
cisco Live!
Let's go

The bridge to possible

Understanding and Troubleshooting the Cisco Catalyst Center

Abhay Kaviya, Customer Success Specialist
@abhaykaviya

cisco Live!

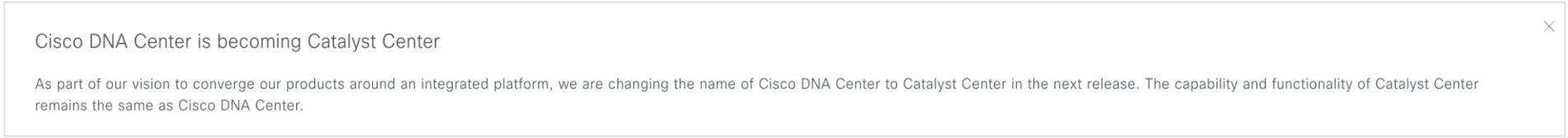
BRKOPS-2464

Cisco DNA Center is now Cisco Catalyst Center

Simplified branding for the Cisco Catalyst Stack.

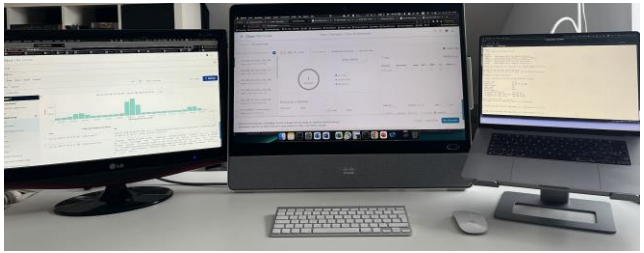
Catalyst Center and Cisco DNA Center are the same product; as Cisco progresses through the rebranding process, both product names can be used interchangeably.

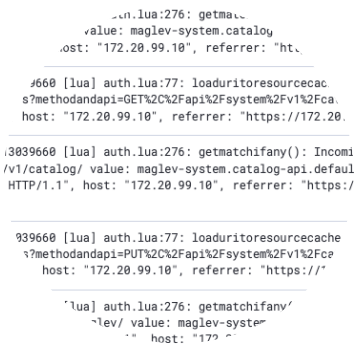
Screenshot visible from 2.3.7.4



Have you ever called TAC?

IP Address	Device Name	Status	ICMP ▲	SNMP	CLI
10.20.10.102			✓	✗	✓





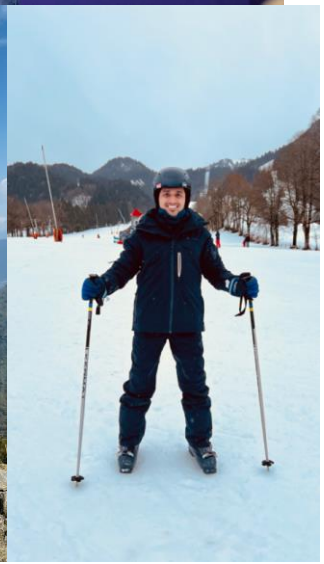
What to expect and not to expect ?

- No deep dive into SD-Access
- No SDA multicast
- No Catalyst center APIs
- No design

- Introduction to Catalyst Center Architecture and troubleshooting tools
- Cisco Catalyst Center Inventory and SWIM
- Cisco Catalyst center Assurance and Upgrades

