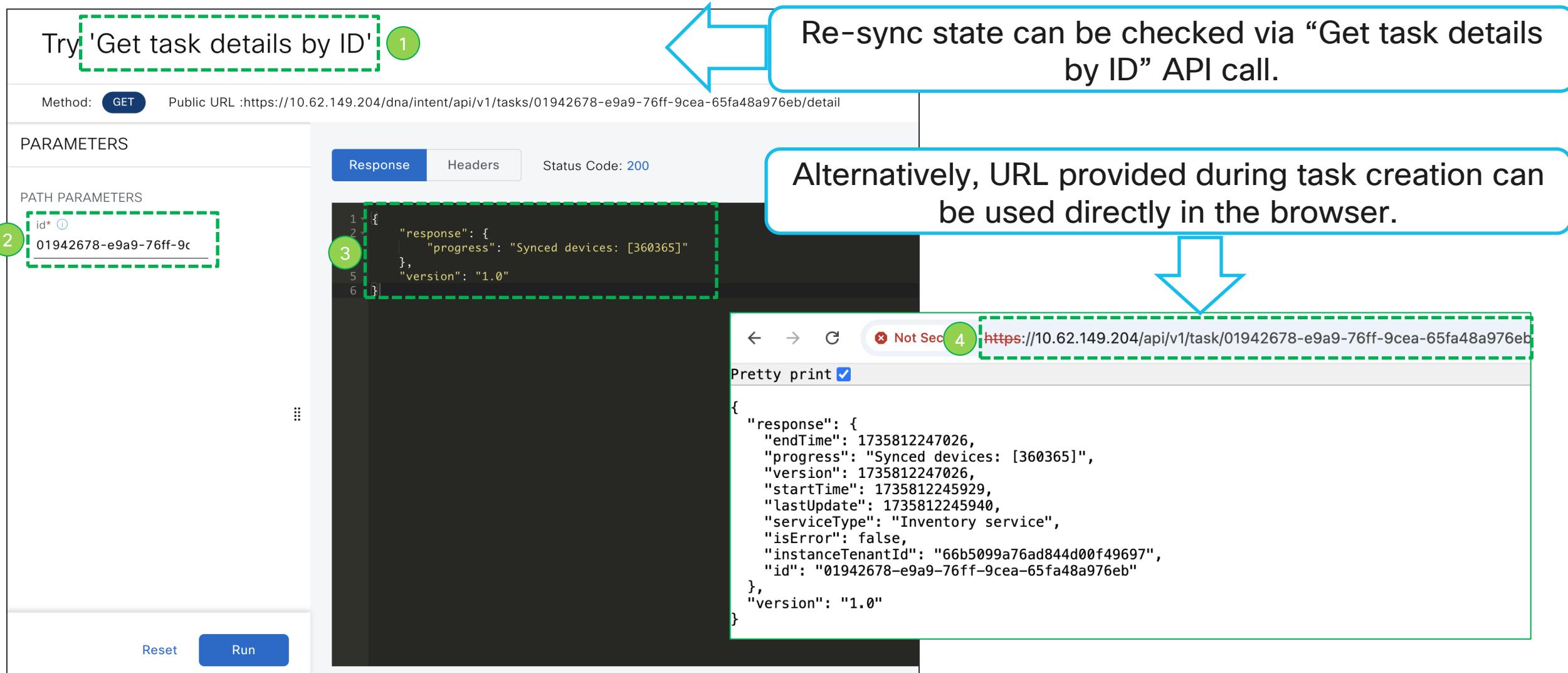
1 {
2 "response": {
3 "progress": "Synced devices: [360365]"
4 },
5 "version": "1.0"
6 }

Re-sync state can be checked via "Get task details by ID" API call.

Alternatively, URL provided during task creation can be used directly in the browser.

4 https://10.62.149.204/api/v1/task/01942678-e9a9-76ff-9cea-65fa48a976eb

Reset Run



The screenshot shows the Catalyst Center API interface. A green box labeled '1' highlights the 'Try 'Get task details by ID'' button. Below it, the 'Method: GET' and 'Public URL' are shown. A green box labeled '2' highlights the 'id' path parameter with the value '01942678-e9a9-76ff-9c'. The 'Response' tab is selected, showing a status code of 200. The response body is a JSON object with fields 'response' and 'version'. The 'response' field contains 'progress' (Synced devices: [360365]) and 'version' (1.0). A green box labeled '3' highlights the 'progress' field. A blue callout box labeled 'Re-sync state can be checked via "Get task details by ID" API call.' points to the 'Get task details by ID' button. Another blue callout box labeled 'Alternatively, URL provided during task creation can be used directly in the browser.' points to a browser window showing the task URL 'https://10.62.149.204/api/v1/task/01942678-e9a9-76ff-9cea-65fa48a976eb'. The browser window also shows the JSON response with the same structure as the API interface.

Catalyst Center: Logs and Database Insights (Grafana)

Tip #3a: Utilise Catalyst Center Monitoring dashboards in Grafana: **System > System 360 > Monitoring**

The screenshot shows the Catalyst Center interface. The left sidebar has a 'System' section (1) with a green dashed box around it. The 'System 360' section (2) is also highlighted with a green dashed box. The main content area shows two cards: 'High Availability' (As of Jan 2, 2025 10:11 AM) and 'Cluster Tools' (As of Jan 2, 2025 10:09 AM). The 'Cluster Tools' card (3) has a 'Monitoring' section highlighted with a green dashed box. The top navigation bar shows 'System / System 360' and the user 'admin'.

Catalyst Center provides advanced monitoring capabilities through 3rd party tool: Grafana

Catalyst Center: Logs and Database Insights (Grafana)

1 Search dashboards

2 Inventory

Multiple dashboards are available for a variety of Catalyst Center services.

Dedicated 'Inventory' dashboard is available, simplifying the analysis of internal logs and structures.

Postgres Queries can be also executed here as instructed by Cisco TAC.

© 2025 Cisco and/or its affiliates. All rights reserved.

BRKTRS-3821

Catalyst Center: Logs and Database Insights (Grafana)

Select the device to troubleshoot.

Get device-id (for force re-sync, etc.)

Validate device values (serial number, hostname, etc.)

The screenshot shows the 'General / Inventory' section of the Catalyst Center. At the top, there are input fields for 'Device IP' (172.16.0.1) and 'Device Id' (360361), both highlighted with a green dashed box and a circled '1'. A blue callout points to these fields with the text 'Select the device to troubleshoot.' and 'Get device-id (for force re-sync, etc.)'. Below these fields is a table with columns: id, hostname, type, collectionstatus, reachabilitystatus, inventorystatusdetail, errorcode, devicesupportlevel, collectioninterval, serialnumber, and lastupdatetime. A row for device 360361 is selected, showing values: CAT9K-BORDE..., Cisco Catalyst C9500-24Y4..., Managed, Reachable, <status><general code="SU..., Supported, Global Default, CAT2345L1PC, 2025-01-02 07:57:22. A green dashed box highlights this row. In the 'Basic Stats' section, there are three cards: 'Devices' (Family: Switches and Hubs, Total: 5), 'Life Cycle State' (Life Cycle State: 3, Total: 5), and 'Inventory Status Detail' (Status Detail: 3001-4000, Total: 3; 4001-5000, Total: 0). A blue callout points to the 'Inventory Status Detail' card with the text 'Validate device values (serial number, hostname, etc.)'. At the bottom, there is a 'Device Operations' chart with a single data series: 'apic-em-inventory-manager-service-6c9b9fc747-mjhwd (Manual Sync)'.

id	hostname	type	collectionstatus	reachabilitystatus	inventorystatusdetail	errorcode	devicesupportlevel	collectioninterval	serialnumber	lastupdatetime
360361	CAT9K-BORDE...	Cisco Catalyst C9500-24Y4...	Managed	Reachable	<status><general code="SU...	Supported	Global Default	CAT2345L1PC	2025-01-02 07:57:22	

General / Inventory

Log Pattern Enter variable value Log Level A Device IP 172.16.0.1 Device Id 360361 1

id hostname type collectionstatus reachabilitystatus inventorystatusdetail errorcode devicesupportlevel collectioninterval serialnumber lastupdatetime

360361 CAT9K-BORDE... Cisco Catalyst C9500-24Y4... Managed Reachable <status><general code="SU... Supported Global Default CAT2345L1PC 2025-01-02 07:57:22

Basic Stats

Devices

Family	Total
Switches and Hubs	5

Life Cycle State

Life Cycle State	Total
3	5

Inventory Status Detail

Status Detail	Total
3001-4000	3
4001-5000	0

GRT Size

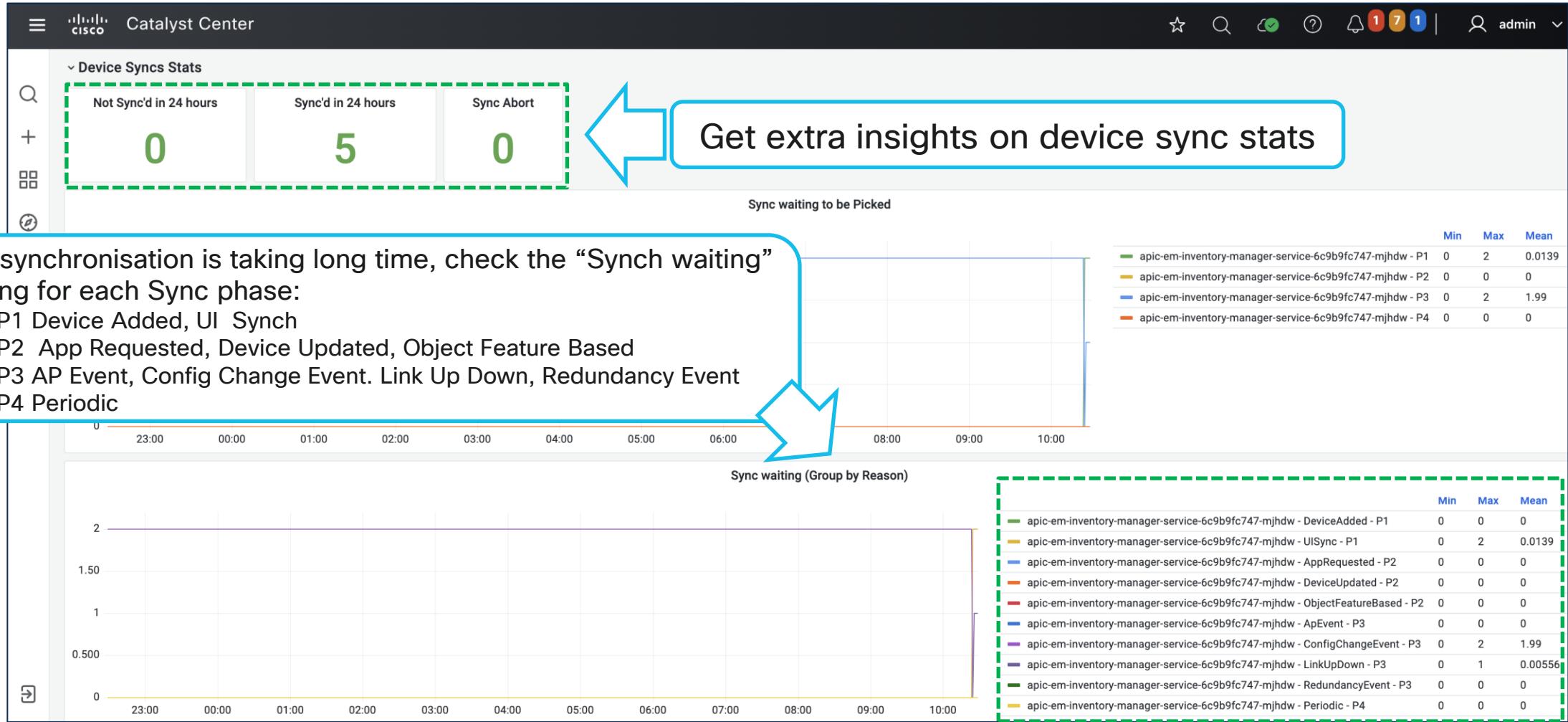
Interfaces

Stats

Device Operations

apic-em-inventory-manager-service-6c9b9fc747-mjhwd (Manual Sync)

Catalyst Center: Logs and Database Insights (Grafana)



Catalyst Center: Logs and Database Insights (Grafana)

The screenshot shows the Catalyst Center Grafana dashboard with two main log panels for device 360361 (172.16.0.1).

Key logs - 360361 (172.16.0.1) (1 panel):

Check key logs for a given device.

Specify time range.

All Logs - 360361 (172.16.0.1) (1 panel):

Check all logs for a given device.

