

Mastering Troubleshooting with Cisco Catalyst Center and SD-Access

CISCO Live !

Won Je Choi
Technical Leader

Cisco Webex App

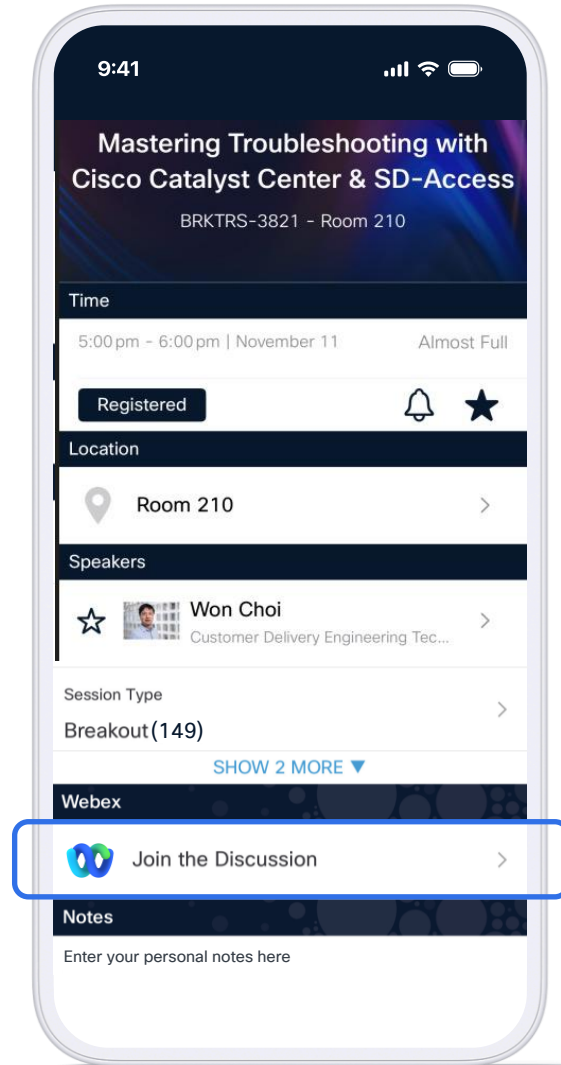
Questions?

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.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKTRS-3821>



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.

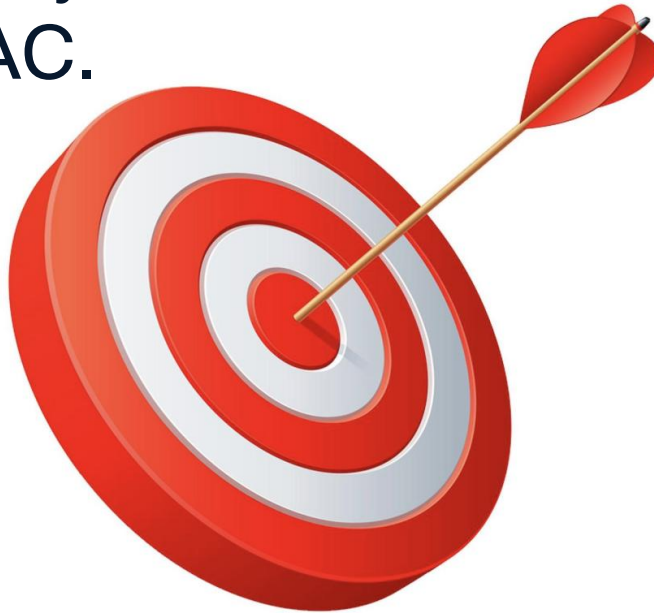
Korean-Australian, Dad to 12-year-old daughter and 9-year-old son; Home Weight Training.

Total 534Km of Ekahau Survey Distance 😊

Filter Results						
Total Survey Events	Total Time	Total Distance	Total APs	Average Time	Average Distance	Average Speed
807	310 h 4 min	866.81 km	175996	22 h 9 min	61.92 km	2.79 km/h
For a normal site survey, Sidekick 2 is fast enough so that it will collect sufficient data at speeds up to 10 km/h. Take a scooter next time if you can.						
Users		Total Survey Events	Total Time	Total Distance ↓	Speed	
WC	Won Choi	435	179 h 40 min	534.77 km	3 km/h	

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

Cisco Catalyst Center

Version 2.3.7.9-70301

[Release Notes](#)

[> Packages](#)

[v 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

Global

AllRoutersSwitchesWireless ControllersAccess PointsSensors

Devices (5)

Focus: Inventory

Take a tourExport

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

0 SelectedTagAdd DeviceEdit DeviceDelete DeviceActions

As of: Jan 2, 2025 10:47 AM

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 Sync Details

Catalyst Center: Inventory Troubleshooting Workflow and issue triage



1 Device Reachability

1a) Validate reachability using “Run Commands” Tool from the Catalyst Center UI.

2 Manageability (Credentials)

2a) Review and Validate credentials using “Edit Device”
2b) Execute UI Inventory Re-sync operations.
2c) Execute API (force) re-sync operations.

3 Monitoring/Grafana (Logs and Database Insights)

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 displays the Catalyst Center interface with a 'Command Runner' window open. The interface includes a top navigation bar, a left sidebar with a 'Global' filter, and a main table of devices. The 'Command Runner' window shows a list of supported commands: man, connect, ping, traceroute, and snmpget, each with its usage instructions. The device table lists five devices, with the first two highlighted by green dashed boxes and numbered 1 and 2. A green circle with the number 3 is placed over the 'Run Commands' button in the 'More' dropdown menu. A blue arrow points from the 'Run Commands' button to the 'Command Runner' window, which is also marked with a green circle and the number 4. A text box at the bottom right contains the text: 'Basic checks (Maglev CLI) are available directly from Catalyst Center UI: Ping, Traceroute, SNMP, connect'. A text box at the bottom left contains the text: 'CTRL+E - Exports the current command history as a text file' and 'CTRL+F - Search within the window for a keyword/phrase'.

Command Runner

```
$ 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 [-LRUbdnfrvVaAB] [-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 {{ipv4-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 informati
on and an OID. Example: snmpget -v 1 -c democisco test.net-snmp.org system.sysUpTime.0 (where, system.sysUpTime.0 = Tim
eticks: (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
$
```

Tags	Device Name	IP Address	Inventory
<input type="checkbox"/>	CAT9K-BORDER-01.cisco.com	172.16.0.1	Software Image
<input type="checkbox"/>	CAT9K-BORDER-02.cisco.com	172.16.0.2	Provision
<input type="checkbox"/>	CAT9K-EDGE-01.cisco.com	172.16.0.3	Telemetry
<input type="checkbox"/>	CAT9K-EDGE-02.cisco.com	172.16.0.4	Device Replacement
<input type="checkbox"/>	CAT9K-EDGE-03.cisco.com	172.16.0.5	Switch Refresh

1 alert Managed Compliant .../Krakow/KRK04 17.12.2 12 minutes ago Sync Details FCW2339G

3 minutes ago Sync Details FCW2339C

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

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**

The image shows a screenshot of the Catalyst Center interface. On the left, a table lists devices. The first device, 'CAT9K-BORDER-01.cisco.com' with IP '172.16.0.1', is selected. A green dashed box highlights the 'Actions' menu, which contains 'Inventory' and 'Edit Device'. A green circle with the number '1' is next to the selection checkbox, '2' is next to 'Edit Device', and '3' is next to the 'Edit Device' button. A blue callout box points to the 'Edit Device' button with the text: 'Ensure that you validate credentials for all connectivity methods.' Below this, another blue callout box points to the 'Edit Device' form with the text: 'Make sure that all configured connection methods are successful.'

Edit Device

Credentials Management IP Resync Interval Device Role

Network Device

Credentials **Validate** 4

Note: CLI and SNMP credentials are mandatory. Please ensure authenticity of credentials. In case of invalid credentials, device will go into a collection failure state.
Changing the device credentials will impact the device's configuration.

CLI* 5

Global credentials are provided only for ease of use when entering credentials. At the device level, only the device-specific credentials are saved.
The device-to-global-credentials association isn't saved.

☒ Select global credential ☐ Add device specific credential

Credential*
dnacadmin

> SNMP* 5

> SNMP Retries and Timeout*

> HTTP(S)

> NETCONF* 5

Catalyst Center: Manageability

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

The screenshot shows the Cisco Catalyst Center web interface. At the top, the navigation bar includes the Cisco logo, the text 'Catalyst Center', and the breadcrumb 'Provision / Inventory'. Below this is a warning banner about provisioning subscriptions. The main content area shows a list of devices under the 'Inventory' focus. One device, 'CAT9K-BORDER-02.cisco.com', is selected. The 'Actions' menu is open, showing options like 'Inventory', 'Software Image', 'Provision', 'Telemetry', 'Device Replacement', 'Switch Refresh', 'Compliance', and 'More'. The 'Resync Device' option is highlighted. A callout box explains the purpose of this action.

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

Global Routers Switches Wireless Controllers Access Points Sensors

Devices (5) Focus: Inventory ▾

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

1 Selected Tag **Actions**

Tags	Device Name	IP Address	Inventory	Manageability	Compliance
<input type="checkbox"/>	CAT9K-BORDER-01.cisco.com	172.16.0.1		Unreachable	Non-Compliant
<input checked="" type="checkbox"/>	CAT9K-BORDER-02.cisco.com	172.16.0.2		Managed	Compliant
<input type="checkbox"/>	CAT9K-EDGE-01.cisco.com	172.16.0.3		Managed	Compliant
<input type="checkbox"/>	CAT9K-EDGE-02.cisco.com	172.16.0.4			
<input type="checkbox"/>	CAT9K-EDGE-03.cisco.com	172.16.0.5	Cisco	Reachable	

Manually re-sync device to update Catalyst Center and repopulate internal database structures.

Catalyst Center: Manageability – Device re-sync progress

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

0 Selected Tag Add Device Edit Device Delete Device Actions

Tags	Device Name	IP Address	Vendor	Reachability	EoX Status	Manageability	Compliance	Site	Image Version	Last Updated
	CAT9K-BORDER-01.cisco.com	172.16.0.1	Cisco	Unreachable	1 alert	Managed Device Unreachable	Non-Compliant	.../Krakow/KRK04	17.12.2	37 minutes ago Sync Details
	CAT9K-BORDER-02.cisco.com	172.16.0.2				Managed	Compliant	.../Krakow/KRK04	17.12.2	13 hours 40 minutes ago Sync Details
	CAT9K-EDGE-01.cisco.com	172.16.0.3				Managed	Compliant	.../Krakow/KRK04	17.12.2	42 minutes ago Sync Details
	CAT9K-EDGE-02.cisco.com	172.16.0.4				Managed Syncing...	Compliant	.../Krakow/KRK04	17.12.2	22 minutes ago Sync Details
	CAT9K-EDGE-03.cisco.com	172.16.0.5				Managed	Compliant	.../Krakow/KRK04	17.12.2	2 hours 31 minutes ago Sync Details

Resync request(s) pending in queue.

Ongoing Sync Details

Start Time

1 minute ago

Reason(s)

User Requested

Requested by Application

Inventory

Previous Sync Details

Start Time

23 minutes ago

Reason(s)

Config Change Event

1

2

Check resync status to get high-level information about its progress.

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 Cisco Catalyst Center web interface. On the left, the navigation menu is open, with 'Platform' highlighted (1) and 'Developer Toolkit' selected (2). The main content area shows the 'Sync Devices' API endpoint (4) under the 'Know Your Network' section. A search bar (3) contains the text 'sync device'. A blue callout box on the right contains the text: 'Force re-sync to assign sync task to a high priority thread.'

Platform / Developer Toolkit

Capabilities and try them out for yourself

or test different APIs in your network environment to build, of Catalyst Center.

sync device

Know Your Network

Know your Network APIs can be used to discover details about clients, sites, topology and devices. It also provides programmatic REST APIs to add devices to the network and export device data.