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



Agenda

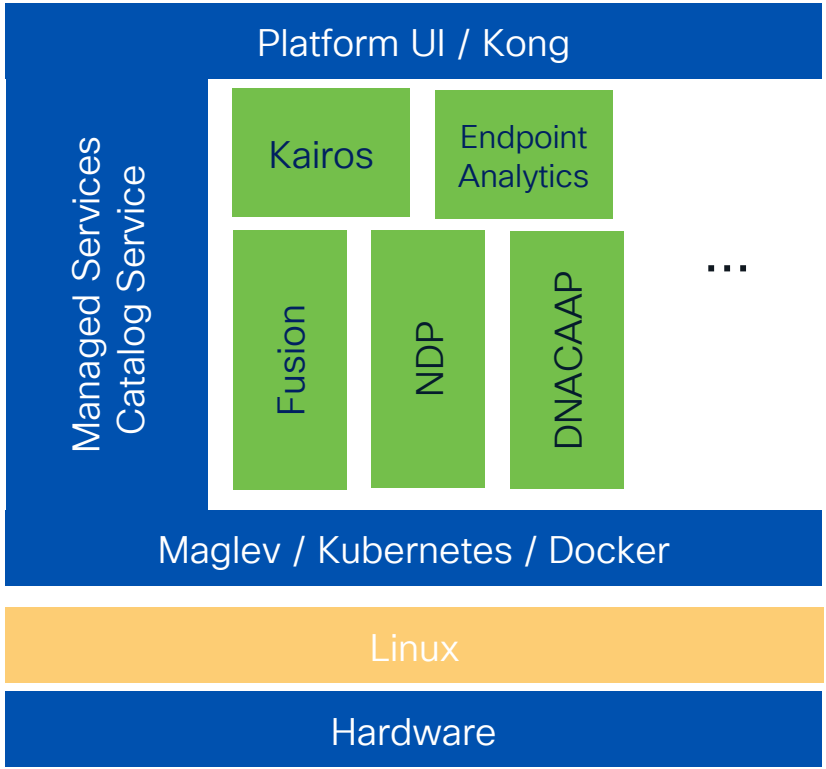
- Cisco Catalyst Center Architecture
- Cisco Catalyst Center Health
- Cisco Catalyst Center Inventory
- Cisco Catalyst Center SWIM
- Cisco Catalyst Center Assurance
- Cisco Catalyst Center Software Upgrades
- Cisco Catalyst Center Troubleshooting Tools (Reference Section)

Cisco Catalyst Center Architecture

Cisco Catalyst Center Architecture

Release 2.3.3.x
2.3.5.x

- The Layers of the Microservices Architecture



Apps or Network Applications
- Automation, Assurance, Platform APIs, AI Network Analytics, Endpoint Analytics

Maglev v1.7
- Managed Services
  - DBaaS (MongoDB, Postgres)
  - Messaging Queues (RabbitMQ, Kafka)
  - Clustering Services (Glusterfs, Zookeeper)
  - Monitoring (InfluxDB, Grafana)
- Catalog Service
- Kubernetes(v1.18.15), Docker(19.3.9)
- North Bound API Gateway – Kong

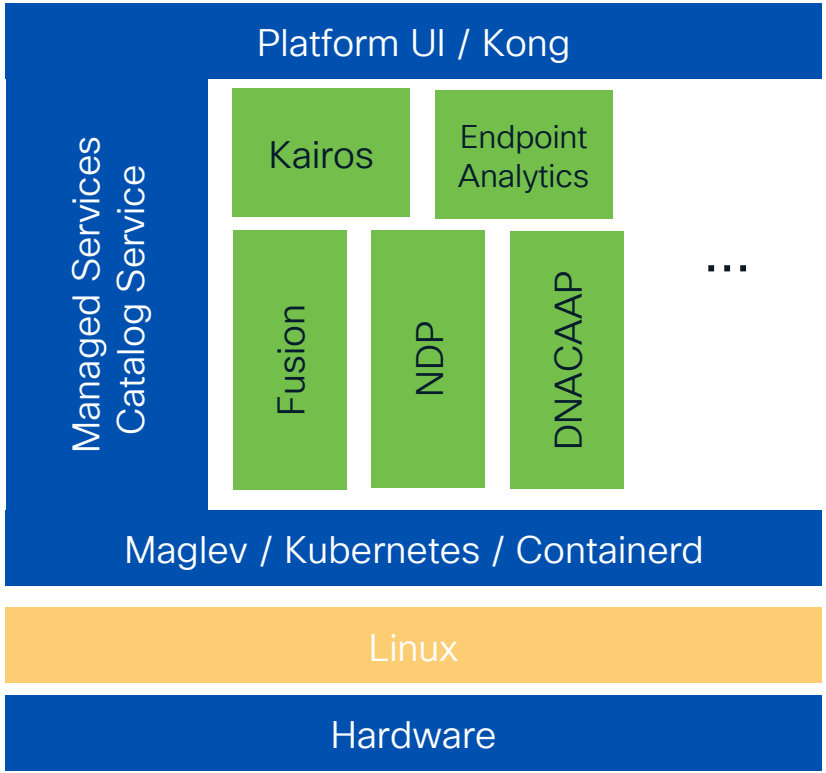
Linux Ubuntu (18.4.1 LTS)