Log entries (extracted from the panels):

Key logs - 360361 (172.16.0.1) Log Entries:

```
> 2025-01-02 06:57:22,085 | INFO | ICE Service - CPU 5 | com.cisco.xmp.inventory | Done with collection. Is tiered:true For Tier:STANDALONE Total call method time: 1619 Feature time: 16 Hook time: 0 Persistence time: 0 | com.cisco.xmp.inventory | For deviceid:360361, statusMessage:<status><general code="SUCCESS"/></status>, successLifeEnum:MANAGED_AND_SYNCHRONIZED | mid=2, MSGNAME=XICE_GENERIC_MSG_INF_02, ch=com.cisco.xmp.inventory, sev=informational
> 2025-01-02 06:57:22,085 | INFO | ICE Service - CPU 5 | com.cisco.xmp.inventory | Interim status after execution of devicePackage SUCCESS deviceId: 360361; CredentialId: 360361; ManagementIP: 172.16.0.1 | mid=2, MSGNAME=XICE_GENERIC_MSG_INF_02, ch=com.cisco.xmp.inventory, sev=informational
> 2025-01-02 06:57:21,222 | INFO | ICE Service - Network 9 | com.cisco.xmp.inventory | getDeviceSize for deviceId: 360361 got result map as: {wirelesspoints=0, protocolendpoints=34, configLines=616} | mid=2, MSGNAME=XICE_GENERIC_MSG_INF_02, ch=com.cisco.xmp.inventory, sev=informational
> 2025-01-02 06:57:20,568 | INFO | XDE ThreadPool 2 | com.cisco.xmp.inventory | 360361: Previous collection status MANAGED_AND_SYNCHRONIZED | mid=2, MSGNAME=XICE_GENERIC_MSG_INF_02, ch=com.cisco.xmp.inventory, sev=informational
> 2025-01-02 06:57:19,955 | INFO | ICE Service - Network 9 | com.cisco.xmp.inventory | For deviceid:360361, statusMessage:<status><general code="SUCCESS"/></status>, successLifeEnum:MANAGED_AND_SYNCHRONIZED | mid=2, MSGNAME=XICE_GENERIC_MSG_INF_02, ch=com.cisco.xmp.inventory, sev=informational
> 2025-01-02 06:57:19,518 | INFO | ICE Service - CPU 1 | com.cisco.xmp.inventory | 360361: Previous collection status MANAGED_AND_SYNCHRONIZED | mid=2, MSGNAME=XICE_GENERIC_MSG_INF_02, ch=com.cisco.xmp.inventory, sev=informational
> 2025-01-02 06:57:19,518 | INFO | ICE Service - CPU 1 | com.cisco.xmp.inventory | Done with collection. Is tiered:true For Tier:OPTIONAL Total call method time: 1619 Feature time: 16 Hook time: 0 Persistence time: 0 | com.cisco.xmp.inventory | For deviceid:360361, statusMessage:<status><general code="SUCCESS"/></status>, successLifeEnum:MANAGED_AND_SYNCHRONIZED | mid=2, MSGNAME=XICE_GENERIC_MSG_INF_02, ch=com.cisco.xmp.inventory, sev=informational
> 2025-01-02 06:57:18,721 | INFO | ICE Service - Network 7 | com.cisco.xmp.inventory | Interim status after execution of devicePackage SUCCESS deviceId: 360361; CredentialId: 360361; ManagementIP: 172.16.0.1 | mid=2, MSGNAME=XICE_GENERIC_MSG_INF_02, ch=com.cisco.xmp.inventory, sev=informational
> 2025-01-02 06:57:18,463 | INFO | XDE ThreadPool 4 | com.cisco.xmp.inventory | getDeviceSize for deviceId: 360361 got result map as: {wirelesspoints=0, protocolendpoints=34, configLines=616} | mid=2, MSGNAME=XICE_GENERIC_MSG_INF_02, ch=com.cisco.xmp.inventory, sev=informational
> 2025-01-02 06:57:17,776 | INFO | ICE Service - Network 12 | com.cisco.xmp.inventory | 360361: Previous collection status MANAGED_AND_SYNCHRONIZED | mid=2, MSGNAME=XICE_GENERIC_MSG_INF_02, ch=com.cisco.xmp.inventory, sev=informational
```

All Logs - 360361 (172.16.0.1) Log Entries:

```
> 2025-01-02 06:57:22,446 | INFO | ICE Service - CPU 5 | com.cisco.xmp.inventory | Discard all orphaned objects for device 360361 | mid=2, MSGNAME=XICE_GENERIC_MSG_INF_02, ch=com.cisco.xmp.inventory, sev=informational
> 2025-01-02 06:57:22,435 | INFO | ICE Service - CPU 5 | com.cisco.xmp.inventory | 360361 : No new collection request | mid=2, MSGNAME=XICE_GENERIC_MSG_INF_02, ch=com.cisco.xmp.inventory, sev=informational
> 2025-01-02 06:57:22,433 | INFO | ICE Service - CPU 5 | com.cisco.xmp.inventory | Removing from syncing set 360361 360361 | mid=2, MSGNAME=XICE_GENERIC_MSG_INF_02, ch=com.cisco.xmp.inventory, sev=informational
> 2025-01-02 06:57:22,429 | INFO | ICE Service - CPU 5 | com.cisco.xmp.inventory | 360361 : Looking for any queued sync tasks | mid=2, MSGNAME=XICE_GENERIC_MSG_INF_02, ch=com.cisco.xmp.inventory, sev=informational
> 2025-01-02 06:57:22,421 | INFO | ICE Service - CPU 5 | com.cisco.xmp.inventory | Complete inventory com.cisco.enc.inventory.policy.ExtendedInventoryCollectionPolicy@5a739a6f for deviceid 360361 at Thu Jan 02 06:57:22 GMT 2025. Total time taken to collect inventory in milliseconds = 2484 | mid=2, MSGNAME=XICE_GENERIC_MSG_INF_02, ch=com.cisco.xmp.inventory, sev=informational
> 2025-01-02 06:57:22,420 | INFO | ICE Service - CPU 5 | com.cisco.xmp.inventory | 360361 Successfully Updated the Granular Status for the operationType:SYNC_OPERATION_INDEPENDENT | mid=2, MSGNAME=XICE_GENERIC_MSG_INF_02, ch=com.cisco.xmp.inventory, sev=informational
> 2025-01-02 06:57:22,418 | INFO | ICE Service - CPU 5 | com.cisco.xmp.inventory | Going to fetch the meId:360361 with operationType:SYNC_OPERATION_INDEPENDENT | mid=2, MSGNAME=XICE_GENERIC_MSG_INF_02, ch=com.cisco.xmp.inventory, sev=informational
> 2025-01-02 06:57:22,409 | INFO | ICE Service - CPU 5 | com.cisco.xmp.inventory | Device id 360361 Time taken in milliseconds to invoke post collection notifier hook com.cisco.enc.prime_inventory.hooks.PostCollectionBaseRadioCleanupHook: 10 | MSGNAME=XICE_GENERIC_MSG_INF_02, ch=com.cisco.xmp.inventory, sev=informational, mid=2
> 2025-01-02 06:57:22,409 | INFO | ICE Service - CPU 5 | c.c.e.p.h.PostCollectionBaseRadioCleanupHook | PostCollectionBaseRadioCleanupHook for device id 360361 ends |
```

Catalyst Center: Logs and Database Insights (Grafana)

General / Inventory

1

Log Pattern: Enter variable value

Log Level: Enter variable value

Device IP: 172.16.0.1

Device Id: 360361

Selected (2): All, ERROR, WARN

reachabilitystatus: Reachable

inventorystatusdetail: <status><general code="SU...

Basic Stats

id	hostname	type
360361	CAT9K-BORDE...	Cisco Catalyst C9500-24

Filter logs further based on severity.

Key logs - 360361 (172.16.0.1)

172.16.0.1 - logs

- View
- Edit
- Share
- Explore
- Inspect
- More...
- Remove

2

ERROR + WARN Logs

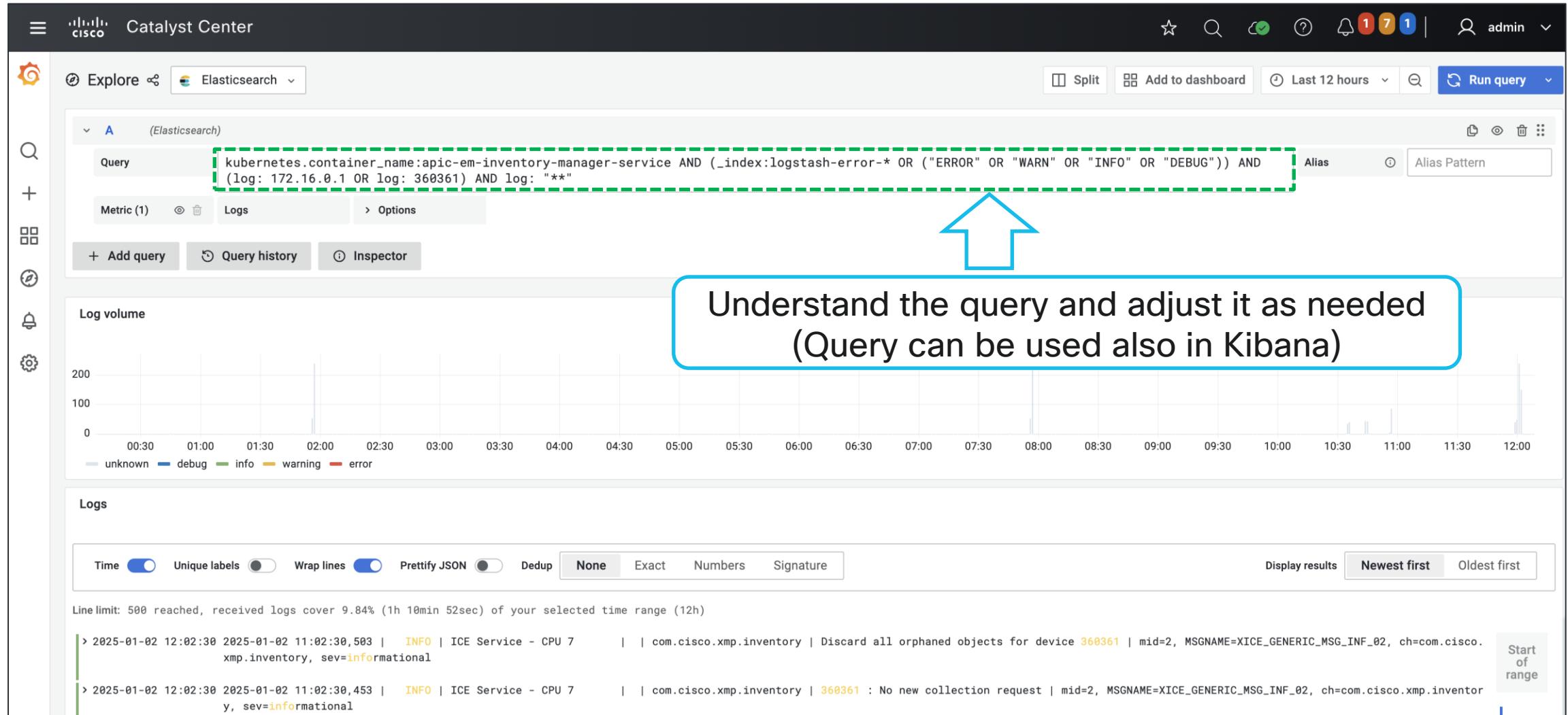
Device packs Execution Time - 360361 (172.16.0.1) (1 panel)

All Logs - 360361 (172.16.0.1)

```
> 2025-01-02 06:56:28,800 | ERROR | ICE Service - Network 1 | com.cisco.xmp.inventory | Exception occurred while updating the privilege level for the device 360361 message :errorId=8 Invalid credential name: PRIVILEGE_LEVEL | mid=1, MSGNAME=XICE_GENERIC_MSG_ERR_01, ch=com.cisco.xmp.inventory, sev=error
> 2025-01-02 00:56:31,790 | ERROR | ICE Service - Network 7 | com.cisco.xmp.inventory | Exception occurred while updating the privilege level for the device 360361 message :errorId=8 Invalid credential name: PRIVILEGE_LEVEL | mid=1, MSGNAME=XICE_GENERIC_MSG_ERR_01, ch=com.cisco.xmp.inventory, sev=error
```

Explore all logs further for a given device

Catalyst Center: Logs and Database Insights (Grafana)



The screenshot shows the Catalyst Center interface for monitoring logs and databases using Elasticsearch. The top navigation bar includes the Cisco logo, the title 'Catalyst Center', and user authentication for 'admin'. The main search bar is set to 'Elasticsearch' and contains a query: `kubernetes.container_name:apic-em-inventory-manager-service AND (_index:logstash-error-* OR ("ERROR" OR "WARN" OR "INFO" OR "DEBUG")) AND (log: 172.16.0.1 OR log: 360361) AND log: "**"`. A large blue callout box with a blue arrow points from the text 'Understand the query and adjust it as needed (Query can be used also in Kibana)' to the query input field. Below the search bar is a 'Log volume' chart showing the count of logs over time, with a legend for log levels: unknown (light blue), debug (dark blue), info (green), warning (orange), and error (red). The chart shows several spikes in log volume, notably around 02:00, 07:30, 08:00, and 12:00. The 'Logs' section below the chart displays log entries in a table format, with options for filtering by time, labels, and pretty JSON. The log entries shown are:

Time	Level	Message
2025-01-02 12:02:30	INFO	ICE Service - CPU 7 com.cisco.xmp.inventory Discard all orphaned objects for device 360361 mid=2, MSGNAME=XICE_GENERIC_MSG_INF_02, ch=com.cisco.xmp.inventory, sev=informational
2025-01-02 12:02:30	INFO	ICE Service - CPU 7 com.cisco.xmp.inventory 360361 : No new collection request mid=2, MSGNAME=XICE_GENERIC_MSG_INF_02, ch=com.cisco.xmp.inventory, sev=informational

A 'Start of range' button is visible on the right side of the log table. The bottom of the interface includes a copyright notice for Cisco and a page number 'BRKTRS-3821'.

Understand the query and adjust it as needed
(Query can be used also in Kibana)

```
kubernetes.container_name:apic-em-inventory-manager-service AND (_index:logstash-error-* OR ("ERROR" OR "WARN" OR "INFO" OR "DEBUG")) AND (log: 172.16.0.1 OR log: 360361) AND log: "**"
```

Catalyst Center: Logs and Database Insights (Grafana)

Tip #3b: Utilise access to Postgres Query in Grafana to run Cisco TAC queries.

The screenshot shows the Catalyst Center interface with the following steps highlighted:

- Specify DB query (as provided by Cisco TAC)**: A callout points to the query input field in the top-left corner, which contains the SQL command: `select * from networkd`.
- Query Output**: A context menu is open over the table, with the "Inspect" option highlighted.
- Inspect: Query Output**: A modal window titled "Inspect: Query Output" is displayed, showing the results of the query. The "Data" tab is selected, displaying a table with the following data:

	<code>id</code>	<code>instanceuuid</code>	<code>hostname</code>	<code>managementip</code>	<code>type</code>	<code>family</code>	<code>series</code>	<code>size</code>
360361	f9bf3ac4-5916-4f83...	CAT9K-BORDER-01...	172.16.0.1	Cisco Catalyst C95...	Switches and Hubs	Cisco Catalyst 9500...	17.12	

Triaging issues using Cisco Catalyst Center with Monitoring(Grafana) Tool

- 1. Check the basics:** Confirm reachability and manageability for all configured access methods.
- 2. Use Monitoring(Grafana) dashboards:** Leverage pre-configured Inventory dashboards for extra visibility on the state of the system.
- 3. DB Queries:** Use Postgres Query Dashlet to effectively run and collect data required by Cisco TAC.
- 4. Grafana Capabilities:** Refer to the official Grafana documentation to understand its key features and capabilities. <https://grafana.com/docs/>

Triaging issues using Cisco Catalyst Center with Log Explorer(Kibana)

