Mastering Troubleshooting with Cisco Catalyst Center and SD-Access

Won Je Choi
Technical Leader

Session ID: BRKTRS-3821

Cisco Webex App

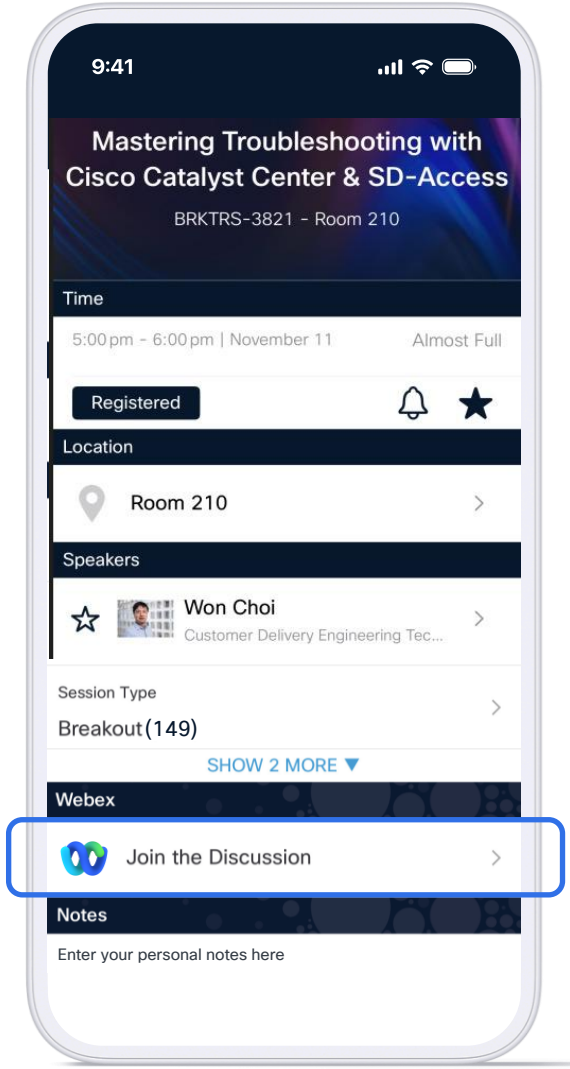
Questions?

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

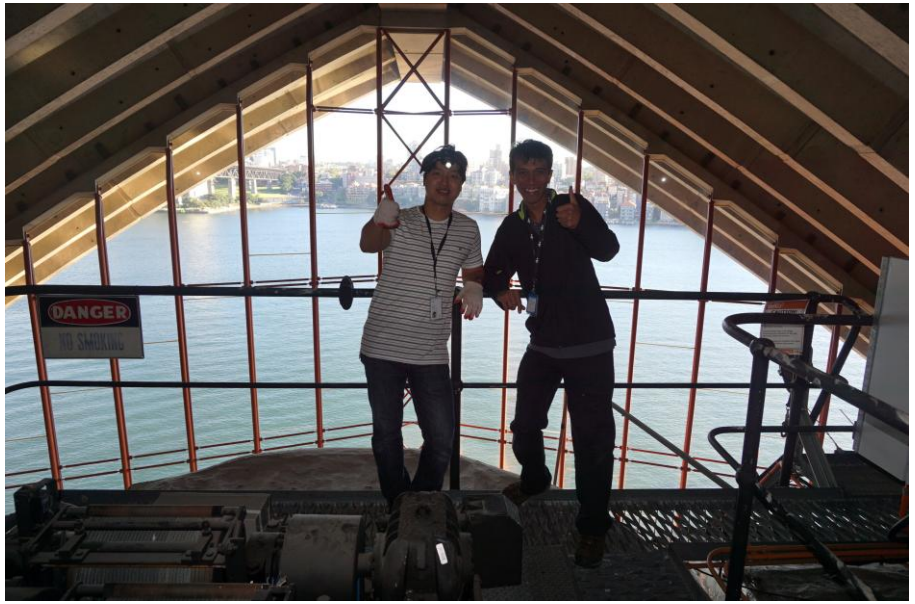
How

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

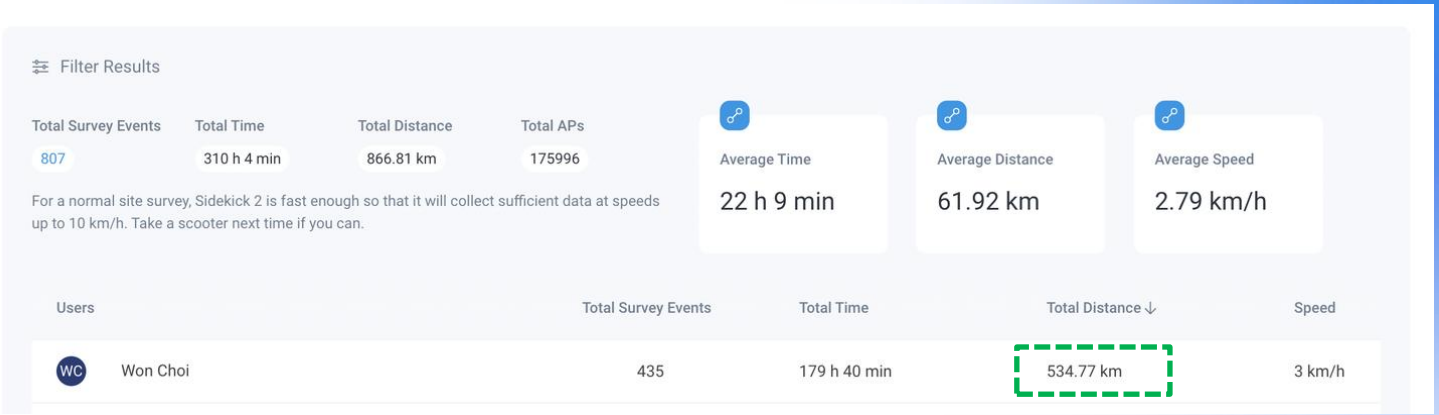
Technical Leader, Sydney TAC

CCIE #16459 (R&S)

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

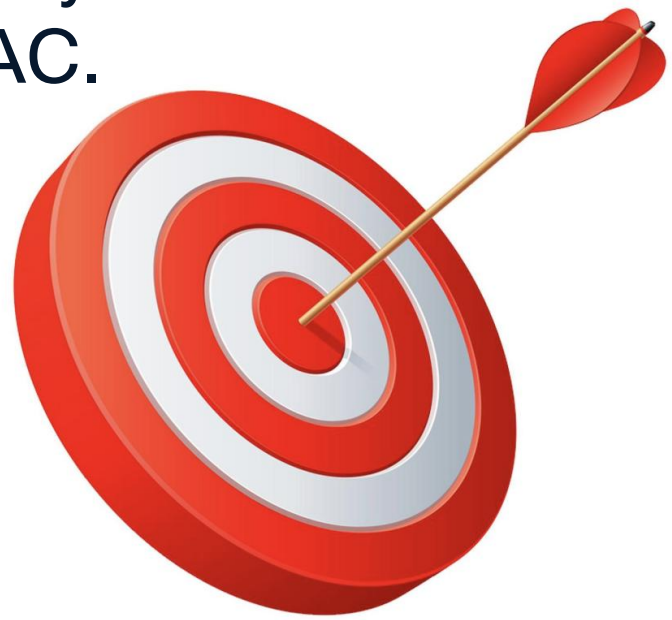
Korean-Australian, Dad to 12-year-old daughter and 9-year-old son; Home Weight Training.

Total 534Km of Ekahau Survey Distance ☺



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

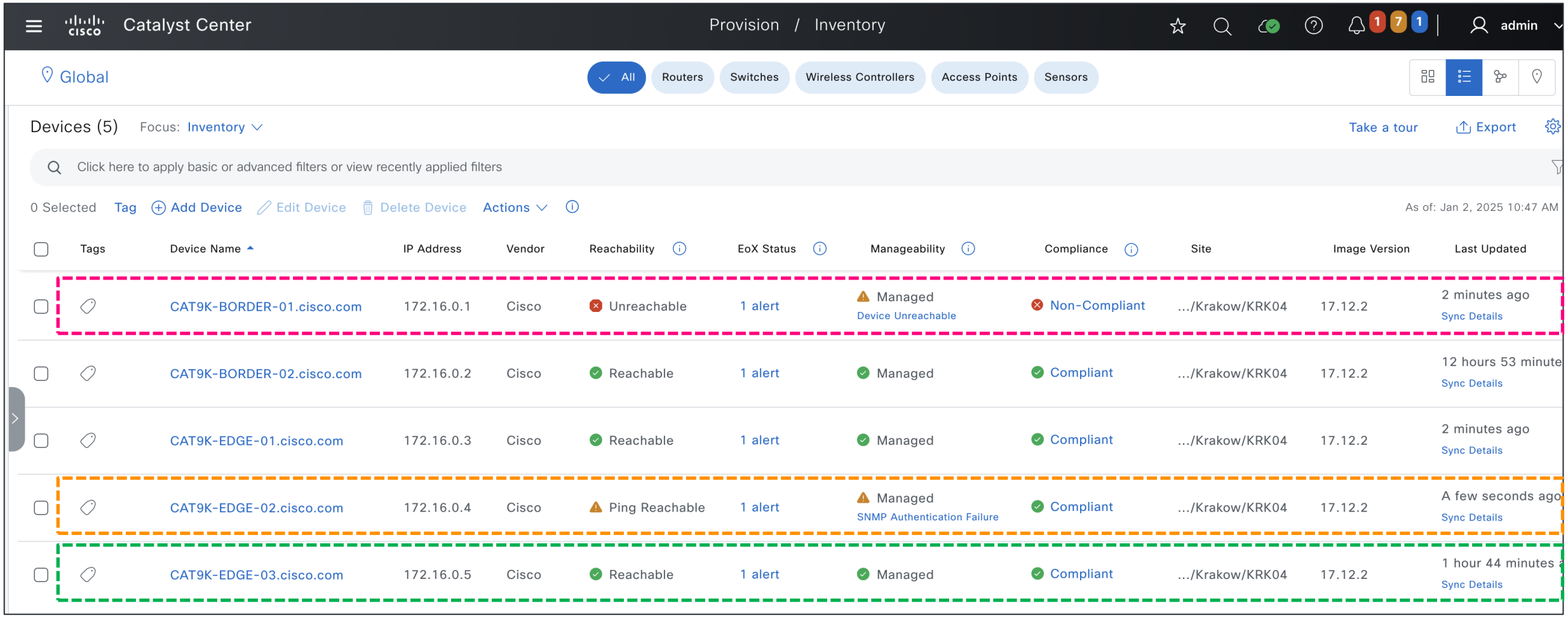
Recommended Release – Cisco Catalyst Center 2.3.7.9

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: Inventory
Troubleshooting Workflow and issue triage

For Your Reference

1 Device Reachability

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

2 Manageability (Credentials)

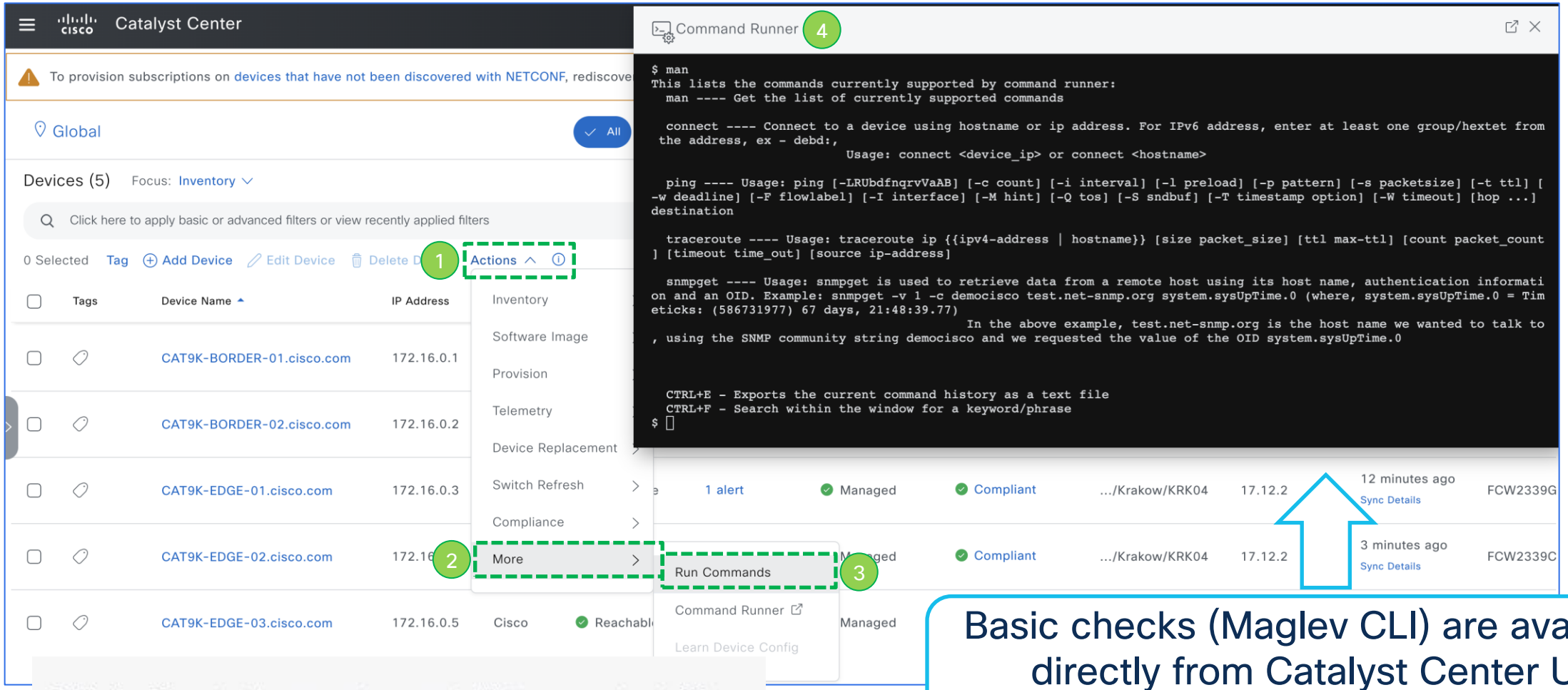
2a) Review and Validate credentials using ”Edit Device”
2b) Execute UI Inventory Re-sync operations.
2c) Execute API (force) re-sync operations.

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

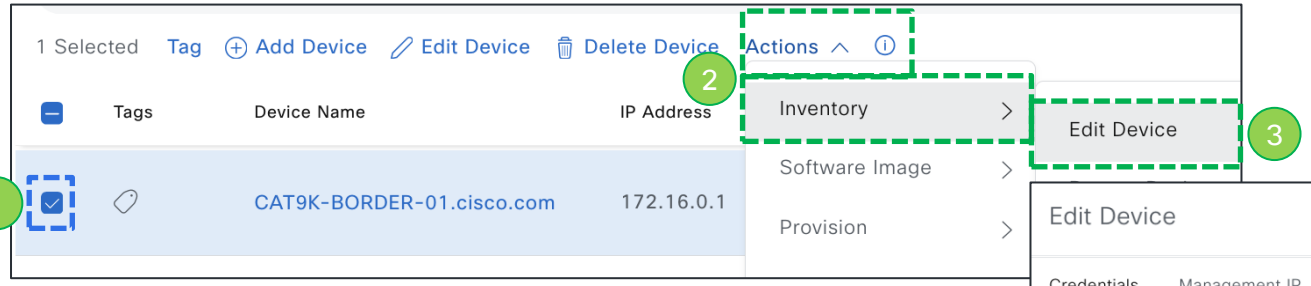
Tip #1a: Utilise the built-in Maglev “Command Runner” for Catalyst Center: **Action > More > Run Commands**



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

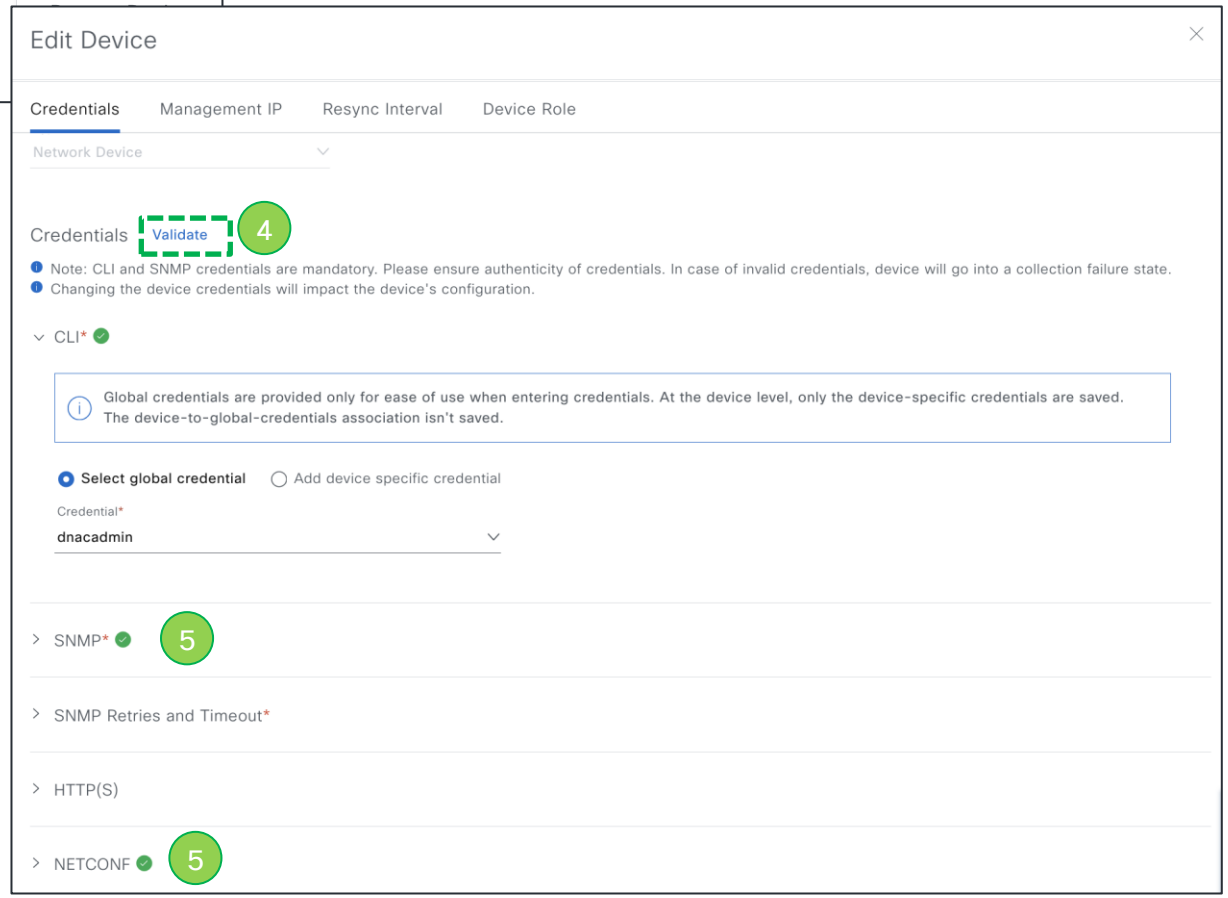
Catalyst Center: Manageability

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



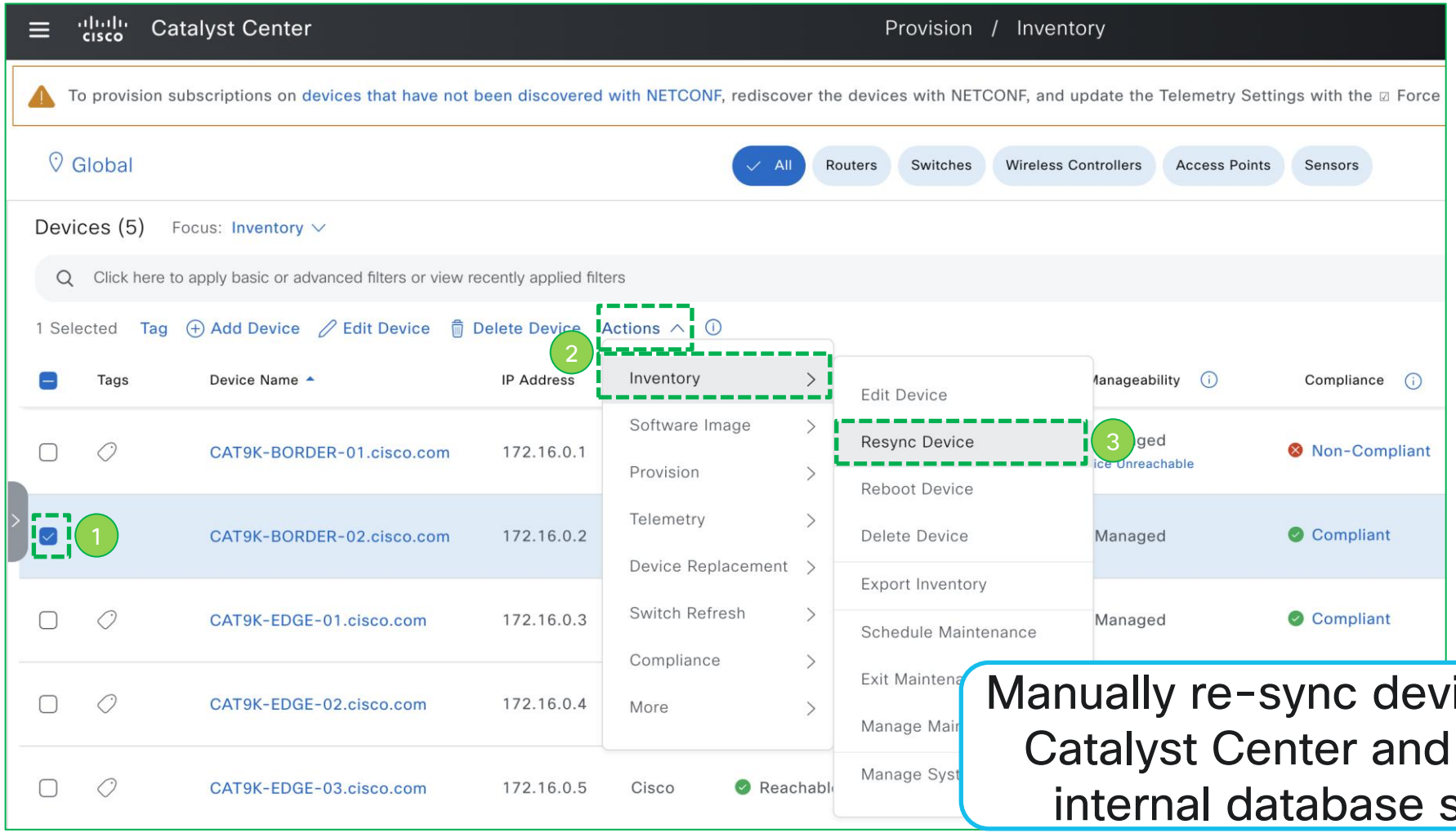
Ensure that you validate credentials for all connectivity methods.