DN1 – 44 core (based on the Cisco UCS C220 M4)
DN2 – 44, 56 or 112 core (based on the Cisco UCS C220 M5)

Cisco Catalyst Center Architecture

Release 2.3.7.x

- The Layers of the Microservices Architecture



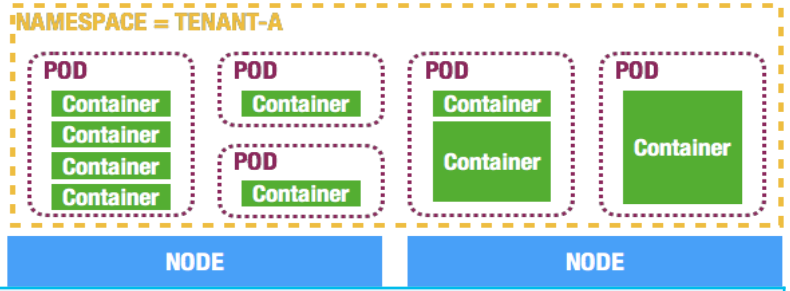
Apps or Network Applications
- Automation, Assurance, Platform APIs, AI Network Analytics, Endpoint Analytics

Maglev ~~v1.7~~ (v3.0)
- Managed Services
  - DBaaS (MongoDB, Postgres)
  - Messaging Queues (RabbitMQ, Kafka)
  - Clustering Services (Glusterfs, Zookeeper)
  - Monitoring (~~InfluxDB~~ Prometheus, Grafana)
- Catalog Service
- Kubernetes~~(v1.18.15)~~ (v1.24.1), ~~Docker(19.3.9)~~ Containerd (v1.22.0)
- North Bound API Gateway – Kong

Linux Ubuntu ~~(18.4.1 LTS)~~ (18.4.6 LTS)

ESXi / AWS

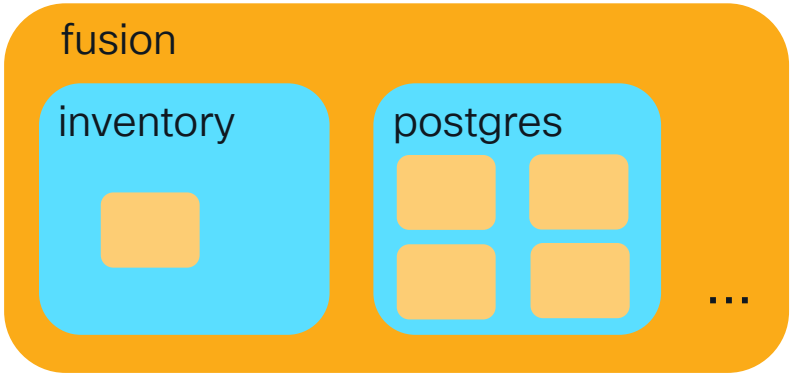
Terminology – Microservices



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	Namespaces are multiple virtual clusters backed by the same physical 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

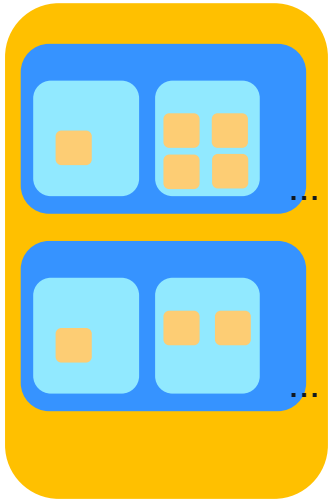
Services (aka micro-services) is a logical abstraction representing a group of K8s pods.