Devices

Method	Name	Description
PUT	Sync Devices	Synchronizes the device (default) then the sync v If forceSync param is tru priority thread if availabl be seen in the child task of each device

Catalyst Center: Manageability – force re-sync via API

Sync Devices

×

PUThttps://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

ParametersRequest BodyResponsesCode Preview

1

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

NameSchemaSample

Content-Type1 - ["string"23]

2

Name	Description	DataType	Required	Default Value
forceSync	forceSync	boolean	No	false

3

Try

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* ⓘ
application/json

QUERY PARAMETERS

☒ Unselect All

1 ☒ forceSync
true

REQUEST BODY

2 ["360365"]

Device ID

Response Headers Status Code: 202

3

```
1 {  
2   "response": {  
3     "taskId": "01942678-e9a9-76ff-9cea-65fa48a976eb",  
4     "url": "/api/v1/task/01942678-e9a9-76ff-9cea-65fa48a976eb"  
5   },  
6   "version": "1.0"  
7 }
```

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

Reset Run

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

id* 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

Pretty print ☒

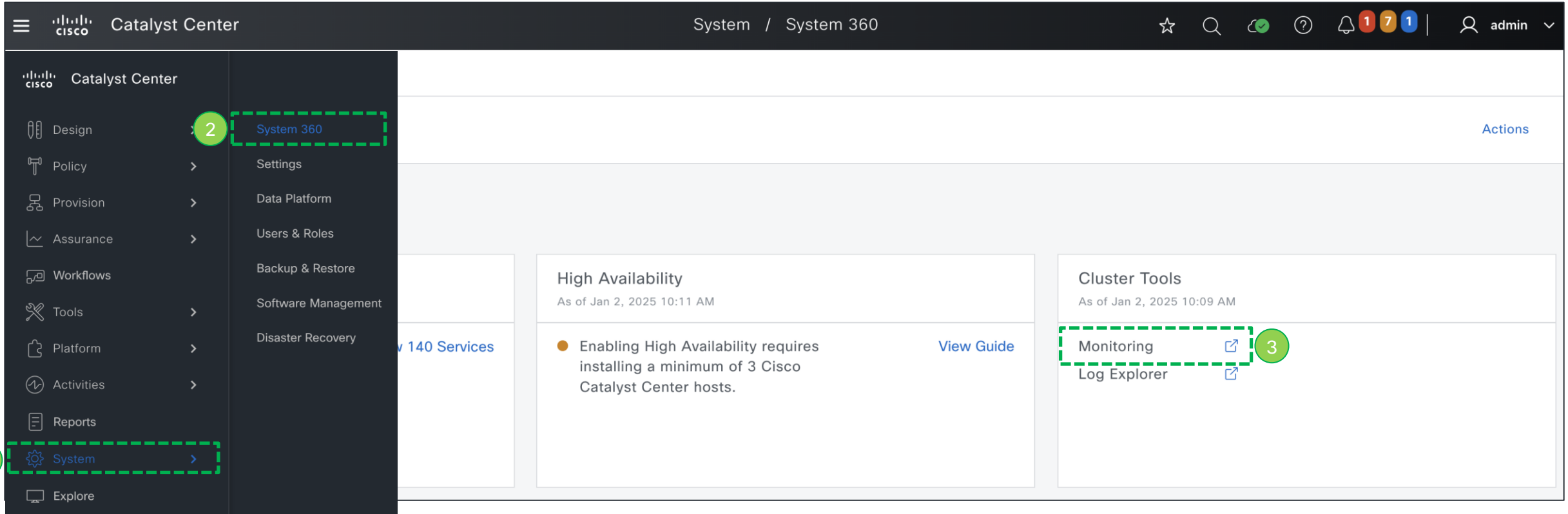
```
{  
  "response": {  
    "endTime": 1735812247026,  
    "progress": "Synced devices: [360365]",  
    "version": 1735812247026,  
    "startTime": 1735812245929,  
    "lastUpdate": 1735812245940,  
    "serviceType": "Inventory service",  
    "isError": false,  
    "instanceTenantId": "66b5099a76ad844d00f49697",  
    "id": "01942678-e9a9-76ff-9cea-65fa48a976eb"  
  },  
  "version": "1.0"  
}
```

Reset

Run

Catalyst Center: Logs and Database Insights (Grafana)

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



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

Catalyst Center: Logs and Database Insights (Grafana)

The screenshot displays the Cisco Catalyst Center Grafana interface. The top navigation bar includes the Cisco logo, the text 'Catalyst Center', and several utility icons (star, search, status, help, notifications) with notification counts (1, 7, 1). A search bar on the left is labeled 'Search dashboards' and is highlighted with a blue dashed box and a green circle with the number '1'. The main dashboard area is a grid of service-specific dashboards, including 'Access Control Application', 'AI Endpoint Analytics', 'API Source ID Metrics', 'Appstack', 'Assurance - Capture File Purg', 'Assurance - Device Processor', 'Assurance - gRPC Collector', 'Cluster', 'Cluster Events', 'Cluster Overview', 'Compliance', 'Data Platform', 'Data Platform - Aggregati', 'Data Platform - Async Co', 'Data Platform - Broker Pe', 'Grouping', 'InfluxDB Metrics Detailed', 'Inventory' (highlighted with a green dashed box and a green circle with the number '2'), 'Kafka', 'Kong', 'Logging Overview', 'MongoDB', 'PNP', 'Pods', 'Policy Assurance - P', 'Postgres Ext', 'Postgres Query' (highlighted with a green dashed box), 'Postgres L', 'SWIM', 'Syslog Pipelines', 'System Services', 'Systemd Services', 'Task Metrics Dashboard', and 'Telegraf'. A blue callout box at the top right states: 'Multiple dashboards are available for a variety of Catalyst Center services.' A blue callout box at the bottom right states: 'Postgres Queries can be also executed here as instructed by Cisco TAC.'

1 Search dashboards

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

2 Inventory

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.

Catalyst Center: Logs and Database Insights (Grafana)

Select the device to troubleshoot.

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

id	hostname	type	collectionstatus	reachabilitystatus	inventorystatusdetail	errorcode	devicesupportlevel	collectioninterv	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

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

Basic Stats

Devices

Family	Total
Switches and Hubs	5

Life Cycle State

Life Cycle Stat	Total
	3
	5

Inventory Status Detail

Status Detail	Total
<status>	

GRT Size

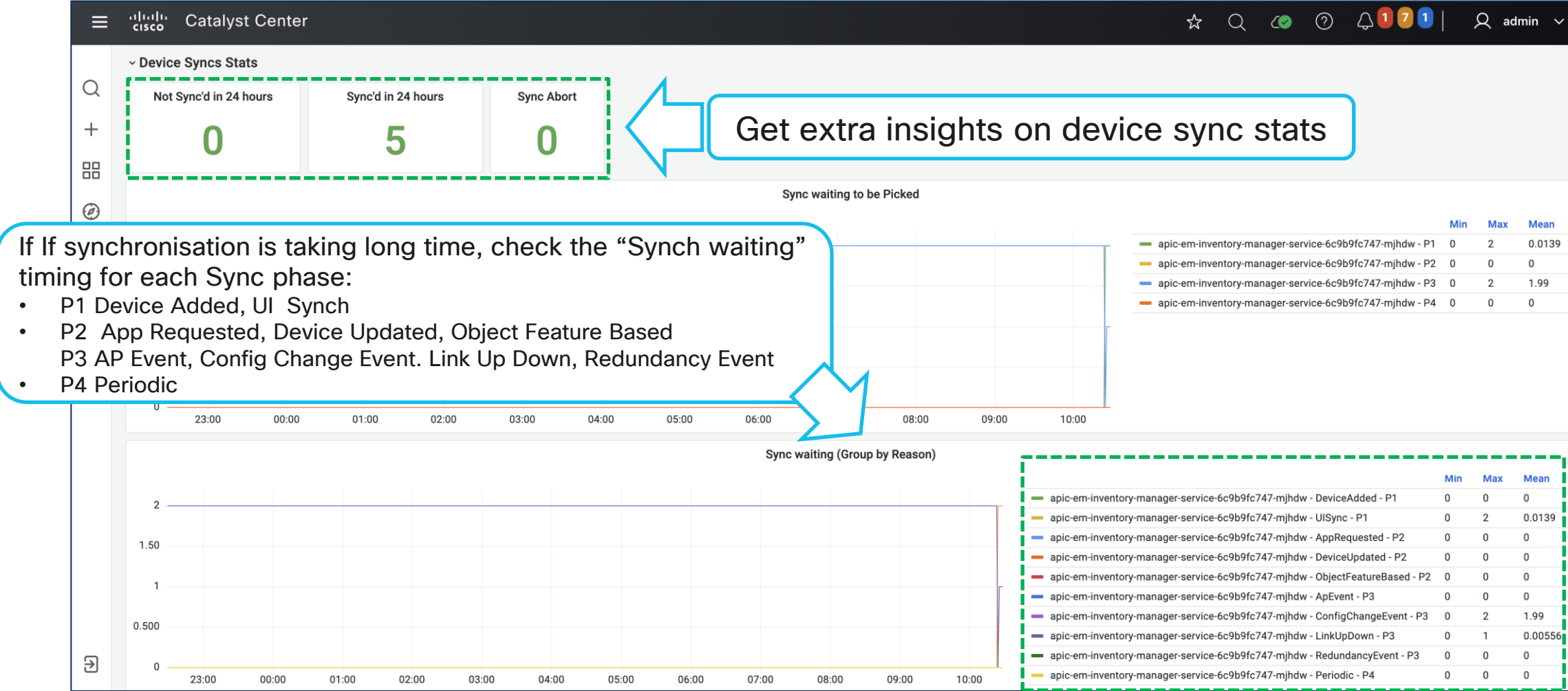
Size Range	Count
1 - 500	2
3001-4000	3
4001-5000	0

Interfaces

Stats

Device Operations

Catalyst Center: Logs and Database Insights (Grafana)



Catalyst Center: Logs and Database Insights (Grafana)

The screenshot displays the Catalyst Center Grafana dashboard. The top navigation bar includes the Cisco logo, 'Catalyst Center' text, and user 'admin'. The left sidebar shows navigation icons. The main content area is titled 'General / Inventory'. A green dashed box highlights the 'Key logs - 360361 (172.16.0.1)' link, with an arrow pointing to it from a blue box containing the text 'Check key logs for a given device.' Another green dashed box highlights the 'Last 12 hours' time range filter, with an arrow pointing to it from a blue box containing the text 'Specify time range.' Below these, another green dashed box highlights the 'All Logs - 360361 (172.16.0.1)' link, with an arrow pointing to it from a blue box containing the text 'Check all logs for a given device.' The log entries are displayed in a table format with columns for timestamp, log level, component, and message.