Make sure that all configured connection methods are successful.



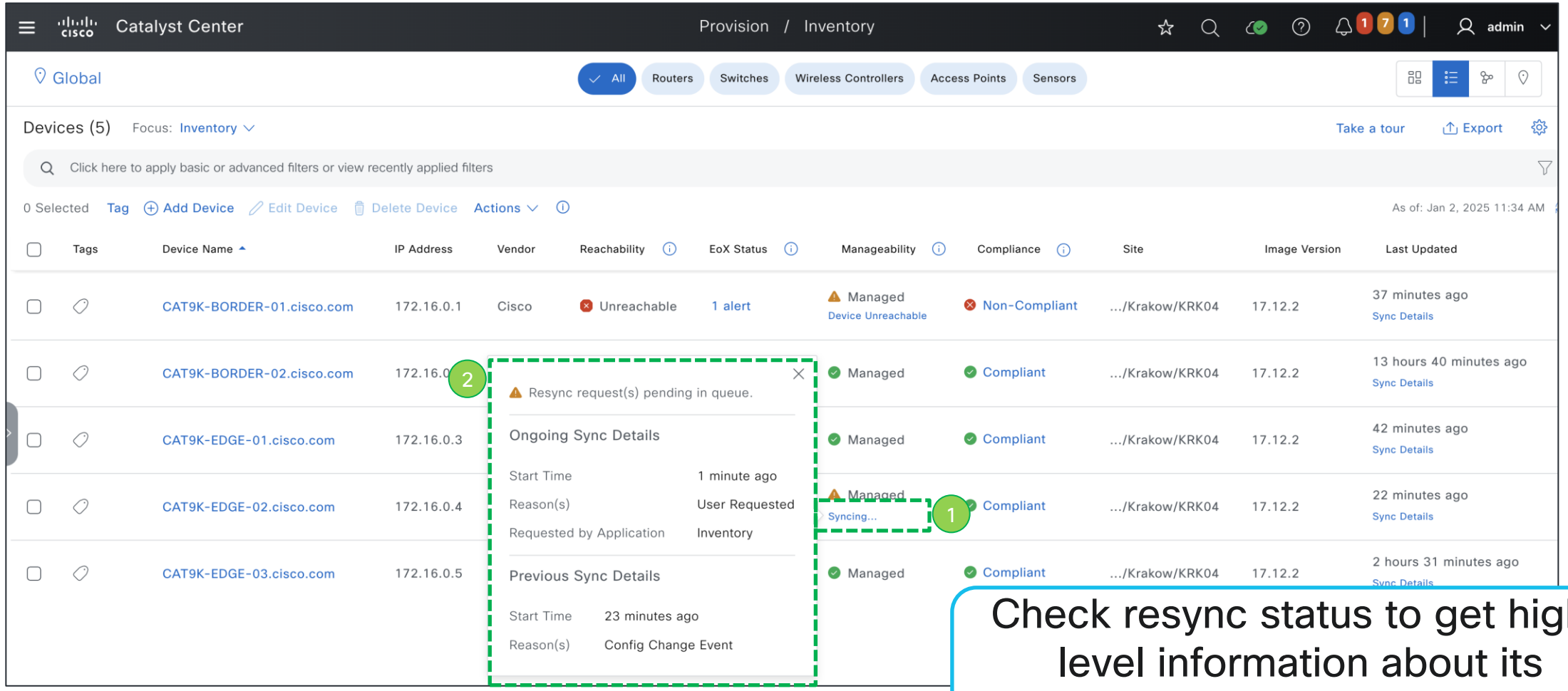
Catalyst Center: Manageability

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



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

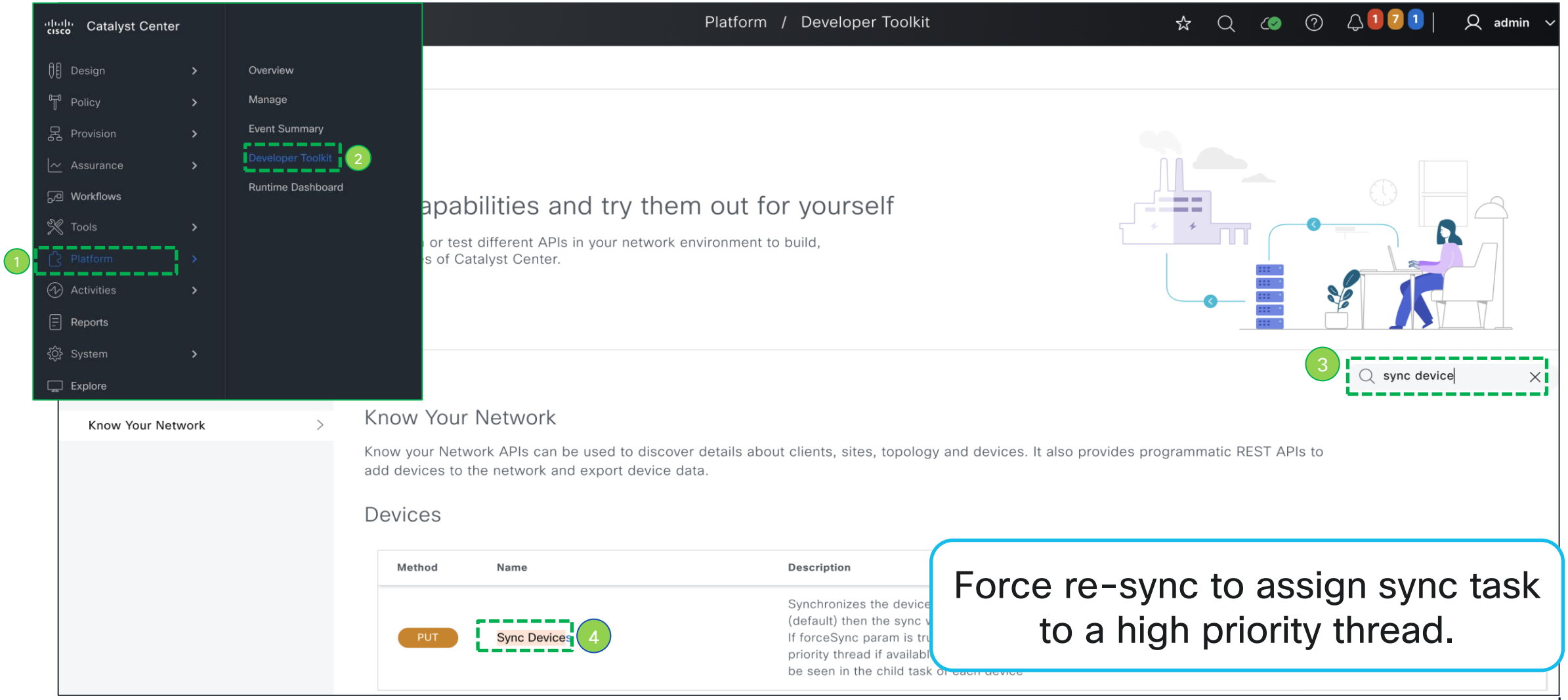
Catalyst Center: Manageability – Device re-sync progress



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

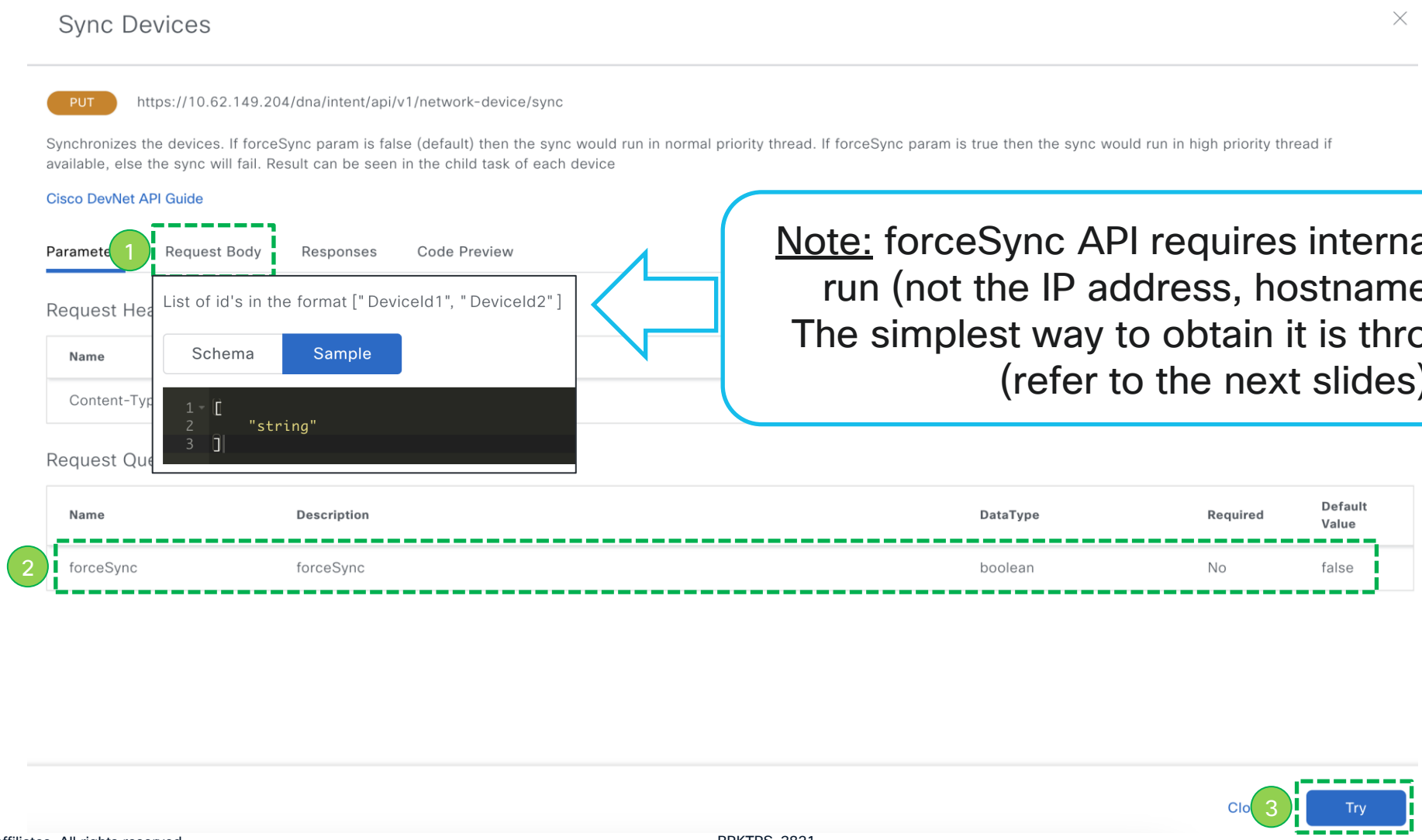
Catalyst Center: Manageability

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



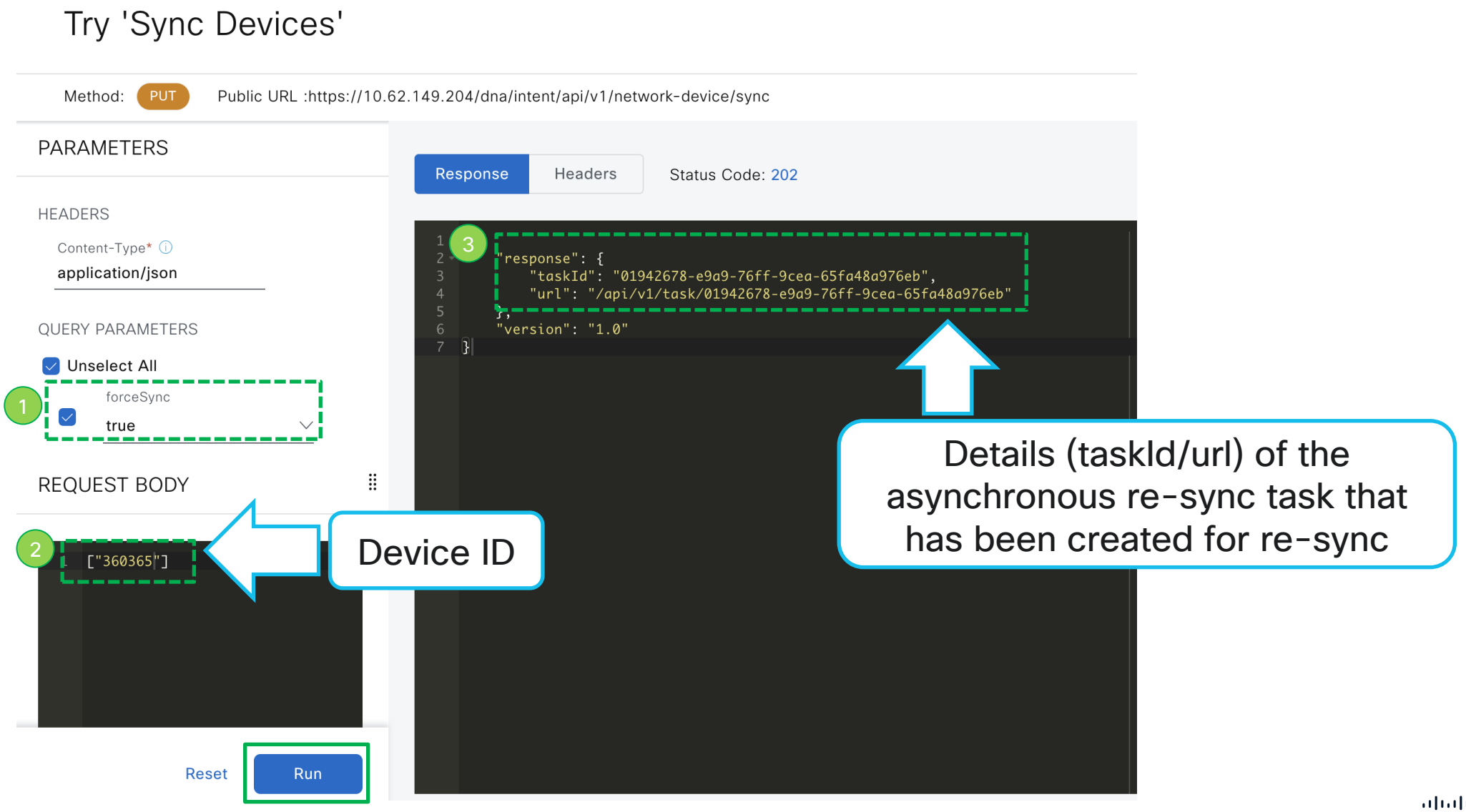
Force re-sync to assign sync task to a high priority thread.

Catalyst Center: Manageability – force re-sync via API

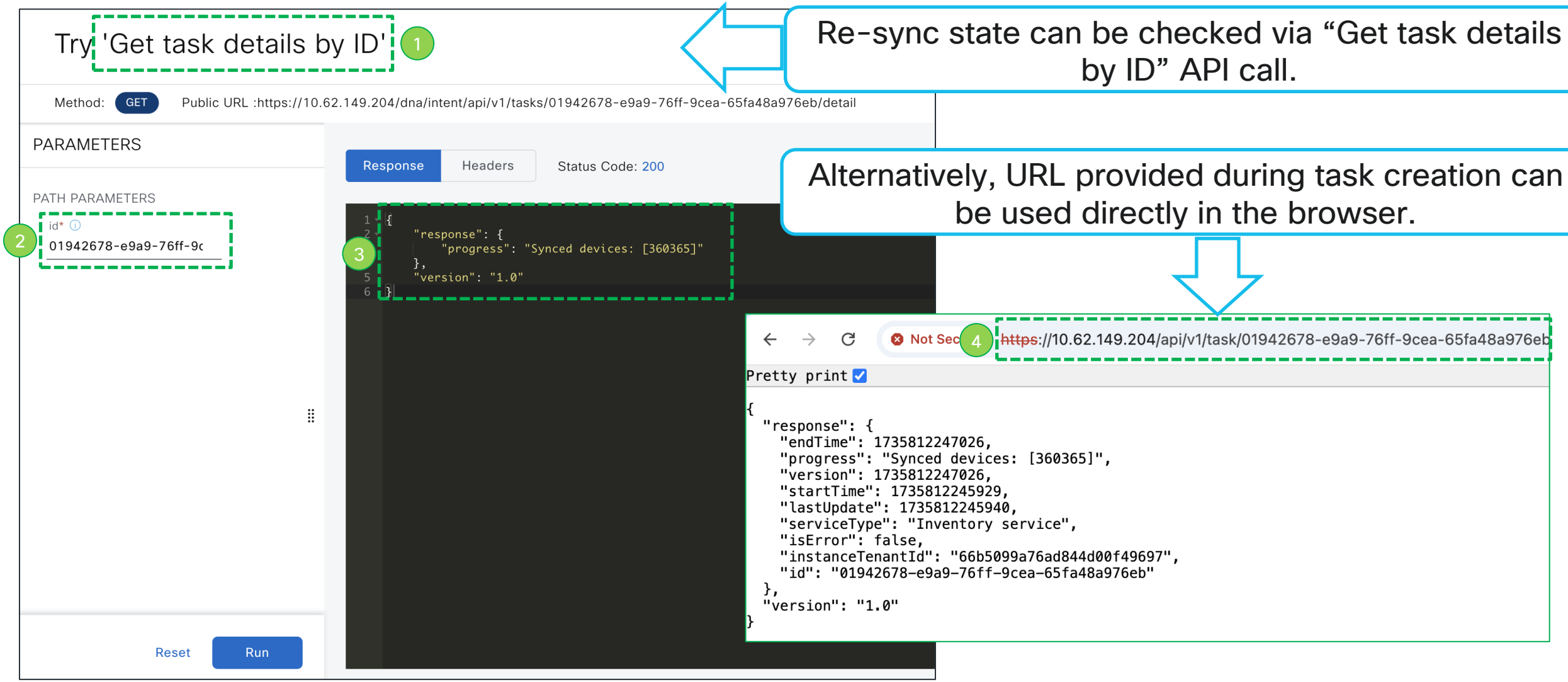


Note: forceSync API requires internal device ID to run (not the IP address, hostname, or UUID). The simplest way to obtain it is through Grafana (refer to the next slides).

