Understanding and Troubleshooting Cisco Catalyst Center

Abhay Kaviya - Customer Success Specialist - @abhaykaviya
Rahul Rammanohar - Principal Engineer

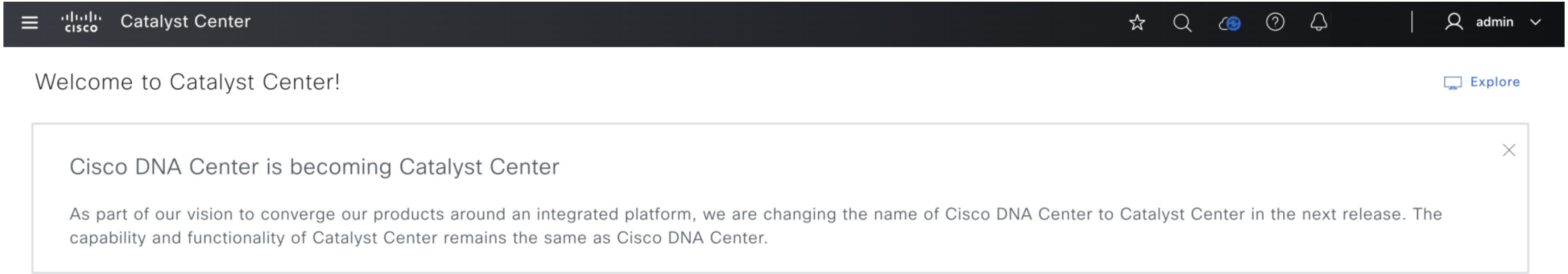
BRKOPS-2464

Cisco DNA Center is now Cisco Catalyst Center

Simplified branding for the Cisco Catalyst Stack.

Catalyst Center and Cisco DNA Center are the same product; as Cisco progresses through the rebranding process, both product names can be used interchangeably.

Screenshot visible from 2.3.7



Welcome to Catalyst Center!

Cisco DNA Center is becoming Catalyst Center

As part of our vision to converge our products around an integrated platform, we are changing the name of Cisco DNA Center to Catalyst Center in the next release. The capability and functionality of Catalyst Center remains the same as Cisco DNA Center.

Webex App

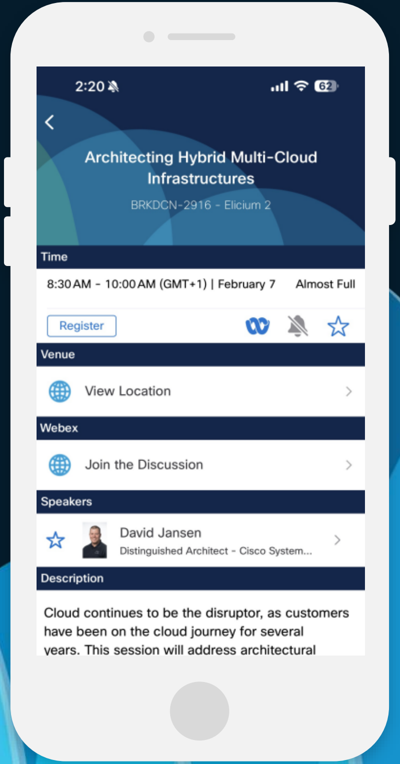
Questions?

Use the Webex app to chat with the speaker after the session

How

1. Find this session in the Cisco Events 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 February 28, 2025.



2:20

Architecting Hybrid Multi-Cloud Infrastructures

BRKDCN-2916 - Elicium 2

Time

8:30 AM - 10:00 AM (GMT+1) | February 7 Almost Full

Register

Venue

View Location

Webex

Join the Discussion

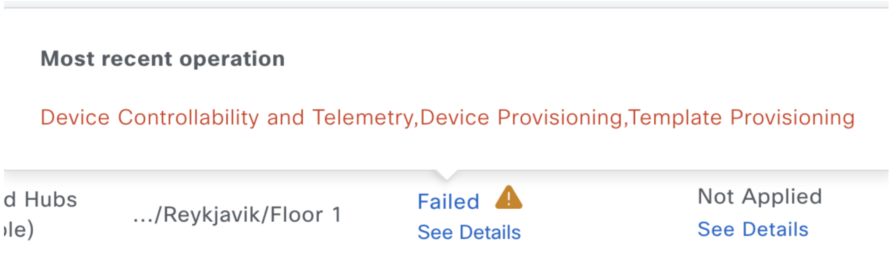
Speakers

David Jansen
Distinguished Architect - Cisco System...

Description

Cloud continues to be the disruptor, as customers have been on the cloud journey for several years. This session will address architectural

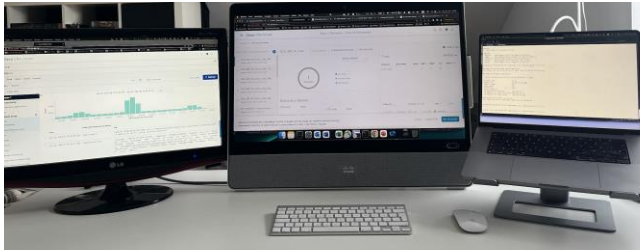
Have you ever called TAC?

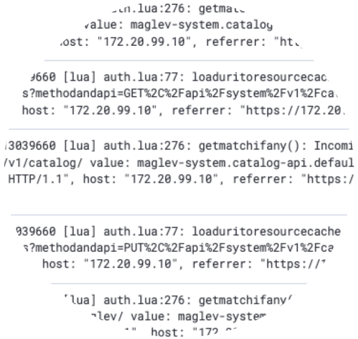


Most recent operation

Device Controllability and Telemetry,Device Provisioning,Template Provisioning

d Hubs ıle)	.../Reykjavik/Floor 1	Failed ⚠ See Details	Not Applied See Details

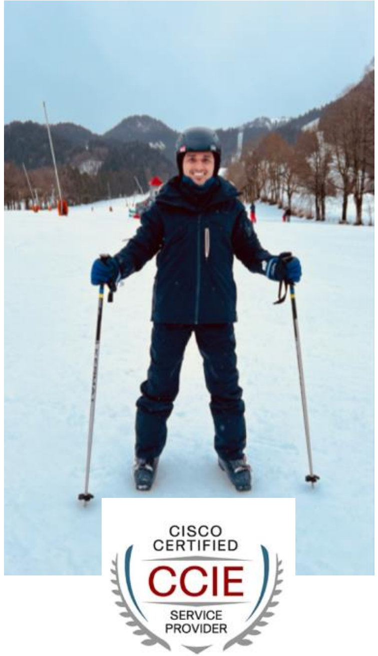




```
              .ın.lua:276: getma..
           value: maglev-system.catalog
        .ost: "172.20.99.10", referrer: "ht.

    9660 [lua] auth.lua:77: loaduritoresourcecac.
    s?methodandapi=GET%2C%2Fapi%2Fsystem%2Fv1%2Fca.
    host: "172.20.99.10", referrer: "https://172.20.

  3039660 [lua] auth.lua:276: getmatchifany(): Incomi
 /v1/catalog/ value: maglev-system.catalog-api.defaul
  HTTP/1.1", host: "172.20.99.10", referrer: "https:/

   939660 [lua] auth.lua:77: loaduritoresourcecache
    s?methodandapi=PUT%2C%2Fapi%2Fsystem%2Fv1%2Fca
       host: "172.20.99.10", referrer: "https://"

           'lua] auth.lua:276: getmatchifany'
              ·lev/ value: maglev-syster
                 ·"  host: "172.
```

Abhay Kaviya

- Joined Cisco in 2014 as a professional services engineer
- Worked in Cisco TAC for Catalyst Center/SDA solution support
- Currently part of Customer success team focused on Catalyst Center and SD-Access adoption



Rahul Rammanohar

- Principal Engineer, TAC Strategy EN, CX
- Location: Bangalore, India
- Focused on introducing automation & improving the serviceability of the Catalyst Center through product improvements and tools
- About to complete 25 years in Cisco across various verticals and locations
- Double CCIE (R&S, SP)
- Love solving complex problems
- Tool creator (mainly Python)
- Travel Buff, Foodie & Cricket fan

Agenda

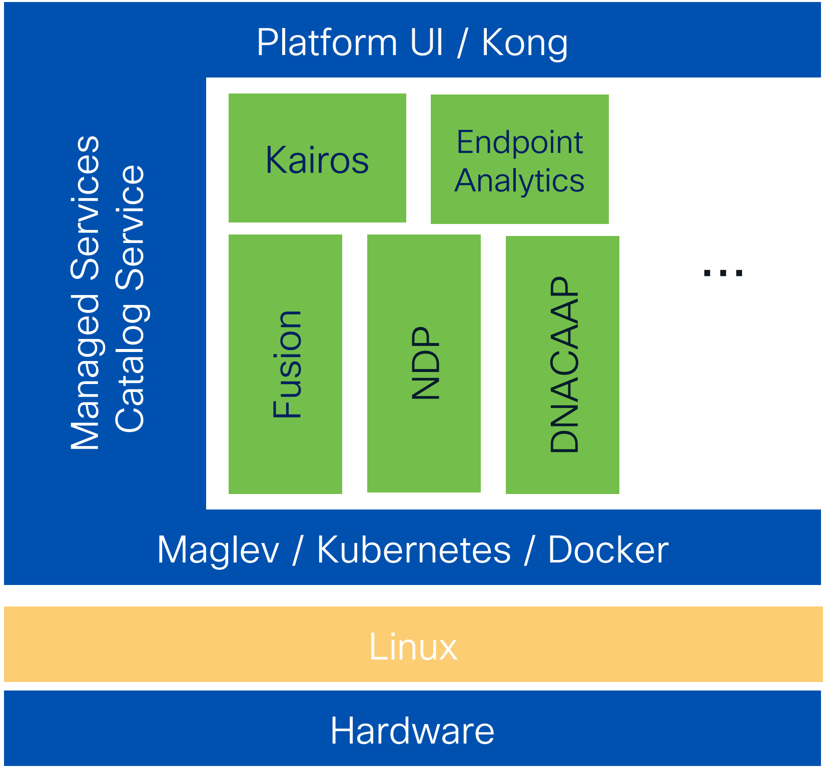
- Catalyst Center Architecture
- Catalyst Center Inventory and Provisioning Troubleshooting
- Catalyst Center SWIM Troubleshooting
- Catalyst Center Assurance Troubleshooting
- Catalyst Center Software Upgrades Troubleshooting
- Catalyst Center Health & Troubleshooting Tools (Reference)

Catalyst Center Architecture

Cisco Catalyst Center Architecture

Release 2.3.5.x
2.3.7.x

- The Layers of the Microservices Architecture



Apps or Network Applications

- Automation, Assurance, Platform APIs, AI Network Analytics, Endpoint Analytics

Maglev v1.7, 1.8

- Managed Services
  - DBaaS (MongoDB(4.2.11), Postgres, Redis)
  - Messaging Queues (RabbitMQ (3.8.3), Kafka)
  - Clustering Services (Glusterfs, Zookeeper)
  - Monitoring (InfluxDB, Grafana)
- Catalog Service
- Kubernetes(v1.18.15), Docker(19.3.9)
- North Bound API Gateway – Kong

Linux Ubuntu (18.4.1 LTS, 18.4.6 LTS)

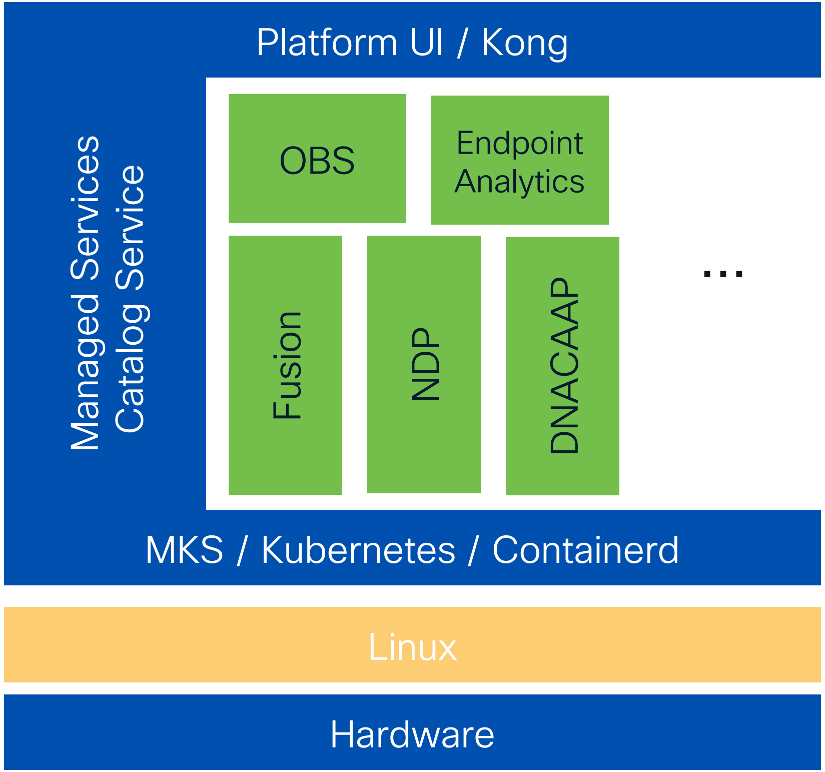
DN2 – 44, 56 or 112 core (based on Cisco UCS 220/480M5)
DN3 – 32, 56 or 80 core (based on Cisco UCS 220 M6)

DN2, DN3, AWS

Cisco Catalyst Center Architecture

Release 2.3.7.x

- The Layers of the Microservices Architecture



Platform UI / Kong

Managed Services
Catalog Service

OBS

Endpoint Analytics

Fusion

NDP

DNACAAP

...

MKS / Kubernetes / Containerd

Linux

Hardware

Apps or Network Applications

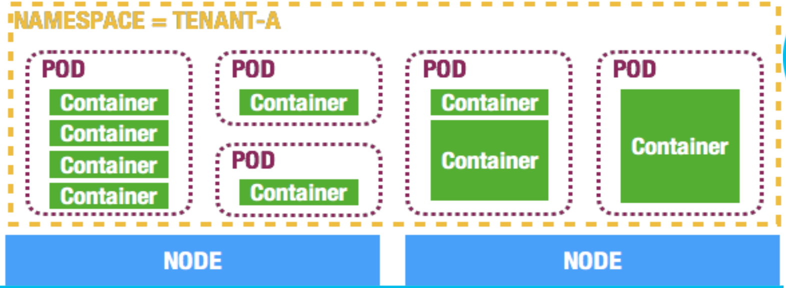
- Automation, Assurance, Platform APIs, AI Network Analytics, Endpoint Analytics

PnC ~~v1.8~~ (v3.0)

- Managed Services
  - DBaaS (MongoDB~~(4.2.11)~~(4.4.13) , Postgres, Redis)
  - Messaging Queues (RabbitMQ~~(3.8.3)~~ (3.13.3), Kafka)
  - Clustering Services (~~Glusterfs~~, ~~Zookeeper~~)
  - Monitoring (~~InfluxDB~~ Prometheus, Grafana)
- Catalog Service
- Kubernetes~~(v1.18.15)~~ (v1.24.4-cisco), ~~Docker(19.3.9)~~ Containerd (v1.6.6)
- North Bound API Gateway – Kong
- Linux Ubuntu ~~(18.4.1 LTS)~~ (18.4.6 LTS)

ESXi

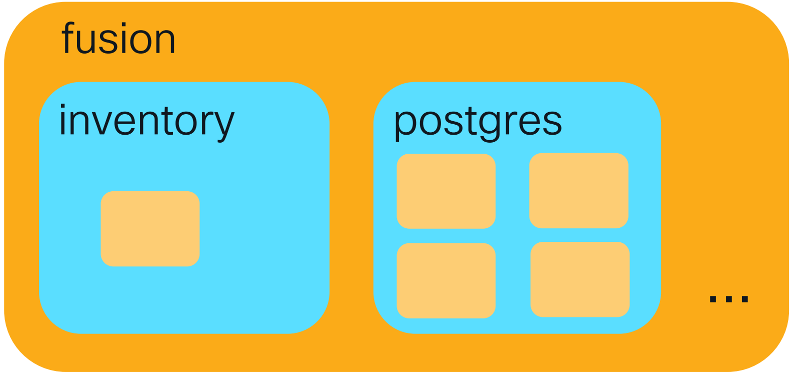
Terminology – Microservices



Container	A container image is a lightweight, stand-alone, executable package of a piece of software that includes everything needed to run it: code, runtime, system tools, system libraries, settings.
Pod	A pod is a group of one or more containers (such as Docker containers), with shared storage/network, and a specification for how to run the containers
Namespace	Provide a mechanism for isolating groups of resources within a single cluster.
Service	A Kubernetes Service is an abstraction which defines a logical set of Pods and a policy by which to access them - sometimes called a micro-service.
Node	A node is a VM or a physical computer that serves as a worker machine in a Kubernetes cluster.

Cisco Catalyst Center Architecture

Microservices Architecture powered by Kubernetes & Docker



Appstack maps to K8s Namespace, is a virtual cluster within the K8s cluster. Administrative and resource controls are defined.

- fusion for Automation
- ndp for Assurance

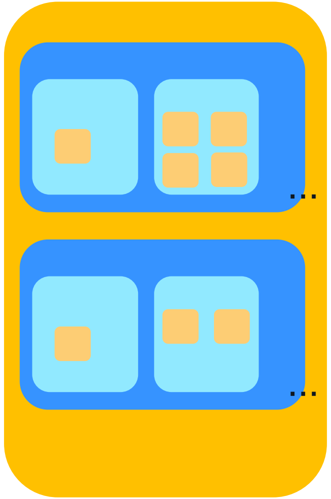
Services (aka micro-services) is a logical abstraction representing a group of K8s pods.

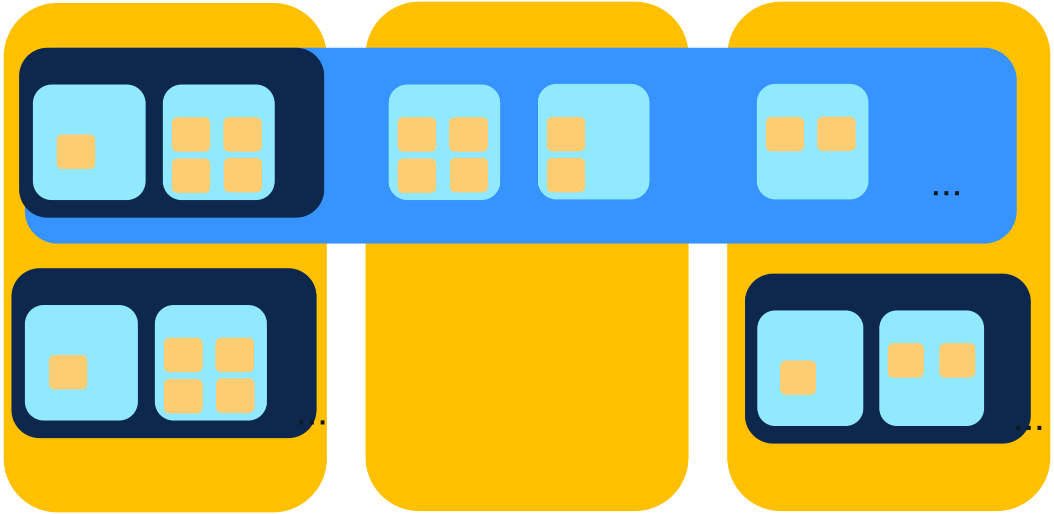
- inventory for Inventory Service
- postgres for storing Inventory collection

Pods is a collection of containers that contain 1 or more Docker containers. The containers in a pod share storage and network.

Cisco Catalyst Center Architecture

Microservices Architecture powered by Kubernetes & Docker





Single Node Cluster

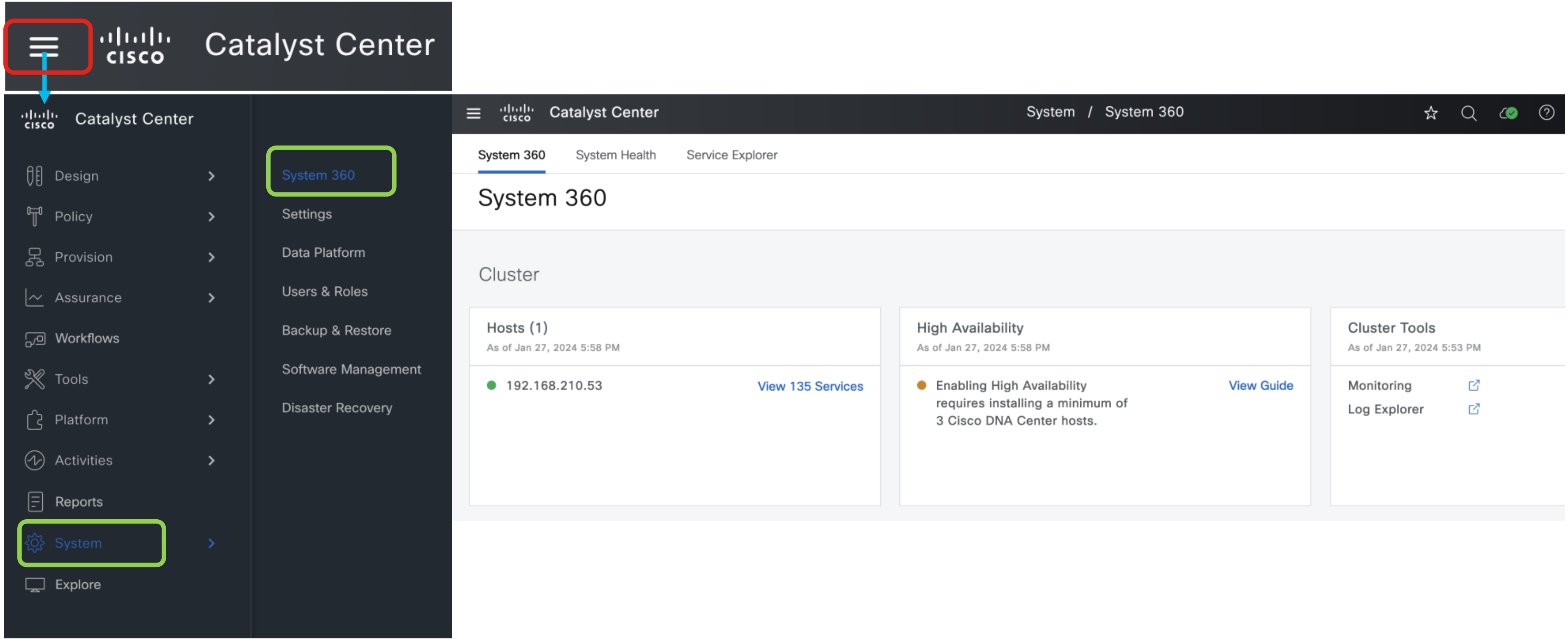
Worker machine where the pods are placed. Can be a physical or virtual appliance.

Three Node Cluster

A High Availability framework that reduces downtime due to failures. Near real-time synchronization across nodes of the cluster. A pod is always placed on a node but pods of a namespace are spread across nodes.

System 360 tools

Catalyst Center UI: System 360



System 360

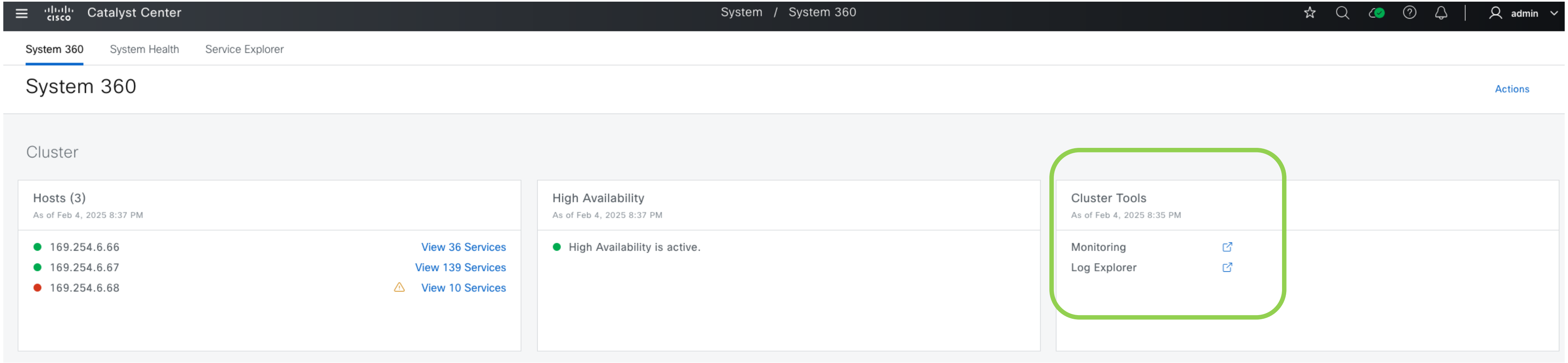
Cluster

Hosts (1)
As of Jan 27, 2024 5:58 PM
● 192.168.210.53 View 135 Services

High Availability
As of Jan 27, 2024 5:58 PM
● Enabling High Availability requires installing a minimum of 3 Cisco DNA Center hosts. View Guide

Cluster Tools
As of Jan 27, 2024 5:53 PM
Monitoring
Log Explorer

Catalyst Center UI: System 360



System 360

Cluster

Hosts (3)
As of Feb 4, 2025 8:37 PM

● 169.254.6.66	View 36 Services
● 169.254.6.67	View 139 Services
● 169.254.6.68	⚠ View 10 Services

High Availability
As of Feb 4, 2025 8:37 PM

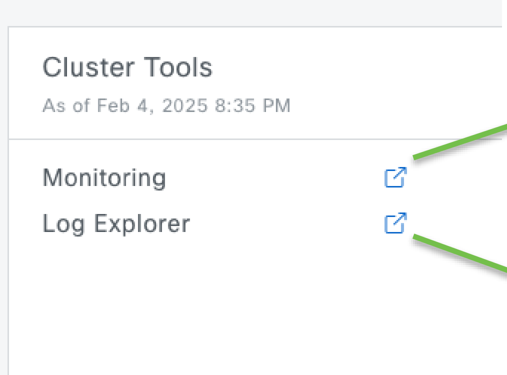
● High Availability is active.

Cluster Tools
As of Feb 4, 2025 8:35 PM

Monitoring

Log Explorer

System 360: Cluster Tools

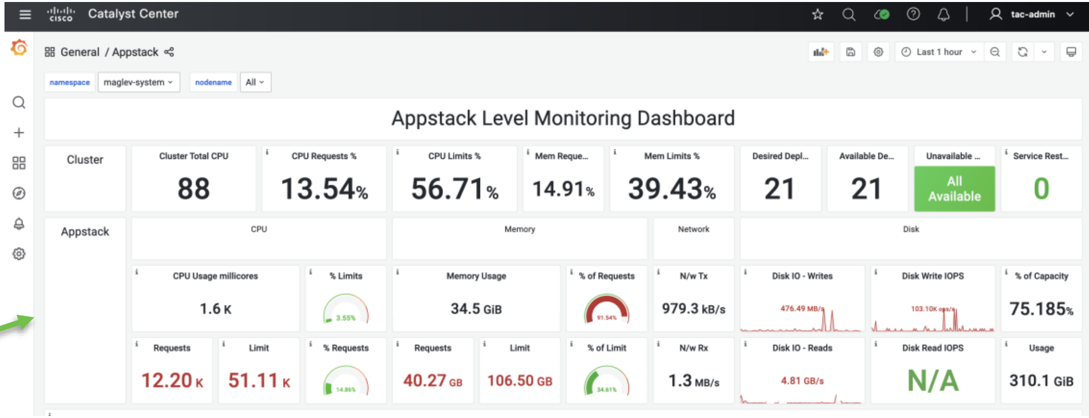


Cluster Tools

As of Feb 4, 2025 8:35 PM

Monitoring ↗

Log Explorer ↗



Catalyst Center · tac-admin

General / Appstack

namespace: maglev-system · nodename: All · Last 1 hour

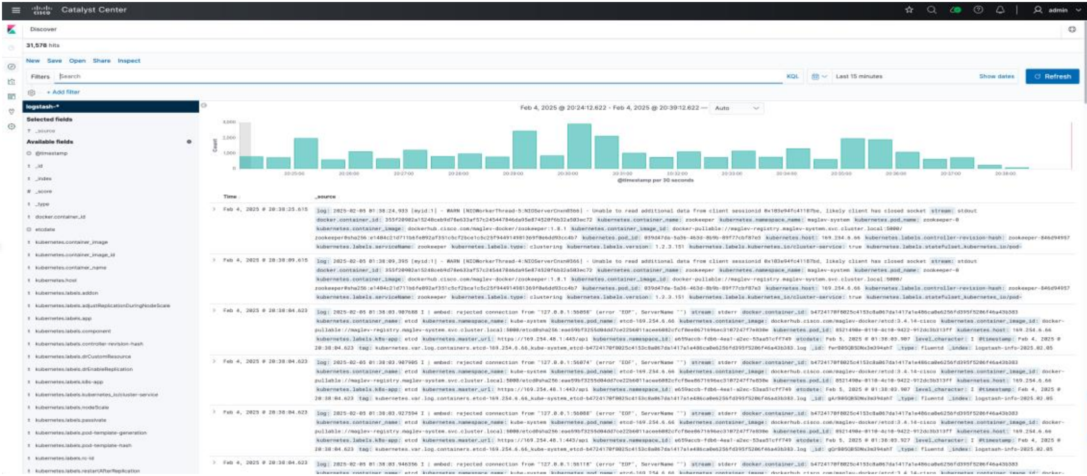
Appstack Level Monitoring Dashboard

Cluster	Cluster Total CPU	CPU Requests %	CPU Limits %	Mem Reque...	Mem Limits %	Desired Depl...	Available De...	Unavailable ...	Service Rest...
	88	13.54%	56.71%	14.91%	39.43%	21	21	All Available	0

Appstack

	CPU		Memory		Network	Disk		
CPU Usage millicores	% Limits	Memory Usage	% of Requests	N/w Tx	Disk IO - Writes	Disk Write IOPS	% of Capacity
1.6 K	3.55%	34.5 GiB	91.54%	979.3 kB/s	476.49 MB/s	103.10K ops/s	75.185%

Requests	Limit	% Requests	Requests	Limit	% of Limit	N/w Rx	Disk IO - Reads	Disk Read IOPS	Usage
12.20 K	51.11 K	14.86%	40.27 GB	106.50 GB	34.61%	1.3 MB/s	4.81 GB/s	N/A	310.1 GiB



Catalyst Center
admin
Discover
31,578 hits
New Save Open Share Inspect
Filters Search
KQL
Last 15 minutes
Show dates
Refresh
+ Add filter
logstash-*
Selected fields
_source
Available fields
@timestamp
_id
_index
_score
_type
docker.container_id
etcdate
kubernetes.container_image
kubernetes.container_image_id
kubernetes.container_name
kubernetes.host
kubernetes.labels.addon
kubernetes.labels.adjustReplicationDuringNodeScale
kubernetes.labels.app
kubernetes.labels.component
kubernetes.labels.controller-revision-hash
kubernetes.labels.drCustomResource
kubernetes.labels.drEnableReplication
kubernetes.labels.k8s-app
kubernetes.labels.kubernetes_io/cluster-service
kubernetes.labels.nodeScale
kubernetes.labels.passivate
kubernetes.labels.pod-template-generation
kubernetes.labels.pod-template-hash
kubernetes.labels.rc-id
kubernetes.labels.restartAfterReplication
Feb 4, 2025 @ 20:24:12.622 - Feb 4, 2025 @ 20:39:12.622 — Auto
Count
3,000
2,000
1,000
0
20:25:00
20:26:00
20:27:00
20:28:00
20:29:00
20:30:00
20:31:00
20:32:00
20:33:00
20:34:00
20:35:00
20:36:00
20:37:00
20:38:00
@timestamp per 30 seconds

```
Time                        _source
> Feb 4, 2025 @ 20:38:25.615  log: 2025-02-05 01:38:24,933 [myid:1] - WARN [NIOWorkerThread-5:NIOServerCnxn@366] - Unable to read additional data from client sessionid 0x103e94fc41187be, likely client has closed socket stream: stdout
                            docker.container_id: 355f20902a15248ceb9d78e633af57c245447846da95e874520f6b32a583ec72 kubernetes.container_name: zookeeper kubernetes.namespace_name: maglev-system kubernetes.pod_name: zookeeper-0
                            kubernetes.container_image: dockerhub.cisco.com/maglev-docker/zookeeper:1.8.1 kubernetes.container_image_id: docker-pullable://maglev-registry.maglev-system.svc.cluster.local:5000/
                            zookeeper@sha256:e1404c21d711b6fe092af351c5cf2bce1c5c25f944914981369f0e6dd93cc4b7 kubernetes.pod_id: 039d47da-5a36-463d-8b9b-09f77cbf87e3 kubernetes.host: 169.254.6.66 kubernetes.labels.controller-revision-hash: zookeeper-846d94957
                            kubernetes.labels.serviceName: zookeeper kubernetes.labels.type: clustering kubernetes.labels.version: 1.2.3.151 kubernetes.labels.kubernetes_io/cluster-service: true kubernetes.labels.statefulset_kubernetes_io/pod-
> Feb 4, 2025 @ 20:38:09.615  log: 2025-02-05 01:38:09,395 [myid:1] - WARN [NIOWorkerThread-4:NIOServerCnxn@366] - Unable to read additional data from client sessionid 0x103e94fc41187bd, likely client has closed socket stream: stdout
                            docker.container_id: 355f20902a15248ceb9d78e633af57c245447846da95e874520f6b32a583ec72 kubernetes.container_name: zookeeper kubernetes.namespace_name: maglev-system kubernetes.pod_name: zookeeper-0
                            kubernetes.container_image: dockerhub.cisco.com/maglev-docker/zookeeper:1.8.1 kubernetes.container_image_id: docker-pullable://maglev-registry.maglev-system.svc.cluster.local:5000/
                            zookeeper@sha256:e1404c21d711b6fe092af351c5cf2bce1c5c25f944914981369f0e6dd93cc4b7 kubernetes.pod_id: 039d47da-5a36-463d-8b9b-09f77cbf87e3 kubernetes.host: 169.254.6.66 kubernetes.labels.controller-revision-hash: zookeeper-846d94957
                            kubernetes.labels.serviceName: zookeeper kubernetes.labels.type: clustering kubernetes.labels.version: 1.2.3.151 kubernetes.labels.kubernetes_io/cluster-service: true kubernetes.labels.statefulset_kubernetes_io/pod-
> Feb 4, 2025 @ 20:38:04.623  log: 2025-02-05 01:38:03.987688 I | embed: rejected connection from "127.0.0.1:55058" (error "EOF", ServerName "") stream: stderr docker.container_id: b4724170f0025c4153c8a067da1417a1e486ca0e6256fd395f5206f46a43b383
                            kubernetes.container_name: etcd kubernetes.namespace_name: kube-system kubernetes.pod_name: etcd-169.254.6.66 kubernetes.container_image: dockerhub.cisco.com/maglev-docker/etcd:3.4.14-cisco kubernetes.container_image_id: docker-
                            pullable://maglev-registry.maglev-system.svc.cluster.local:5000/etcd@sha256:eae59bf3255d04dd7ce2256011acee6082cfcf8ee0671696ec3107247f7e030e kubernetes.pod_id: 8521490e-0110-4c10-9422-912dc3b313ff kubernetes.host: 169.254.6.66
                            kubernetes.labels.k8s-app: etcd kubernetes.master_url: https://169.254.48.1:443/api kubernetes.namespace_id: e659acc0-fdb6-4ea1-a2ec-53aa51cff749 etcdate: Feb 5, 2025 @ 01:38:03.987 level_character: I @timestamp: Feb 4, 2025 @
                            20:38:04.623 tag: kubernetes.var.log.containers.etcd-169.254.6.66_kube-system_etcd-b4724170f0025c4153c8a067da1417a1e486ca0e6256fd395f5206f46a43b383.log _id: fer085Q8SDNx3m394ahT _type: fluentd _index: logstash-info-2025.02.05
```

Catalyst Center Command Line Interface?

- **maglev** commands:
  - Python wrapper script for Kong API interface.
  - Primarily used in managing and monitoring system packages

Note: UI Username and password, separate from linux CLI maglev user

- **magctl** commands:
  - Many commands and output similar to kubectl
  - Primary commands for monitoring and troubleshooting system services and containers

Catalyst Center CLI Commands

- ssh maglev@Catalyst Center_IP -p 2222

- Identify the service in charge of the task you are interested in:
  - magctl appstack status

- Individual service log retrieval:
  - Raw log: **magctl service logs -r** <service name> (ie: magctl service logs –r inventory-manager)
  - Last N lines: **magctl service logs -r** <service name> | tail –n N
  - Live log: **magctl service logs -rf** <service name> (follow the live log, equivalent of tail –f)

- Service management:
  - Soft restart: **magctl service restart** <service-name> (restarts the container)
  - Hard restart: **magctl service restart –d** <service-name> (restarts the pod)
  - **Note: In case of hard restart, pod is deleted && re-created = non-persistant storage/inside container app data loss!**

  - Display config & current status: **magctl service status** <service-name>
  - Display stateful information: **magctl service display** <service-name>

Catalyst Center Inventory and Provisioning Troubleshooting

Cisco Catalyst Center Inventory

Automation Capabilities from Inventory Page

Network Visibility

- Software Version
- Device Family
- Device PID
- Security Advisories
- Health
- Compliance ...

Network Operations

- Upgrading
- Provisioning
- RMA
- Run Commands ...

Main Role of Inventory

Inventory Collection (Sync)

- Data collection via SNMP, CLI or Netconf
- Reports reachability & manageability status
- Convert data to database objects

Release 2.3.x.x onwards

Cisco Catalyst Center Inventory

Inventory Sync Enhancements

Reprioritization of Sync Tasks (SNMP Trap floodings don’t starve other priority syncs…)

Grafana Inventory Dashboard (additional visibility and troubleshooting)

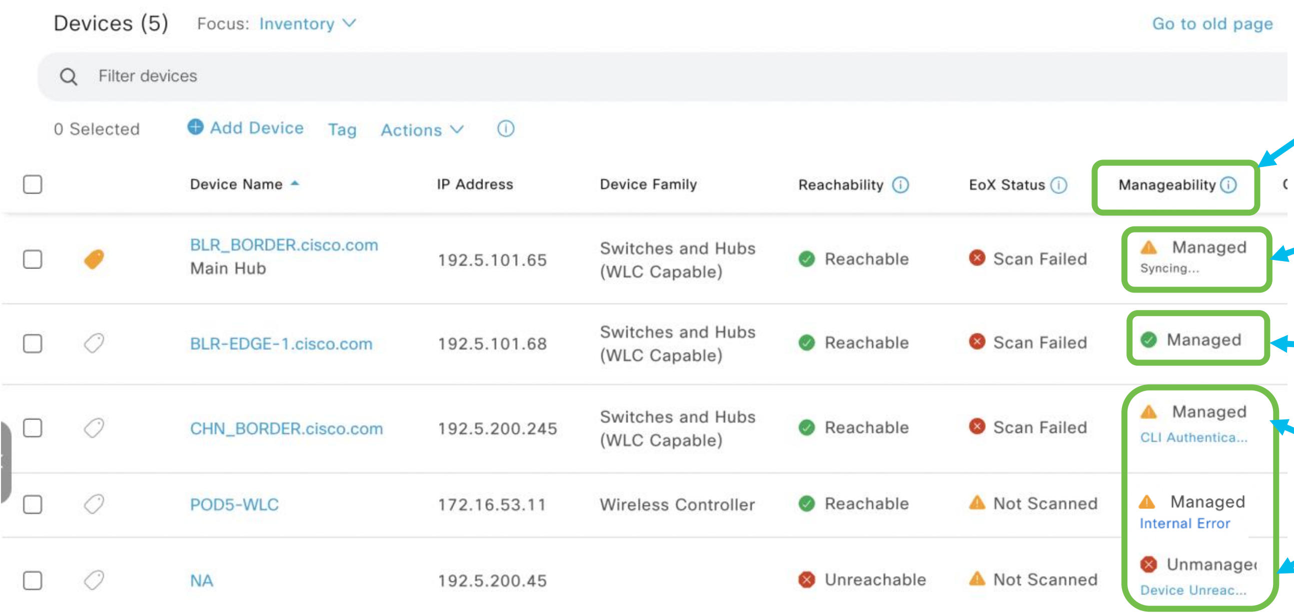
Multiple Memory Optimizations (shorter sync times especially for scaled setups, prevention of out of memory / crashes)

Visibility into Sync Errors (no more Partial Collection Failures)

Provision / Inventory

Customer Voice

Q1: “Is my device managed / in Sync with the Cisco Catalyst Center?”



Devices (5)   Focus: Inventory ∨   Go to old page

Filter devices

0 Selected   Add Device   Tag   Actions ∨   ⓘ

□		Device Name ▲	IP Address	Device Family	Reachability ⓘ	EoX Status ⓘ	Manageability ⓘ	(
□		BLR_BORDER.cisco.com Main Hub	192.5.101.65	Switches and Hubs (WLC Capable)	✓ Reachable	✕ Scan Failed	⚠ Managed Syncing...	
□		BLR-EDGE-1.cisco.com	192.5.101.68	Switches and Hubs (WLC Capable)	✓ Reachable	✕ Scan Failed	✓ Managed	
□		CHN_BORDER.cisco.com	192.5.200.245	Switches and Hubs (WLC Capable)	✓ Reachable	✕ Scan Failed	⚠ Managed CLI Authentica...	
□		POD5-WLC	172.16.53.11	Wireless Controller	✓ Reachable	⚠ Not Scanned	⚠ Managed Internal Error	
□		NA	192.5.200.45		✕ Unreachable	⚠ Not Scanned	✕ Unmanage Device Unreac...	

Whether the device is managed by Cisco Catalyst Center or not

Sync in progress

Successfully Managed

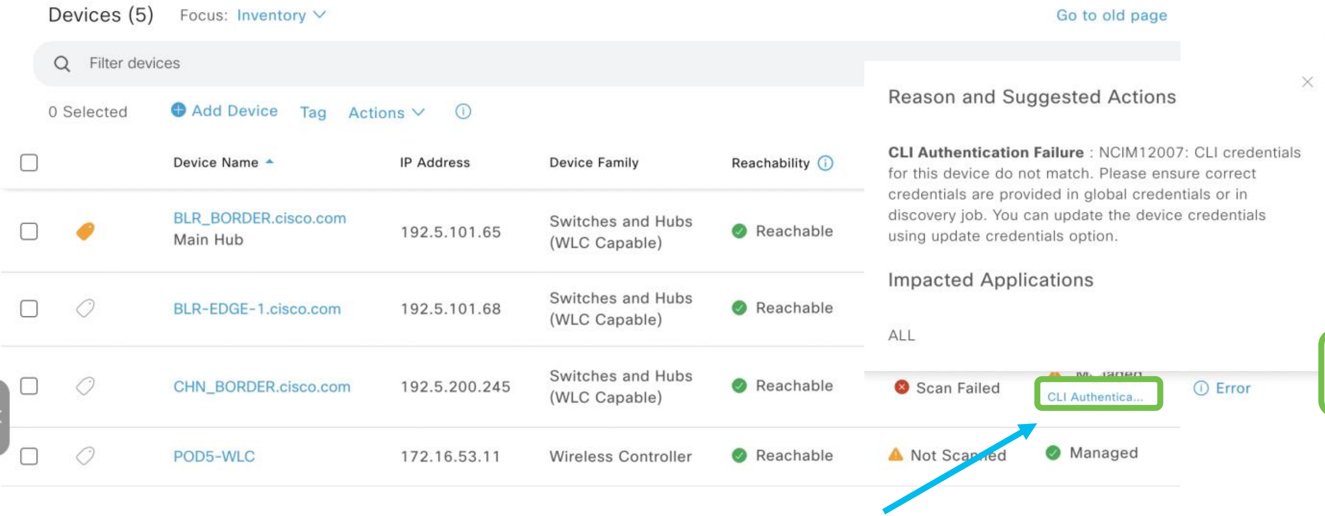
Errors

Provision / Inventory

Customer Voice

Q2: “Why is my device in an unmanaged or constant syncing or errored state?”

Reason and Suggested Actions menu



Devices (5) Focus: Inventory Go to old page

Filter devices

0 Selected Add Device Tag Actions

Device Name	IP Address	Device Family	Reachability			
BLR_BORDER.cisco.com Main Hub	192.5.101.65	Switches and Hubs (WLC Capable)	Reachable			
BLR-EDGE-1.cisco.com	192.5.101.68	Switches and Hubs (WLC Capable)	Reachable			
CHN_BORDER.cisco.com	192.5.200.245	Switches and Hubs (WLC Capable)	Reachable	Scan Failed	CLI Authentica...	Error
POD5-WLC	172.16.53.11	Wireless Controller	Reachable	Not Scanned	Managed	

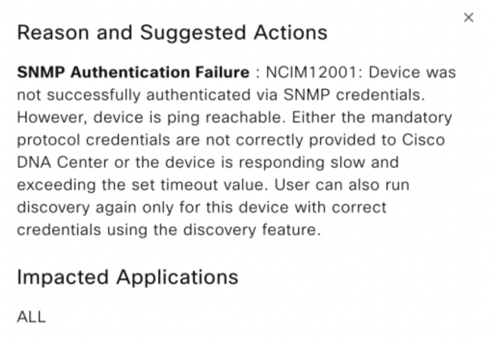
Reason and Suggested Actions

CLI Authentication Failure : NCIM12007: CLI credentials for this device do not match. Please ensure correct credentials are provided in global credentials or in discovery job. You can update the device credentials using update credentials option.

Impacted Applications

ALL

More details on clicking the error message

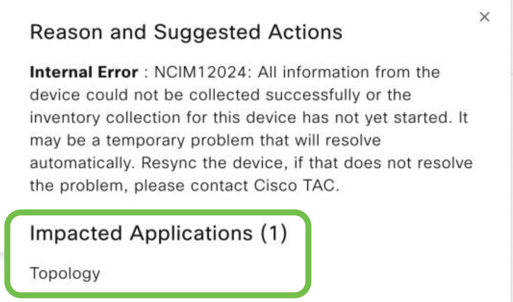


Reason and Suggested Actions

SNMP Authentication Failure : NCIM12001: Device was not successfully authenticated via SNMP credentials. However, device is ping reachable. Either the mandatory protocol credentials are not correctly provided to Cisco DNA Center or the device is responding slow and exceeding the set timeout value. User can also run discovery again only for this device with correct credentials using the discovery feature.

Impacted Applications

ALL



Reason and Suggested Actions

Internal Error : NCIM12024: All information from the device could not be collected successfully or the inventory collection for this device has not yet started. It may be a temporary problem that will resolve automatically. Resync the device, if that does not resolve the problem, please contact Cisco TAC.

Impacted Applications (1)

Topology

Affected Application

Customer Voice

Q2: “Why is my device in an unmanaged or constant syncing or errored state?”

Provision / Inventory

View Device Details

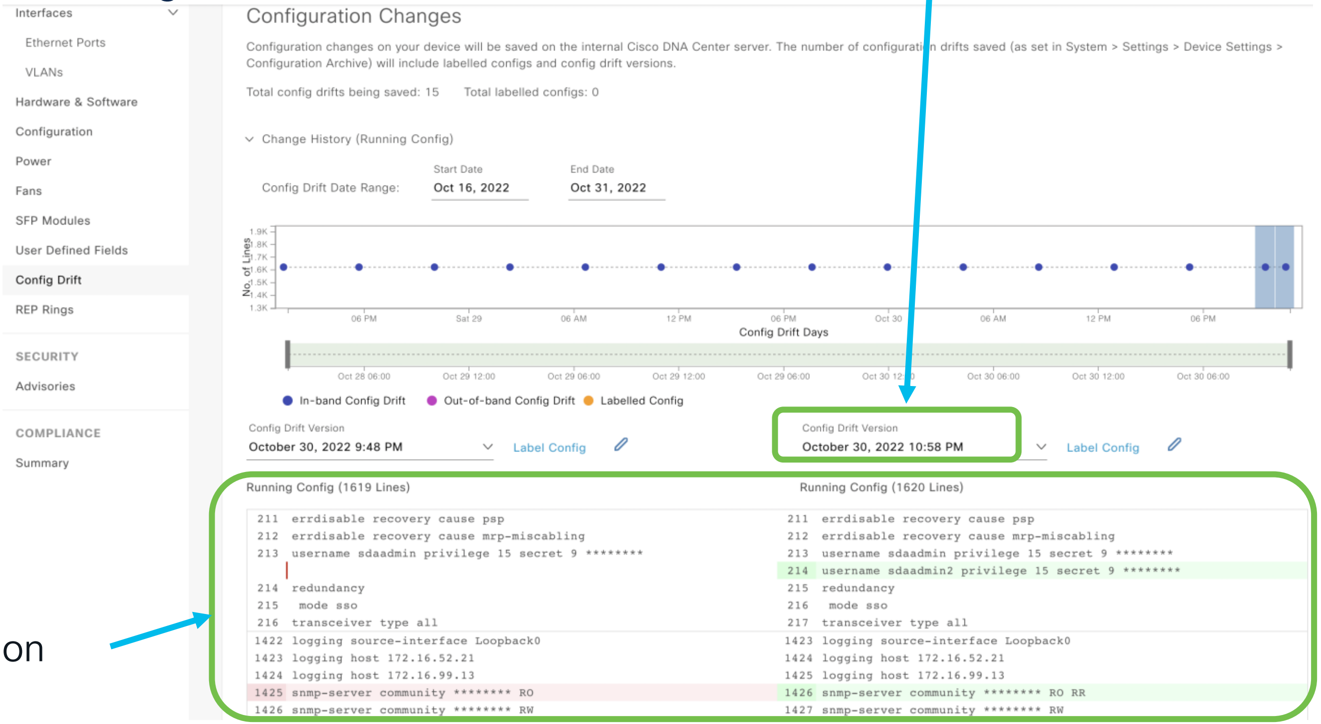
Check for configuration changes

- Config Drift
- Device CLI

Changes to

- SNMP
- AAA
- HTTPS
- Netconf
- Certificates

Timestamp



Configuration Changes

Configuration changes on your device will be saved on the internal Cisco DNA Center server. The number of configuration drifts saved (as set in System > Settings > Device Settings > Configuration Archive) will include labelled configs and config drift versions.