#2 Provisioning Use-Case

Catalyst Center: Provisioning workflow

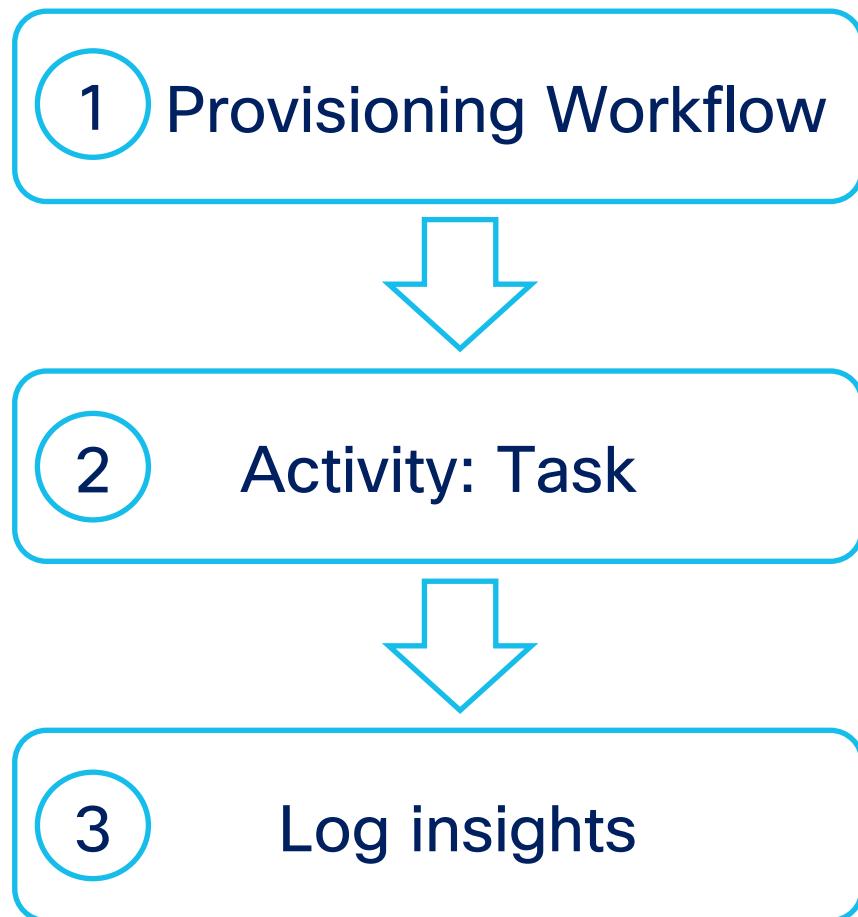
The screenshot shows the Catalyst Center interface for the KRK04 fabric site. The left sidebar displays navigation links for Fabric Infrastructure, Layer 3 Virtual Networks, Layer 2 Virtual Networks, Anycast Gateways, Wireless SSIDs, Authentication Template, and Port Assignment. The main content area is titled 'Devices (5)' and lists five devices: CAT9K-BORDER-01.cisco.com, CAT9K-BORDER-02.cisco.com, CAT9K-EDGE-01.cisco.com, CAT9K-EDGE-02.cisco.com, and CAT9K-EDGE-03.cisco.com. Each device entry includes columns for Tags, Device Name, IP Address, Fabric Role, Fabric Zone, Reachability, Fabric Provisioning Status, and Compliance Status. The 'Fabric Role' column for the first two border nodes shows 'BN | CP', while the others show 'EN'. The 'Reachability' column for all devices shows a green checkmark and the word 'Reachable'. The 'Fabric Provisioning Status' column shows 'Success' for all devices. The 'Compliance Status' column shows 'Compliant' for all devices. A red dashed box highlights an error message for the first border node: 'Error: Unable to push to device 172.16.0.1 using protocol ssh2 the CLI vrf definition DEVICE_VN. FlowId: d3bbb67a-dc5f-44ca-9788-d09c127adef0'.

Tags	Device Name	IP Address	Fabric Role	Fabric Zone	Reachability	Fabric Provisioning Status	Compliance Status
<input type="checkbox"/>	CAT9K-BORDER-01.cisco.com	172.16.0.1	BN CP	--	Reachable	Success	Compliant
<input type="checkbox"/>	CAT9K-BORDER-02.cisco.com	172.16.0.2	BN CP	--	Reachable	Success	Compliant
<input type="checkbox"/>	CAT9K-EDGE-01.cisco.com	172.16.0.3	EN	--	Reachable	Success	Compliant
<input type="checkbox"/>	CAT9K-EDGE-02.cisco.com	172.16.0.4	EN	--	Reachable	Success	Compliant
<input type="checkbox"/>	CAT9K-EDGE-03.cisco.com	172.16.0.5	EN	--	Reachable	Success	Compliant

Standard view and typical provisioning issues (SDA provisioning errors)

Catalyst Center: Provisioning

Troubleshooting workflow and issue triage



- 1a) Validate provisioning status in Inventory page (Focus: Provisioning)
- 2a) Verify Task/Audit Log details.
2b) Collect task ID and/or contextual ID.
- 3a) Use Kibana tool to perform an in-depth analysis of the logs
3b) For any UI related action investigation, collect X-Correlation ID.
3c) Use the Correlation ID or X-Correlation ID to identify the relevant logs.
3d) Fine tune the filtering on the Log Explorer/Kibana.

Catalyst Center: Provisioning

Tip #1a: Check the provisioning status on the Inventory page. Select Focus: Provision > See Details

To provision subscriptions on devices that have not been discovered with NETCONF, rediscover the devices with NETCONF, and update the Telemetry Settings with the Force Configuration Push option.

Global

Focus: Provision

Recent Provisioning Results

Time	Task	Status	As of
January 2, 2025 4:29 PM	Device Controllability and Telemetry	SUCCESS	Jan 3, 2025 9:20 AM
January 2, 2025 5:04 PM	Fabric Provisioning	FAILED	16 hours ago
	Unable to push to device 172.16.0.1 using protocol ssh2 the CLI vrf definition DEVICE_VN		
	Device response: % Feature is not supported		
.../Krakow/KRK04	Reachable	Success	16 hours ago
.../Krakow/KRK04	Reachable	Success	16 hours ago
.../Krakow/KRK04	Reachable	Success	16 hours ago
.../Krakow/KRK04	Reachable	Success	16 hours ago

Catalyst Center: Activity – Tasks

Tip #2a: Double-click on provisioning details and check the Task status: : Activities > Tasks

1. Activities

2. Tasks

3. Device Details

4. Provision Details

Modifying Fabric at KRK04 (border transit)

Task • PROVISION

Completed • Failed

Start: Jan 2, 2025 5:03 PM End: Jan 2, 2025 5:04 PM

As of: 9:26:53 AM Refresh

TASK PROGRESS

5 4 1 0 0 0 0 0

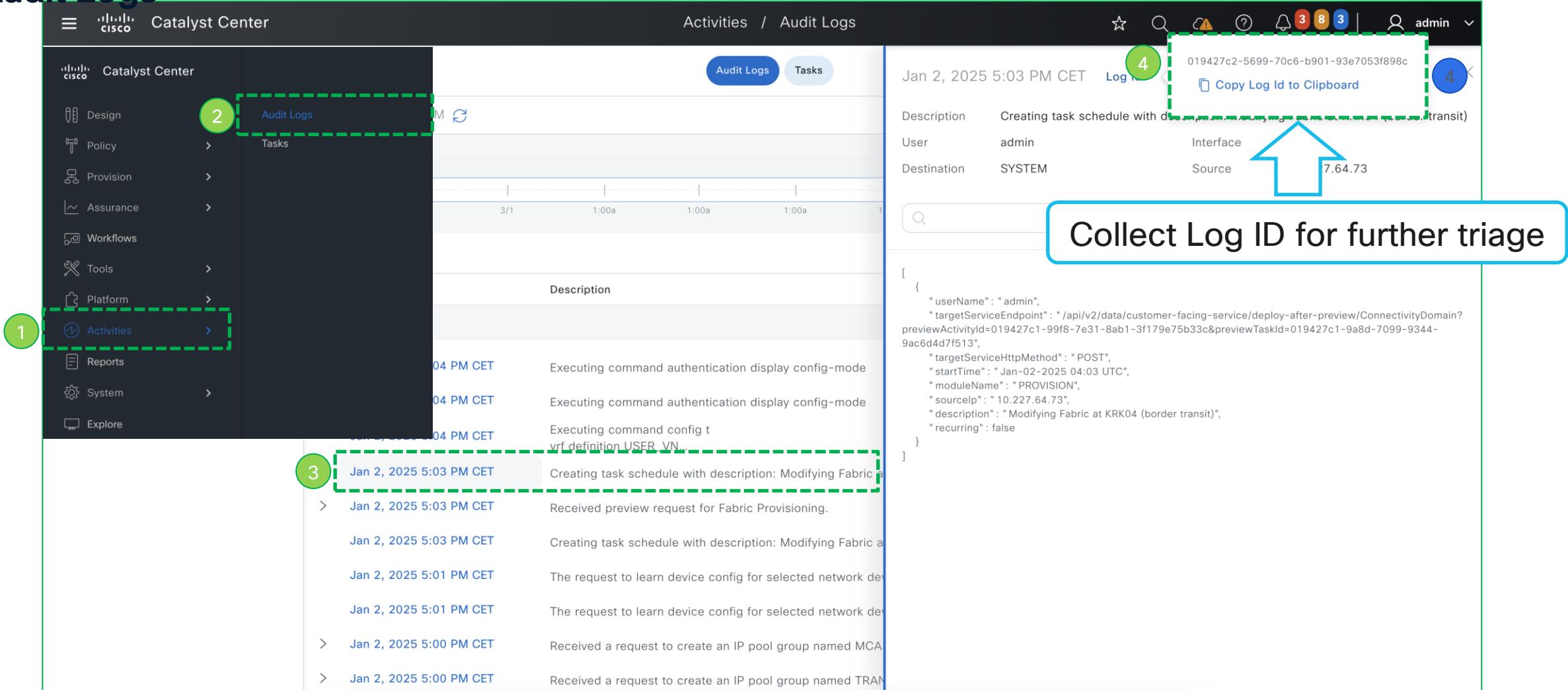
Total Success Failed Stopped In Progress Not Started

This task was created to deploy configuration that was previously previewed as a work item. [View Work Item Details](#)

Device Name	Status	Total Time to Provision
CAT9K-BORDER-01.cisco.com	FAILED	Recent Provisioning Results
CAT9K-BORDER-02.cisco.com	SUCCESS	Time January 2, 2025 5:03 PM Task Fabric Provisioning Status ROLLBACK_SUCCESS Error
CAT9K-EDGE-01.cisco.com	SUCCESS	Unable to push to device 172.16.0.1 using protocol ssh2 the CLI vrf definition DEVICE_VN

Catalyst Center: Activity – Audit Logs

Tip #2b: Retrieve the Log ID corresponding to a specific provisioning transaction: Activities > Audit Logs



1. Activities

2. Audit Logs

3. Log entry: Jan 2, 2025 5:03 PM CET, Description: Creating task schedule with description: Modifying Fabric at KRK04 (border transit)

4. Log ID: 019427c2-5699-70c6-b901-93e7053f898c

Collect Log ID for further triage

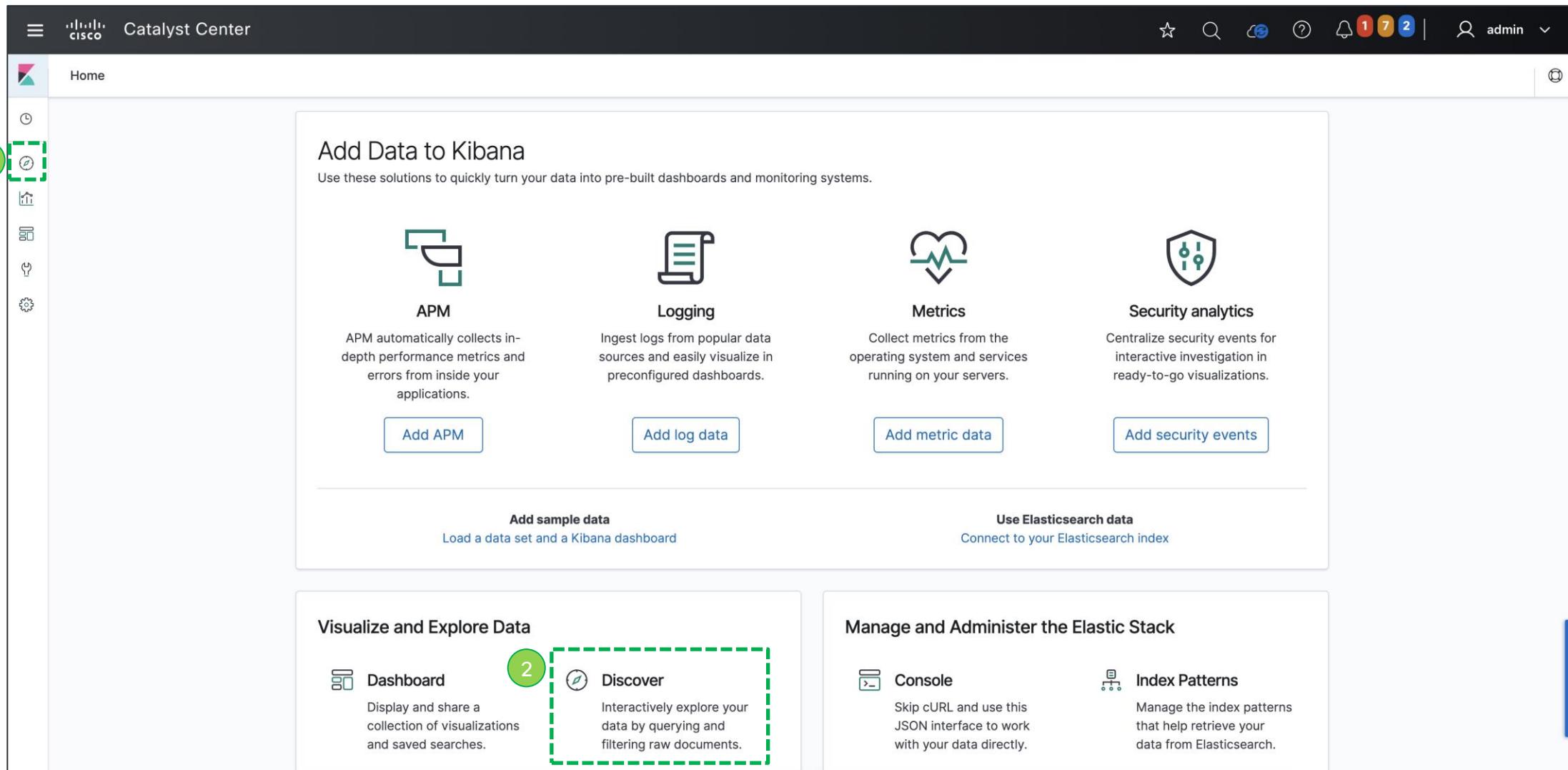
```
[{"user": "admin", "targetServiceEndpoint": "/api/v2/data/customer-facing-service/deploy-after-preview/ConnectivityDomain?previewActivityId=019427c1-99f8-7e31-8ab1-3f179e75b33c&previewTaskId=019427c1-9a8d-7099-9344-9ac6d4d7f513", "targetServiceHttpMethod": "POST", "startTime": "Jan-02-2025 04:03 UTC", "moduleName": "PROVISION", "sourceIp": "10.227.64.73", "description": "Modifying Fabric at KRK04 (border transit)", "recurring": false}
```

Catalyst Center: Log Explorer

Tip #3a): Use Log Explorer (Kibana) to find all relevant log messages for a given Task:
System > System 360 > Log Explorer

The screenshot shows the Catalyst Center interface. The left sidebar has a green dashed box around the 'System' item, with a green circle containing the number '1' to its left. The 'System 360' item under 'System' is also highlighted with a green dashed box and a green circle containing the number '2' to its left. The right side of the interface shows two cards: 'High Availability' (As of Jan 2, 2025 10:11 AM) and 'Cluster Tools' (As of Jan 2, 2025 10:09 AM). The 'Cluster Tools' card has a green dashed box around the 'Log Explorer' item, with a green circle containing the number '3' to its left. A large blue arrow points upwards from the 'Log Explorer' item towards a callout box. The callout box contains the text 'Navigate to Log Explorer for log analysis'.