Catalyst Center: Manageability – force re-sync via API

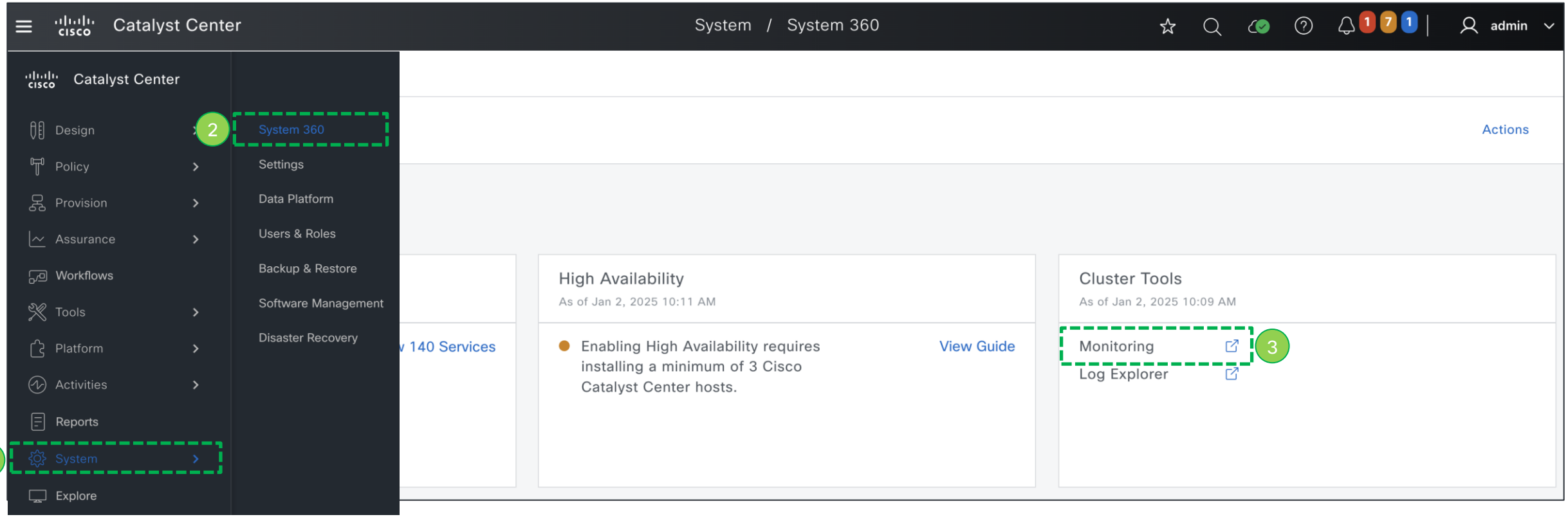


Catalyst Center: Manageability – force re-sync via API



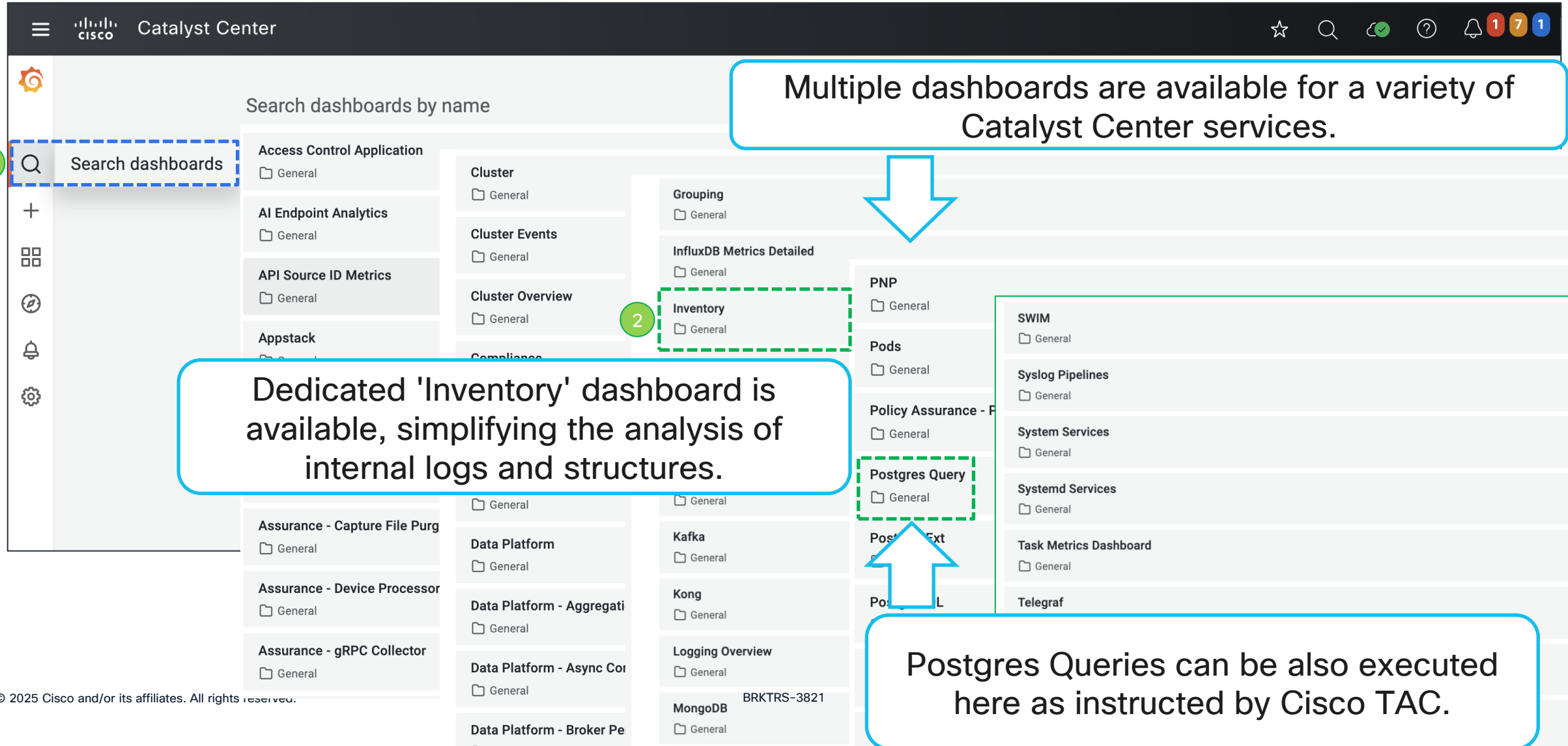
Catalyst Center: Logs and Database Insights (Grafana)

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

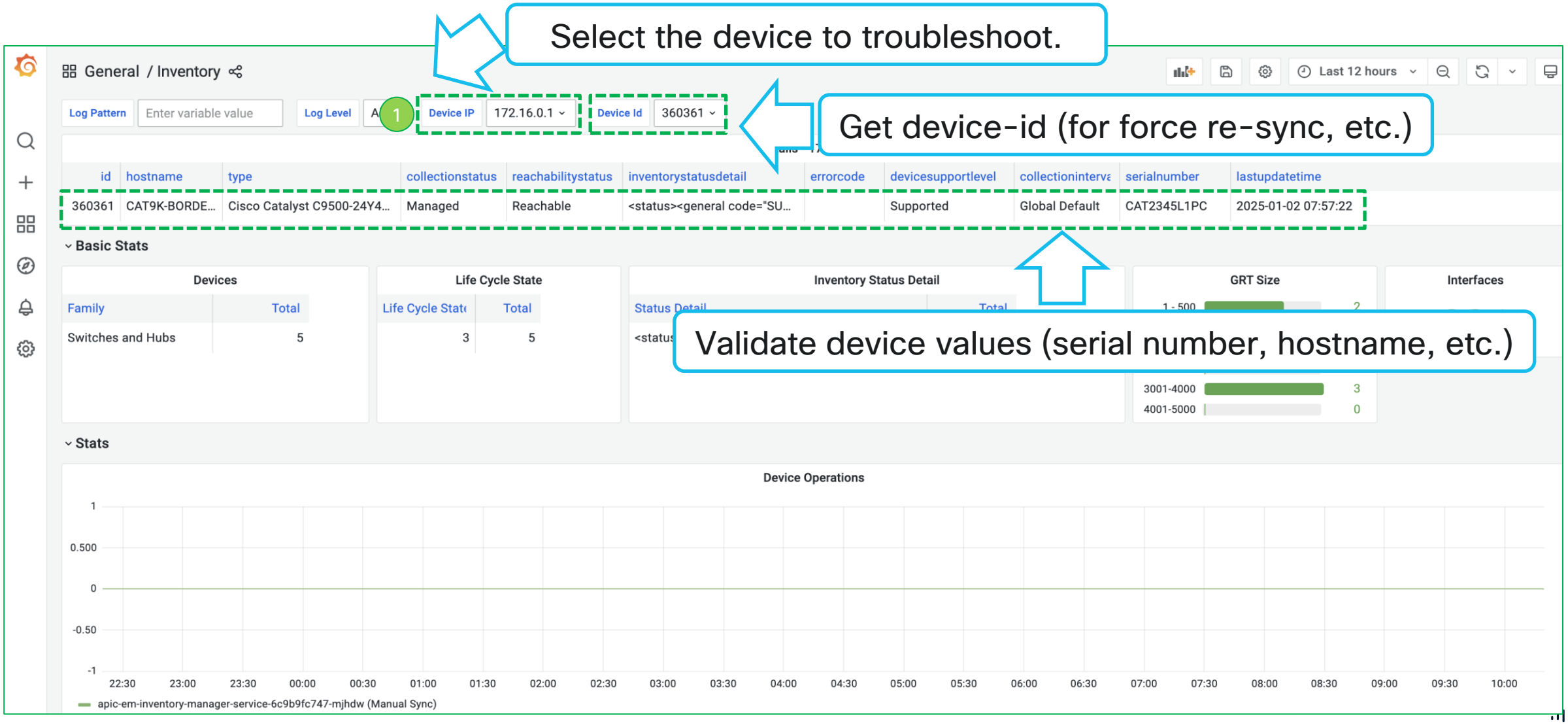


Catalyst Center provides advanced monitoring capabilities through 3rd party tool: Grafana

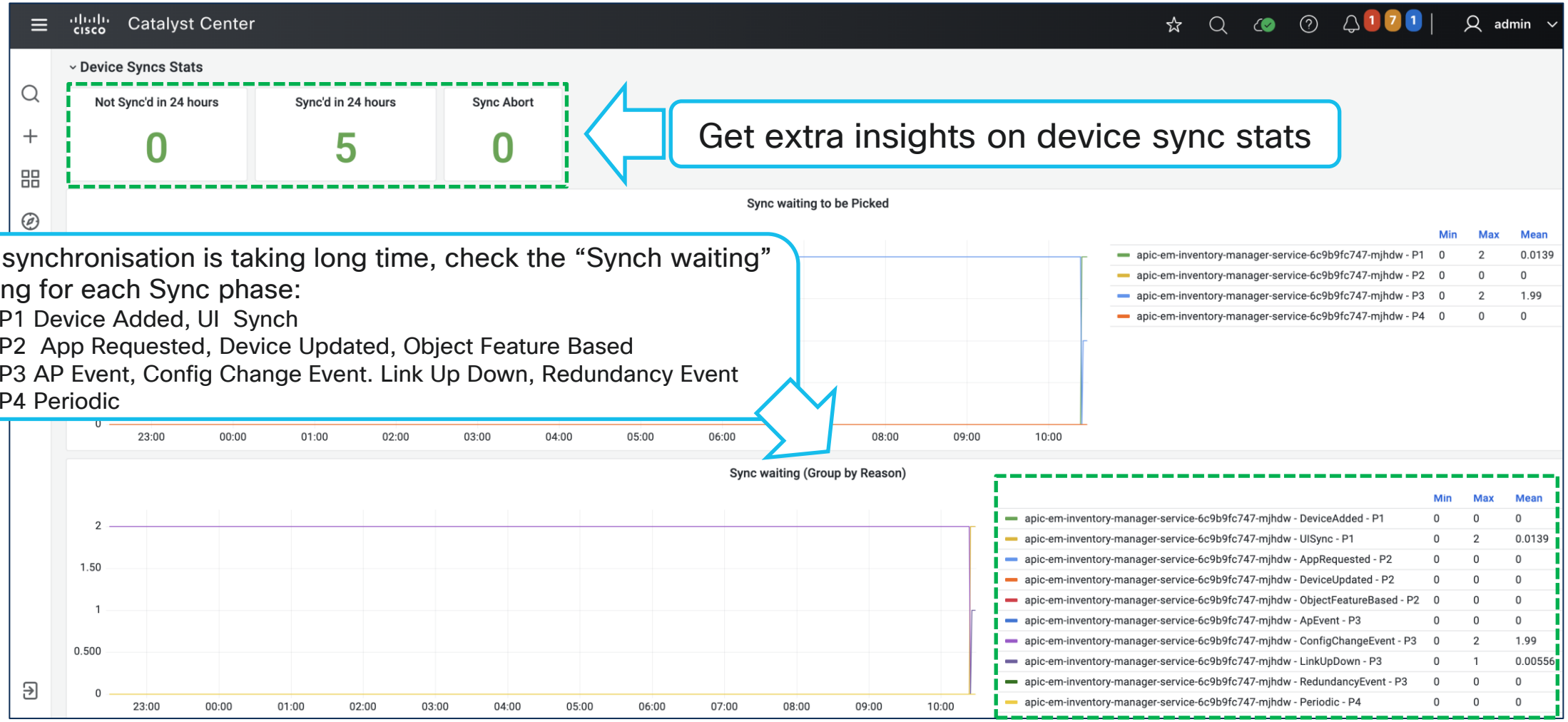
Catalyst Center: Logs and Database Insights (Grafana)



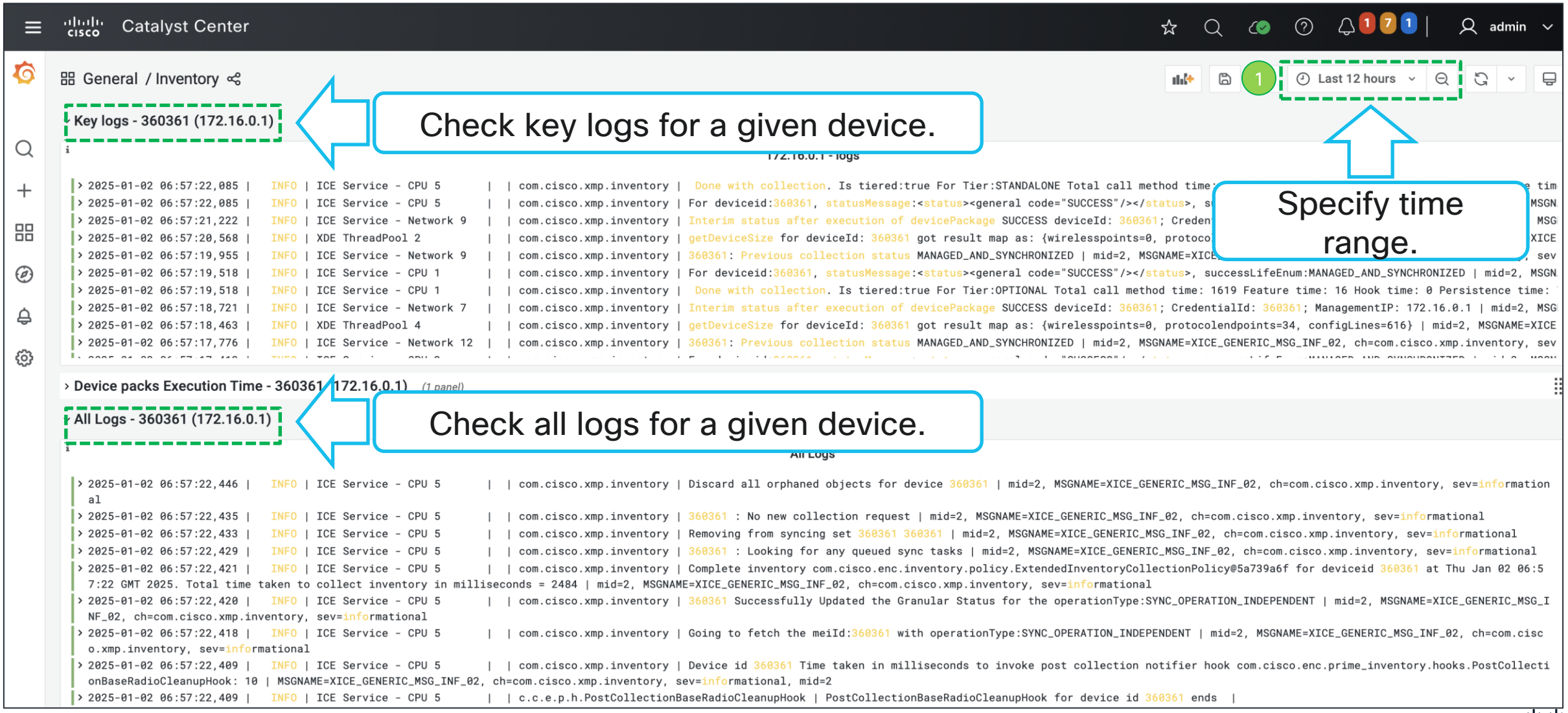
Catalyst Center: Logs and Database Insights (Grafana)



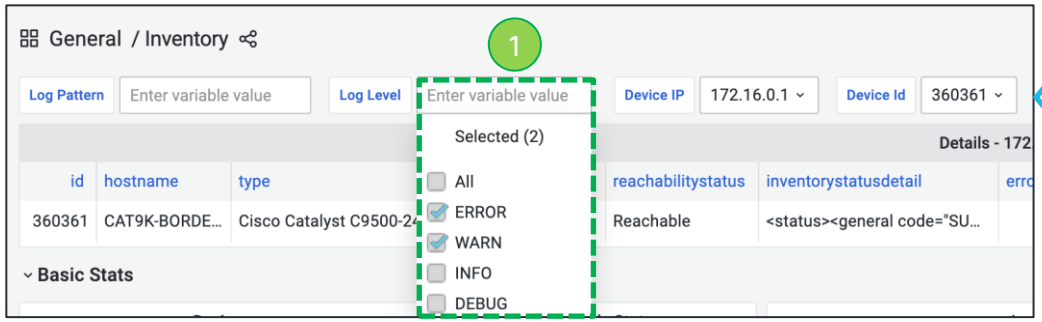
Catalyst Center: Logs and Database Insights (Grafana)



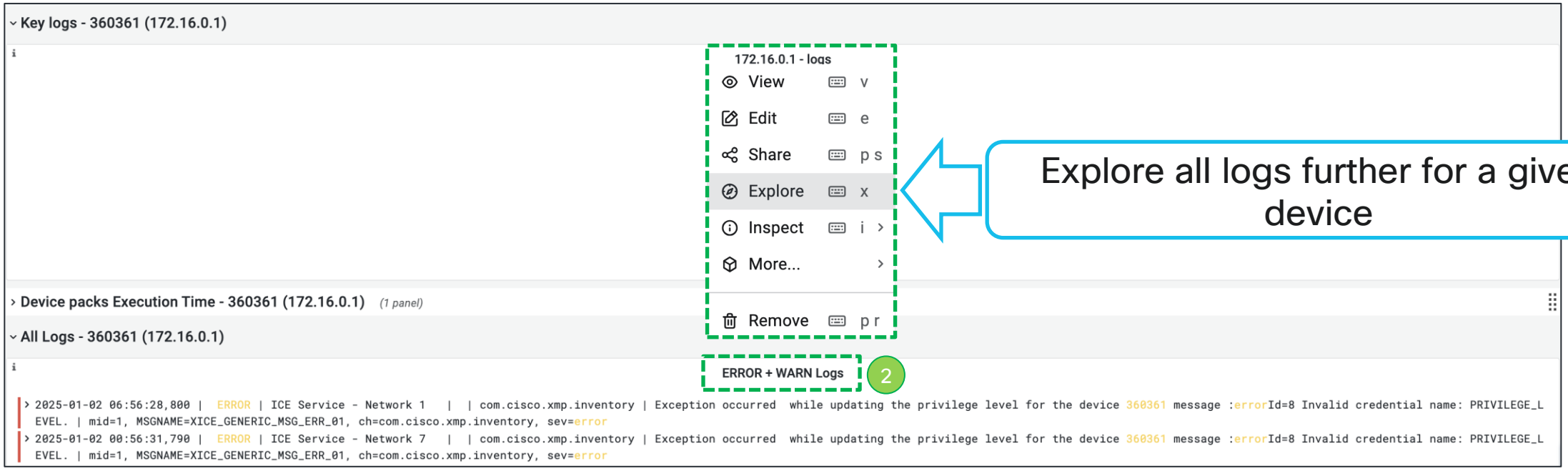
Catalyst Center: Logs and Database Insights (Grafana)



Catalyst Center: Logs and Database Insights (Grafana)

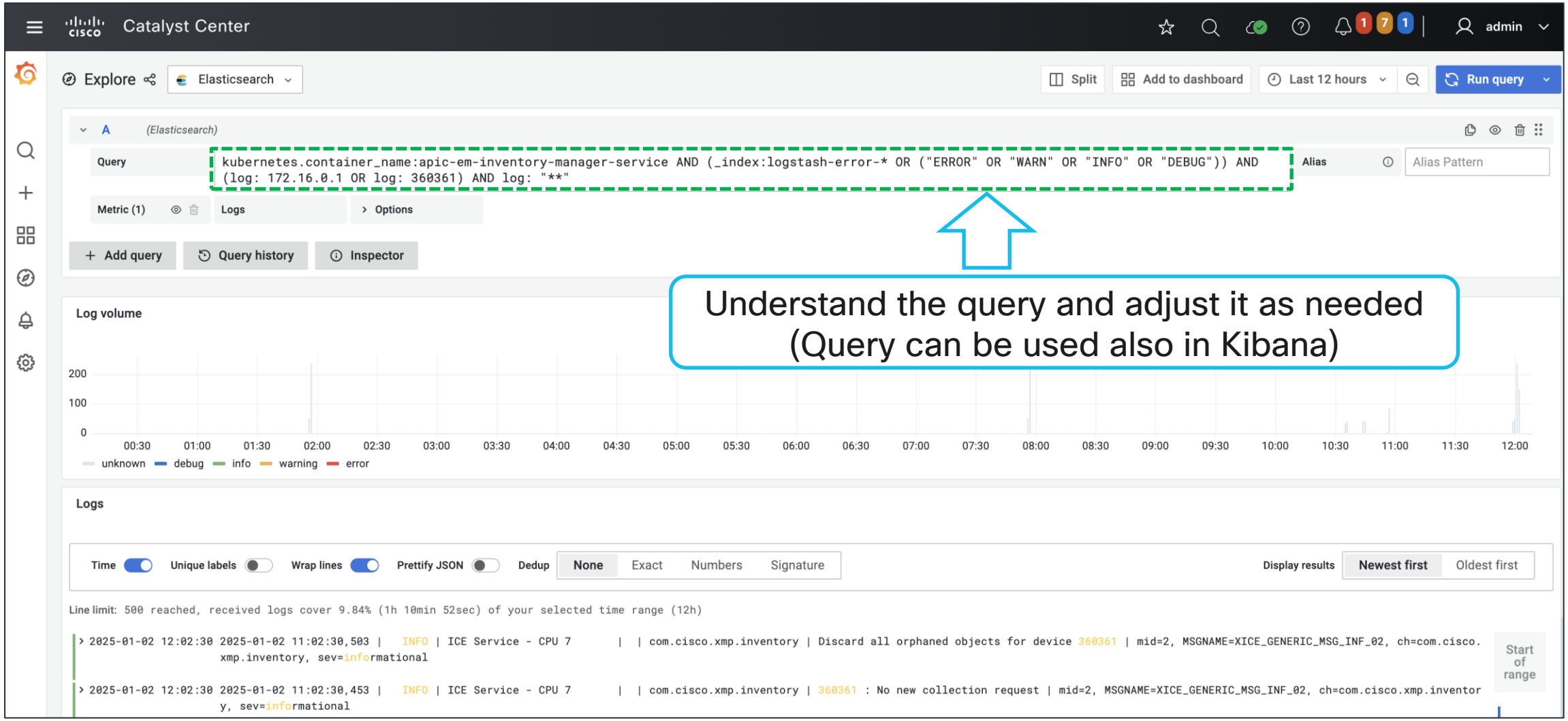


Filter logs further based on severity.