- 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.

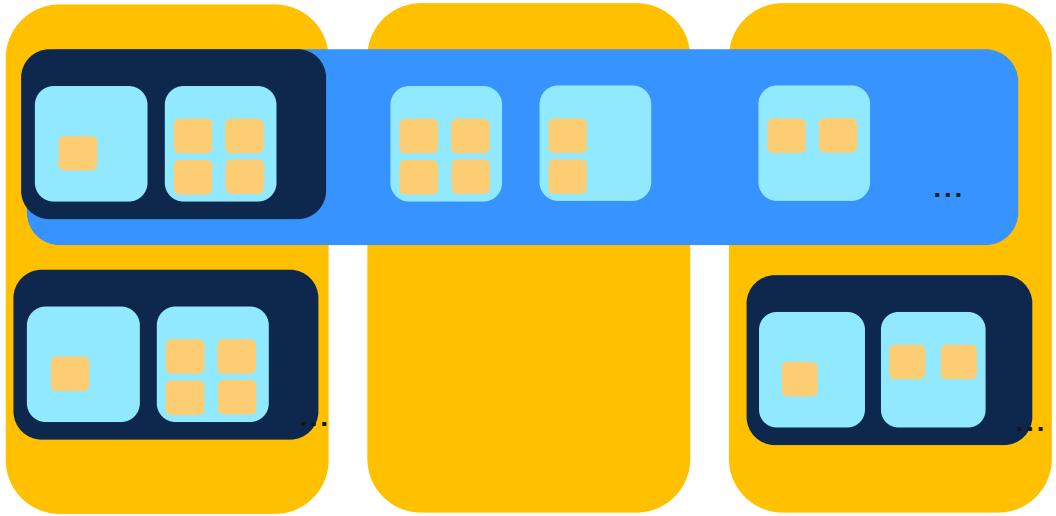
Cisco Catalyst Center Architecture

Microservices Architecture powered by Kubernetes & Docker