Catalyst Center: Log Explorer (Kibana)



1

Home

Add Data to Kibana

Use these solutions to quickly turn your data into pre-built dashboards and monitoring systems.

APM
APM automatically collects in-depth performance metrics and errors from inside your applications.

Logging
Ingest logs from popular data sources and easily visualize in preconfigured dashboards.

Metrics
Collect metrics from the operating system and services running on your servers.

Security analytics
Centralize security events for interactive investigation in ready-to-go visualizations.

[Add APM](#)

[Add log data](#)

[Add metric data](#)

[Add security events](#)

Add sample data
Load a data set and a Kibana dashboard

Use Elasticsearch data
Connect to your Elasticsearch index

Visualize and Explore Data

Dashboard
Display and share a collection of visualizations and saved searches.

Discover
Interactively explore your data by querying and filtering raw documents.

Console
Skip CURL and use this JSON interface to work with your data directly.

Index Patterns
Manage the index patterns that help retrieve your data from Elasticsearch.

2

Catalyst Center: Log Explorer (Kibana)

The screenshot shows the Catalyst Center Log Explorer (Kibana) interface. At the top, a search bar contains the text "019427c2-5699-70c6-b901-93e7053f898c". A green box labeled "1" highlights this search term. A blue box labeled "Filter logs by specifying specific Log ID." has an arrow pointing to the search bar. To the right, a time range is set from "Jan 2, 2025 @ 16:30:00.0" to "Jan 2, 2025 @ 17:30:00.0". A green box labeled "2" highlights this range. A blue box labeled "Narrow down time window." has an arrow pointing to the time range. On the left, a sidebar shows "Selected fields" including "kubernetes.container_name", "kubernetes.host", "kubernetes.namespace_name", "kubernetes.pod_name", and "log". A green box labeled "3" highlights these fields. A blue box labeled "Add extra columns to gain deeper insights into the Catalyst Center microservices involved in a specific Task (E.g. Pod, Container and Host)" has an arrow pointing to the "Available fields" section, which includes "@timestamp" and "t_id". At the bottom, a table displays log messages with columns "kubernetes.namespace_name", "kubernetes.host", and "kubernetes.container_name". A green box labeled "4" highlights a specific log entry. A blue box labeled "Examine the log messages." has an arrow pointing to this entry. The log message content is partially visible, showing details about a task ID, activity ID, and preview activity ID.

Filter logs by specifying specific Log ID.

Narrow down time window.

Add extra columns to gain deeper insights into the Catalyst Center microservices involved in a specific Task (E.g. Pod, Container and Host)

Examine the log messages.

kubernetes.namespace_name	kubernetes.host	kubernetes.container_name
fusion	100.64.0.1	scheduler-service
9.64.0.1	spf-service-manager-service	spf-service-manager-service-767db5dbbf-h4xv4
2025-01-02 16:04:37,647	INFO	w-NotificationContainer-4 c.c.e.sch
		WorkSpecification@2ff6d99c[actionComplete=<null>,cr
		eateTime=1735833853245, cronExpression=<null>,description=Modifying Fabric a
		ndTime=0,featureName=<null>,groupName=<null>,int
		erfaceName=<null>,lastUpdateTime=173583385329,metaData=<null>,modul
		e=PROVISION.notificationHeader={Content-Tvne=application/json. Preview-Prim
		7c2-5699-70c6-b901-93e7053f898c, requestType=DEPLOY_AFTER_PREVIEW corre
		lationId=b68abf5f-c98d-44ce-a906-b688433fc65c

Catalyst Center: Log Messages

Example: ActivityIDs & correlatonIds

Table	JSON
①	@timestamp Jan 2, 2025 @ 17:04:37.648
t _id	PobDJ5QBhx64c0lyL45x
t _index	logstash-info-2025.01.02
# _score	-
t _type	fluentd
t docker.container_id	ed9460a6389d6fb2dc7e1191eb48201409c4423622e6eaf3fb2b321cdc602b14
t kubernetes.container_image	maglev-registry.maglev-system.svc.cluster.local:5000/fusion/spf-service-manager-service:7.1.720.60128
t kubernetes.container_image_id	docker-pullable://maglev-registry.maglev-system.svc.cluster.local:5000/fusion/spf-service-manager-service@sha256:5faf76485e385bba05b8a6010a402c7a93fe8bcae9f533840d9cbf5af044c5b8
t kubernetes.container_name	spf-service-manager-service
t kubernetes.host	100.64.0.1
t kubernetes.labels.pod-template-hash	767db5dbbf
t kubernetes.labels.serviceName	spf-service-manager-service
t kubernetes.labels.version	7.1.720.60128
t kubernetes.master_url	https://169.254.48.1:443/api
t kubernetes.namespace_id	8c9e3ebf-e47d-46f0-9af0-633998526e81
t kubernetes.namespace_name	fusion
t kubernetes.pod_id	15690304-cfcd-4ae1-89df-e567ab9f6826
t kubernetes.pod_name	spf-service-manager-service-767db5dbbf-h4xv4
t log	2025-01-02 16:04:37,647 INFO w-NotificationContainer-4 c.c.a.c.s.n.SPFWWorkflowCompletionEventCallback taskId = 019427c1-99f8-7e31-8ab1-3f179e75b33c, currentActivityId = 019427c2-5699-70c6-b901-93e7053f898c, previewTaskId = 019427c1-99f8-7e31-8ab1-3f179e75b33c, currentActivityId = 019427c2-5699-70c6-b901-93e7053f898c, previewActivityId = 019427c1-99f8-7e31-8ab1-3f179e75b33c, currentCorrelationId = b68abf5f-c98d-44ce-a906-b688433fc65c, previewCorrelationId = b68abf5f-c98d-44ce-a906-b688433fc65c, requestType = DEPLOY_AFTER_PREVIEW, correlationId=b68abf5f-c98d-44ce-a906-b688433fc65c
t stream	stdout
t tag	kubernetes.var.log.containers.spf-service-manager-service-767db5dbbf-h4xv4_fusion_spf-service-manager-service-ed9460a6389d6fb2dc7e1191eb48201409c4423622e6eaf3fb2b321cdc602b14.log

Catalyst Center – Log IDs

Activity ID: a user/system action designed to achieve a specific configuration, monitoring, or troubleshooting goal within the network (e.g. provisioning activities, monitoring activities, policy management, software management, etc.).

(NEW) Correlation ID: is a unique identifier assigned to a request or a group of related requests that span multiple systems or components. It allows for tracking and correlating logs and activities across different services within Catalyst Center.

Catalyst Center: Log Explorer

Tip #3b: Use the browser's 'Developer Tools' to get the X-Correlation ID for any UI related investigation.

The screenshot shows the Catalyst Center interface for provisioning a device. The main page displays steps for initial checks, device compliance, and device level validations, all of which are successful. A callout box highlights the 'x-Correlation-id header can be now found in all HTTP Requests generated by Catalyst Center API Gateway'. A green circle labeled '1' points to the Network tab in the browser's developer tools, which shows an API request with the X-Correlation-ID header. A green circle labeled '2' points to the X-Correlation-ID value in the browser's developer tools headers.

x-Correlation-id header can be now found in all HTTP Requests generated by Catalyst Center API Gateway

1

2

Name	Request URL:	Request Method:	Status Code:
icon-font.c7a3b775e861aa0df6c8fdc688a8f61...	https://10.62.149.204/api/v2/data/customer-facing-service/deviceinfo?minify=true&networkDeviceId=f9bf3ac4-596-4f83-85b3-26d87f01f6c	GET	200 OK 10.62.149.204:443 strict-origin-when-cross-origin
DeviceInfo?minify=true&networkDeviceId=f9bf...			
vcr-precomputation			
post?filter=a-dnaconprem,u-dna-provision-de...			
vcr-precheck			
status?taskId=a716fc53-4cbe-447c-a421-586...			

Request Headers:

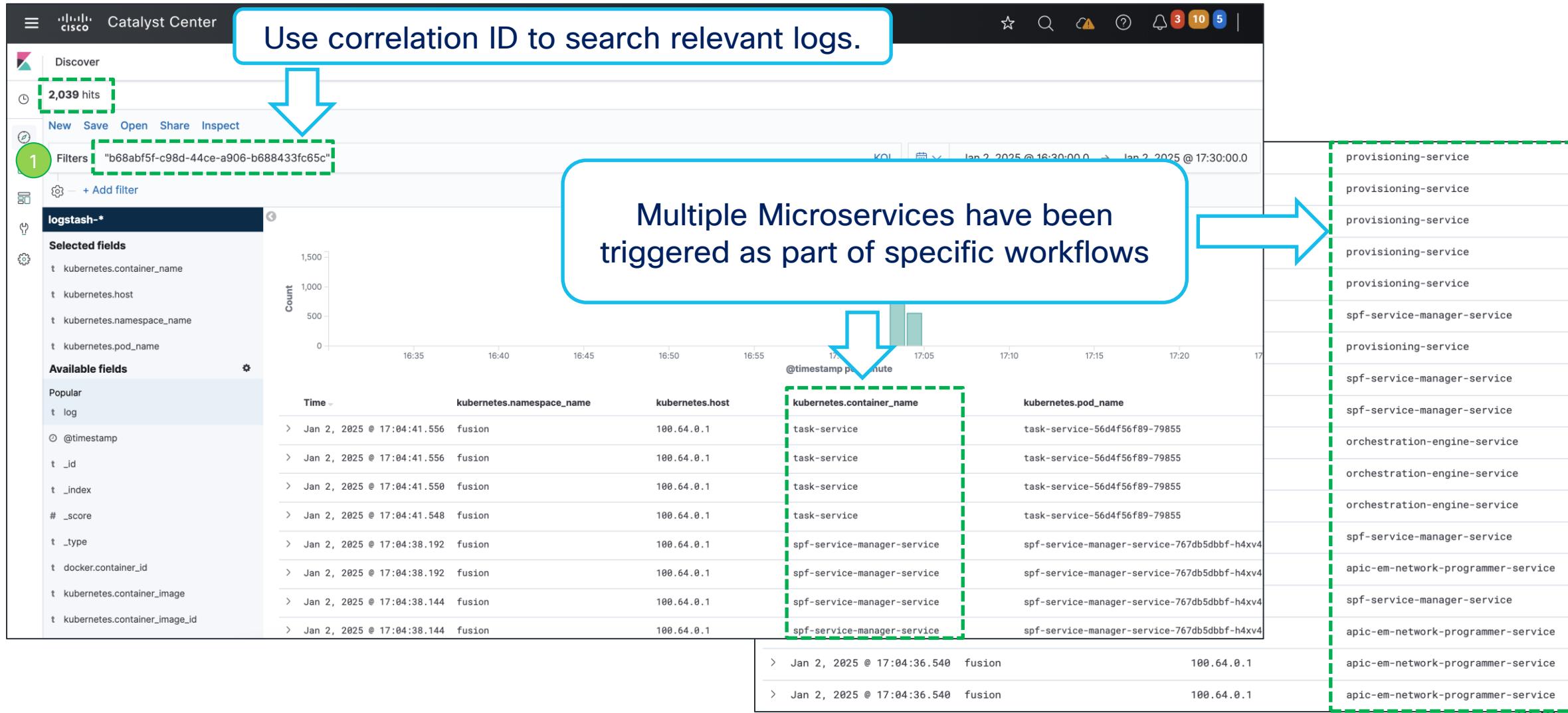
- no-store
- 3805
- default-src 'self' 'unsafe-inline' 'unsafe-eval' blob: data: application/json; charset=utf-8
- Thu, 02 Jan 2025 13:43:53 GMT
- no-cache
- Strict-Transport-Security: max-age=31536000; includeSubDomains
- Via: api-gateway
- X-Content-Type-Options: nosniff
- X-Correlation-Id: e5fd5ead-7d74-4bc0-9915-aa1688e4fbe5
- X-Frame-Options: SAMEORIGIN
- X-Xss-Protection: 1; mode=block

Response Headers:

- Content-Type: application/json, text/plain, */*
- Accept-Encoding: gzip, deflate, br, zstd
- Accept-Language: pl,en-US;q=0.9,en;q=0.8
- Cache-Control: no-cache
- Cookie: isConnectedHack=true; X-JWT-ACCESS-TOKEN=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9eyJzdWIiOiJmNl1MDk5ZDc2YWQ4NDRKMDBmNDk2OWEiLCJhdXR0U291cmNljoiaW50ZXJuYWwiLCJ0ZW5hbnROY

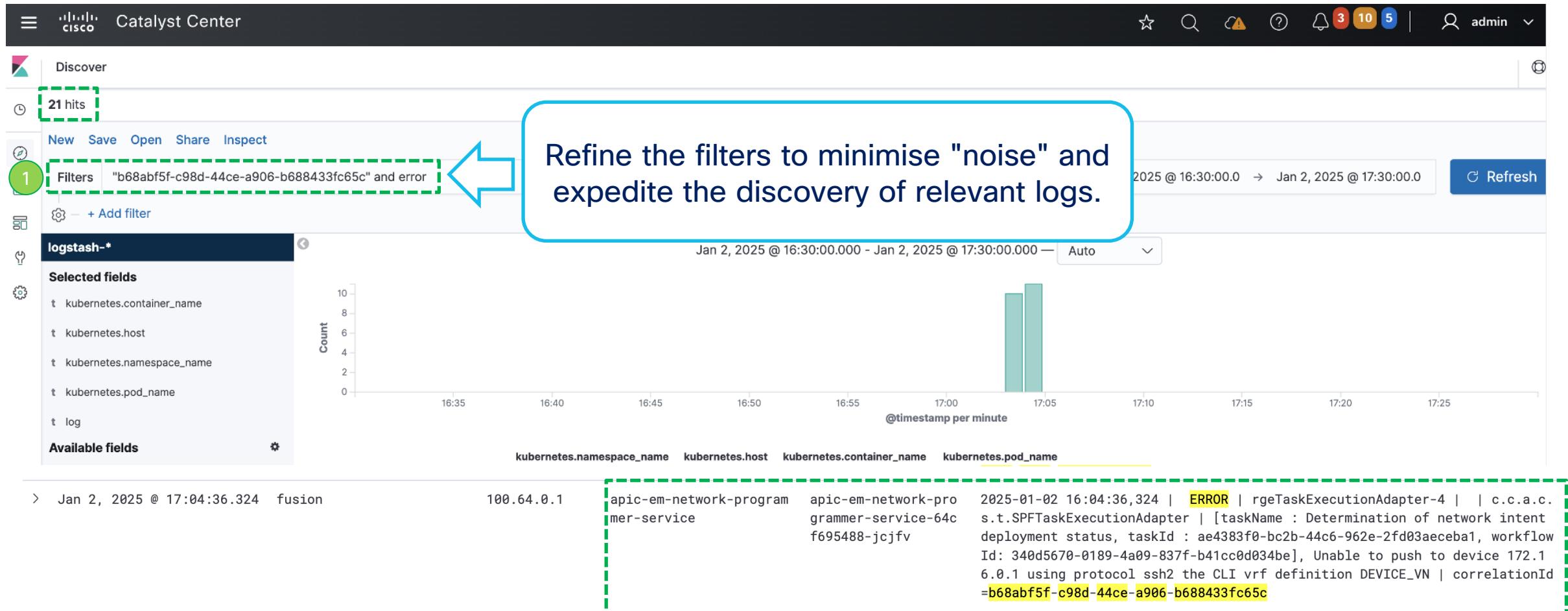
Catalyst Center : Log Explorer (Kibana)

Tip #3c: Use CorrelationID to find all relevant log messages across all microservices.