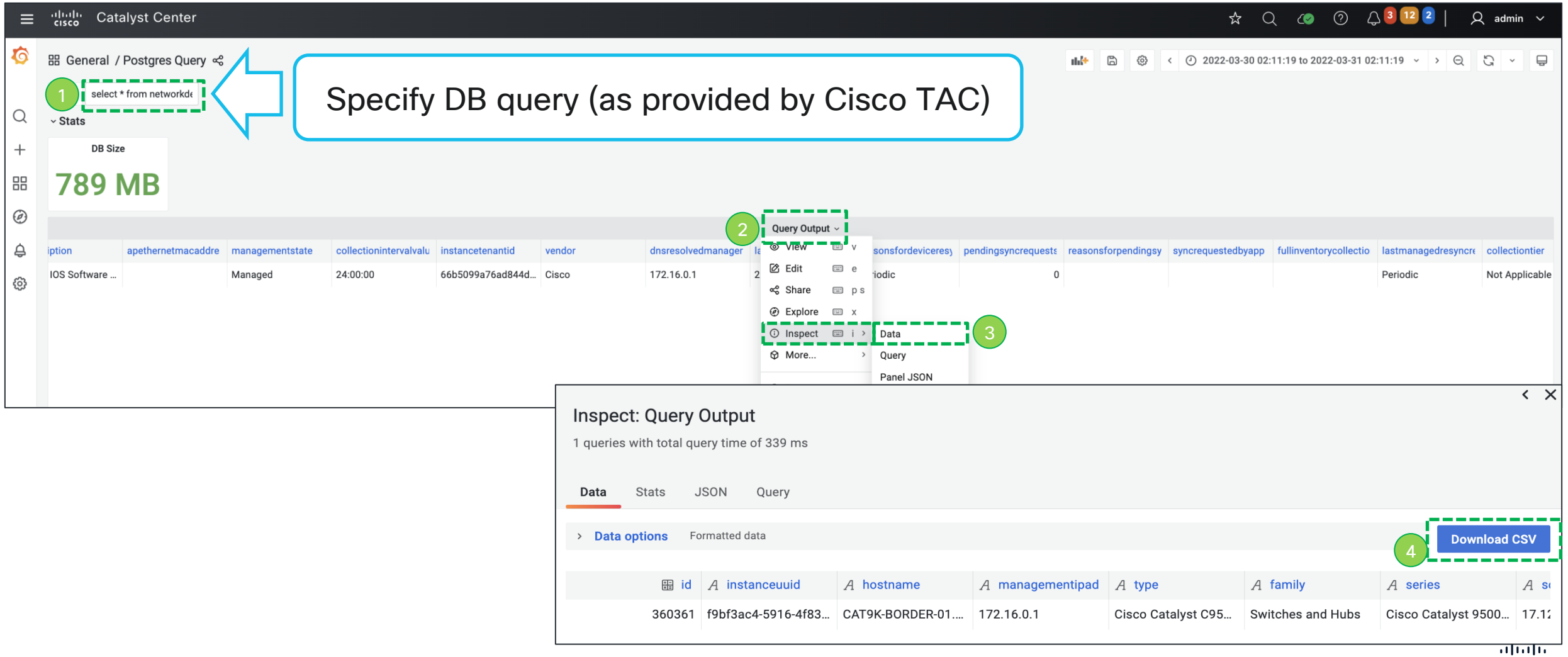
Explore all logs further for a given device

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.



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.

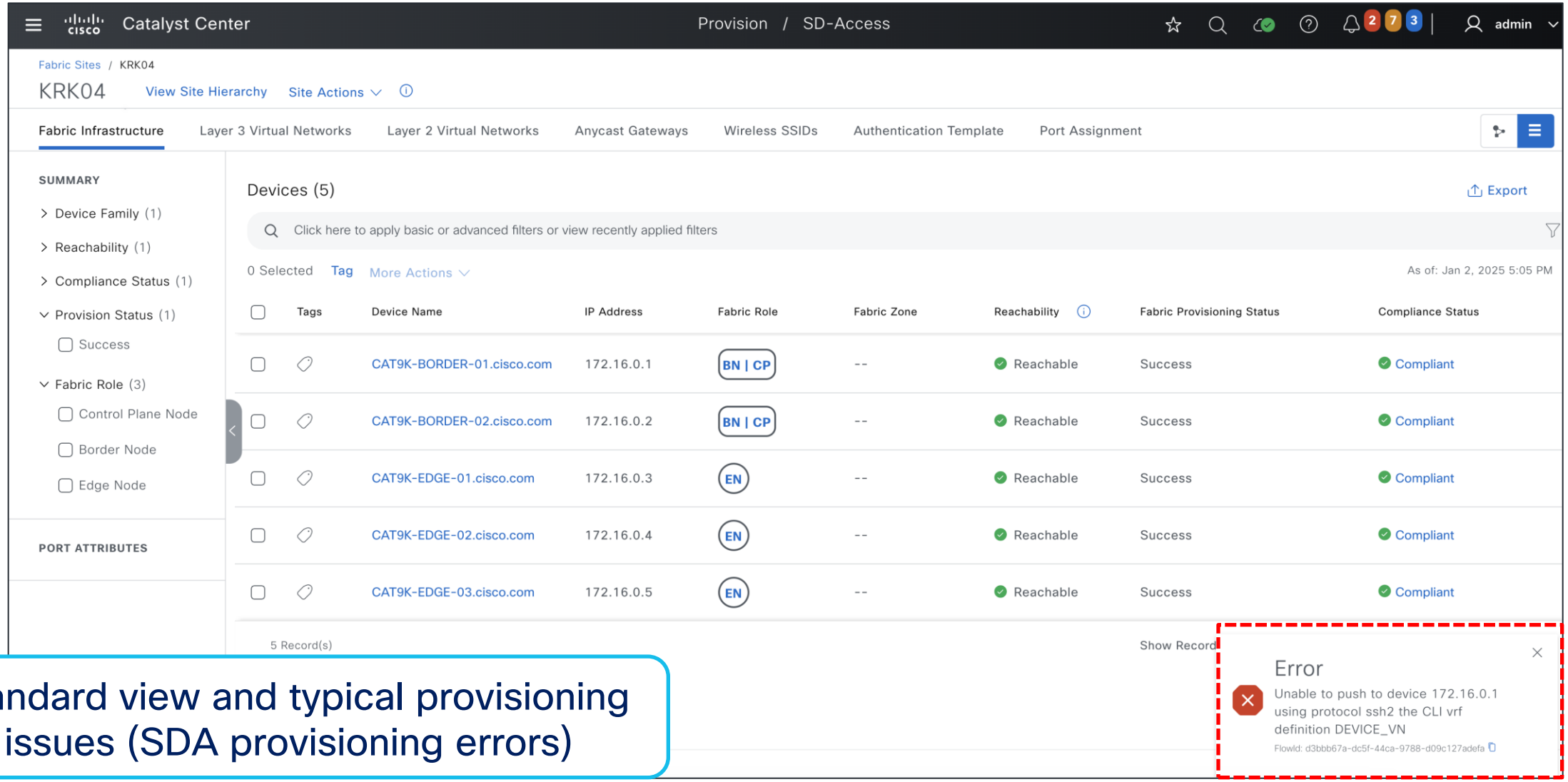
3. DB Queries: Use Postgres Query Dashlet to effectively run and collect data required by Cisco TAC.

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

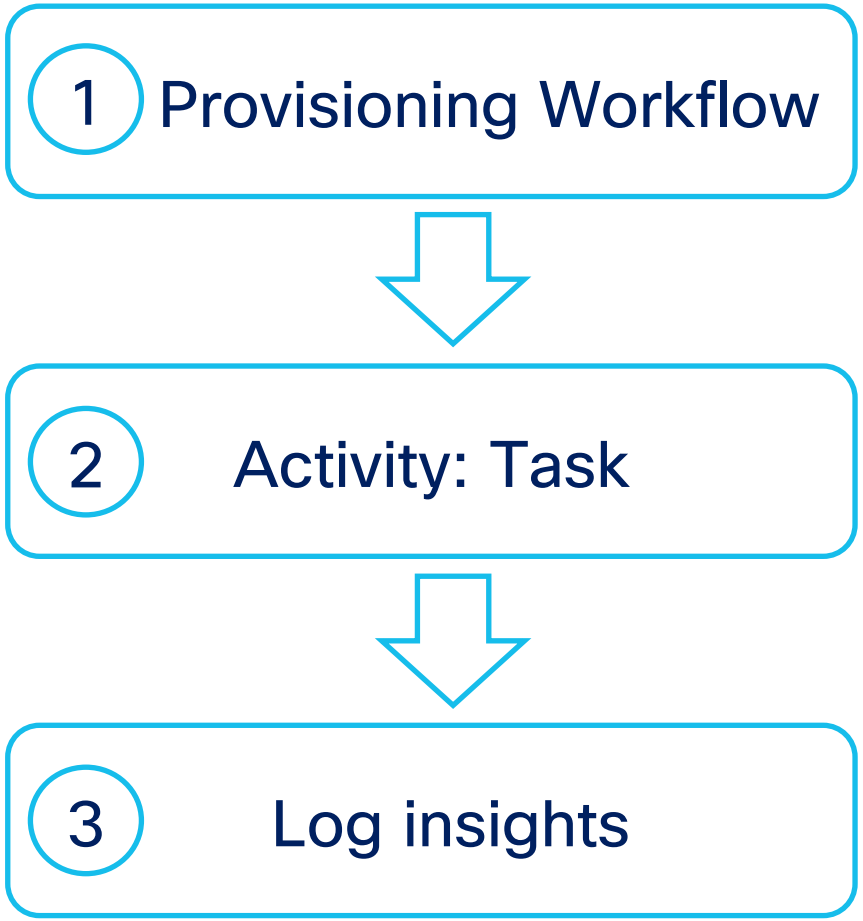
Catalyst Center: Provisioning workflow



Standard view and typical provisioning issues (SDA provisioning errors)

Catalyst Center: Provisioning
Troubleshooting workflow and issue triage

For Your Reference



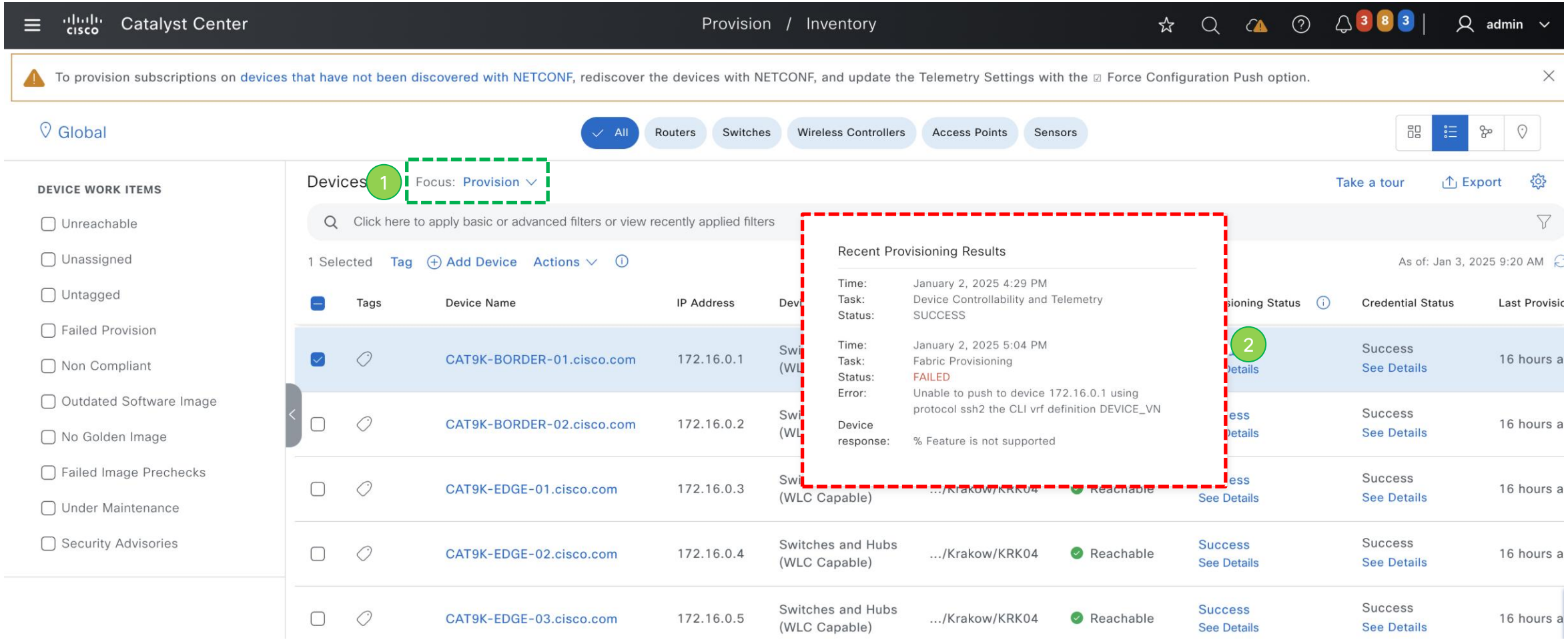
1a) Validate provisioning status in Inventory page (Focus: Provisioning)

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.