Total config drifts being saved: 15   Total labelled configs: 0

Change History (Running Config)

Config Drift Date Range: Start Date Oct 16, 2022 End Date Oct 31, 2022

Config Drift Version: October 30, 2022 9:48 PM

Config Drift Version: October 30, 2022 10:58 PM

Running Config (1619 Lines)

```
211  errdisable recovery cause psp
212  errdisable recovery cause mrp-miscabling
213  username sdaadmin privilege 15 secret 9 ********

214  redundancy
215   mode sso
216  transceiver type all
1422 logging source-interface Loopback0
1423 logging host 172.16.52.21
1424 logging host 172.16.99.13
1425 snmp-server community ******** RO
1426 snmp-server community ******** RW
```

Running Config (1620 Lines)

```
211  errdisable recovery cause psp
212  errdisable recovery cause mrp-miscabling
213  username sdaadmin privilege 15 secret 9 ********
214  username sdaadmin2 privilege 15 secret 9 ********
215  redundancy
216   mode sso
217  transceiver type all
1423 logging source-interface Loopback0
1424 logging host 172.16.52.21
1425 logging host 172.16.99.13
1426 snmp-server community ******** RO RR
1427 snmp-server community ******** RW
```

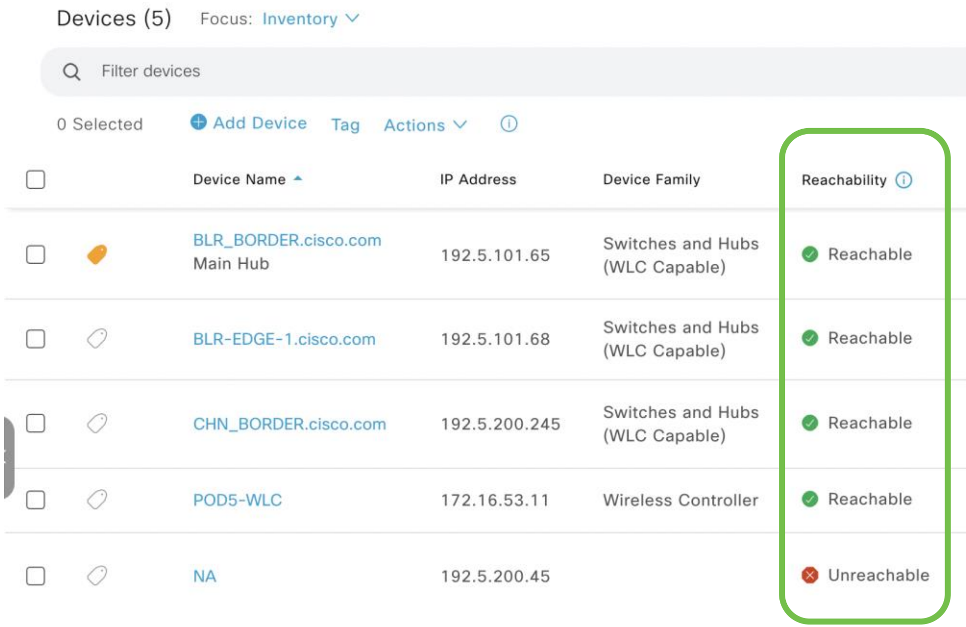
Configuration Diff

Provision / Inventory

Customer Voice

Q2: "Why is my device in an unmanaged or constant syncing or errored state?"

Check 'Reachability' column to determine reachability



Devices (5)   Focus: Inventory

Filter devices

0 Selected   Add Device   Tag   Actions

□		Device Name	IP Address	Device Family	Reachability
□		BLR_BORDER.cisco.com Main Hub	192.5.101.65	Switches and Hubs (WLC Capable)	✓ Reachable
□		BLR-EDGE-1.cisco.com	192.5.101.68	Switches and Hubs (WLC Capable)	✓ Reachable
□		CHN_BORDER.cisco.com	192.5.200.245	Switches and Hubs (WLC Capable)	✓ Reachable
□		POD5-WLC	172.16.53.11	Wireless Controller	✓ Reachable
□		NA	192.5.200.45		☒ Unreachable

Status	Reachability
Reachable	Reachable via all mandatory protocols
Ping Reachable	Reachable via ICMP
Unreachable	Unreachable via all mandatory protocols

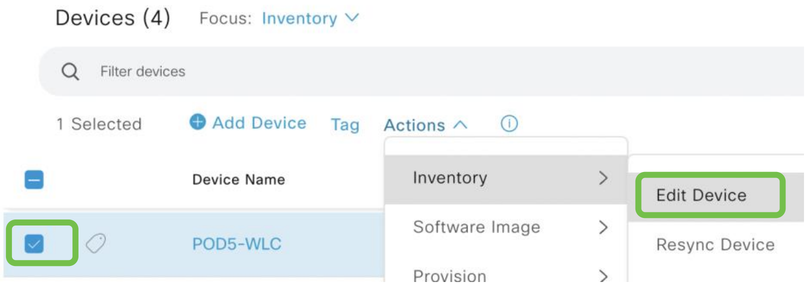
Provision / Inventory

Customer Voice

Q2: “Why is my device in an unmanaged or constant syncing or errored state?”

Verify Credentials

Step 1. Select device in Inventory



Devices (4) Focus: Inventory

Filter devices

1 Selected | Add Device | Tag | Actions

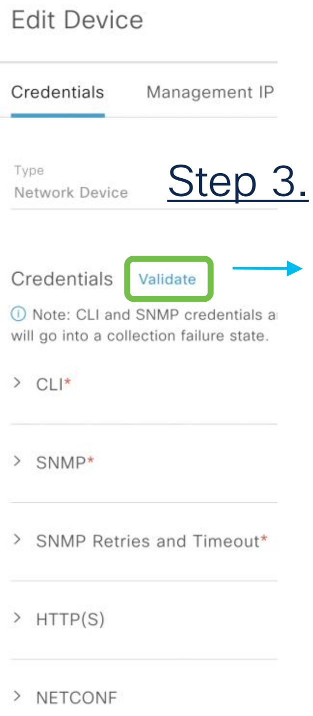
Device Name

☑ POD5-WLC

Inventory >
Software Image >
Provision >

Edit Device
Resync Device

Step 2. Select ‘Edit Device’ in the menu Actions → Inventory



Edit Device

Credentials | Management IP

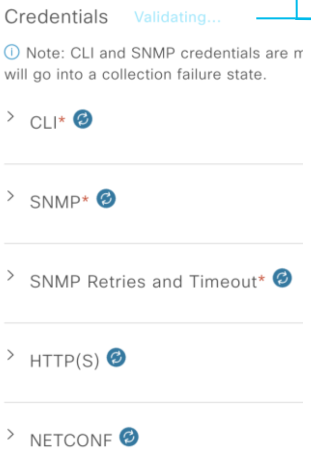
Type
Network Device

Credentials Validate

ⓘ Note: CLI and SNMP credentials a
will go into a collection failure state.

> CLI*
> SNMP*
> SNMP Retries and Timeout*
> HTTP(S)
> NETCONF

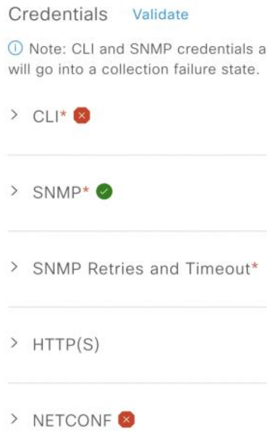
Step 3. Click Validate



Credentials Validating...

ⓘ Note: CLI and SNMP credentials are n
will go into a collection failure state.

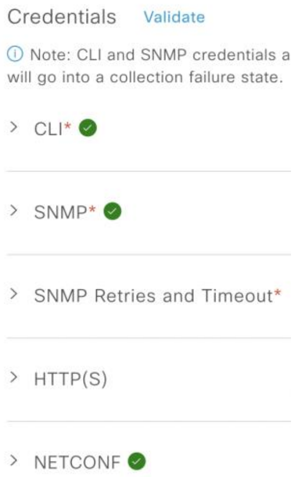
> CLI*
> SNMP*
> SNMP Retries and Timeout*
> HTTP(S)
> NETCONF



Credentials Validate

ⓘ Note: CLI and SNMP credentials a
will go into a collection failure state.

> CLI* ☒
> SNMP* ✓
> SNMP Retries and Timeout*
> HTTP(S)
> NETCONF ☒



Credentials Validate

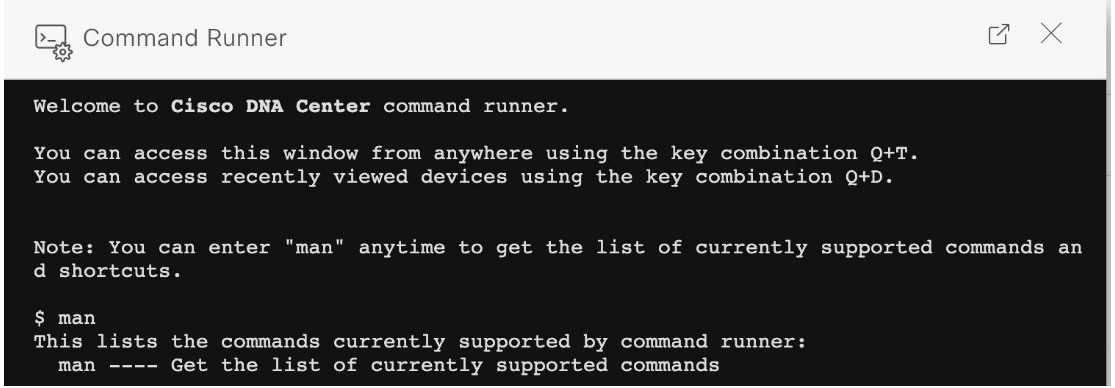
ⓘ Note: CLI and SNMP credentials a
will go into a collection failure state.

> CLI* ✓
> SNMP* ✓
> SNMP Retries and Timeout*
> HTTP(S)
> NETCONF ✓

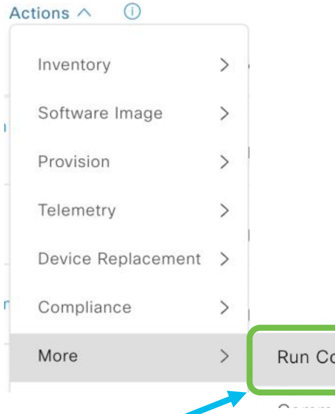
Customer Voice

Q2: “Why is my device in an unmanaged or constant syncing or errored state?”

Check device reachability from Cisco Catalyst Center



```
Welcome to Cisco DNA Center command runner.

You can access this window from anywhere using the key combination Q+T.
You can access recently viewed devices using the key combination Q+D.


Note: You can enter "man" anytime to get the list of currently supported commands an
d shortcuts.

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



Command runner for Cisco Catalyst Center

If ‘Unreachable’:

traceroute <IP address>
ping <IP address>
ping6 <IP address>

If ‘Ping Reachable’:

snmpget -v <version> <IP address> -c <community> <OID>

Netconf connectivity

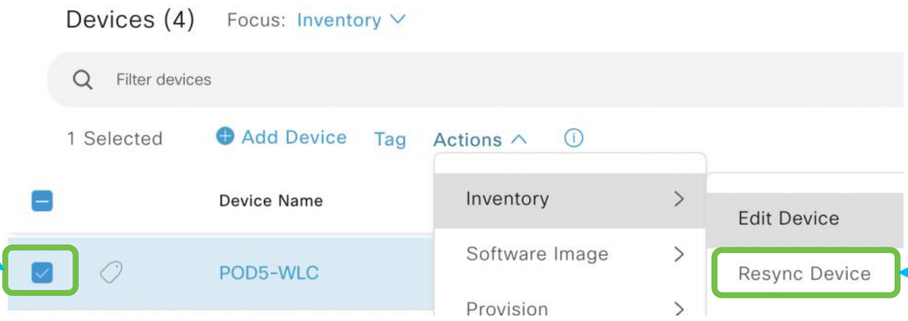
ssh –p 830 <username>@<IP address>

Provision / Inventory

Customer Voice

Q2: "Why is my device in an unmanaged or constant syncing or errored state?"

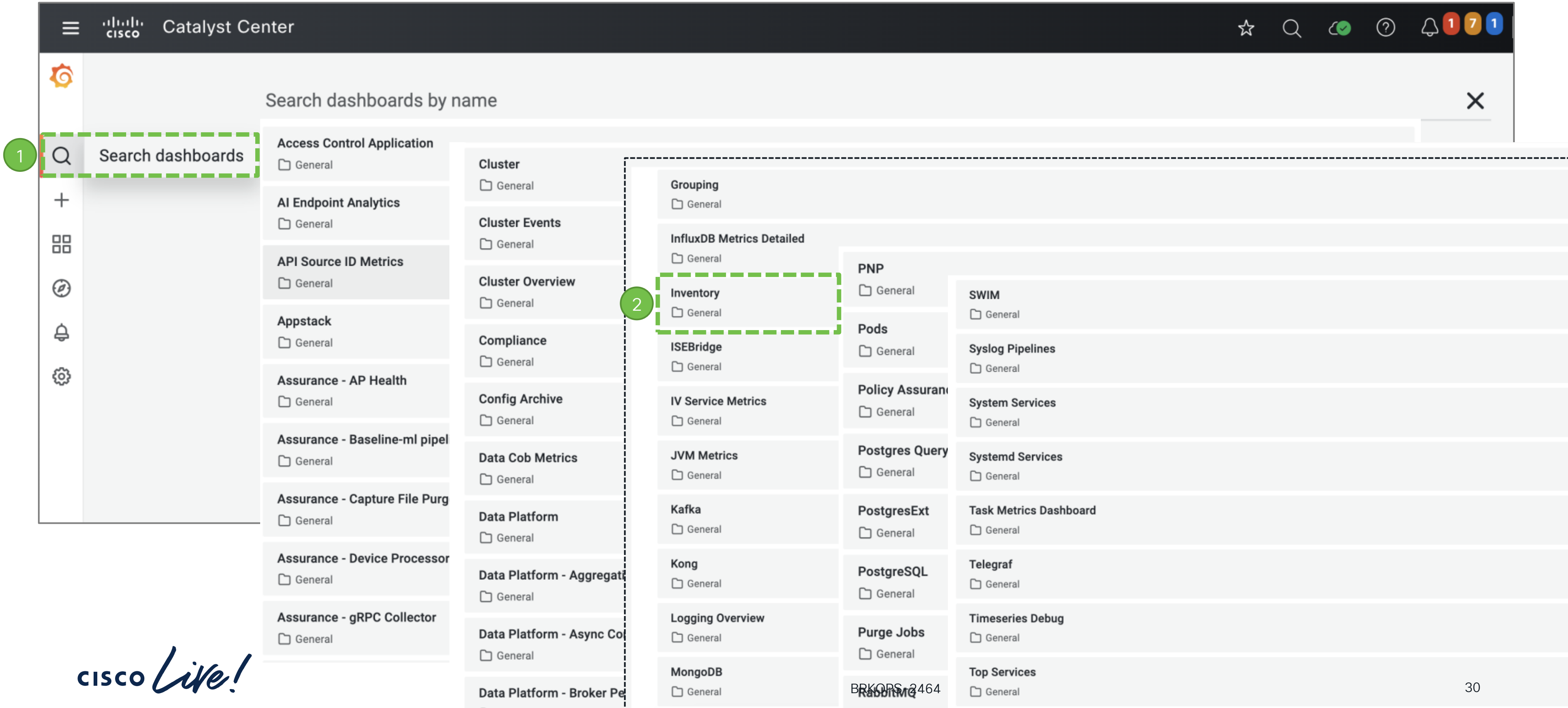
Resync the device



Step 1. Select the device

Step 2. Click to manually force a resync of the device

Inventory: Database Insights (Grafana)



Catalyst Center

Search dashboards by name

1 Search dashboards

Access Control Application
General

AI Endpoint Analytics
General

API Source ID Metrics
General

Appstack
General

Assurance - AP Health
General

Assurance - Baseline-ml pipel
General

Assurance - Capture File Purg
General

Assurance - Device Processor
General

Assurance - gRPC Collector
General

Cluster
General

Cluster Events
General

Cluster Overview
General

Compliance
General

Config Archive
General

Data Cob Metrics
General

Data Platform
General

Data Platform - Aggregati
General

Data Platform - Async Co
General

Data Platform - Broker Pe

Grouping
General

InfluxDB Metrics Detailed
General

2 Inventory
General

ISEBridge
General

IV Service Metrics
General

JVM Metrics
General

Kafka
General

Kong
General

Logging Overview
General

MongoDB
General

PNP
General

Pods
General

Policy Assuran
General

Postgres Query
General

PostgresExt
General

PostgreSQL
General

Purge Jobs
General

RabbitMQ

SWIM
General

Syslog Pipelines
General

System Services
General

Systemd Services
General

Task Metrics Dashboard
General

Telegraf
General

Timeseries Debug
General

Top Services
General

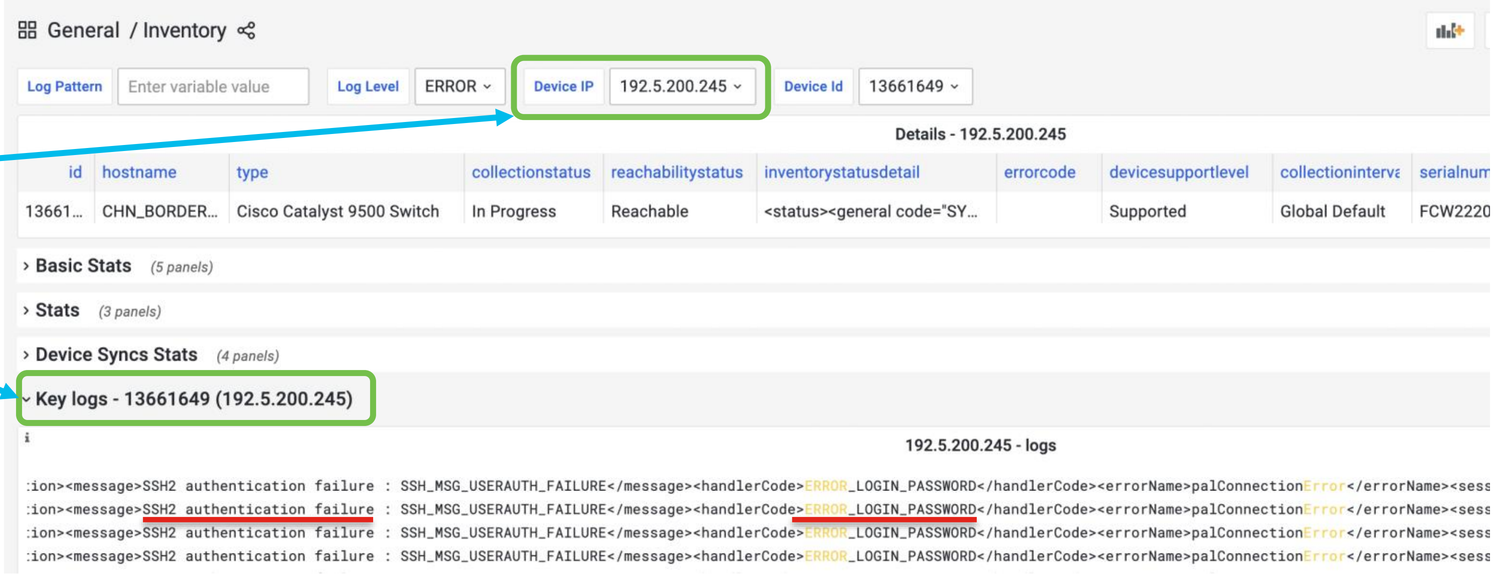
Customer Voice

Q2: “Why is my device in an unmanaged or constant syncing or errored state?”

View Inventory Service logs (Inventory Grafana Dashboard or the CLI)

Step 1. Select device IP

Step 2. Select ‘Key logs’ to view Service logs



Log Pattern: Enter variable value | Log Level: ERROR | Device IP: 192.5.200.245 | Device Id: 13661649

Details - 192.5.200.245

id	hostname	type	collectionstatus	reachabilitystatus	inventorystatusdetail	errorcode	devicesupportlevel	collectioninterva	serialnum
13661...	CHN_BORDER...	Cisco Catalyst 9500 Switch	In Progress	Reachable	<status><general code="SY...		Supported	Global Default	FCW2220

› Basic Stats (5 panels)

› Stats (3 panels)

› Device Syncs Stats (4 panels)

⌄ Key logs - 13661649 (192.5.200.245)

192.5.200.245 - logs