Key logs - 360361 (172.16.0.1)

Timestamp	Log Level	Component	Message
> 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:
> 2025-01-02 06:57:22,085	INFO	ICE Service - CPU 5	com.cisco.xmp.inventory For deviceid:360361, statusMessage:<status><general code="SUCCESS"/></status>, s
> 2025-01-02 06:57:21,222	INFO	ICE Service - Network 9	com.cisco.xmp.inventory Interim status after execution of devicePackage SUCCESS deviceId: 360361; Creden
> 2025-01-02 06:57:20,568	INFO	XDE ThreadPool 2	com.cisco.xmp.inventory getDeviceSize for deviceId: 360361 got result map as: {wirelesspoints=0, proto
> 2025-01-02 06:57:19,955	INFO	ICE Service - Network 9	com.cisco.xmp.inventory 360361: Previous collection status MANAGED_AND_SYNCHRONIZED mid=2, MSGNAME=XICE
> 2025-01-02 06:57:19,518	INFO	ICE Service - CPU 1	com.cisco.xmp.inventory For deviceid:360361, statusMessage:<status><general code="SUCCESS"/></status>, successLifeEnum:MANAGED_AND_SYNCHRONIZED mid=2, MSGN
> 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:
> 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, MSG
> 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
> 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

All Logs - 360361 (172.16.0.1)

Timestamp	Log Level	Component	Message
> 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=information
> 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 06:5
> 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_I
> 2025-01-02 06:57:22,418	INFO	ICE Service - CPU 5	com.cisco.xmp.inventory Going to fetch the meiId:360361 with operationType:SYNC_OPERATION_INDEPENDENT mid=2, MSGNAME=XICE_GENERIC_MSG_INF_02, ch=com.cisc
> 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.PostCollecti
> 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

Log Pattern: Enter variable value

Log Level: Enter variable value

Device IP: 172.16.0.1

Device Id: 360361

Selected (2)

- ☐ All
- ☒ ERROR
- ☒ WARN
- ☐ INFO
- ☐ DEBUG

id	hostname	type
360361	CAT9K-BORDE...	Cisco Catalyst C9500-2

Basic Stats

reachabilitystatus: Reachable

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

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

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

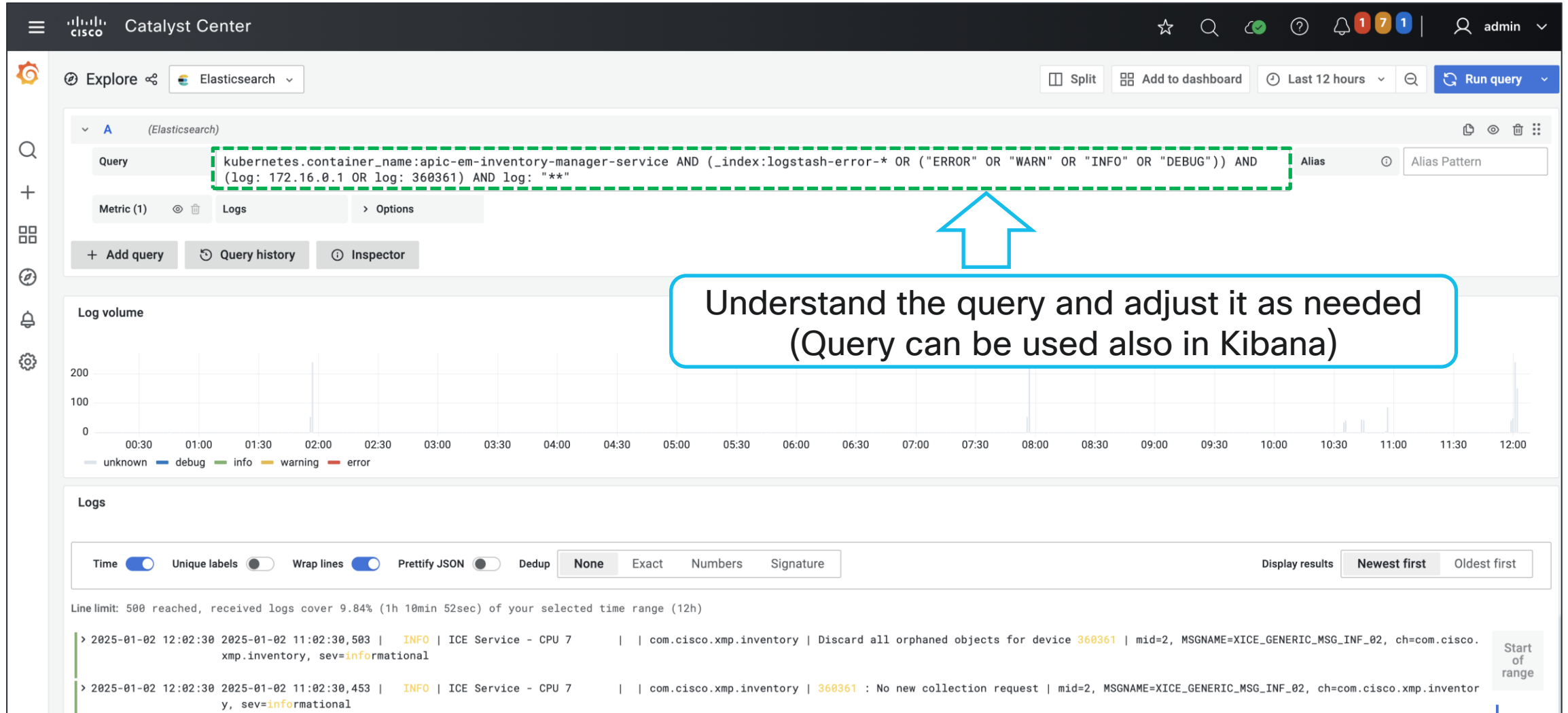
All Logs - 360361 (172.16.0.1)

ERROR + WARN Logs

```
> 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_L  
EVEL. | 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_L  
EVEL. | 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)



Catalyst Center: Logs and Database Insights (Grafana)

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

1

select * from networkde

Specify DB query (as provided by Cisco TAC)

2

Query Output

3

Data

Inspect: Query Output

1 queries with total query time of 339 ms

Data

Stats

JSON

Query

>

Data options

Formatted data

4

Download CSV

id	instanceuuid	hostname	managementipad	type	family	series	...
360361	f9bf3ac4-5916-4f83...	CAT9K-BORDER-01....	172.16.0.1	Cisco Catalyst C95...	Switches and Hubs	Cisco Catalyst 9500...	17.1...

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

Cisco

Catalyst Center

Provision / SD-Access

☆

🔍

🔄

?

🔔

2

7

3

admin

▼

Fabric Sites / KRK04

KRK04

View Site Hierarchy

Site Actions

📄

Fabric Infrastructure

Layer 3 Virtual Networks

Layer 2 Virtual Networks

Anycast Gateways

Wireless SSIDs

Authentication Template

Port Assignment

🔗

☰

SUMMARY

> Device Family (1)

> Reachability (1)

> Compliance Status (1)

> Provision Status (1)

☐ Success

> Fabric Role (3)

☐ Control Plane Node

☐ Border Node

☐ Edge Node

PORT ATTRIBUTES

Devices (5)

📄 Export

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

0 Selected

Tag

More Actions

As of: Jan 2, 2025 5:05 PM

☐	Tags	Device Name	IP Address	Fabric Role	Fabric Zone	Reachability	Fabric Provisioning Status	Compliance Status
☐	🔗	CAT9K-BORDER-01.cisco.com	172.16.0.1	BN CP	--	🟢 Reachable	Success	🟢 Compliant
☐	🔗	CAT9K-BORDER-02.cisco.com	172.16.0.2	BN CP	--	🟢 Reachable	Success	🟢 Compliant
☐	🔗	CAT9K-EDGE-01.cisco.com	172.16.0.3	EN	--	🟢 Reachable	Success	🟢 Compliant
☐	🔗	CAT9K-EDGE-02.cisco.com	172.16.0.4	EN	--	🟢 Reachable	Success	🟢 Compliant
☐	🔗	CAT9K-EDGE-03.cisco.com	172.16.0.5	EN	--	🟢 Reachable	Success	🟢 Compliant

5 Record(s)

Show Record

Standard view and typical provisioning issues (SDA provisioning errors)

Error

Unable to push to device 172.16.0.1
using protocol ssh2 the CLI vrf
definition DEVICE_VN

FlowId: d3bbb67a-dc5f-44ca-9788-d09c127adefa

Catalyst Center: Provisioning

Troubleshooting workflow and issue triage

1 Provisioning Workflow



2 Activity: Task



3 Log insights

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

Catalyst Center

Provision / Inventory

383

admin

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

✓ All

Routers

Switches

Wireless Controllers

Access Points

Sensors

DEVICE WORK ITEMS

☐ Unreachable

☐ Unassigned

☐ Untagged

☐ Failed Provision

☐ Non Compliant

☐ Outdated Software Image

☐ No Golden Image

☐ Failed Image Prechecks

☐ Under Maintenance

☐ Security Advisories

Devices

1

Focus: Provision

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

1 Selected Tag + Add Device Actions

Tags	Device Name	IP Address	Device Type	Provisioning Status	Credential Status	Last Provisioned
<input checked="" type="checkbox"/>	CAT9K-BORDER-01.cisco.com	172.16.0.1	Switch (WLC Capable)	Success	Success	16 hours ago
<input type="checkbox"/>	CAT9K-BORDER-02.cisco.com	172.16.0.2	Switch (WLC Capable)	Success	Success	16 hours ago
<input type="checkbox"/>	CAT9K-EDGE-01.cisco.com	172.16.0.3	Switch (WLC Capable)	Success	Success	16 hours ago
<input type="checkbox"/>	CAT9K-EDGE-02.cisco.com	172.16.0.4	Switches and Hubs (WLC Capable)	Success	Success	16 hours ago
<input type="checkbox"/>	CAT9K-EDGE-03.cisco.com	172.16.0.5	Switches and Hubs (WLC Capable)	Success	Success	16 hours ago

Recent Provisioning Results

As of: Jan 3, 2025 9:20 AM

Time: January 2, 2025 4:29 PM

Task: Device Controllability and Telemetry

Status: SUCCESS

Time: January 2, 2025 5:04 PM

Task: Fabric Provisioning

Status: FAILED

Error: Unable to push to device 172.16.0.1 using protocol ssh2 the CLI vrf definition DEVICE_VN

Device response: % Feature is not supported

Provisioning Status

Credential Status

Last Provisioned

2

See Details

Success

See Details

16 hours ago

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

BRKTRS-3821

CISCO

Catalyst Center: Activity – Tasks

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

1

Activities

2

Tasks

Task

Completed

Failed

3

Device Details

Provision Details

4

Task

Completed

Failed

Start

Jan 2, 2025 5:03 PM

Update

Jan 2, 2025 5:04 PM

End

Jan 2, 2025 5:04 PM

Device Name

CAT9K-BORDER-01.cisco.com

CAT9K-BORDER-02.cisco.com

CAT9K-EDGE-01.cisco.com

Status

FAILED

SUCCESS

SUCCESS

Total Time to Provision

Recent Provisioning Results

Time January 2, 2025 5:03 PM Task Fabric Provisioning Status ROLLBACK_SUCCESS Error Unable to push to device 172.16.0.1 using protocol ssh2 the CLI vrf definition DEVICE_VN

Catalyst Center

Activities / Tasks

☆ 🔍 ⚠️ ? 🔔 3 8 3 | 👤 admin

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

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

Search Table

Filter

Device Name

Status

Total Time to Provision

Catalyst Center: Activity – Audit Logs

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

The screenshot shows the Catalyst Center interface with the following elements highlighted by numbered callouts:

- 1:** The **Activities** link in the left-hand navigation menu.
- 2:** The **Audit Logs** link in the sub-menu.
- 3:** A specific log entry in the main table: "Jan 2, 2025 5:03 PM CET" with the description "Creating task schedule with description: Modifying Fabric a".
- 4:** The details view for the selected log entry, showing the Log ID "019427c2-5699-70c6-b901-93e7053f898c" and a "Copy Log Id to Clipboard" button.

The details view also displays the following information:

- Description:** Creating task schedule with description: Modifying Fabric a (border transit)
- User:** admin
- Destination:** SYSTEM
- Interface:** 7.64.73
- Source:** 7.64.73

A blue callout box with the text "Collect Log ID for further triage" points to the Log ID and the copy button.