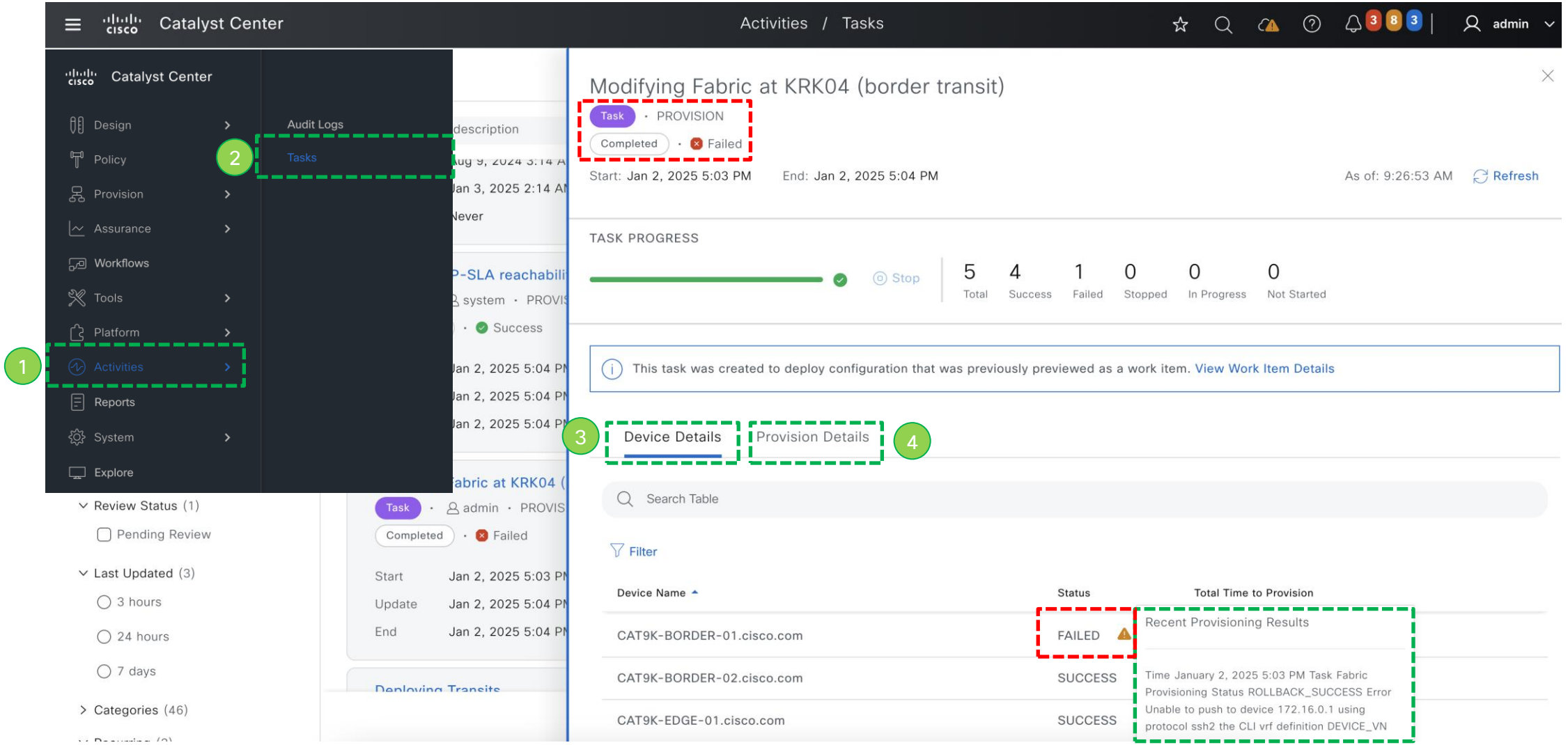
Catalyst Center: Provisioning

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



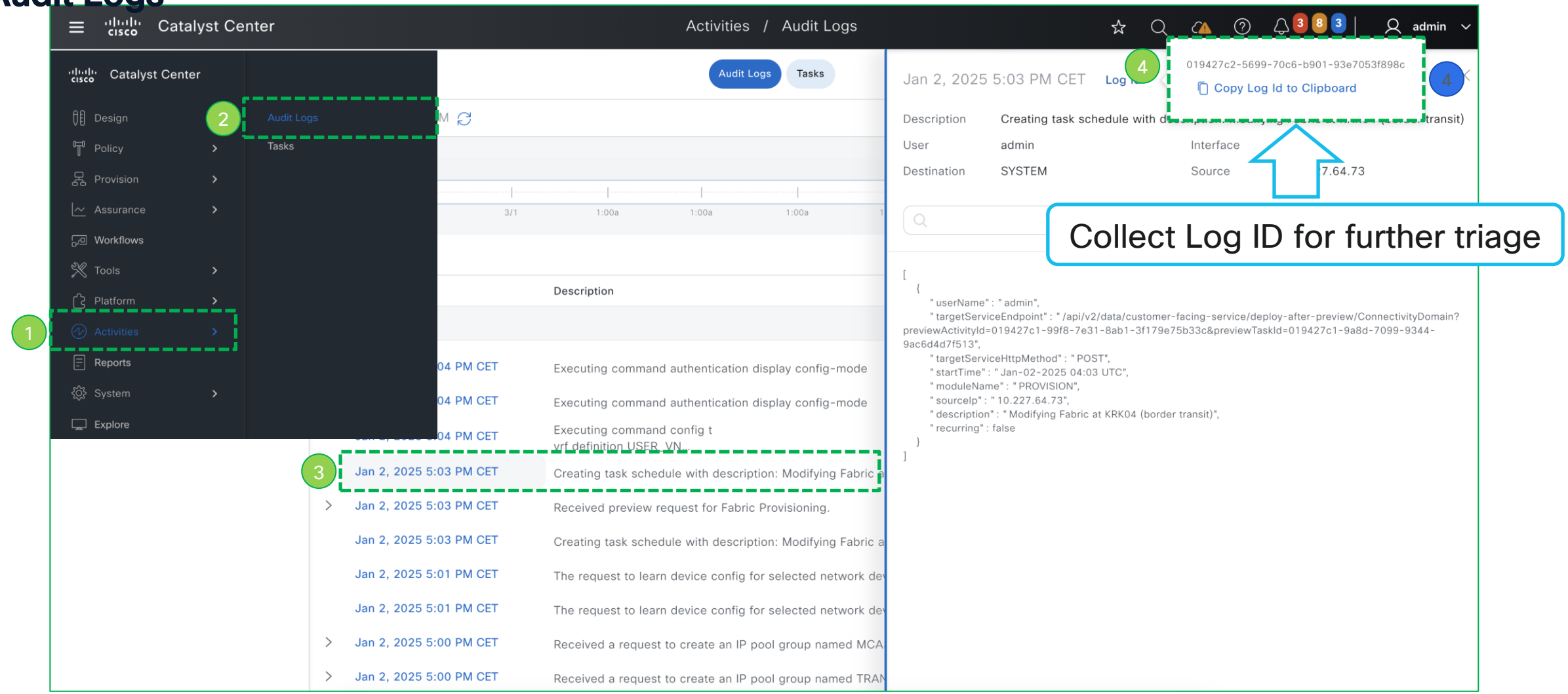
Catalyst Center: Activity – Tasks

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



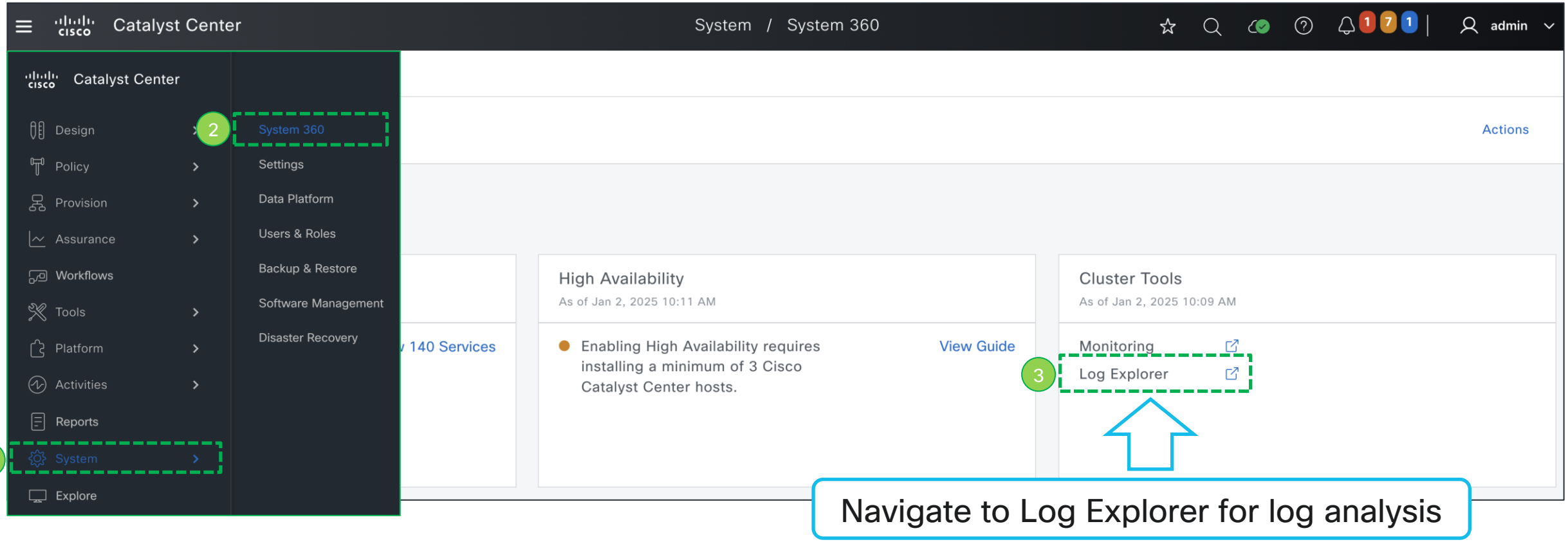
Catalyst Center: Activity – Audit Logs

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

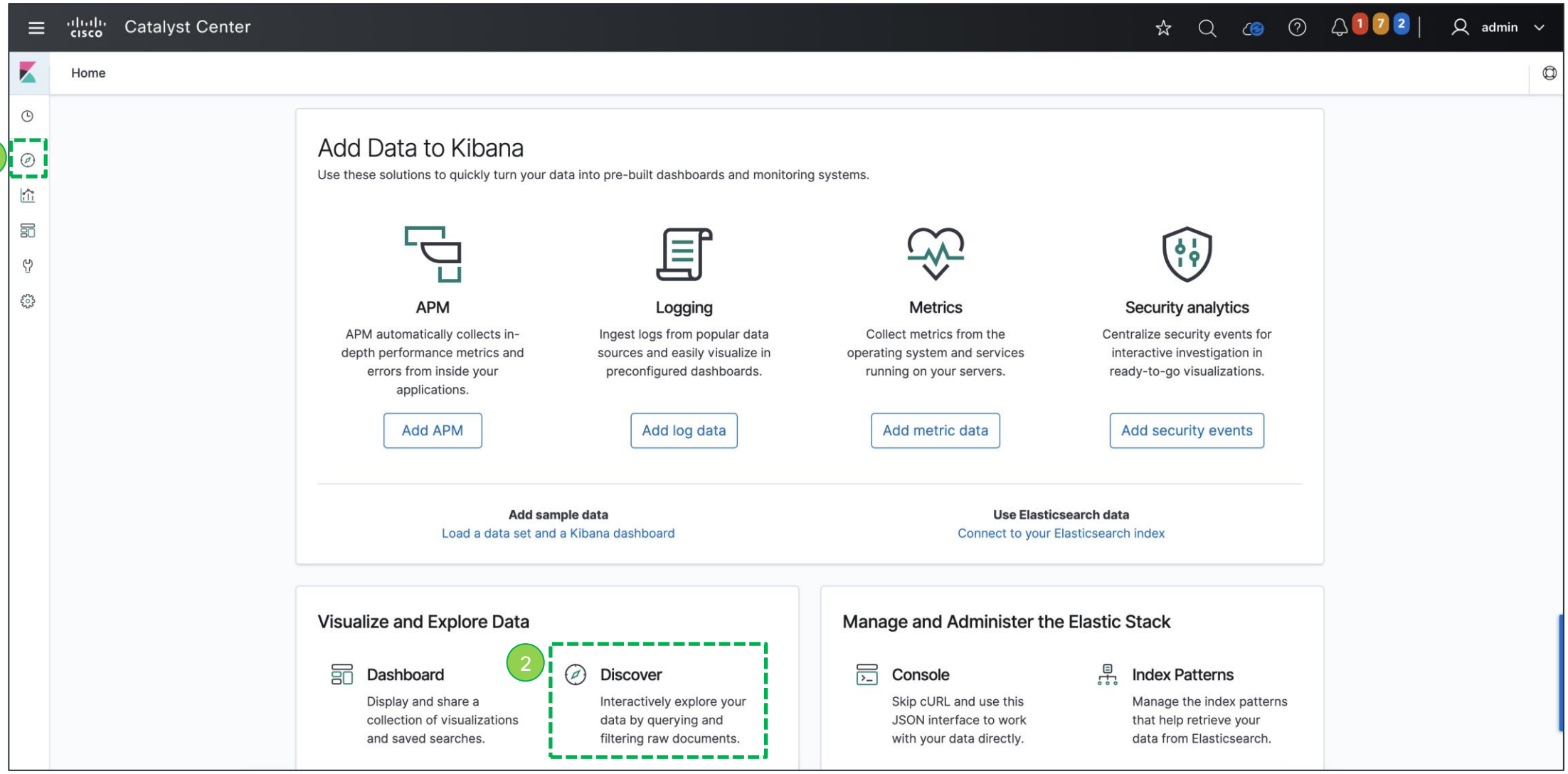


Catalyst Center: Log Explorer

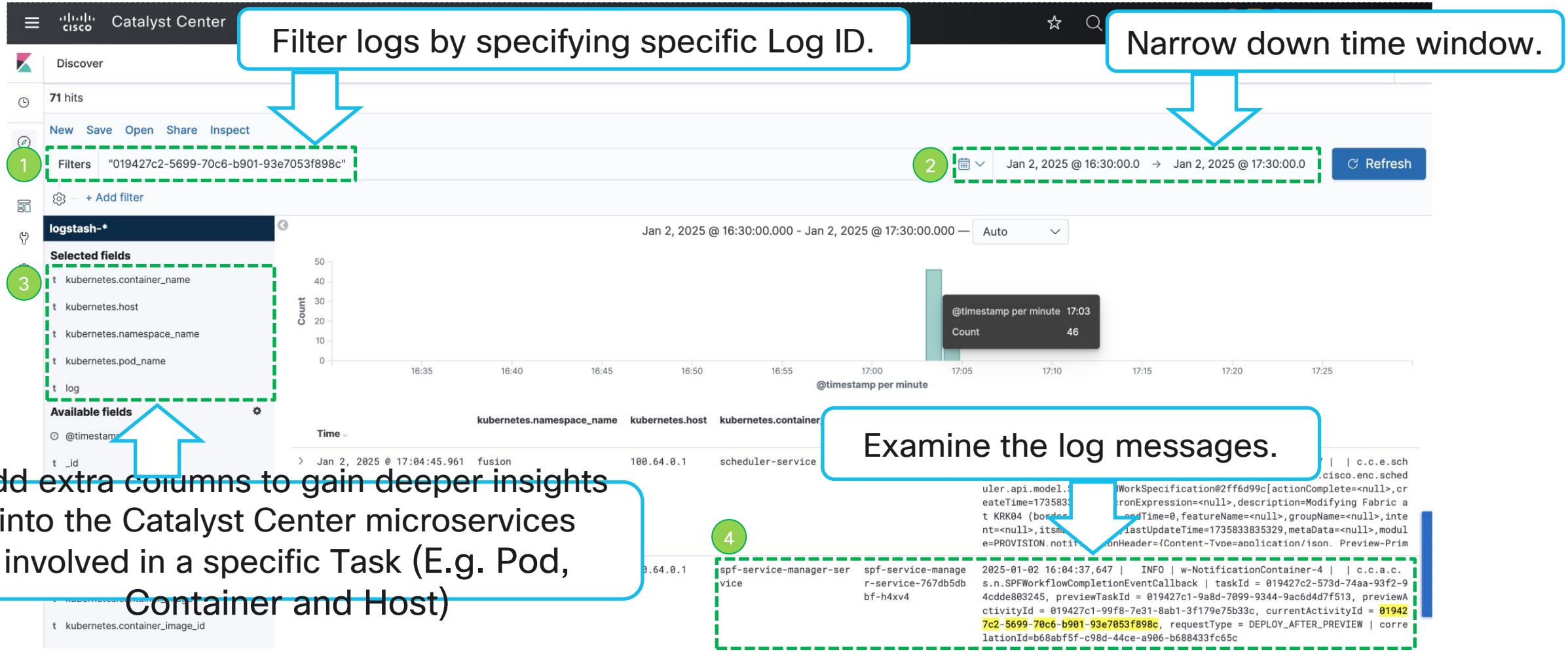
Tip #3a): Use Log Explorer (Kibana) to find all relevant log messages for a given Task:
System > System 360 > Log Explorer



Catalyst Center: Log Explorer (Kibana)



Catalyst Center: Log Explorer (Kibana)



Catalyst Center: Log Messages

Example: ActivityIDs & correlatonIds

Table JSON

clock	@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-46f0-9afd-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-Notifica…ntainer-4 | | c.c.a.c.s.n.SPFWorkflowCompletionEventCallback | taskId = 01942…-74aa-93f2-94cdde803245, previewTaskId = 019427c1-…8d-7099-9344-9ac6d4d7f513, previewActivityId = 019427c1-99f8-7e31-8ab1-3f179e75b33c, current…tActivityId = 019427c2-5699-70c6-b901-93e7053f898c, 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

Activity ID

Correlation ID

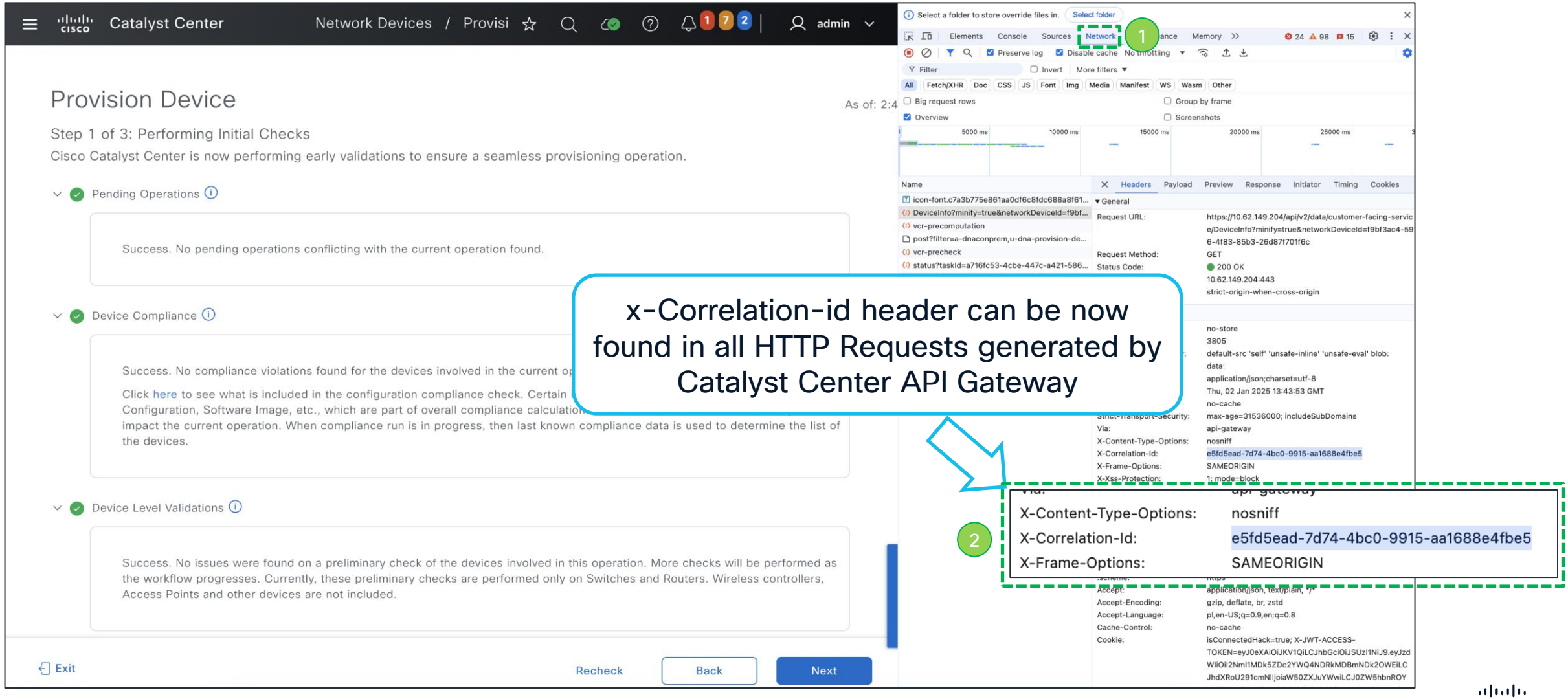
Catalyst Center – Log IDs

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.

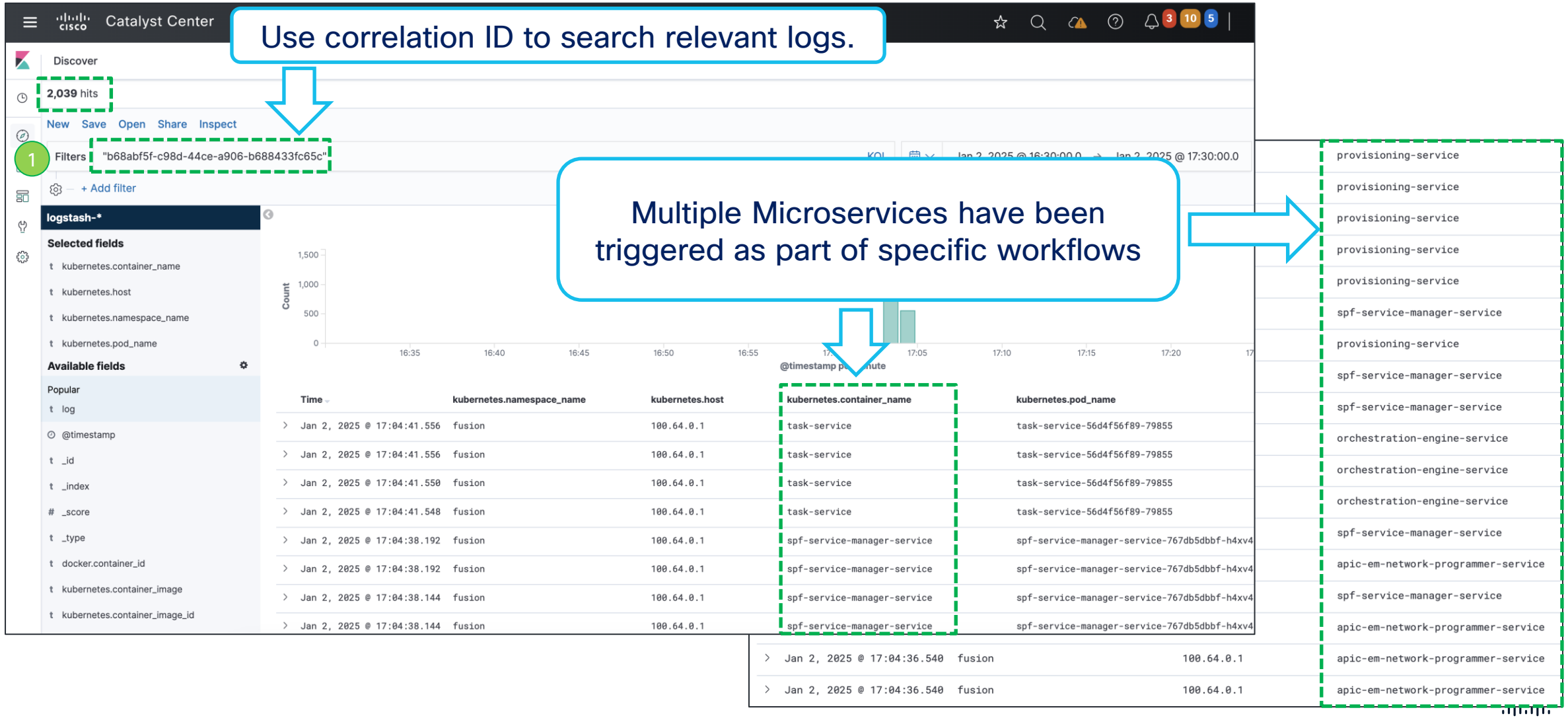
Catalyst Center: Log Explorer

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



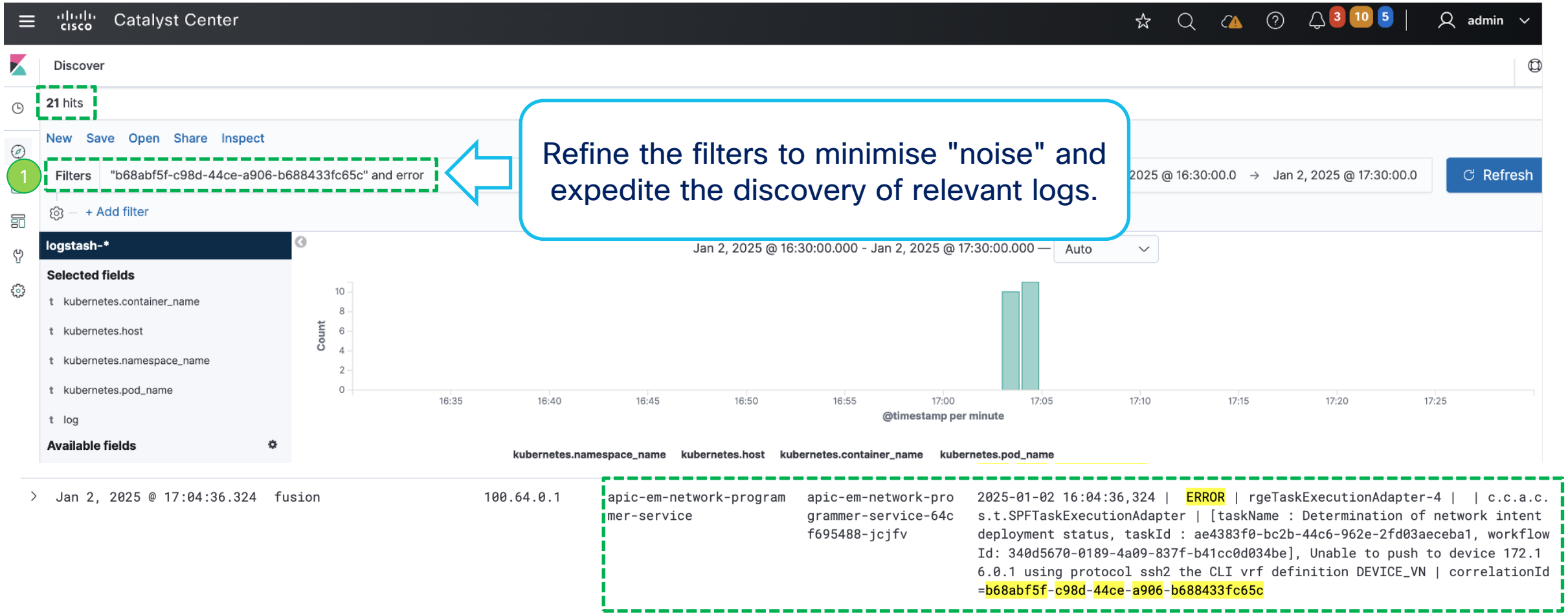
Catalyst Center : Log Explorer (Kibana)

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.