Catalyst Center: Log Explorer (Kibana)

Tip #3d: Combine the CorrelationID with keywords (e.g., error, warning) to filter log.



Refine the filters to minimise "noise" and expedite the discovery of relevant logs.

Selected fields: t_kubernetes.container_name, t_kubernetes.host, t_kubernetes.namespace_name, t_kubernetes.pod_name, t_log

Timestamp	Host	Namespace	Container	Pod	Log
Jan 2, 2025 @ 17:04:36.324	fusion	100.64.0.1	apic-em-network-programmer-service	apic-em-network-processor-service-64cf695488-jcjfv	2025-01-02 16:04:36,324 ERROR rgeTaskExecutionAdapter-4 c.c.a.c.s.t.SPFTaskExecutionAdapter [taskName : Determination of network intent deployment status, taskId : ae4383f0-bc2b-44c6-962e-2fd03aeceba1, workflowId: 340d5670-0189-4a09-837f-b41cc0d034be], Unable to push to device 172.16.0.1 using protocol ssh2 the CLI vrf definition DEVICE_VN correlationId =b68abf5f-c98d-44ce-a906-b688433fc65c

Triaging issues using Cisco Catalyst Center with Logging Monitor/Kibana

Key takeaways:

- 1. Check the basics:** confirm provisioning status in Inventory tab and verify task details.
- 2. Identify IDs:** Locate the task ID, activity ID, or correlation ID associated with any problematic activity.
- 3. Log Analysis:** Utilise the Catalyst Center Log Analyser (Kibana) to delve into all system logs for further investigation.
- 4. Kibana Capabilities:** Refer to the official Kibana documentation to explore and analyse data with Kibana.
<https://www.elastic.co/docs/explore-analyze>

SD-Access: Triaging Fabric & Network issues

3) DHCP / Host Onboarding Use-Case

End-point: DHCP (Host on-boarding)

Commonly Reported Scenario

Linux:

```
dhclient[1234]: DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 3
dhclient[1234]: No DHCPOFFERS received.
dhclient[1234]: Unable to obtain a lease on first try.
```

No DHCP Offer received by the end-point.

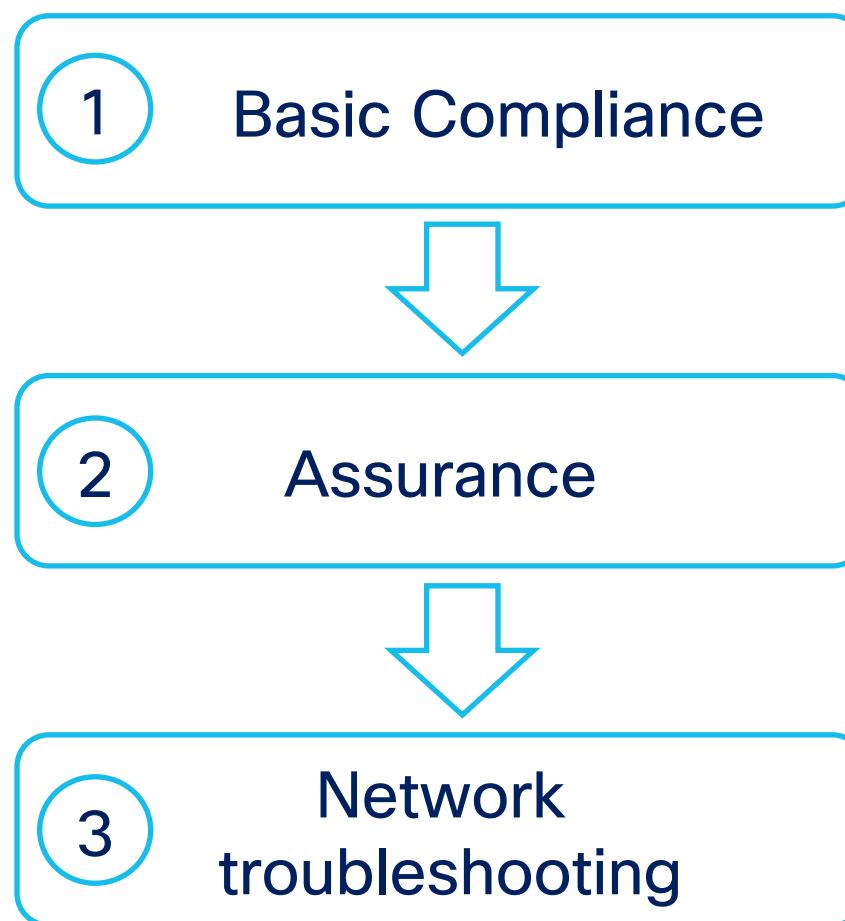
Windows:

IP address assigned by Automatic Private IP Addressing (APIPA) feature.

Ethernet adapter Ethernet:

```
Connection-specific DNS Suffix . :
Autoconfiguration IPv4 Address. . . . . : 169.254.1.2
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . :
```

SD-Access: DHCP Troubleshooting workflow and issue triage



- 1a) Check and confirm Fabric Provisioning Tasks Status
- 1b) Check and confirm Configuration Drift Status
- 1c) Check and confirm Compliance Status
- 1d) Resolve Compliance issues

- 2a) Check and confirm the operational status under Assurance
- 2b) Check potential defects impacting via Network Bug Identifier

- 3a) Perform Network troubleshooting via Command Runner
- 3b) Perform Network troubleshooting via Run Commands

Fabric sites – Provisioning

Tip #1a: Check Fabric Provisioning state: Provisioning > Fabric Sites



The screenshot shows the Catalyst Center interface with the following navigation path: Provisioning > SD-Access > Fabric Sites. The 'Fabric Sites' link is highlighted with a green dashed box and a green circle labeled '2'. The left sidebar also has a green dashed box around the 'Provision' link under the 'Design' category, with a green circle labeled '1'. A callout box with a blue border and a blue arrow points from the bottom of the 'Fabric Sites' section to the text: 'Ensure that the SD-Access Fabric is fully provisioned according to the original intent.' The bottom left of the interface shows a 'Provisioning Tasks' section with a timeline from 4p to 2p, showing green bars for 'Tasks Deployed' and red bars for 'Errors'. A green circle labeled '3' is on the legend for 'Tasks Deployed'.

Ensure that the SD-Access Fabric is fully provisioned according to the original intent.

Fabric Device - Config Drift

Tip #1b: Verify Configuration drift: Fabric Infrastructure > Select the Device > More > Config Drift

The screenshot shows the Catalyst Center interface for a device named CAT9K-EDGE-01.cisco.com (172.16.0.3). The interface is divided into two main sections: a left sidebar and a right main content area.

Left Sidebar (Fabric Infrastructure):

- Fabric Sites / KRK04
- View Site Hierarchy
- Site Actions
- Fabric Infrastructure (selected)
- Layer 3 Virtual Networks
- Layer 2 Virtual Network

Right Main Content Area:

Device Details: CAT9K-EDGE-01.cisco.com (172.16.0.3)
Reachable Uptime: 16 days 18 hrs 25 mins Device Role: ACCESS

Config Drift Overview: Config Drift Date Range: Sep 5, 2024 to Jan 3, 2025. The chart shows the number of lines of configuration drift over time, with a peak around Sep 15 and another around Nov 17.

Config Drift Versions:

- Config Drift Version: Nov 30, 2024 01:31 PM (Label Config: 29 ip name-server 100.64.0.100, 30 ip domain lookup source-interface Loopback0, 31 ip domain name dna-pod.lab, 32 ip dhcp snooping)
- Config Drift Version: Dec 09, 2024 05:10 PM (Label Config: 29 ip name-server 100.64.0.100, 30 ip domain lookup source-interface Loopback0, 31 ip domain name dna-pod.lab, 32 ip dhcp snooping vlan 1, 33 ip dhcp snooping)

Callout 1: A green circle with the number 1 points to the 'More' button in the top right corner of the main content area.

Callout 2: A green circle with the number 2 points to the 'Config Drift' link in the dropdown menu that appears when the 'More' button is clicked.

Callout 3: A green circle with the number 3 points to the 'Config Drift' section in the main content area, which is highlighted with a green dashed box.

Text Callout: A blue callout box with a blue arrow points to the 'Config Drift' section in the main content area. The text inside the box reads: "Verify any configuration changes between the working and non-working setup."

Fabric Infrastructure – Compliance

Tip #1c: Check Compliance Status: Fabric Infrastructure > Compliance Status

Screenshot of the Cisco Catalyst Center interface showing the Fabric Infrastructure > Compliance Status page for KRK04.

1 **Fabric Infrastructure** (highlighted with a green dashed box)

2 **Compliance Status** (highlighted with a green dashed box)

Check compliance status for all devices in the fabric.

Tags	Device Name	IP Address	Fabric Role	Fabric Zone	Reachability	Fabric Provisioning Status
<input type="checkbox"/>	CAT9K-BORDER-01.cisco.com	172.16.0.1	BN CP	--	Reachable	Success
<input type="checkbox"/>	CAT9K-BORDER-02.cisco.com	172.16.0.2	BN CP	--	Reachable	Success
<input type="checkbox"/>	CAT9K-EDGE-01.cisco.com	172.16.0.3	EN	--	Reachable	Success
<input type="checkbox"/>	CAT9K-EDGE-02.cisco.com	172.16.0.4	EN	--	Reachable	Success
<input type="checkbox"/>	CAT9K-EDGE-03.cisco.com	172.16.0.5	EN	--	Reachable	Success

5 Record(s) Show Records: 25 1 - 5 1 >

Compliance Summary

Tip #1d: Auto-fix all Compliance Issues: “Fix All Configuration Compliance Issues”

Fix compliance issues and re-run compliance checks.

Verify all non-compliance issues detected by Catalyst Center.

1

2

3

3, 2025 4:08 PM

Run Compliance Check

1 Network Settings

3 General: 3 Open Violations

57 mins since in sync

0 Lines added: 0 Lines removed: 0 Lines modified: 0

2

3

SD-Access Unsupported Configuration BETA

© 2025 Cisco and/or its affiliates. All rights reserved.

BRKTRS-3821

CISCO

Compliance Fix – Configuration preview

Catalyst Center Provision / SD-Access admin

CAT9K-BORDER-01.cisco.com - Compliance Fix As of: 12:00:55 PM Refresh

Step 3 of 3: Preview Configuration
Review the device configuration provided below by clicking on each device. When you are done, click Deploy to apply the configuration to the device.

Device IP: 172.16.0.1 Site: Global/Poland/Krakow/

Configurations - Side by side view Status: Ready

Search by device name View by Configuration Source • All

Search configuration

1 Configuration to be Deployed 39 Line(s)

```
5 interface TwentyFiveGigE1/0/20
6 switchport mode trunk
7 switchport trunk allowed vlan all
8 exit
9 ip access-list extended ACL_WEAUTH_REDIRECT
10 no 80 deny ip any host 100.64.0.2
11 90 deny ip any host 100.64.0.2
12 exit
13 router lisp
14 site site_uci
15 authentication-key ***** 97fffa0bfe9144852
16 aaa group server radius dnac-client-radius-group
17 server name dnac-radius_100.64.0.2
18 exit
19 aaa group server radius dnac-network-radius-group
20 server name dnac-radius_100.64.0.2
21 exit
22 radius server dnac-radius_100.64.0.2
23 pac key *****
24 exit
25 radius-server vsa send authentication
26 radius-server vsa send accounting
27 line vty 0 15
28 login authentication VTY_authen
29 authorization exec VTY_author
30 aaa server radius dynamic-author
31 client 100.64.0.2 server-key *****
32 client 10.62.146.192 server-key *****
33 exit
34 ip domain lookup source-interface Loopback0
35 ip domain lookup
36 ip name-server 100.64.0.100
37 ip domain name cisco.com
38
39 do cts credentials id f9hf3ac459164f8385b126d87f701f6c password *****
```

2 Running Configuration 834 Line(s)

```
1 Building configuration...
2
3 Current configuration : 26995 bytes
4 !
5 ! Last configuration change at 09:58:04 UTC Fri Jan 3 2025 by dnacadmin
6 !
7 version 17.12
8 service tcp-keepalives-in
9 service tcp-keepalives-out
10 service timestamps debug datetime msec
11 service timestamps log datetime msec
12 service password-encryption
13 service sequence-numbers
14 service call-home
15 no platform punt-keepalive disable-kernel-core
16 no platform punt-keepalive settings
17
18 hostname CAT9K-BORDER-01
19 !
20 !
21 vrf definition DEVICE_VN
22 rd 1:4099
23 !
24 address-family ipv4
25 route-target export 1:4099
26 route-target import 1:4099
27 exit-address-family
28 !
29 vrf definition Mgmt-vrf
30 !
31 address-family ipv4
32 exit-address-family
33 !
34 address-family ipv6
35 exit-address-family
```

Is this feature helpful?

Exit and Preview Later Discard Deploy

Validate the configuration that is pushed to your network as part of the compliance fix.

Catalyst Center: SD Access Assurance

Tip #2a: Check Assurance data

The screenshot shows the Catalyst Center interface with the SD-Access tab selected. A callout box labeled 'Verify any reported health issues related to fabric.' points to the summary statistics. Another callout box labeled 'Check issues reported by Catalyst Centre.' points to the table of reported issues.