```
[{"timestamp": "Jan 2, 2025 5:03 PM CET", "description": "Creating task schedule with description: Modifying Fabric a", "log_id": "019427c2-5699-70c6-b901-93e7053f898c"}, {"timestamp": "Jan 2, 2025 5:03 PM CET", "description": "Received preview request for Fabric Provisioning.", "log_id": "019427c1-99f8-7e31-8ab1-3f179e75b33c"}, {"timestamp": "Jan 2, 2025 5:03 PM CET", "description": "Creating task schedule with description: Modifying Fabric a", "log_id": "019427c1-9a8d-7099-9344-9ac6d4d7f513"}, {"timestamp": "Jan 2, 2025 5:01 PM CET", "description": "The request to learn device config for selected network device", "log_id": "019427c1-9a8d-7099-9344-9ac6d4d7f513"}, {"timestamp": "Jan 2, 2025 5:01 PM CET", "description": "The request to learn device config for selected network device", "log_id": "019427c1-9a8d-7099-9344-9ac6d4d7f513"}, {"timestamp": "Jan 2, 2025 5:00 PM CET", "description": "Received a request to create an IP pool group named MCA", "log_id": "019427c1-9a8d-7099-9344-9ac6d4d7f513"}, {"timestamp": "Jan 2, 2025 5:00 PM CET", "description": "Received a request to create an IP pool group named TRAN", "log_id": "019427c1-9a8d-7099-9344-9ac6d4d7f513"}]
```

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 displays the Cisco Catalyst Center web interface. The top navigation bar shows 'System / System 360' and a user profile 'admin'. The left sidebar contains a menu with the following items: Design, Policy, Provision, Assurance, Workflows, Tools, Platform, Activities, Reports, System (highlighted with a green dashed box and a green circle '1'), and Explore. The 'System' item is expanded, showing a sub-menu with 'System 360' (highlighted with a green dashed box and a green circle '2'), Settings, Data Platform, Users & Roles, Backup & Restore, Software Management, and Disaster Recovery. The main content area is divided into two panels. The left panel, titled 'High Availability', contains a bullet point: 'Enabling High Availability requires installing a minimum of 3 Cisco Catalyst Center hosts.' The right panel, titled 'Cluster Tools', contains a 'Monitoring' section with a 'Log Explorer' link (highlighted with a green dashed box and a green circle '3'). A blue arrow points from a text box at the bottom right to the 'Log Explorer' link.

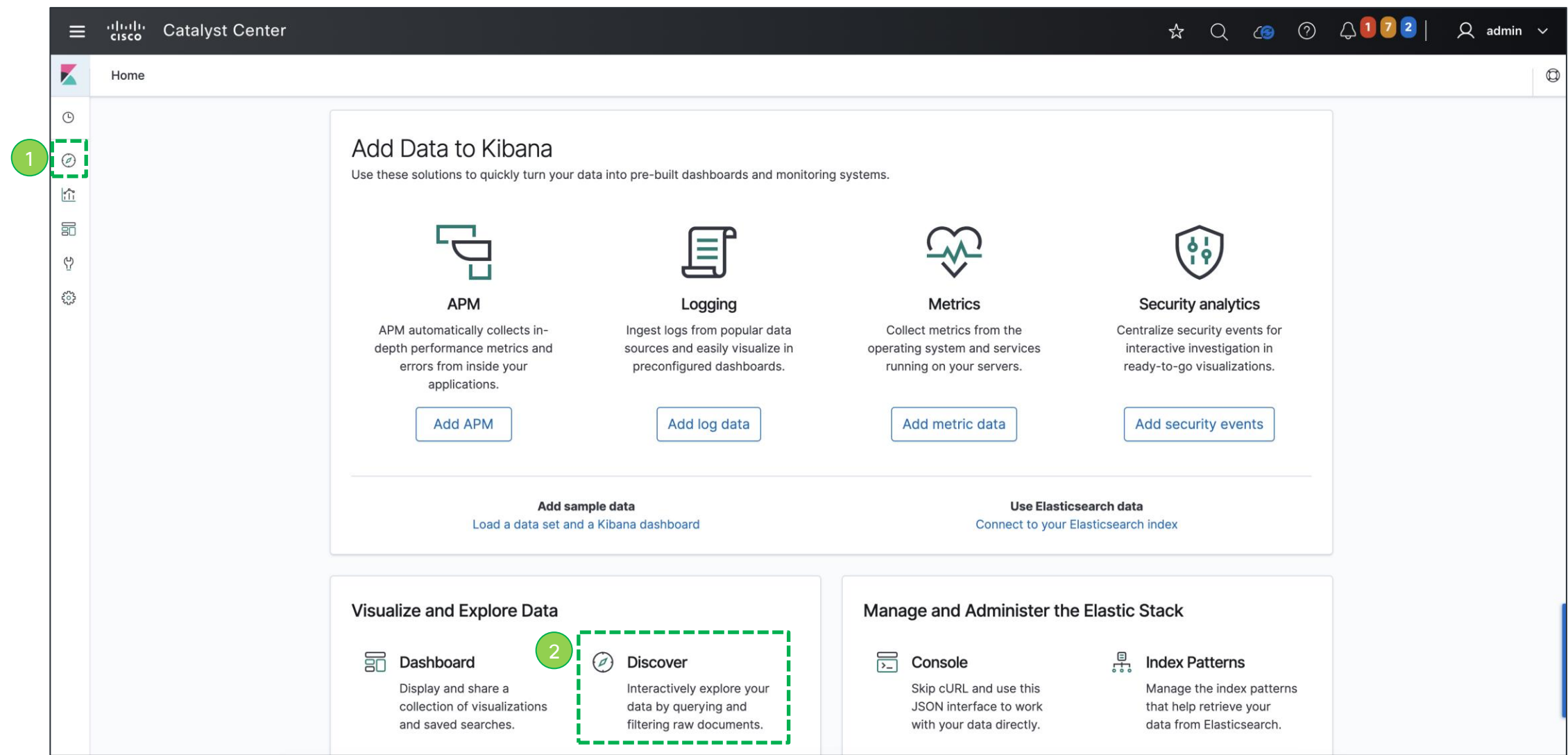
1

2

3

Navigate to Log Explorer for log analysis

Catalyst Center: Log Explorer (Kibana)



Catalyst Center: Log Explorer (Kibana)

The screenshot displays the Catalyst Center Log Explorer interface. It includes a sidebar with a 'Discover' section showing 71 hits. The main area features a search bar, a time range selector, a field selector, and a list of log messages. Four numbered callouts highlight specific features:

- Filter logs by specifying specific Log ID.** This callout points to the 'Filters' field, which contains the Log ID: "019427c2-5699-70c6-b901-93e7053f898c".
- Narrow down time window.** This callout points to the time range selector, which shows the time window: Jan 2, 2025 @ 16:30:00.0 → Jan 2, 2025 @ 17:30:00.0.
- Add extra columns to gain deeper insights into the Catalyst Center microservices involved in a specific Task (E.g. Pod, Container and Host)** This callout points to the 'Selected fields' list, which includes:
 - kubernetes.container_name
 - kubernetes.host
 - kubernetes.namespace_name
 - kubernetes.pod_name
 - log
- Examine the log messages.** This callout points to the log messages list, which shows details for a specific log entry, including the Log ID: 019427c2-5699-70c6-b901-93e7053f898c.

Catalyst Center: Log Messages

Example: ActivityIDs & correlatonIds

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

Activity ID

Correlation ID

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.

Catalyst Center

Network Devices / Provisi

admin

Provision Device

Step 1 of 3: Performing Initial Checks

Cisco Catalyst Center is now performing early validations to ensure a seamless provisioning operation.

Pending Operations

Success. No pending operations conflicting with the current operation found.

Device Compliance

Success. No compliance violations found for the devices involved in the current op

Click [here](#) to see what is included in the configuration compliance check. Certain

Configuration, Software Image, etc., which are part of overall compliance calculation

impact the current operation. When compliance run is in progress, then last known compliance data is used to determine the list of

the devices.

Device Level Validations

Success. No issues were found on a preliminary check of the devices involved in this operation. More checks will be performed as

the workflow progresses. Currently, these preliminary checks are performed only on Switches and Routers. Wireless controllers,

Access Points and other devices are not included.

Exit

Recheck

Back

Next

Network

1

As of: 2:4

Filter

Overview

5000 ms

10000 ms

15000 ms

20000 ms

25000 ms

Name

icon-font.c7a3b775e861aa0df6c8fdc688a8f61...

DeviceInfo?minify=true&networkDeviceId=f9bf...

vcr-precomputation

post?filter=a-dnaconprem,u-dna-provision-de...

vcr-precheck

status?taskId=a716fc53-4cbe-447c-a421-586...

X Headers

Request URL:

https://10.62.149.204/api/v2/data/customer-facing-servic

e/DeviceInfo?minify=true&networkDeviceId=f9bf3ac4-59

6-4f83-85b3-26d87f701f6c

Request Method:

GET

Status Code:

200 OK

10.62.149.204:443

strict-origin-when-cross-origin

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

max-age=31536000; includeSubDomains

api-gateway

nosniff

e5fd5ead-7d74-4bc0-9915-aa1688e4fbe5

SAMEORIGIN

1: mode=block

X-Content-Type-Options:

nosniff

X-Correlation-Id:

e5fd5ead-7d74-4bc0-9915-aa1688e4fbe5

X-Frame-Options:

SAMEORIGIN

Accept:

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=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzU1IiwiaXNjaW50ZXJlbnR5Ijoi

Wl0iLCJ2bnMiOiJMDk5ZDc2YWQ4NDRkMDBmNDk2OWwILCJhdXRoU291cmNlIjoiaW50ZXJlbnR5Ijoi

JhdXRoU291cmNlIjoiaW50ZXJlbnR5Ijoi

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

2

Catalyst Center : Log Explorer (Kibana)

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

Discover

2,039 hits

New Save Open Share Inspect

1 Filters "b68abf5f-c98d-44ce-a906-b688433fc65c"

+ Add filter

logstash-*

Selected fields

t kubernetes.container_name
t kubernetes.host
t kubernetes.namespace_name
t kubernetes.pod_name

Available fields

Popular
t log
@timestamp
t _id
t _index
_score
t _type
t docker.container_id
t kubernetes.container_image
t kubernetes.container_image_id

Count

1,500
1,000
500
0

16:35 16:40 16:45 16:50 16:55 17:00 17:05 17:10 17:15 17:20 17:25

@timestamp p minute

Time	kubernetes.namespace_name	kubernetes.host	kubernetes.container_name	kubernetes.pod_name
> Jan 2, 2025 @ 17:04:41.556	fusion	100.64.0.1	task-service	task-service-56d4f56f89-79855
> Jan 2, 2025 @ 17:04:41.556	fusion	100.64.0.1	task-service	task-service-56d4f56f89-79855
> Jan 2, 2025 @ 17:04:41.550	fusion	100.64.0.1	task-service	task-service-56d4f56f89-79855
> Jan 2, 2025 @ 17:04:41.548	fusion	100.64.0.1	task-service	task-service-56d4f56f89-79855
> Jan 2, 2025 @ 17:04:38.192	fusion	100.64.0.1	spf-service-manager-service	spf-service-manager-service-767db5dbbf-h4xv4
> Jan 2, 2025 @ 17:04:38.192	fusion	100.64.0.1	spf-service-manager-service	spf-service-manager-service-767db5dbbf-h4xv4
> Jan 2, 2025 @ 17:04:38.144	fusion	100.64.0.1	spf-service-manager-service	spf-service-manager-service-767db5dbbf-h4xv4
> Jan 2, 2025 @ 17:04:38.144	fusion	100.64.0.1	spf-service-manager-service	spf-service-manager-service-767db5dbbf-h4xv4
> Jan 2, 2025 @ 17:04:36.540	fusion	100.64.0.1		
> Jan 2, 2025 @ 17:04:36.540	fusion	100.64.0.1		

Use correlation ID to search relevant logs.

Multiple Microservices have been triggered as part of specific workflows

provisioning-service
provisioning-service
provisioning-service
provisioning-service
spf-service-manager-service
provisioning-service
spf-service-manager-service
spf-service-manager-service
orchestration-engine-service
orchestration-engine-service
spf-service-manager-service
apic-em-network-programmer-service
spf-service-manager-service
apic-em-network-programmer-service
apic-em-network-programmer-service
apic-em-network-programmer-service

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

BRKTRS-3821

CISCO

Catalyst Center: Log Explorer (Kibana)

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

Catalyst Center

Discover

21 hits

New Save Open Share Inspect

1 Filters "b68abf5f-c98d-44ce-a906-b688433fc65c" and error

+ Add filter

logstash-*

Selected fields

- kubernetes.container_name
- kubernetes.host
- kubernetes.namespace_name
- kubernetes.pod_name
- log

Available fields

Jan 2, 2025 @ 16:30:00.0 → Jan 2, 2025 @ 17:30:00.0

Refresh

Jan 2, 2025 @ 16:30:00.000 - Jan 2, 2025 @ 17:30:00.000 — Auto

Count

@timestamp per minute

kubernetes.namespace_name

kubernetes.host

kubernetes.container_name

kubernetes.pod_name

> Jan 2, 2025 @ 17:04:36.324 fusion 100.64.0.1

apic-em-network-programmer-service

apic-em-network-programmer-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

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

apic-em-network-programmer-service
apic-em-network-programmer-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

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

BRKTRS-3821

CISCO

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:

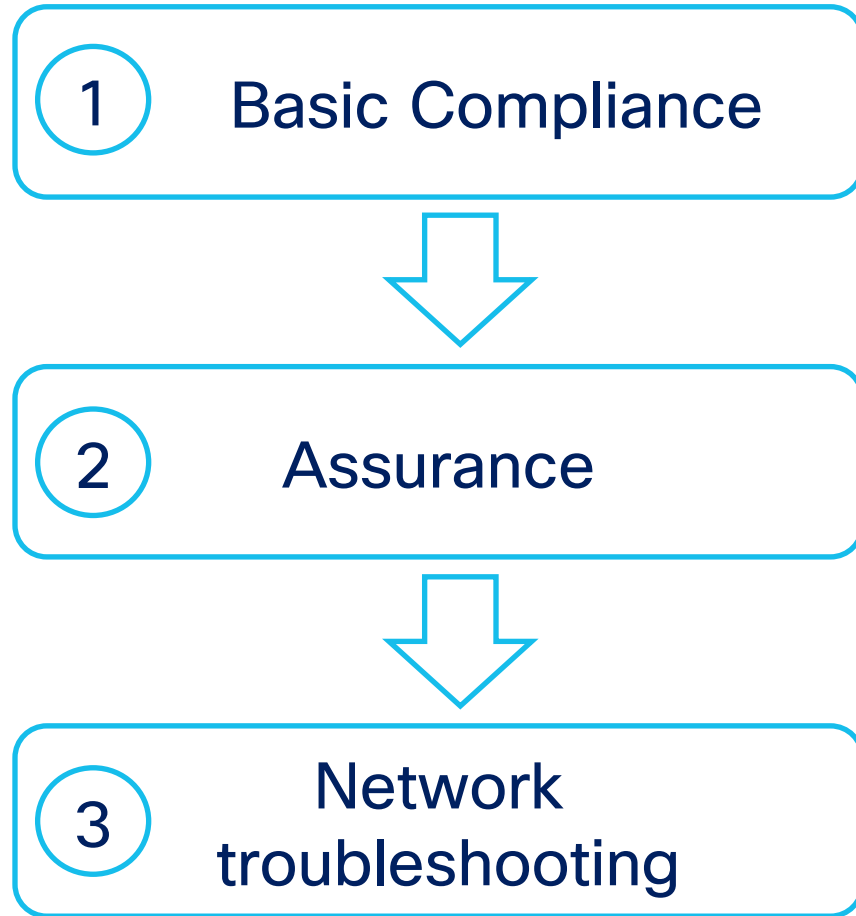
IP address assigned by Automatic
Private IP Addressing (APIPA) feature.

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 Cisco Catalyst Center interface. The top navigation bar includes the Cisco logo, the text 'Catalyst Center', and the breadcrumb 'Provision / SD-Access / Fabric Sites'. On the right of the top bar are icons for favorites, search, status, help, notifications (7, 10, 5), and a user profile 'admin'. The left sidebar contains a menu with 'Design', 'Policy', 'Provision' (highlighted with a green dashed box and a green circle '1'), 'Assurance', 'Workflows', and 'Tools'. The 'Provision' menu is expanded, showing 'Inventory', 'Plug and Play', 'LAN Automation', 'Inventory Insights', 'Zero-Trust Overview', and 'Fabric Sites' (highlighted with a green dashed box and a green circle '2'). The main content area is titled 'Provisioning Tasks' and shows a time-based bar chart for the period '24 Hours: Jan 2, 2025 2:25 PM - Jan 3, 2025 2:25 PM'. The chart has a legend at the bottom left (highlighted with a green dashed box and a green circle '3') with three categories: 'Tasks Deployed' (green), 'Tasks In-Progress' (purple), and 'Errors' (red). A blue callout box with a white arrow points to the legend, containing the text: '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 displays the Cisco Catalyst Center interface for managing fabric infrastructure. The left sidebar shows the navigation menu with 'Fabric Infrastructure' selected. The main panel shows the configuration drift verification process for the device 'CAT9K-EDGE-01.cisco.com'.

Left Panel (Fabric Infrastructure):

- SUMMARY**
 - > Device Family (1)
 - > Reachability (1)
 - > Compliance Status (1)
 - > Provision Status (1)
 - ☐ Success
 - > Fabric Role (3)
 - ☐ Control Plane Node
 - ☐ Border Node
 - ☐ Edge Node
- Devices (5)**
 - Click here to apply basic or advanced filters
 - 0 Selected **Tag** **More Actions** ▾
 - ☐ **Tags** **Device Name**
 - ☐ CAT9K-BORDER-01.cisco.com
 - ☐ CAT9K-BORDER-02.cisco.com
 - ☐ CAT9K-EDGE-01.cisco.com

Right Panel (Device Details):

- CAT9K-EDGE-01.cisco.com (172.16.0.3)**
- Reachable Uptime: 16 days 18 hrs 25 mins Device Role: ACCESS
- Details** **Fabric** **Advisories** **REP Rings** **Configuration** **VLANs** **Power** **Fans** **SFP Modules** **User Defined Fields** **More** ▾
- Config Drift Date Range:** **Start Date** **End Date**
Sep 5, 2024 Jan 3, 2025
- No. of Lines** (Y-axis: 600 to 1.6K) **Config Drift Days** (X-axis: Sep 08 to Nov 24)
- Legend:** ● In-band Config Drift ● Out-of-band Config Drift ● Labelled Config
- Config Drift Version** **Nov 30, 2024 01:31 PM** **Label Config**
- Running Config (749 Lines)**