Single Node Cluster

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

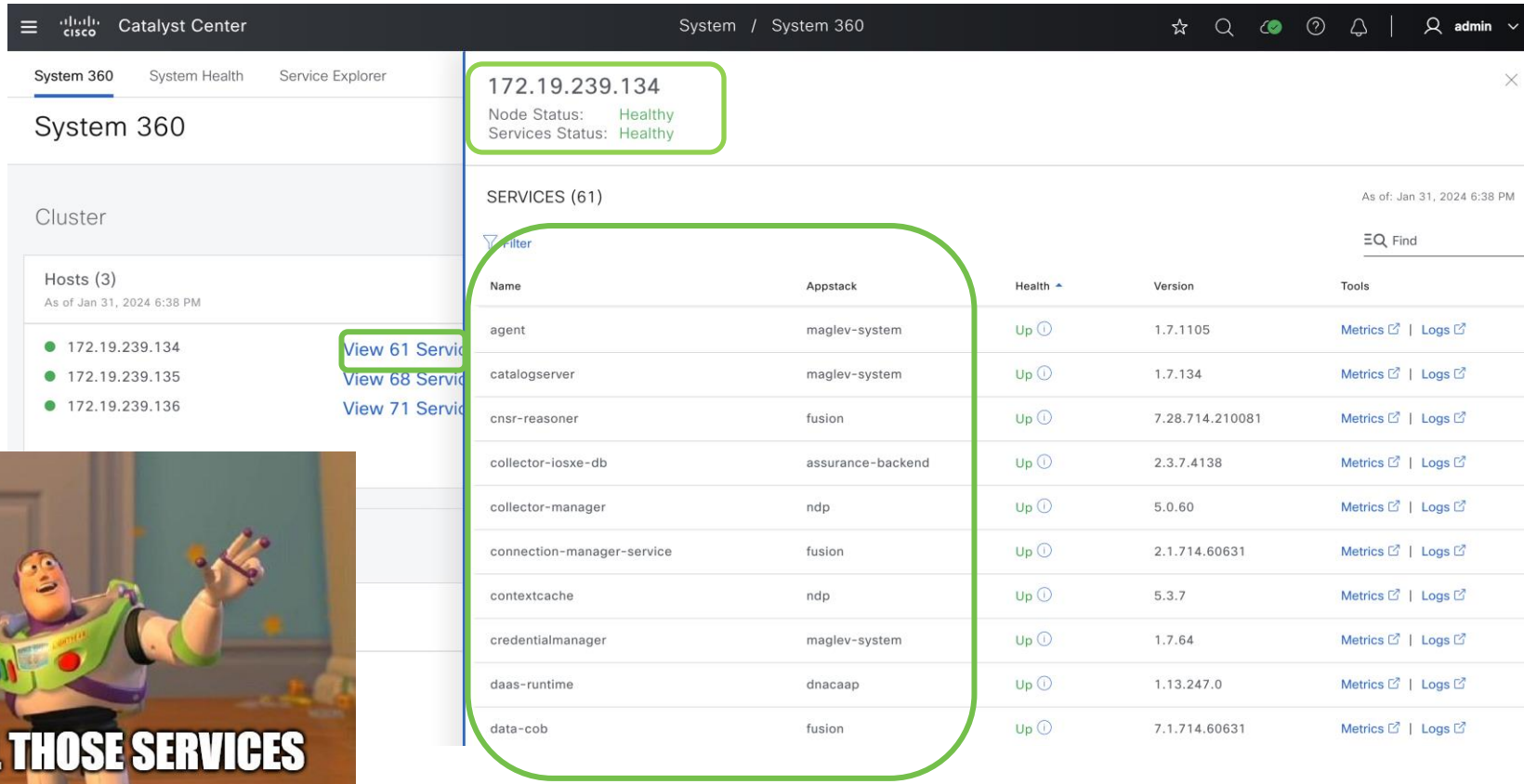


Three Node Cluster

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.