SUMMARY Health as of Jan 9, 2025 1:28 PM

Fabric Sites	Layer 3 Virtual Networks	Fabric Devices	Transits	Telemetry Status	ISSUES
1	2	5	1	Good	5 P1 0 P2 5 Total
2 Unhealthy					

Issues (5)

Priority	Issue Type	Device Role	Category	Issue Count	Site Count (Area)	Device Count	Last Occurred Time
P1	Fabric Border node internet is unavailable	BORDER ROUTER	Connected	4	1	2	Jan 9, 2025 12:57 PM
P1	Fabric BGP session status is down with Peer Device	BORDER ROUTER	Connected	1	1	1	Jan 9, 2025 12:35 PM

© 2025 Cisco and/or its affiliates. All rights reserved.

BRKTRS-3821

Verify any reported health issues related to fabric.

Check issues reported by Catalyst Centre.

Catalyst Center: SD Access Assurance

Fabric BGP session status is down with Peer Device / Issue Instance

P1 BGP v4 neighborship(s) on Fabric Border 'CAT9K-BORDER-01.cisco.com' in Fabric Site 'Global/Poland/Krakow/KRK04' is down

Status: **Open** |

Issue Profile: global | Edit Issue Settings

INSIGHTS

BGP v4 neighborship(s) on Fabric Border 'CAT9K-BORDER-01.cisco.com' in Fabric Site 'Global/Poland/Krakow/KRK04' is down.

Device: [CAT9K-BORDER-01.cisco.com](#) |

Time: Jan 9, 2025 12:35 PM

Location: Global/Poland/Krakow/KRK04

Fabric Site: Global/Poland/Krakow/KRK04

1 Problem Details

2 Suggested Actions

Problem Details

2 session(s) down. The table below illustrates the applicable sessions for this device, along with their respective status, IP address, destination, VN name, and IP type.

Understand problems reported by Catalyst Centre

	Status	IP Address	Destination	VN Name	IP Type
		172.16.200.10	172.16.200.10	DEVICE_VN	ipv4
<input type="checkbox"/>		172.16.200.14	172.16.200.14	USER_VN	ipv4

Catalyst Center: SD Access Assurance

Fabric BGP session status is down with Peer Device / Issue Instance

P1 BGP v4 neighborship(s) on Fabric Border 'CAT9K-BORDER-01.cisco.com' in Fabric Site 'Global/Poland/Krakow/KRK04' is down

Status: Open | [Edit](#)

Issue Profile: global [Edit Issue Settings](#)

INSIGHTS

BGP v4 neighborship(s) on Fabric Border 'CAT9K-BORDER-01.cisco.com' in Fabric Site 'Global/Poland/Krakow/KRK04' is down.

Device: [CAT9K-BORDER-01.cisco.com](#)

Time: Jan 9, 2025 12:35 PM

Location: Global/Poland/Krakow/KRK04

Fabric Site: Global/Poland/Krakow/KRK04

Problem Details

Suggested Actions (2)

1 [Preview All](#)

2 [Run automatic checks to further triage the issue in the network.](#)

1 ✓ Verify the BGP session status.

✓ Verify the BGP session status for all vpnv4 neighbors
`show bgp vpnv4 unicast all summary`

BGP activity 98/51 prefixes, 271/187 paths, scan interval 60 secs
39 networks peaked at 22:44:50 Jan 7 2025 UTC (1d14h ago)

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
172.16.0.2	4	65000	4031	4029	155	0	0	01:51:57	2d12h
172.16.200.10	4	65100	0	0	1	0	0	01:51:57	Idle
172.16.200.14	4	65100	0	0	1	0	0	01:51:57	Idle
CAT9K-BORDER-01#									

✓ Verify the BGP session status for all ipv4 neighbors
`show bgp ipv4 unicast summary`

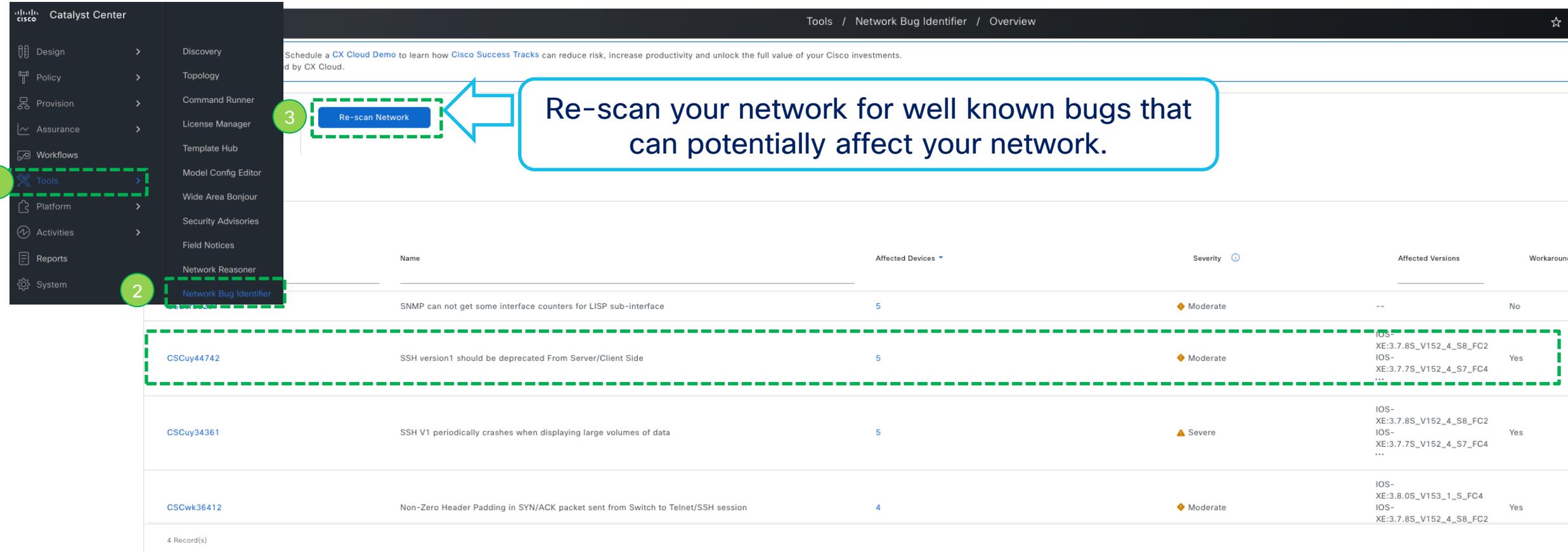
Success

Success

Success

Catalyst Center: Network Troubleshooting (DHCP)

Tip #2b: Check potential defects impacting your network: Tools > Network Bug Identifier



1

2

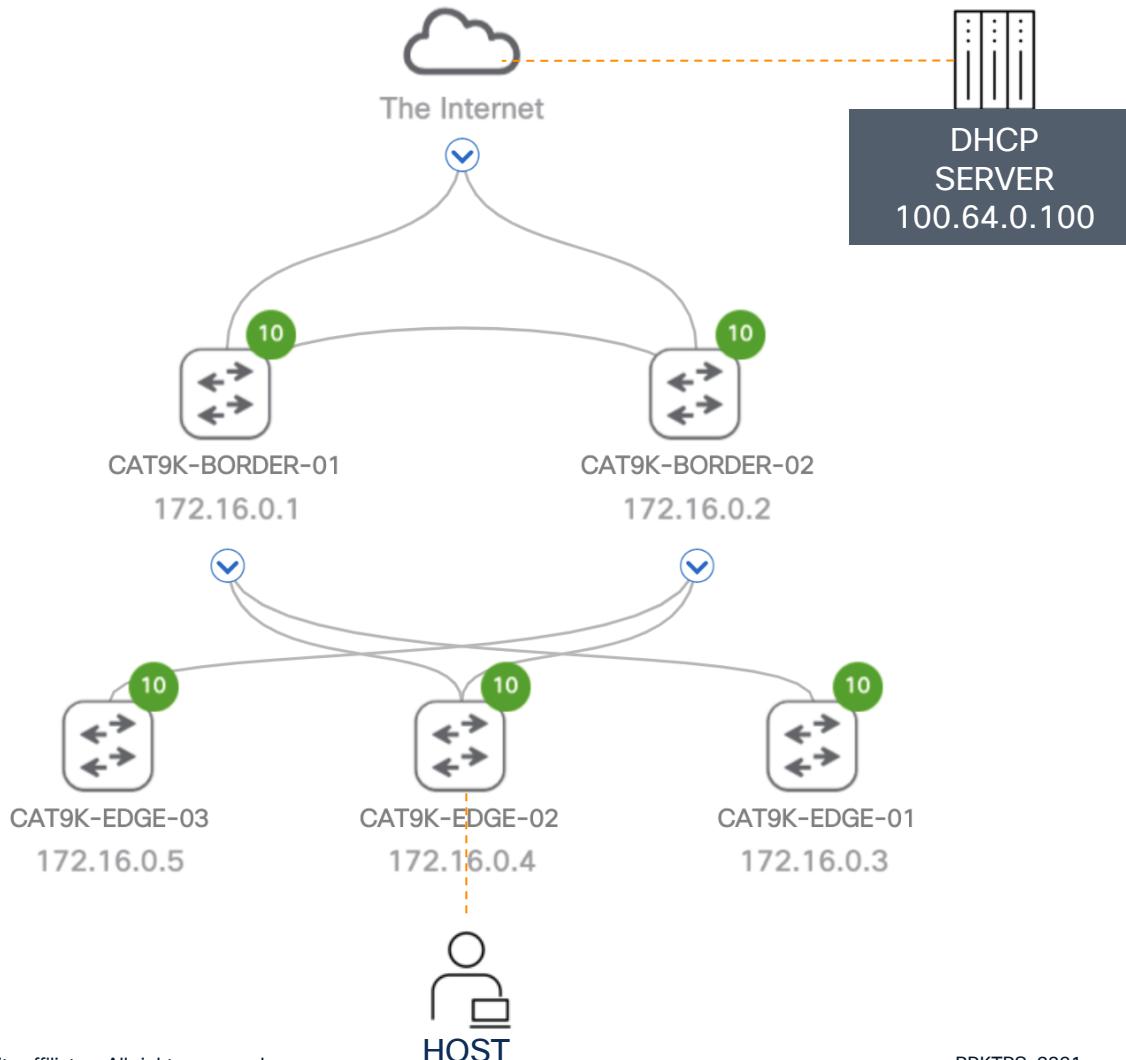
3

Re-scan your network for well known bugs that can potentially affect your network.

Name	Affected Devices	Severity	Affected Versions	Workaround
SNMP can not get some interface counters for LISP sub-interface	5	Moderate	--	No
CSCuy44742 SSH version1 should be deprecated From Server/Client Side	5	Moderate	IOS- XE:3.7.8S_V152_4_S8_FC2 IOS- XE:3.7.7S_V152_4_S7_FC4 ...	Yes
CSCuy34361 SSH V1 periodically crashes when displaying large volumes of data	5	Severe	IOS- XE:3.7.8S_V152_4_S8_FC2 IOS- XE:3.7.7S_V152_4_S7_FC4 ...	Yes
CSCwk36412 Non-Zero Header Padding in SYN/ACK packet sent from Switch to Telnet/SSH session	4	Moderate	IOS- XE:3.8.0S_V153_1_S_FC4 IOS- XE:3.7.8S_V152_4_S8_FC2	Yes

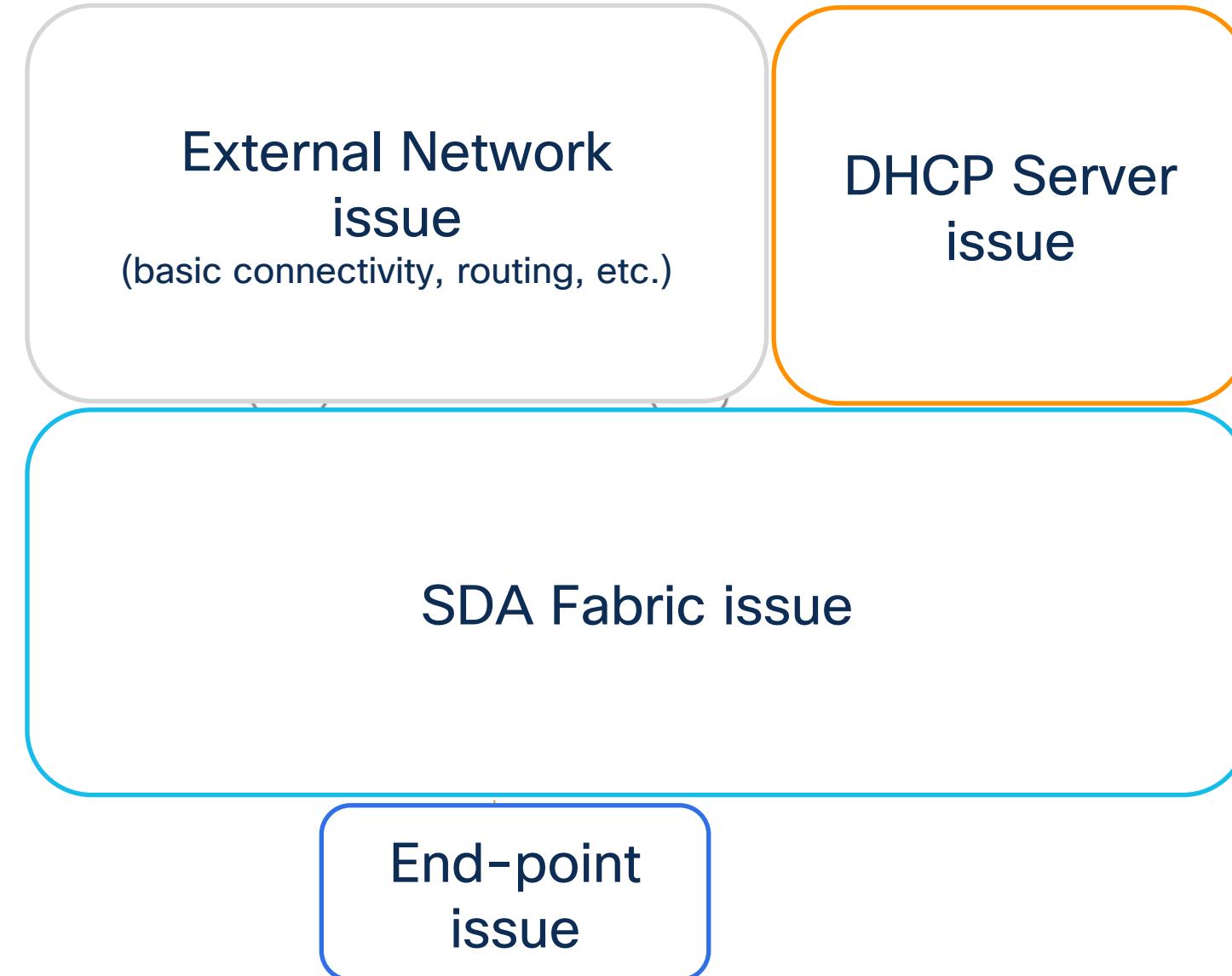
4 Record(s)