```
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**
- Running Config (751 Lines)**

```
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
```

Annotations:

- 1:** More ▾ (Dropdown menu)
- 2:** Config Drift (Selected option in dropdown menu)
- 3:** Verify any configuration changes between the working and non-working setup. (Callout box pointing to the config drift comparison)

Fabric Infrastructure – Compliance

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

Catalyst Center

Provision / SD-Access

3

10

5

admin

Fabric Sites / KRK04

KRK04

View Site Hierarchy

Site Actions

1

Fabric Infrastructure

Layer 3 Virtual Networks

Layer 2 Virtual Networks

Anycast Gateways

Wireless SSIDs

Authentication Template

Port Assignment

SUMMARY

> Device Family (1)

> Reachability (1)

> Compliance Status (1)

> Provision Status (1)

> Fabric Role (3)

PORT ATTRIBUTES

Devices (5)

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

0 Selected Tag More Actions

	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	Non-Compliant
<input type="checkbox"/>		CAT9K-BORDER-02.cisco.com	172.16.0.2	BN CP	--	Reachable	Success	Non-Compliant
<input type="checkbox"/>		CAT9K-EDGE-01.cisco.com	172.16.0.3	EN	--	Reachable	Success	Non-Compliant
<input type="checkbox"/>		CAT9K-EDGE-02.cisco.com	172.16.0.4	EN	--	Reachable	Success	Non-Compliant
<input type="checkbox"/>		CAT9K-EDGE-03.cisco.com	172.16.0.5	EN	--	Reachable	Success	Non-Compliant

5 Record(s)

Check compliance status for all devices in the fabric.

2

Compliance Status

Non-Compliant

Non-Compliant

Non-Compliant

Non-Compliant

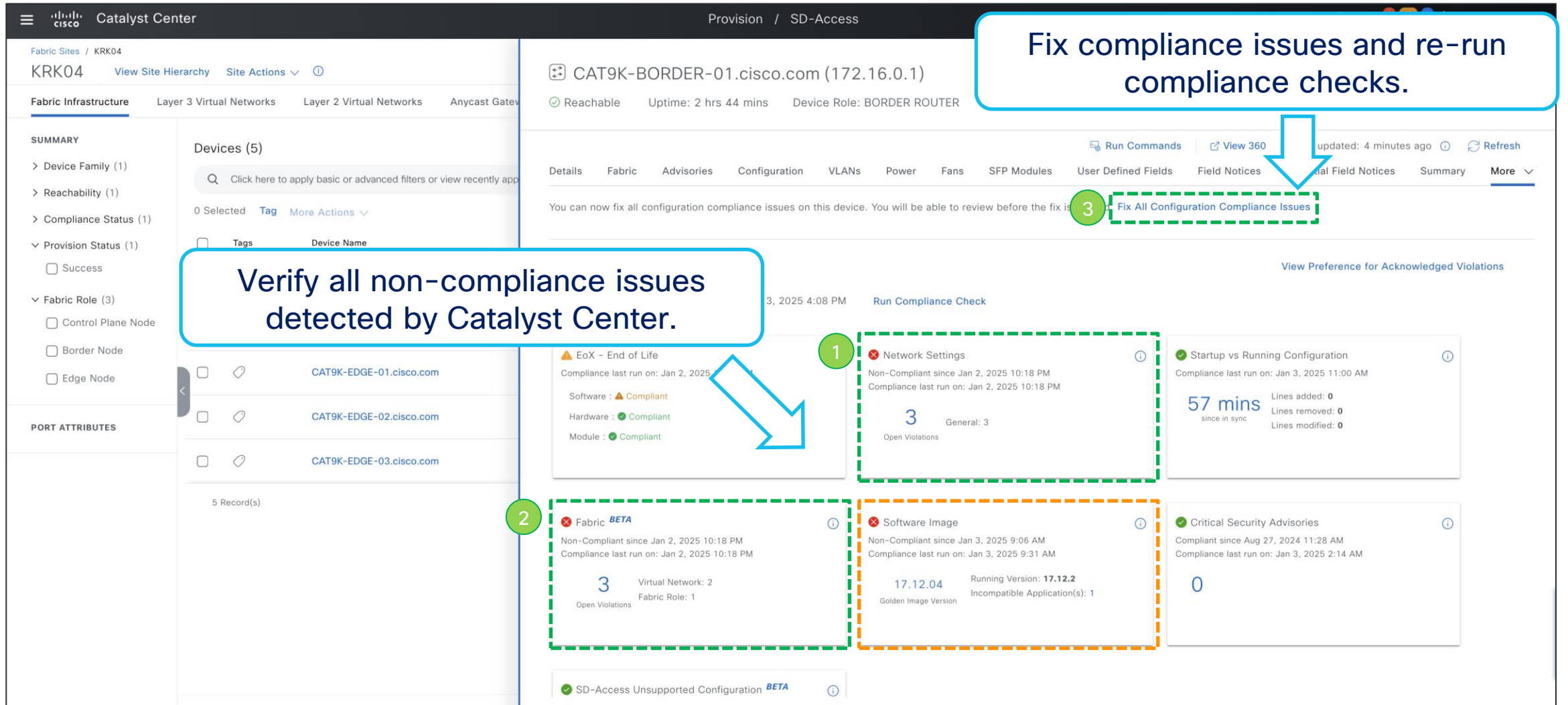
Non-Compliant

As of: Jan 3, 2025 11:52 AM

Show Records: 25 1 - 5

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.

Fix All Configuration Compliance Issues

1

2

3

Network Settings
Non-Compliant since Jan 2, 2025 10:18 PM
Compliance last run on: Jan 2, 2025 10:18 PM
3 Open Violations
General: 3

Startup vs Running Configuration
Compliance last run on: Jan 3, 2025 11:00 AM
57 mins since in sync
Lines added: 0
Lines removed: 0
Lines modified: 0

Fabric BETA
Non-Compliant since Jan 2, 2025 10:18 PM
Compliance last run on: Jan 2, 2025 10:18 PM
3 Open Violations
Virtual Network: 2
Fabric Role: 1

Software Image
Non-Compliant since Jan 3, 2025 9:06 AM
Compliance last run on: Jan 3, 2025 9:31 AM
17.12.04 Golden Image Version
Running Version: 17.12.2
Incompatible Application(s): 1

Critical Security Advisories
Compliant since Aug 27, 2024 11:28 AM
Compliance last run on: Jan 3, 2025 2:14 AM
0

SD-Access Unsupported Configuration BETA

Compliance Fix – Configuration preview

CAT9K-BORDER-01.cisco.com – Compliance Fix

Step 3 of 3: Preview Configuration

Review the device configuration provided below by clicking on each device. When you are done, click the Deploy button to push the configuration to the device.