```
:ion><message>SSH2 authentication failure : SSH_MSG_USERAUTH_FAILURE</message><handlerCode>ERROR_LOGIN_PASSWORD</handlerCode><errorName>palConnectionError</errorName><sess
:ion><message>SSH2 authentication failure : SSH_MSG_USERAUTH_FAILURE</message><handlerCode>ERROR_LOGIN_PASSWORD</handlerCode><errorName>palConnectionError</errorName><sess
:ion><message>SSH2 authentication failure : SSH_MSG_USERAUTH_FAILURE</message><handlerCode>ERROR_LOGIN_PASSWORD</handlerCode><errorName>palConnectionError</errorName><sess
:ion><message>SSH2 authentication failure : SSH_MSG_USERAUTH_FAILURE</message><handlerCode>ERROR_LOGIN_PASSWORD</handlerCode><errorName>palConnectionError</errorName><sess
```

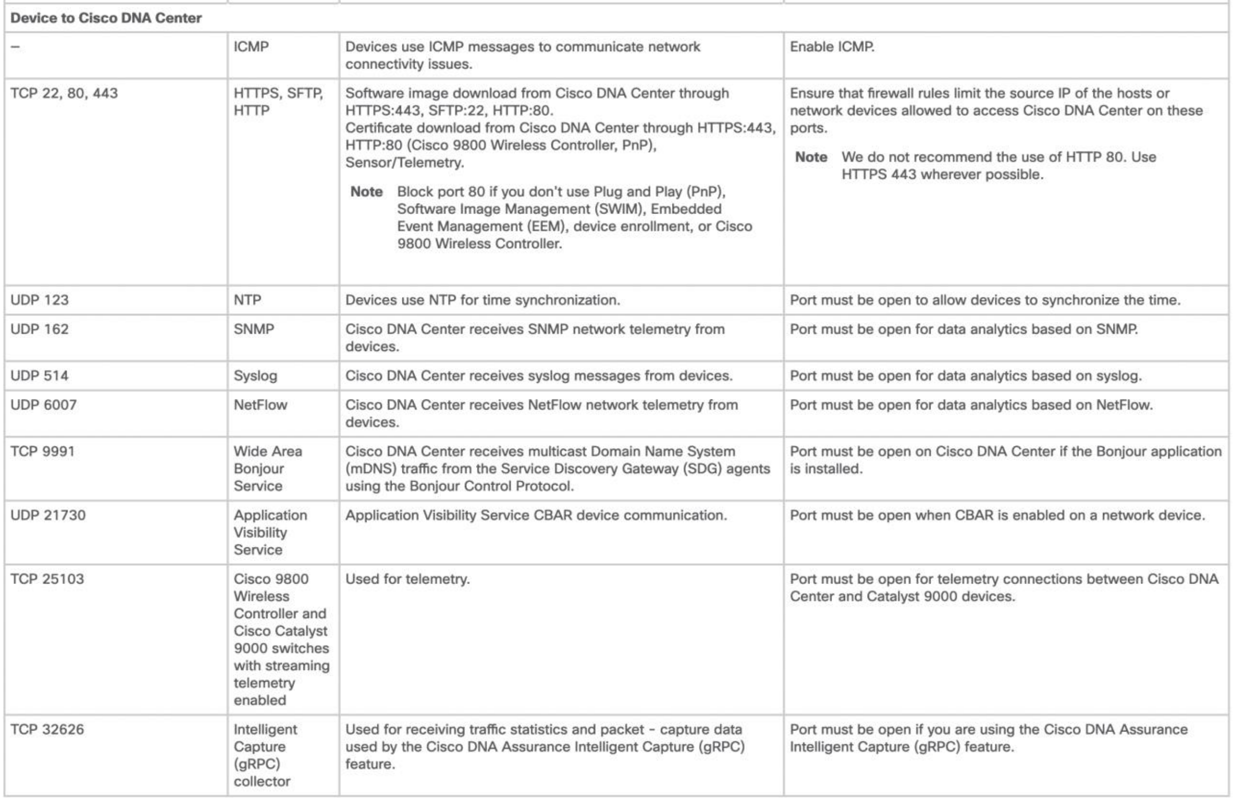
Most useful in an XL or Cluster setup where multiple Inventory instances exist

Customer Voice

Q2: “Why is my device in an unmanaged or constant syncing or errored state?”

Ensure no firewall blocking necessary ports

Cisco Catalyst Center to device **inbound** ports to be kept open



Device to Cisco DNA Center			
–	ICMP	Devices use ICMP messages to communicate network connectivity issues.	Enable ICMP.
TCP 22, 80, 443	HTTPS, SFTP, HTTP	Software image download from Cisco DNA Center through HTTPS:443, SFTP:22, HTTP:80. Certificate download from Cisco DNA Center through HTTPS:443, HTTP:80 (Cisco 9800 Wireless Controller, PnP), Sensor/Telemetry. **Note** Block port 80 if you don't use Plug and Play (PnP), Software Image Management (SWIM), Embedded Event Management (EEM), device enrollment, or Cisco 9800 Wireless Controller.	Ensure that firewall rules limit the source IP of the hosts or network devices allowed to access Cisco DNA Center on these ports. **Note** We do not recommend the use of HTTP 80. Use HTTPS 443 wherever possible.
UDP 123	NTP	Devices use NTP for time synchronization.	Port must be open to allow devices to synchronize the time.
UDP 162	SNMP	Cisco DNA Center receives SNMP network telemetry from devices.	Port must be open for data analytics based on SNMP.
UDP 514	Syslog	Cisco DNA Center receives syslog messages from devices.	Port must be open for data analytics based on syslog.
UDP 6007	NetFlow	Cisco DNA Center receives NetFlow network telemetry from devices.	Port must be open for data analytics based on NetFlow.
TCP 9991	Wide Area Bonjour Service	Cisco DNA Center receives multicast Domain Name System (mDNS) traffic from the Service Discovery Gateway (SDG) agents using the Bonjour Control Protocol.	Port must be open on Cisco DNA Center if the Bonjour application is installed.
UDP 21730	Application Visibility Service	Application Visibility Service CBAR device communication.	Port must be open when CBAR is enabled on a network device.
TCP 25103	Cisco 9800 Wireless Controller and Cisco Catalyst 9000 switches with streaming telemetry enabled	Used for telemetry.	Port must be open for telemetry connections between Cisco DNA Center and Catalyst 9000 devices.
TCP 32626	Intelligent Capture (gRPC) collector	Used for receiving traffic statistics and packet - capture data used by the Cisco DNA Assurance Intelligent Capture (gRPC) feature.	Port must be open if you are using the Cisco DNA Assurance Intelligent Capture (gRPC) feature.

*from Cisco.com

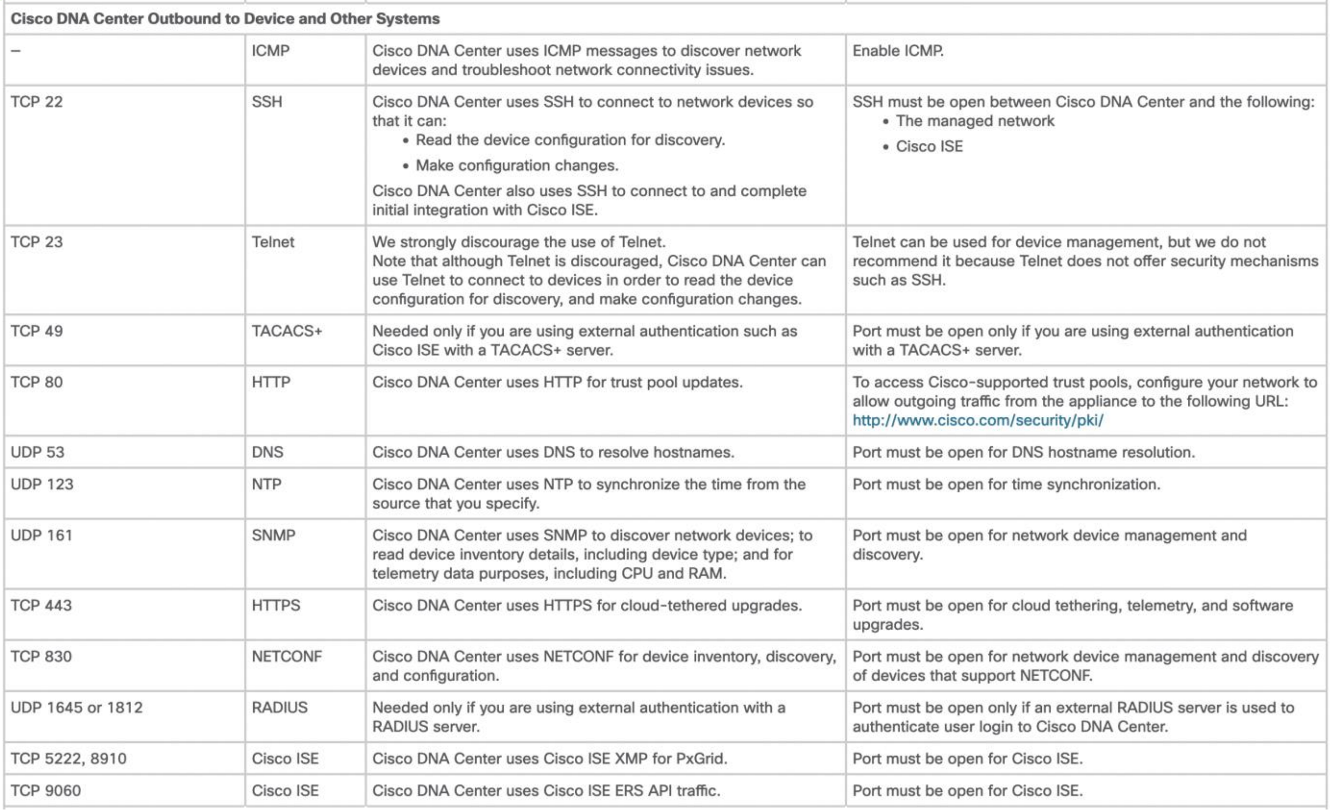
cisco Live!

Customer Voice

Q2: “Why is my device in an unmanaged or constant syncing or errored state?”

Ensure no firewall blocking necessary ports

Cisco Catalyst Center to device **outbound** ports to be kept open

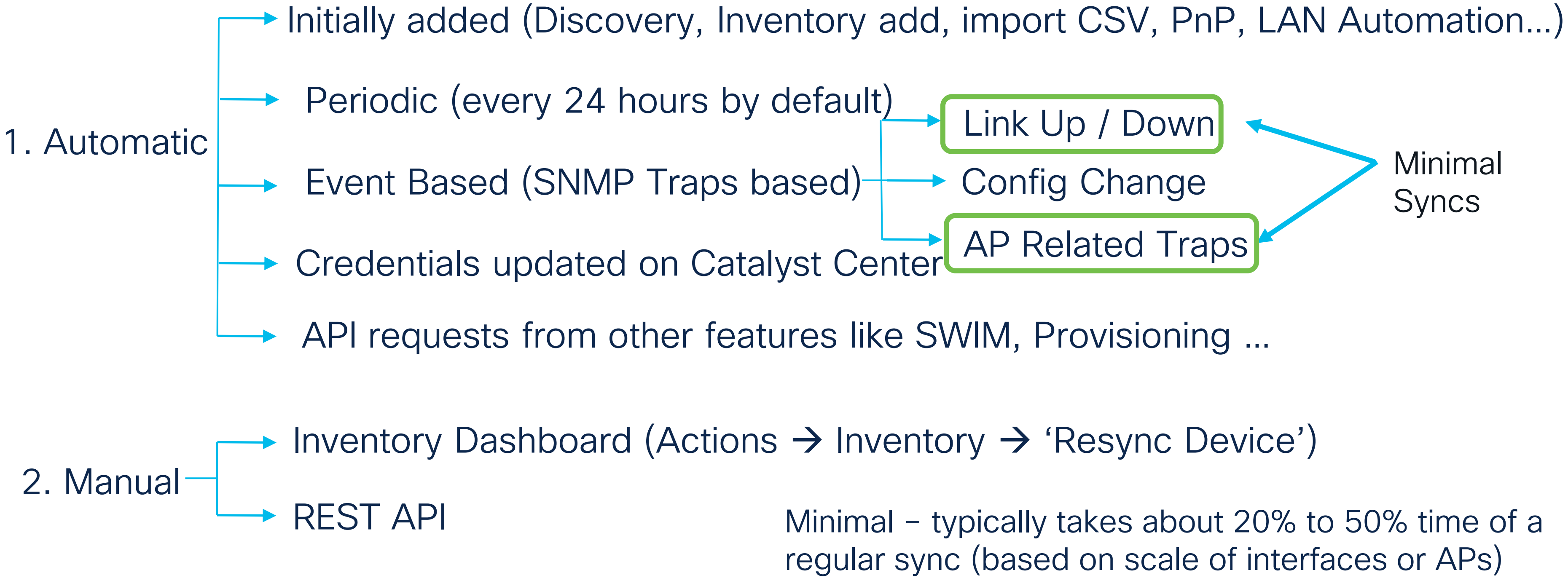


Cisco DNA Center Outbound to Device and Other Systems			
–	ICMP	Cisco DNA Center uses ICMP messages to discover network devices and troubleshoot network connectivity issues.	Enable ICMP.
TCP 22	SSH	Cisco DNA Center uses SSH to connect to network devices so that it can: • Read the device configuration for discovery. • Make configuration changes. Cisco DNA Center also uses SSH to connect to and complete initial integration with Cisco ISE.	SSH must be open between Cisco DNA Center and the following: • The managed network • Cisco ISE
TCP 23	Telnet	We strongly discourage the use of Telnet. Note that although Telnet is discouraged, Cisco DNA Center can use Telnet to connect to devices in order to read the device configuration for discovery, and make configuration changes.	Telnet can be used for device management, but we do not recommend it because Telnet does not offer security mechanisms such as SSH.
TCP 49	TACACS+	Needed only if you are using external authentication such as Cisco ISE with a TACACS+ server.	Port must be open only if you are using external authentication with a TACACS+ server.
TCP 80	HTTP	Cisco DNA Center uses HTTP for trust pool updates.	To access Cisco-supported trust pools, configure your network to allow outgoing traffic from the appliance to the following URL: http://www.cisco.com/security/pki/
UDP 53	DNS	Cisco DNA Center uses DNS to resolve hostnames.	Port must be open for DNS hostname resolution.
UDP 123	NTP	Cisco DNA Center uses NTP to synchronize the time from the source that you specify.	Port must be open for time synchronization.
UDP 161	SNMP	Cisco DNA Center uses SNMP to discover network devices; to read device inventory details, including device type; and for telemetry data purposes, including CPU and RAM.	Port must be open for network device management and discovery.
TCP 443	HTTPS	Cisco DNA Center uses HTTPS for cloud-tethered upgrades.	Port must be open for cloud tethering, telemetry, and software upgrades.
TCP 830	NETCONF	Cisco DNA Center uses NETCONF for device inventory, discovery, and configuration.	Port must be open for network device management and discovery of devices that support NETCONF.
UDP 1645 or 1812	RADIUS	Needed only if you are using external authentication with a RADIUS server.	Port must be open only if an external RADIUS server is used to authenticate user login to Cisco DNA Center.
TCP 5222, 8910	Cisco ISE	Cisco DNA Center uses Cisco ISE XMP for PxGrid.	Port must be open for Cisco ISE.
TCP 9060	Cisco ISE	Cisco DNA Center uses Cisco ISE ERS API traffic.	Port must be open for Cisco ISE.

*from Cisco.com

Customer Voice

Q3: “When does the Inventory connect to my device to collect data?”



1. Automatic
   - Initially added (Discovery, Inventory add, import CSV, PnP, LAN Automation...)
   - Periodic (every 24 hours by default)
   - Event Based (SNMP Traps based)
     - Link Up / Down
     - Config Change
     - AP Related Traps
   - Credentials updated on Catalyst Center
   - API requests from other features like SWIM, Provisioning ...

Minimal Syncs

2. Manual
   - Inventory Dashboard (Actions → Inventory → ‘Resync Device’)
   - REST API

Minimal – typically takes about 20% to 50% time of a regular sync (based on scale of interfaces or APs)

Catalyst Center Device Provisioning Troubleshooting

What is Provisioning?

Every time we push any configuration to our network devices, we are provisioning them

Initial Provisioning

- Authentication Templates Methods
  - Closed, Open, Easy Connect
- Network Settings
  - AAA, DNS, NTP, etc.

Configuration Template Provisioning

- Templates based in device family, type, tags, etc.

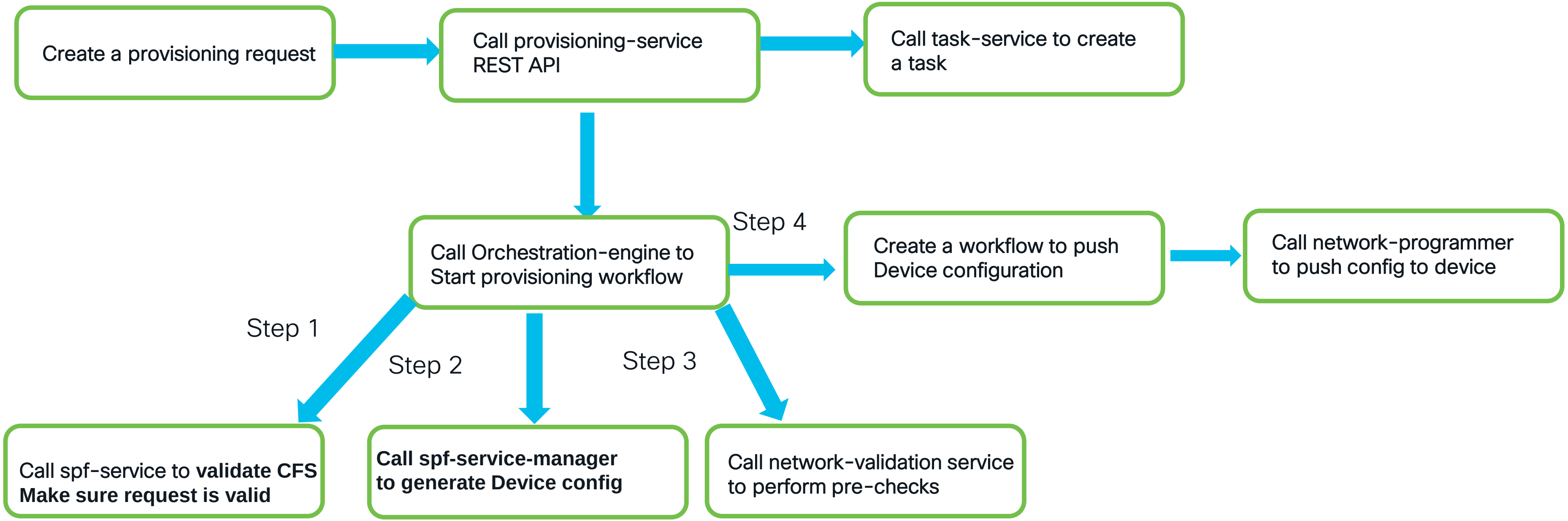
Fabric Provisioning

- Border vs CP vs Edge
- VNs, LISP, VXLAN, BGP, redistribution

Host Onboarding

- L2 (VLANs), L3 (Anycast SVIs), IP Address Pools,
- CTS (TrustSec – Policy Plane)
- IPDT (Device Tracking)

Provisioning workflow



Create a provisioning request

Call provisioning-service REST API

Call task-service to create a task

Call Orchestration-engine to Start provisioning workflow

Step 1

Call spf-service to **validate CFS** **Make sure request is valid**

Step 2

Call spf-service-manager to generate Device config

Step 3

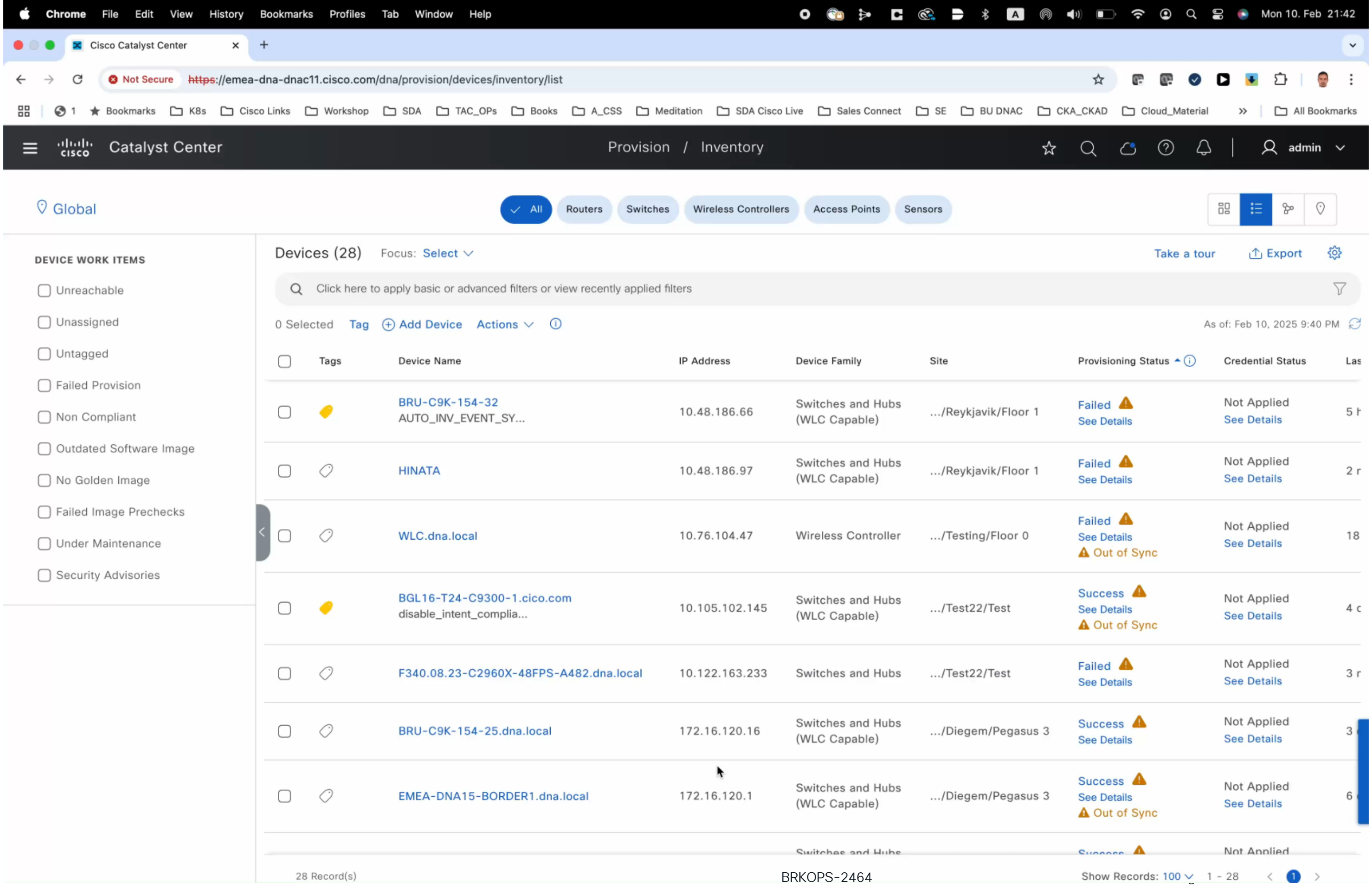
Call network-validation service to perform pre-checks

Step 4

Create a workflow to push Device configuration

Call network-programmer to push config to device

Demo



Chrome File Edit View History Bookmarks Profiles Tab Window Help
Mon 10. Feb 21:42
Cisco Catalyst Center
Not Secure https://emea-dna-dnac11.cisco.com/dna/provision/devices/inventory/list
1 Bookmarks K8s Cisco Links Workshop SDA TAC_OPs Books A_CSS Meditation SDA Cisco Live Sales Connect SE BU DNAC CKA_CKAD Cloud_Material All Bookmarks
Catalyst Center
Provision / Inventory
admin
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 (28) Focus: Select

Take a tour Export

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

0 Selected Tag Add Device Actions

As of: Feb 10, 2025 9:40 PM

□	Tags	Device Name	IP Address	Device Family	Site	Provisioning Status	Credential Status	Las
□	🏷	BRU-C9K-154-32 AUTO_INV_EVENT_SY...	10.48.186.66	Switches and Hubs (WLC Capable)	.../Reykjavik/Floor 1	Failed ⚠ See Details	Not Applied See Details	5 h
□	🏷	HINATA	10.48.186.97	Switches and Hubs (WLC Capable)	.../Reykjavik/Floor 1	Failed ⚠ See Details	Not Applied See Details	2 r
□	🏷	WLC.dna.local	10.76.104.47	Wireless Controller	.../Testing/Floor 0	Failed ⚠ See Details ⚠ Out of Sync	Not Applied See Details	18
□	🏷	BGL16-T24-C9300-1.cico.com disable_intent_complia...	10.105.102.145	Switches and Hubs (WLC Capable)	.../Test22/Test	Success ⚠ See Details ⚠ Out of Sync	Not Applied See Details	4 c
□	🏷	F340.08.23-C2960X-48FPS-A482.dna.local	10.122.163.233	Switches and Hubs	.../Test22/Test	Failed ⚠ See Details	Not Applied See Details	3 r
□	🏷	BRU-C9K-154-25.dna.local	172.16.120.16	Switches and Hubs (WLC Capable)	.../Diegem/Pegasus 3	Success ⚠ See Details	Not Applied See Details	3
□	🏷	EMEA-DNA15-BORDER1.dna.local	172.16.120.1	Switches and Hubs (WLC Capable)	.../Diegem/Pegasus 3	Success ⚠ See Details ⚠ Out of Sync	Not Applied See Details	6
				Switches and Hubs		Success ⚠	Not Applied	

28 Record(s) Show Records: 100 1 - 28 1

Catalyst Center SWIM Troubleshooting

SWIM Recap

Upgrading & Patching the Operating System running on the switches, routers, firewalls & other networking devices.

2.3.7

Design > Image Repository

- Imports / stores the required images & patches (SMU)
- Marking the images as Golden
- Import the ISSU Compatibility Matrix

Inventory (Software Images focus)

- Provisioning software images to the devices (Distribution + Activation)
- Check Image update status
- Perform Image update readiness

System > Settings

- Configure up to 3 external image distribution servers
- Change the protocol order of an image distribution server

Workflows (Image Update)

- Plan multiple device upgrades using the ‘Image Update’ workflow
- Support flexible device ordering

SWIM Recap

Upgrading & Patching the Operating System running on the switches, routers, firewalls & other networking devices.

SWIM Basics

- Pre-checks
  - Startup config check
  - Config register value
  - Flash memory
  - File transfer protocol
  - Service entitlement
- HTTPS, SCP & SFTP (WLC) are the supported file transfer protocols

Change in Operation from 2.3.x

1. Distribute Operation

Copy Images to flash
install add file <Image Name>
ap image pre-download (ewlc 9800)

2. Activate Operation

install activate <image name>
install commit

*Moved from Activate step to Distribute.

Common SWIM Issues – Image Repository

Issue 1. – Image information has not been updated

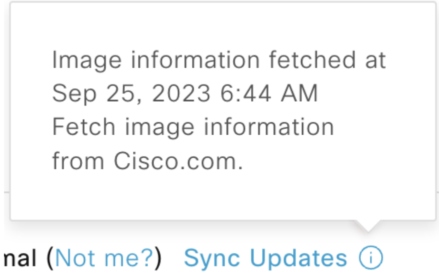


Image information fetched at Sep 25, 2023 6:44 AM
Fetch image information from Cisco.com.

nal (Not me?) Sync Updates ⓘ

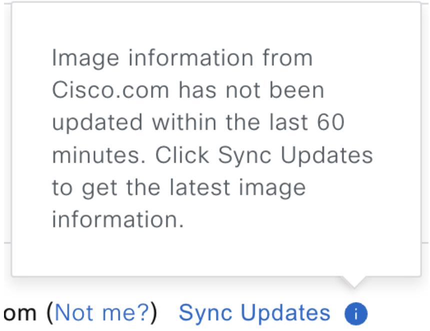


Image information from Cisco.com has not been updated within the last 60 minutes. Click Sync Updates to get the latest image information.

om (Not me?) Sync Updates ⓘ

Common Reasons:

1. Connectivity - Firewall

To check SSL/TLS certificate revocation status using OCSP/CRL, access the following URLs; access must be allowed either directly or through the proxy server.

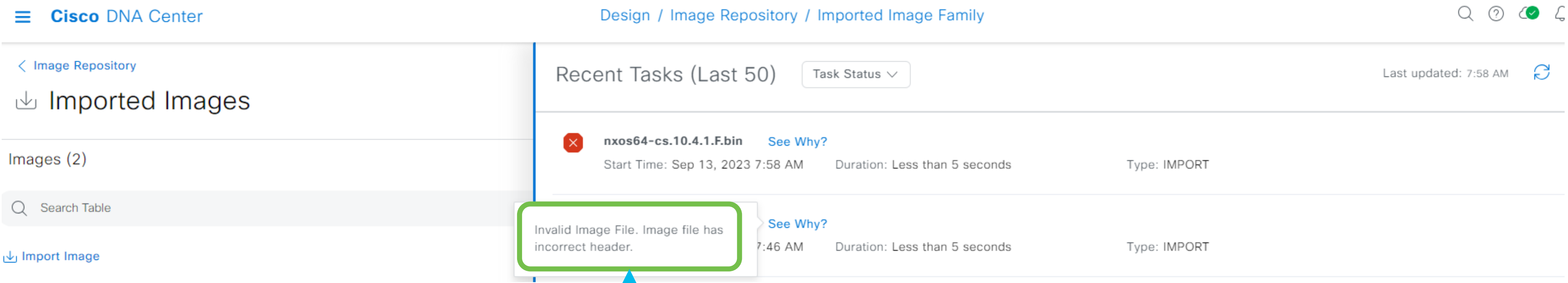
- http://ocsp.quovadisglobal.com
- http://crl.quovadisglobal.com/*
- http://*.identrust.com

2. Cisco.com credentials

Ensure that Cisco.com account credentials are provided in the settings or the image repository window and the accounts have the permission to download the software images.

Common SWIM Issues – Image Repository

Issue 2. – Unsupported image, pls check the compatibility matrix



nxos64-cs.10.4.1.F.bin See Why?
Start Time: Sep 13, 2023 7:58 AM Duration: Less than 5 seconds Type: IMPORT

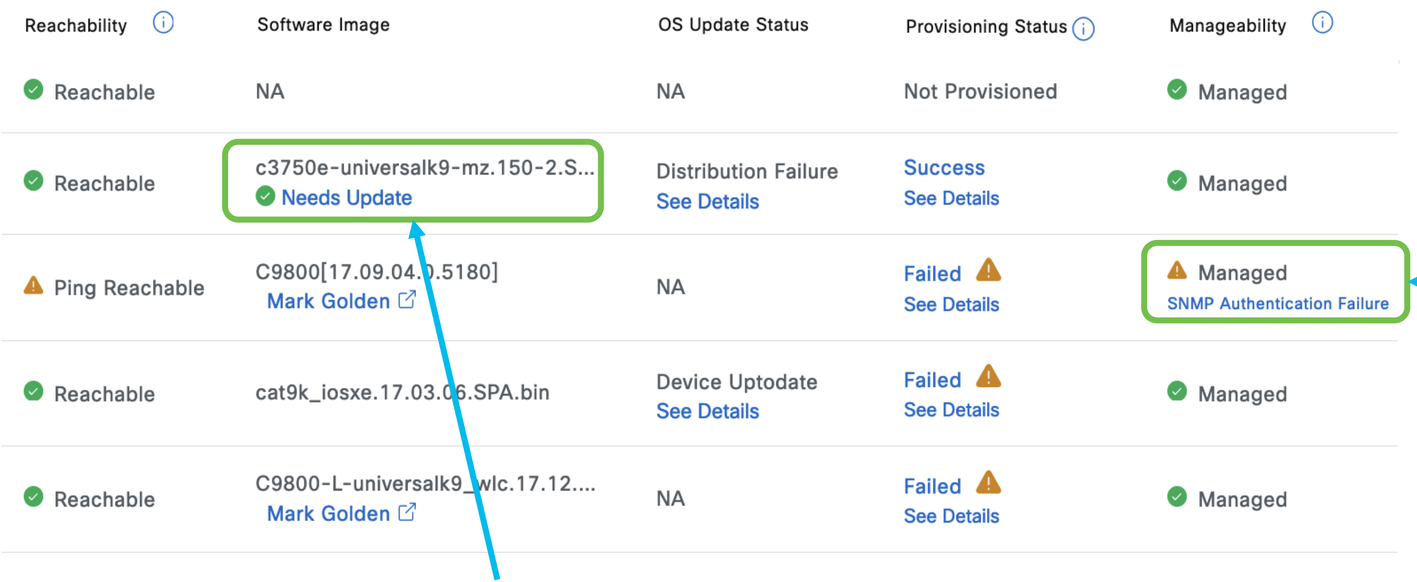
Invalid Image File. Image file has incorrect header.

See Why?
7:46 AM Duration: Less than 5 seconds Type: IMPORT

Error indicates that the image is invalid

Common SWIM Issues – Distribution + Activation

Inventory (Software Image Focus)



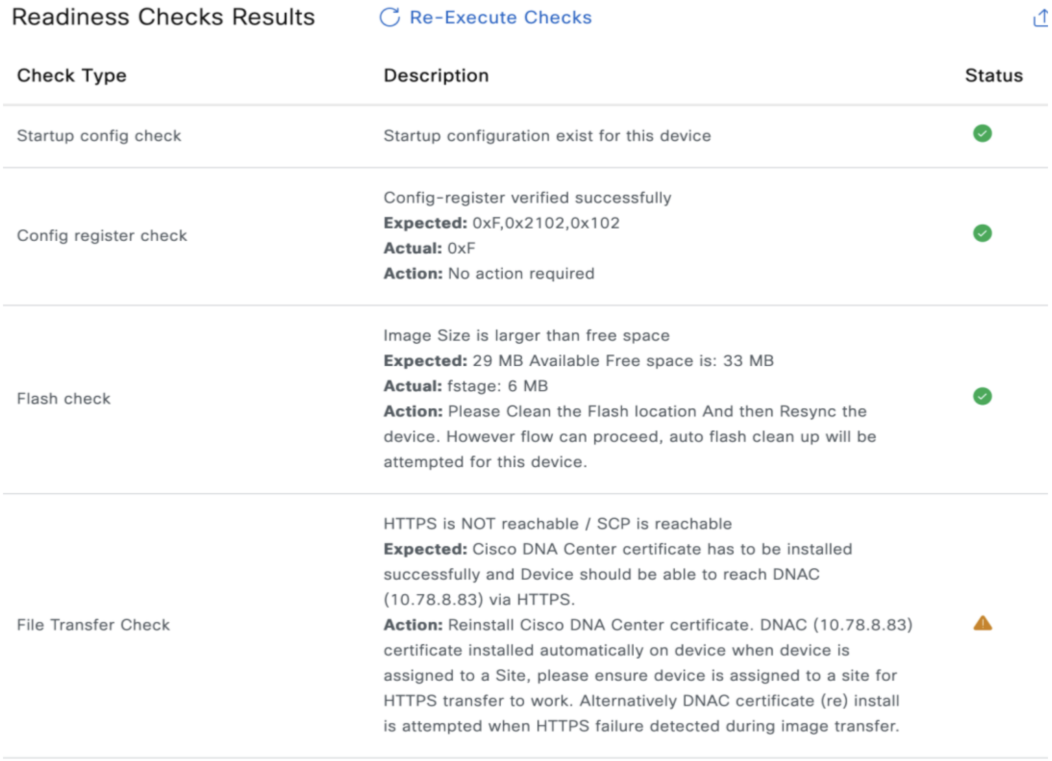
Reachability ⓘ	Software Image	OS Update Status	Provisioning Status ⓘ	Manageability ⓘ
✓ Reachable	NA	NA	Not Provisioned	✓ Managed
✓ Reachable	c3750e-universalk9-mz.150-2.S... ✓ Needs Update	Distribution Failure See Details	Success See Details	✓ Managed
⚠ Ping Reachable	C9800[17.09.04.0.5180] Mark Golden	NA	Failed ⚠ See Details	⚠ Managed SNMP Authentication Failure
✓ Reachable	cat9k_iosxe.17.03.06.SPA.bin	Device Uptodate See Details	Failed ⚠ See Details	✓ Managed
✓ Reachable	C9800-L-universalk9_wlc.17.12.... Mark Golden	NA	Failed ⚠ See Details	✓ Managed

1. Device needs to be Managed & Reachable

2. Click on 'Needs Update' to check for status or rerun Readiness Check

Common SWIM Issues – Distribution + Activation

Checks to avoid common distribution/activation issues can be performed by clicking on ‘Needs Update’.



Readiness Checks Results

Check Type	Description	Status
Startup config check	Startup configuration exist for this device	✓
Config register check	Config-register verified successfully **Expected:** 0xF,0x2102,0x102 **Actual:** 0xF **Action:** No action required	✓
Flash check	Image Size is larger than free space **Expected:** 29 MB Available Free space is: 33 MB **Actual:** fstage: 6 MB **Action:** Please Clean the Flash location And then Resync the device. However flow can proceed, auto flash clean up will be attempted for this device.	✓
File Transfer Check	HTTPS is NOT reachable / SCP is reachable **Expected:** Cisco DNA Center certificate has to be installed successfully and Device should be able to reach DNAC (10.78.8.83) via HTTPS. **Action:** Reinstall Cisco DNA Center certificate. DNAC (10.78.8.83) certificate installed automatically on device when device is assigned to a Site, please ensure device is assigned to a site for HTTPS transfer to work. Alternatively DNAC certificate (re) install is attempted when HTTPS failure detected during image transfer.	⚠

Failed scenario for Flash Check

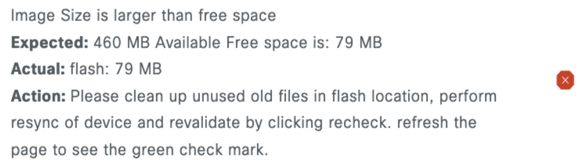
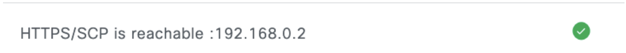


Image Size is larger than free space **Expected:** 460 MB Available Free space is: 79 MB **Actual:** flash: 79 MB **Action:** Please clean up unused old files in flash location, perform resync of device and revalidate by clicking recheck. refresh the page to see the green check mark.	✗

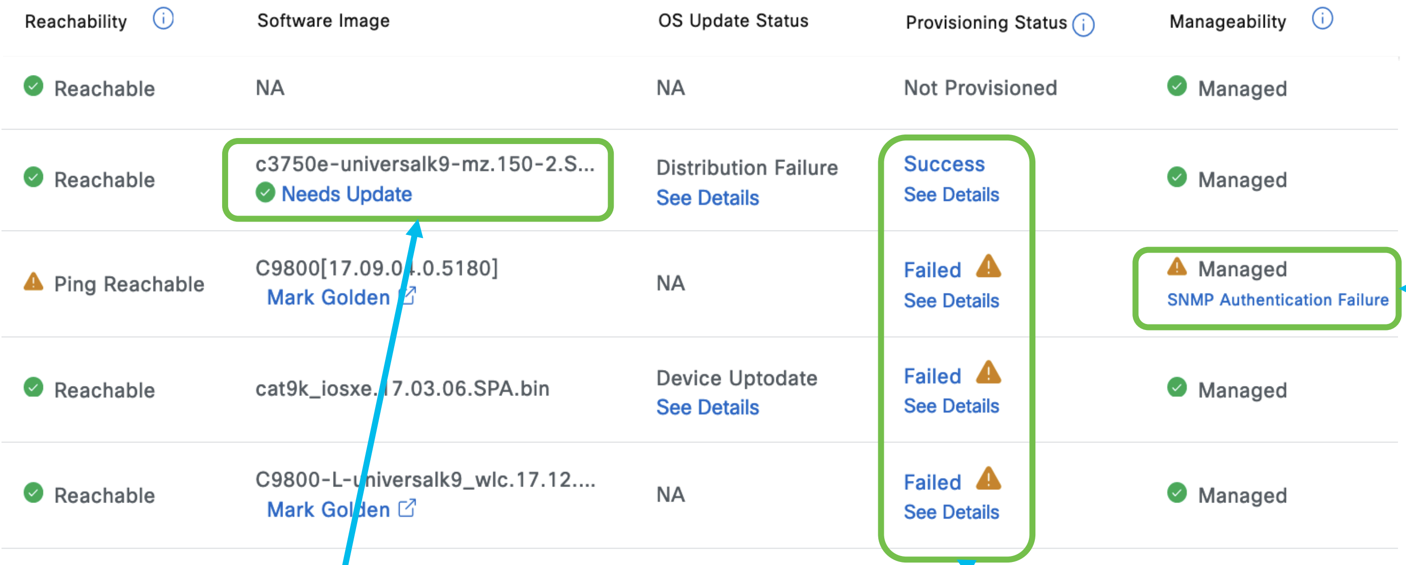
Success scenario for File Transfer Check



HTTPS/SCP is reachable :192.168.0.2	✓

Common SWIM Issues – Distribution + Activation

Inventory (Software Image Focus)



Reachability	Software Image	OS Update Status	Provisioning Status	Manageability
✓ Reachable	NA	NA	Not Provisioned	✓ Managed
✓ Reachable	c3750e-universalk9-mz.150-2.S... ✓ Needs Update	Distribution Failure See Details	Success See Details	✓ Managed
⚠ Ping Reachable	C9800[17.09.04.0.5180] Mark Golden	NA	Failed ⚠ See Details	⚠ Managed SNMP Authentication Failure
✓ Reachable	cat9k_iosxe.17.03.06.SPA.bin	Device Uptodate See Details	Failed ⚠ See Details	✓ Managed
✓ Reachable	C9800-L-universalk9_wlc.17.12.... Mark Golden	NA	Failed ⚠ See Details	✓ Managed

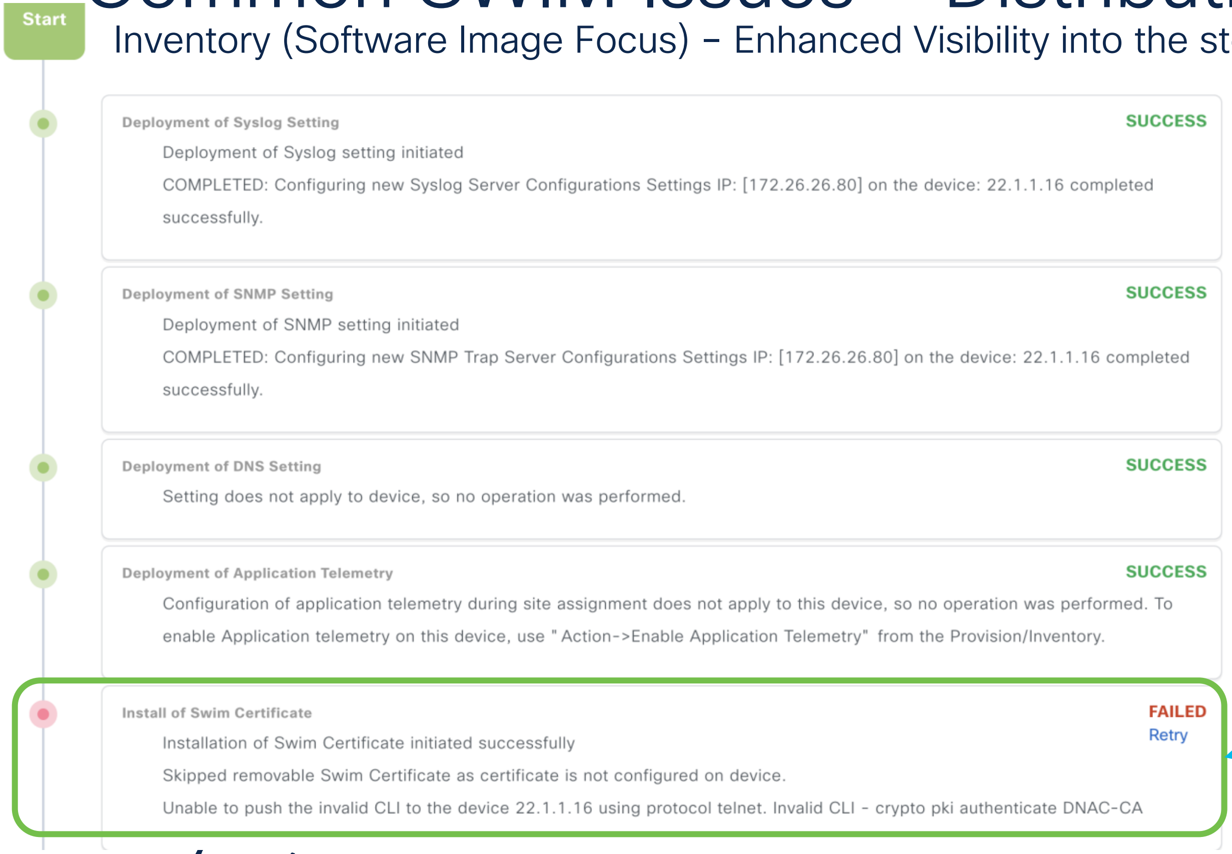
1. Device needs to be Managed & Reachable

2. Click on 'Needs Update' to check for status and rerun Readiness Check

3. Click on 'See Details' for a detailed view on the Image Provisioning status

Common SWIM Issues – Distribution + Activation

Inventory (Software Image Focus) – Enhanced Visibility into the steps performed



Deployment of Syslog Setting — SUCCESS

Deployment of Syslog setting initiated

COMPLETED: Configuring new Syslog Server Configurations Settings IP: [172.26.26.80] on the device: 22.1.1.16 completed successfully.

Deployment of SNMP Setting — SUCCESS

Deployment of SNMP setting initiated

COMPLETED: Configuring new SNMP Trap Server Configurations Settings IP: [172.26.26.80] on the device: 22.1.1.16 completed successfully.

Deployment of DNS Setting — SUCCESS

Setting does not apply to device, so no operation was performed.

Deployment of Application Telemetry — SUCCESS

Configuration of application telemetry during site assignment does not apply to this device, so no operation was performed. To enable Application telemetry on this device, use " Action->Enable Application Telemetry" from the Provision/Inventory.

Install of Swim Certificate — FAILED

Retry

Installation of Swim Certificate initiated successfully

Skipped removable Swim Certificate as certificate is not configured on device.

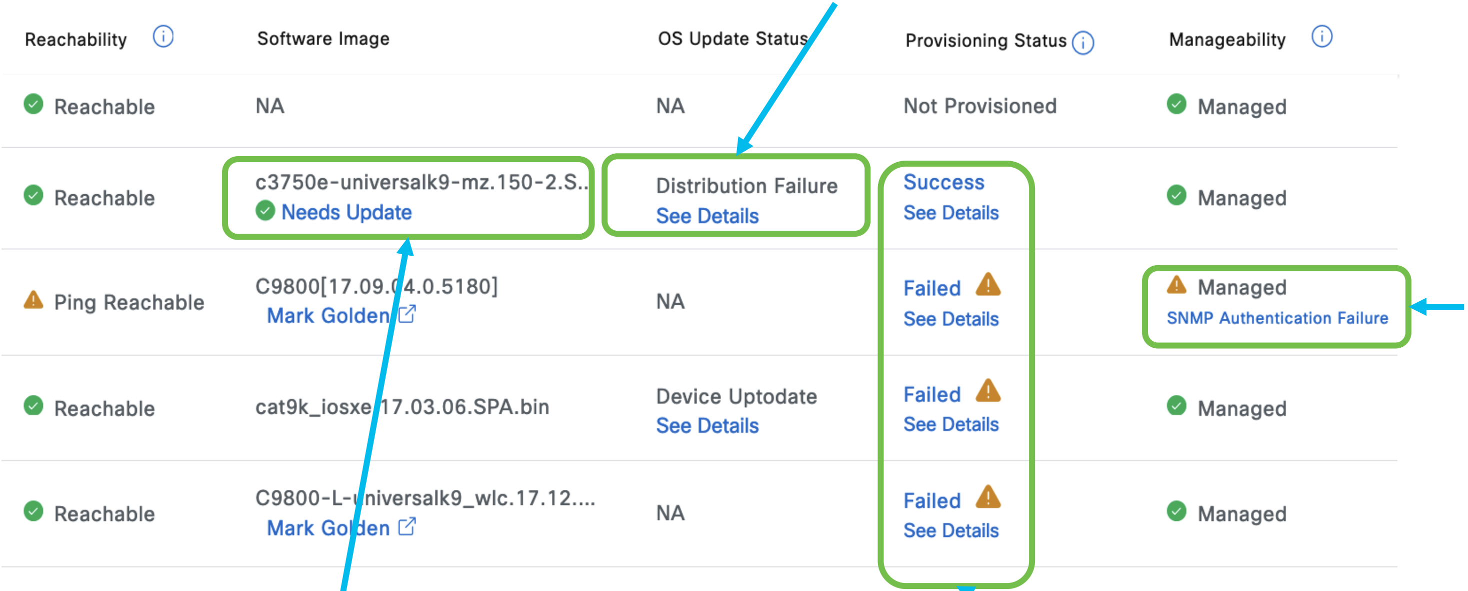
Unable to push the invalid CLI to the device 22.1.1.16 using protocol telnet. Invalid CLI - crypto pki authenticate DNAC-CA

Example of a Failure

Common SWIM Issues – Distribution + Activation

Inventory (Software Image Focus)

4. 'See Details' To view the distribution/activation failures



Reachability ⓘ	Software Image	OS Update Status	Provisioning Status ⓘ	Manageability ⓘ
✓ Reachable	NA	NA	Not Provisioned	✓ Managed
✓ Reachable	c3750e-universalk9-mz.150-2.S.. ✓ Needs Update	Distribution Failure See Details	Success See Details	✓ Managed
⚠ Ping Reachable	C9800[17.09.04.0.5180] Mark Golden ↗	NA	Failed ⚠ See Details	⚠ Managed SNMP Authentication Failure
✓ Reachable	cat9k_iosxe.17.03.06.SPA.bin	Device Uptodate See Details	Failed ⚠ See Details	✓ Managed
✓ Reachable	C9800-L-universalk9_wlc.17.12.... Mark Golden ↗	NA	Failed ⚠ See Details	✓ Managed

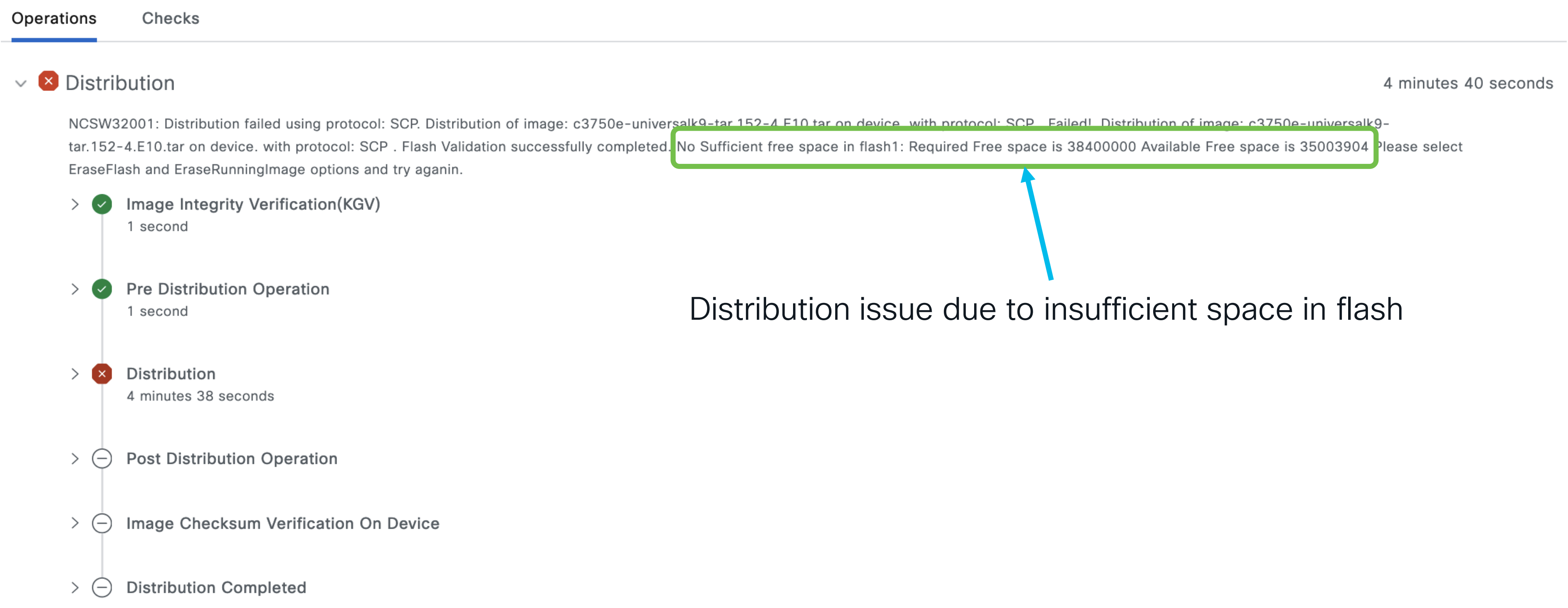
1. Device needs to be Managed & Reachable

2. Click on 'Needs Update' to check for status and rerun Readiness Check

3. Click on 'See Details' for a detailed view on the Image Provisioning status

Common SWIM Issues – Distribution + Activation

Inventory (Software Image Focus) – Enhanced Visibility into the steps performed



Distribution — 4 minutes 40 seconds

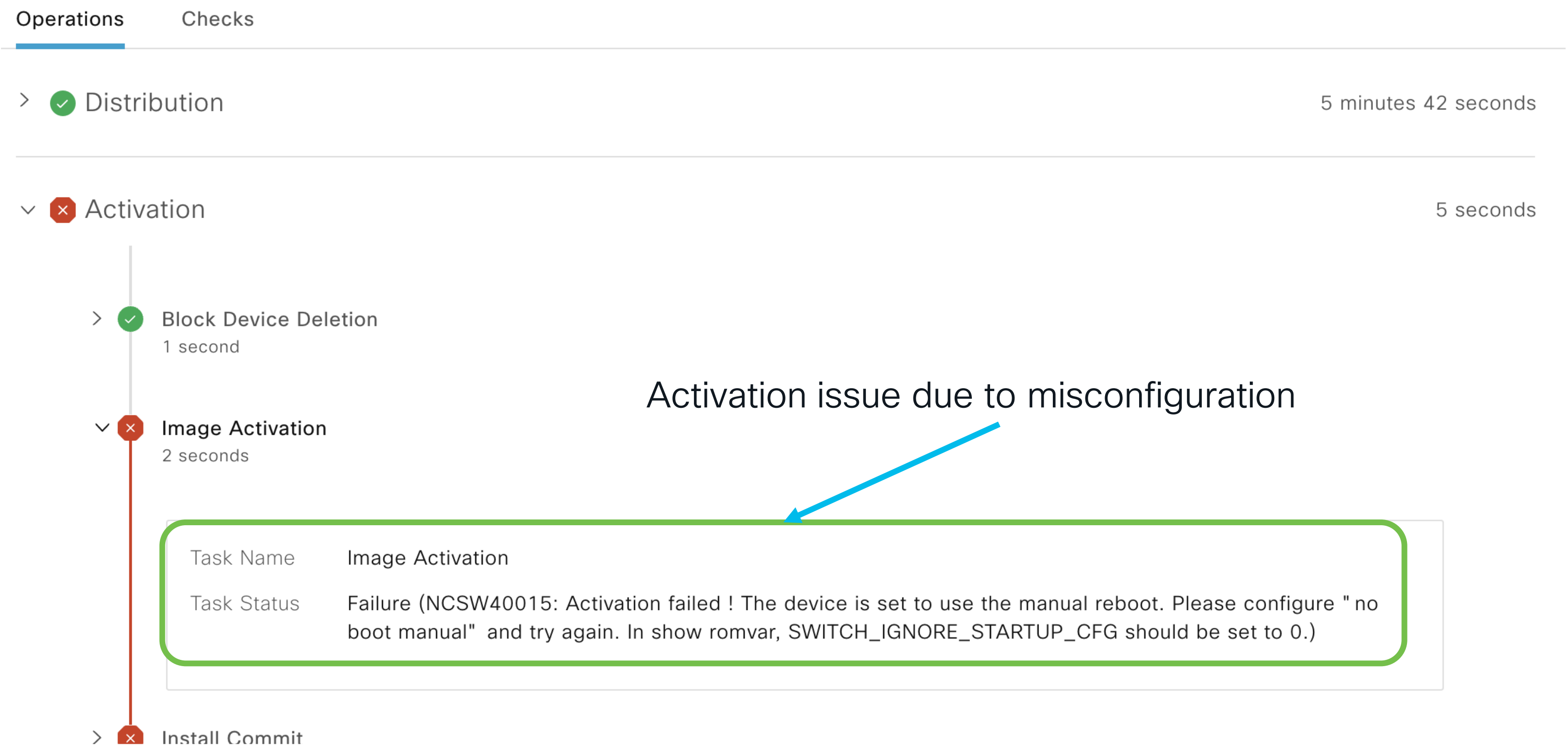
NCSW32001: Distribution failed using protocol: SCP. Distribution of image: c3750e-universalk9-tar.152-4.E10.tar on device. with protocol: SCP . Failed! Distribution of image: c3750e-universalk9-tar.152-4.E10.tar on device. with protocol: SCP . Flash Validation successfully completed. No Sufficient free space in flash1: Required Free space is 38400000 Available Free space is 35003904 Please select EraseFlash and EraseRunningImage options and try aganin.

- ✓ Image Integrity Verification(KGV) — 1 second
- ✓ Pre Distribution Operation — 1 second
- ✕ Distribution — 4 minutes 38 seconds
- ⊖ Post Distribution Operation
- ⊖ Image Checksum Verification On Device
- ⊖ Distribution Completed

Distribution issue due to insufficient space in flash

Common SWIM Issues – Distribution + Activation

Inventory (Software Image Focus) – Enhanced Visibility into the steps performed



✓ Distribution 5 minutes 42 seconds

✕ Activation 5 seconds

✓ Block Device Deletion
1 second

✕ Image Activation
2 seconds

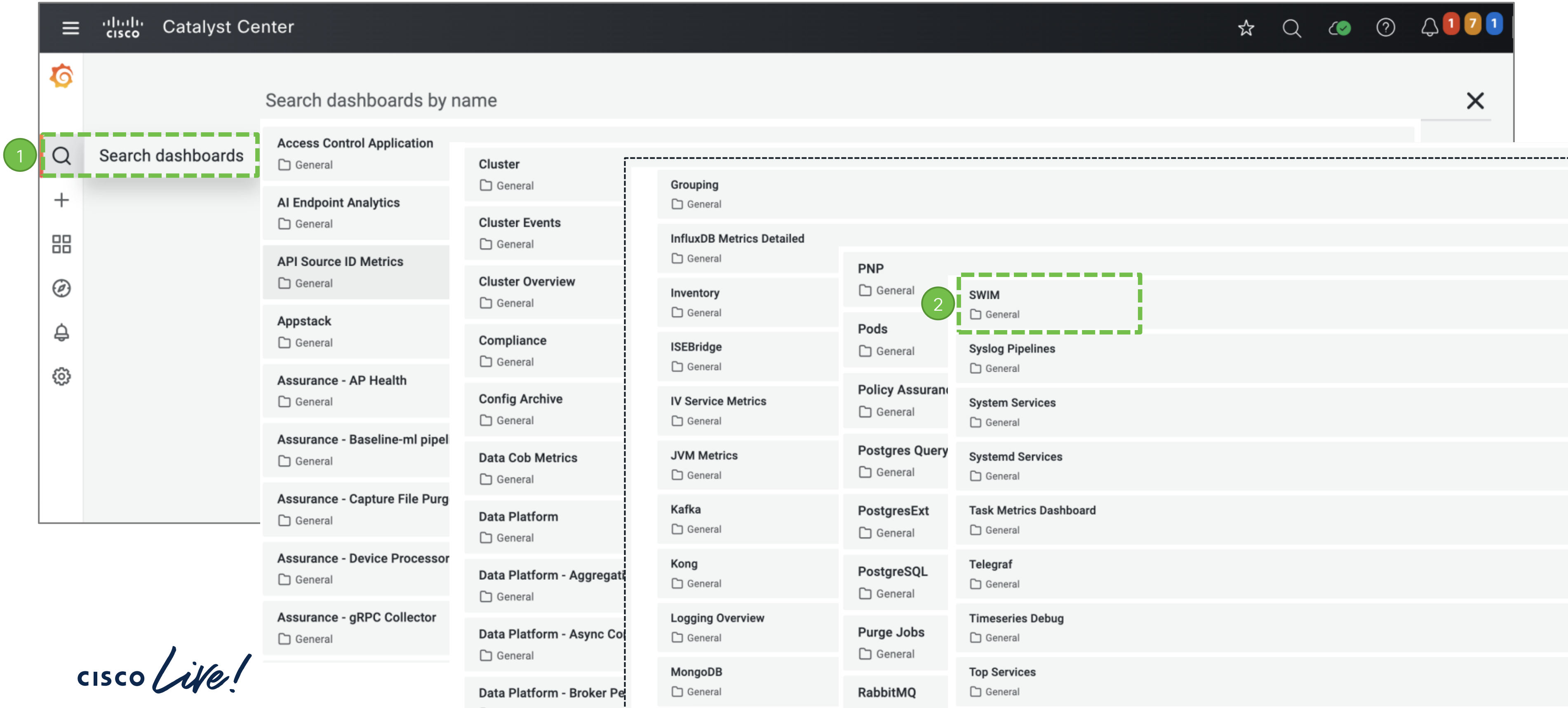
Task Name Image Activation

Task Status Failure (NCSW40015: Activation failed ! The device is set to use the manual reboot. Please configure " no boot manual" and try again. In show romvar, SWITCH_IGNORE_STARTUP_CFG should be set to 0.)

✕ Install Commit

Activation issue due to misconfiguration

SWIM: Database Insights (Grafana)



Search dashboards

Search dashboards by name

Access Control Application
General

AI Endpoint Analytics
General

API Source ID Metrics
General

Appstack
General

Assurance - AP Health
General

Assurance - Baseline-ml pipel
General

Assurance - Capture File Purg
General

Assurance - Device Processor
General

Assurance - gRPC Collector
General

Cluster
General

Cluster Events
General

Cluster Overview
General

Compliance
General

Config Archive
General

Data Cob Metrics
General

Data Platform
General

Data Platform - Aggregati
General

Data Platform - Async Co
General

Data Platform - Broker Pe

Grouping
General

InfluxDB Metrics Detailed
General

Inventory
General

ISEBridge
General

IV Service Metrics
General

JVM Metrics
General

Kafka
General

Kong
General

Logging Overview
General

MongoDB
General

PNP
General

Pods
General

Policy Assuran
General

Postgres Query
General

PostgresExt
General

PostgreSQL
General

Purge Jobs
General

RabbitMQ

SWIM
General

Syslog Pipelines
General

System Services
General

Systemd Services
General

Task Metrics Dashboard
General

Telegraf
General

Timeseries Debug
General

Top Services
General

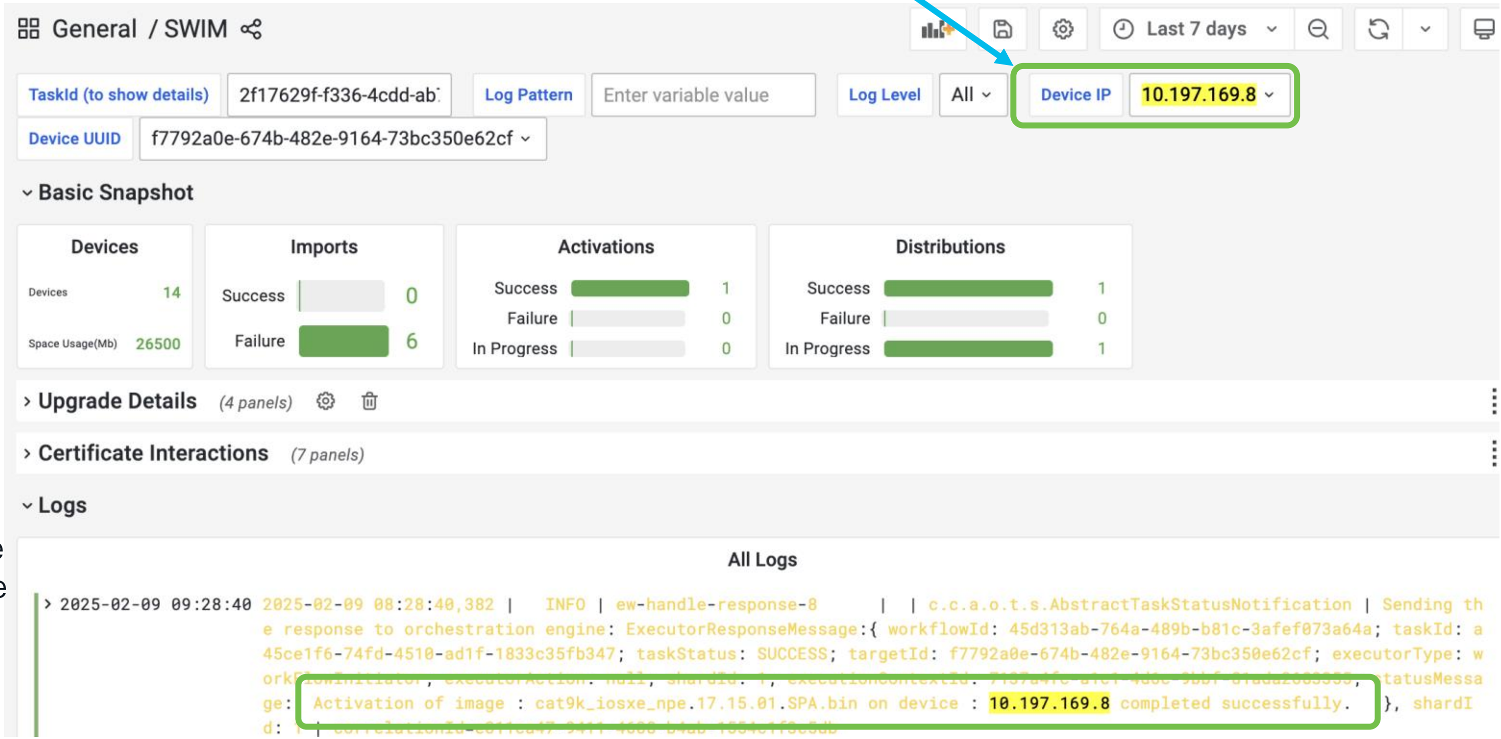
Common SWIM Issues – Distribution + Activation

SWIM Grafana Dashboard with Key Logs from Kibana

Select Device

Summary for all devices in the timestamp selected

‘Logs’ to view Service logs filtered for device



General / SWIM

Last 7 days

TaskId (to show details): 2f17629f-f336-4cdd-ab

Log Pattern: Enter variable value

Log Level: All

Device IP: 10.197.169.8

Device UUID: f7792a0e-674b-482e-9164-73bc350e62cf

Basic Snapshot

Devices	
Devices	14
Space Usage(Mb)	26500

Imports	
Success	0
Failure	6

Activations	
Success	1
Failure	0
In Progress	0

Distributions	
Success	1
Failure	0
In Progress	1

Upgrade Details (4 panels)

Certificate Interactions (7 panels)

Logs

All Logs