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:

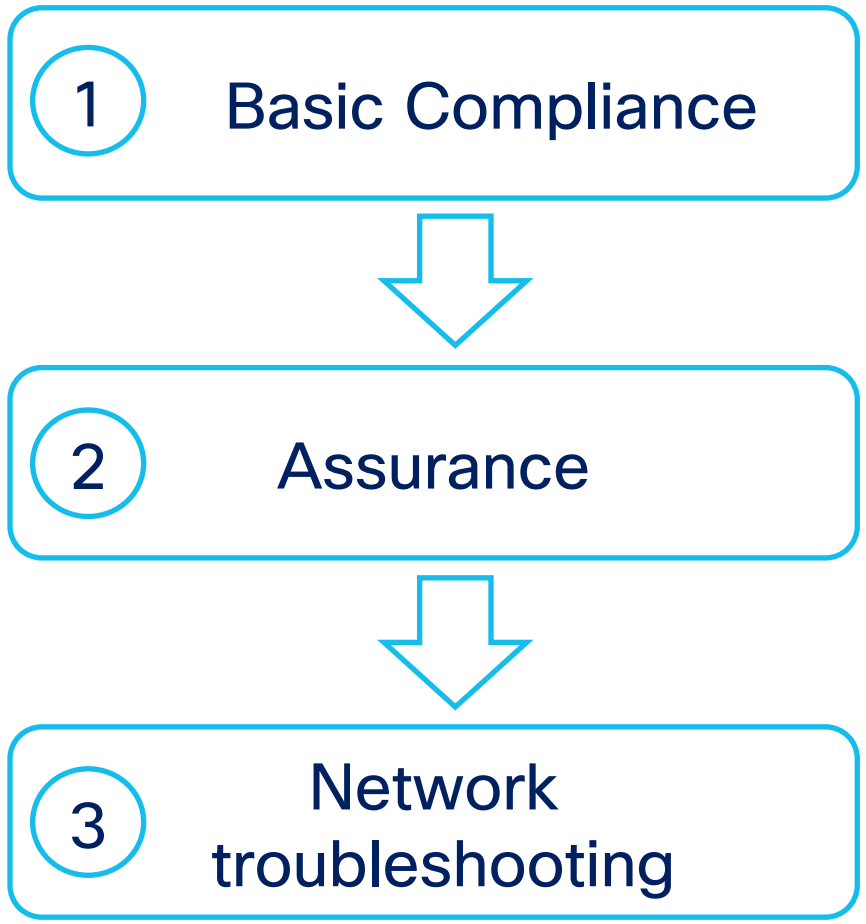
IP address assigned by Automatic Private IP Addressing (APIPA) feature.

```
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

For Your Reference



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

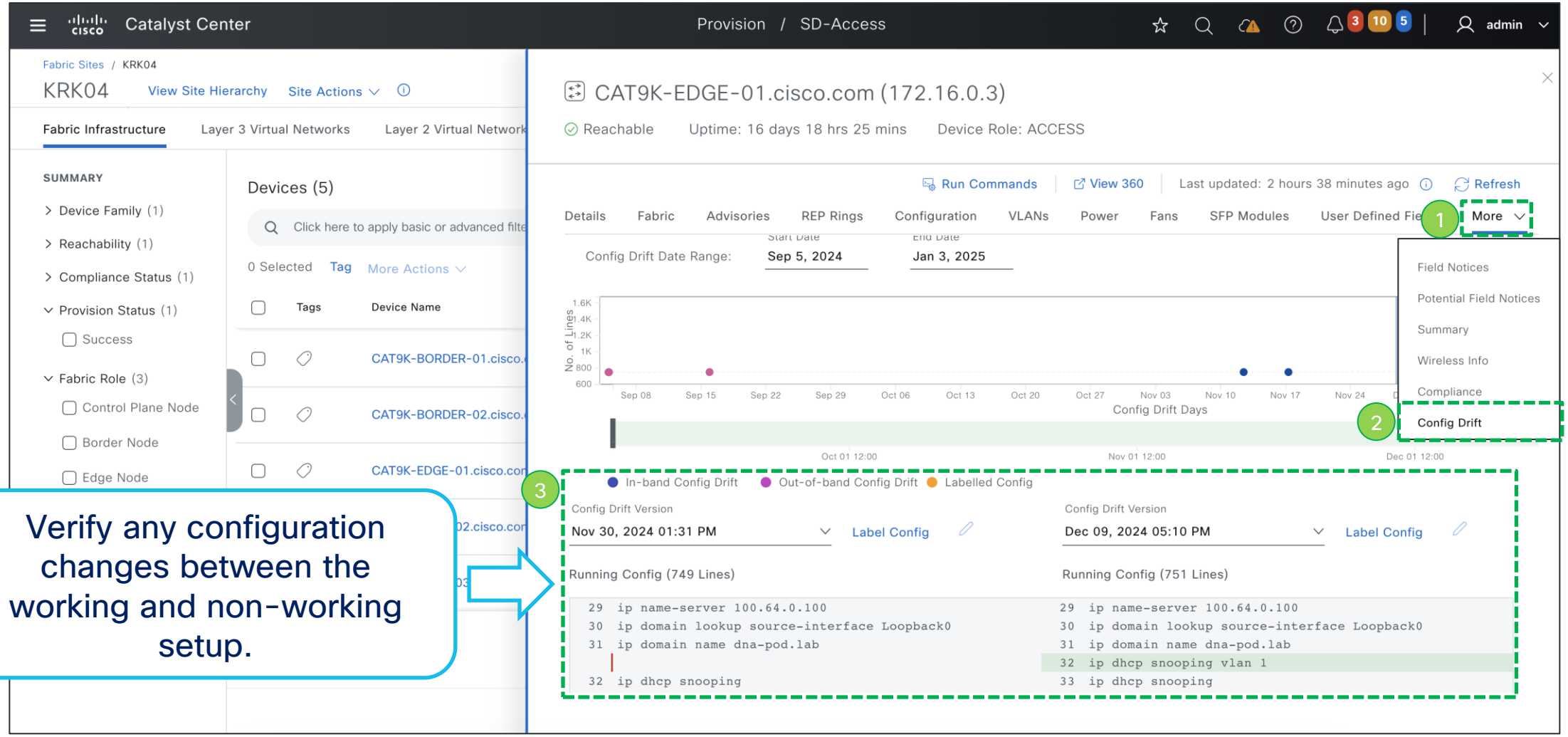
3a) Perform Network troubleshooting via Command Runner
3b) Perform Network troubleshooting via Run Commands

Fabric sites – Provisioning

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

Fabric Device – Config Drift

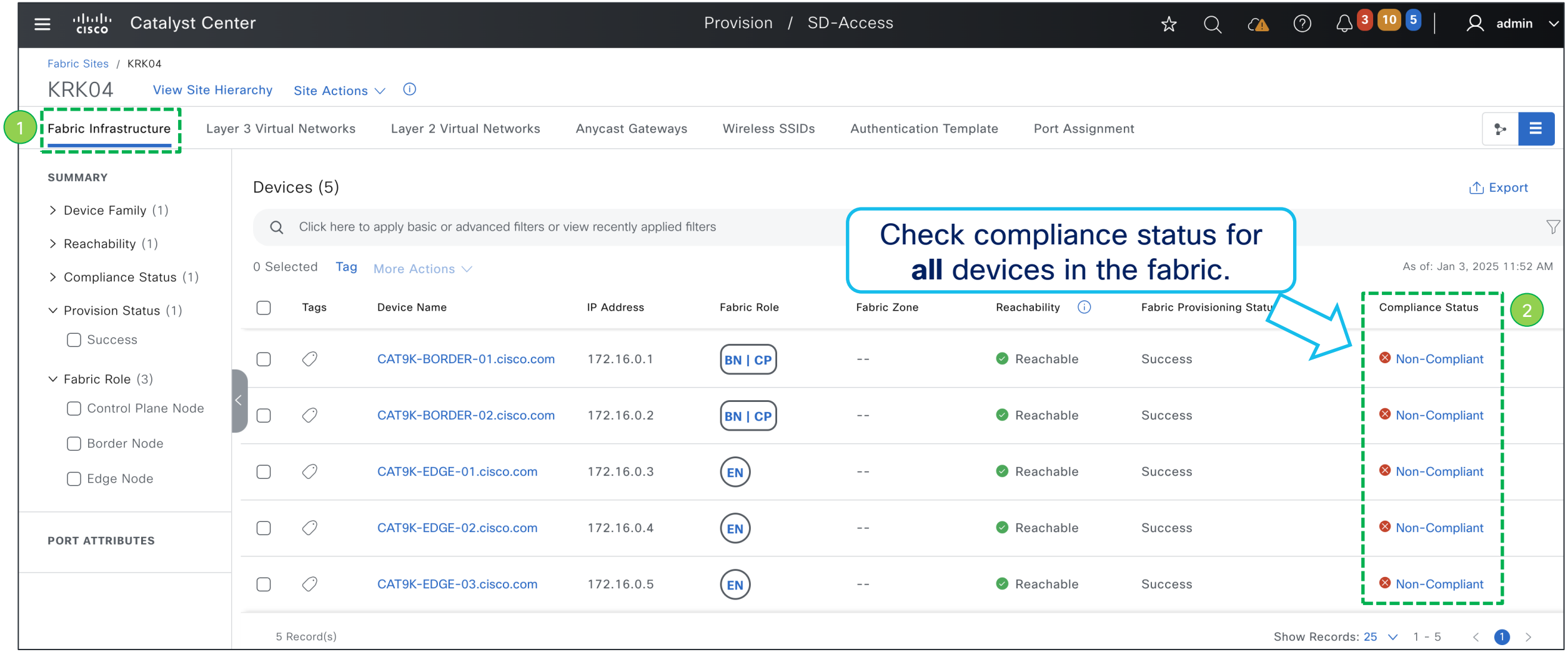
Tip #1b: Verify Configuration drift: **Fabric Infrastructure > Select the Device > More > Config Drift**



Verify any configuration changes between the working and non-working setup.

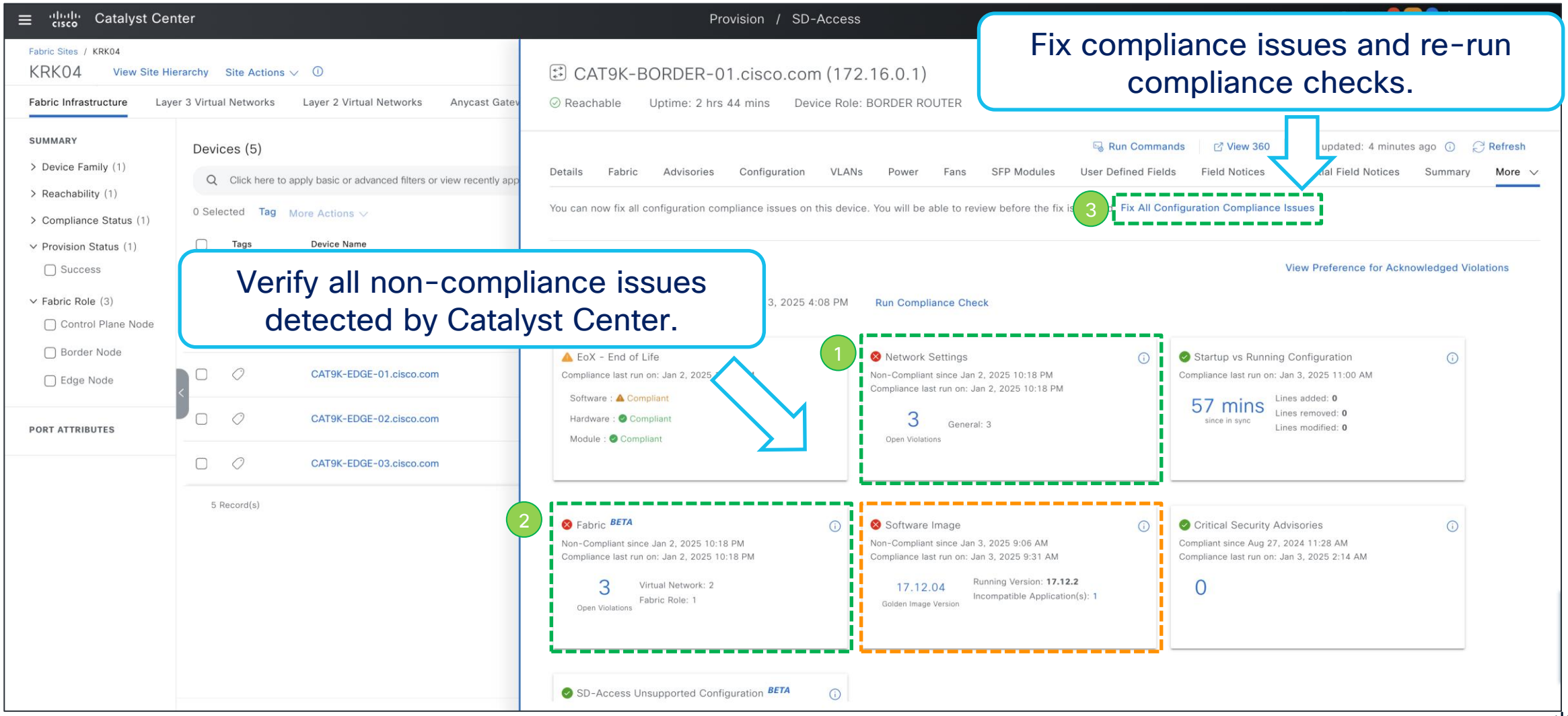
Fabric Infrastructure – Compliance

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

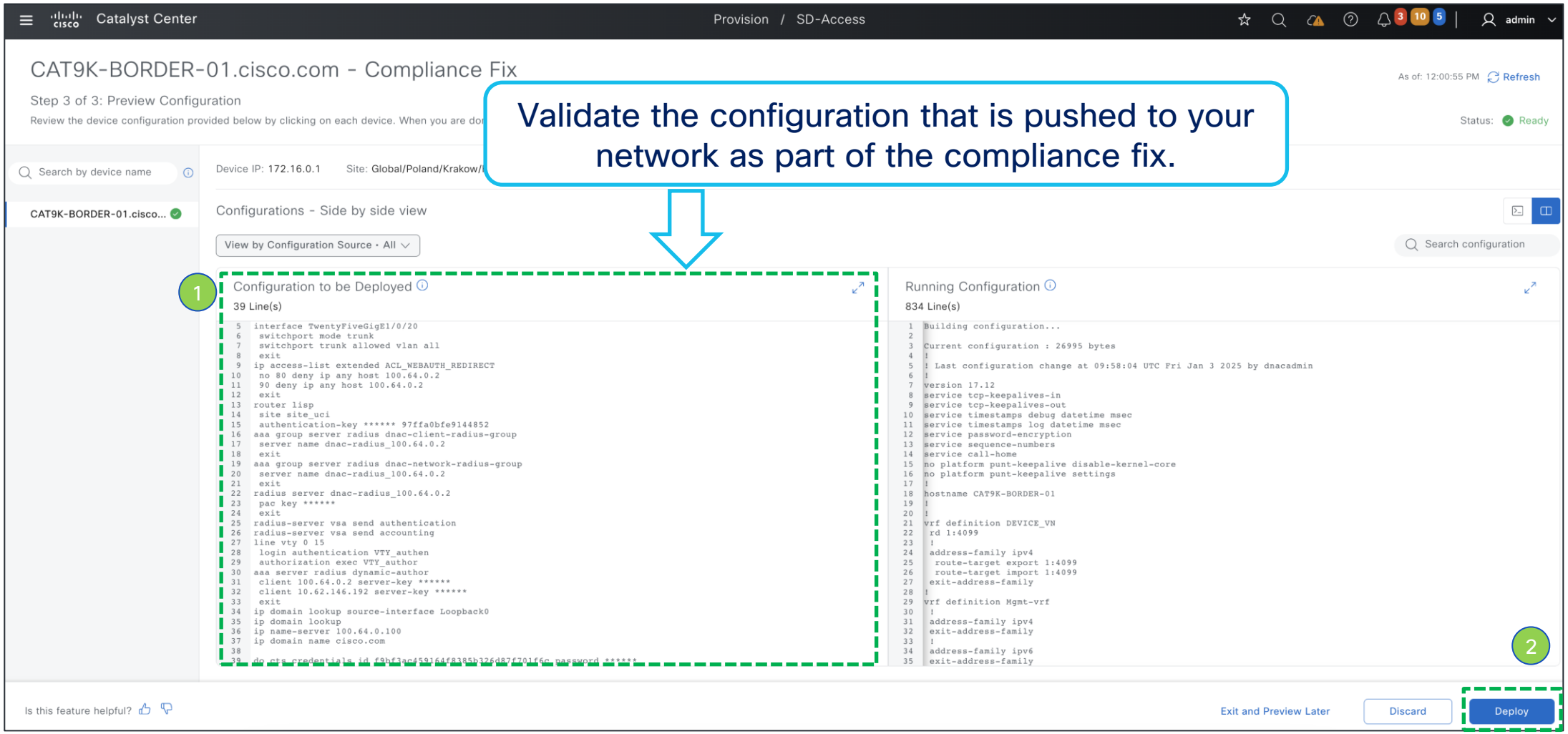


Compliance Summary

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

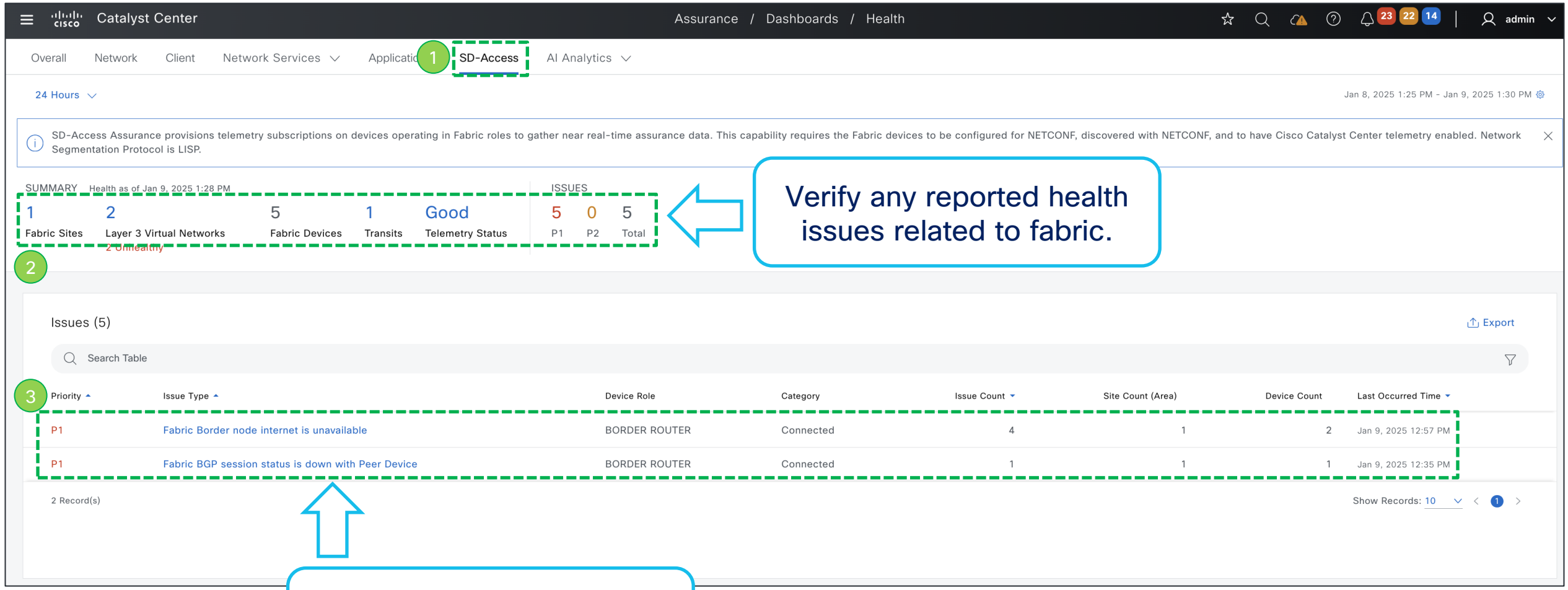


Compliance Fix – Configuration preview



Catalyst Center: SD Access Assurance

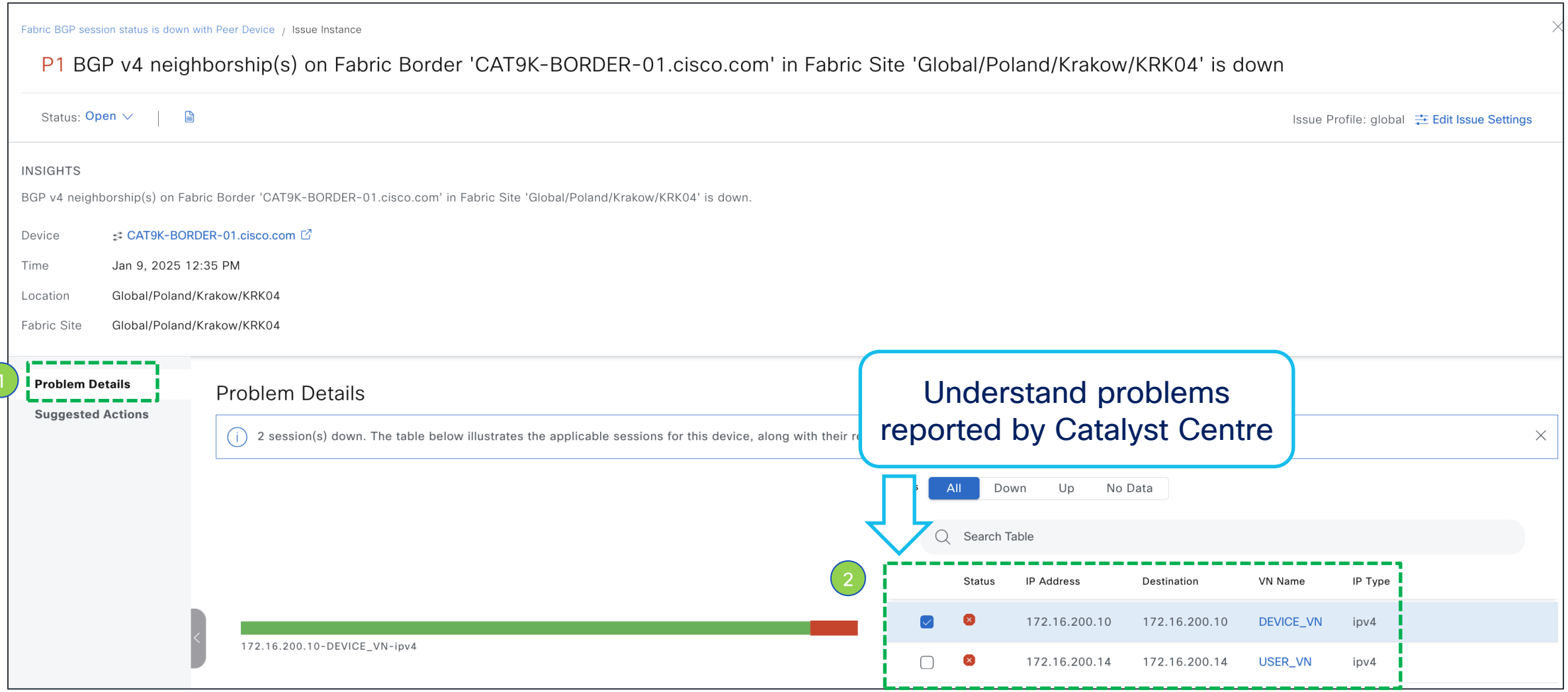
Tip #2a: Check Assurance data



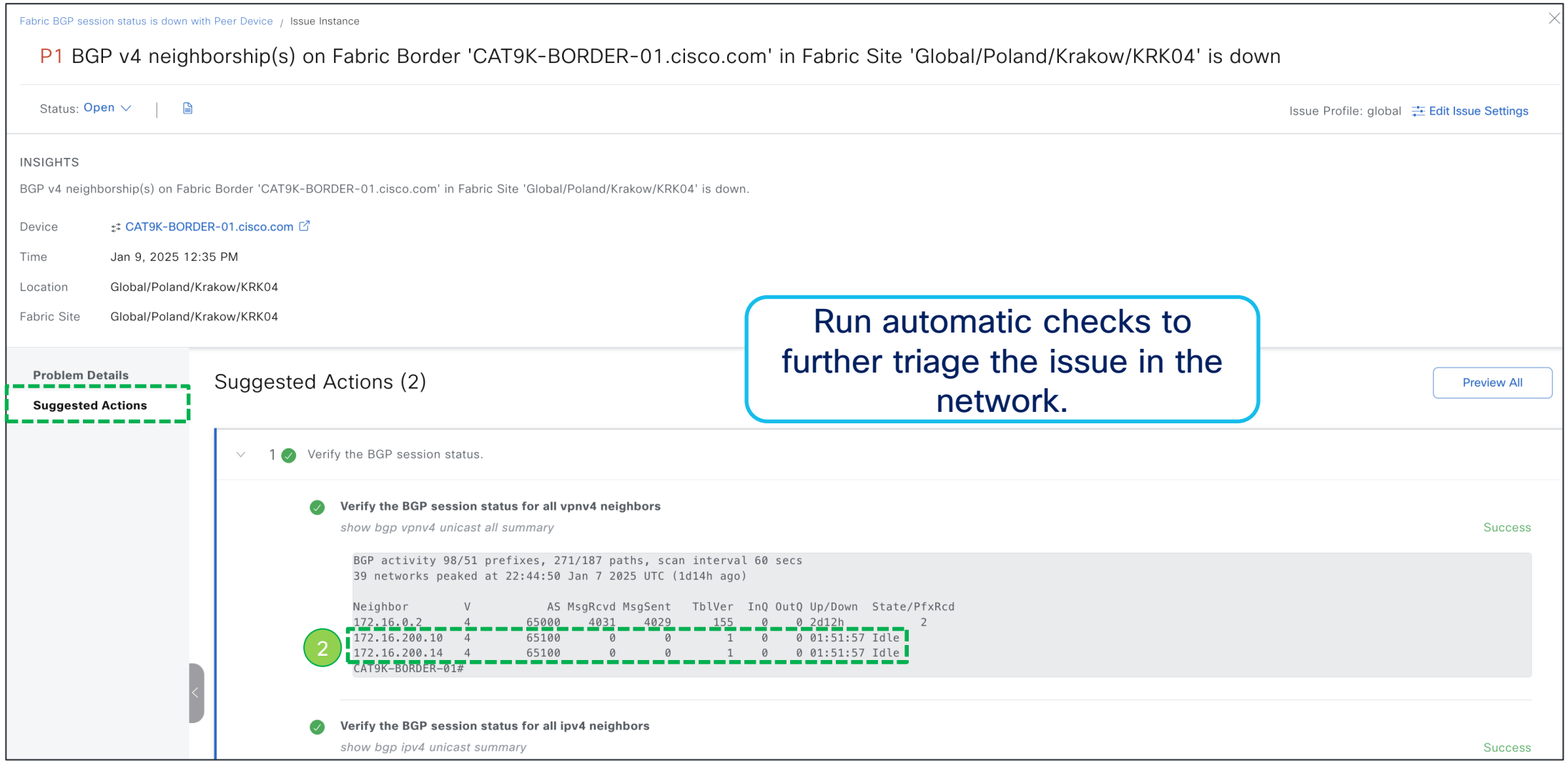
Verify any reported health issues related to fabric.

Check issues reported by Catalyst Centre.