As of: 12:00:55 PM [Refresh](#)

Status: ● Ready

Search by device name

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

Configurations – Side by side view

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_WEBAUTH_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 ***** 97ffa0bfe9144852
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_authen
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 not store credentials id f9bfc3a459764f68395b326d87f701f6c password *****
```

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](#)**

Catalyst Center: SD Access Assurance

Tip #2a: Check Assurance data

Assurance / Dashboards / Health

Overall

Network

Client

Network Services

Application

SD-Access

AI Analytics

24 Hours

Jan 8, 2025 1:25 PM - Jan 9, 2025 1:30 PM

SD-Access Assurance provisions telemetry subscriptions on devices operating in Fabric roles to gather near real-time assurance data. This capability requires the Fabric devices to be configured for NETCONF, discovered with NETCONF, and to have Cisco Catalyst Center telemetry enabled. Network Segmentation Protocol is LISP.

1

2

5

1

Good

Fabric Sites

Layer 3 Virtual Networks

Fabric Devices

Transits

Telemetry Status

5

0

5

P1

P2

Total

Issues (5)

Export

Search Table

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

2 Record(s)

Show Records: 10

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

Suggested Actions

Problem Details

i

2 session(s) down. The table below illustrates the applicable sessions for this device, along with their r

All

Down

Up

No Data

Search Table

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

2

Understand problems reported by Catalyst Centre

172.16.200.10-DEVICE_VN-ipv4

Catalyst Center: SD Access Assurance

1

Problem Details

Suggested Actions

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

Suggested Actions (2)

1

Verify the BGP session status.

Verify the BGP session status for all vpnv4 neighbors

show bgp vpnv4 unicast all summary

Success

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	2d12h	2
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#

2

Verify the BGP session status for all ipv4 neighbors

show bgp ipv4 unicast summary

Success

Run automatic checks to further triage the issue in the network.

Preview All

Catalyst Center: Network Troubleshooting (DHCP)

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

1

Tools

2

Network Bug Identifier

3

Re-scan Network

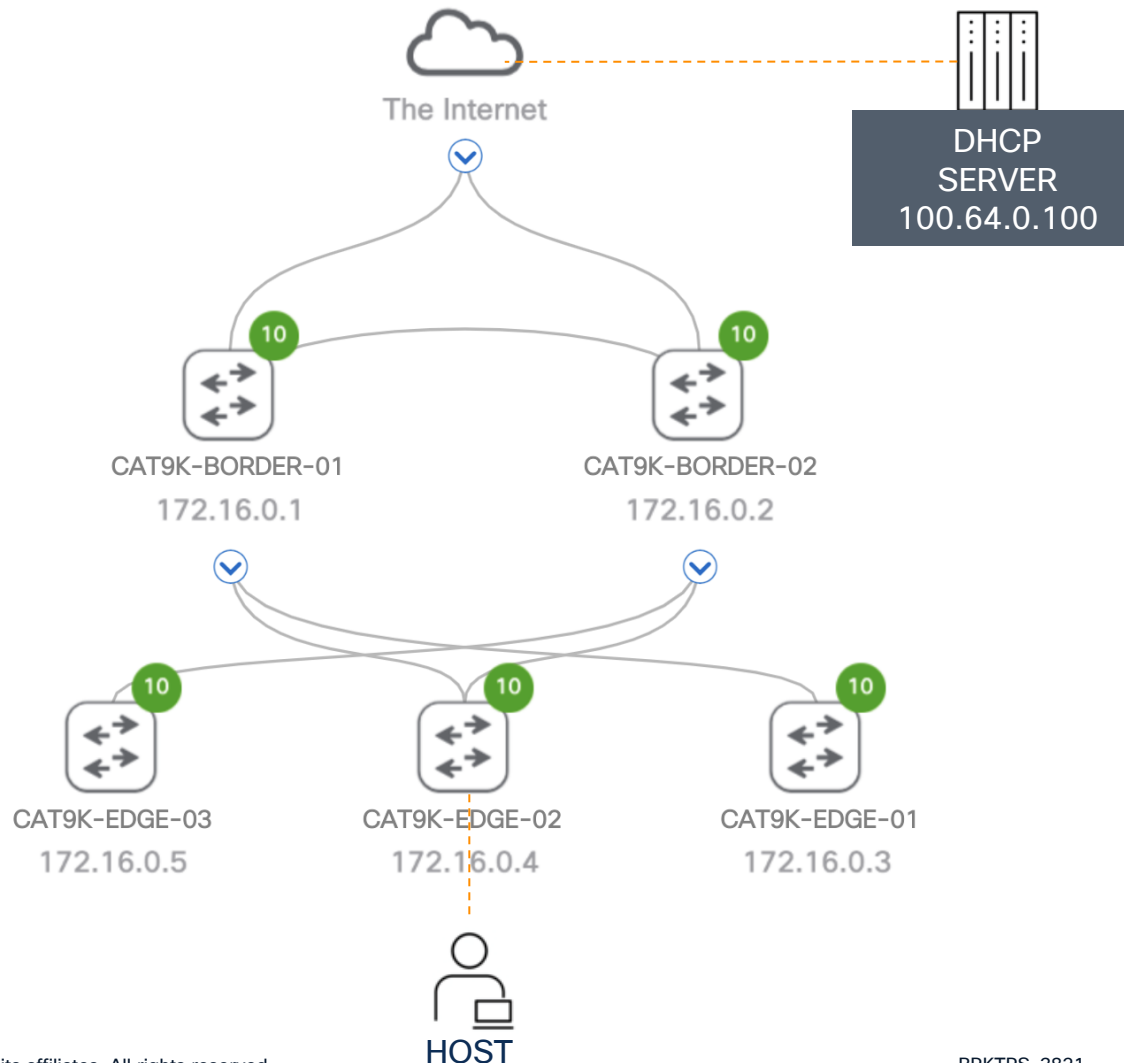
Re-scan your network for well known bugs that can potentially affect your network.

Name	Affected Devices	Severity	Affected Versions	Workaround
SNMP can not get some interface counters for LISP sub-interface	5	Moderate	--	No
CSCCuy44742 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
CSCCuy34361 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
CSCCwk36412 Non-Zero Header Padding in SYN/ACK packet sent from Switch to Telnet/SSH session	4	Moderate	IOS- XE:3.8.0S_V153_1_S1_FC4 IOS- XE:3.7.8S_V152_4_S8_FC2	Yes

4 Record(s)

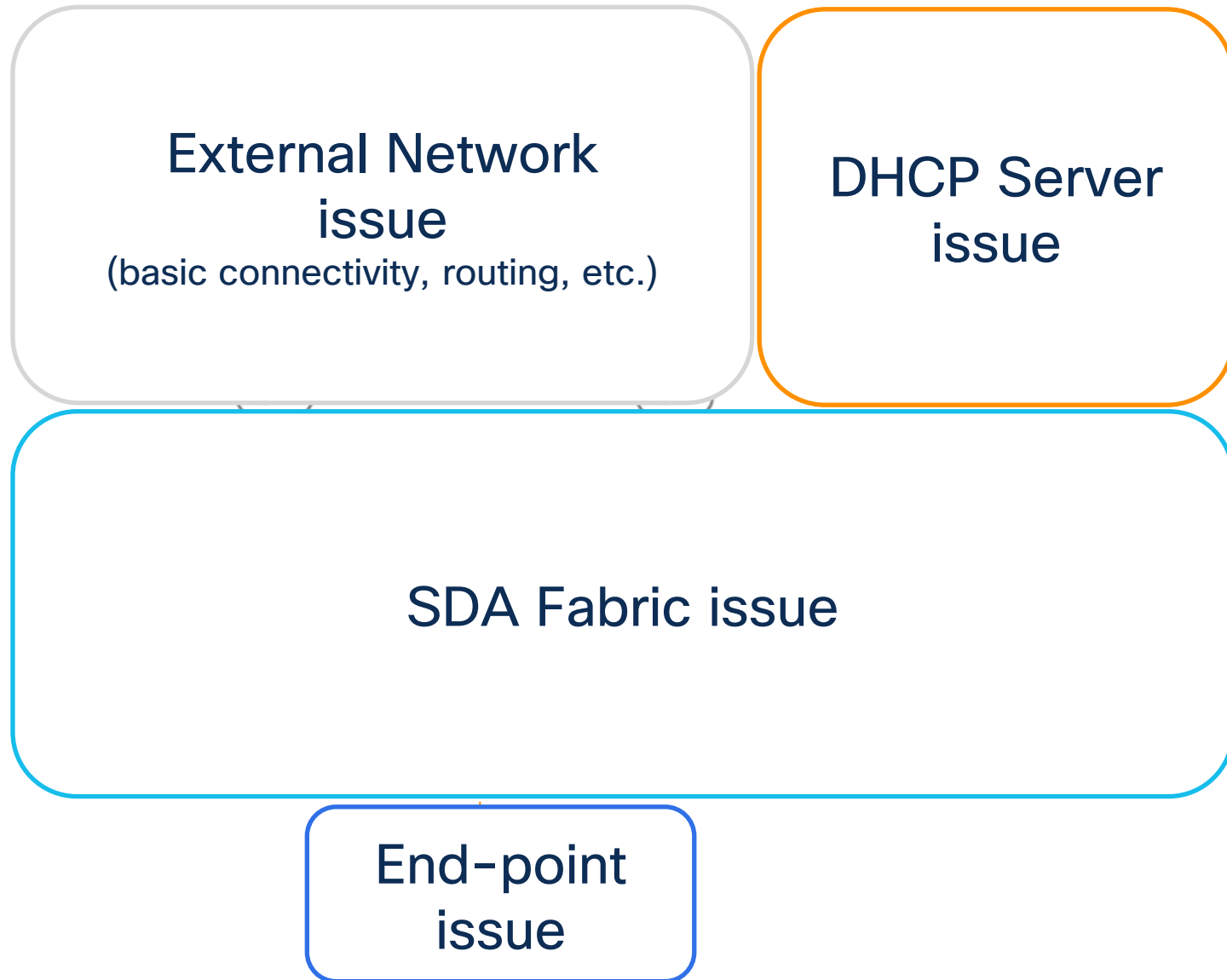


Catalyst Center: Network Troubleshooting (DHCP)



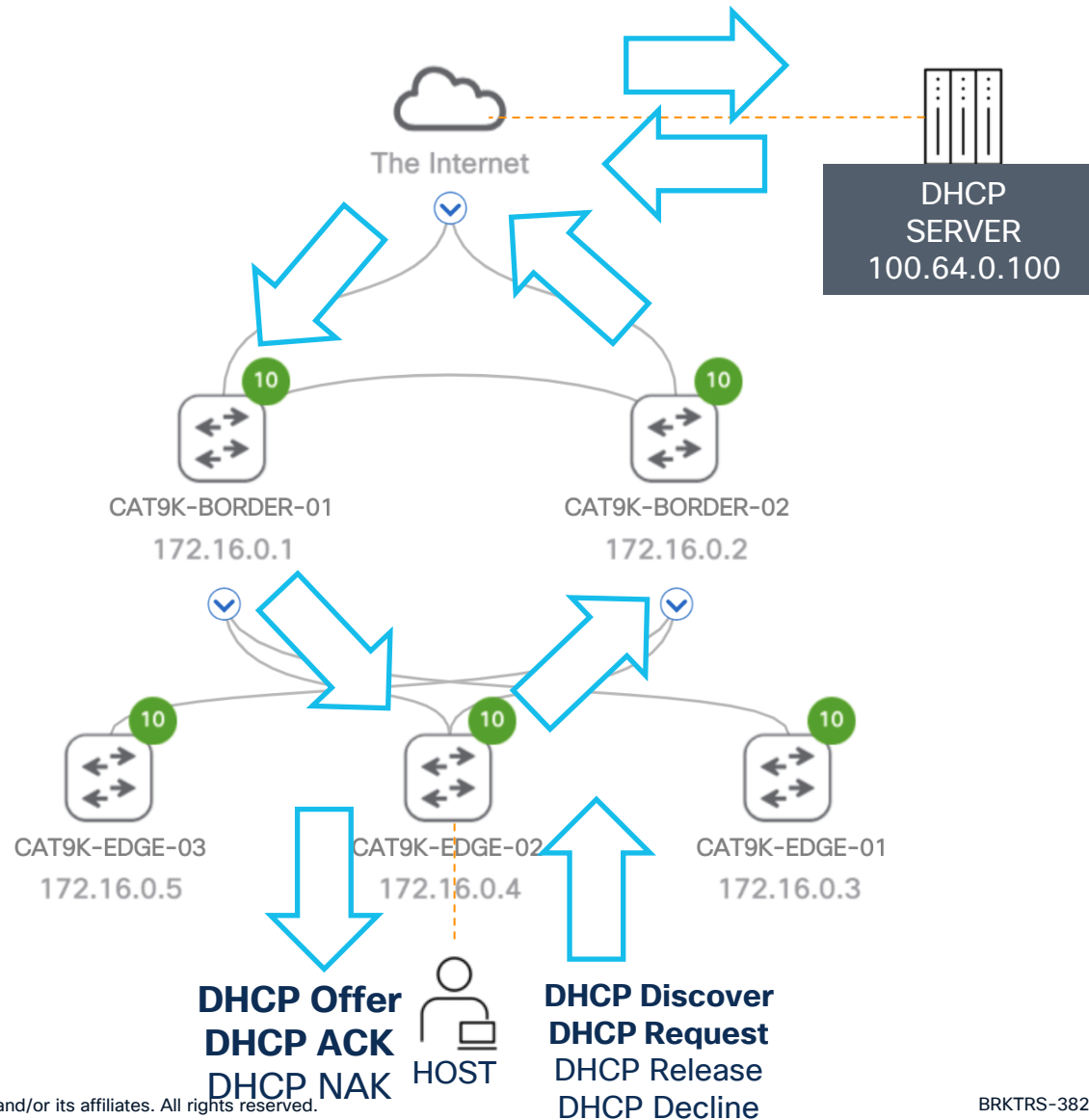
Only when all previous checks (configuration, assurance, compliance, known bugs) have been checked, start low level network troubleshooting.

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 screenshot shows the Cisco Catalyst Center interface. On the left sidebar, the 'Tools' menu item is highlighted with a green dashed box and a green circle labeled '1'. The 'Command Runner' option is also highlighted with a green dashed box and a green circle labeled '2'. A text box on the right shows the CLI command: `CLI: show platform dhcpsnooping client stats <MAC-ADDRESS>`. The main interface shows the 'Command Runner' tool with a search bar and a list of devices. A blue callout box points to the device list with the text: 'Select all relevant devices for initial triage (e.g. edge & borders)'. The device list shows three devices: 'CAT9K-BORDER-01.cisco.com (172.16.0.1)', 'CAT9K-BORDER-02.cisco.com (172.16.0.2)', and 'CAT9K-EDGE-02.cisco.com (172.16.0.4)'. A green dashed box highlights the 'Select devices*' section, and a green circle labeled '3' is next to it. Below the device list, the 'Select/Enter commands*' section is highlighted with a green dashed box, and a green circle labeled '4' is next to it. A blue callout box points to this section with the text: 'Provide a specific CLI command to be run concurrently on all devices.' The command entered is `sh platform dhcpsnooping client stats 7c21.0d1d.9ec6`.

1

2

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

3

4

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

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

Catalyst Center: Network Troubleshooting (DHCP)

Catalyst Center

Tools / Command Runner

☆

🔍

🟢

?

🔔

15

16

6

< Command Runner

Device List | Selected 3

1

✔ Command(s) executed successfully.

▼ CAT9K-BORDER-01.cisco.com (172.16.0.1)

✔ sh platform dhcp snooping client stats 7c21.0d1d.9ec6

▼ CAT9K-BORDER-02.cisco.com (172.16.0.2)

✔ sh platform dhcp snooping client stats 7c21.0d1d.9ec6

▼ CAT9K-EDGE-02.cisco.com (172.16.0.4)

✔ sh platform dhcp snooping client stats 7c21.0d1d.9ec6

CLI Output

2

↑ Upload to Case

↑ Export all CLI output

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

sh platform dhcp snooping client stats 7c21.0d1d.9ec6

DHCP SN: DHCP snooping server

DHCPD: DHCP protocol daemon

L2FWD: Transmit Packet to driver in L2 format

FWD: Transmit Packet to driver

<MessageType>(B): Dhcp message's response expected as 'B'roadcast

<MessageType>(U): Dhcp message's response expected as 'U'nicast

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	DHCP OFFER(B)	PUNT:RECEIVED
2025/01/12 11:23:35.265	3C51.0EE4.D8FF	192.168.10.254	123	DHCP OFFER(B)	LISP:GLEAN
2025/01/12 11:23:35.274	3C51.0EE4.D8FF	192.168.10.254	122	DHCP ACK(B)	PUNT:RECEIVED
2025/01/12 11:23:35.274	3C51.0EE4.D8FF	192.168.10.254	123	DHCP ACK(B)	LISP:GLEAN

CAT9K-BORDER-01#

CLI outputs gathered simultaneously from all devices.

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

BRKTRS-3821

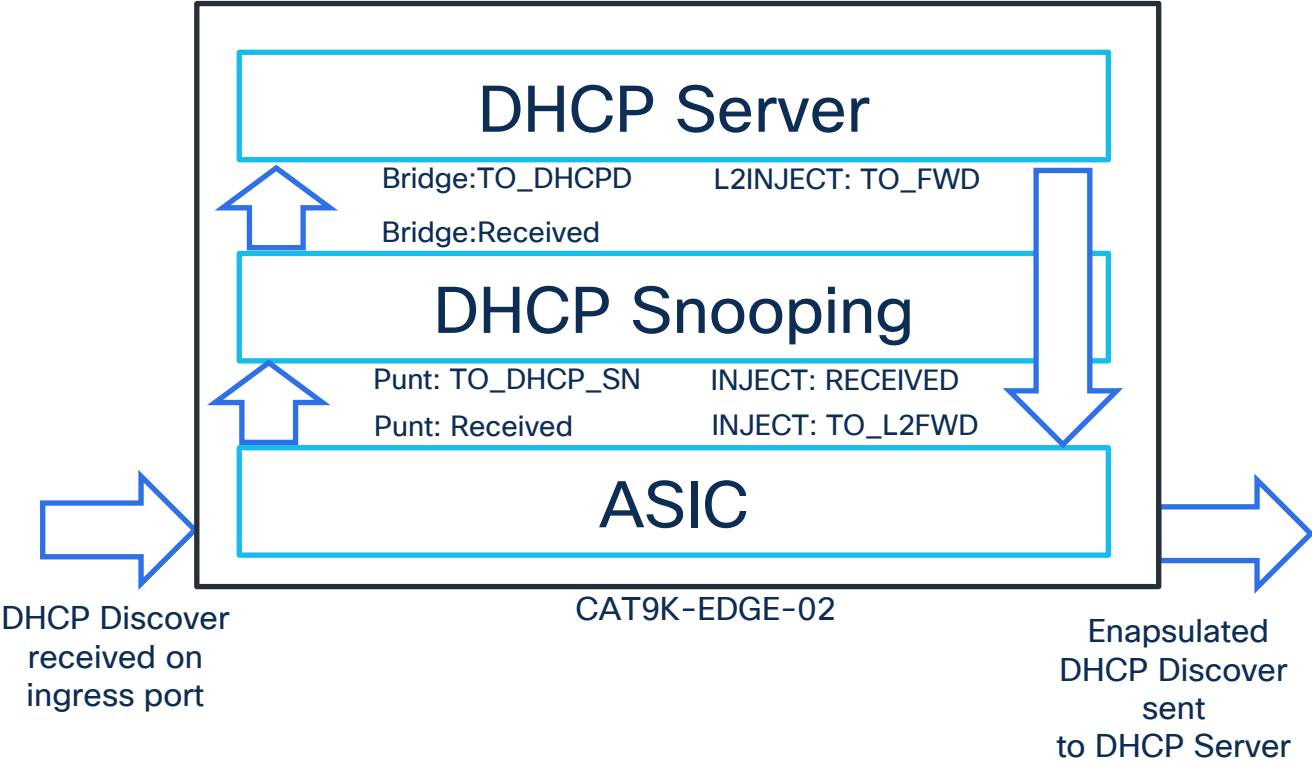
Catalyst Center: Network Troubleshooting (DHCP)

CAT9K-EDGE-02