```
> 2025-02-09 09:28:40 2025-02-09 08:28:40,382 |   INFO | ew-handle-response-8      |  | c.c.a.o.t.s.AbstractTaskStatusNotification | Sending th
                      e response to orchestration engine: ExecutorResponseMessage:{ workflowId: 45d313ab-764a-489b-b81c-3afef073a64a; taskId: a
                      45ce1f6-74fd-4510-ad1f-1833c35fb347; taskStatus: SUCCESS; targetId: f7792a0e-674b-482e-9164-73bc350e62cf; executorType: w
                      orkFlowInitiator; executorAction: null; shardId: 1; executionContextId: [illegible]; statusMessa
                      ge: Activation of image : cat9k_iosxe_npe.17.15.01.SPA.bin on device : 10.197.169.8 completed successfully. }, shardI
                      d: 1 | correlationId=[illegible]
```

Catalyst Center Assurance Troubleshooting

Assurance an End-to-End Visibility and Insights

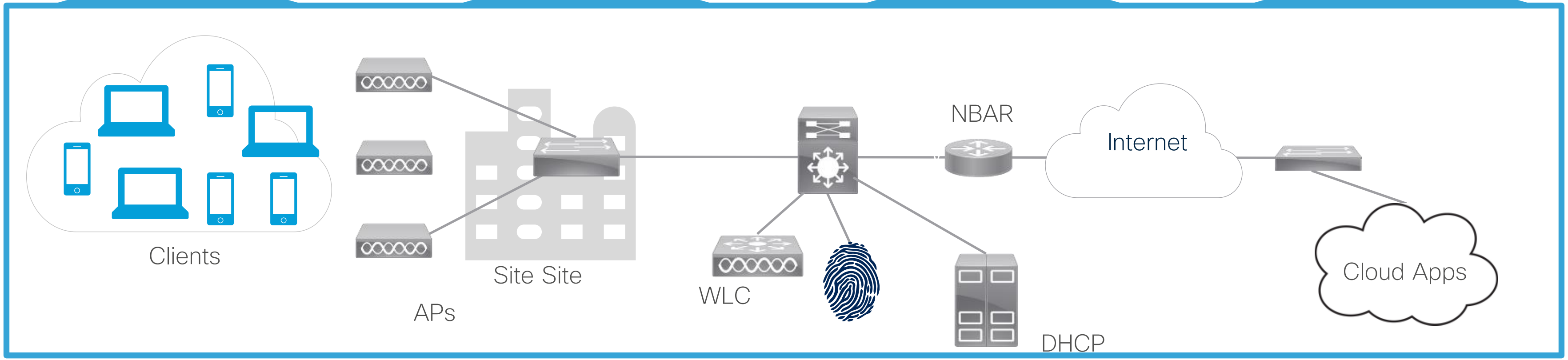
2.2.3

End user Client health and visibility

Network & Services health

Application visibility and performance

SD-Access health and status

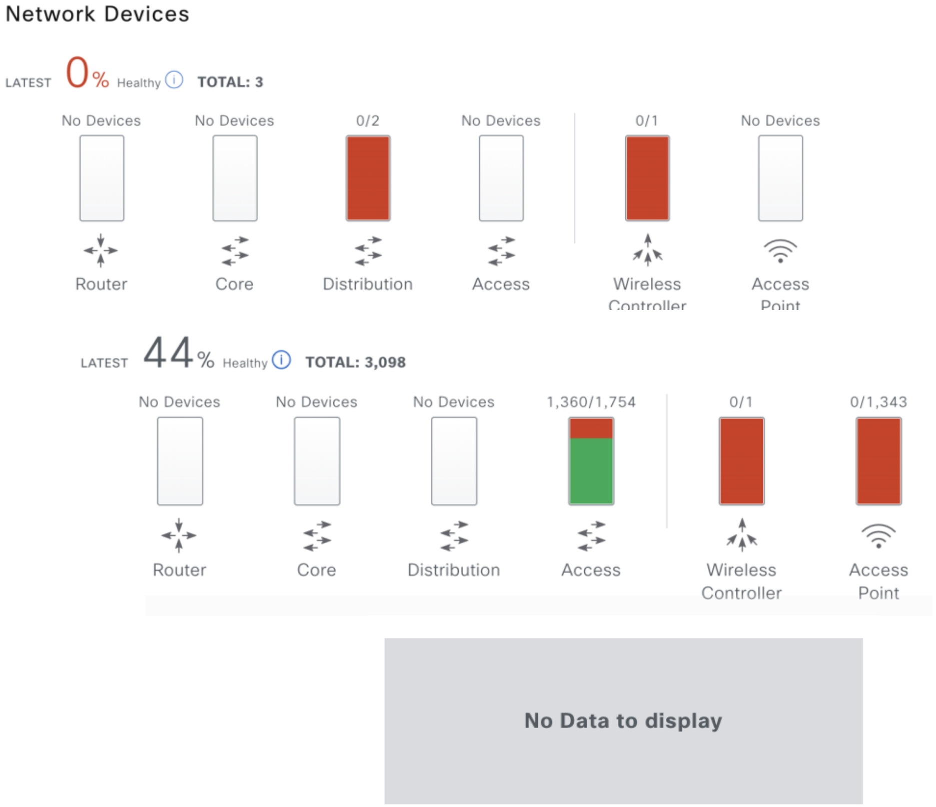


Assurance – Top issues

No Device Health Score

Low Device Health Score

No Application Health



Network Devices

LATEST 0% Healthy ⓘ TOTAL: 3

No Devices	No Devices	0/2	No Devices	0/1	No Devices
Router	Core	Distribution	Access	Wireless Controller	Access Point

LATEST 44% Healthy ⓘ TOTAL: 3,098

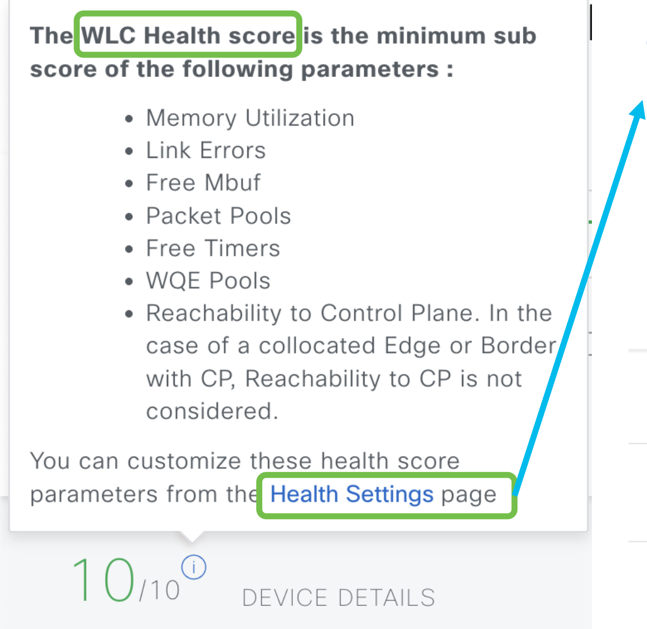
No Devices	No Devices	No Devices	1,360/1,754	0/1	0/1,343
Router	Core	Distribution	Access	Wireless Controller	Access Point

No Data to display

Network / Device 360

Health Score - WLC

Assurance / Settings / Health Score Settings

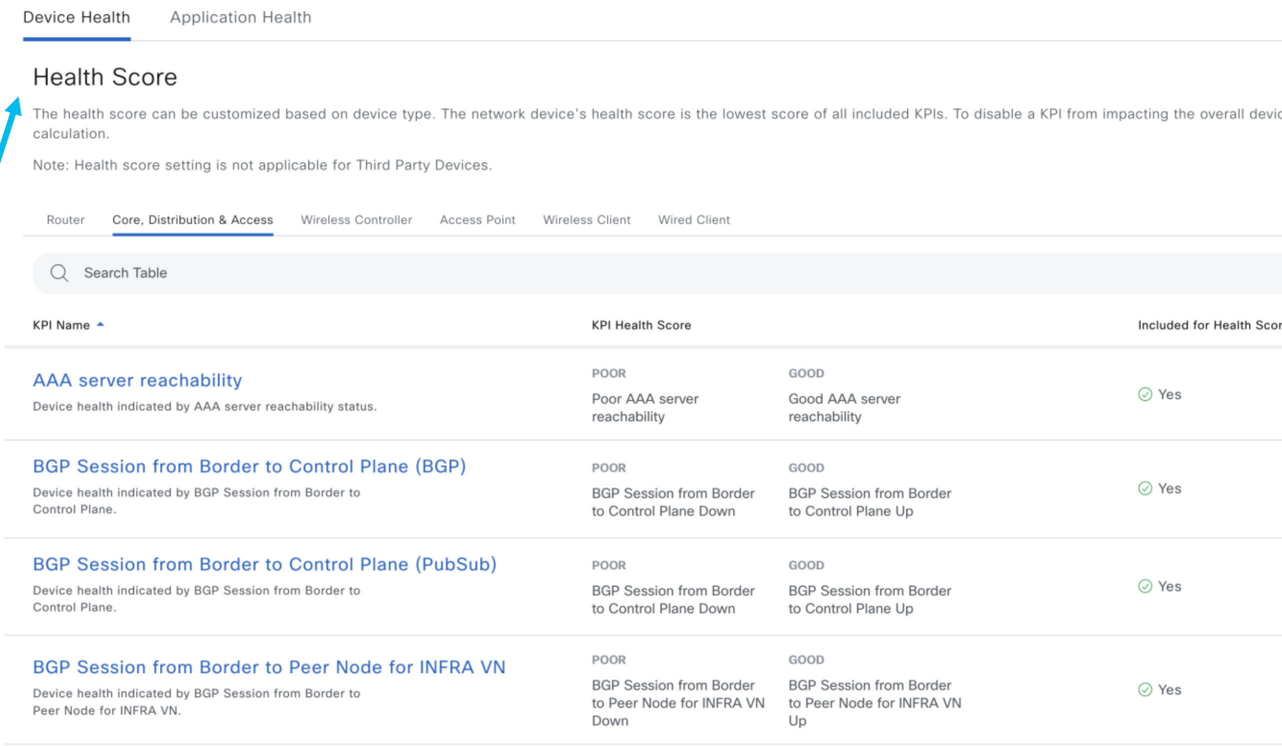


The WLC Health score is the minimum sub score of the following parameters :

- Memory Utilization
- Link Errors
- Free Mbuf
- Packet Pools
- Free Timers
- WQE Pools
- Reachability to Control Plane. In the case of a collocated Edge or Border with CP, Reachability to CP is not considered.

You can customize these health score parameters from the Health Settings page

10/10 DEVICE DETAILS



Health Score

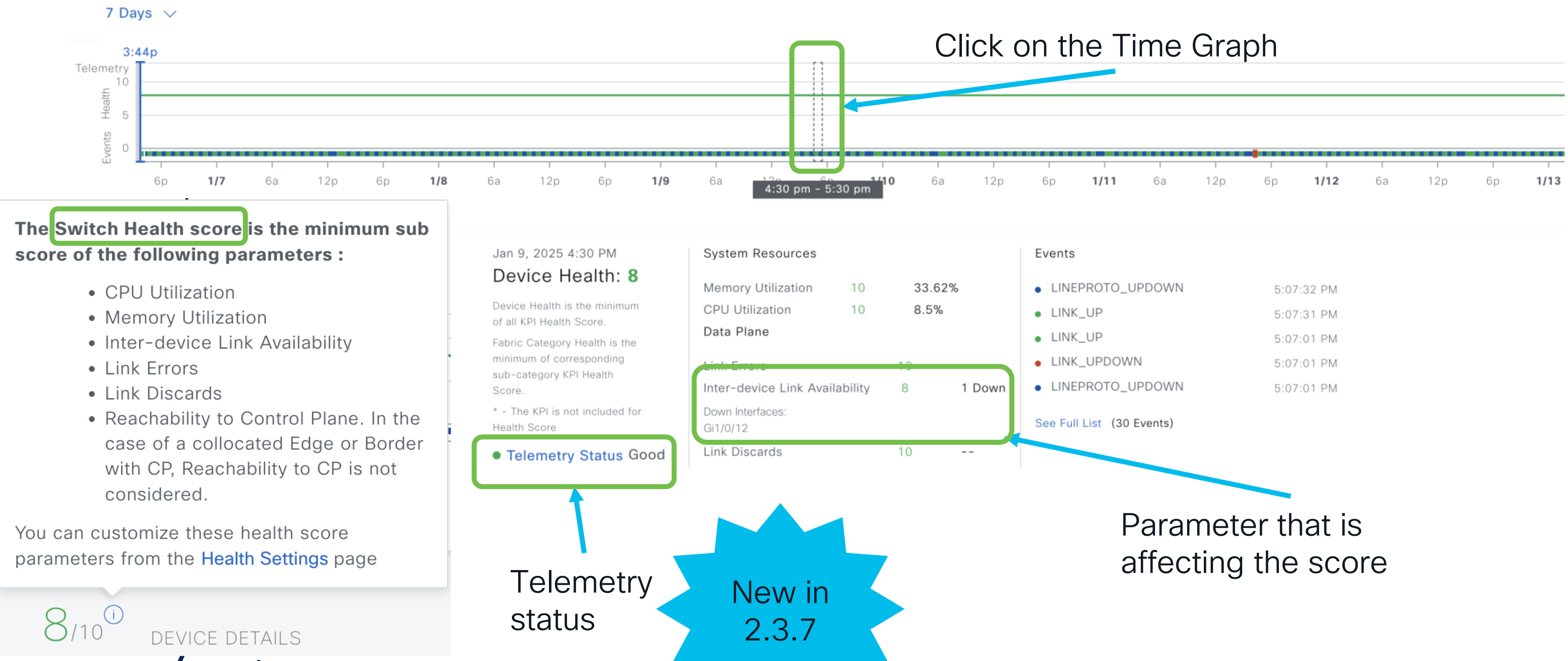
The health score can be customized based on device type. The network device's health score is the lowest score of all included KPIs. To disable a KPI from impacting the overall devic calculation.

Note: Health score setting is not applicable for Third Party Devices.

KPI Name	KPI Health Score		Included for Health Scor
AAA server reachability Device health indicated by AAA server reachability status.	POOR Poor AAA server reachability	GOOD Good AAA server reachability	✓ Yes
BGP Session from Border to Control Plane (BGP) Device health indicated by BGP Session from Border to Control Plane.	POOR BGP Session from Border to Control Plane Down	GOOD BGP Session from Border to Control Plane Up	✓ Yes
BGP Session from Border to Control Plane (PubSub) Device health indicated by BGP Session from Border to Control Plane.	POOR BGP Session from Border to Control Plane Down	GOOD BGP Session from Border to Control Plane Up	✓ Yes
BGP Session from Border to Peer Node for INFRA VN Device health indicated by BGP Session from Border to Peer Node for INFRA VN.	POOR BGP Session from Border to Peer Node for INFRA VN Down	GOOD BGP Session from Border to Peer Node for INFRA VN Up	✓ Yes

Network / Device 360

Health Score - Switch



Click on the Time Graph

The Switch Health score is the minimum sub score of the following parameters :

- CPU Utilization
- Memory Utilization
- Inter-device Link Availability
- Link Errors
- Link Discards
- Reachability to Control Plane. In the case of a collocated Edge or Border with CP, Reachability to CP is not considered.

You can customize these health score parameters from the Health Settings page

8/10 DEVICE DETAILS

Jan 9, 2025 4:30 PM

Device Health: 8

Device Health is the minimum of all KPI Health Score.

Fabric Category Health is the minimum of corresponding sub-category KPI Health Score.

* - The KPI is not included for Health Score

● Telemetry Status Good

System Resources

Memory Utilization	10	33.62%
CPU Utilization	10	8.5%
Data Plane		
Link Errors	10	
Inter-device Link Availability	8	1 Down
Down Interfaces: Gi1/0/12		
Link Discards	10	--

Events

● LINEPROTO_UPDOWN	5:07:32 PM
● LINK_UP	5:07:31 PM
● LINK_UP	5:07:01 PM
● LINK_UPDOWN	5:07:01 PM
● LINEPROTO_UPDOWN	5:07:01 PM

See Full List (30 Events)

Telemetry status

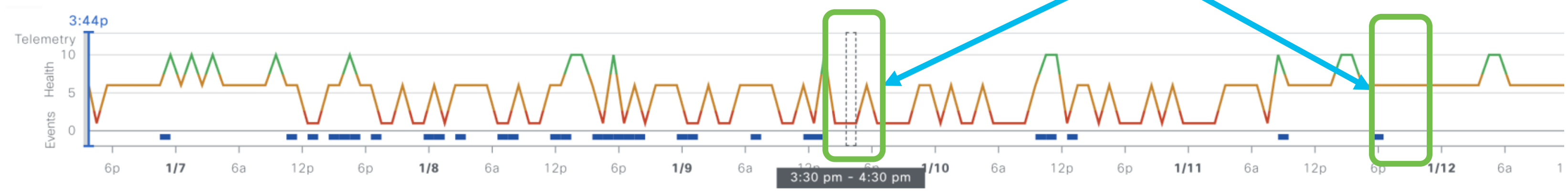
New in 2.3.7

Parameter that is affecting the score

Network / Device 360

Health Score - AP

Click on the Time Graph

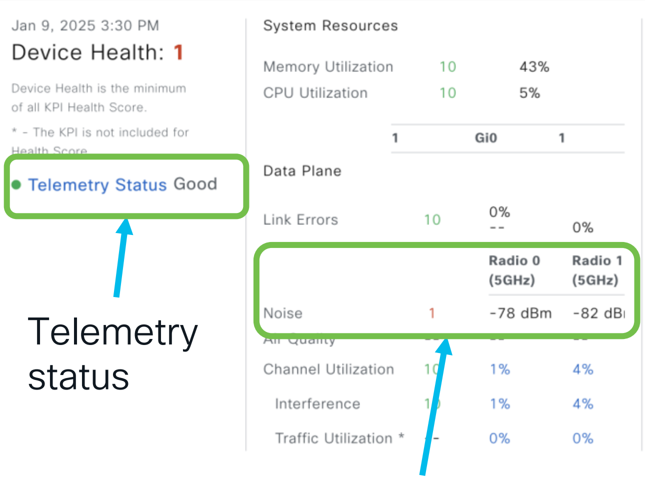


The AP Health score is the minimum sub score of the following parameters:

- CPU Utilization
- Memory Utilization
- Air Quality
- Interference
- Noise
- Radio Utilization
- Link Errors

You can customize these health score parameters from the Health Settings page

6/10 ⓘ DEVICE DETAILS



Jan 9, 2025 3:30 PM

Device Health: 1

Device Health is the minimum of all KPI Health Score.

* - The KPI is not included for Health Score

● Telemetry Status Good

System Resources

Memory Utilization	10	43%
CPU Utilization	10	5%

1	Gi0	1

Data Plane

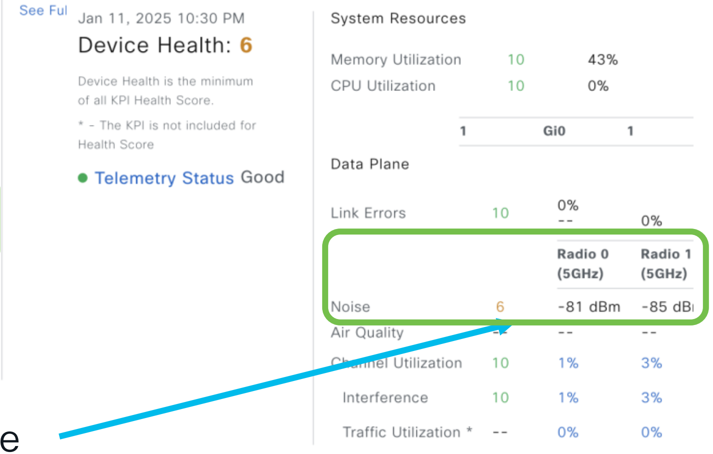
Link Errors	10	0% --	0%

		Radio 0 (5GHz)	Radio 1 (5GHz)
Noise	1	-78 dBm	-82 dBı
Air Quality	--	--	--
Channel Utilization	10	1%	4%
Interference	10	1%	4%
Traffic Utilization *	--	0%	0%

Events

See Ful

Telemetry status



Jan 11, 2025 10:30 PM

Device Health: 6

Device Health is the minimum of all KPI Health Score.

* - The KPI is not included for Health Score

● Telemetry Status Good

System Resources

Memory Utilization	10	43%
CPU Utilization	10	0%

1	Gi0	1

Data Plane

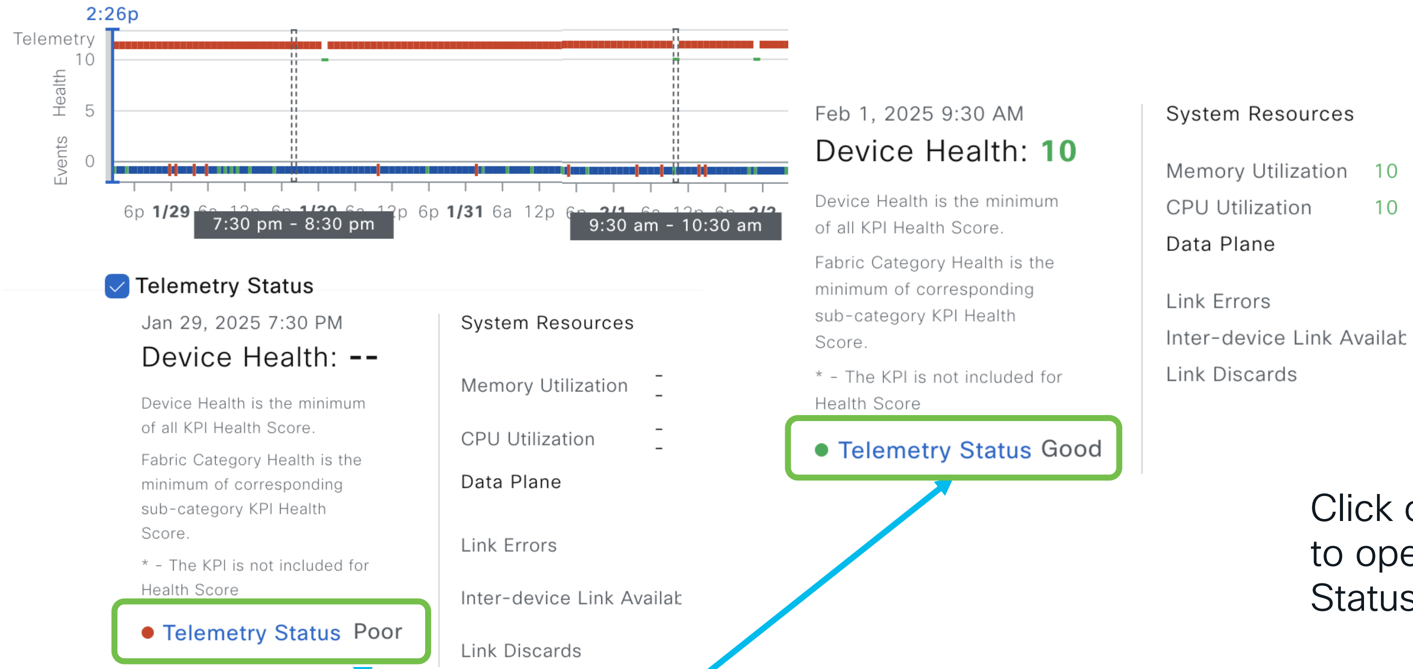
Link Errors	10	0% --	0%

		Radio 0 (5GHz)	Radio 1 (5GHz)
Noise	6	-81 dBm	-85 dBı
Air Quality	--	--	--
Channel Utilization	10	1%	3%
Interference	10	1%	3%
Traffic Utilization *	--	0%	0%

Parameter causing low score

Release 2.3.7.x onwards

Health Score – Telemetry Status


2:26p
Telemetry
Health
Events
10
5
0
6p 1/29 6a 12p 6p 1/30 6a 12p 6p 1/31 6a 12p 6p 2/1 6a 12p 6p 2/2
7:30 pm - 8:30 pm
9:30 am - 10:30 am

☑ Telemetry Status

Jan 29, 2025 7:30 PM

Device Health: --

Device Health is the minimum of all KPI Health Score.

Fabric Category Health is the minimum of corresponding sub-category KPI Health Score.

* - The KPI is not included for Health Score

● Telemetry Status Poor

System Resources

Memory Utilization --

CPU Utilization --

Data Plane

Link Errors

Inter-device Link Availat

Link Discards

Feb 1, 2025 9:30 AM

Device Health: 10

Device Health is the minimum of all KPI Health Score.

Fabric Category Health is the minimum of corresponding sub-category KPI Health Score.

* - The KPI is not included for Health Score

● Telemetry Status Good

System Resources

Memory Utilization 10

CPU Utilization 10

Data Plane

Link Errors

Inter-device Link Availat

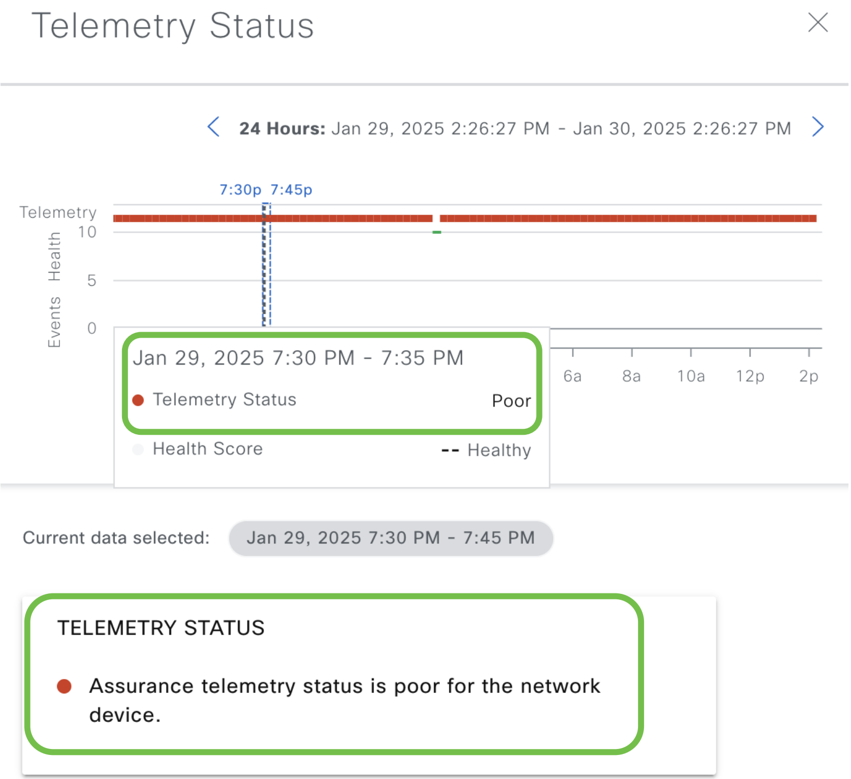
Link Discards

Telemetry status

Click on ‘Telemetry status’ to open the new Telemetry Status Dashboard

Release 2.3.7.x onwards

Health Score – Telemetry Status



Telemetry Status

24 Hours: Jan 29, 2025 2:26:27 PM - Jan 30, 2025 2:26:27 PM

Jan 29, 2025 7:30 PM - 7:35 PM

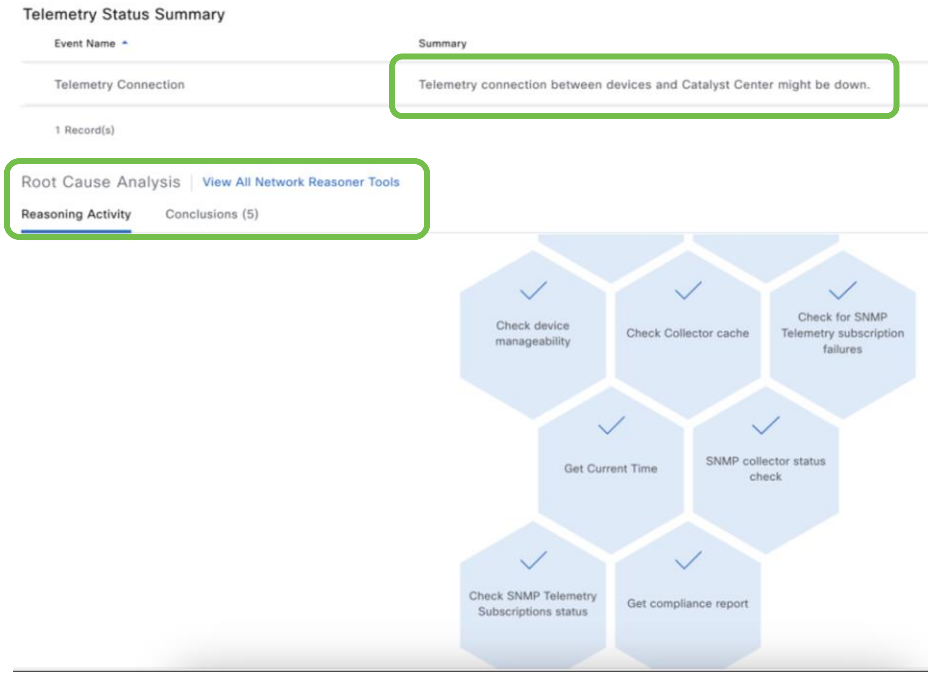
● Telemetry Status Poor

Health Score -- Healthy

Current data selected: Jan 29, 2025 7:30 PM - 7:45 PM

TELEMETRY STATUS

● Assurance telemetry status is poor for the network device.



Telemetry Status Summary

Event Name	Summary
Telemetry Connection	Telemetry connection between devices and Catalyst Center might be down.

1 Record(s)

Root Cause Analysis | View All Network Reasoner Tools

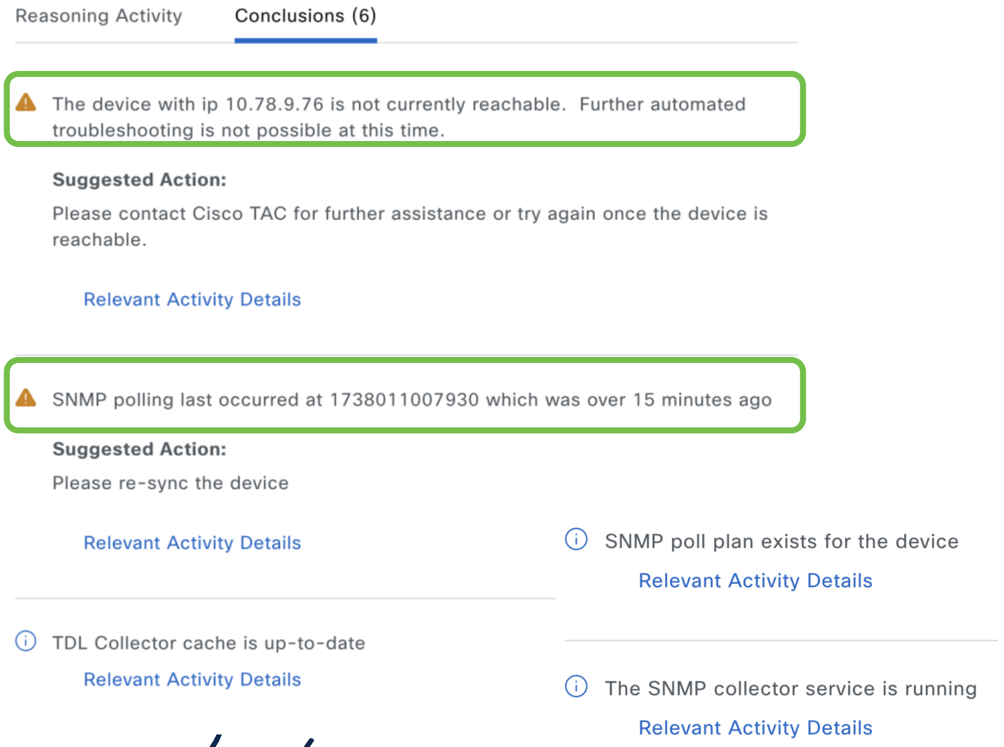
Reasoning Activity   Conclusions (5)

Check device manageability
Check Collector cache
Check for SNMP Telemetry subscription failures
Get Current Time
SNMP collector status check
Check SNMP Telemetry Subscriptions status
Get compliance report

Release 2.3.7.x onwards

Health Score – Telemetry Status

Telemetry Status Dashboard (continued)



Reasoning Activity | Conclusions (6)

⚠ The device with ip 10.78.9.76 is not currently reachable. Further automated troubleshooting is not possible at this time.

Suggested Action:

Please contact Cisco TAC for further assistance or try again once the device is reachable.

Relevant Activity Details

⚠ SNMP polling last occurred at 1738011007930 which was over 15 minutes ago

Suggested Action:

Please re-sync the device

Relevant Activity Details

ⓘ TDL Collector cache is up-to-date

Relevant Activity Details

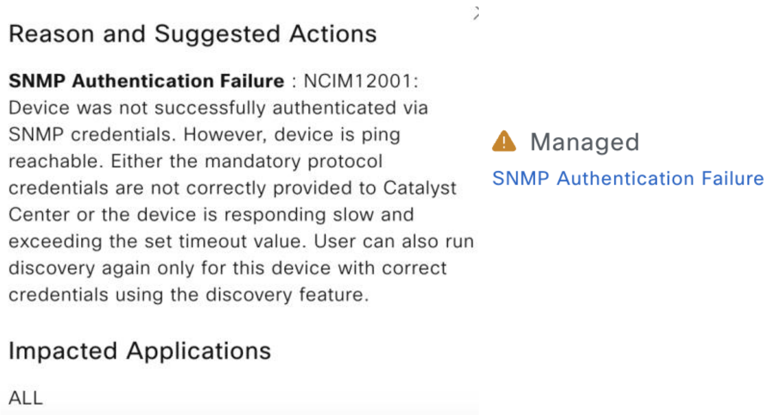
ⓘ SNMP poll plan exists for the device

Relevant Activity Details

ⓘ The SNMP collector service is running

Relevant Activity Details

Inventory Dashboard



Reason and Suggested Actions

SNMP Authentication Failure : NCIM12001: Device was not successfully authenticated via SNMP credentials. However, device is ping reachable. Either the mandatory protocol credentials are not correctly provided to Catalyst Center or the device is responding slow and exceeding the set timeout value. User can also run discovery again only for this device with correct credentials using the discovery feature.

Impacted Applications

ALL

⚠ Managed

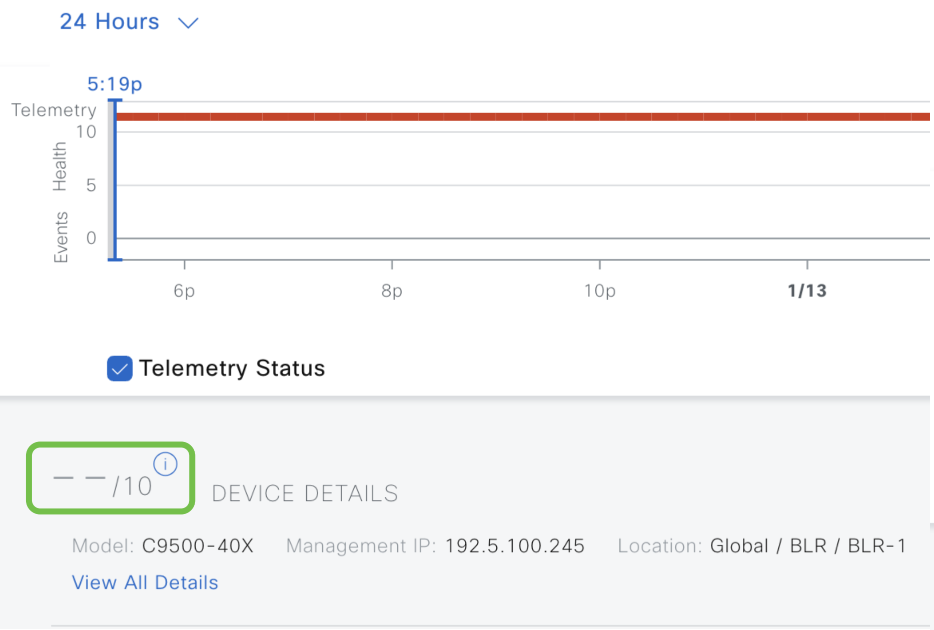
SNMP Authentication Failure

- If the “Telemetry Status” is not good, checks are executed every 6 hours
- Checks executed for switches, routers and WLCs

Network / Device 360

Health Score – Blank or No Score

Switch BLR-Border.cisco.com View Device Details



☑ Telemetry Status

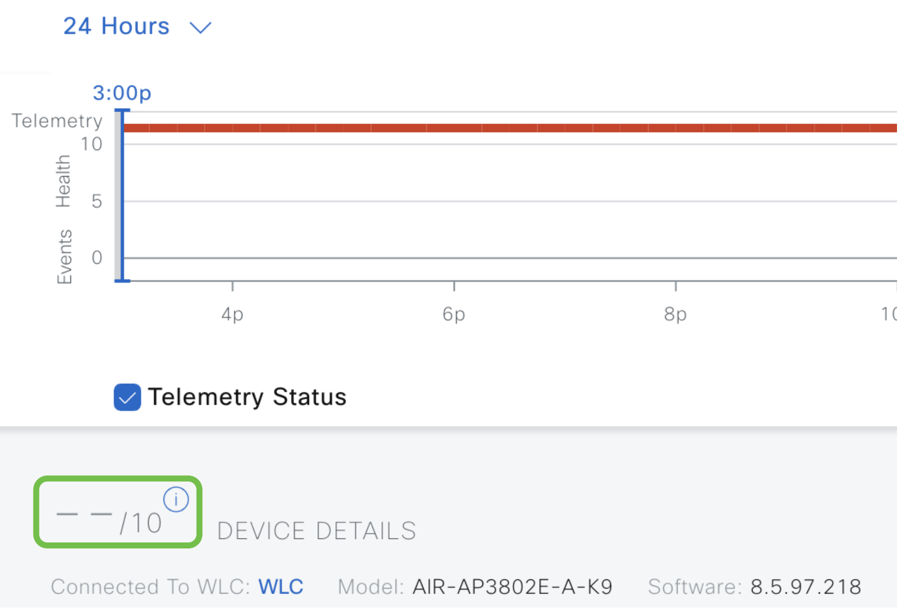
-- /10

DEVICE DETAILS

Model: C9500-40X Management IP: 192.5.100.245 Location: Global / BLR / BLR-1

View All Details

AP ewlc-ap-211-858 View Device Details



☑ Telemetry Status

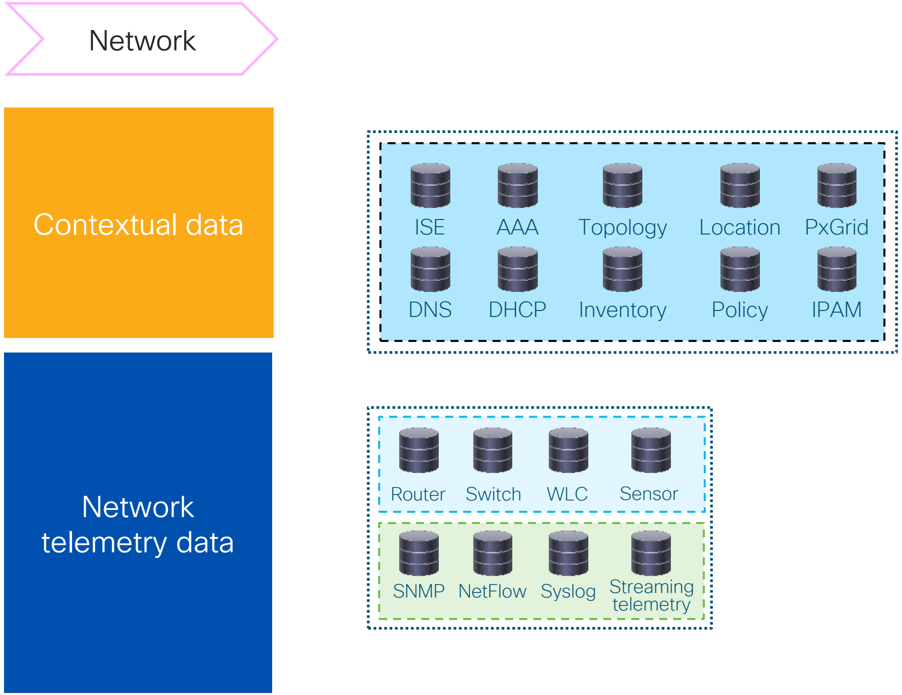
-- /10

DEVICE DETAILS

Connected To WLC: WLC Model: AIR-AP3802E-A-K9 Software: 8.5.97.218

cisco Live!

Assurance System Flow



Network

Contextual data

ISE
AAA
Topology
Location
PxGrid
DNS
DHCP
Inventory
Policy
IPAM

Network telemetry data

Router
Switch
WLC
Sensor
SNMP
NetFlow
Syslog
Streaming telemetry

Assurance Settings & States on the Catalyst Center

Device Specific

Choose Provision > Inventory

- Manageability State should be Managed
- Reachability State should be Reachable
- Device should be assigned to a site
- For Application Health – From Actions menu, choose Telemetry, click ‘Enable Application Telemetry’

Affects Multiple Devices

Choose Design > Network Settings > Telemetry

- Ensure Catalyst Center is set for SNMP trap server, Syslog server & Netflow collector server
- For Assurance from Wired clients, ensure “Cisco Catalyst Center Wired Endpoint Data Collection At This Site” is enabled
- For Wireless Assurance, ensure “Wireless Telemetry” is enabled

Release 2.3.3.x onwards

Device Checks

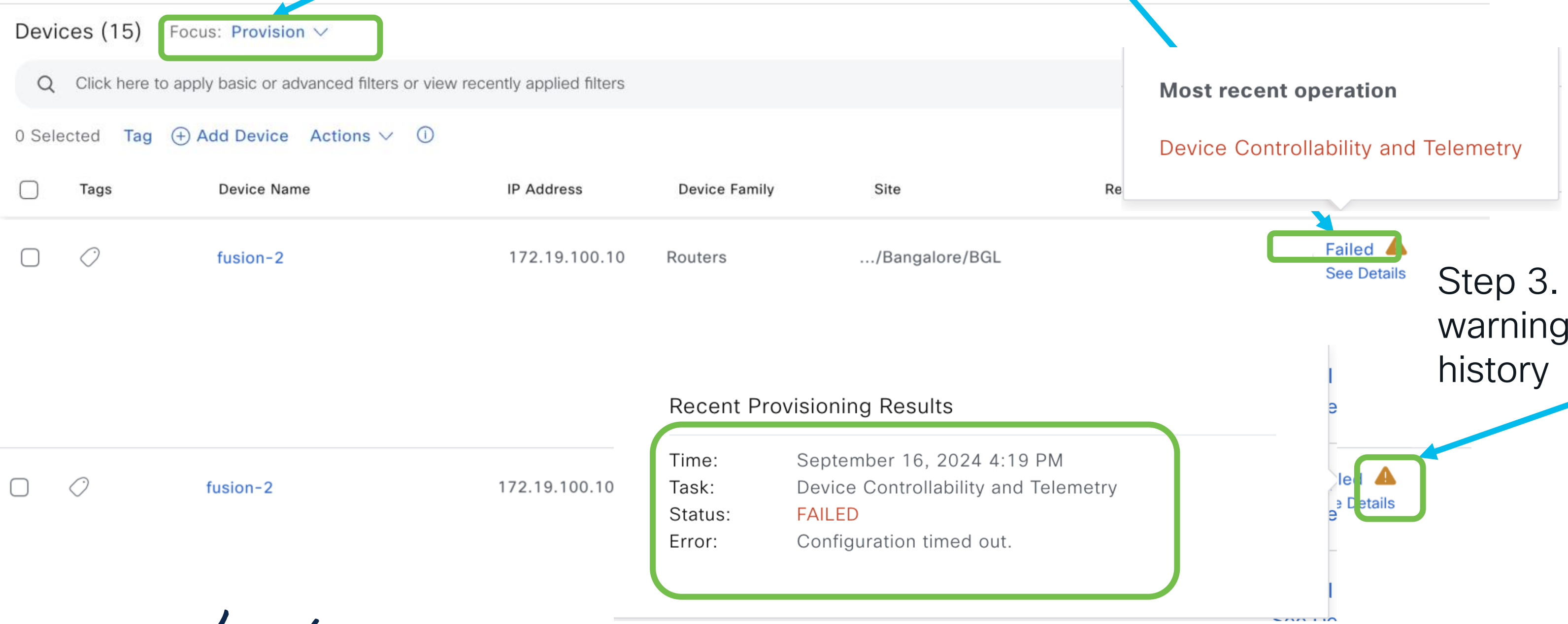
Configurations and Certificates

Verify Catalyst Center has provisioned the necessary configurations successfully from Inventory page

Step 1. Change focus to 'Provision'

Step 2. Hover over the Success / Failed

Step 3. Hover over the warning to see a history



Most recent operation

Device Controllability and Telemetry

Recent Provisioning Results

Time: September 16, 2024 4:19 PM
Task: Device Controllability and Telemetry
Status: FAILED
Error: Configuration timed out.

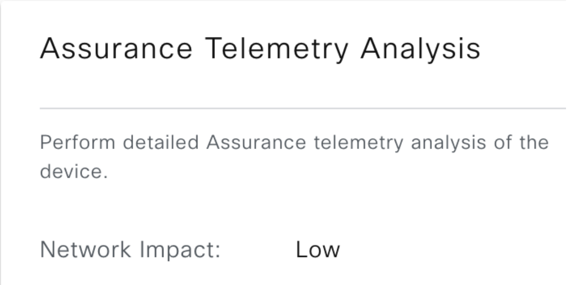
Device Checks

Verification Routines using the Network Reasoner

Release 2.3.5.x onwards

A sequence of network machine reasoning steps that verify various Assurance configurations and settings on the network and the Catalyst Center.

Step 1. Select Assurance Telemetry Analysis from Tools → Network Reasoner

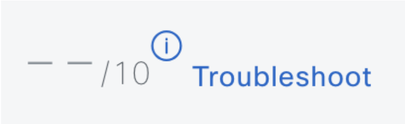


Assurance Telemetry Analysis

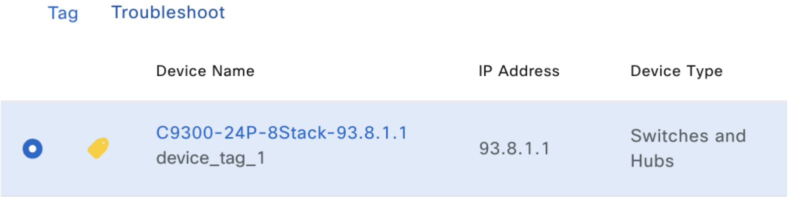
Perform detailed Assurance telemetry analysis of the device.

Network Impact: Low

New Launch point in 2.3.7.x from Assurance -> Network -> Device 360



Step 2. Choose one device & click on Troubleshoot



		Device Name	IP Address	Device Type
●	🏷	C9300-24P-8Stack-93.8.1.1 device_tag_1	93.8.1.1	Switches and Hubs

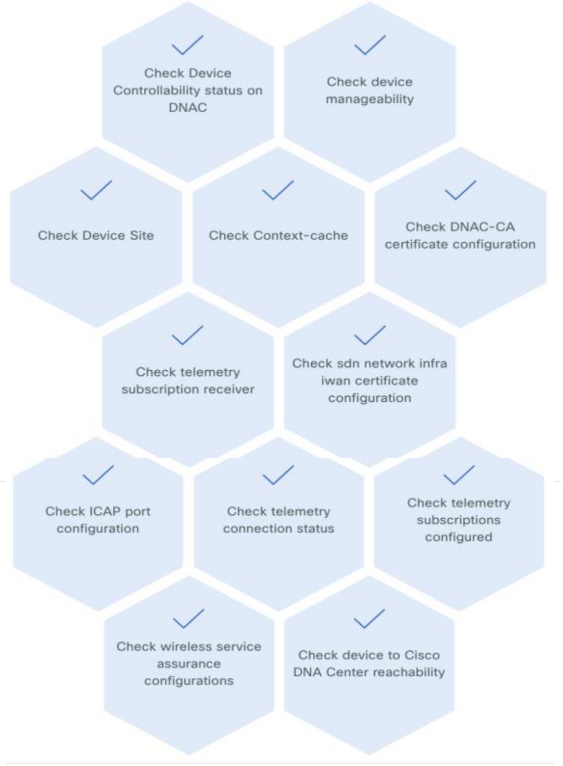
Device Checks

Verification Routines using the Network Reasoner

Release 2.3.5.x onwards

Example 1. Sample output for a Catalyst switch

2.3.5



✓ Check Device Controllability status on DNAC

✓ Check device manageability

✓ Check Device Site

✓ Check Context-cache

✓ Check DNAC-CA certificate configuration

✓ Check telemetry subscription receiver

✓ Check sdn network infra iwan certificate configuration

✓ Check ICAP port configuration

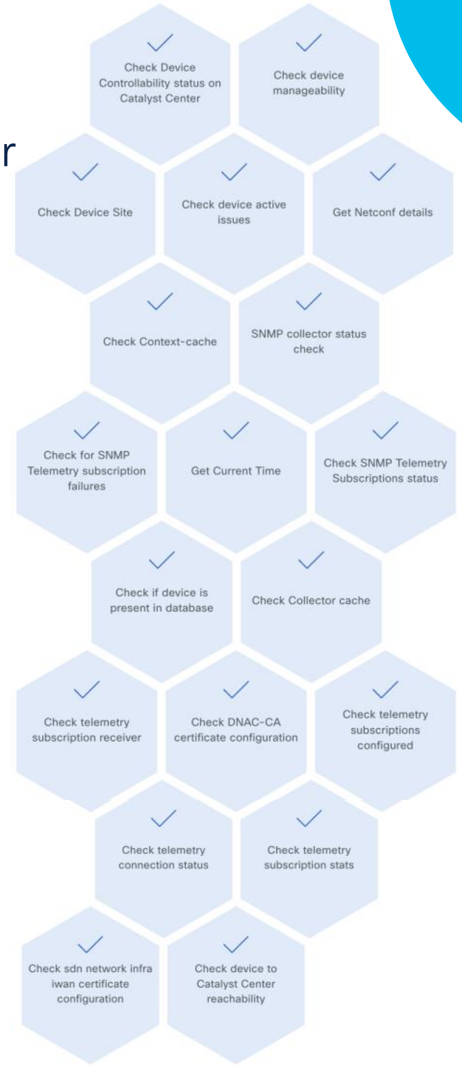
✓ Check telemetry connection status

✓ Check telemetry subscriptions configured

✓ Check wireless service assurance configurations

✓ Check device to Cisco DNA Center reachability

2.3.7



✓ Check Device Controllability status on Catalyst Center

✓ Check device manageability

✓ Check Device Site

✓ Check device active issues

✓ Get Netconf details

✓ Check Context-cache

✓ SNMP collector status check

✓ Check for SNMP Telemetry subscription failures

✓ Get Current Time

✓ Check SNMP Telemetry Subscriptions status

✓ Check if device is present in database

✓ Check Collector cache

✓ Check telemetry subscription receiver

✓ Check DNAC-CA certificate configuration

✓ Check telemetry subscriptions configured

✓ Check telemetry connection status

✓ Check telemetry subscription stats

✓ Check sdn network infra iwan certificate configuration

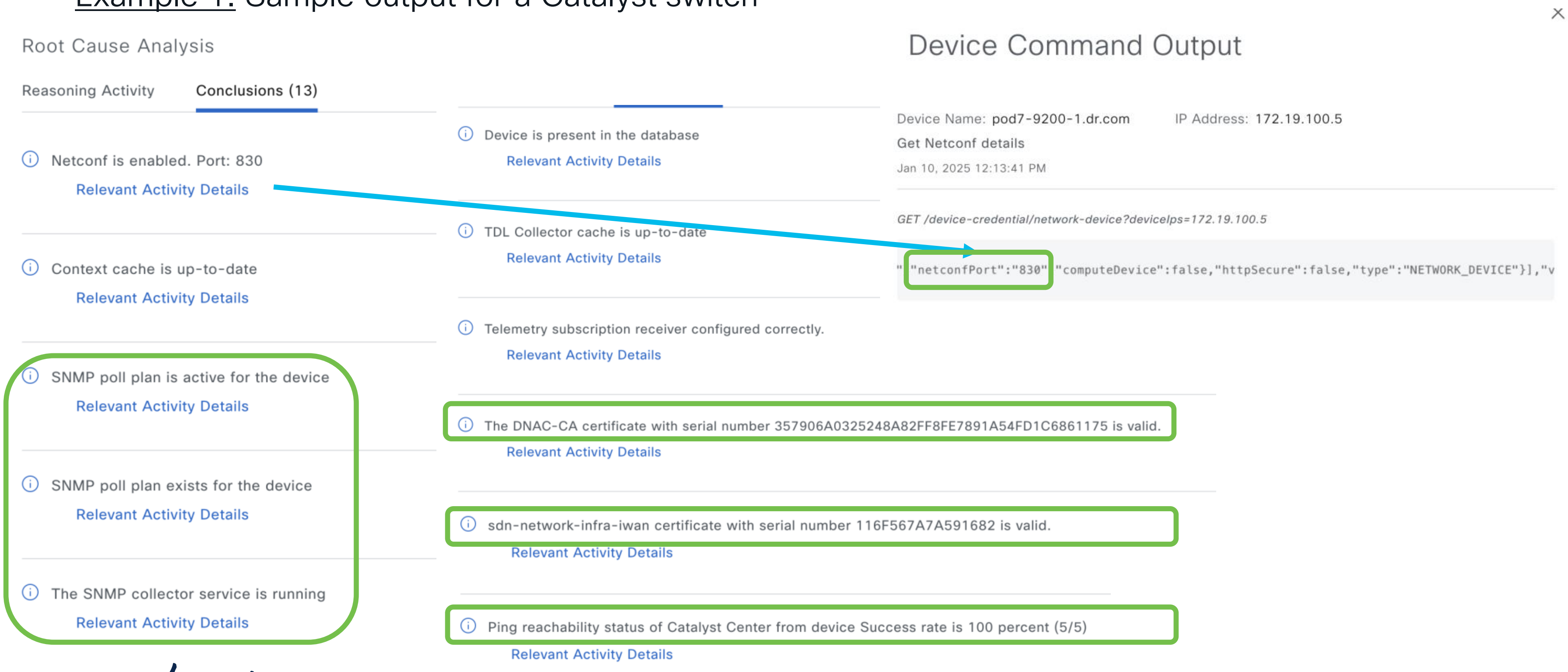
✓ Check device to Catalyst Center reachability

Release 2.3.5.x onwards

Device Checks

Verification Routines using the Network Reasoner

Example 1. Sample output for a Catalyst switch



Root Cause Analysis

Reasoning Activity | Conclusions (13)

Netconf is enabled. Port: 830
Relevant Activity Details

Context cache is up-to-date
Relevant Activity Details

SNMP poll plan is active for the device
Relevant Activity Details

SNMP poll plan exists for the device
Relevant Activity Details

The SNMP collector service is running
Relevant Activity Details

Device is present in the database
Relevant Activity Details

TDL Collector cache is up-to-date
Relevant Activity Details

Telemetry subscription receiver configured correctly.
Relevant Activity Details

The DNAC-CA certificate with serial number 357906A0325248A82FF8FE7891A54FD1C6861175 is valid.
Relevant Activity Details

sdn-network-infra-iwan certificate with serial number 116F567A7A591682 is valid.
Relevant Activity Details

Ping reachability status of Catalyst Center from device Success rate is 100 percent (5/5)
Relevant Activity Details

Device Command Output

Device Name: pod7-9200-1.dr.com   IP Address: 172.19.100.5

Get Netconf details

Jan 10, 2025 12:13:41 PM

GET /device-credential/network-device?deviceIps=172.19.100.5

```
" "netconfPort":"830" "computeDevice":false,"httpSecure":false,"type":"NETWORK_DEVICE"}],"v
```

cisco Live!

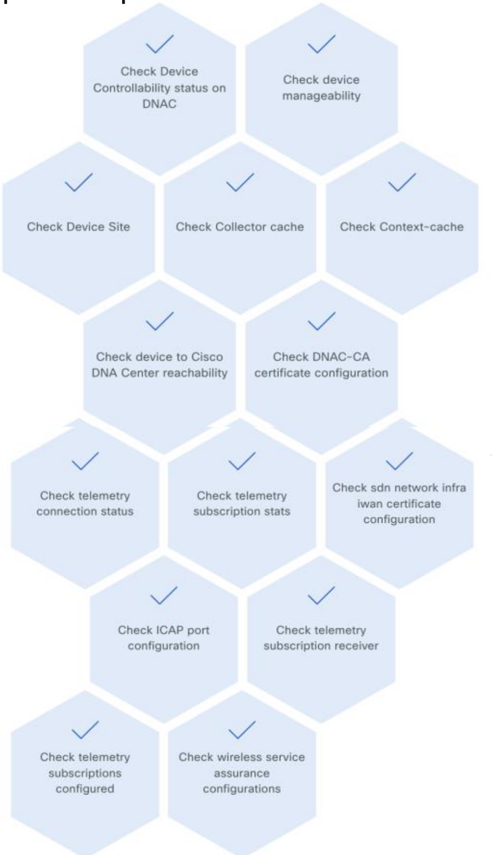
Device Checks

Verification Routines using the Network Reasoner

Example 2. Sample output for a 9800 WLC

Release 2.3.5.x onwards

2.3.5



✓ Check Device Controllability status on DNAC

✓ Check device manageability

✓ Check Device Site

✓ Check Collector cache

✓ Check Context-cache

✓ Check device to Cisco DNA Center reachability

✓ Check DNAC-CA certificate configuration

✓ Check telemetry connection status

✓ Check telemetry subscription stats

✓ Check sdn network infra iwan certificate configuration

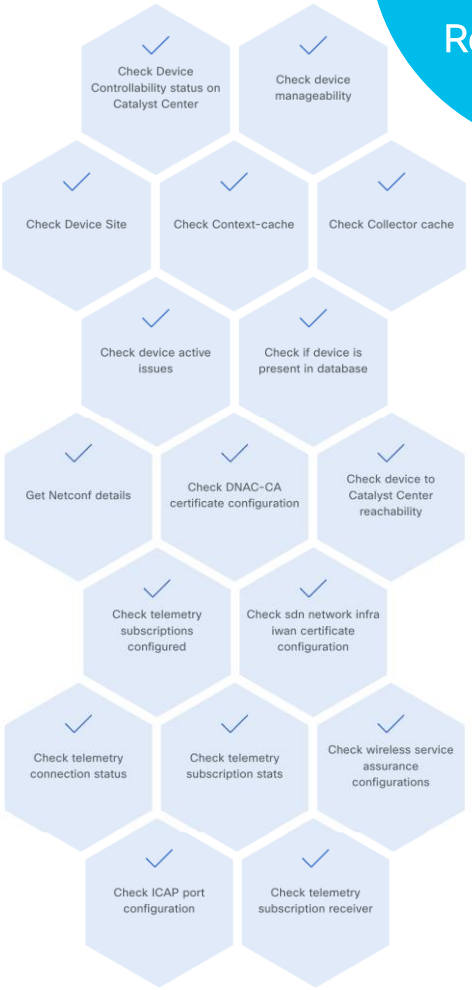
✓ Check ICAP port configuration

✓ Check telemetry subscription receiver

✓ Check telemetry subscriptions configured

✓ Check wireless service assurance configurations

2.3.7



✓ Check Device Controllability status on Catalyst Center

✓ Check device manageability

✓ Check Device Site

✓ Check Context-cache

✓ Check Collector cache

✓ Check device active issues

✓ Check if device is present in database

✓ Get Netconf details

✓ Check DNAC-CA certificate configuration

✓ Check device to Catalyst Center reachability

✓ Check telemetry subscriptions configured

✓ Check sdn network infra iwan certificate configuration

✓ Check telemetry connection status

✓ Check telemetry subscription stats

✓ Check wireless service assurance configurations

✓ Check ICAP port configuration

✓ Check telemetry subscription receiver

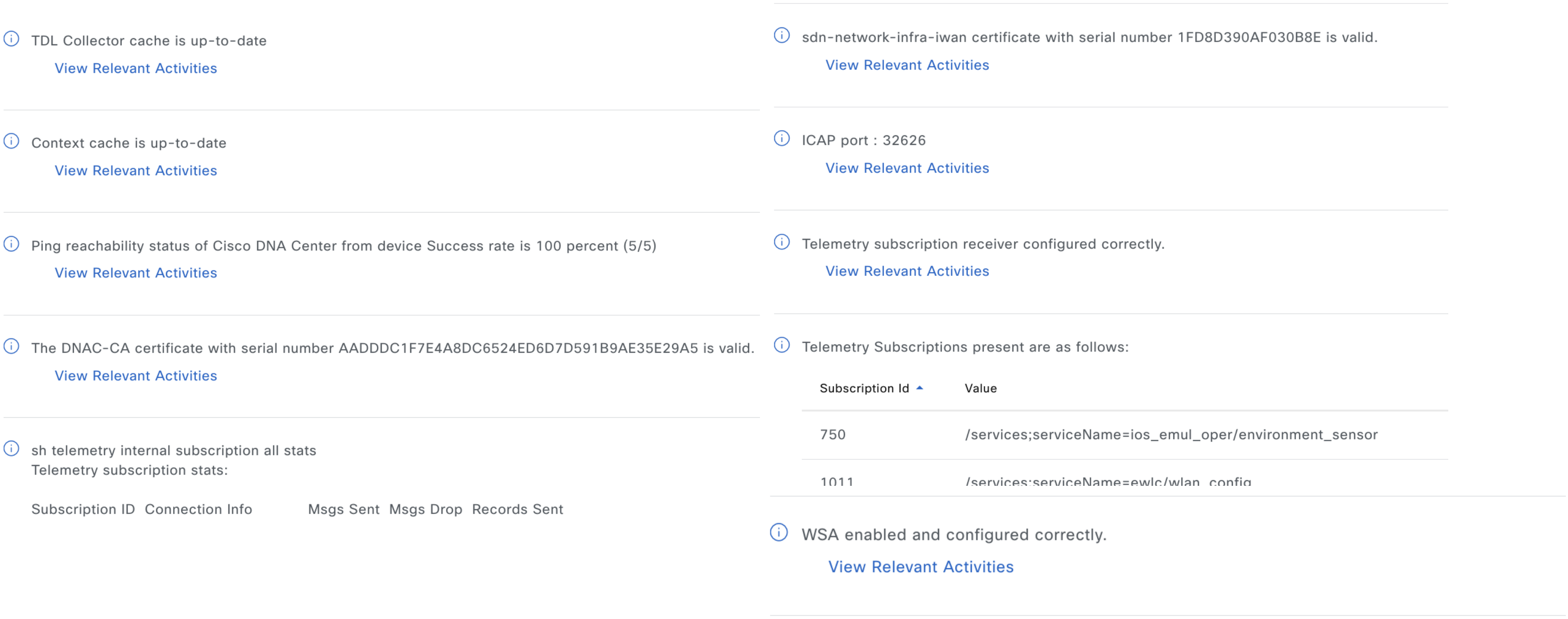
cisco Live!

Release 2.3.5.x onwards

Device Checks

Verification Routines using the Network Reasoner

Example 2. Sample output for a 9800 WLC



ⓘ TDL Collector cache is up-to-date

View Relevant Activities

ⓘ Context cache is up-to-date

View Relevant Activities

ⓘ Ping reachability status of Cisco DNA Center from device Success rate is 100 percent (5/5)

View Relevant Activities

ⓘ The DNAC-CA certificate with serial number AADDDC1F7E4A8DC6524ED6D7D591B9AE35E29A5 is valid.

View Relevant Activities

ⓘ sh telemetry internal subscription all stats