Catalyst Center: Network Troubleshooting (DHCP)



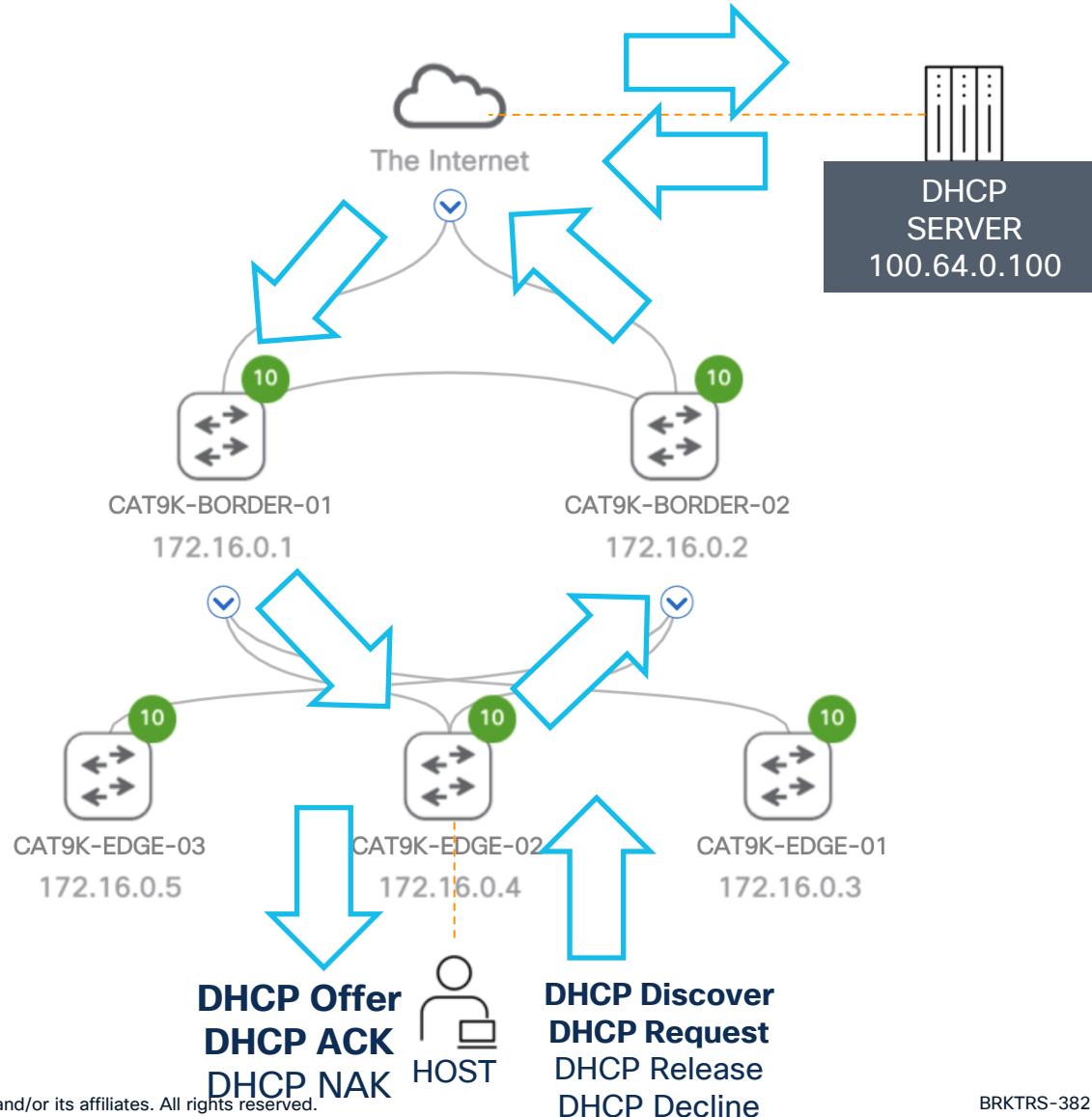
Only when all previous checks (configuration, assurance, compliance, known bugs) have been checked, start low level network troubleshooting.

Catalyst Center: Network Troubleshooting (DHCP)



Catalyst Center: Network troubleshooting (DHCP)

Example of DHCP packet flow



DHCP packets do not have to go through same devices (path can be asymmetric based on load-balancing rules within fabric / outside of the fabric)

Catalyst Center: Network Troubleshooting (DHCP)

Tip #3a: Execute Command Runner on multiple devices simultaneously: Tools > Command Runner

The image shows the Catalyst Center interface with the 'Tools > Command Runner' path highlighted by a green dashed box and numbered 1 and 2. A CLI command 'CLI: show platform dhcpsnooping client stats <MAC-ADDRESS>' is displayed in a box. The main interface shows a list of devices for triage and a command input field. A callout box 3 points to the device list, and a callout box 4 points to the command input field.

1 Tools

2 Command Runner

CLI: show platform dhcpsnooping client stats <MAC-ADDRESS>

Select all relevant devices for initial triage (e.g. edge & borders).

Select devices*

CAT9K-BORDER-01.cisco.com (172.16.0.1) × CAT9K-BORDER-02.cisco.com (172.16.0.2) × CAT9K-EDGE-02.cisco.com (172.16.0.4) ×

Select/Enter commands*

sh platform dhcpsnooping client stats 7c21.0d1d.9ec6 ×

Provide a specific CLI command to be run concurrently on all devices.

Catalyst Center: Network Troubleshooting (DHCP)

1  Command(s) executed successfully.

2    Upload to Case  Export all CLI output

Device List | Selected 3

CLI Output

CAT9K-BORDER-01.cisco.com (172.16.0.1) | sh platform dhcpsnooping client stats 7c21.0d1d.9ec6

1 E

1. **CAT9K-BORDER-01.cisco.com (172.16.0.1)**

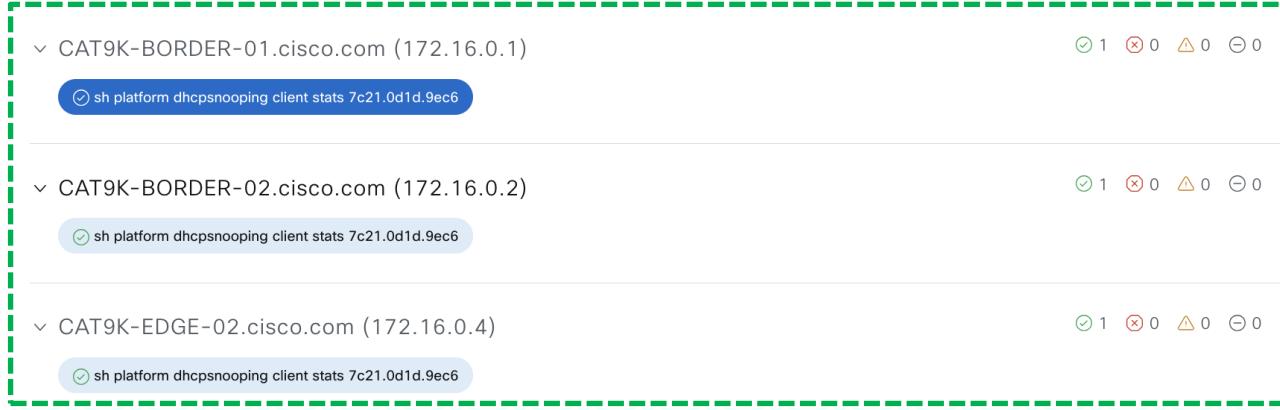
sh platform dhcpsnooping client stats 7c21.0d1d.9ec6

2. **CAT9K-BORDER-02.cisco.com (172.16.0.2)**

sh platform dhcpsnooping client stats 7c21.0d1d.9ec6

3. **CAT9K-EDGE-02.cisco.com (172.16.0.4)**

sh platform dhcpsnooping client stats 7c21.0d1d.9ec6

  1  0  0  0 

 1  0  0  0 

 1  0  0  0 

Timestamp	Destination MAC	Destination Ip	VLAN	Message	Handler:Action
2025/01/12 11:23:35.265	3C51.0EE4.D8FF	192.168.10.254	122	DHCPOFFER(B)	PUNT:RECEIVED
2025/01/12 11:23:35.265	3C51.0EE4.D8FF	192.168.10.254	123	DHCPOFFER(B)	LISP:GLEAN
2025/01/12 11:23:35.274	3C51.0EE4.D8FF	192.168.10.254	122	DHCPACK(B)	PUNT:RECEIVED
2025/01/12 11:23:35.274	3C51.0EE4.D8FF	192.168.10.254	123	DHCPACK(B)	LISP:GLEAN
CAT9K-BORDER-01#					

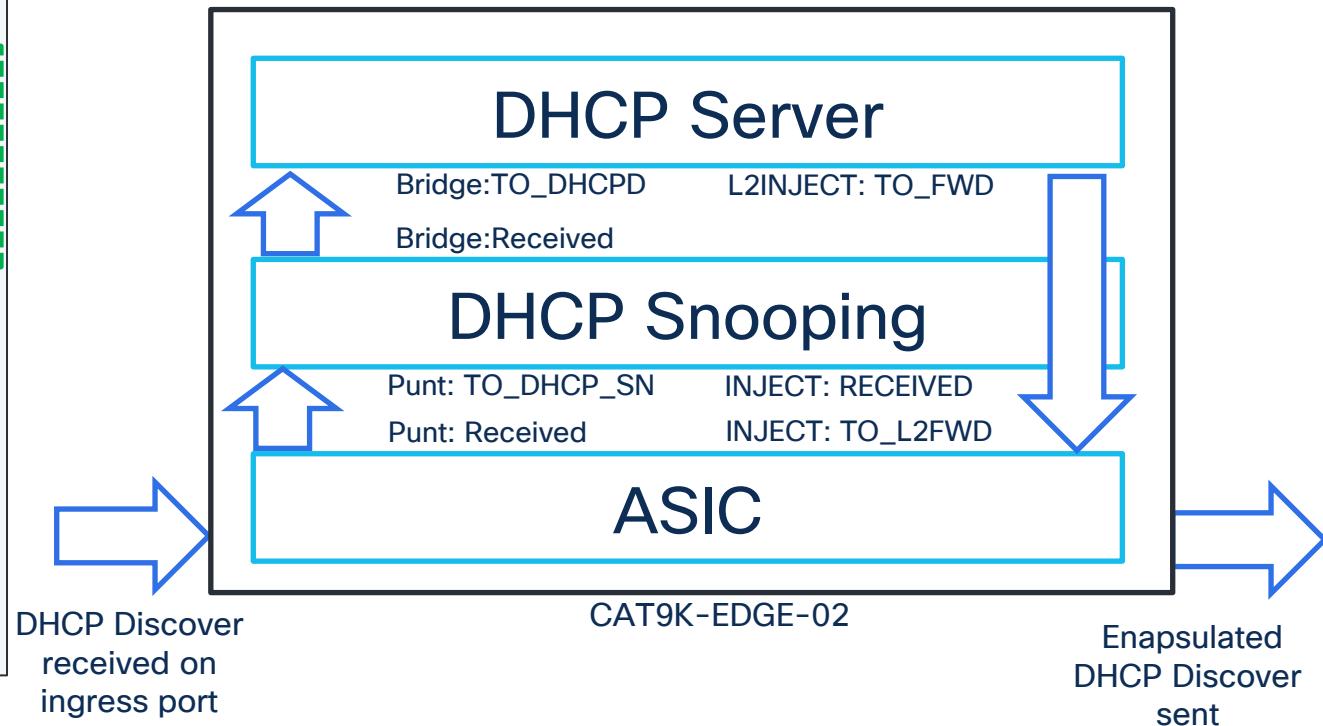
CLI outputs gathered simultaneously from all devices.

Catalyst Center: Network Troubleshooting (DHCP)

CAT9K-EDGE-02

Timestamp	Destination MAC	Destination Ip	VLAN	Message	Handler:Action
2025/01/12 11:23:34.263	FFFF.FFFF.FFFF	255.255.255.255	1020	DHCPDISCOVER(B)	PUNT:RECEIVED
2025/01/12 11:23:34.263	FFFF.FFFF.FFFF	255.255.255.255	1020	DHCPDISCOVER(B)	PUNT:TO_DHCP_SN
2025/01/12 11:23:34.264	FFFF.FFFF.FFFF	255.255.255.255	1020	DHCPDISCOVER(B)	BRIDGE:RECEIVED
2025/01/12 11:23:34.264	FFFF.FFFF.FFFF	255.255.255.255	1020	DHCPDISCOVER(B)	BRIDGE:TO_DHCPD
2025/01/12 11:23:34.264	FFFF.FFFF.FFFF	255.255.255.255	1020	DHCPDISCOVER(B)	BRIDGE:TO_INJECT
2025/01/12 11:23:34.264	FFFF.FFFF.FFFF	255.255.255.255	1020	DHCPDISCOVER(B)	L2INJECT:TO_FWD
2025/01/12 11:23:34.265	0100.0CCC.CCCC	100.64.0.100	0	DHCPDISCOVER(B)	INJECT:RECEIVED
2025/01/12 11:23:34.265	0100.0CCC.CCCC	100.64.0.100	0	DHCPDISCOVER(B)	INJECT:TO_L2FWD
2025/01/12 11:23:35.267	FFFF.FFFF.FFFF	192.168.10.254	1020	DHCPOFFER(B)	PUNT:RECEIVED
2025/01/12 11:23:35.267	0200.0000.0000	255.255.255.255	0	DHCPOFFER(B)	INJECT:RECEIVED
2025/01/12 11:23:35.267	FFFF.FFFF.FFFF	255.255.255.255	0	DHCPOFFER(B)	INTERCEPT:RECEIVED
2025/01/12 11:23:35.267	FFFF.FFFF.FFFF	255.255.255.255	1020	DHCPOFFER(B)	INTERCEPT:TO_DHCPSN
2025/01/12 11:23:35.269	FFFF.FFFF.FFFF	255.255.255.255	1020	DHCPREQUEST(B)	PUNT:RECEIVED
2025/01/12 11:23:35.269	FFFF.FFFF.FFFF	255.255.255.255	1020	DHCPREQUEST(B)	PUNT:TO_DHCP_SN
2025/01/12 11:23:35.272	FFFF.FFFF.FFFF	255.255.255.255	1020	DHCPREQUEST(B)	BRIDGE:RECEIVED
2025/01/12 11:23:35.272	FFFF.FFFF.FFFF	255.255.255.255	1020	DHCPREQUEST(B)	BRIDGE:TO_DHCPD
2025/01/12 11:23:35.272	FFFF.FFFF.FFFF	255.255.255.255	1020	DHCPREQUEST(B)	BRIDGE:TO_INJECT
2025/01/12 11:23:35.272	FFFF.FFFF.FFFF	255.255.255.255	1020	DHCPREQUEST(B)	L2INJECT:TO_FWD
2025/01/12 11:23:35.272	0000.0000.0000	100.64.0.100	0	DHCPREQUEST(B)	INJECT:RECEIVED
2025/01/12 11:23:35.272	0000.0000.0000	100.64.0.100	0	DHCPREQUEST(B)	INJECT:TO_L2FWD
2025/01/12 11:23:35.276	FFFF.FFFF.FFFF	192.168.10.254	1020	DHCPCPACK(B)	PUNT:RECEIVED
2025/01/12 11:23:35.276	FFFF.FFFF.FFFF	255.255.255.255	0	DHCPCPACK(B)	INJECT:RECEIVED
2025/01/12 11:23:35.276	FFFF.FFFF.FFFF	255.255.255.255	0	DHCPCPACK(B)	INTERCEPT:RECEIVED
2025/01/12 11:23:35.276	FFFF.FFFF.FFFF	255.255.255.255	1020	DHCPCPACK(B)	INTERCEPT:TO_DHCPSN