```
sh platform dhcp Snooping client stats 7c21.0d1d.9ec6
DHCP SN: 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'roadcast
<MessageType>(U): Dhcp message's response expected as 'U'nicast
Packet Trace for client MAC 7C21.0D1D.9EC6:
```

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	DHCP OFFER(B)	PUNT:RECEIVED
2025/01/12 11:23:35.267	0200.0000.0000	255.255.255.255	0	DHCP OFFER(B)	INJECT:RECEIVED
2025/01/12 11:23:35.267	FFFF.FFFF.FFFF	255.255.255.255	0	DHCP OFFER(B)	INTERCEPT:RECEIVED
2025/01/12 11:23:35.267	FFFF.FFFF.FFFF	255.255.255.255	1020	DHCP OFFER(B)	INTERCEPT:TO_DHCP SN
2025/01/12 11:23:35.269	FFFF.FFFF.FFFF	255.255.255.255	1020	DHCP REQUEST(B)	PUNT:RECEIVED
2025/01/12 11:23:35.269	FFFF.FFFF.FFFF	255.255.255.255	1020	DHCP REQUEST(B)	PUNT:TO_DHCP SN
2025/01/12 11:23:35.272	FFFF.FFFF.FFFF	255.255.255.255	1020	DHCP REQUEST(B)	BRIDGE:RECEIVED
2025/01/12 11:23:35.272	FFFF.FFFF.FFFF	255.255.255.255	1020	DHCP REQUEST(B)	BRIDGE:TO_DHCPD
2025/01/12 11:23:35.272	FFFF.FFFF.FFFF	255.255.255.255	1020	DHCP REQUEST(B)	BRIDGE:TO_INJECT
2025/01/12 11:23:35.272	FFFF.FFFF.FFFF	255.255.255.255	1020	DHCP REQUEST(B)	L2INJECT:TO_FWD
2025/01/12 11:23:35.272	0000.0000.0000	100.64.0.100	0	DHCP REQUEST(B)	INJECT:RECEIVED
2025/01/12 11:23:35.272	0000.0000.0000	100.64.0.100	0	DHCP REQUEST(B)	INJECT:TO_L2FWD
2025/01/12 11:23:35.276	FFFF.FFFF.FFFF	192.168.10.254	1020	DHCP ACK(B)	PUNT:RECEIVED
2025/01/12 11:23:35.276	FFFF.FFFF.FFFF	255.255.255.255	0	DHCP ACK(B)	INJECT:RECEIVED
2025/01/12 11:23:35.276	FFFF.FFFF.FFFF	255.255.255.255	0	DHCP ACK(B)	INTERCEPT:RECEIVED
2025/01/12 11:23:35.276	FFFF.FFFF.FFFF	255.255.255.255	1020	DHCP ACK(B)	INTERCEPT:TO_DHCP SN

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

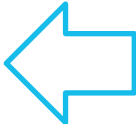


Catalyst Center: Network Troubleshooting (DHCP)

CAT9K-BORDER-01 & CAT9K-BORDER-02

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