Catalyst Center: SD Access Assurance

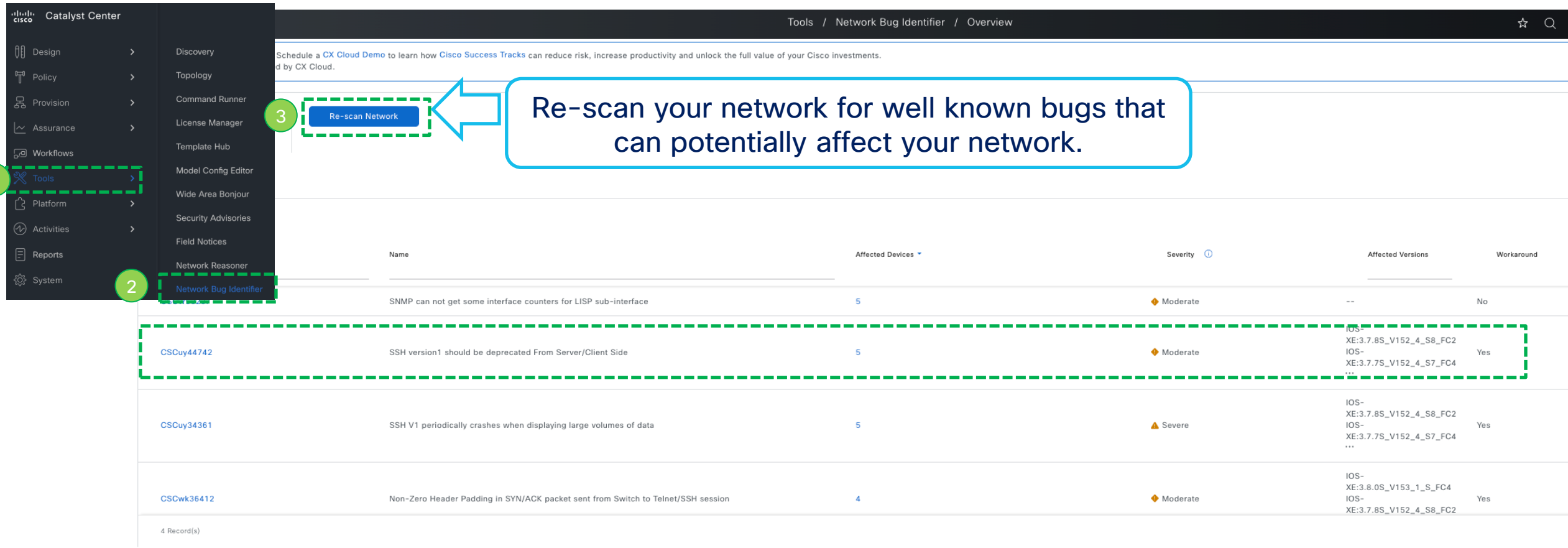


Catalyst Center: SD Access Assurance

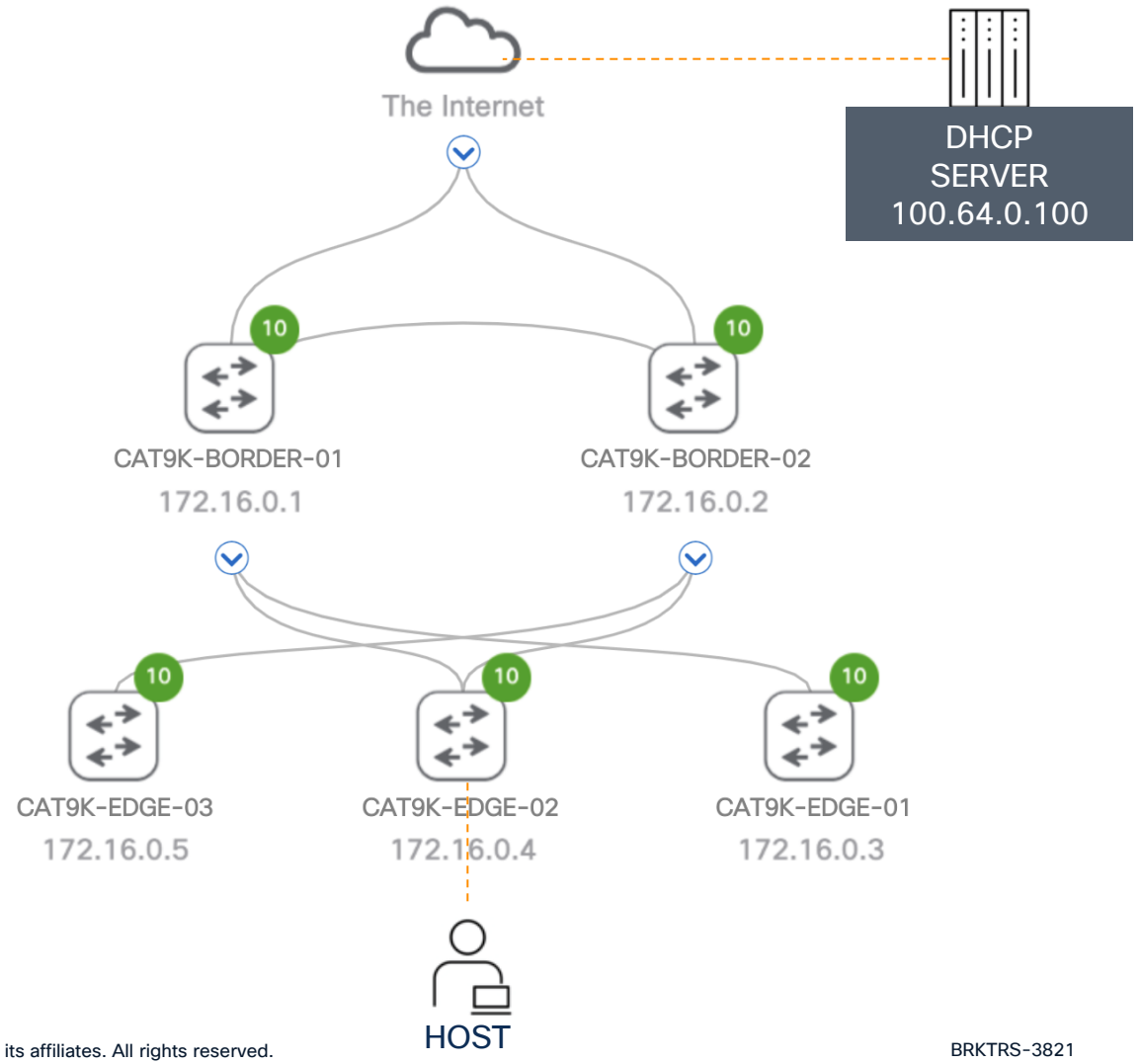


Catalyst Center: Network Troubleshooting (DHCP)

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

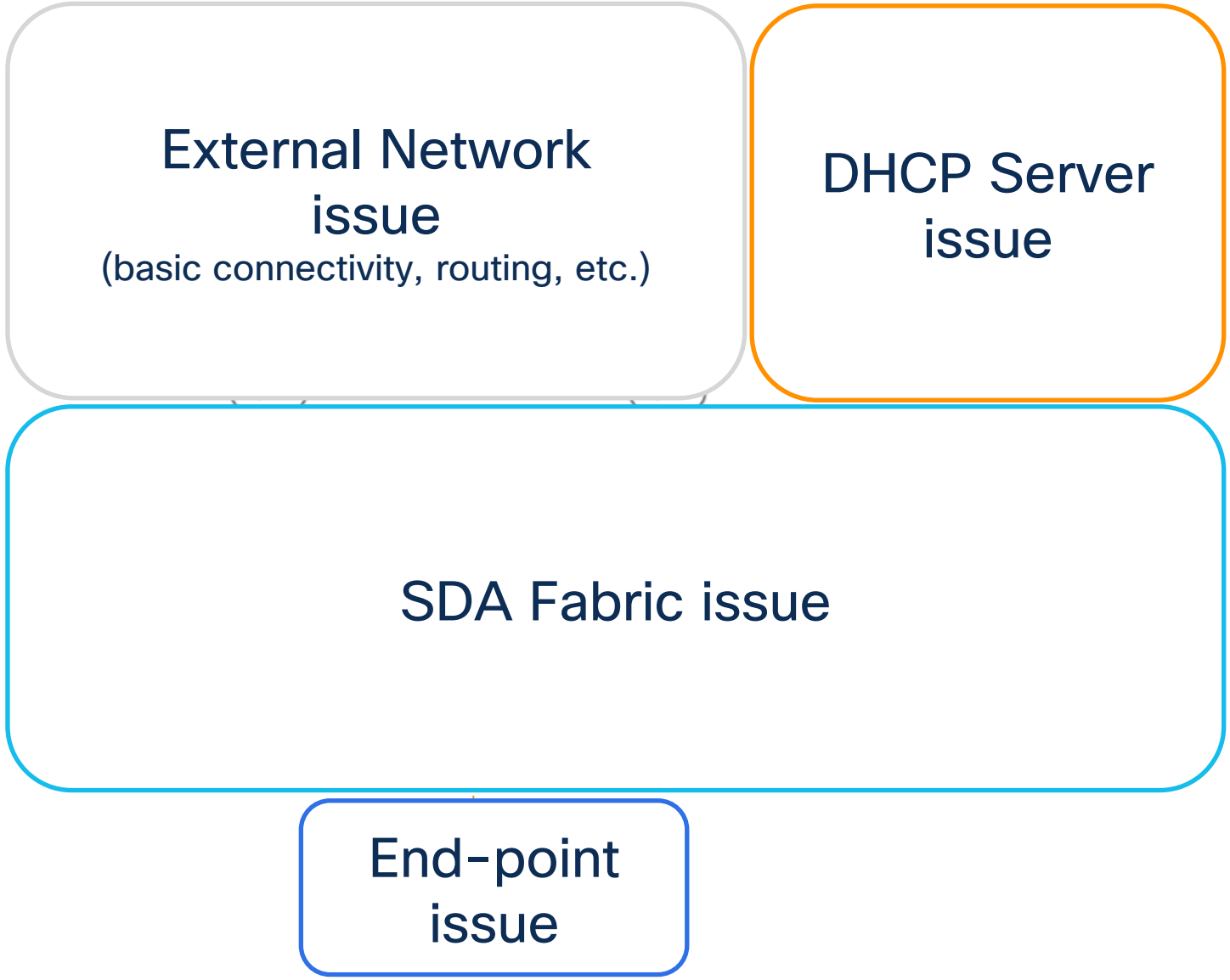


Catalyst Center: Network Troubleshooting (DHCP)



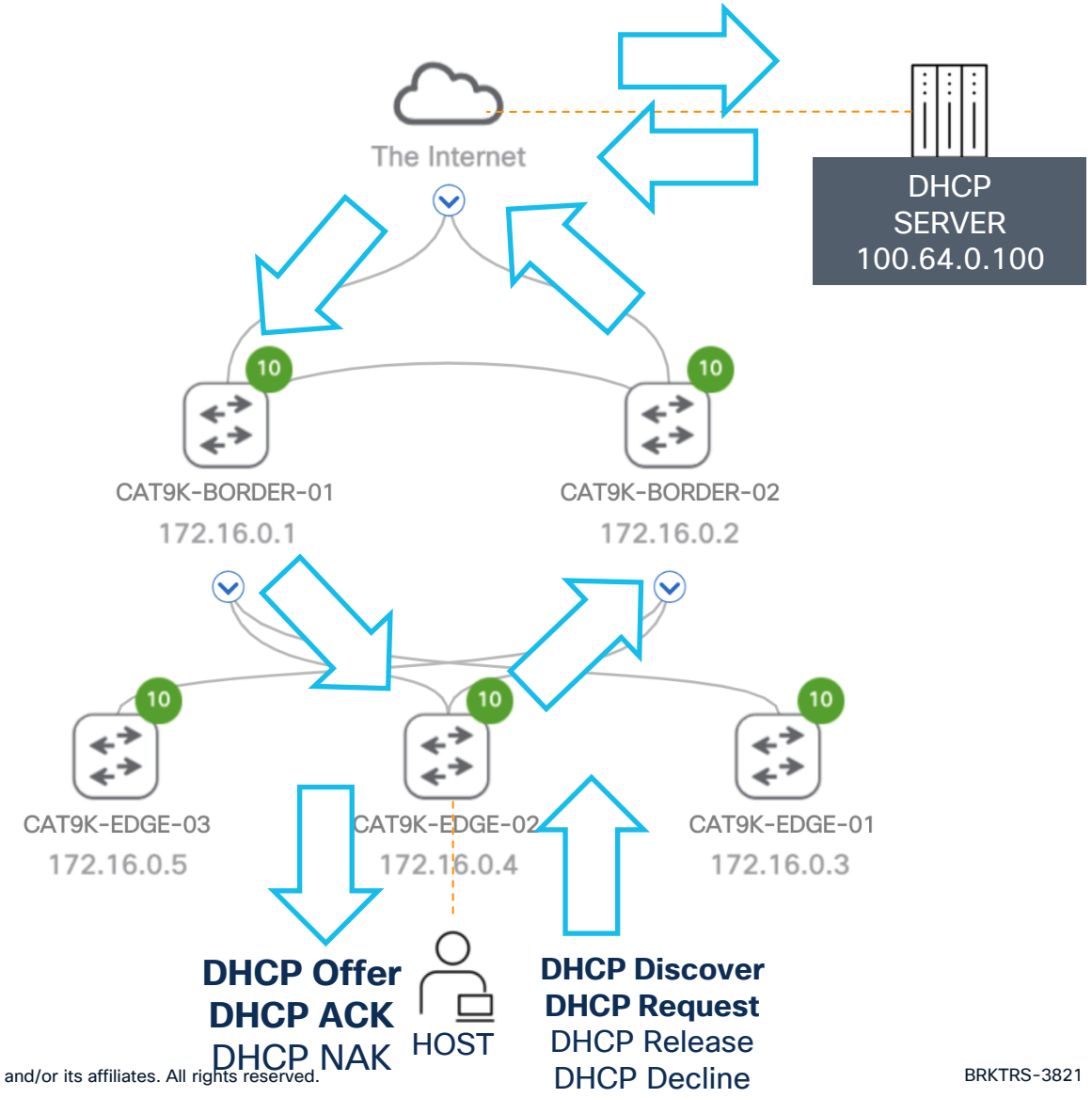
Only when all previous checks (configuration, assurance, compliance, known bugs) have been checked, start low level network troubleshooting.

Catalyst Center: Network Troubleshooting (DHCP)



Catalyst Center: Network troubleshooting (DHCP)

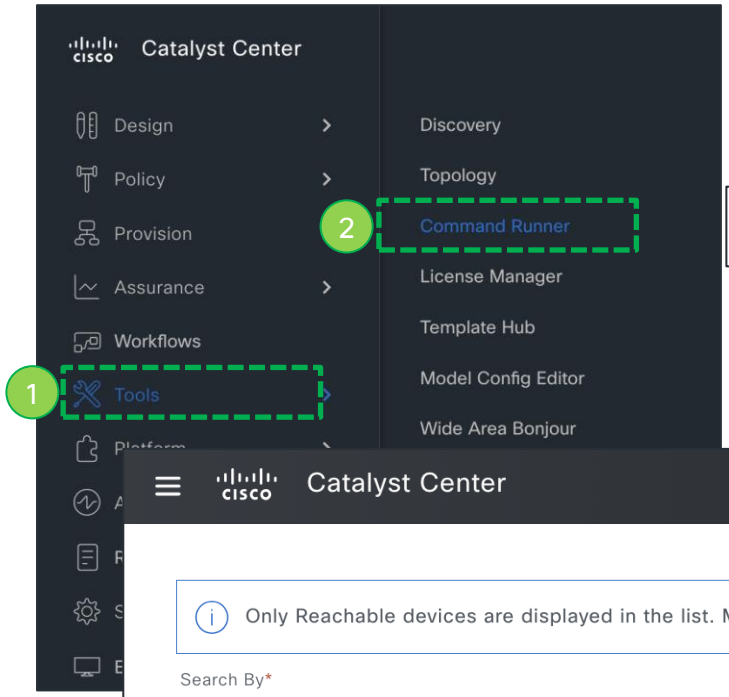
Example of DHCP packet flow



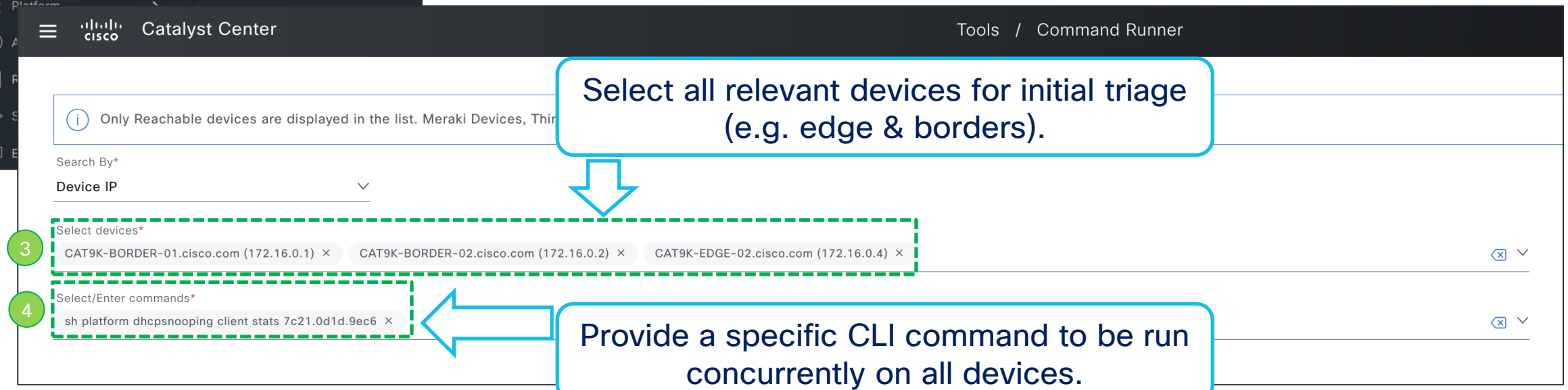
DHCP packets do not have to go through same devices (path can be asymmetric based on load-balancing rules within fabric / outside of the fabric)

Catalyst Center: Network Troubleshooting (DHCP)

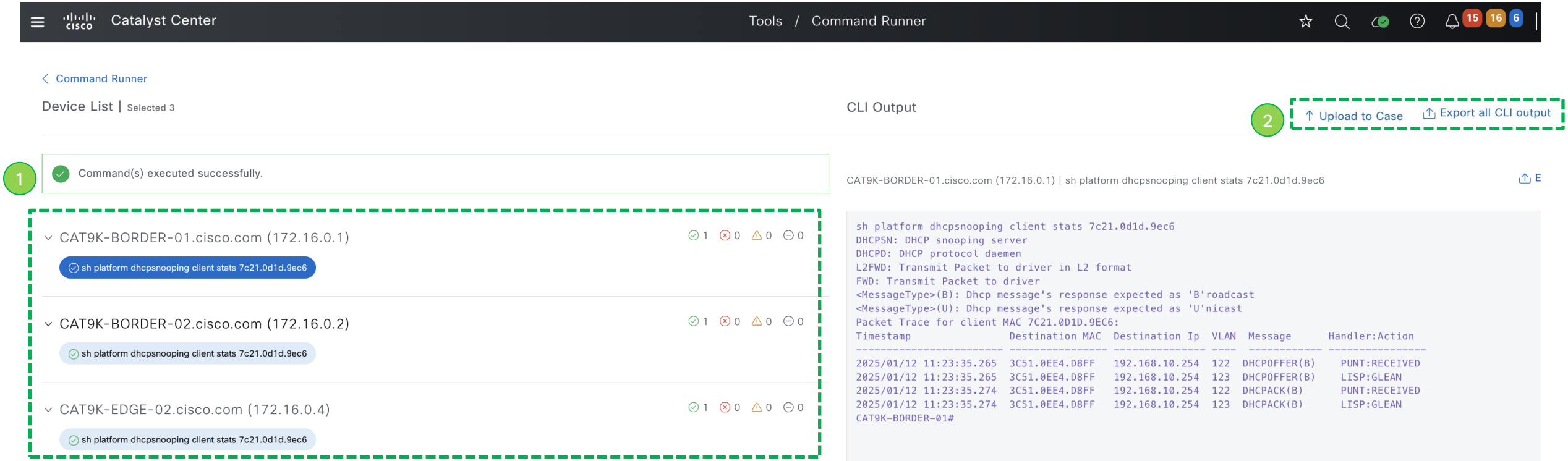
Tip #3a: Execute Command Runner on multiple devices simultaneously: **Tools > Command Runner**




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



Catalyst Center: Network Troubleshooting (DHCP)



CLI outputs gathered simultaneously from all devices.

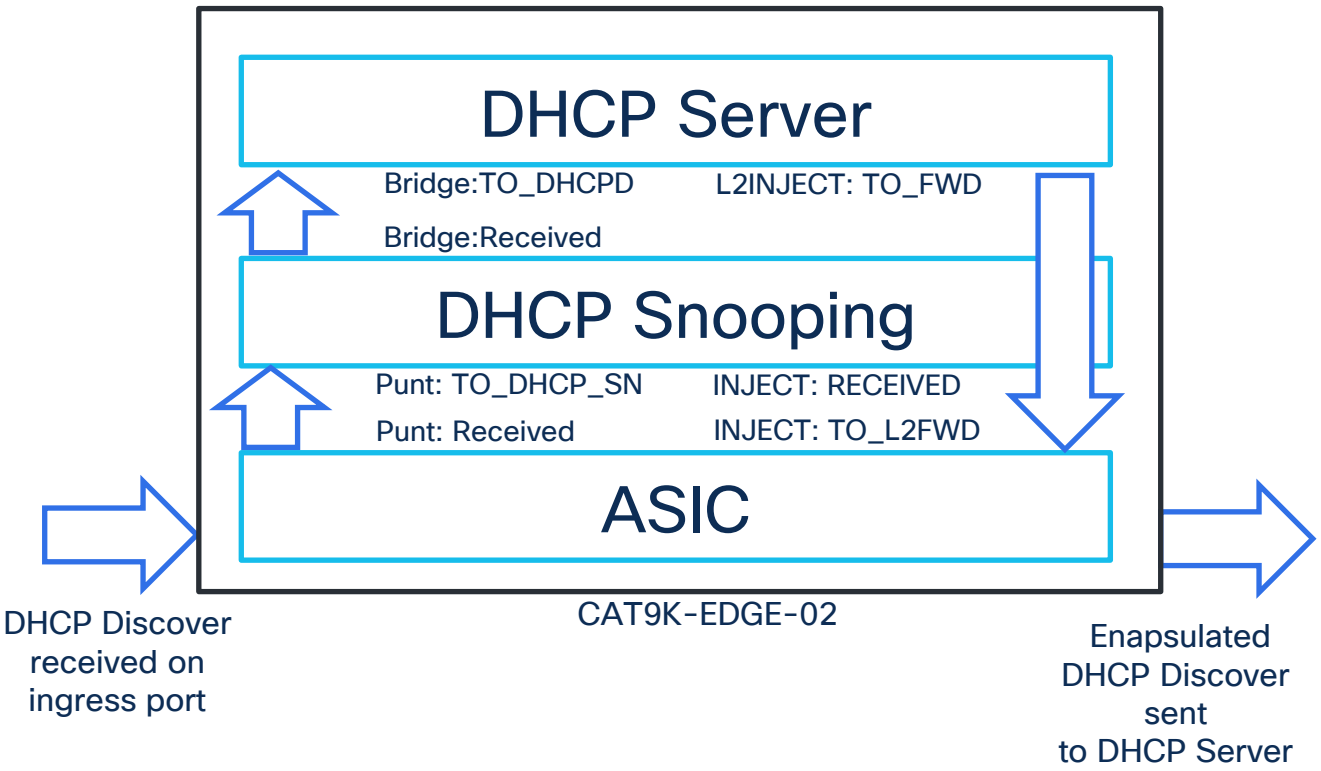
Catalyst Center: Network Troubleshooting (DHCP)

CAT9K-EDGE-02