```
Telemetry subscription stats:

Subscription ID  Connection Info          Msgs Sent  Msgs Drop  Records Sent
```

ⓘ sdn-network-infra-iwan certificate with serial number 1FD8D390AF030B8E is valid.

View Relevant Activities

ⓘ ICAP port : 32626

View Relevant Activities

ⓘ Telemetry subscription receiver configured correctly.

View Relevant Activities

ⓘ Telemetry Subscriptions present are as follows:

Subscription Id ▲	Value
750	/services;serviceName=ios_emul_oper/environment_sensor
1011	/services;serviceName=ewlc/wlan_config

ⓘ WSA enabled and configured correctly.

View Relevant Activities

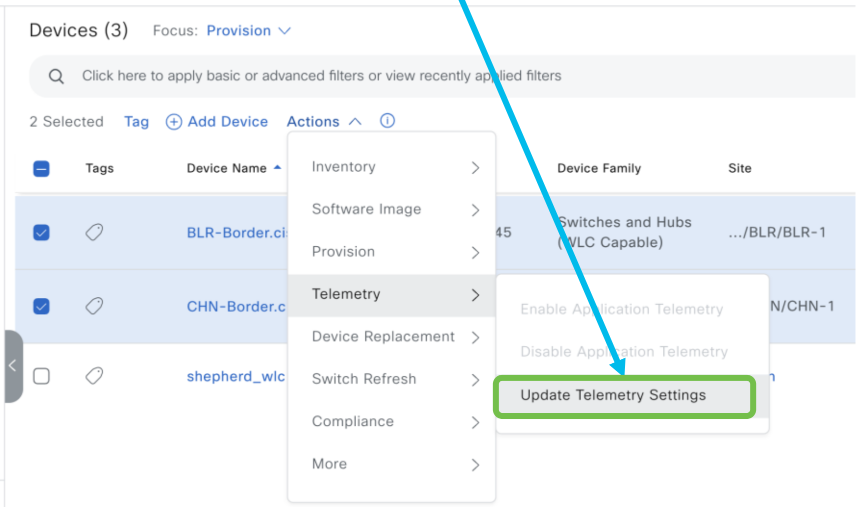
Device Checks

Configurations and Certificates

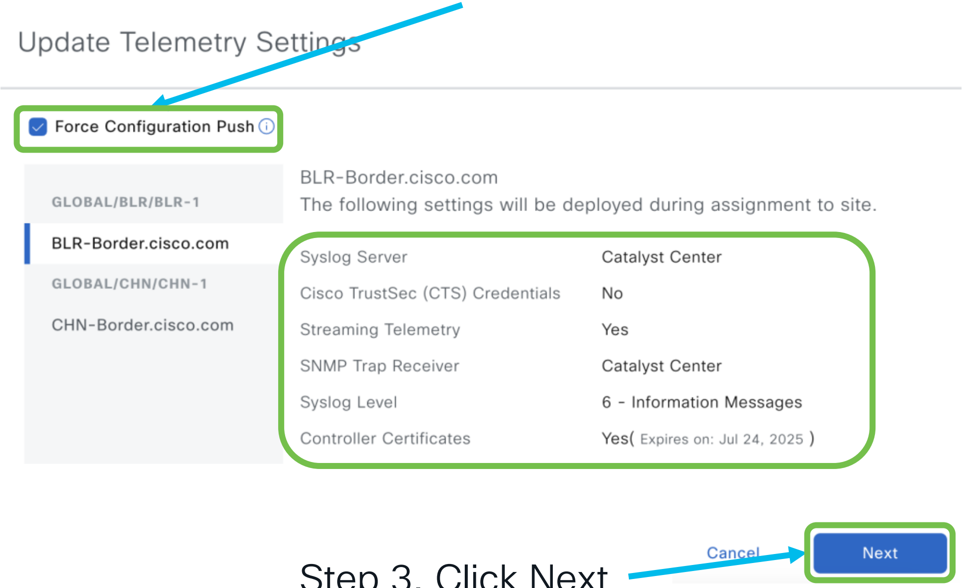
Release 2.3.3.x onwards

To push the necessary telemetry configurations to the device again from the Inventory page

Step 1. Select device(s) and then choose 'Update Telemetry Settings'



Step 2. A new popup with selected devices shows up, choose 'Force Configuration Push'



Update Telemetry Settings

☑ Force Configuration Push

GLOBAL/BLR/BLR-1

BLR-Border.cisco.com

GLOBAL/CHN/CHN-1

CHN-Border.cisco.com

BLR-Border.cisco.com

The following settings will be deployed during assignment to site.

Syslog Server	Catalyst Center
Cisco TrustSec (CTS) Credentials	No
Streaming Telemetry	Yes
SNMP Trap Receiver	Catalyst Center
Syslog Level	6 - Information Messages
Controller Certificates	Yes(Expires on: Jul 24, 2025)

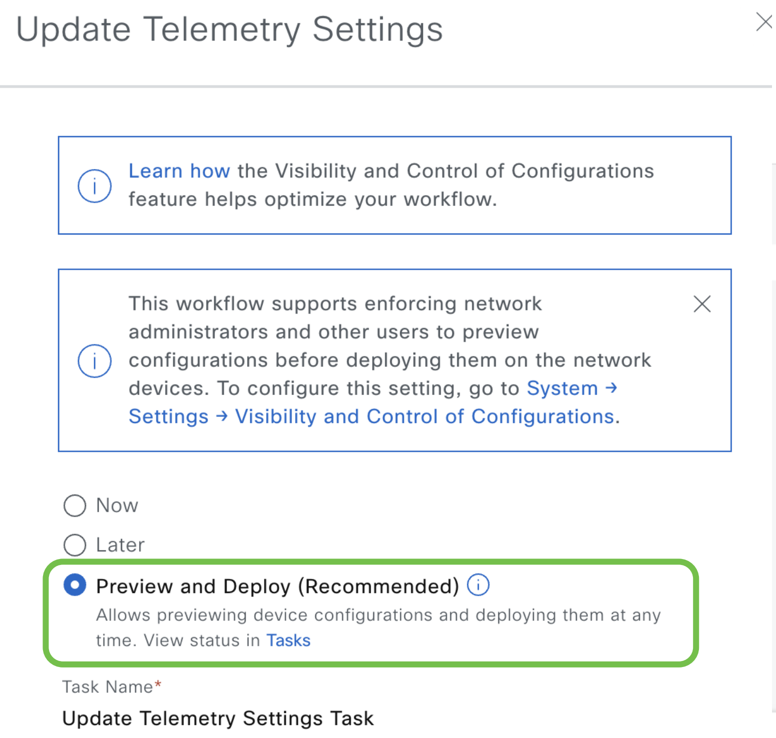
Step 3. Click Next

Release 2.3.7.x onwards

Device Checks

Configurations and Certificates

To push the necessary telemetry configurations to the device again from the Inventory page



Update Telemetry Settings

ⓘ Learn how the Visibility and Control of Configurations feature helps optimize your workflow.

ⓘ This workflow supports enforcing network administrators and other users to preview configurations before deploying them on the network devices. To configure this setting, go to System → Settings → Visibility and Control of Configurations.

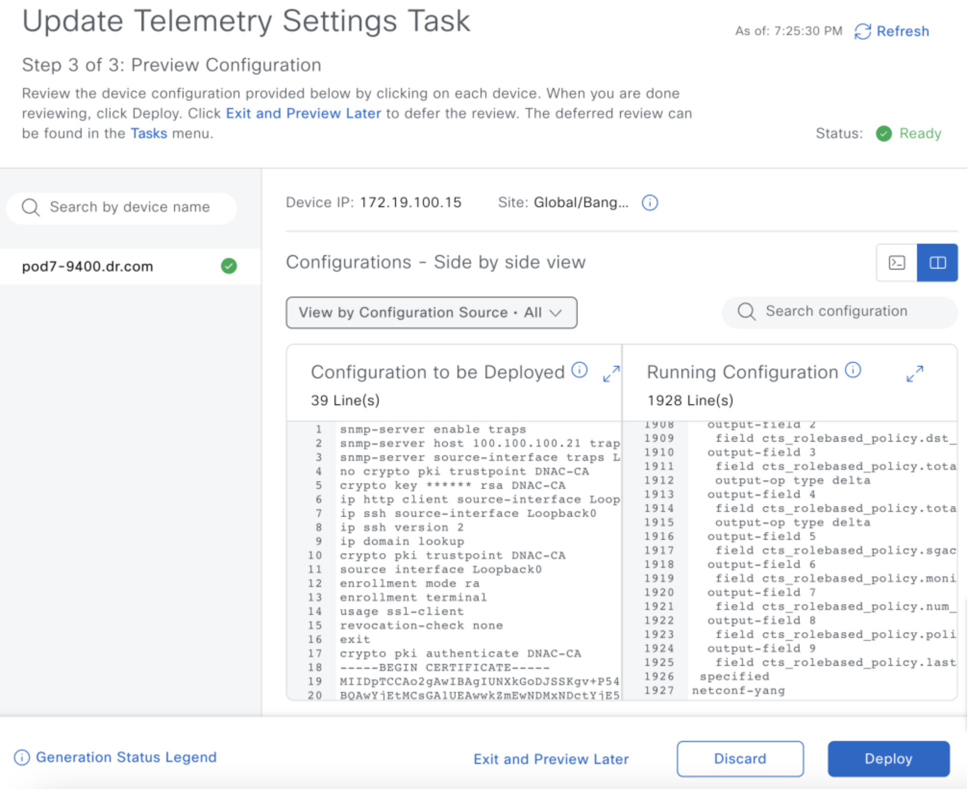
○ Now

○ Later

● Preview and Deploy (Recommended) ⓘ
Allows previewing device configurations and deploying them at any time. View status in Tasks

Task Name*

Update Telemetry Settings Task



Update Telemetry Settings Task

As of: 7:25:30 PM Refresh

Step 3 of 3: Preview Configuration

Review the device configuration provided below by clicking on each device. When you are done reviewing, click Deploy. Click Exit and Preview Later to defer the review. The deferred review can be found in the Tasks menu.

Status: ✓ Ready

Search by device name

pod7-9400.dr.com ✓

Device IP: 172.19.100.15 Site: Global/Bang... ⓘ

Configurations - Side by side view

View by Configuration Source · All

Search configuration

Configuration to be Deployed ⓘ
39 Line(s)

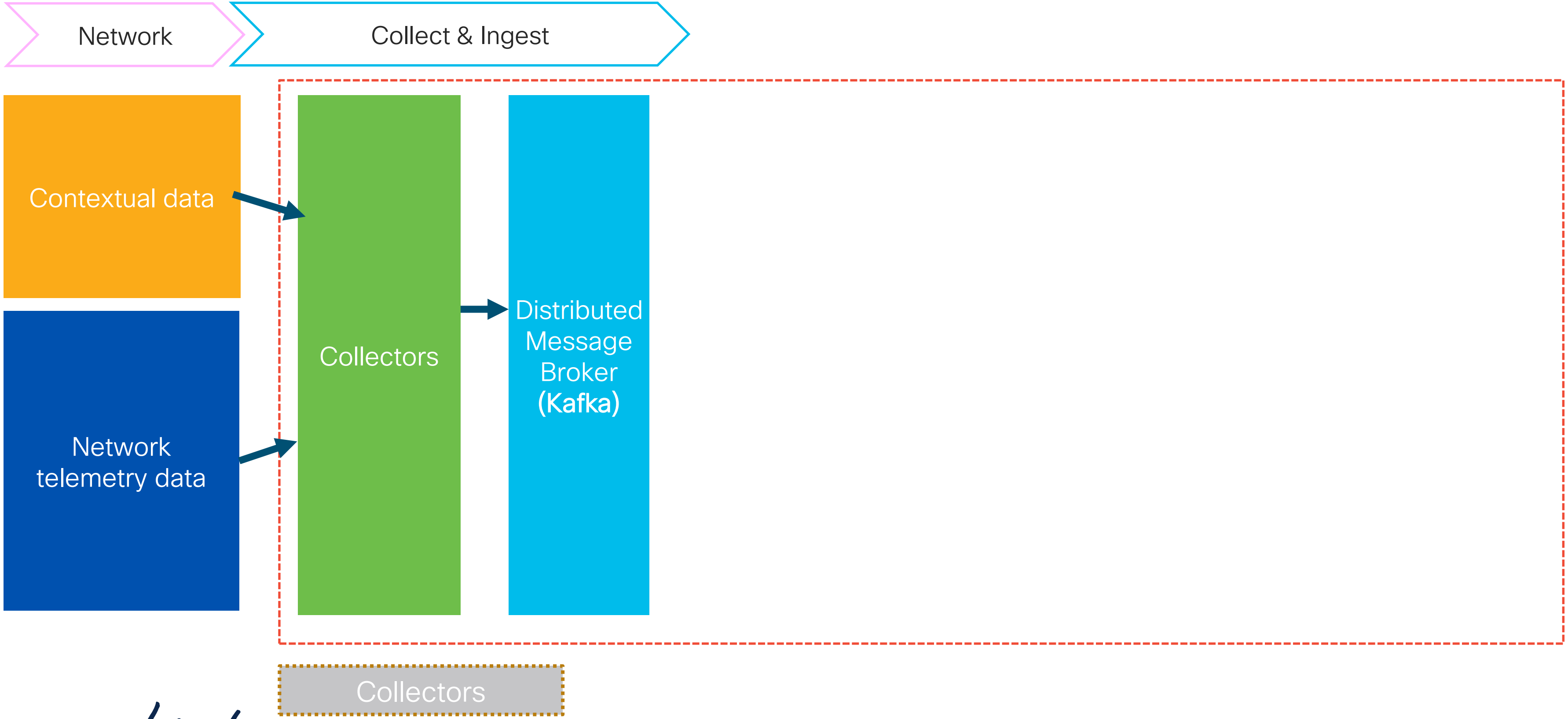
```
snmp-server enable traps
snmp-server host 100.100.100.21 trap
snmp-server source-interface traps L
no crypto pki trustpoint DNAC-CA
crypto key ****** rsa DNAC-CA
ip http client source-interface Loop
ip ssh source-interface Loopback0
ip ssh version 2
ip domain lookup
crypto pki trustpoint DNAC-CA
source interface Loopback0
enrollment mode ra
enrollment terminal
usage ssl-client
revocation-check none
exit
crypto pki authenticate DNAC-CA
-----BEGIN CERTIFICATE-----
MIIDpTCCAo2gAwIBAgIUNXkGoDJSSKgv+P54
BQAwYjEtMCsGA1UEAwwkZmEwNDMxNDctYjE5
```

Running Configuration ⓘ
1928 Line(s)

```
   output-field 2
    field cts_rolebased_policy.dst_
   output-field 3
    field cts_rolebased_policy.tota
    output-op type delta
   output-field 4
    field cts_rolebased_policy.tota
    output-op type delta
   output-field 5
    field cts_rolebased_policy.sgac
   output-field 6
    field cts_rolebased_policy.moni
   output-field 7
    field cts_rolebased_policy.num_
   output-field 8
    field cts_rolebased_policy.poli
   output-field 9
    field cts_rolebased_policy.last
 specified
netconf-yang
```

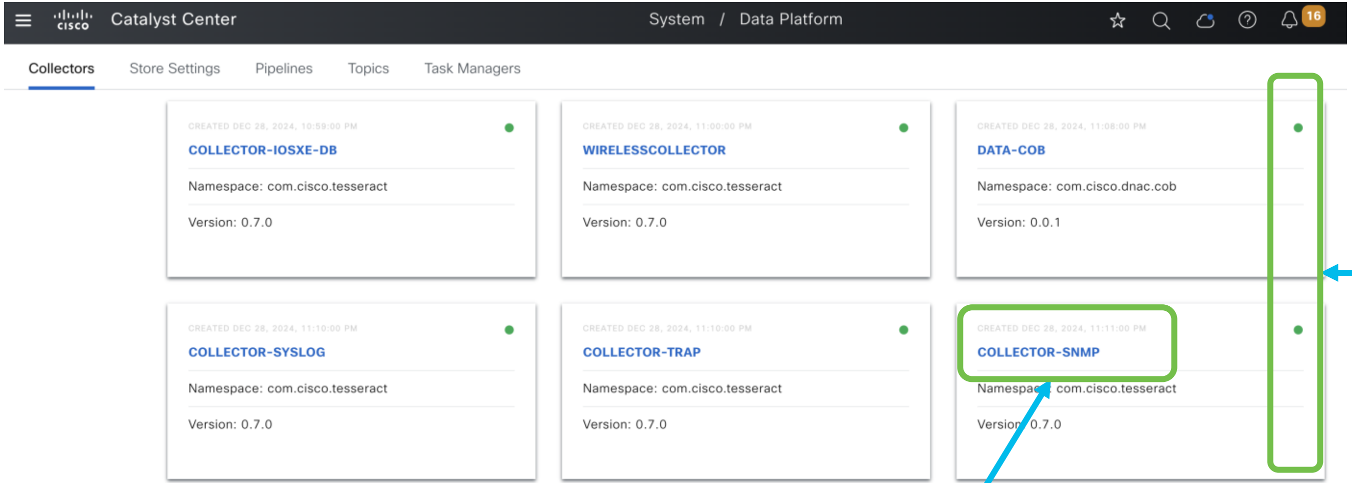
ⓘ Generation Status Legend

Assurance System Flow



System / Data Platform

Assurance Collectors Check



CREATED DEC 28, 2024, 10:59:00 PM
COLLECTOR-IOSXE-DB
Namespace: com.cisco.tesseract
Version: 0.7.0

CREATED DEC 28, 2024, 11:00:00 PM
WIRELESSCOLLECTOR
Namespace: com.cisco.tesseract
Version: 0.7.0

CREATED DEC 28, 2024, 11:08:00 PM
DATA-COB
Namespace: com.cisco.dnac.cob
Version: 0.0.1

CREATED DEC 28, 2024, 11:10:00 PM
COLLECTOR-SYSLOG
Namespace: com.cisco.tesseract
Version: 0.7.0

CREATED DEC 28, 2024, 11:10:00 PM
COLLECTOR-TRAP
Namespace: com.cisco.tesseract
Version: 0.7.0

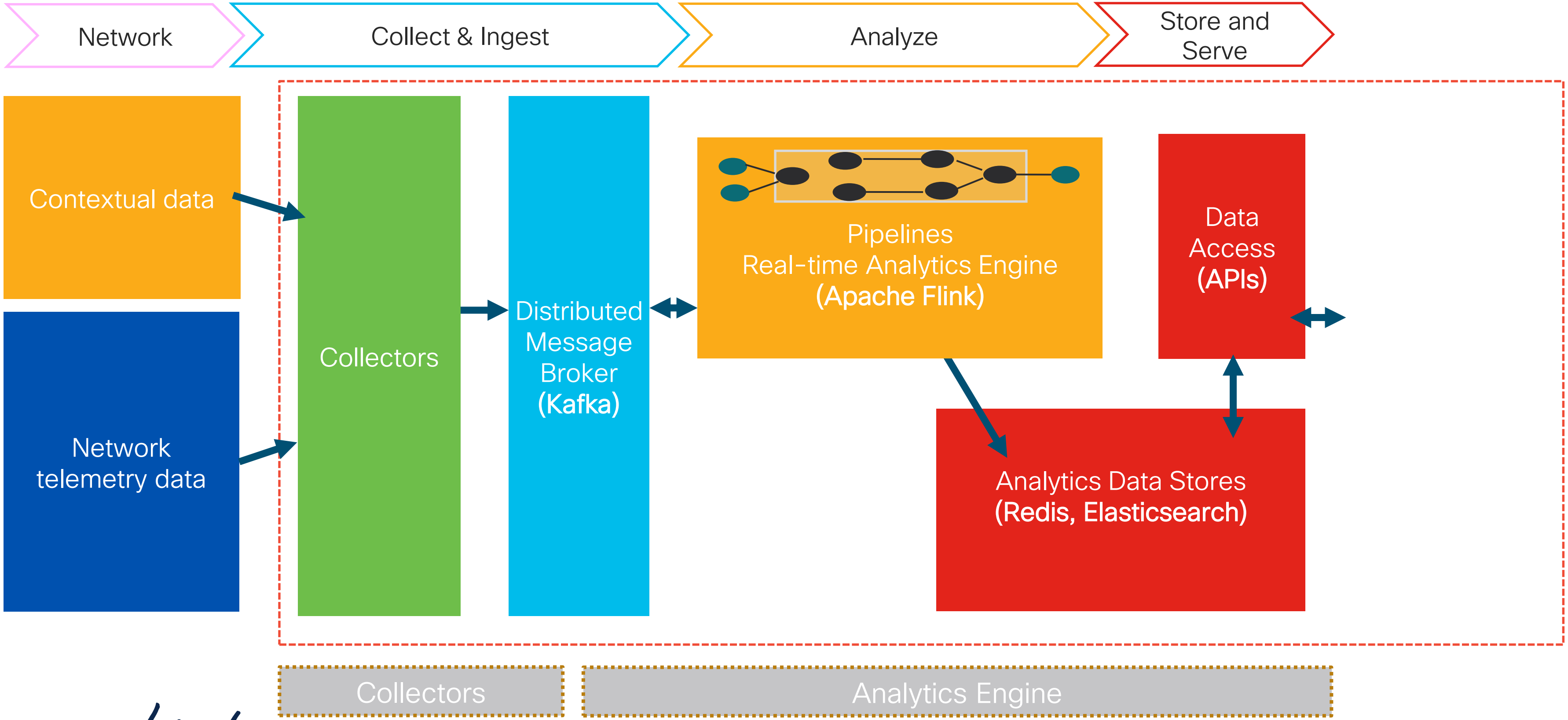
CREATED DEC 28, 2024, 11:11:00 PM
COLLECTOR-SNMP
Namespace: com.cisco.tesseract
Version: 0.7.0

Status of the Collectors

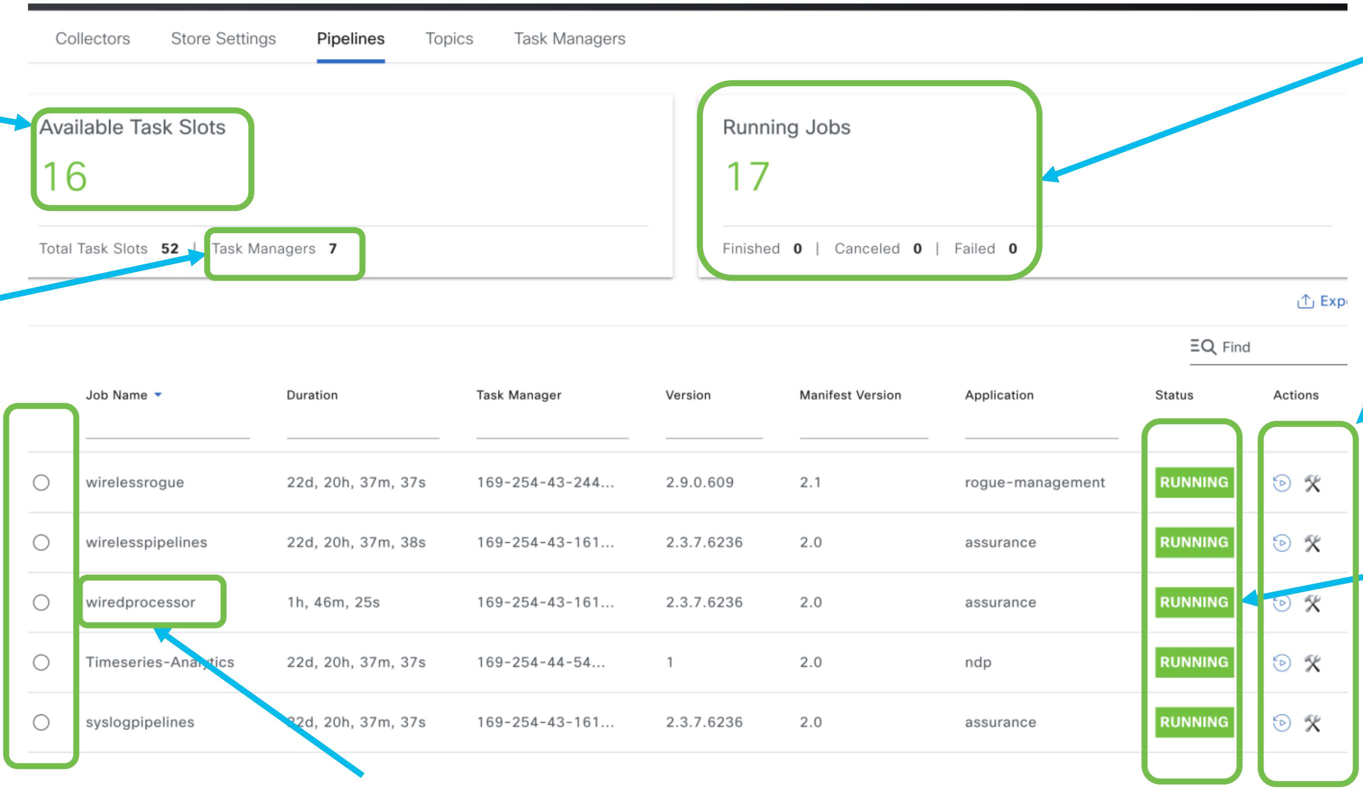
Click on a Collector to view the status, uptime, service name ...

Change SNMP polling frequency

Assurance System Flow



Assurance Pipelines Check



Collectors | Store Settings | **Pipelines** | Topics | Task Managers

Available Task Slots
16

Total Task Slots **52** | Task Managers **7**

Running Jobs
17

Finished **0** | Canceled **0** | Failed **0**

Exp

Find

	Job Name	Duration	Task Manager	Version	Manifest Version	Application	Status	Actions
○	wirelessrogue	22d, 20h, 37m, 37s	169-254-43-244...	2.9.0.609	2.1	rogue-management	RUNNING	
○	wirelesspipelines	22d, 20h, 37m, 38s	169-254-43-161...	2.3.7.6236	2.0	assurance	RUNNING	
○	wiredprocessor	1h, 46m, 25s	169-254-43-161...	2.3.7.6236	2.0	assurance	RUNNING	
○	Timeseries-Analytics	22d, 20h, 37m, 37s	169-254-44-54...	1	2.0	ndp	RUNNING	
○	syslogpipelines	22d, 20h, 37m, 37s	169-254-43-161...	2.3.7.6236	2.0	assurance	RUNNING	

Slots available to run Pipelines

Services to run the Pipelines

Click to view the metrics, topics, exceptions

Pipelines

Actions

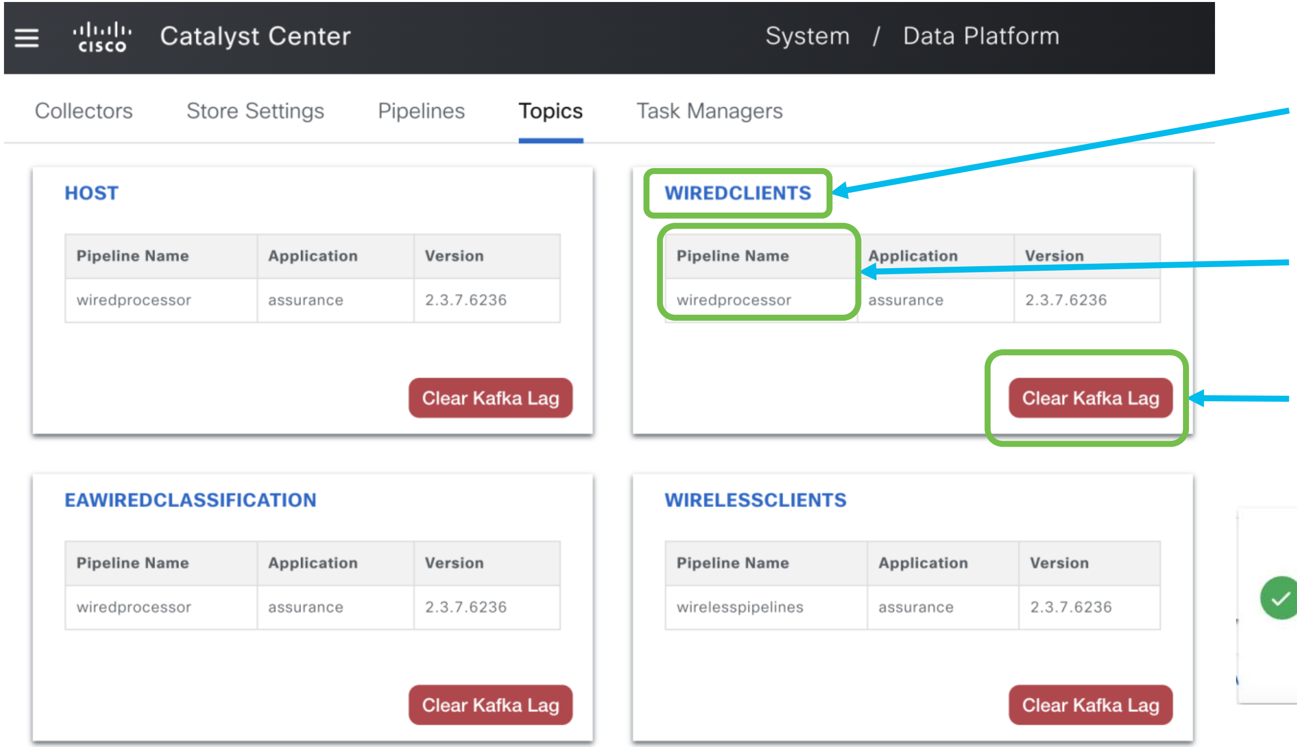
Status of the Pipelines

Responsible for Wired Clients

System / Data Platform

Release 2.3.7.x onwards

Assurance Kafka View



HOST

Pipeline Name	Application	Version
wiredprocessor	assurance	2.3.7.6236

WIREDCLIENTS

Pipeline Name	Application	Version
wiredprocessor	assurance	2.3.7.6236

EAWIREDCLASSIFICATION

Pipeline Name	Application	Version
wiredprocessor	assurance	2.3.7.6236

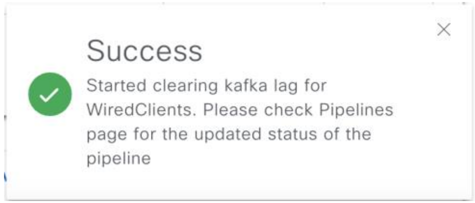
WIRELESSCLIENTS

Pipeline Name	Application	Version
wirelesspipelines	assurance	2.3.7.6236

Kafka Topic

Subscribed Pipeline

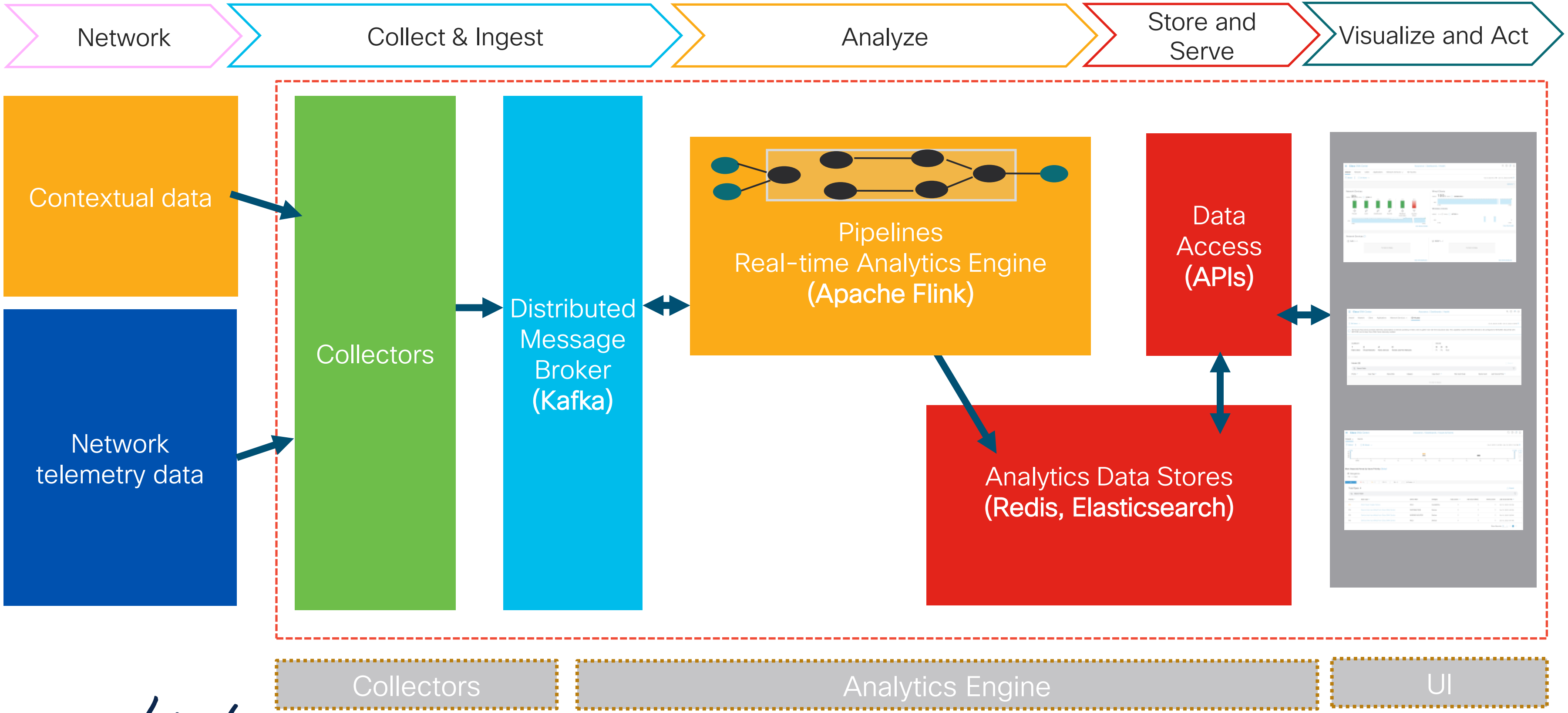
Click to clear a Kafka lag



Success

Started clearing kafka lag for WiredClients. Please check Pipelines page for the updated status of the pipeline

Assurance System Flow



Network

Collect & Ingest

Analyze

Store and Serve

Visualize and Act

Contextual data

Network telemetry data

Collectors

Distributed Message Broker **(Kafka)**

Pipelines
Real-time Analytics Engine
(Apache Flink)

Data Access **(APIs)**

Analytics Data Stores **(Redis, Elasticsearch)**

Collectors

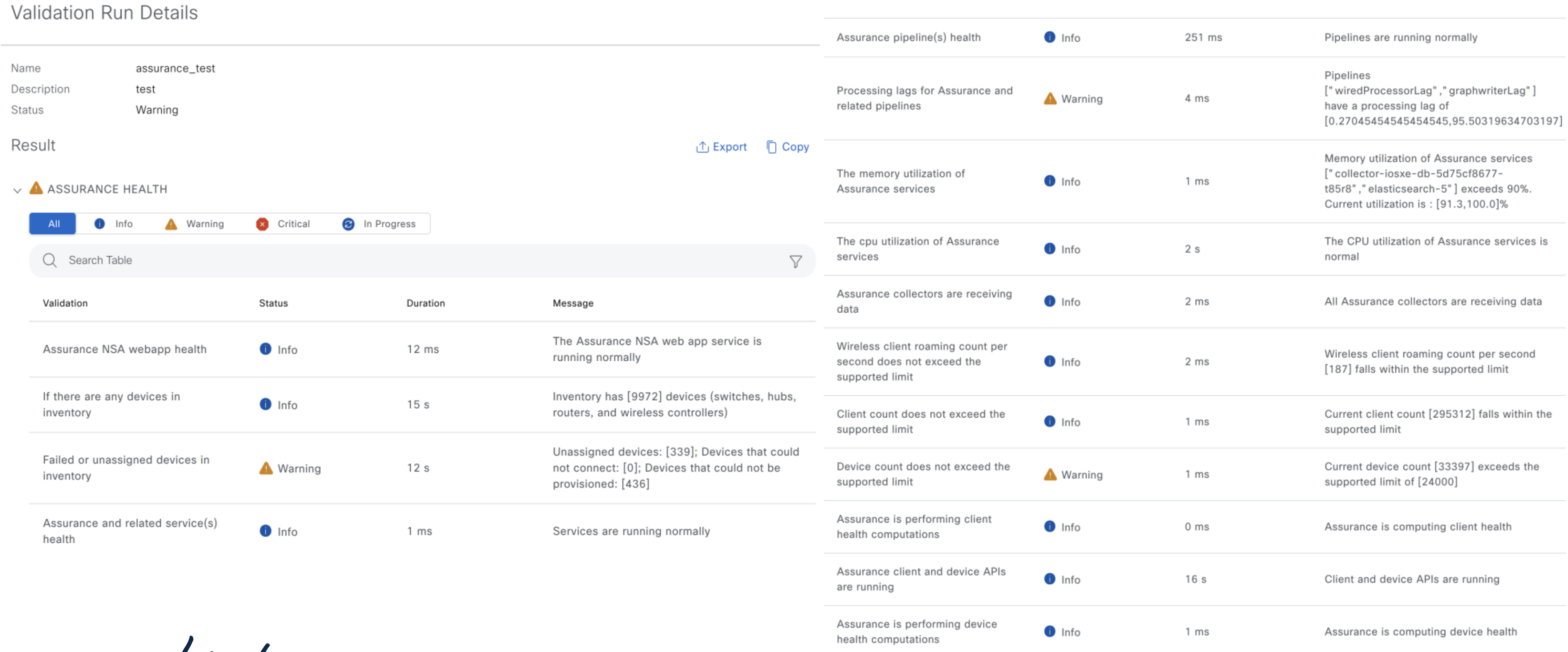
Analytics Engine

UI

Release 2.3.5.x onwards

Assurance – Network Health

Validation Tool – (System → System Health → Tools)



Validation Run Details

Name	assurance_test
Description	test
Status	Warning

Result

Validation	Status	Duration	Message
Assurance NSA webapp health	Info	12 ms	The Assurance NSA web app service is running normally
If there are any devices in inventory	Info	15 s	Inventory has [9972] devices (switches, hubs, routers, and wireless controllers)
Failed or unassigned devices in inventory	Warning	12 s	Unassigned devices: [339]; Devices that could not connect: [0]; Devices that could not be provisioned: [436]
Assurance and related service(s) health	Info	1 ms	Services are running normally
Assurance pipeline(s) health	Info	251 ms	Pipelines are running normally
Processing lags for Assurance and related pipelines	Warning	4 ms	Pipelines ["wiredProcessorLag","graphwriterLag"] have a processing lag of [0.27045454545454545,95.50319634703197]
The memory utilization of Assurance services	Info	1 ms	Memory utilization of Assurance services ["collector-iosxe-db-5d75cf8677-t85r8","elasticsearch-5"] exceeds 90%. Current utilization is : [91.3,100.0]%
The cpu utilization of Assurance services	Info	2 s	The CPU utilization of Assurance services is normal
Assurance collectors are receiving data	Info	2 ms	All Assurance collectors are receiving data
Wireless client roaming count per second does not exceed the supported limit	Info	2 ms	Wireless client roaming count per second [187] falls within the supported limit
Client count does not exceed the supported limit	Info	1 ms	Current client count [295312] falls within the supported limit
Device count does not exceed the supported limit	Warning	1 ms	Current device count [33397] exceeds the supported limit of [24000]
Assurance is performing client health computations	Info	0 ms	Assurance is computing client health
Assurance client and device APIs are running	Info	16 s	Client and device APIs are running
Assurance is performing device health computations	Info	1 ms	Assurance is computing device health

All Releases

Cisco AI Analytics

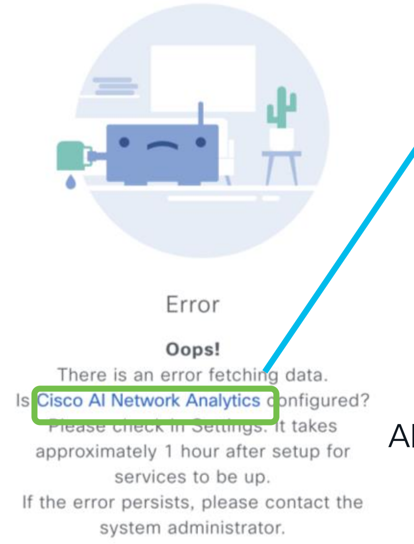
Leverages advanced machine learning techniques and an advanced cloud learning platform

AI Analytics Features

- AI Network Analytics (Network Heatmap, Baseline Dashboard, AP Performance Advisories…)
- AI Enhanced RRM

Most Common Issue

Almost all TAC SRs are related to cloud connect



Error

Oops!

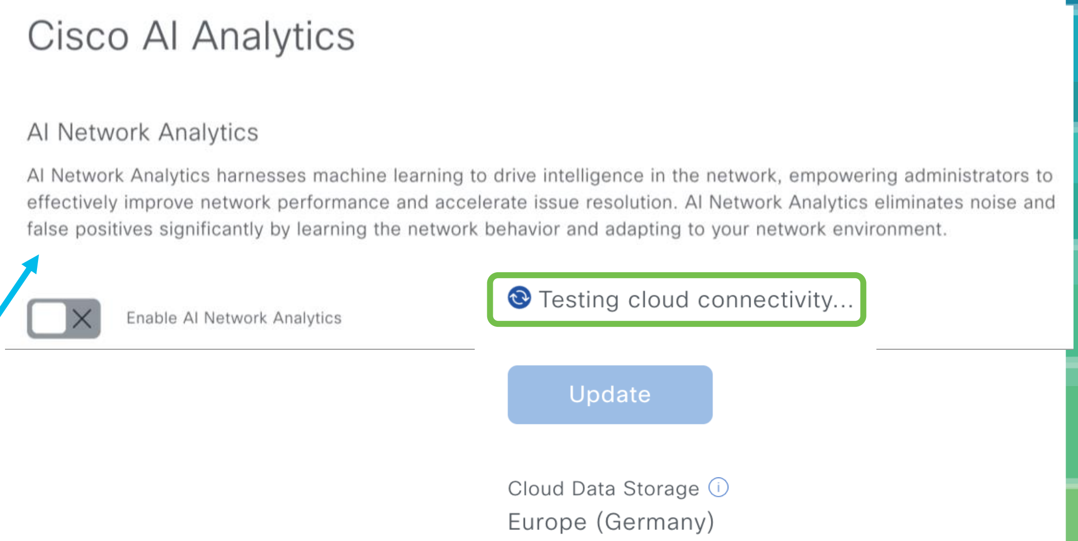
There is an error fetching data.

Is Cisco AI Network Analytics configured?

Please check in Settings. It takes approximately 1 hour after setup for services to be up.

If the error persists, please contact the system administrator.

Feature enabled in Settings → External Services



Cisco AI Analytics

AI Network Analytics

AI Network Analytics harnesses machine learning to drive intelligence in the network, empowering administrators to effectively improve network performance and accelerate issue resolution. AI Network Analytics eliminates noise and false positives significantly by learning the network behavior and adapting to your network environment.

☒ Enable AI Network Analytics

Testing cloud connectivity...

Cloud Data Storage ⓘ

Europe (Germany)

Allow outbound HTTPS (TCP 443) access to the cloud hosts

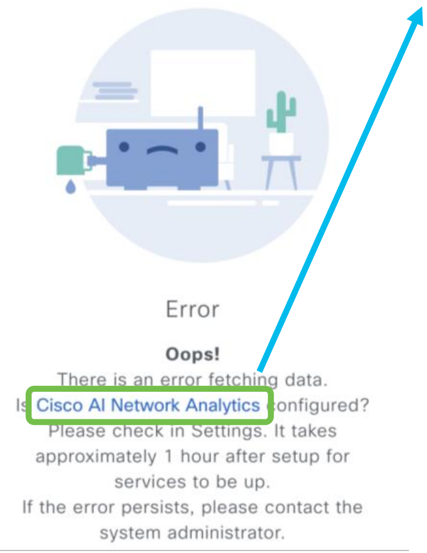
- https://api.use1.prd.kairos.ciscolabs.com (US East Region)
- https://api.euc1.prd.kairos.ciscolabs.com (EU Central Region)

Settings / External Services

Release 2.3.5.x onwards

Cisco AI Analytics - Troubleshooting

Cloud Connectivity Check performed Automatically



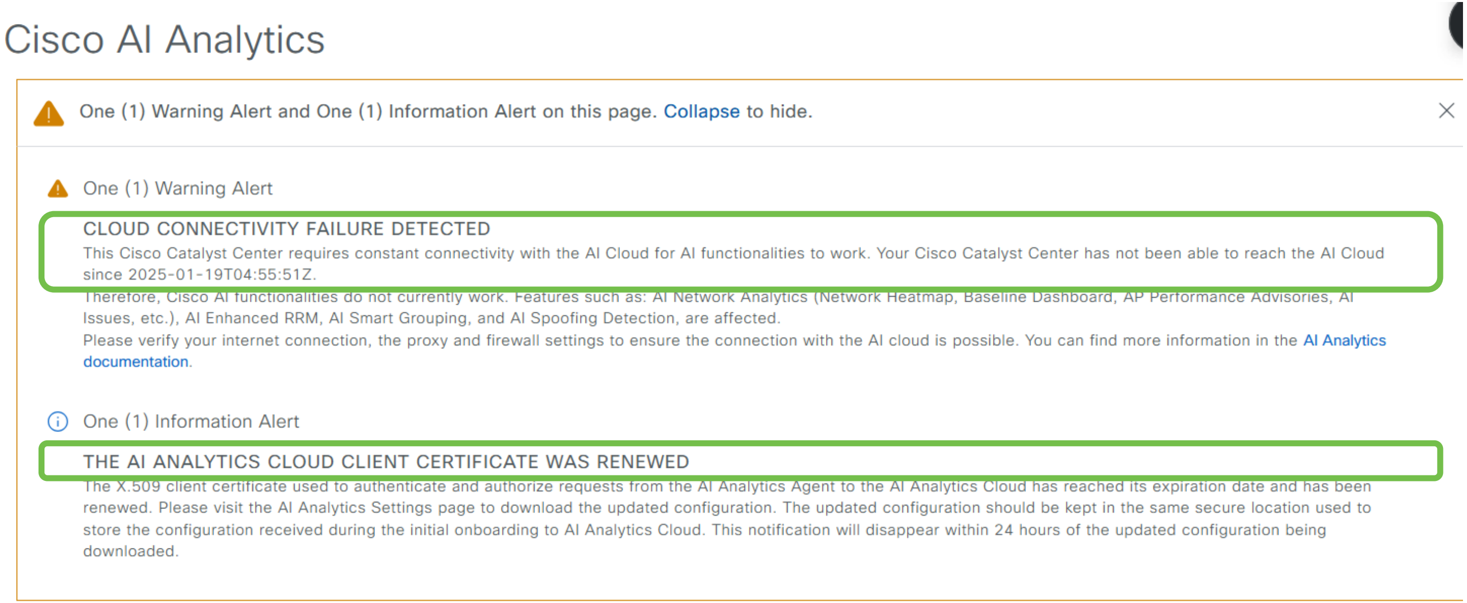
Error

Oops!

There is an error fetching data.

Is Cisco AI Network Analytics configured? Please check in Settings. It takes approximately 1 hour after setup for services to be up.

If the error persists, please contact the system administrator.



Cisco AI Analytics

One (1) Warning Alert and One (1) Information Alert on this page. Collapse to hide.

One (1) Warning Alert

CLOUD CONNECTIVITY FAILURE DETECTED

This Cisco Catalyst Center requires constant connectivity with the AI Cloud for AI functionalities to work. Your Cisco Catalyst Center has not been able to reach the AI Cloud since 2025-01-19T04:55:51Z.

Therefore, Cisco AI functionalities do not currently work. Features such as: AI Network Analytics (Network Heatmap, Baseline Dashboard, AP Performance Advisories, AI Issues, etc.), AI Enhanced RRM, AI Smart Grouping, and AI Spoofing Detection, are affected.

Please verify your internet connection, the proxy and firewall settings to ensure the connection with the AI cloud is possible. You can find more information in the AI Analytics documentation.

One (1) Information Alert

THE AI ANALYTICS CLOUD CLIENT CERTIFICATE WAS RENEWED

The X.509 client certificate used to authenticate and authorize requests from the AI Analytics Agent to the AI Analytics Cloud has reached its expiration date and has been renewed. Please visit the AI Analytics Settings page to download the updated configuration. The updated configuration should be kept in the same secure location used to store the configuration received during the initial onboarding to AI Analytics Cloud. This notification will disappear within 24 hours of the updated configuration being downloaded.

All Versions

Cisco AI Analytics - Troubleshooting

CLI Based Troubleshooting