```
sh platform dhcp snooping client stats 7c21.0d1d.9ec6
DHCP SN: DHCP snooping server
DHCPD: DHCP protocol daemon
L2FWD: Transmit Packet to driver in L2 format
FWD: Transmit Packet to driver
<MessageType>(B): Dhcp message's response expected as 'B'roadcast
<MessageType>(U): Dhcp message's response expected as 'U'nicast
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  DHCP OFFER(B)  PUNT:RECEIVED
2025/01/12 11:23:35.265 3C51.0EE4.D8FF 192.168.10.254 123  DHCP OFFER(B)  LISP:GLEAN
2025/01/12 11:23:35.274 3C51.0EE4.D8FF 192.168.10.254 122  DHCP ACK(B)    PUNT:RECEIVED
2025/01/12 11:23:35.274 3C51.0EE4.D8FF 192.168.10.254 123  DHCP ACK(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 dhcp snooping client stats 7c21.0d1d.9ec6

```
sh platform dhcp snooping client stats 7c21.0d1d.9ec6
DHCP SN: DHCP snooping server
DHCPD: DHCP protocol daemon
L2FWD: Transmit Packet to driver in L2 format
FWD: Transmit Packet to driver
<MessageType>(B): Dhcp message's response expected as 'B'roadcast
<MessageType>(U): Dhcp message's response expected as 'U'nicast
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

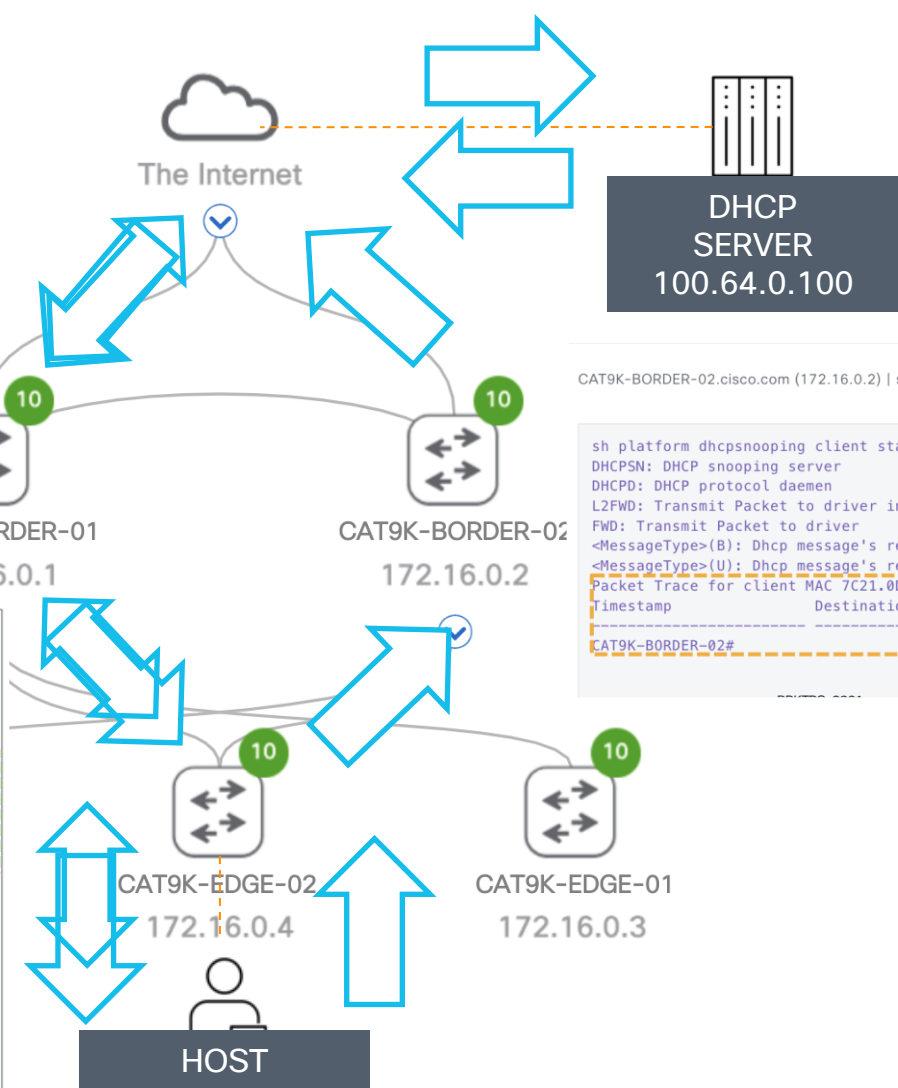
CAT9K-BORDER-01.cisco.com (172.16.0.1) | sh platform dhcp snooping client stats 7c21.0d1d.9ec6

```
sh platform dhcp snooping client stats 7c21.0d1d.9ec6
DHCP SN: DHCP snooping server
DHCPD: DHCP protocol daemon
L2FWD: Transmit Packet to driver in L2 format
FWD: Transmit Packet to driver
<MessageType>(B): Dhcp message's response expected as 'B'roadcast
<MessageType>(U): Dhcp message's response expected as 'U'nicast
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  DHCP OFFER(B)  PUNT:RECEIVED
2025/01/12 11:23:35.265  3C51.0EE4.D8FF  192.168.10.254  123  DHCP OFFER(B)  LISP:GLEAN
2025/01/12 11:23:35.274  3C51.0EE4.D8FF  192.168.10.254  122  DHCP ACK(B)    PUNT:RECEIVED
2025/01/12 11:23:35.274  3C51.0EE4.D8FF  192.168.10.254  123  DHCP ACK(B)    LISP:GLEAN
```

CAT9K-BORDER-01#

sh platform dhcp snooping client stats 7c21.0d1d.9ec6

```
sh platform dhcp snooping client stats 7c21.0d1d.9ec6
DHCP SN: DHCP snooping server
DHCPD: DHCP protocol daemon
L2FWD: Transmit Packet to driver in L2 format
FWD: Transmit Packet to driver
<MessageType>(B): Dhcp message's response expected as 'B'roadcast
<MessageType>(U): Dhcp message's response expected as 'U'nicast
Packet Trace for client MAC 7C21.0D1D.9EC6:
Timestamp      Destination MAC  Destination Ip  VLAN  Message      Handler:Action
-----
2025/01/12 11:23:34.263  FFFF.FFFF.FFFF  255.255.255.255  1020  DHCP DISCOVER(B)  PUNT:RECEIVED
2025/01/12 11:23:34.263  FFFF.FFFF.FFFF  255.255.255.255  1020  DHCP DISCOVER(B)  PUNT:TO_DHCP SN
2025/01/12 11:23:34.264  FFFF.FFFF.FFFF  255.255.255.255  1020  DHCP DISCOVER(B)  BRIDGE:RECEIVED
2025/01/12 11:23:34.264  FFFF.FFFF.FFFF  255.255.255.255  1020  DHCP DISCOVER(B)  BRIDGE:TO_DHCPD
2025/01/12 11:23:34.264  FFFF.FFFF.FFFF  255.255.255.255  1020  DHCP DISCOVER(B)  BRIDGE:TO_INJECT
2025/01/12 11:23:34.264  FFFF.FFFF.FFFF  255.255.255.255  1020  DHCP DISCOVER(B)  L2INJECT:TO_FWD
2025/01/12 11:23:34.265  0100.0CCC.CCCC  100.64.0.100    0    DHCP DISCOVER(B)  INJECT:RECEIVED
2025/01/12 11:23:34.265  0100.0CCC.CCCC  100.64.0.100    0    DHCP DISCOVER(B)  INJECT:TO_L2FWD
2025/01/12 11:23:35.267  FFFF.FFFF.FFFF  192.168.10.254  1020  DHCP OFFER(B)    PUNT:RECEIVED
2025/01/12 11:23:35.267  0200.0000.0000  255.255.255.255  0    DHCP OFFER(B)    INJECT:RECEIVED
2025/01/12 11:23:35.267  FFFF.FFFF.FFFF  255.255.255.255  0    DHCP OFFER(B)    INTERCEPT:RECEIVED
2025/01/12 11:23:35.267  FFFF.FFFF.FFFF  255.255.255.255  1020  DHCP OFFER(B)    INTERCEPT:TO_DHCP SN
2025/01/12 11:23:35.269  FFFF.FFFF.FFFF  255.255.255.255  1020  DHCP REQUEST(B)  PUNT:RECEIVED
2025/01/12 11:23:35.269  FFFF.FFFF.FFFF  255.255.255.255  1020  DHCP REQUEST(B)  PUNT:TO_DHCP SN
2025/01/12 11:23:35.272  FFFF.FFFF.FFFF  255.255.255.255  1020  DHCP REQUEST(B)  BRIDGE:RECEIVED
2025/01/12 11:23:35.272  FFFF.FFFF.FFFF  255.255.255.255  1020  DHCP REQUEST(B)  BRIDGE:TO_DHCPD
2025/01/12 11:23:35.272  FFFF.FFFF.FFFF  255.255.255.255  1020  DHCP REQUEST(B)  BRIDGE:TO_INJECT
2025/01/12 11:23:35.272  FFFF.FFFF.FFFF  255.255.255.255  1020  DHCP REQUEST(B)  L2INJECT:TO_FWD
2025/01/12 11:23:35.272  0000.0000.0000  100.64.0.100    0    DHCP REQUEST(B)  INJECT:RECEIVED
2025/01/12 11:23:35.272  0000.0000.0000  100.64.0.100    0    DHCP REQUEST(B)  INJECT:TO_L2FWD
2025/01/12 11:23:35.276  FFFF.FFFF.FFFF  192.168.10.254  1020  DHCP ACK(B)      PUNT:RECEIVED
2025/01/12 11:23:35.276  FFFF.FFFF.FFFF  255.255.255.255  0    DHCP ACK(B)      INJECT:RECEIVED
2025/01/12 11:23:35.276  FFFF.FFFF.FFFF  255.255.255.255  0    DHCP ACK(B)      INTERCEPT:RECEIVED
2025/01/12 11:23:35.276  FFFF.FFFF.FFFF  255.255.255.255  1020  DHCP ACK(B)      INTERCEPT:TO_DHCP SN
```



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

sh platform dhcp snooping client stats 7c21.0d1d.9ec6

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

Network troubleshooting (DHCP)

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

Catalyst Center

Global

DEVICE WORK ITEMS

☐ Unreachable

☐ Unassigned

☐ Untagged

☐ Failed Provision

☐ Non Compliant

☐ Outdated Software Image

☐ No Golden Image

☐ Failed Image Prechecks

☐ Under Maintenance

☐ Security Advisories

Devices (5) Focus Provision

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

1 Selected Tag + Add Device Actions

Tags	Device Name	Inventory
<input checked="" type="checkbox"/>	CAT9K-BORD	Software Image
<input type="checkbox"/>	CAT9K-BORD	Provision
<input type="checkbox"/>	CAT9K-EDGE	Telemetry
<input type="checkbox"/>	CAT9K-EDGE	Device Replacement
<input type="checkbox"/>	CAT9K-EDGE	Switch Refresh
<input type="checkbox"/>	CAT9K-EDGE	Compliance
<input type="checkbox"/>	CAT9K-EDGE	More
<input type="checkbox"/>	CAT9K-EDGE-03.cisco.com	172.16.0.4

Command Runner

CAT9K-EDGE-02.cisco.com@172.16.0.4

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 gil/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 0x9ald13f
4	16.882267	0.0.0.0 -> 255.255.255.255	DHCP 373	DHCP Discover - Transaction ID 0x9ald13f
6	20.882322	0.0.0.0 -> 255.255.255.255	DHCP 373	DHCP Discover - Transaction ID 0x9ald13f
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

CAT9K-EDGE-02.cisco.com>

Run Commands

Command Runner

Learn Device Config

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

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

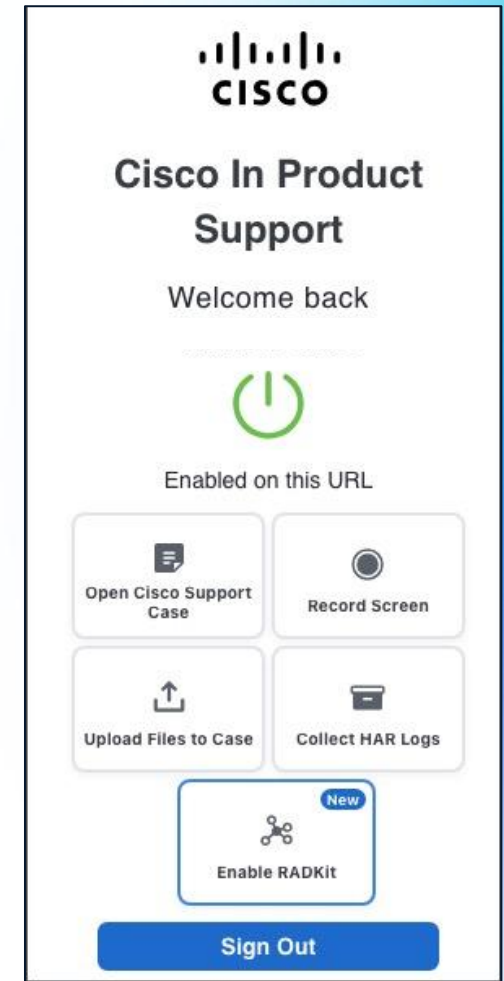
Cisco In Product Support Assistant Extension

<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.

 Unleash the Power of TAC's Virtual Assistance
Activate Cisco In Product Support



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

The Cisco Live! logo is positioned on the right side of a white rectangular area. It consists of the word "CISCO" in a bold, black, sans-serif font, followed by the word "Live" in a lighter weight of the same font, and a large black exclamation mark. The background of the slide features a dynamic pattern of blue and white wavy lines, with a thin, multi-colored arc (pink, orange, yellow) visible in the upper right corner.

CISCO Live !