```
sh platform dhcpsnooping client stats 7c21.0d1d.9ec6
DHCPSN: 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_DHCPSN
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_DHCPSN
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 DHCPACK(B)      PUNT:RECEIVED
2025/01/12 11:23:35.276  FFFF.FFFF.FFFF   255.255.255.255 0    DHCPACK(B)      INJECT:RECEIVED
2025/01/12 11:23:35.276  FFFF.FFFF.FFFF   255.255.255.255 0    DHCPACK(B)      INTERCEPT:RECEIVED
2025/01/12 11:23:35.276  FFFF.FFFF.FFFF   255.255.255.255 1020 DHCPACK(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
DHCPSN: 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 11:23:35.265  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
DHCPSN: 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
----------------------- ---------------- --------------- ----  ------------ ----------------
CAT9K-BORDER-02#
```

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

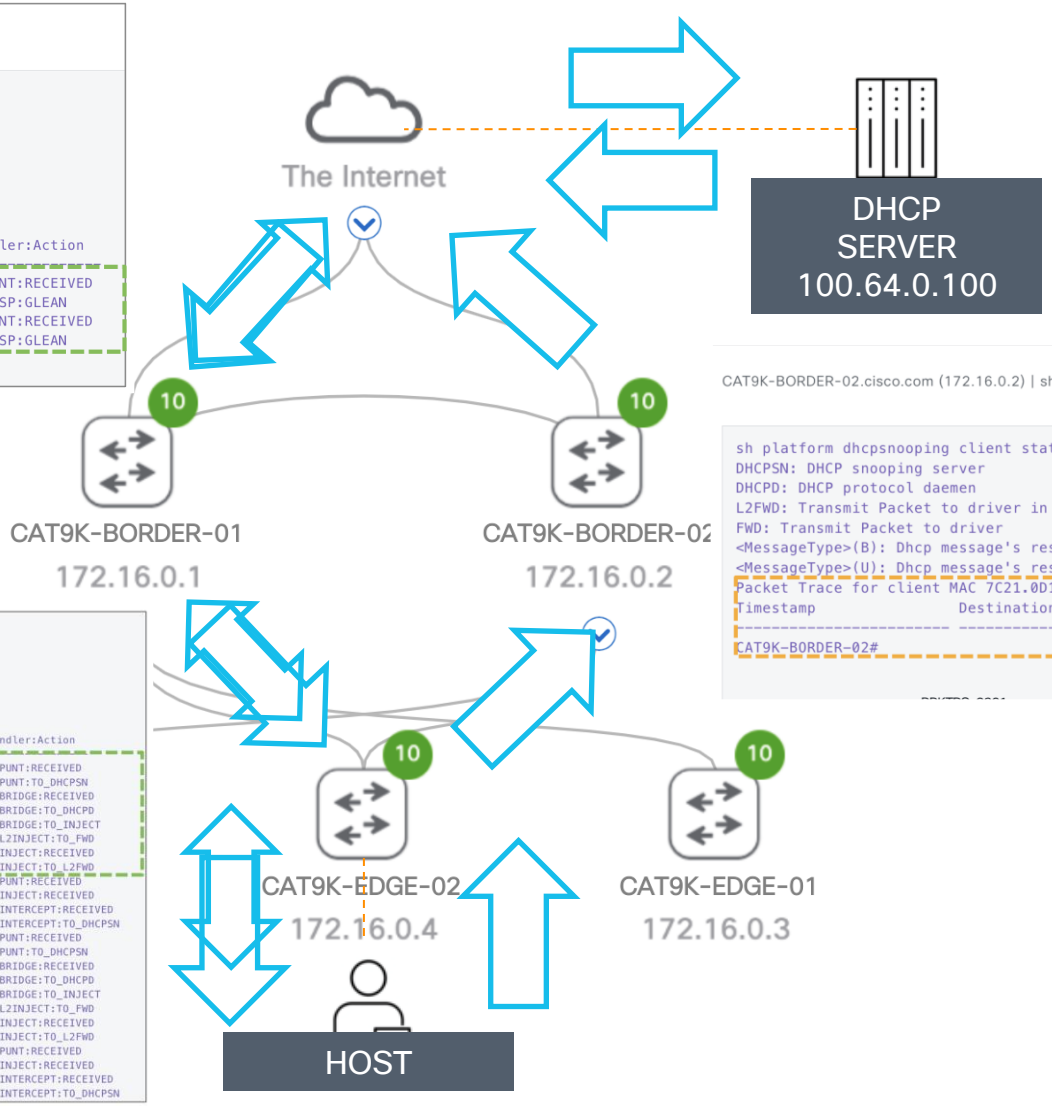
Catalyst Center: Network troubleshooting (DHCP)

Example of DHCP packet flow

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

```
sh platform dhcpsnooping client stats 7c21.0d1d.9ec6
DHCPSN: 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 11:23:35.265  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#
```



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
DHCPSN: 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
-----------------------  ---------------  --------------  ----  -----------  ---------------
CAT9K-BORDER-02#
```

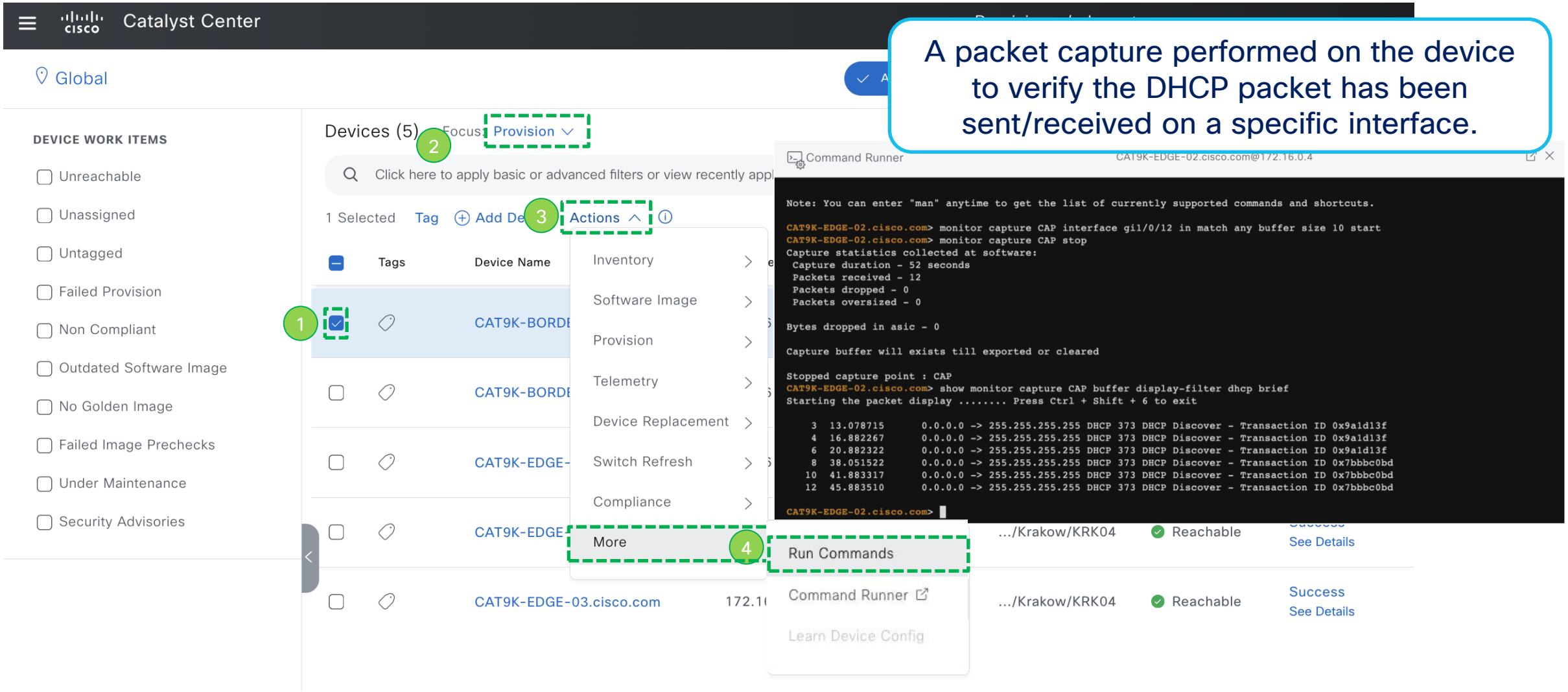
```
sh platform dhcpsnooping client stats 7c21.0d1d.9ec6
DHCPSN: DHCP snooping server
DHCPD: DHCP protocol daemen
L2FWD: Transmit Packet to driver in L2 format
FWD: Transmit Packet to driver
<MessageType>(B): Dhcp message's response expected as 'B'roadcast
<MessageType>(U): Dhcp message's response expected 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_DHCPSN
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_DHCPSN
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 DHCPACK(B)      PUNT:RECEIVED
2025/01/12 11:23:35.276  FFFF.FFFF.FFFF   255.255.255.255 0    DHCPACK(B)      INJECT:RECEIVED
2025/01/12 11:23:35.276  FFFF.FFFF.FFFF   255.255.255.255 0    DHCPACK(B)      INTERCEPT:RECEIVED
2025/01/12 11:23:35.276  FFFF.FFFF.FFFF   255.255.255.255 1020 DHCPACK(B)      INTERCEPT:TO_DHCPSN
```

Network troubleshooting (DHCP)

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

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.

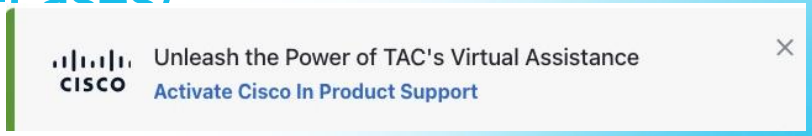
3. Bugs: Scan your network for potential well-known defects.

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

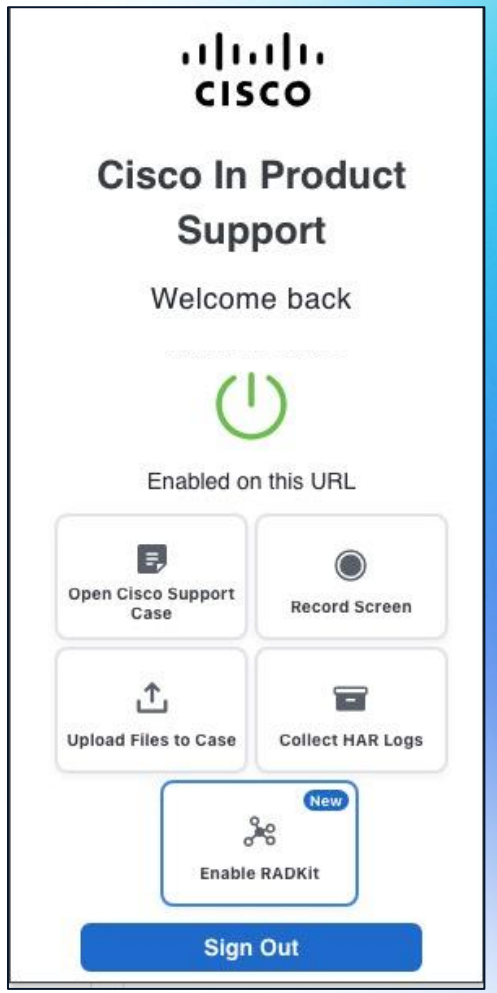
Cisco In Product Support Assistant Extension

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.



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 Extensio**

Complete your session evaluations

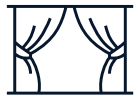
Complete a minimum of 4 session surveys and the Overall Event Survey to claim a Cisco Live T-Shirt.

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 !


CISCO