```
$ magctl appstack status
NAMESPACE                  NAME                                                          READY   STATUS
RESTARTS   AGE    IP              NODE          NOMINATED NODE   READINESS GATES
ai-network-analytics       apiproxy-85998b7d5d-gqgpq                                     1/1     Running
1          38d    169.254.43.143  192.168.5.11  <none>           <none>
ai-network-analytics       kairos-agent-598db4d8c7-sk65t                                 1/1     Running
3          38d    169.254.44.15   192.168.5.11  <none>           <none>
...
```

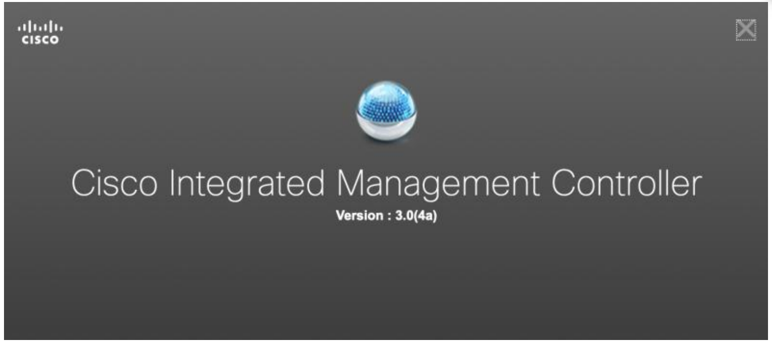
```
$ magctl service logs -a ai-network-analytics kairos-agent

...
| 68571 | 2025-01-27T15:30:14.007Z | INFO | config.server | c19426b6-b7f6-449a-8121-fcfa93c55b5c |
60357c6875dceb00caa5b63e | cloud is reachable |
| 68572 | 2025-01-27T15:30:14.007Z | INFO | config.server | c19426b6-b7f6-449a-8121-fcfa93c55b5c |
60357c6875dceb00caa5b63e | request succeeded |
| 68573 | 2025-01-27T15:30:21.986Z | ERROR | config.server | None | None | unable to resolve FQDN of ip …
...
```

Catalyst Center Software Upgrades Troubleshooting

Catalyst Center Upgrades

Cisco IMC (firmware)

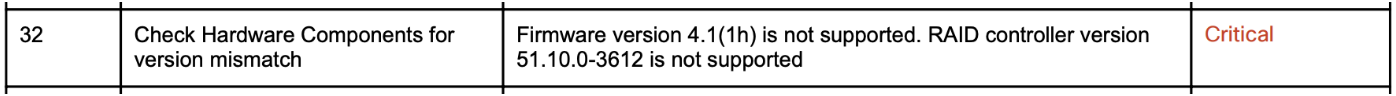
Ensure the firmware version matches the supported version for the Catalyst Center release.



Cisco Integrated Management Controller

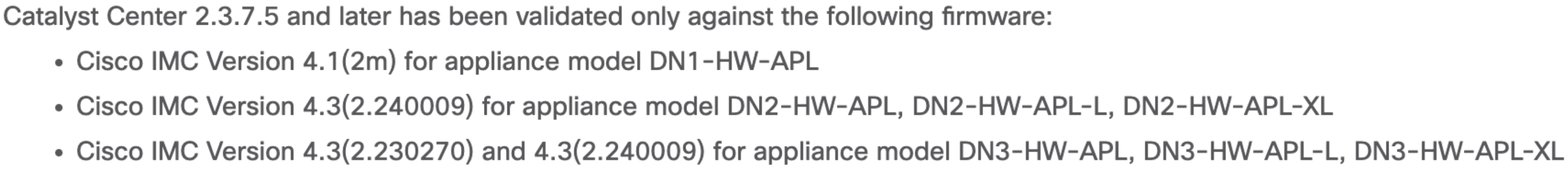
Version : 3.0(4a)

Validation Tool check



32	Check Hardware Components for version mismatch	Firmware version 4.1(1h) is not supported. RAID controller version 51.10.0-3612 is not supported	Critical

From the 2.3.7 release notes (same versions for 2.3.5):



Catalyst Center 2.3.7.5 and later has been validated only against the following firmware:

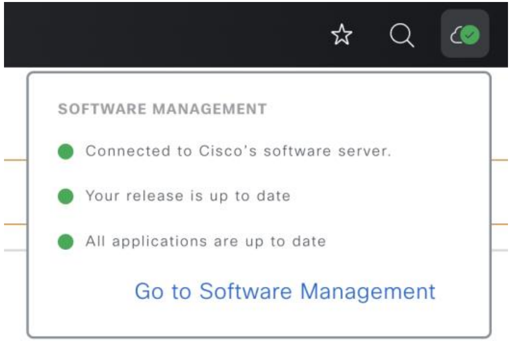
- Cisco IMC Version 4.1(2m) for appliance model DN1-HW-APL
- Cisco IMC Version 4.3(2.240009) for appliance model DN2-HW-APL, DN2-HW-APL-L, DN2-HW-APL-XL
- Cisco IMC Version 4.3(2.230270) and 4.3(2.240009) for appliance model DN3-HW-APL, DN3-HW-APL-L, DN3-HW-APL-XL

[2.3.7 Release Notes]()

Release 2.3.5.x onwards

Catalyst Center Software Version

No Action



SOFTWARE MANAGEMENT

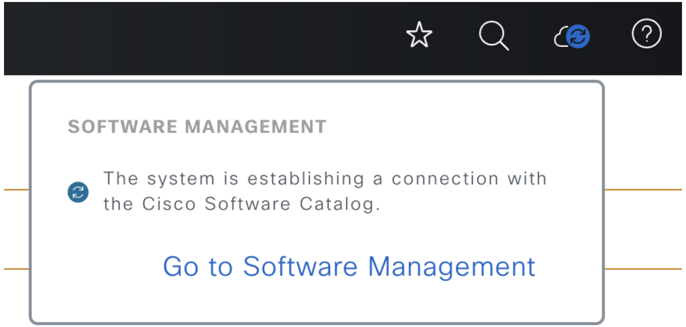
🟢 Connected to Cisco's software server.

🟢 Your release is up to date

🟢 All applications are up to date

Go to Software Management

Checking with the cloud catalog server

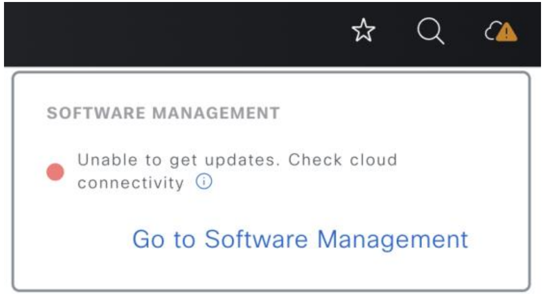


SOFTWARE MANAGEMENT

The system is establishing a connection with the Cisco Software Catalog.

Go to Software Management

Troubleshoot Connectivity

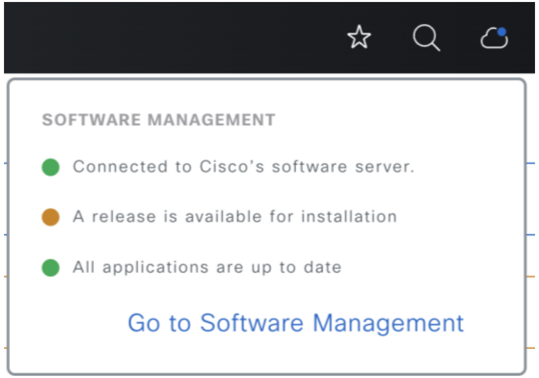


SOFTWARE MANAGEMENT

🔴 Unable to get updates. Check cloud connectivity ⓘ

Go to Software Management

DNS Resolution to https://www.ciscoconnectdna.com:443



SOFTWARE MANAGEMENT

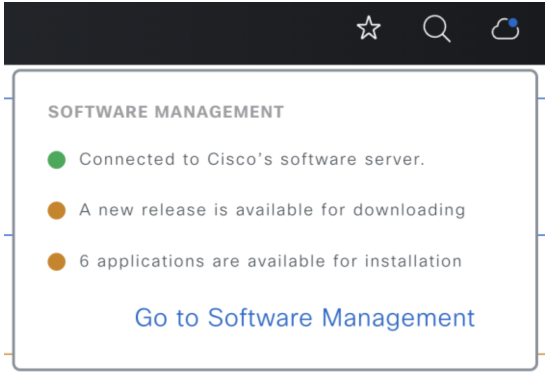
🟢 Connected to Cisco's software server.

🟠 A release is available for installation

🟢 All applications are up to date

Go to Software Management

Upgrade Required



SOFTWARE MANAGEMENT

🟢 Connected to Cisco's software server.

🟠 A new release is available for downloading

🟠 6 applications are available for installation

Go to Software Management

Choosing a Target Release

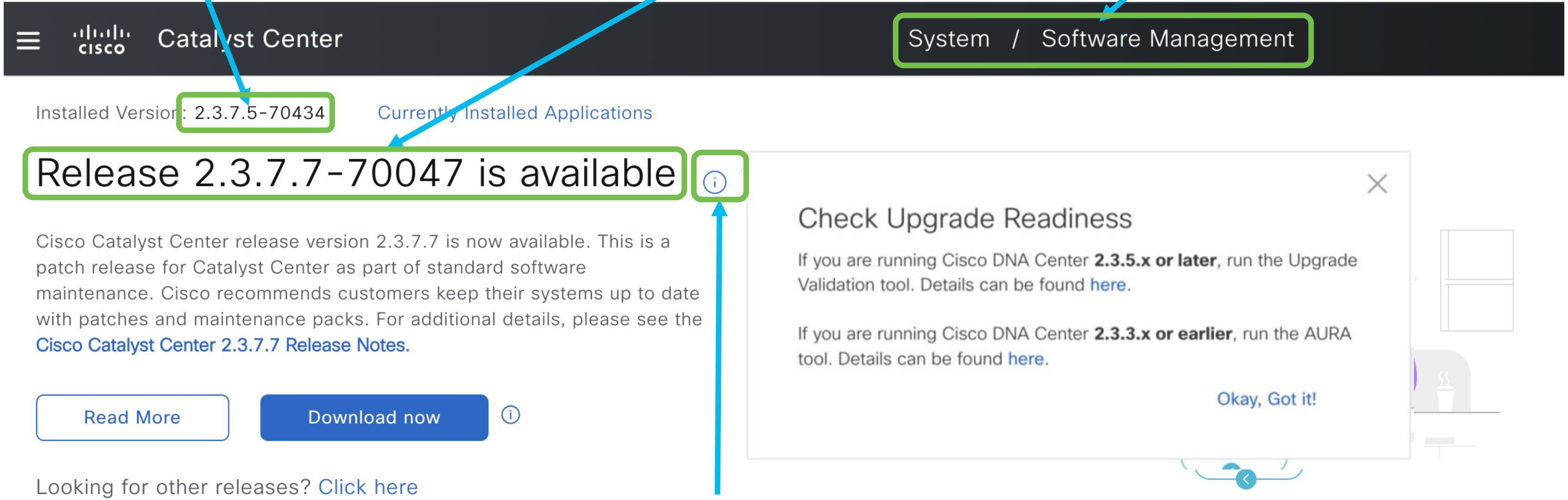
The New Way - Simplified

Release 2.3.x.x onwards

The current version

The latest available option (by default)

Software Update is now Software Management



Installed Version: 2.3.7.5-70434

Currently Installed Applications

Release 2.3.7.7-70047 is available

Cisco Catalyst Center release version 2.3.7.7 is now available. This is a patch release for Catalyst Center as part of standard software maintenance. Cisco recommends customers keep their systems up to date with patches and maintenance packs. For additional details, please see the Cisco Catalyst Center 2.3.7.7 Release Notes.

Looking for other releases? Click here

Check Upgrade Readiness

If you are running Cisco DNA Center **2.3.5.x or later**, run the Upgrade Validation tool. Details can be found here.

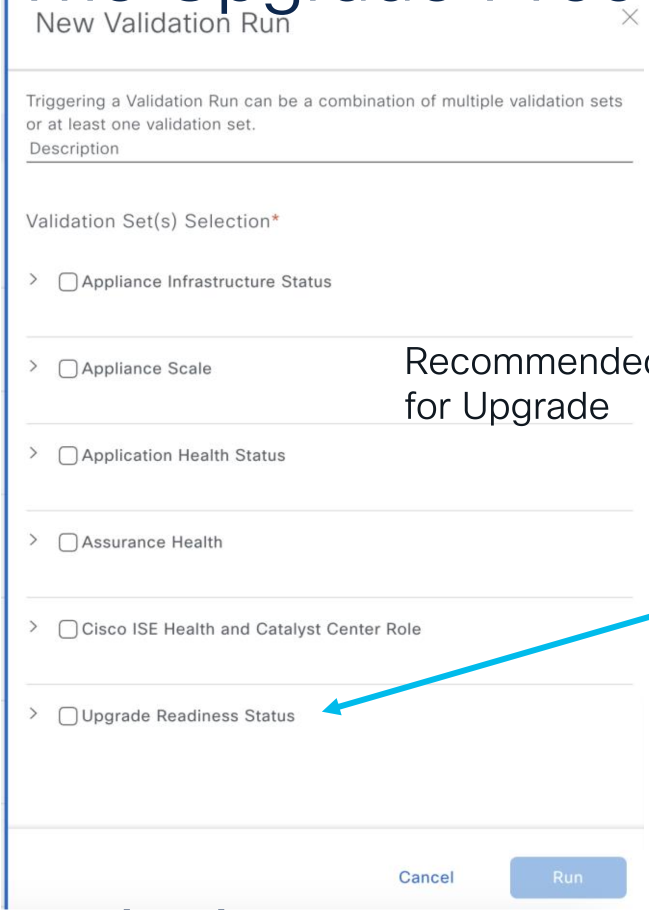
If you are running Cisco DNA Center **2.3.3.x or earlier**, run the AURA tool. Details can be found here.

Info to check for Upgrade Readiness

The Upgrade Process (Prerequisites)

Release 2.3.5.x onwards

System Health / Validation Tool



New Validation Run

Triggering a Validation Run can be a combination of multiple validation sets or at least one validation set.

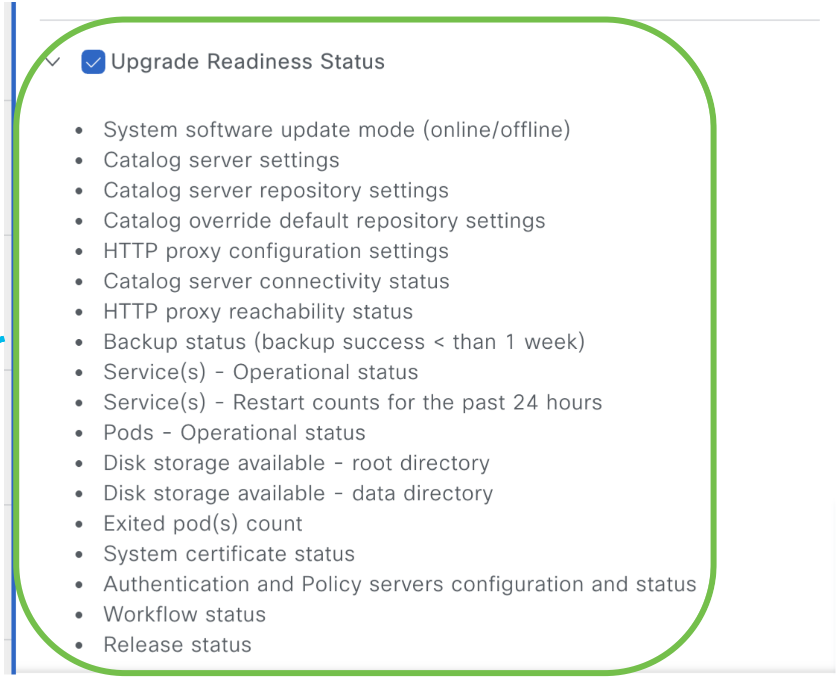
Description

Validation Set(s) Selection*

- › □ Appliance Infrastructure Status
- › □ Appliance Scale
- › □ Application Health Status
- › □ Assurance Health
- › □ Cisco ISE Health and Catalyst Center Role
- › □ Upgrade Readiness Status

Recommended for Upgrade

Checks focussed on Upgrade Readiness



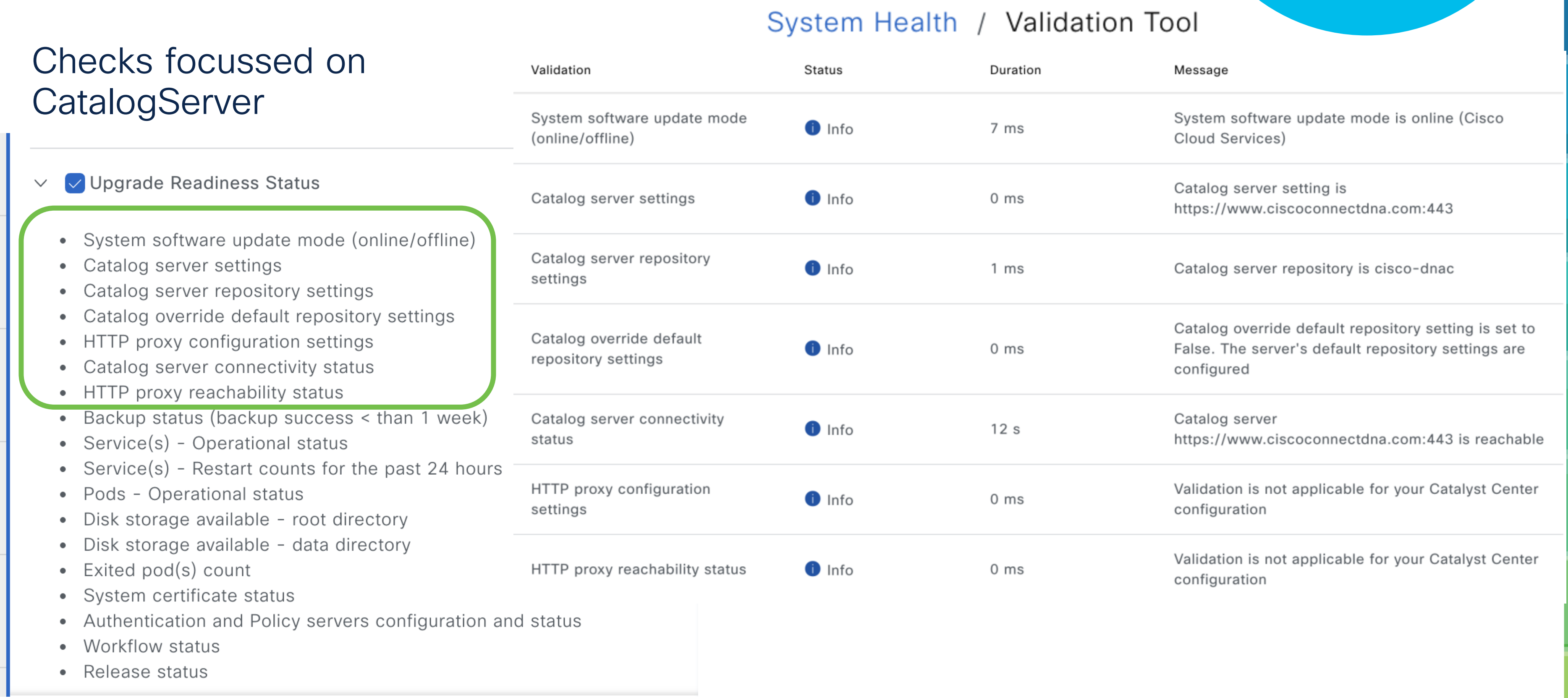
☑ Upgrade Readiness Status

- System software update mode (online/offline)
- Catalog server settings
- Catalog server repository settings
- Catalog override default repository settings
- HTTP proxy configuration settings
- Catalog server connectivity status
- HTTP proxy reachability status
- Backup status (backup success < than 1 week)
- Service(s) - Operational status
- Service(s) - Restart counts for the past 24 hours
- Pods - Operational status
- Disk storage available - root directory
- Disk storage available - data directory
- Exited pod(s) count
- System certificate status
- Authentication and Policy servers configuration and status
- Workflow status
- Release status

The Upgrade Process (Prerequisites)

Release 2.3.5.x onwards

Checks focussed on CatalogServer



☑ Upgrade Readiness Status

- System software update mode (online/offline)
- Catalog server settings
- Catalog server repository settings
- Catalog override default repository settings
- HTTP proxy configuration settings
- Catalog server connectivity status
- HTTP proxy reachability status
- Backup status (backup success < than 1 week)
- Service(s) - Operational status
- Service(s) - Restart counts for the past 24 hours
- Pods - Operational status
- Disk storage available - root directory
- Disk storage available - data directory
- Exited pod(s) count
- System certificate status
- Authentication and Policy servers configuration and status
- Workflow status
- Release status

System Health / Validation Tool

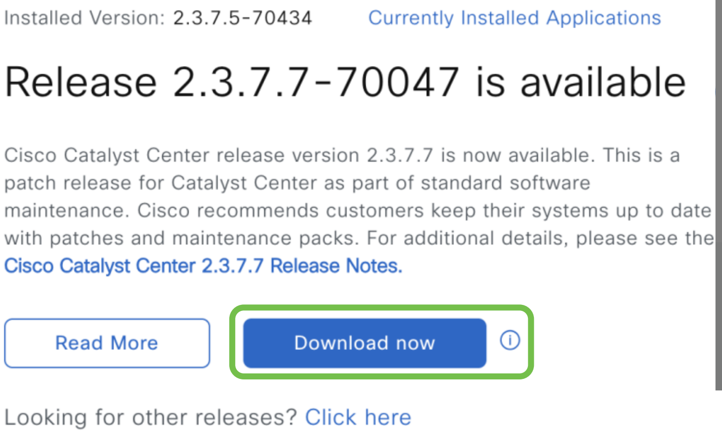
Validation	Status	Duration	Message
System software update mode (online/offline)	Info	7 ms	System software update mode is online (Cisco Cloud Services)
Catalog server settings	Info	0 ms	Catalog server setting is https://www.ciscoconnectdna.com:443
Catalog server repository settings	Info	1 ms	Catalog server repository is cisco-dnac
Catalog override default repository settings	Info	0 ms	Catalog override default repository setting is set to False. The server's default repository settings are configured
Catalog server connectivity status	Info	12 s	Catalog server https://www.ciscoconnectdna.com:443 is reachable
HTTP proxy configuration settings	Info	0 ms	Validation is not applicable for your Catalyst Center configuration
HTTP proxy reachability status	Info	0 ms	Validation is not applicable for your Catalyst Center configuration

The Upgrade Process

The New Way - Reduced to 2 Compulsory + 1 Optional Step

Release 2.3.x.x onwards

Step 1. Click ‘Download Now’ to **download** the System & Application packages

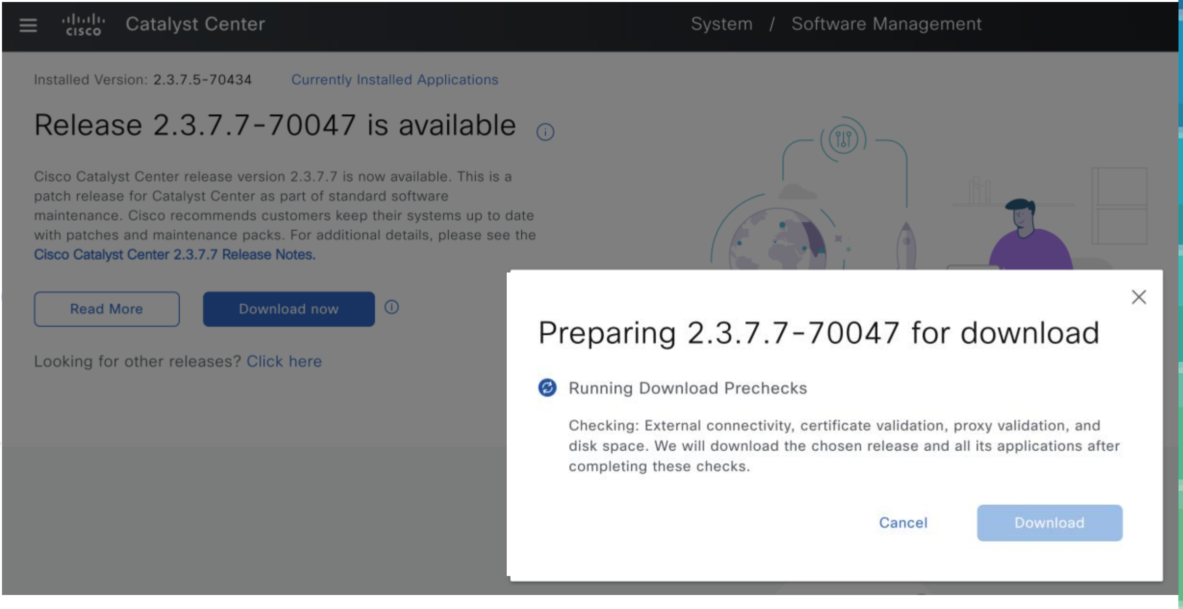


Installed Version: 2.3.7.5-70434 Currently Installed Applications

Release 2.3.7.7-70047 is available

Cisco Catalyst Center release version 2.3.7.7 is now available. This is a patch release for Catalyst Center as part of standard software maintenance. Cisco recommends customers keep their systems up to date with patches and maintenance packs. For additional details, please see the Cisco Catalyst Center 2.3.7.7 Release Notes.

Looking for other releases? Click here



Installed Version: 2.3.7.5-70434 Currently Installed Applications

Release 2.3.7.7-70047 is available

Cisco Catalyst Center release version 2.3.7.7 is now available. This is a patch release for Catalyst Center as part of standard software maintenance. Cisco recommends customers keep their systems up to date with patches and maintenance packs. For additional details, please see the Cisco Catalyst Center 2.3.7.7 Release Notes.

Looking for other releases? Click here

Preparing 2.3.7.7-70047 for download

Running Download Prechecks

Checking: External connectivity, certificate validation, proxy validation, and disk space. We will download the chosen release and all its applications after completing these checks.

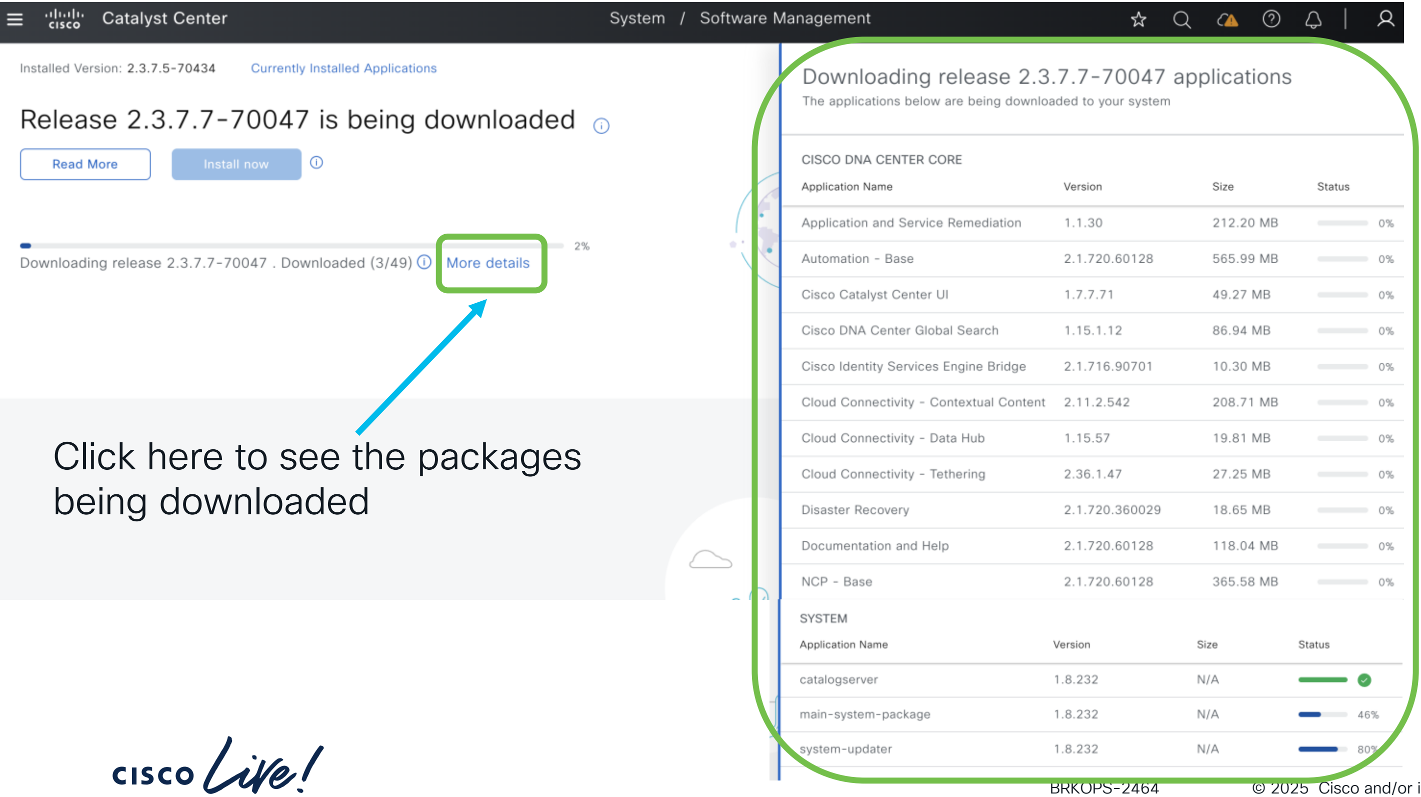
System and Applications packages **downloaded** in the same step

The Upgrade Process

The New Way - Reduced to 2 Compulsory + 1 Optional Step

Release 2.3.x.x onwards

System and Applications packages downloaded in the same step



Installed Version: 2.3.7.5-70434   Currently Installed Applications

Release 2.3.7.7-70047 is being downloaded

Downloading release 2.3.7.7-70047 . Downloaded (3/49) More details 2%

Click here to see the packages being downloaded

Downloading release 2.3.7.7-70047 applications

The applications below are being downloaded to your system

CISCO DNA CENTER CORE

Application Name	Version	Size	Status
Application and Service Remediation	1.1.30	212.20 MB	0%
Automation - Base	2.1.720.60128	565.99 MB	0%
Cisco Catalyst Center UI	1.7.7.71	49.27 MB	0%
Cisco DNA Center Global Search	1.15.1.12	86.94 MB	0%
Cisco Identity Services Engine Bridge	2.1.716.90701	10.30 MB	0%
Cloud Connectivity - Contextual Content	2.11.2.542	208.71 MB	0%
Cloud Connectivity - Data Hub	1.15.57	19.81 MB	0%
Cloud Connectivity - Tethering	2.36.1.47	27.25 MB	0%
Disaster Recovery	2.1.720.360029	18.65 MB	0%
Documentation and Help	2.1.720.60128	118.04 MB	0%
NCP - Base	2.1.720.60128	365.58 MB	0%

SYSTEM

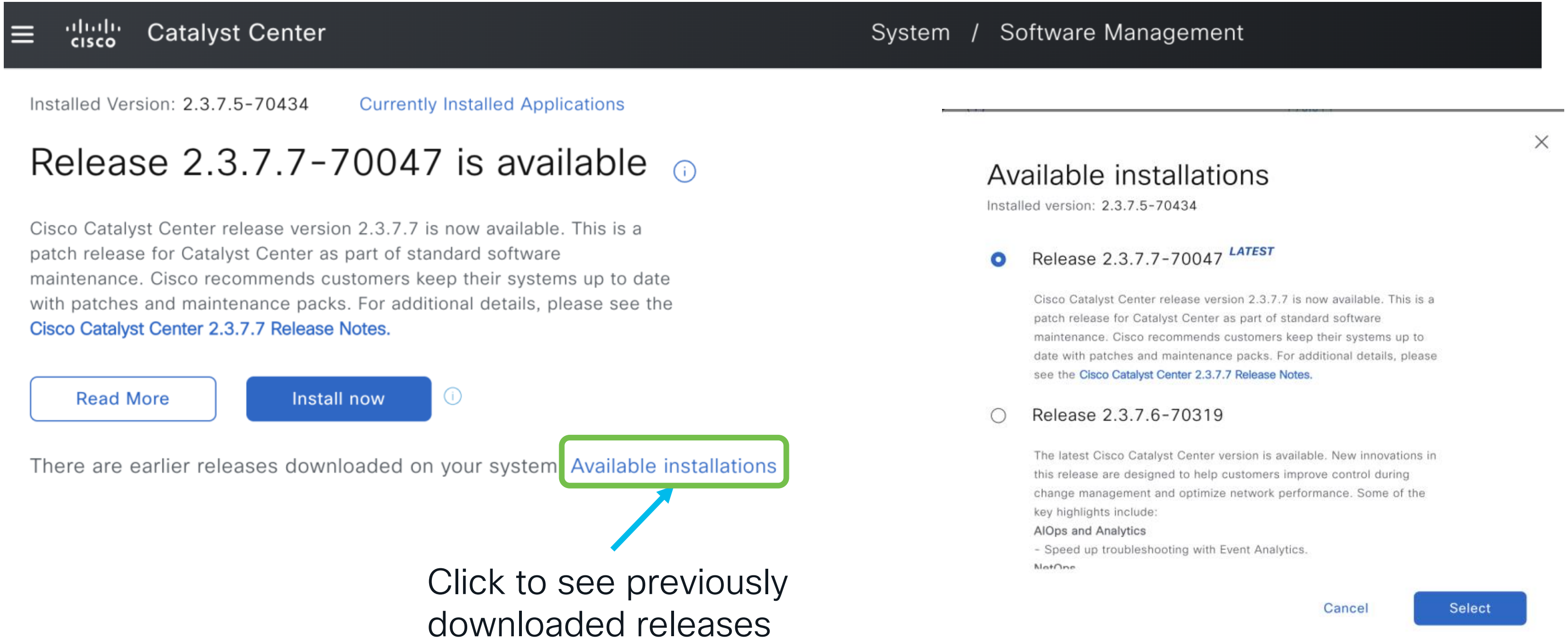
Application Name	Version	Size	Status
catalogserver	1.8.232	N/A	✓
main-system-package	1.8.232	N/A	46%
system-updater	1.8.232	N/A	80%

- Visibility into the packages being downloaded and overall downloaded percent
- The Catalyst Center is not locked during this step
- System packages downloaded first

The Upgrade Process

The New Way - Reduced to 2 Compulsory + 1 Optional Step

Release 2.3.x.x onwards



Installed Version: 2.3.7.5-70434 Currently Installed Applications

Release 2.3.7.7-70047 is available

Cisco Catalyst Center release version 2.3.7.7 is now available. This is a patch release for Catalyst Center as part of standard software maintenance. Cisco recommends customers keep their systems up to date with patches and maintenance packs. For additional details, please see the Cisco Catalyst Center 2.3.7.7 Release Notes.

There are earlier releases downloaded on your system Available installations

Available installations

Installed version: 2.3.7.5-70434

● Release 2.3.7.7-70047 LATEST

Cisco Catalyst Center release version 2.3.7.7 is now available. This is a patch release for Catalyst Center as part of standard software maintenance. Cisco recommends customers keep their systems up to date with patches and maintenance packs. For additional details, please see the Cisco Catalyst Center 2.3.7.7 Release Notes.

○ Release 2.3.7.6-70319

The latest Cisco Catalyst Center version is available. New innovations in this release are designed to help customers improve control during change management and optimize network performance. Some of the key highlights include:

AIOps and Analytics

- Speed up troubleshooting with Event Analytics.

NetOps

Click to see previously downloaded releases

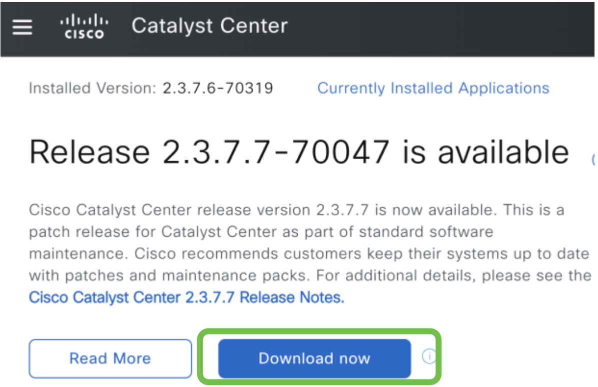
The Upgrade Process

The New Way - Reduced to 2 Compulsory + 1 Optional Step

Release 2.3.x.x onwards

Step 1. Click 'Download Now' to **download** the System & Application packages

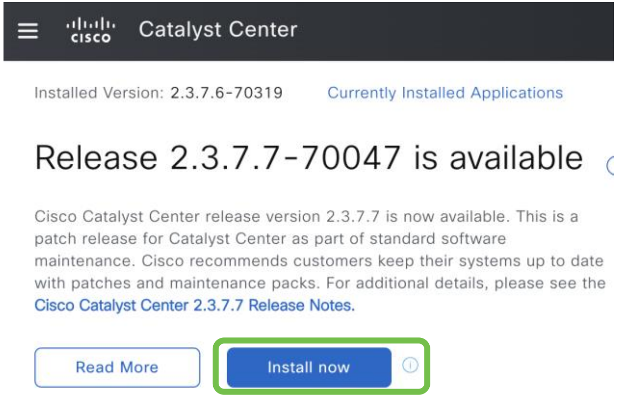
Step 2. Click 'Install Now' to **install** the System & Application packages



Installed Version: 2.3.7.6-70319 Currently Installed Applications

Release 2.3.7.7-70047 is available

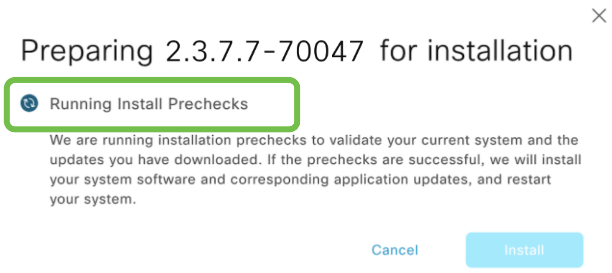
Cisco Catalyst Center release version 2.3.7.7 is now available. This is a patch release for Catalyst Center as part of standard software maintenance. Cisco recommends customers keep their systems up to date with patches and maintenance packs. For additional details, please see the Cisco Catalyst Center 2.3.7.7 Release Notes.



Installed Version: 2.3.7.6-70319 Currently Installed Applications

Release 2.3.7.7-70047 is available

Cisco Catalyst Center release version 2.3.7.7 is now available. This is a patch release for Catalyst Center as part of standard software maintenance. Cisco recommends customers keep their systems up to date with patches and maintenance packs. For additional details, please see the Cisco Catalyst Center 2.3.7.7 Release Notes.



Preparing 2.3.7.7-70047 for installation

Running Install Prechecks

We are running installation prechecks to validate your current system and the updates you have downloaded. If the prechecks are successful, we will install your system software and corresponding application updates, and restart your system.

System and Applications packages **downloaded** in the same step

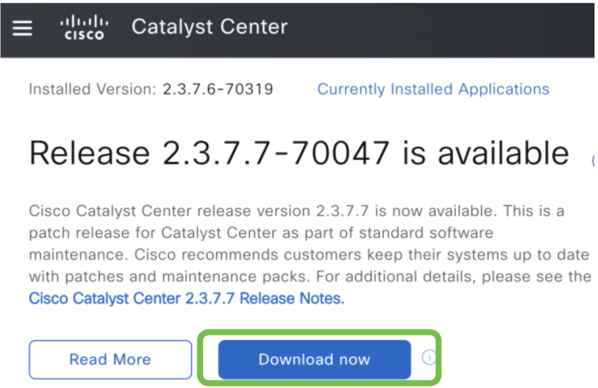
System and Applications packages **installed** in the same step

The Upgrade Process

The New Way - Reduced to 2 Compulsory + 1 Optional Step

Release 2.3.x.x onwards

Step 1. Click ‘Download Now’ to **download** the System & Application packages



Catalyst Center

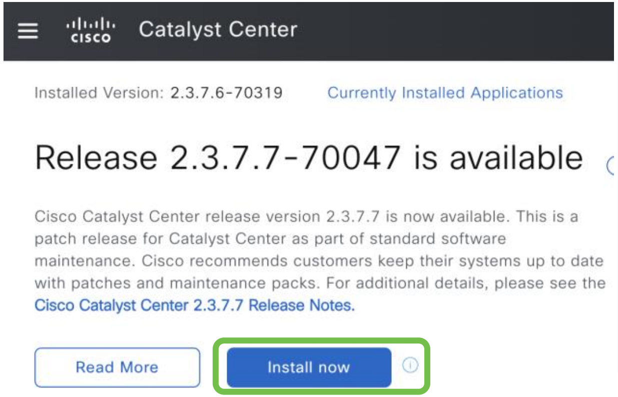
Installed Version: 2.3.7.6-70319 Currently Installed Applications

Release 2.3.7.7-70047 is available

Cisco Catalyst Center release version 2.3.7.7 is now available. This is a patch release for Catalyst Center as part of standard software maintenance. Cisco recommends customers keep their systems up to date with patches and maintenance packs. For additional details, please see the Cisco Catalyst Center 2.3.7.7 Release Notes.

System and Applications packages **downloaded** in the same step

Step 2. Click ‘Install Now’ to **install** the System & Application packages



Catalyst Center

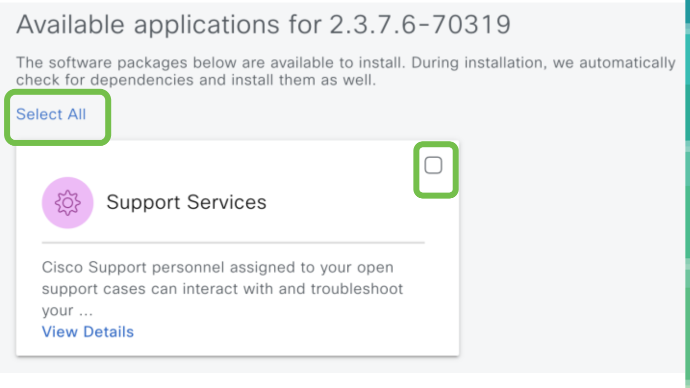
Installed Version: 2.3.7.6-70319 Currently Installed Applications

Release 2.3.7.7-70047 is available

Cisco Catalyst Center release version 2.3.7.7 is now available. This is a patch release for Catalyst Center as part of standard software maintenance. Cisco recommends customers keep their systems up to date with patches and maintenance packs. For additional details, please see the Cisco Catalyst Center 2.3.7.7 Release Notes.

System and Applications packages **installed** in the same step

Step 3 (optional). Install Optional Application packages



Available applications for 2.3.7.6-70319

The software packages below are available to install. During installation, we automatically check for dependencies and install them as well.

Cisco Support personnel assigned to your open support cases can interact with and troubleshoot your ...

Optional packages for the installed release at the bottom of the page

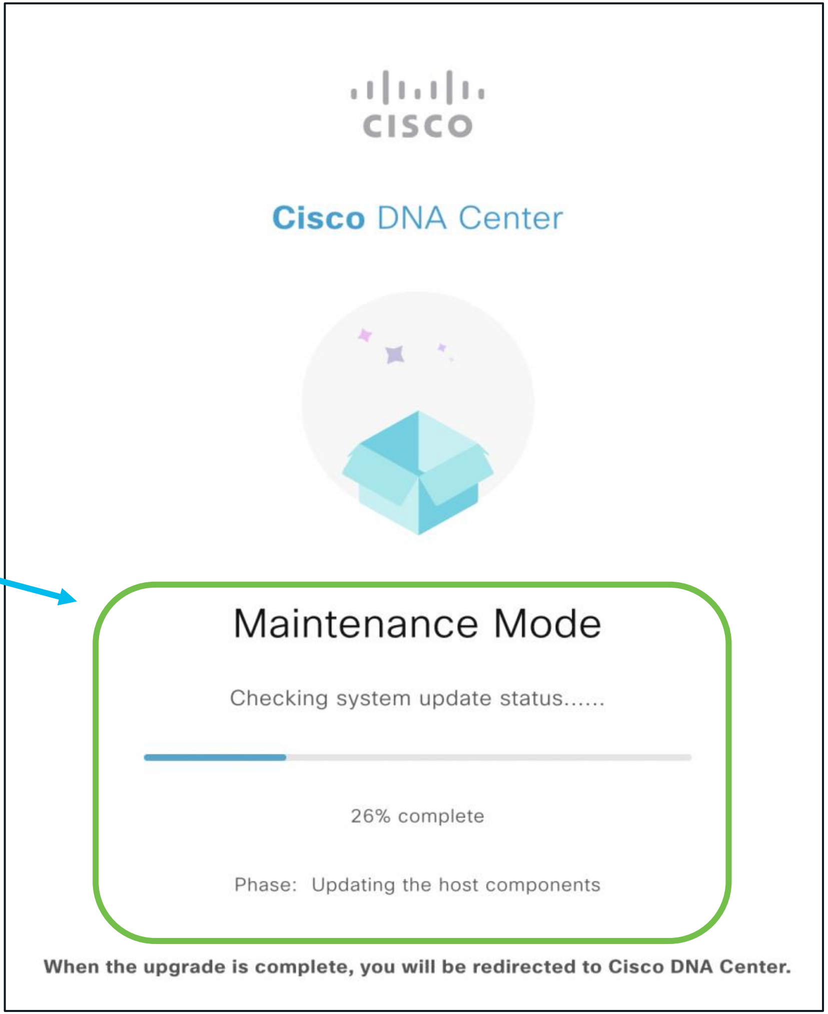
Software Upgrade Process Enhancements

Changes	2.2.x and below	Introduced in 2.3.x
Choosing a Target Release	• Either the latest patch release or the next available release • Can be confusing	• Multiple options • Easy to understand single drop down window
Upgrade Process (compulsory steps)	3 Steps 1. Click 'Update' to upgrade the System packages 2. Click 'Download All' to download the Applications packages 3. Click 'Update All' to upgrade the Applications packages	2 Steps 1. Click 'Download' to download all packages (System + Applications) 2. Click 'Install' to install all packages (System + Applications)
Prechecks	No Prechecks part of Workflow	Prechecks added as part of workflow (prior to step 1 & 2)
Maintenance Mode (UI is not accessible in this mode)	Recommended not to use the Cisco Catalyst Center from Step 1 (Maintenance mode from Step 1)	Recommended not to use the Cisco Catalyst Center from Step 2 (Maintenance mode from Step 2)

The Upgrade Process

- Monitoring from UI

- UI is locked
- Monitoring the upgrade process via UI
- Chrome browser recommended



Maintenance Mode

Checking system update status......

26% complete

Phase: Updating the host components

When the upgrade is complete, you will be redirected to Cisco DNA Center.

Its Monday morning and you are still stuck in maintenance mode

The Upgrade Process

Monitoring and Troubleshooting System Upgrade

1. System Upgrade

Main Maglev Services

- catalogserver
- system-updater
- maglevserver
- workflow-worker

2. Applications Upgrade

Monitoring the System Upgrade progress

New commands from 2.3.x

```
$ maglev system_update progress

INSTALLED_VERSION    CURRENTLY_PROCESSED_VERSION    CURRENT_PHASE
UPDATE_PROGRESS_PERCENT    CURRENT_PHASE_DETAILS
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
1.8.222              1.8.222                                   successful
100                          The system has been successfully updated
```