Cisco Catalyst Center Architecture

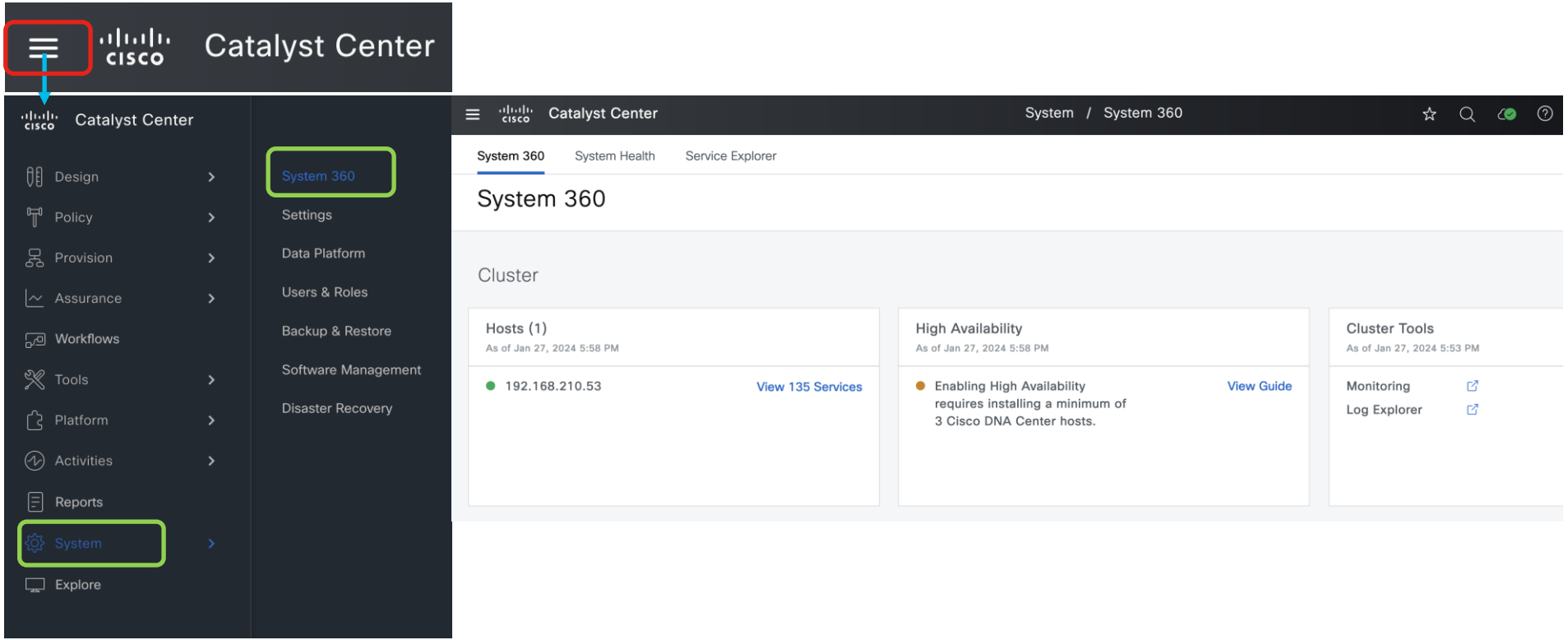
View Micro Services via UI

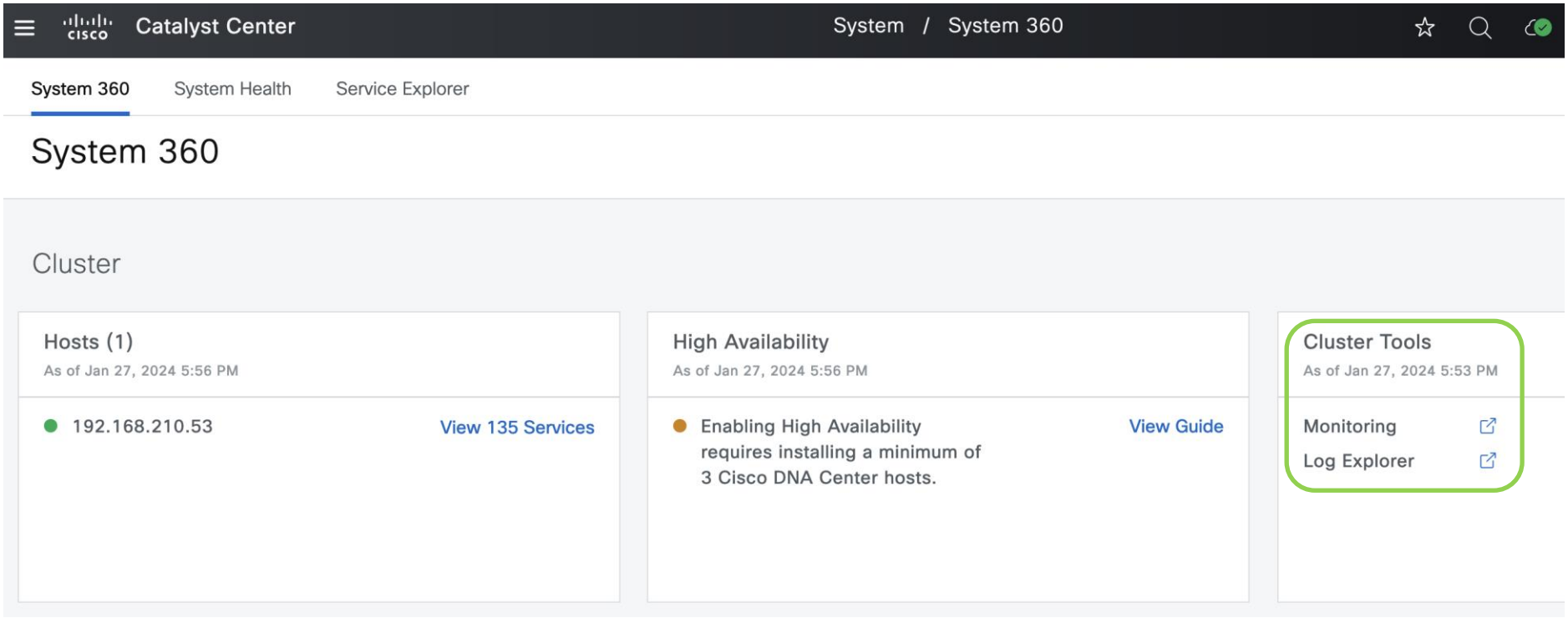