DHCP Discover from the host Received and Sent out to DHCP Server



Catalyst Center: Network Troubleshooting (DHCP)

CAT9K-BORDER-01 & CAT9K-BORDER-02

CAT9K-BORDER-01.cisco.com (172.16.0.1) | sh platform dhcpsnooping client stats 7c21.0d1d.9ec6

```
sh platform dhcpsnooping client stats 7c21.0d1d.9ec6
DHCPDN: DHCP snooping server
DHCPD: DHCP protocol daemen
L2FWD: Transmit Packet to driver in L2 format
FWD: Transmit Packet to driver
<MessageType>(B): Dhcp message's response expected as 'B'broadcast
<MessageType>(U): Dhcp message's response expected as 'U'unicast
Packet Trace for client MAC 7C21.0D1D.9EC6:
Timestamp          Destination MAC  Destination Ip  VLAN  Message      Handler:Action
2025/01/12 11:23:35.265 3C51.0EE4.D8FF  192.168.10.254 122  DHCPOFFER(B)  PUNT:RECEIVED
2025/01/12 11:23:35.265 3C51.0EE4.D8FF  192.168.10.254 123  DHCPOFFER(B)  LISP:GLEAN
2025/01/12 11:23:35.274 3C51.0EE4.D8FF  192.168.10.254 122  DHCPACK(B)   PUNT:RECEIVED
2025/01/12 11:23:35.274 3C51.0EE4.D8FF  192.168.10.254 123  DHCPACK(B)   LISP:GLEAN
CAT9K-BORDER-01#
```

DHCP Offer/ACK packet from DHCP Server seen on **BORDER-01** (towards EDGE)

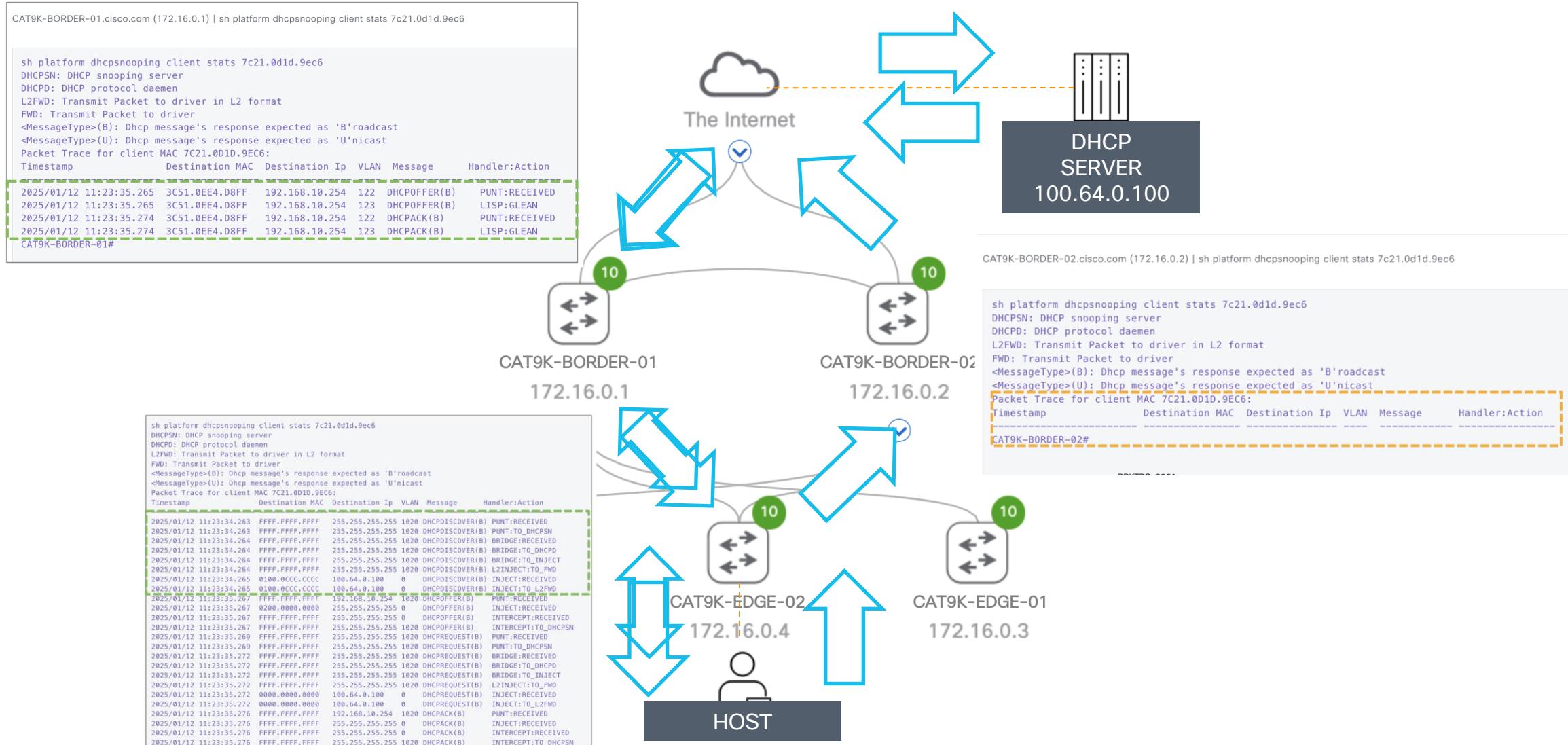
CAT9K-BORDER-02.cisco.com (172.16.0.2) | sh platform dhcpsnooping client stats 7c21.0d1d.9ec6

```
sh platform dhcpsnooping client stats 7c21.0d1d.9ec6
DHCPDN: DHCP snooping server
DHCPD: DHCP protocol daemen
L2FWD: Transmit Packet to driver in L2 format
FWD: Transmit Packet to driver
<MessageType>(B): Dhcp message's response expected as 'B'broadcast
<MessageType>(U): Dhcp message's response expected as 'U'unicast
Packet Trace for client MAC 7C21.0D1D.9EC6:
Timestamp          Destination MAC  Destination Ip  VLAN  Message      Handler:Action
CAT9K-BORDER-02#
```

No DHCP Offer/ACK packets from DHCP Server seen on **BORDER-02**.

Catalyst Center: Network troubleshooting (DHCP)

Example of DHCP packet flow



Network troubleshooting (DHCP)

Tip #3b: Utilise “Run Commands” for Embedded Packet Capture (EPC).

The screenshot shows the Cisco Catalyst Center interface. On the left, the 'DEVICE WORK ITEMS' sidebar lists various device status filters. In the center, the 'Devices (5)' list shows four devices: CAT9K-BORDE, CAT9K-EDGE-, CAT9K-EDGE-, and CAT9K-EDGE-. The 'CAT9K-EDGE-' device is selected, indicated by a green circle with the number 1. The 'Actions' dropdown menu for this device is open, with the 'Run Commands' option highlighted by a green circle with the number 4. A callout box with a green border and a blue border contains the text: 'A packet capture performed on the device to verify the DHCP packet has been sent/received on a specific interface.' The 'Run Commands' window shows the output of a packet capture for a DHCP transaction, with the transaction ID 0x9a1d13f and other details.

A packet capture performed on the device to verify the DHCP packet has been sent/received on a specific interface.

```
Note: You can enter "man" anytime to get the list of currently supported commands and shortcuts.  
CAT9K-EDGE-02.cisco.com> monitor capture CAP interface g1/0/12 in match any buffer size 10 start  
CAT9K-EDGE-02.cisco.com> monitor capture CAP stop  
Capture statistics collected at software:  
Capture duration - 52 seconds  
Packets received - 12  
Packets dropped - 0  
Packets oversized - 0  
Bytes dropped in asic - 0  
Capture buffer will exists till exported or cleared  
Stopped capture point : CAP  
CAT9K-EDGE-02.cisco.com> show monitor capture CAP buffer display-filter dhcp brief  
Starting the packet display ..... Press Ctrl + Shift + 6 to exit  
3 13.078715 0.0.0.0 -> 255.255.255.255 DHCP 373 DHCP Discover - Transaction ID 0x9a1d13f  
4 16.882267 0.0.0.0 -> 255.255.255.255 DHCP 373 DHCP Discover - Transaction ID 0x9a1d13f  
6 20.882322 0.0.0.0 -> 255.255.255.255 DHCP 373 DHCP Discover - Transaction ID 0x9a1d13f  
8 38.051522 0.0.0.0 -> 255.255.255.255 DHCP 373 DHCP Discover - Transaction ID 0x7bbbc0bd  
10 41.883317 0.0.0.0 -> 255.255.255.255 DHCP 373 DHCP Discover - Transaction ID 0x7bbbc0bd  
12 45.883510 0.0.0.0 -> 255.255.255.255 DHCP 373 DHCP Discover - Transaction ID 0x7bbbc0bd
```

SD-Access: Triaging Fabric & Network issues

Key takeaways:

- 1. Check the basics:** Verify that the correct configuration has been applied to all devices and that Catalyst Center is fully in sync with the Network.
- 2. Assurance:** Verify recent changes in the fabric configuration (working vs non-working setup), compliance, check health of the devices/fabric/VNs and reported issues.
- 3. Bugs:** Scan your network for potential well-known defects.
- 4. Network troubleshooting:** Utilise existing tools, such as Command Runner, to more effectively validate the network's state (multiple CLIs & multiple devices at once)

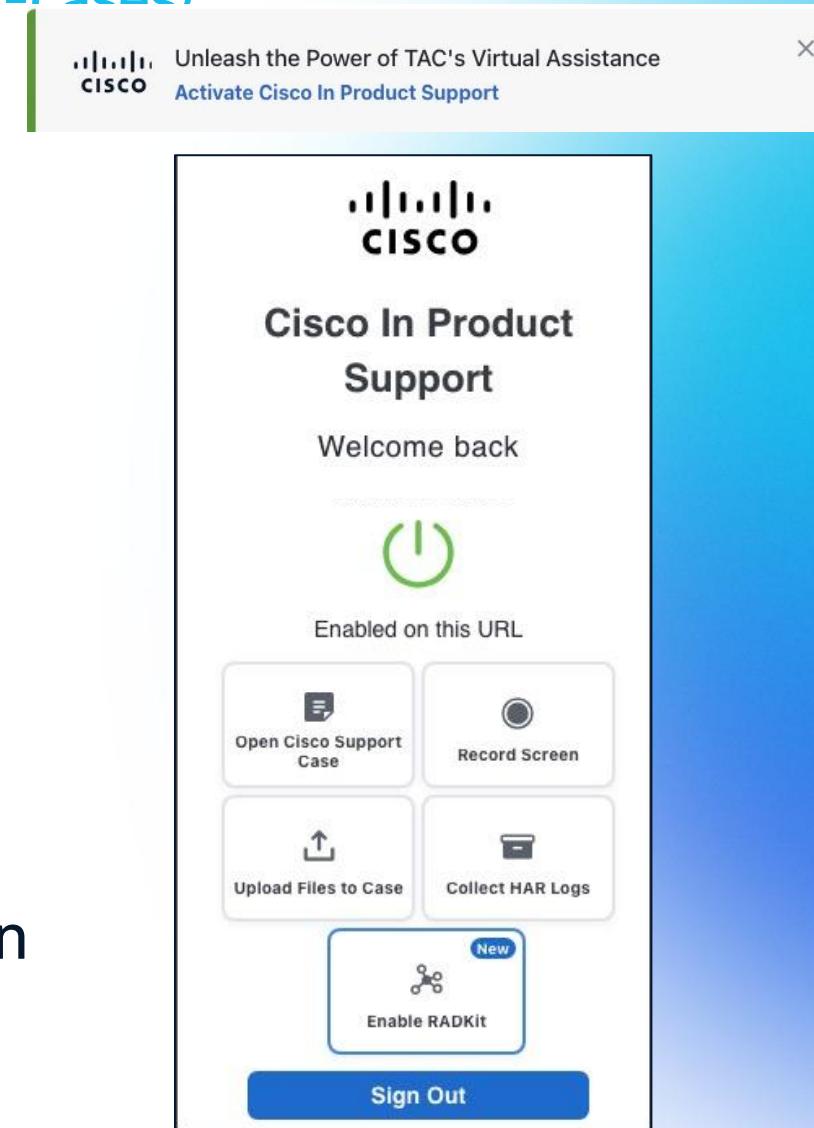
Additional Tool – In Product Support Assistant Extension

Cisco In Product Support Assistant Extension

<https://inproductexperience.cisco.com/docs/catalyst-center/use-cases/>

Cisco In Product Support Assistant allows following:

- Open Cisco TAC case directly from Cisco Catalyst Center UI.
- ‘Record screen’ activities, for sharing with TAC.
- Collect HAR(HTTP ARchive format) Logs for Cisco Catalyst Center UI Troubleshooting.
- Upload files to the existing/new TAC SR case (max 5GB).
- Enable RADKit(<https://radkit.cisco.com/>) using built in Remote Support Authorisation on Catalyst Center.



<https://go2.cisco.com/IPS>

Session Summary

Learn new techniques, tools (**Grafana**, **Kibana**) and useful tips and tricks (**20+ tips**) to further boost your troubleshooting proficiency whether you are tackling issues independently (**3 most common use-cases for Catalyst Center & SD-Access**) or collaborating with Cisco TAC (**In Product Support Assistant Extension**)



Complete your session evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a Cisco Live T-Shirt.



Earn up to 800 points by completing all surveys and climb the Cisco Live Challenge leaderboard.



Level up and earn exclusive prizes!



Complete your surveys in the Cisco Live Events app.

Continue your education



Visit the Cisco Stand for related demos



Book your one-on-one Meet the Expert meeting



Attend the interactive education with Capture the Flag, and Walk-in Labs



Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Contact me at: choiwon@cisco.com

CISCO Live !