```
$ maglev system_update progress --legacy
$ maglev system_updater update_info
```

Command prior to 2.3.x

```
System update status:
  Version successfully installed : 1.8.222

  Updater State:
    Currently processed version   : NONE
    State                         : IDLE
    Sub-State                     : NONE
    Details                       : The system has been successfully updated
    Source                        : system-updater
    Abort pending                 : False
```

*These commands can show tracebacks during the upgrade process, this is normal. Try again later.

The Upgrade Process

Monitoring and Troubleshooting System Upgrade

1. System Upgrade
   - a. Preparation (0% to 31%)
   - b. Upgrade (32% to 94%)
   - c. Post Upgrade (95% to 100%)
2. Applications Upgrade

*The percentages vary based on version

Preparation: (0-6%) Maintenance mode, System update hooks downloading and installation, download & upgrade of Services catalogserver, systemupdater

```
$ maglev system_updater update_info
System update status:
  Version successfully installed : 1.7.1013
  Version currently processed    : 1.8.222
    Update phase                 : Installing System updater pre update
hooks
    Update details               : Deploying hooks for pre system update
    Progress                     : 1%

  Updater State:
    Currently processed version  : 1.8.222
    State                        : HANDLE_PREINIT_HOOKS
    Sub-State                    : DOWNLOADED_HOOKS
    Details                      : Deploying hooks for pre system update
    Source                       : system-updater
    Abort pending                : False
```

The Upgrade Process

Monitoring and Troubleshooting System Upgrade

1. System Upgrade

   a. Preparation (0% to 31%)

   b. Upgrade (32% to 94%)

   c. Post Upgrade (95% to 100%)

2. Applications Upgrade

Preparation: Download packages to the Nodes (7% - 30%)

```
$ maglev system_updater update_info
System update status:
  Version successfully installed : 1.7.1013
  Version currently processed    : 1.8.222
    Update phase                 : Downloading the host update packages
    Update details               : Copying the host packages to all the
nodes
    Progress                     : 7%

  Updater State:
    Currently processed version  : 1.8.222
    State                        : DOWNLOADING_UPDATES
    Sub-State                    : INSTALLED_SYSTEMUPDATER
    Details                      : Downloading the host components
    Source                       : system-updater
    Abort pending                : False
```

The Upgrade Process

Monitoring and Troubleshooting System Upgrade

1. System Upgrade
   - a. Preparation (0% to 31%)
   - b. Upgrade (32% to 94%)
   - c. Post Upgrade (95% to 100%)
2. Applications Upgrade

Preparation: Applications are shut down (31%)

```
$ maglev system_updater update_info
System update status:
  Version successfully installed : 1.7.1013
  Version currently processed    : 1.8.222
    Update phase                 : Disabling the applications
    Update details               : Disabling user applications
    Progress                     : 31%

  Updater State:
    Currently processed version  : 1.8.222
    State                        : DOWNLOADING_UPDATES
    Sub-State                    : DOWNLOADED_MAIN_PACKAGE
    Details                      : Disabling user applications
    Source                       : system-updater
    Abort pending                : False
```

Most upgrade related field issues are seen till this point

The Upgrade Process

Monitoring and Troubleshooting System Upgrade

1. System Upgrade
   a. Preparation (0% to 31%)
   b. Upgrade (32% to 94%)
   c. Post Upgrade(95% to 100%)
2. Applications Upgrade

Broken down into multiple sub phases

- Quick check of the system

memory requirements in '/' and 'data', NTP service, old file clean-ups, system setting changes… (upgrade can fail at this stage if requirements are not met)

- Upgrade Linux Kernel, Docker & Kubernetes
- Upgrade Maglev Server & its Services (Kong, Rabbitmq, Glusterfs, Mongodb, Cassandra…)
- Certificates refresh
- Check Cluster health

- Nodes are upgraded one at a time in a cluster
- Multiple checks and balances in place
- Restart is usually after Linux Kernel upgrade and after Kubernetes upgrade (if required)

The Upgrade Process

Monitoring and Troubleshooting System Upgrade

1. System Upgrade
   a. Preparation (0% to 31%)
   b. Upgrade (32% to 94%)
   c. Post Upgrade (95% to 100%)
2. Applications Upgrade

System Upgrade in progress (32% - 94%)

```
$ maglev system_updater update_info
System update status:
  Version successfully installed : 1.7.1013
  Version currently processed    : 1.8.222
    Update phase                 : failed
    Update details               : Updating node 10.10.10.10 failed
    Progress                     : 34%

  Updater State:
    Currently processed version  : 1.8.222
    State                        : FAILED
    Sub-State                    : INSTALLED_HOST_COMPONENTS
    Details                      : Updating node 10.10.10.10 failed
    Source                       : system-updater
    Abort pending                : False
```

Systemd Services to upgrade Linux, K8S…

- maglev-node-updater
- maglev-hook-installer

Logs

- magctl service logs -r system-updater
- cat log/maglev-node-updater-<IP Addr>.log
- cat log/maglev-hook-installer.log

The Upgrade Process

Monitoring and Troubleshooting System Upgrade

1. System Upgrade
   a. Preparation (0% to 31%)
   b. Upgrade (32% to 94%)
   c. Post Upgrade (95% to 100%)
2. Applications Upgrade

System Upgrade in progress (32% - 94%)

```
System-updater logs:

| 2004 | 2025-01-30T00:56:41.565Z | ERROR | 57 | ThreadPoolExecutor-4_2 |
140303126214400 | node-updater | node_updater.py:709 | Node update took
longer to complete in node 169.254.1.21 |
| 2005 | 2025-01-30T00:56:41.589Z | ERROR | 57 | MainThread |
140304732464960 | system-updater | system_update_orchestrator.py:452 |
Status: 1/Node update took longer to complete in 169.254.1.21
```

Systemd Services to upgrade Linux, K8S…

- maglev-node-updater
- maglev-hook-installer

Logs

- magctl service logs -r system-updater
- cat log/maglev-node-updater-<IP Addr>.log
- cat log/maglev-hook-installer.log

The Upgrade Process

Monitoring and Troubleshooting System Upgrade

1. System Upgrade
   - a. Preparation (0% to 31%)
   - b. Upgrade (32% to 94%)
   - c. Post Upgrade (95% to 100%)
2. Applications Upgrade

System upgrade completed

```
$ maglev system_updater update_info
System update status:
  Version successfully installed : 1.8.222

  Updater State:
    Currently processed version  : 1.8.222
    State                        : INSTALLING_UPDATES
    Sub-State                    : COMPLETED
    Details                      : The system has been successfully updated
    Source                       : system-updater
    Abort pending                : False
```

The Upgrade Process

Monitoring and Troubleshooting System Upgrade

1. System Upgrade
    a. Preparation (0% to 31%)
    b. Upgrade (32% to 94%)
    c. Post Upgrade (95% to 100%)
2. Applications Upgrade

Applications upgrade starts after System Upgrade

```
$ maglev package status
NAME                             DISPLAY_NAME
DEPLOYED        AVAILABLE         STATUS                         PROGRESS
------------------------------------------------------------------------------
-------------------------------------------------------------
network-visibility          Network Controller Platform
2.1.718.60779   2.1.720.60128 DEPLOYED
…
```

Applications upgrade - Failure

```
...
network-visibility          Network Controller Platform
2.1.718.60779   2.1.720.60128   UPGRADE_ERROR - Exception in task - Maximum
wait time 5400 seconds exceeded for the following services to be ready:
apic-em-pki-broker-service
```

Maglev Services to upgrade Applications

- workflow-worker
- maglev-server

Logs

- magctl service logs -r <affected application >
- magctl appstack status ← view all the services and status
- maglev package status

The Upgrade Process

Monitoring and Troubleshooting System Upgrade

1. System Upgrade

   a. Preparation (0% to 31%)

   b. Upgrade (32% to 94%)

   c. Post Upgrade (95% to 100%)

2. Applications Upgrade

Failure troubleshooting

```
$ magctl appstack status
NAMESPACE                          NAME
READY    STATUS       RESTARTS   AGE      IP                NODE             NOMINATED NODE
READINESS GATES
fusion                             apic-em-pki-broker-service-595ddd545b-txqnt
1/2      Running      93          6d4h    169.254.41.122    10.128.249.10    <none>
<none>

Service apic-em-pki-broker-service logs:

2025-01-24 07:06:29,791 |  ERROR | pool-4-thread-1            |  |
c.c.e.pki.impl.utils.MakeRestCalls | There was an exception while connecting to the URL
http://localhost:16029/pki-is-ejbca-ready |
2025-01-24 07:06:30,828 |  ERROR | main                       |  |
c.c.grapevine.api.SecurityManager | DiskConfig file:/media/floppy/config.json not found.
|
```

Maglev Services to upgrade Applications

- workflow-worker
- maglev-server

Logs

- magctl service logs -r <affected application >
- magctl appstack status ← view all the services and status
- maglev package status

The Upgrade Process

Monitoring and Troubleshooting System Upgrade

1. System Upgrade

Monitoring Services involved in the System upgrade

```
magctl service logs -r maglevserver
magctl service logs -r system-updater
magctl service logs -r workflow-worker
```

Node Agnostic

```
cat log/maglev-node-updater-<IP Addr>.log
cat log/maglev-hook-installer.log
```

Node Specific

```
* Use flags -rf for live logs or -r to dump all the logs on screen/file
```

2. Applications Upgrade

Monitoring Services involved in the Applications upgrade

```
magctl service logs -r maglevserver
magctl service logs -r workflow-worker
magctl service status [service name]
maglev package status
```

Node Agnostic

```
* Use flags -rf for live logs or -r to dump all the logs on screen/file
```

The Upgrade Process (Prerequisites)

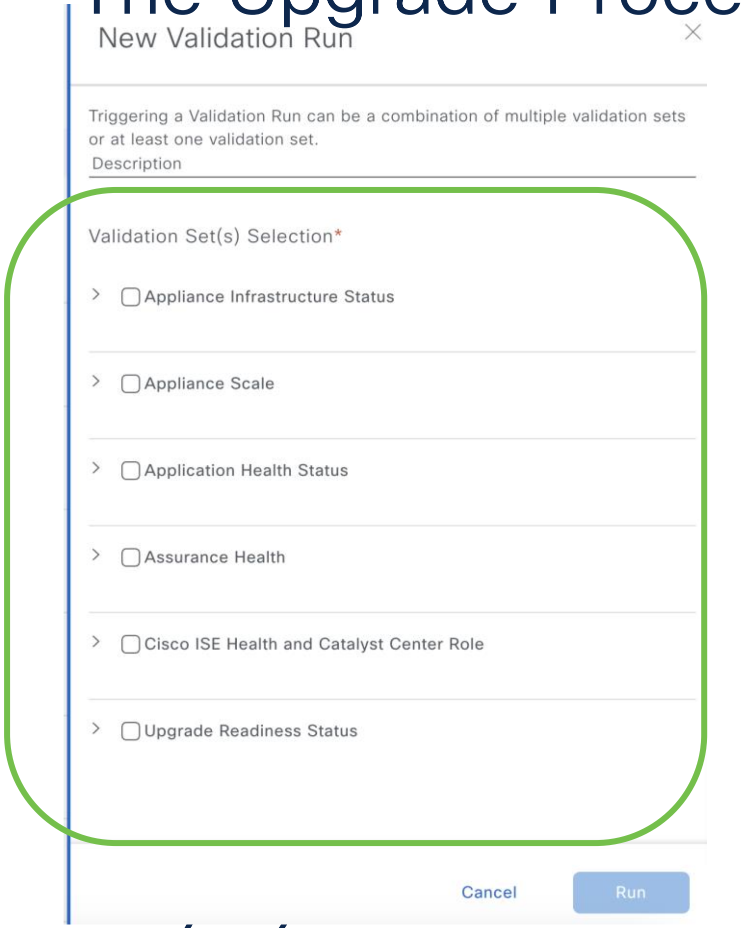
- Healthy Backup
- Healthy Hardware
- Open required ports on the Firewall
- Prechecks:
  - 1.2.8 to 2.3.3.x > AURA from every node OR
  - 2.3.5.x > Validation Tool

(validated by the tools and part of upgrade prechecks - NTP synced, DNS resolution, Valid internal Certificates, Catalogserver settings, Memory requirements, Proxy settings, Known software bugs that have a signature ...)

- Google Chrome Recommended
- Contact TAC for resolution of errors/warnings from AURA, Validation Tool or Upgrade failures
- Contact Customer Success for upgrade assistance
- Choose the target release and the upgrade path (N-2 supported)
- Network device compatibility (SDA)
- Upgrade Guide on Cisco.com

*There is no option to switch back to an earlier release once the upgrade has started

The Upgrade Process (Post Checks)



New Validation Run

Triggering a Validation Run can be a combination of multiple validation sets or at least one validation set.

Description

Validation Set(s) Selection*

- › □ Appliance Infrastructure Status
- › □ Appliance Scale
- › □ Application Health Status
- › □ Assurance Health
- › □ Cisco ISE Health and Catalyst Center Role
- › □ Upgrade Readiness Status

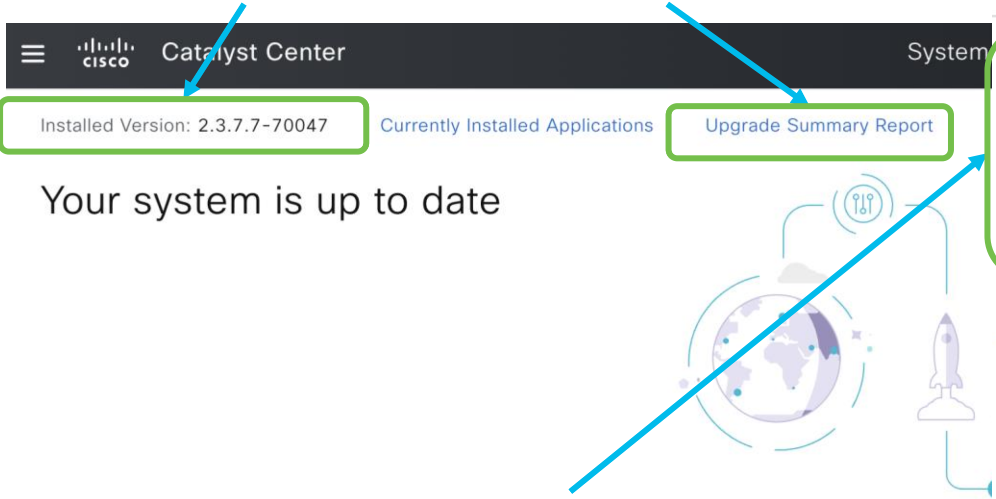
System Health / Validation Tool

- Execute another round of Validation tool with all validation sets after upgrade

The Upgrade Process (Post Checks)

Installed Version

Introduced in 2.3.7.7



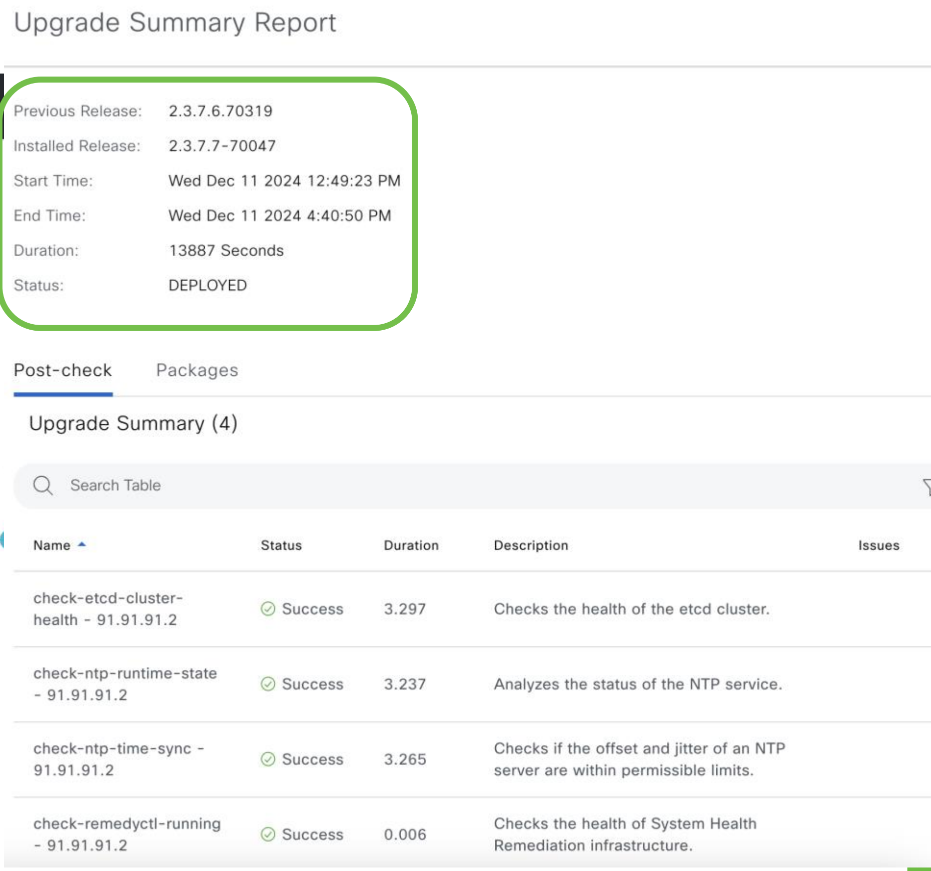
Installed Version: 2.3.7.7-70047

Currently Installed Applications

Upgrade Summary Report

Your system is up to date

A summary of the most recent upgrade with timestamps



Upgrade Summary Report

Previous Release:	2.3.7.6.70319
Installed Release:	2.3.7.7-70047
Start Time:	Wed Dec 11 2024 12:49:23 PM
End Time:	Wed Dec 11 2024 4:40:50 PM
Duration:	13887 Seconds
Status:	DEPLOYED

Upgrade Summary (4)

Name ▲	Status	Duration	Description	Issues
check-etcd-cluster-health - 91.91.91.2	✓ Success	3.297	Checks the health of the etcd cluster.	
check-ntp-runtime-state - 91.91.91.2	✓ Success	3.237	Analyzes the status of the NTP service.	
check-ntp-time-sync - 91.91.91.2	✓ Success	3.265	Checks if the offset and jitter of an NTP server are within permissible limits.	
check-remedyctl-running - 91.91.91.2	✓ Success	0.006	Checks the health of System Health Remediation infrastructure.	

Catalyst Center Health (Reference)

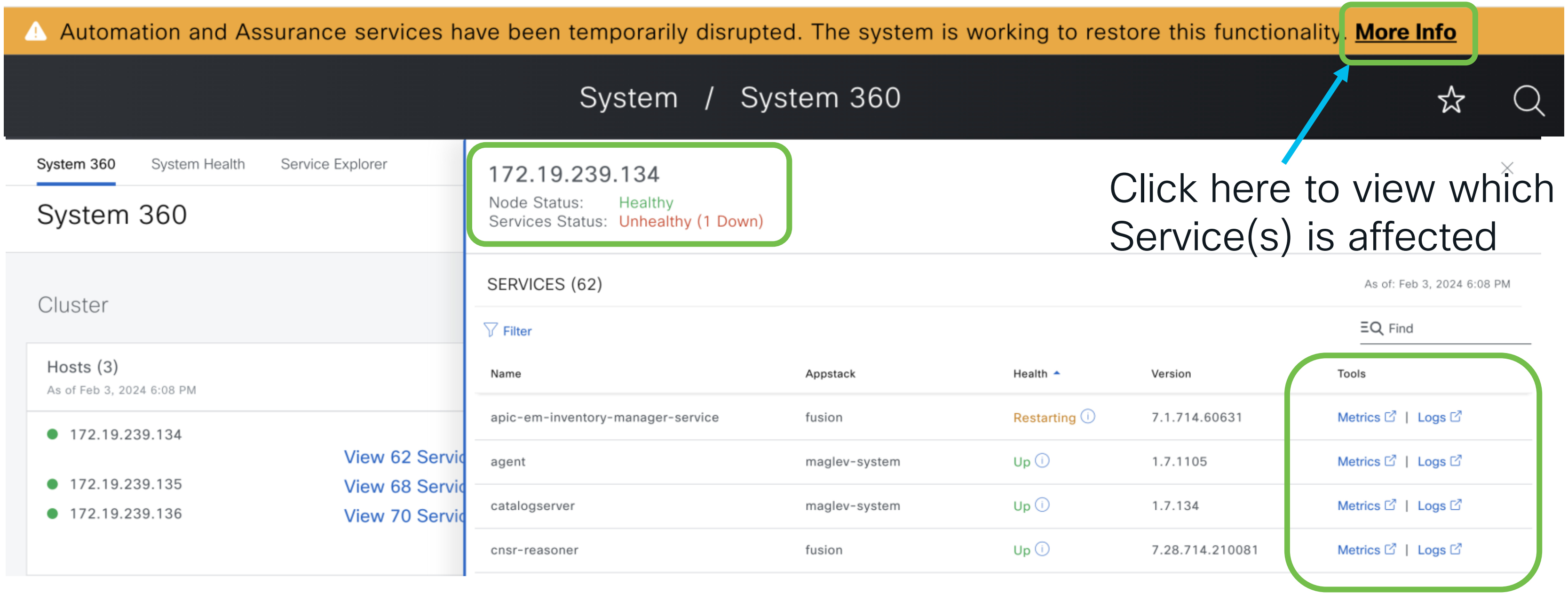
System / System 360

Release 2.2.x Onwards

System in Self Monitoring Mode

Software Services

Banner at the top of the screen indicating one or more Services are down.



⚠ Automation and Assurance services have been temporarily disrupted. The system is working to restore this functionality. **More Info**

System / System 360

System 360 | System Health | Service Explorer

System 360

Cluster

Hosts (3)
As of Feb 3, 2024 6:08 PM

● 172.19.239.134 — View 62 Servic
● 172.19.239.135 — View 68 Servic
● 172.19.239.136 — View 70 Servic

172.19.239.134
Node Status: Healthy
Services Status: Unhealthy (1 Down)

SERVICES (62)

As of: Feb 3, 2024 6:08 PM

Filter

Find

Name	Appstack	Health ▲	Version	Tools
apic-em-inventory-manager-service	fusion	Restarting ⓘ	7.1.714.60631	Metrics ↗ | Logs ↗
agent	maglev-system	Up ⓘ	1.7.1105	Metrics ↗ | Logs ↗
catalogserver	maglev-system	Up ⓘ	1.7.134	Metrics ↗ | Logs ↗
cnsr-reasoner	fusion	Up ⓘ	7.28.714.210081	Metrics ↗ | Logs ↗

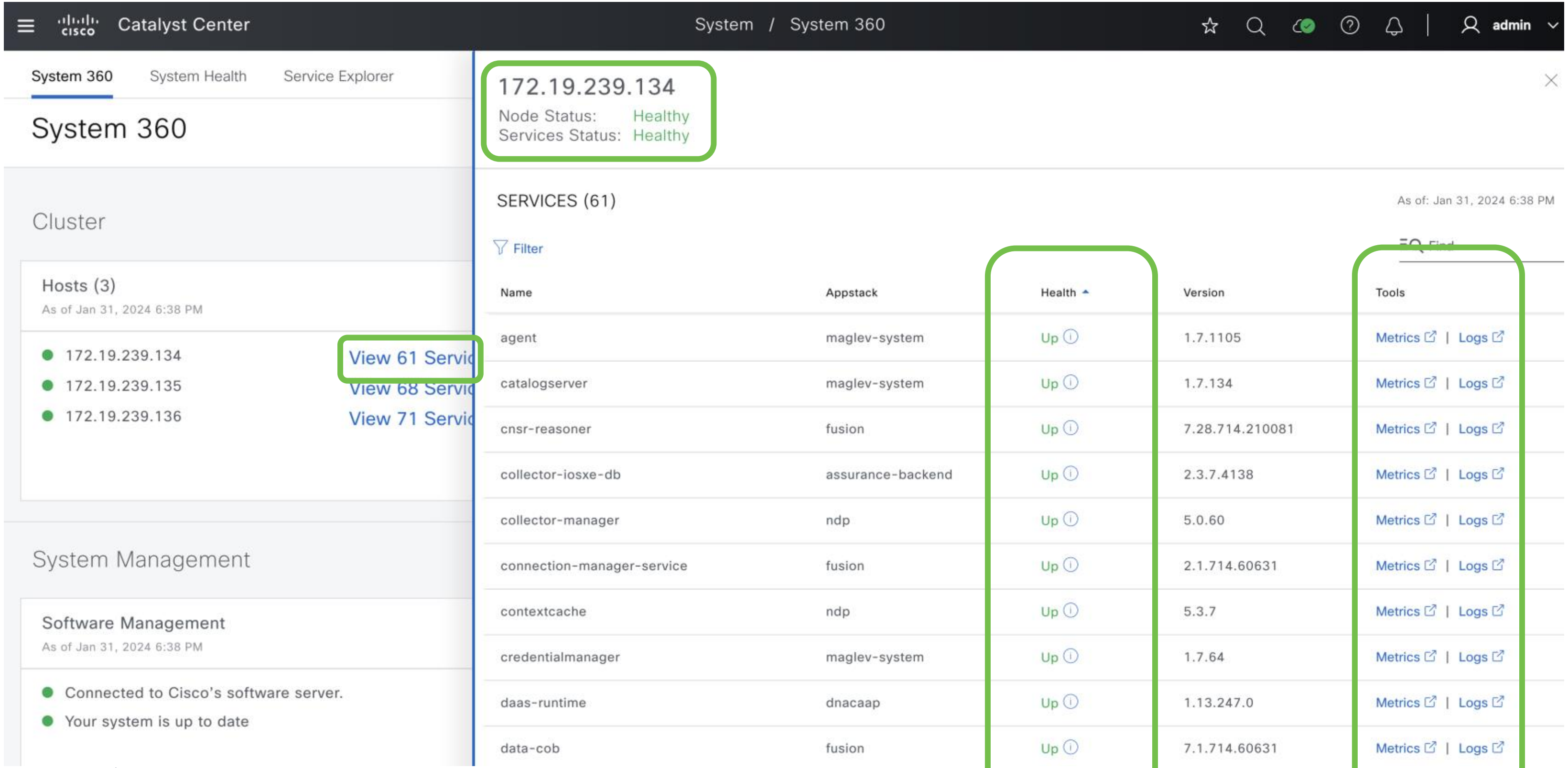
Click here to view which Service(s) is affected

System / System 360

Release 2.2.x Onwards

System in Self Monitoring Mode

Software Services



Catalyst Center — System / System 360 — admin

System 360 | System Health | Service Explorer

System 360

Cluster

Hosts (3)
As of Jan 31, 2024 6:38 PM

- ● 172.19.239.134 — View 61 Servic
- ● 172.19.239.135 — View 68 Servic
- ● 172.19.239.136 — View 71 Servic

System Management

Software Management
As of Jan 31, 2024 6:38 PM

- ● Connected to Cisco's software server.
- ● Your system is up to date

172.19.239.134
Node Status: Healthy
Services Status: Healthy

SERVICES (61)

As of: Jan 31, 2024 6:38 PM

Filter

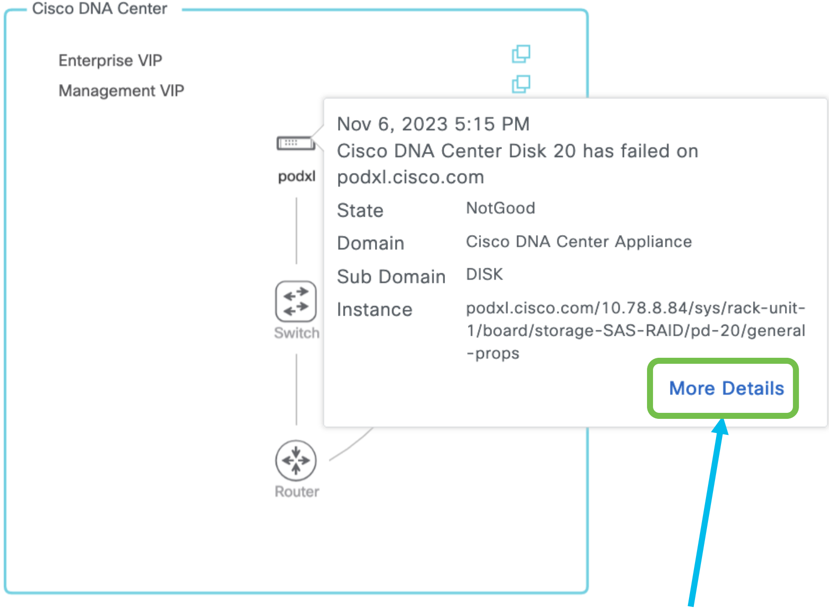
Name	Appstack	Health ▲	Version	Tools
agent	maglev-system	Up ⓘ	1.7.1105	Metrics ↗ | Logs ↗
catalogserver	maglev-system	Up ⓘ	1.7.134	Metrics ↗ | Logs ↗
cnsr-reasoner	fusion	Up ⓘ	7.28.714.210081	Metrics ↗ | Logs ↗
collector-iosxe-db	assurance-backend	Up ⓘ	2.3.7.4138	Metrics ↗ | Logs ↗
collector-manager	ndp	Up ⓘ	5.0.60	Metrics ↗ | Logs ↗
connection-manager-service	fusion	Up ⓘ	2.1.714.60631	Metrics ↗ | Logs ↗
contextcache	ndp	Up ⓘ	5.3.7	Metrics ↗ | Logs ↗
credentialmanager	maglev-system	Up ⓘ	1.7.64	Metrics ↗ | Logs ↗
daas-runtime	dnacaap	Up ⓘ	1.13.247.0	Metrics ↗ | Logs ↗
data-cob	fusion	Up ⓘ	7.1.714.60631	Metrics ↗ | Logs ↗

System / System 360

Release 2.3.5.x Onwards

System in Self Monitoring Mode

Hardware Health



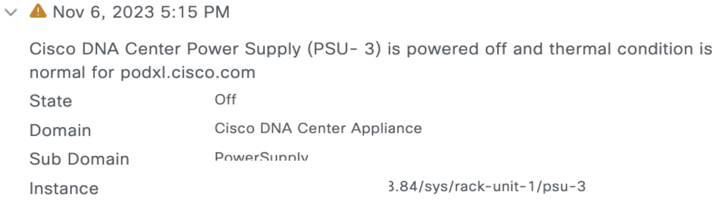
Nov 6, 2023 5:15 PM
Cisco DNA Center Disk 20 has failed on podxl.cisco.com

State	NotGood
Domain	Cisco DNA Center Appliance
Sub Domain	DISK
Instance	podxl.cisco.com/10.78.8.84/sys/rack-unit-1/board/storage-SAS-RAID/pd-20/general-props

More Details

Click here to view additional details

Power Supply powered off

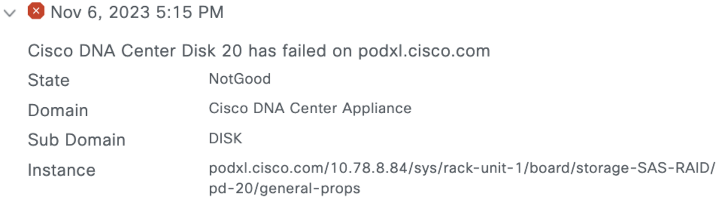


Nov 6, 2023 5:15 PM

Cisco DNA Center Power Supply (PSU- 3) is powered off and thermal condition is normal for podxl.cisco.com

State	Off
Domain	Cisco DNA Center Appliance
Sub Domain	PowerSupply
Instance	3.84/sys/rack-unit-1/psu-3

Disk / Raid failure



Nov 6, 2023 5:15 PM

Cisco DNA Center Disk 20 has failed on podxl.cisco.com

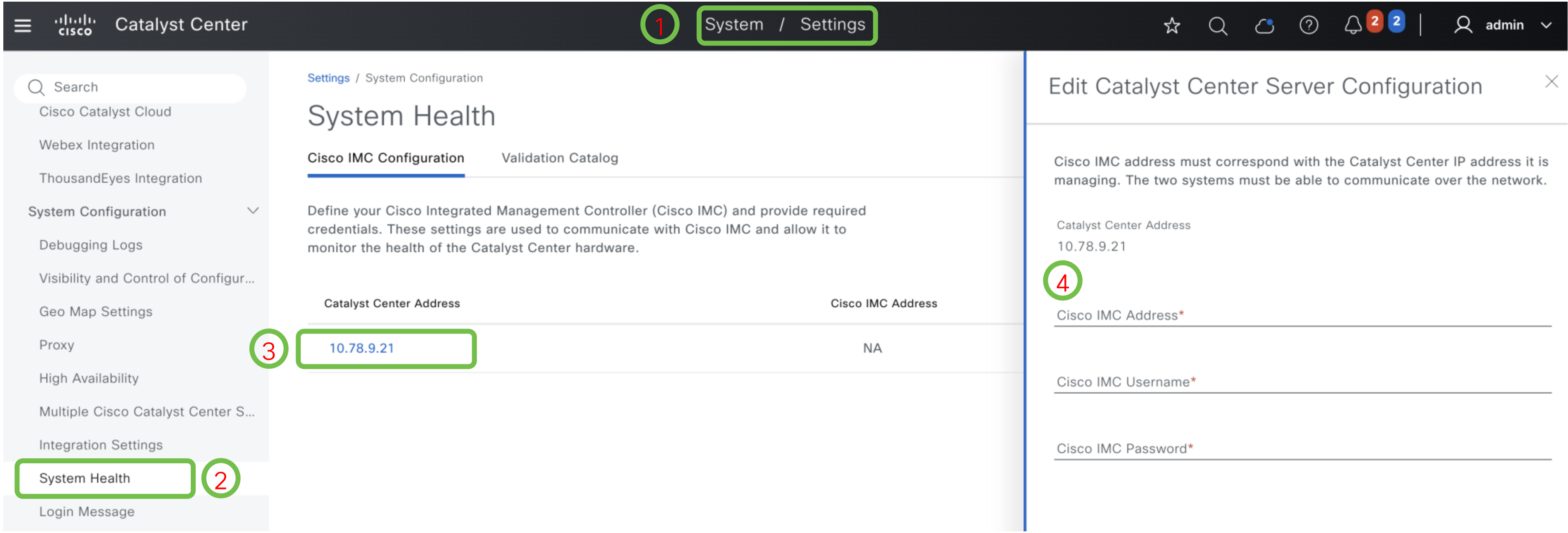
State	NotGood
Domain	Cisco DNA Center Appliance
Sub Domain	DISK
Instance	podxl.cisco.com/10.78.8.84/sys/rack-unit-1/board/storage-SAS-RAID/pd-20/general-props

System / Settings

Release 2.3.5.x Onwards

System in Self Monitoring Mode

Hardware Health



System Health

Cisco IMC Configuration | Validation Catalog

Define your Cisco Integrated Management Controller (Cisco IMC) and provide required credentials. These settings are used to communicate with Cisco IMC and allow it to monitor the health of the Catalyst Center hardware.

Catalyst Center Address	Cisco IMC Address
10.78.9.21	NA

Edit Catalyst Center Server Configuration

Cisco IMC address must correspond with the Catalyst Center IP address it is managing. The two systems must be able to communicate over the network.

Catalyst Center Address
10.78.9.21

Cisco IMC Address*

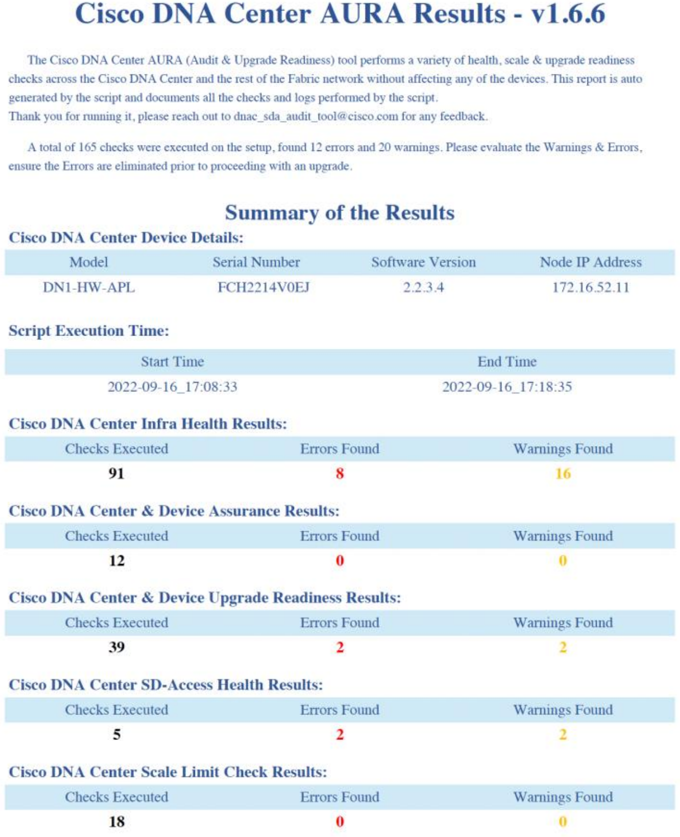
Cisco IMC Username*

Cisco IMC Password*

AURA - Health Checker Tool

Release 1.2.8 to 2.3.5.x

- **AURA** is our tool that covers health, scale & upgrade readiness checks across the Use Cases
- Simple & Straight Forward:
  - Copy **one** executable file to the Catalyst Center and execute it on the Catalyst Center
  - Using existing pre-installed libraries/software ONLY
  - Only input required – Catalyst Center passwords
  - Automatically generated PDF report & Zipped Log file that can be automatically uploaded to Cisco SR
  - **Not Intrusive** – only DB reads, show commands and API calls
- Execution time: Each node <15mins. SDA=depends on scale (approx. 30min for 30 SDA Devices)
- Built in APAC and adopted across Cisco Internal teams, Partners and Customers globally



Cisco DNA Center AURA Results - v1.6.6

The Cisco DNA Center AURA (Audit & Upgrade Readiness) tool performs a variety of health, scale & upgrade readiness checks across the Cisco DNA Center and the rest of the Fabric network without affecting any of the devices. This report is auto generated by the script and documents all the checks and logs performed by the script.
Thank you for running it, please reach out to dnac_sda_audit_tool@cisco.com for any feedback.

A total of 165 checks were executed on the setup, found 12 errors and 20 warnings. Please evaluate the Warnings & Errors, ensure the Errors are eliminated prior to proceeding with an upgrade.

Summary of the Results

Cisco DNA Center Device Details:

Model	Serial Number	Software Version	Node IP Address
DN1-HW-APL	FCH2214V0EJ	2.2.3.4	172.16.52.11

Script Execution Time:

Start Time	End Time
2022-09-16_17:08:33	2022-09-16_17:18:35

Cisco DNA Center Infra Health Results:

Checks Executed	Errors Found	Warnings Found
91	**8**	**16**

Cisco DNA Center & Device Assurance Results:

Checks Executed	Errors Found	Warnings Found
12	**0**	**0**

Cisco DNA Center & Device Upgrade Readiness Results:

Checks Executed	Errors Found	Warnings Found
39	**2**	**2**

Cisco DNA Center SD-Access Health Results:

Checks Executed	Errors Found	Warnings Found
5	**2**	**2**

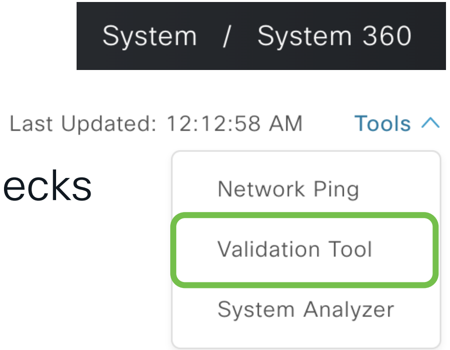
Cisco DNA Center Scale Limit Check Results:

Checks Executed	Errors Found	Warnings Found
18	**0**	**0**

Validation Tool

Release 2.3.5.x Onwards

- On Demand Cisco Catalyst Center Health Checks



☐ Appliance Infrastructure Status

- System software update mode (online/offline)
- Cluster - member identifier
- Cluster - hostname
- Kubelet status
- Docker status
- DNS resolution status
- DNS reachability status
- Check and verify DNS server configuration requirements
- CPU utilization - Cluster average
- Memory utilization - Cluster average
- CCO credentials configuration status
- Appstack status
- Filesystem utilization status
- Cassandra service status
- Elasticsearch service (maglev-system appstack) status
- Elasticsearch service (ndp appstack) status
- GlusterFS service status
- InfluxDB service status
- MongoDB service status
- Postgres service status
- RabbitMQ service status
- Zookeeper service status
- Health of Kafka service (ndp appstack)
- Health of Redis service
- Cluster node(s) status
- Processor units status
- Memory units status
- Storage units status
- Network adapter units status
- Storage virtual drives status
- Power supply units status
- Kubernetes Node Diagnosis - Memory Pressure, Disk Pressure, PID Pressure, Kubelet Ready

☐ Appliance Scale

- Total device count
- Wired device (switches and hubs + routers + wireless controllers) count
- Wireless device (access Points + sensors) count
- Physical port count
- Interface count
- Total client count (concurrent)
- Wired client count (concurrent)
- Wireless client count (concurrent)
- Transient client count
- Site count
- IP pool count
- Netflows count
- Policies count
- Security groups count

☐ Assurance Health

- Assurance NSA webapp health
- If there are any devices in inventory
- Failed or unassigned devices in inventory
- Assurance and related service(s) health
- Assurance pipeline(s) health
- Processing lags for Assurance and related pipelines
- The memory utilization of Assurance services
- The cpu utilization of Assurance services
- Assurance collectors are receiving data
- Wireless client roaming count per second does not exceed the supported limit
- Client count does not exceed the supported limit
- Device count does not exceed the supported limit
- Assurance is performing client health computations
- Assurance client and device APIs are running
- Assurance is performing device health computations

☐ Cisco ISE Health and Cisco DNA Center Role

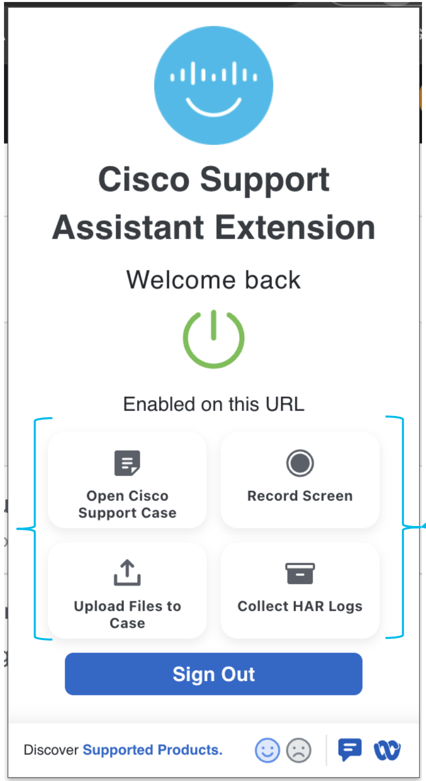
- Cisco ISE Health Status
- Cisco DNA Center role (*applicable only on Multiple Cisco DNA Center enabled deployment)
- Group Based Policy Migration Status

☐ Upgrade Readiness Status

- System software update mode (online/offline)
- Catalog server settings
- Catalog server repository settings
- Catalog override default repository settings
- HTTP proxy configuration settings
- Catalog server connectivity status
- HTTP proxy reachability status
- Backup status (backup success < than 1 week)
- Service(s) - Operational status
- Service(s) - Restart counts for the past 24 hours
- Pods - Operational status
- Disk storage available - root directory
- Disk storage available - data directory
- Exited pod(s) count
- System certificate status
- Authentication and Policy servers configuration and status
- Workflow status
- Release status

Release 2.3.5.x onwards

Cisco Support Assistant Extension



Cisco Support Assistant Extension

Welcome back

Enabled on this URL

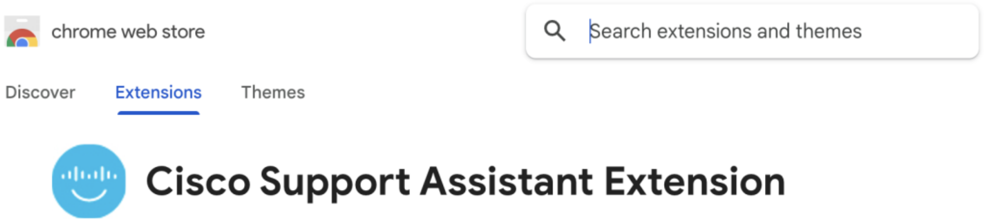
Discover **Supported Products.**

Common features enabled across multiple products

Supported Browsers

Google Chrome

Microsoft Edge



Cisco Support Assistant Extension

Other Supported Products/Webpages

Cisco Secure Firewall (v7.0+)

Cisco Catalyst 9800 Series WLC

Cisco XDR

Secure Endpoint

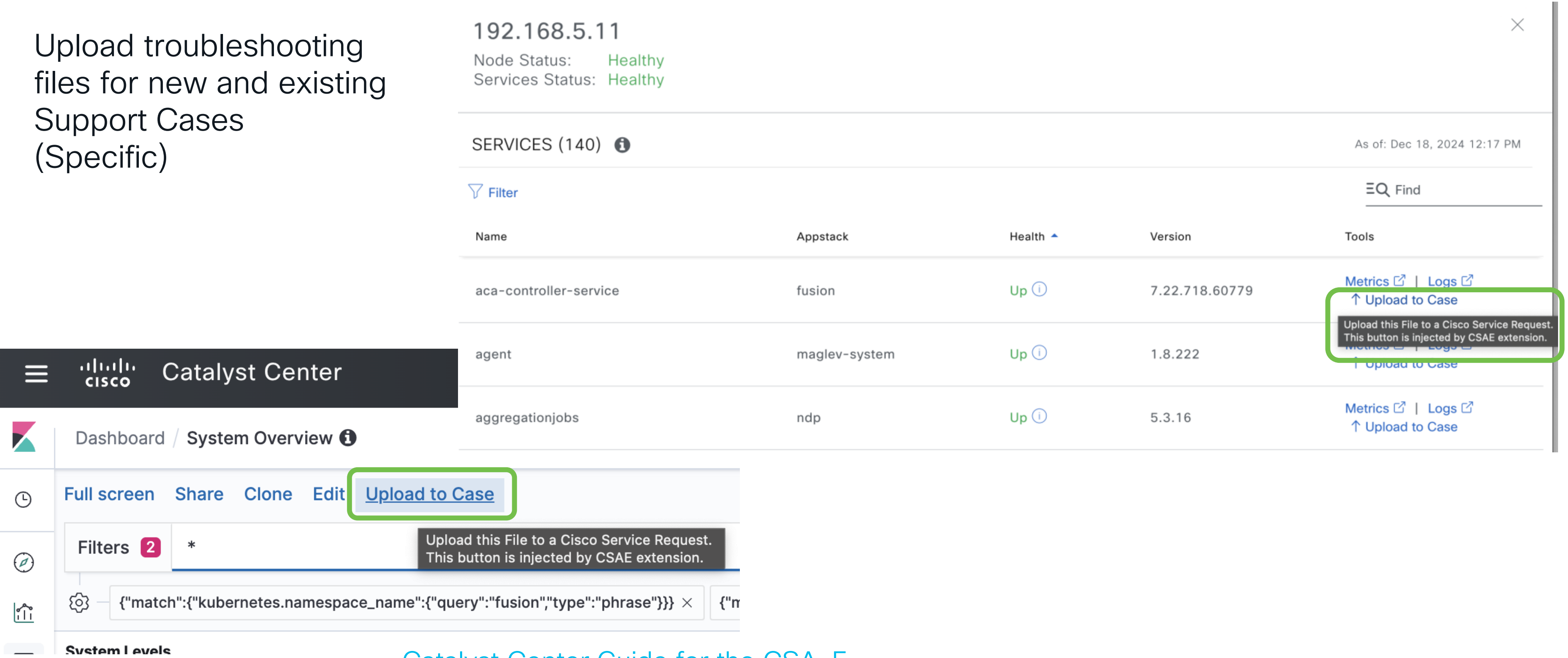
Field Notice Pages

Catalyst Center Guide for the CSA-E

Release 2.3.5.x onwards

Cisco Support Assistant Extension

Upload troubleshooting files for new and existing Support Cases (Specific)



192.168.5.11

Node Status: Healthy
Services Status: Healthy

SERVICES (140)

As of: Dec 18, 2024 12:17 PM

Name	Appstack	Health	Version	Tools
aca-controller-service	fusion	Up	7.22.718.60779	Metrics | Logs ↑ Upload to Case
agent	maglev-system	Up	1.8.222	Metrics | Logs ↑ Upload to Case
aggregationjobs	ndp	Up	5.3.16	Metrics | Logs ↑ Upload to Case

Upload this File to a Cisco Service Request. This button is injected by CSAE extension.

Catalyst Center

Dashboard / System Overview

Full screen Share Clone Edit Upload to Case

Filters 2 *

Upload this File to a Cisco Service Request. This button is injected by CSAE extension.

{"match":{"kubernetes.namespace_name":{"query":"fusion","type":"phrase"}}} × {"m

System Levels

Catalyst Center Guide for the CSA-E

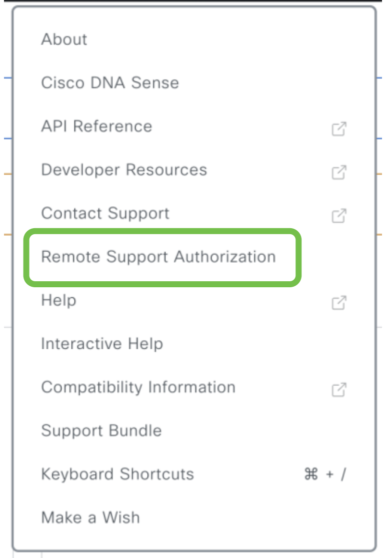
Catalyst Center Troubleshooting Tools & Other Services (Reference)

Collecting Logs for Troubleshooting

- Remote Support Authorization using RADKit

Allows a Cisco Support TAC engineer to securely, temporarily, interactively and remotely access the Cisco Catalyst Center.

- GA in 2.3.5.x
- Securely – Cisco SDL process approved, data encrypted & outbound connection only.
- Temporarily – Customer builds the credentials and authorizes the support engineer for a fixed time slot.
- Interactively – TAC engineer can connect to the UI or CLI, collect logs, run commands and performing quick troubleshooting using scripts.
- Remotely – Useful for remotely troubleshooting the Cisco Catalyst Center and / or the networking devices with all activities tracked on the Cisco Catalyst Center.

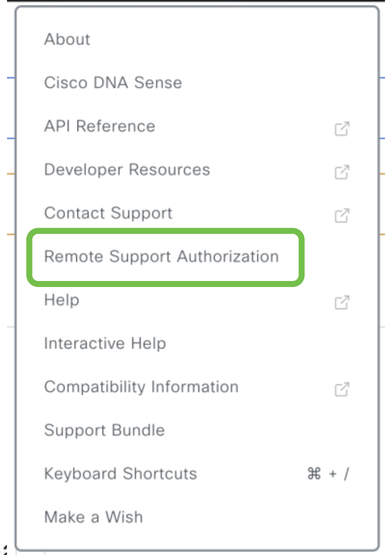


For more details reach out to us at the RADKit Community Page

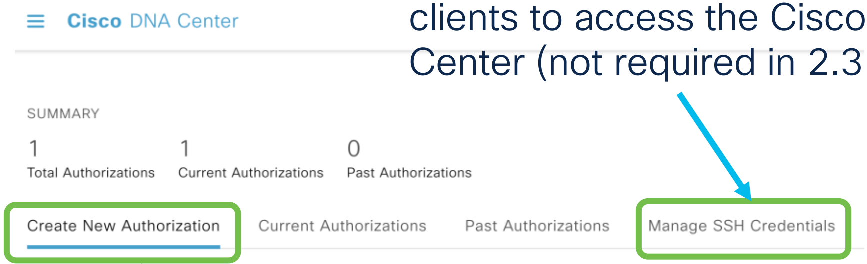
Collecting Logs for Troubleshooting

- Remote Support Authorization using RADKit

Customer View is **UI** based and authorizes a Cisco TAC Engineer in **2 steps** via the Remote Support Authorization Dashboard.



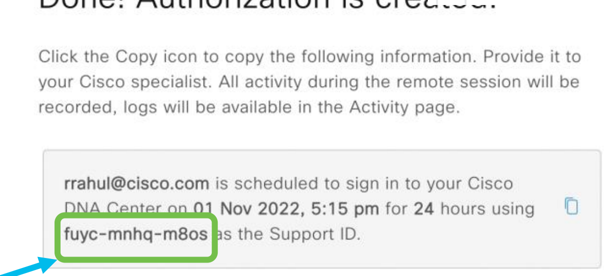
<u>Step 1.</u> Provide password for RADKit clients to access the Cisco Catalyst Center (not required in 2.3.7.6)



SUMMARY

1 Total Authorizations
1 Current Authorizations
0 Past Authorizations

<u>Step 2.</u> Schedule access for 24 hours (default) for a specific Cisco email id.



Done! Authorization is crea...

Click the Copy icon to copy the following information. Provide it to your Cisco specialist. All activity during the remote session will be recorded, logs will be available in the Activity page.

rrahul@cisco.com is scheduled to sign in to your Cisco DNA Center on **01 Nov 2022, 5:15 pm** for **24** hours using **fuyc-mnhq-m8os** as the Support ID.

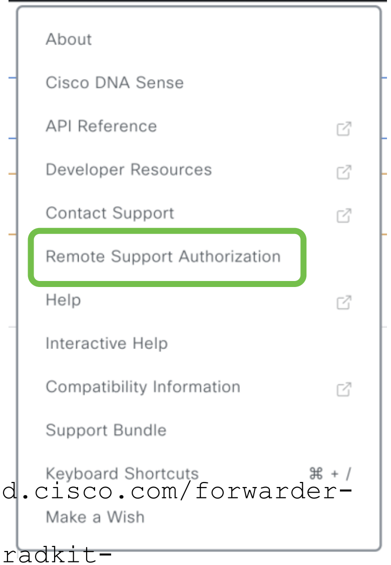
<u>Step 3.</u> Share the support ID with the TAC engineer.

For more details reach out to us at the RADKit Community Page

Collecting Logs for Troubleshooting

- Remote Support Authorization using RADKit

TAC engineer view is via RADKit client. Able to run python scripts interactively to multiple devices **simultaneously**.



```
>>> client = sso_login("rrahul@cisco.com")
>>>
>>> service = client.service("fuyc-mnhq-m8os")
07:23:38.197Z INFO  | internal | Connecting to forwarder [uri='wss://prod.radkit-cloud.cisco.com/forwarder-
1/websocket/']
07:23:39.040Z INFO  | internal | Connection to forwarder successful [uri='wss://prod.radkit-
cloud.cisco.com/forwarder-1/websocket/']
>>>
>>> #service.inventory # to view the entire inventory
>>>
>>> #service.inventory['maglev1'].exec("ls -l") # to execute command
>>>
>>> service.inventory['border-1'].interactive()
08:05:41.928Z INFO | starting interactive session (will be closed when detached)
Attaching to border-1 ...
Type: ~. to detach. ~? for other shortcuts. When using nested SSH sessions, add an extra ~ per level of
nesting.
border-1#
```

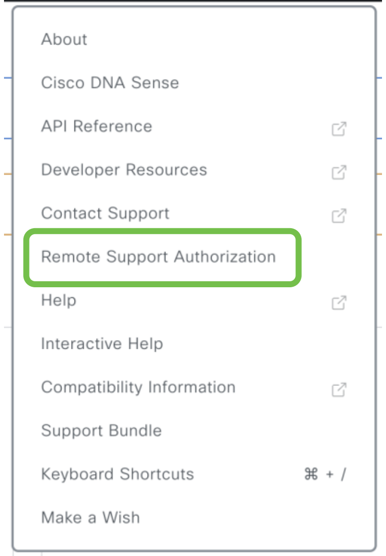
For more details reach out to us at the RADKit Community Page

Collecting Logs for Troubleshooting

- Remote Support Authorization using RADKit

New in **2.3.7.6**

- Secure SSH connectivity without the need of username/password.
- Read-only access to the CLI for maglev and magctl commands.
- Access added to the Catalyst Center ESXi.



For more details reach out to us at the RADKit Community Page

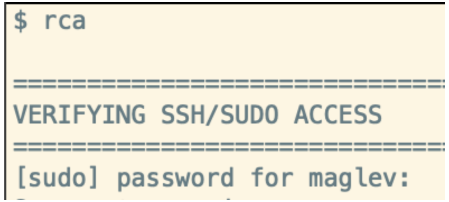
All Versions

Collecting Logs for Troubleshooting

- RCA from CLI

Generating RCA

Single command in all releases

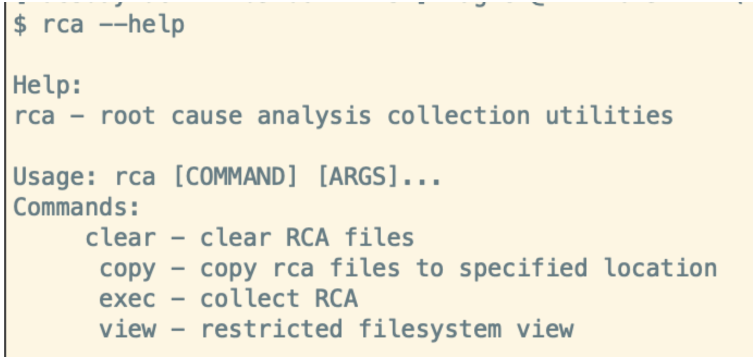


```
$ rca

================================
VERIFYING SSH/SUDO ACCESS
================================
[sudo] password for maglev:
```

Repeat on all nodes of a cluster

Commands to delete, copy & view RCAs

2.3.x & above



```
$ rca --help

Help:
rca - root cause analysis collection utilities

Usage: rca [COMMAND] [ARGS]...
Commands:
     clear - clear RCA files
      copy - copy rca files to specified location
      exec - collect RCA
      view - restricted filesystem view
```

2.2.x & below

Linux commands (scp, vim, rm …)
RCAs stored in folder /data/rca/

All Versions

Collecting Logs for Troubleshooting

- Logs from CLI for any Service

```
$ magctl service logs --help
Usage: magctl service logs [OPTIONS] SERVICE

  Connects to Elastic Search and pulls logs

Options:
  -o, --output [json]   Print log records in json
  -m, --mins TEXT       How many minutes in the past to search for logs
  -r, --raw             View raw log files
  -c, --container TEXT  Show logs for this container
  -t, --timezone TEXT   View logs in selected timezone ie America/Los_Angeles,
                        Asia/Calcutta
  -f, --follow          Follow logs when using --raw
  -p, --previous        Show logs from previous running instance of service
                        (if available)
  -t, --tail INTEGER    lines of recent log file to display. Defaults to -1,
                        showing all log lines
  -a, --appstack TEXT   AppStack on which to perform the operation
  --help                Show this message and exit.
```

Commonly used

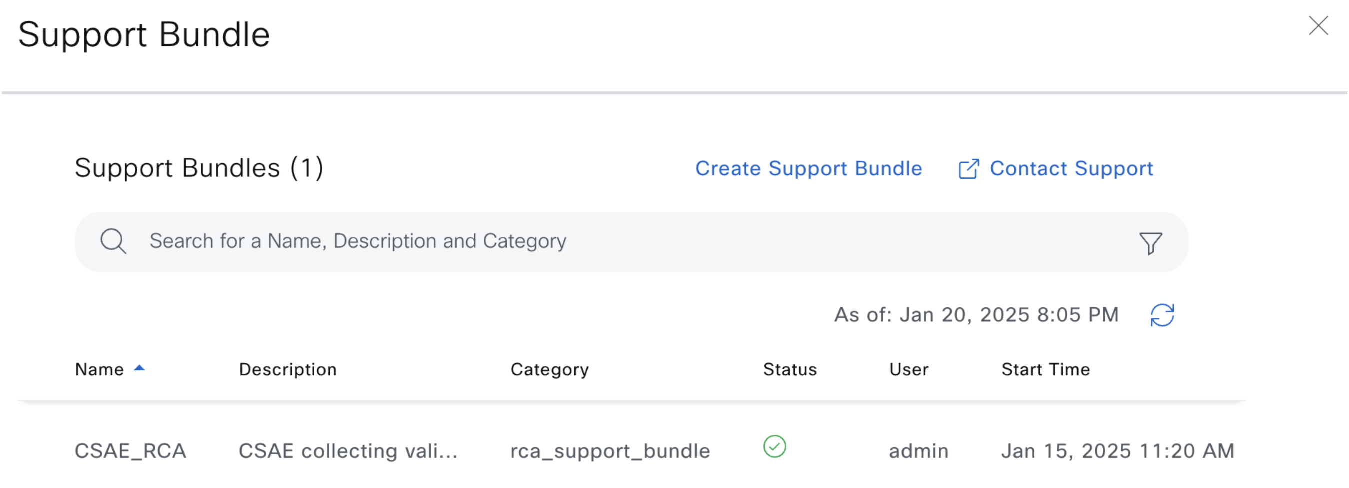
```
magctl service logs -r <service name>
magctl service logs -rf <service name>
magctl service logs -rt 10 <service name>
```

* Works with Magshell

Release 2.3.7.6 onwards

Collecting Logs for Troubleshooting

Option to create and view RCA bundles from the UI, both general and specific.

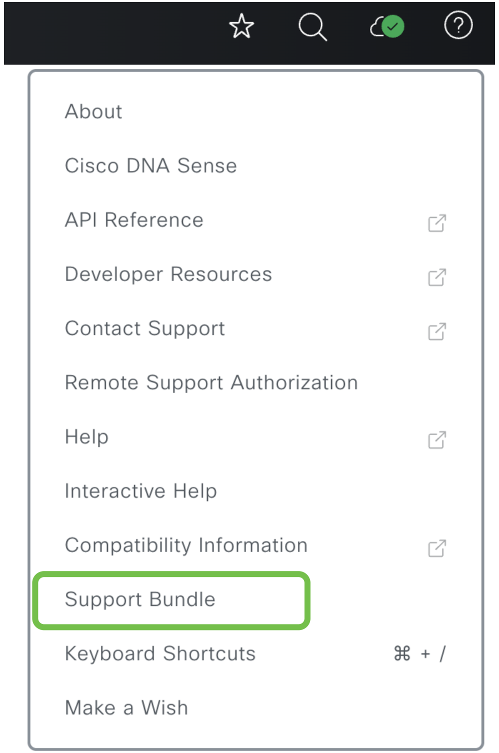


Support Bundle

Support Bundles (1)

As of: Jan 20, 2025 8:05 PM

Name	Description	Category	Status	User	Start Time
CSAE_RCA	CSAE collecting vali...	rca_support_bundle	✓	admin	Jan 15, 2025 11:20 AM



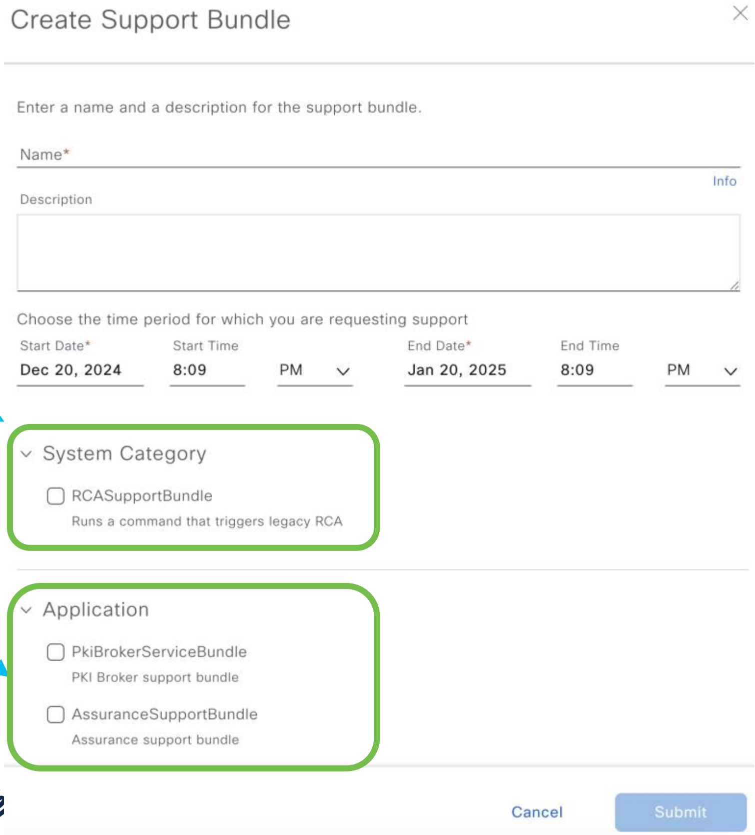
Release 2.3.7.6 onwards

Collecting Logs for Troubleshooting

Option to create and view RCA bundles from the UI, both general and specific.

Legacy RCA

Application Specific RCAs



Create Support Bundle

Enter a name and a description for the support bundle.

Name*

Info

Description

Choose the time period for which you are requesting support

Start Date*	Start Time		End Date*	End Time	
Dec 20, 2024	8:09	PM	Jan 20, 2025	8:09	PM

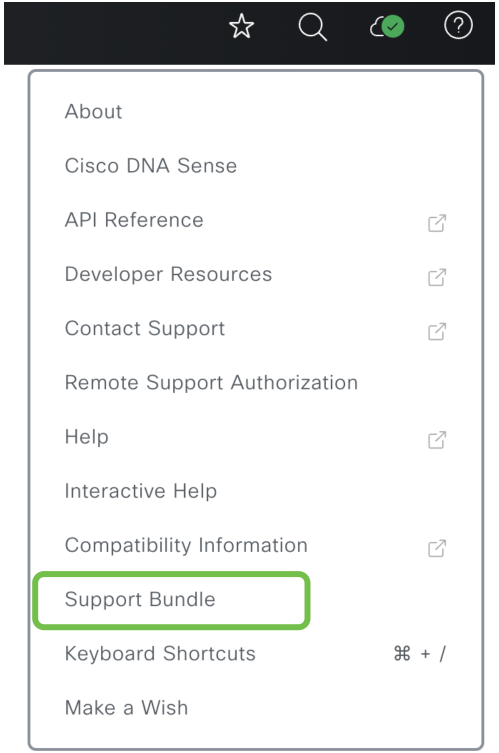
System Category

□ RCASupportBundle
Runs a command that triggers legacy RCA

Application

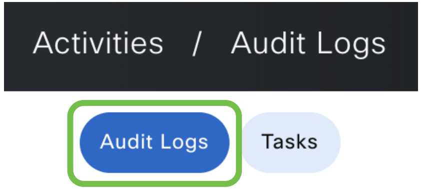
□ PkiBrokerServiceBundle
PKI Broker support bundle

□ AssuranceSupportBundle
Assurance support bundle



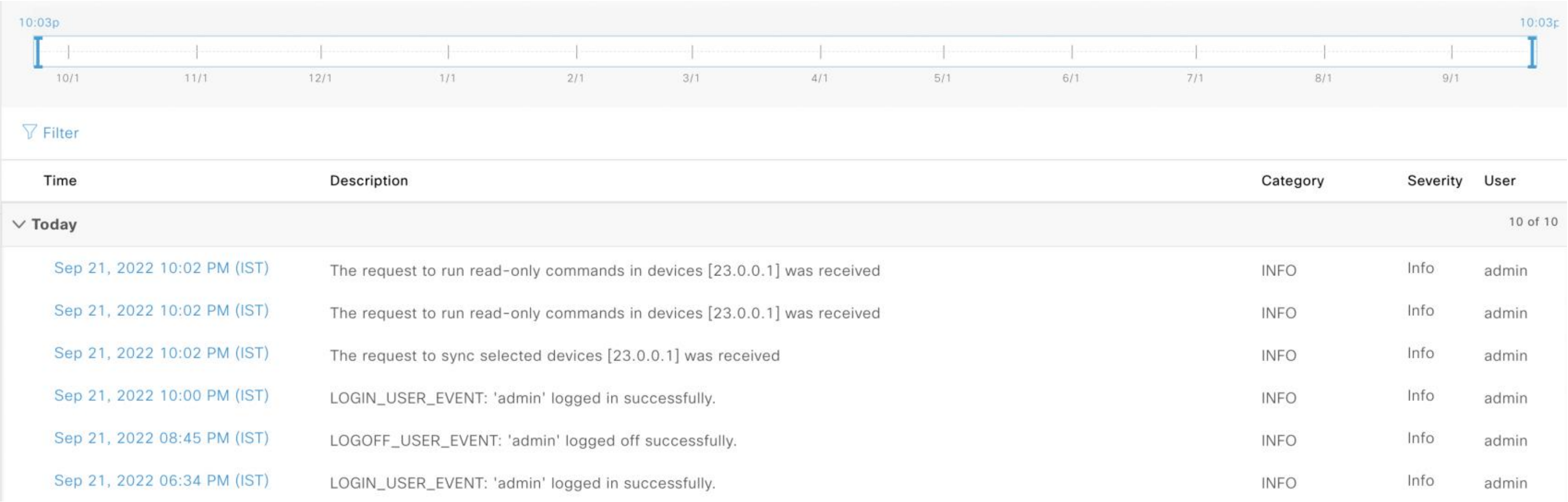
Collecting Audit Logs for Troubleshooting

Collecting Logs for Troubleshooting



- Audit Logs

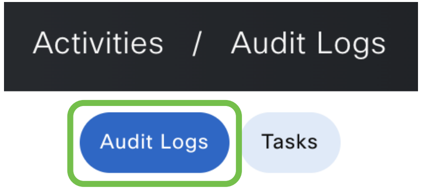
Audit logs captures all critical events/activities on the Cisco Catalyst Center



Today — 10 of 10

Time	Description	Category	Severity	User
Sep 21, 2022 10:02 PM (IST)	The request to run read-only commands in devices [23.0.0.1] was received	INFO	Info	admin
Sep 21, 2022 10:02 PM (IST)	The request to run read-only commands in devices [23.0.0.1] was received	INFO	Info	admin
Sep 21, 2022 10:02 PM (IST)	The request to sync selected devices [23.0.0.1] was received	INFO	Info	admin
Sep 21, 2022 10:00 PM (IST)	LOGIN_USER_EVENT: 'admin' logged in successfully.	INFO	Info	admin
Sep 21, 2022 08:45 PM (IST)	LOGOFF_USER_EVENT: 'admin' logged off successfully.	INFO	Info	admin
Sep 21, 2022 06:34 PM (IST)	LOGIN_USER_EVENT: 'admin' logged in successfully.	INFO	Info	admin

*1,000,000 notifications are maintained (regardless of type) and are stored for one year.


Activities / Audit Logs

Audit Logs

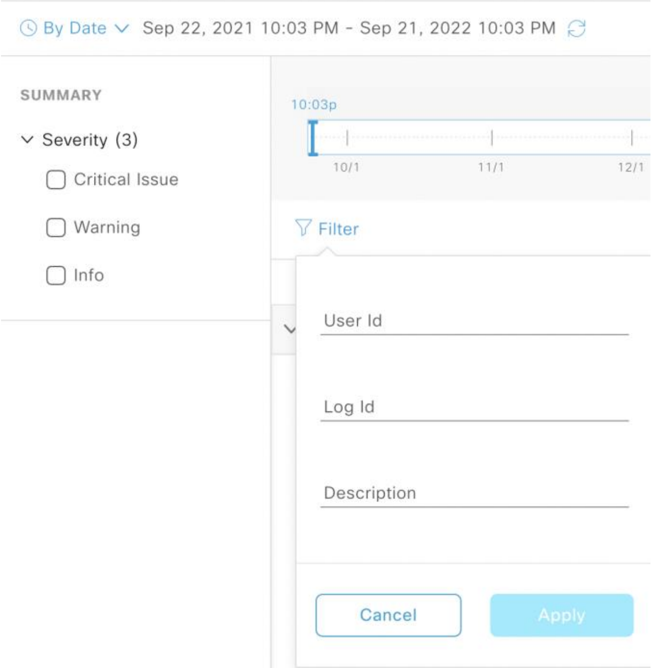
Tasks

Collecting Logs for Troubleshooting

- Audit Logs

5 Filters available on the top left corner

- Date
- Message Severity
- User Id
- Log Id
- Description


By Date Sep 22, 2021 10:03 PM - Sep 21, 2022 10:03 PM

SUMMARY

Severity (3)

□ Critical Issue

□ Warning

□ Info

Filter

User Id

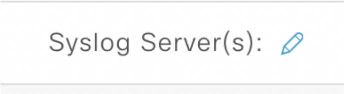
Log Id

Description

Cancel

Apply

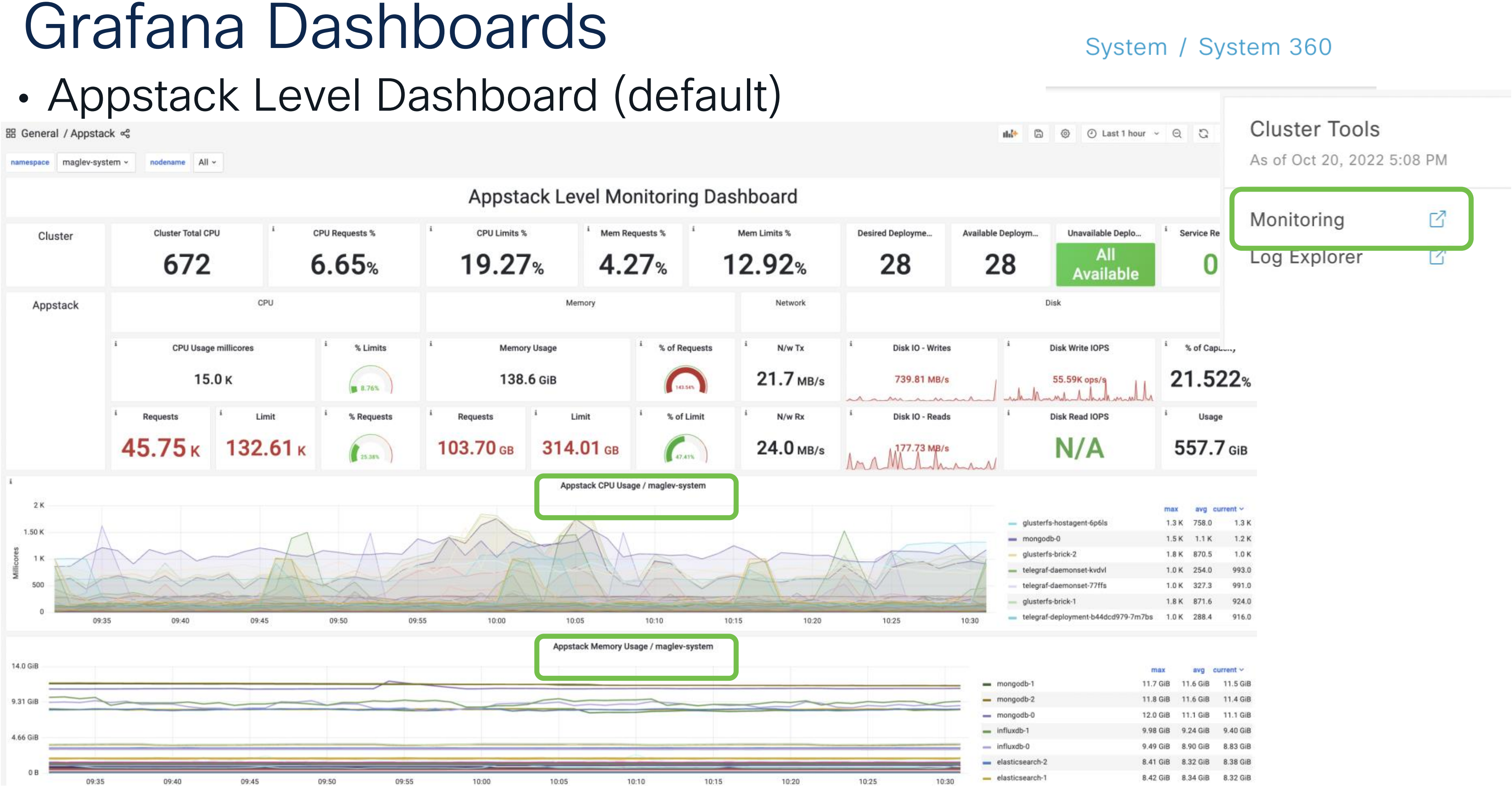
Option on the top right corner to export logs to a syslog server


Syslog Server(s):

Monitoring Service Statistics

Grafana Dashboards

- Appstack Level Dashboard (default)



System / System 360

Cluster Tools

As of Oct 20, 2022 5:08 PM

Monitoring

Log Explorer

General / Appstack

Last 1 hour

namespace: maglev-system

nodename: All

Appstack Level Monitoring Dashboard

Cluster

Cluster Total CPU	CPU Requests %	CPU Limits %	Mem Requests %	Mem Limits %	Desired Deployme...	Available Deploym...	Unavailable Deplo...	Service Re
672	6.65%	19.27%	4.27%	12.92%	28	28	All Available	0

Appstack

CPU

CPU Usage millicores	% Limits
15.0 K	8.76%

Requests	Limit	% Requests
45.75 K	132.61 K	25.38%

Memory

Memory Usage	% of Requests
138.6 GiB	143.54%

Requests	Limit	% of Limit
103.70 GB	314.01 GB	47.41%

Network

N/w Tx	N/w Rx
21.7 MB/s	24.0 MB/s

Disk

Disk IO - Writes	Disk Write IOPS	% of Capa...
739.81 MB/s	55.59K ops/s	21.522%

Disk IO - Reads	Disk Read IOPS	Usage
177.73 MB/s	N/A	557.7 GiB

Appstack CPU Usage / maglev-system

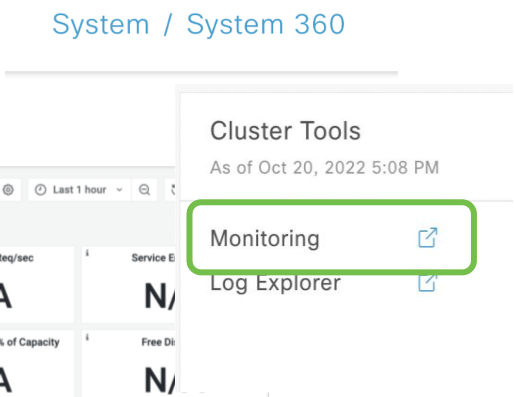
	max	avg	current
glusterfs-hostagent-6p6ls	1.3 K	758.0	1.3 K
mongodb-0	1.5 K	1.1 K	1.2 K
glusterfs-brick-2	1.8 K	870.5	1.0 K
telegraf-daemonset-kvdvl	1.0 K	254.0	993.0
telegraf-daemonset-77ffs	1.0 K	327.3	991.0
glusterfs-brick-1	1.8 K	871.6	924.0
telegraf-deployment-b44dcd979-7m7bs	1.0 K	288.4	916.0

Appstack Memory Usage / maglev-system

	max	avg	current
mongodb-1	11.7 GiB	11.6 GiB	11.5 GiB
mongodb-2	11.8 GiB	11.6 GiB	11.4 GiB
mongodb-0	12.0 GiB	11.1 GiB	11.1 GiB
influxdb-1	9.98 GiB	9.24 GiB	9.40 GiB
influxdb-0	9.49 GiB	8.90 GiB	8.83 GiB
elasticsearch-2	8.41 GiB	8.32 GiB	8.38 GiB
elasticsearch-1	8.42 GiB	8.34 GiB	8.32 GiB

Grafana Dashboards

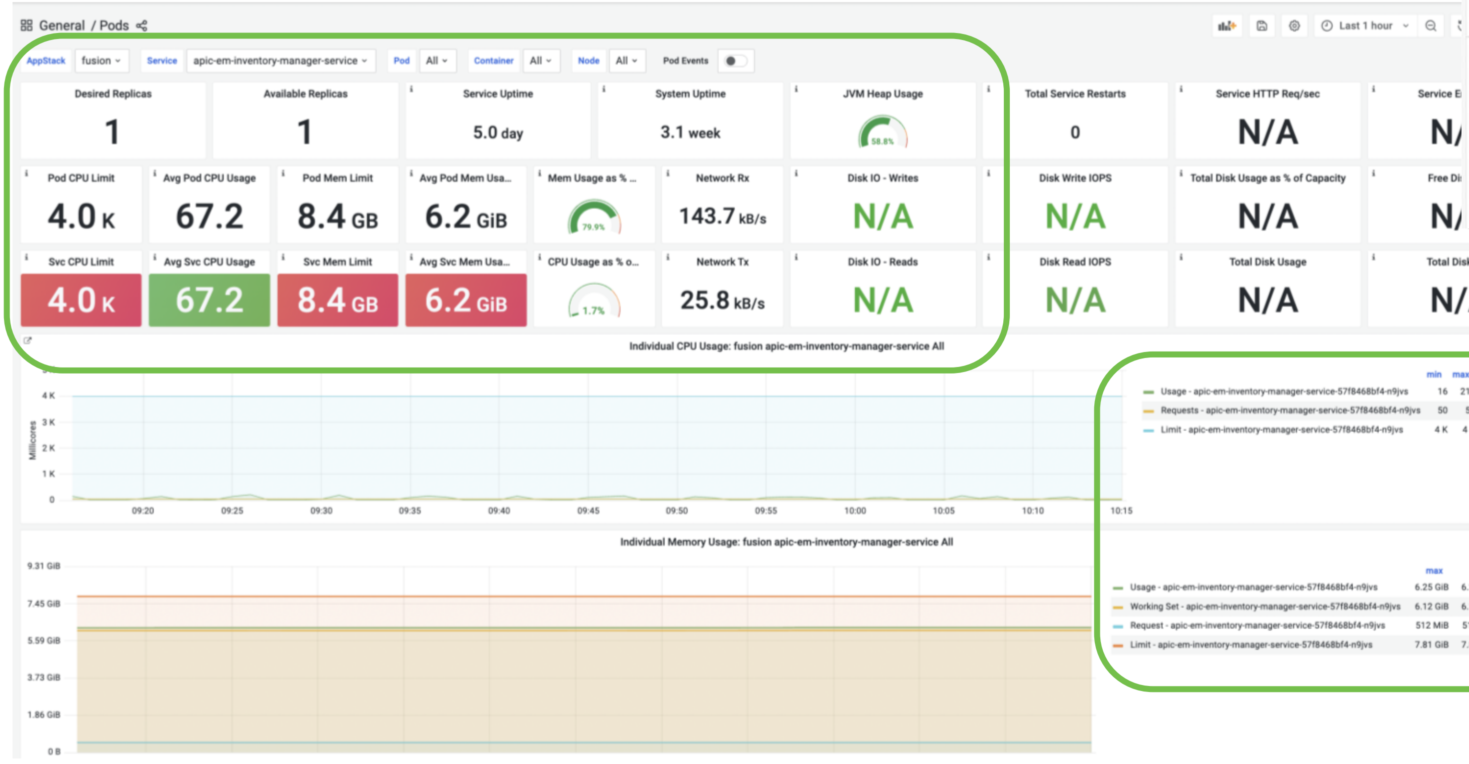
- Monitoring Service level Memory and CPU requirements (Live)



System / System 360

Cluster Tools

As of Oct 20, 2022 5:08 PM



General / Pods

AppStack: fusion | Service: apic-em-inventory-manager-service | Pod: All | Container: All | Node: All | Pod Events

Desired Replicas	Available Replicas	Service Uptime	System Uptime	JVM Heap Usage	Total Service Restarts	Service HTTP Req/sec	Service E
1	1	5.0 day	3.1 week	58.8%	0	N/A	N/

Pod CPU Limit	Avg Pod CPU Usage	Pod Mem Limit	Avg Pod Mem Usa...	Mem Usage as % ...	Network Rx	Disk IO - Writes	Disk Write IOPS	Total Disk Usage as % of Capacity	Free Di
4.0 K	67.2	8.4 GB	6.2 GiB	79.9%	143.7 kB/s	N/A	N/A	N/A	N/

Svc CPU Limit	Avg Svc CPU Usage	Svc Mem Limit	Avg Svc Mem Usa...	CPU Usage as % o...	Network Tx	Disk IO - Reads	Disk Read IOPS	Total Disk Usage	Total Disk Size
4.0 K	67.2	8.4 GB	6.2 GiB	1.7%	25.8 kB/s	N/A	N/A	N/A	N/A

Individual CPU Usage: fusion apic-em-inventory-manager-service All

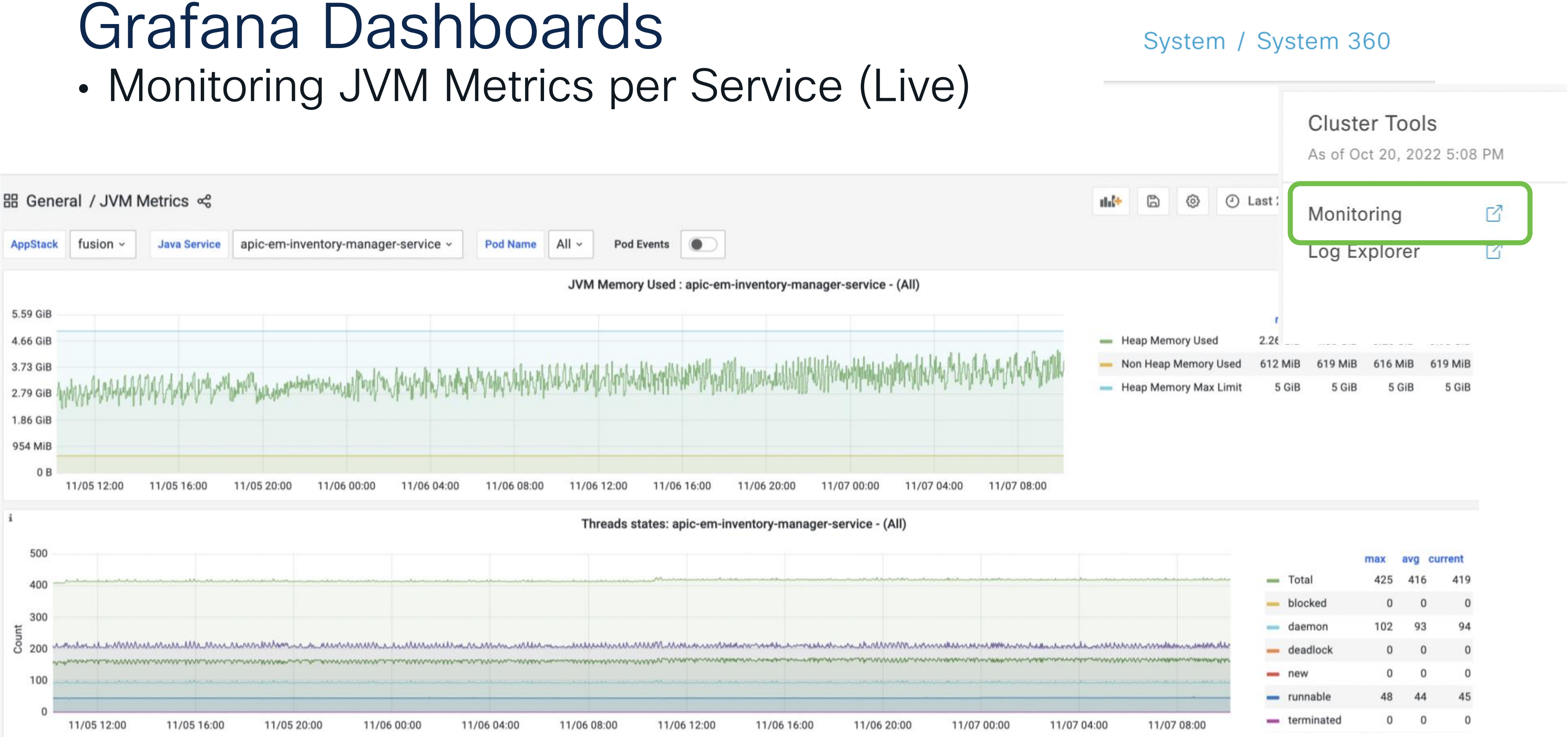
	min	max	avg	current
Usage - apic-em-inventory-manager-service-57f8468bf4-n9jvs	16	215	67.2	19
Requests - apic-em-inventory-manager-service-57f8468bf4-n9jvs	50	50	50	50
Limit - apic-em-inventory-manager-service-57f8468bf4-n9jvs	4 K	4 K	4 K	4 K

Individual Memory Usage: fusion apic-em-inventory-manager-service All

	max	avg	current
Usage - apic-em-inventory-manager-service-57f8468bf4-n9jvs	6.25 GiB	6.25 GiB	6.25 GiB
Working Set - apic-em-inventory-manager-service-57f8468bf4-n9jvs	6.12 GiB	6.11 GiB	6.12 GiB
Request - apic-em-inventory-manager-service-57f8468bf4-n9jvs	512 MiB	512 MiB	512 MiB
Limit - apic-em-inventory-manager-service-57f8468bf4-n9jvs	7.81 GiB	7.81 GiB	7.81 GiB

Grafana Dashboards

- Monitoring JVM Metrics per Service (Live)



System / System 360

Cluster Tools

As of Oct 20, 2022 5:08 PM

General / JVM Metrics

AppStack: fusion · Java Service: apic-em-inventory-manager-service · Pod Name: All

JVM Memory Used : apic-em-inventory-manager-service - (All)

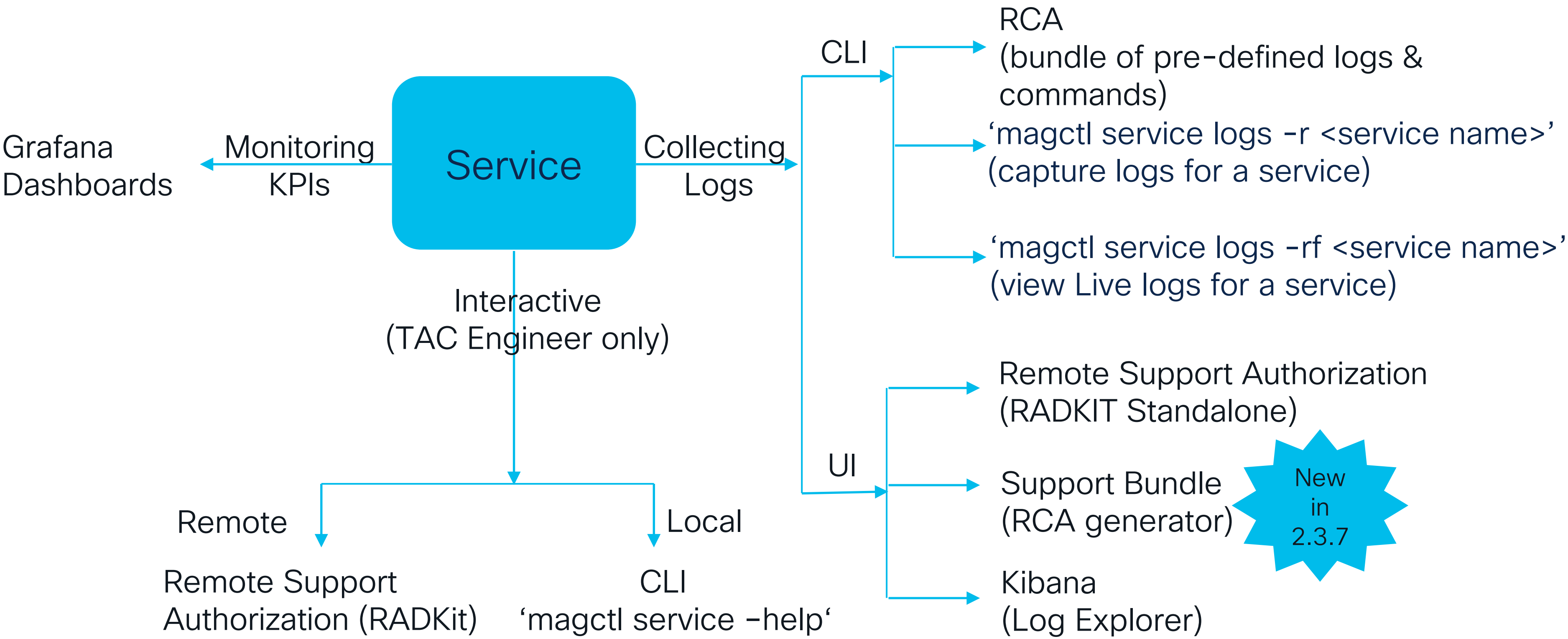
Heap Memory Used	2.26	[illegible]	[illegible]	[illegible]
Non Heap Memory Used	612 MiB	619 MiB	616 MiB	619 MiB
Heap Memory Max Limit	5 GiB	5 GiB	5 GiB	5 GiB

Threads states: apic-em-inventory-manager-service - (All)

	max	avg	current
Total	425	416	419
blocked	0	0	0
daemon	102	93	94
deadlock	0	0	0
new	0	0	0
runnable	48	44	45
terminated	0	0	0

*Most Services are Java based

Troubleshooting Services – Cheat sheet



RCA (bundle of pre-defined logs & commands)

‘magctl service logs -r <service name>’ (capture logs for a service)

‘magctl service logs -rf <service name>’ (view Live logs for a service)

Remote Support Authorization (RADKIT Standalone)

Support Bundle (RCA generator)

Kibana (Log Explorer)

Remote Support Authorization (RADKit)

CLI ‘magctl service –help‘

Wrap Up

Microservices - Reference

Inventory

- inventory-manager
- postgres
- dna-maps-service
- kong
- network-design-service
- network-poller-service

Provisioning

- provisioning-service
- orchestration-engine service
- spf-service-manager
- network-programmer
- network-validation service

ISE Integration

- pki-broker
- network-design
- Ise-bridge
- kong

SWIM

- swim
- network-design
- network-programmer
- kong

Upgrades

- catalogserver
- workflow-worker
- system-updater
- kong

LAN Automation

- onboarding-service
- connection-manager
- network-orchestration
- Inventory-manager

License Manager

- licensemanager
- license-service
- kong

PnP

- onboarding-service
- connection-manager
- inventory-manager

Key takeaways

- System 360 to monitor your Catalyst Center services, resources and logs
- Add your devices to inventory and use Grafana to troubleshoot issues
- Troubleshoot device provisioning by checking the service logs
- Troubleshoot device upgrades using Grafana dashboards
- Troubleshoot assurance using in-built UI Tool
- Troubleshoot upgrades using maglev CLI

Fill Out Your Session Surveys

Participants who fill out a minimum of 4 session surveys and the overall event survey will get a unique Cisco Live t-shirt.

(from 11:30 on Thursday, while supplies last)

All surveys can be taken in the Cisco Events mobile app or by logging in to the Session Catalog and clicking the 'Participant Dashboard'

Content Catalog

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at ciscolive.com/on-demand. Sessions from this event will be available from March 3.

Contact us at: akaviya@cisco.com, rrahul@cisco.com

CISCO Live!

Cisco Live EMEA Catalyst Center Learning Map

Sunday–9th

LTRENS-2890 7:45AM
ThousandEyes Network Agent Deployment on Cisco Catalyst 9000 Series Through Cisco Catalyst Center

LABENT-1809 7:45AM
Cisco Catalyst Center Monitoring and Troubleshooting

LABDEV-3752 8:30AM
Building Cisco SD-Access with Cisco Catalyst Center and ISE

LABOPS-1470 9:15AM
Click Once, Configure Everything with Cisco Catalyst Center using Configuration Templates

LABEWN-2697 10:45AM
Configure and Monitor AI-RRM with Cisco Catalyst Center

LABOPS-2779 10:45AM
Deploying Cisco Catalyst Center Virtual Appliance in AWS

TECOPS-1111 1:30PM
Let's Onboard, Configure and Optimize the brownfield Cisco Catalyst Wireless Infrastructure using NetOps and AIOps capabilities of Cisco Catalyst Center

○ TECOPS-2158 1:30PM
Cisco Catalyst Center Out-of-the-Box and Custom Integrations

TECOPS-2501 1:45PM
Mastering Catalyst Center: Troubleshooting Tips for Network automation and management

Monday–10th

TECOPS-2002 8:30AM
How to leverage Cisco Catalyst Center to build a Zero Trust Campus Network

TECOPS-2823 8:45AM
How to Leverage Cisco Catalyst Center to its Greatest Potential

TECOPS-2113 8:45AM
Building Custom Apps with Splunk Add-On Builder to Enhance Cross-Technology Operations with Cisco Catalyst Center and Splunk

BRKOPS-2402 4:00PM
Automate the Deployment of a Wireless Network with the Help of Cisco Catalyst Center

LABOPS-1399 Walk in Lab
Exploring AI Ops: AI's Potential in Network Operations

Tuesday–11th

BRKCOC-2483 8:00AM
Cisco IT: Streamlining Network Management and Decisions with Catalyst Center Automation and Splunk

○ BRKOPS-1894 8:00AM
Cisco Meraki Dashboard Meets Cisco Catalyst Center – Better Together!

○ BRKIPV-1007 8:00AM
Deploying Catalyst Center for IPv6 Networks

LTROPS-2341 8:30AM
Build a Flexible Network Automation Workflow with GitLab CI/CD, Catalyst Center, NetBox, and Ansible

BRKOPS-2464 12:00PM
Understanding and Troubleshooting the Cisco Catalyst Center

BRKOPS-2038 12:00PM
The Flow of Things: Navigating and Properly Enabling NetFlow-based Solutions through Cisco Catalyst Center

○ DEVNET-3000 3:00PM
Open-Source GenAI Bot for Catalyst Center

Wednesday–12th

○ DEVNET-1087 9:30AM
Cisco Catalyst Center Platform: APIs, Event Notifications, Integrations, and DevOps Resources

CSSENT-1144 11:00AM
Driving IT/OT Excellence with AI-Powered Cisco Catalyst Center at the Worldwide Vehicle Industry

BRKOPS-2416 1:15PM
7 Habits for Optimizing Your Cisco Catalyst Center Environment

LTRENS-3751 2:00PM
SD-Access as Code with Cisco Catalyst Center and ISE Automation

BRKOPS-2442 3:15PM
Leveraging Digital Twin Technology for Advanced Network Management with Cisco Catalyst Center

○ IBOOPS-2882 4:00PM
Let's Talk about Cisco Catalyst Center Integrations

○ BRKIOT-2362 5:00PM
Converge IT and OT Networks with Cisco Catalyst Center: In-Depth look into Industrial Networks

Thursday–13th

○ BRKOPS-1461 8:30AM
Discovering and Managing Brownfield Deployment with Cisco Catalyst Center

IBOOPS-2391 8:30AM
AI/ML in Cisco Catalyst Center: Transforming Network Operations

○ BRKOPS-2596 10:30AM
Revolutionize Your Network Management with Cisco Catalyst Center: Physical or Virtual on AWS or VMware

○ BRKOPS-3429 10:30AM
Simplify Network Management using GenAI and Cisco Catalyst Center APIs

BRKEWN-2667 1:00PM
Cisco Wireless Supercharged by Catalyst Center: The Ultimate Guide

○ BRKOPS-2608 2:15PM
Architecting your Cisco Catalyst Center for Resiliency and Business Continuity -

BRKTRS-3821 2:15PM
Mastering Troubleshooting with Cisco Catalyst Center & SD-Access

○ BU-led sessions

cisco Live!

Thank you

cisco Live!

GO BEYOND