Cisco Catalyst Center System 360

cisco Live!

Catalyst Center UI: System 360





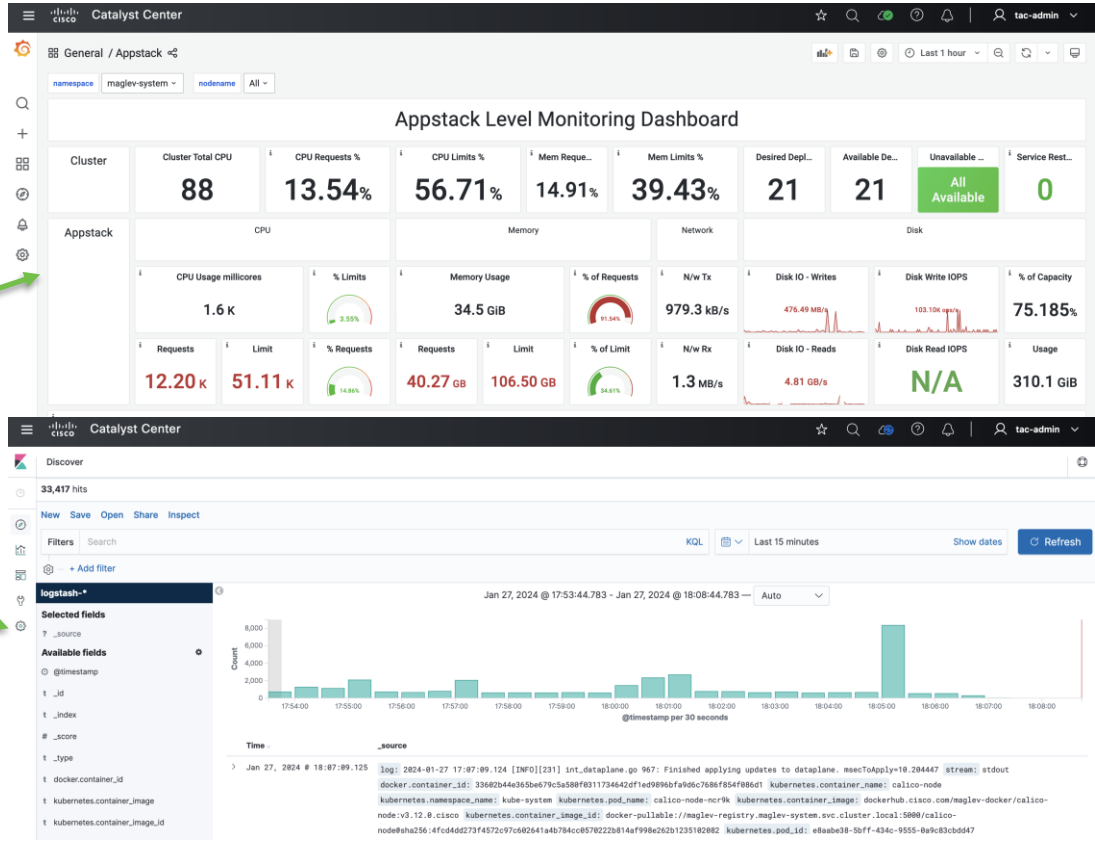
System 360: Cluster Tools

Cluster Tools

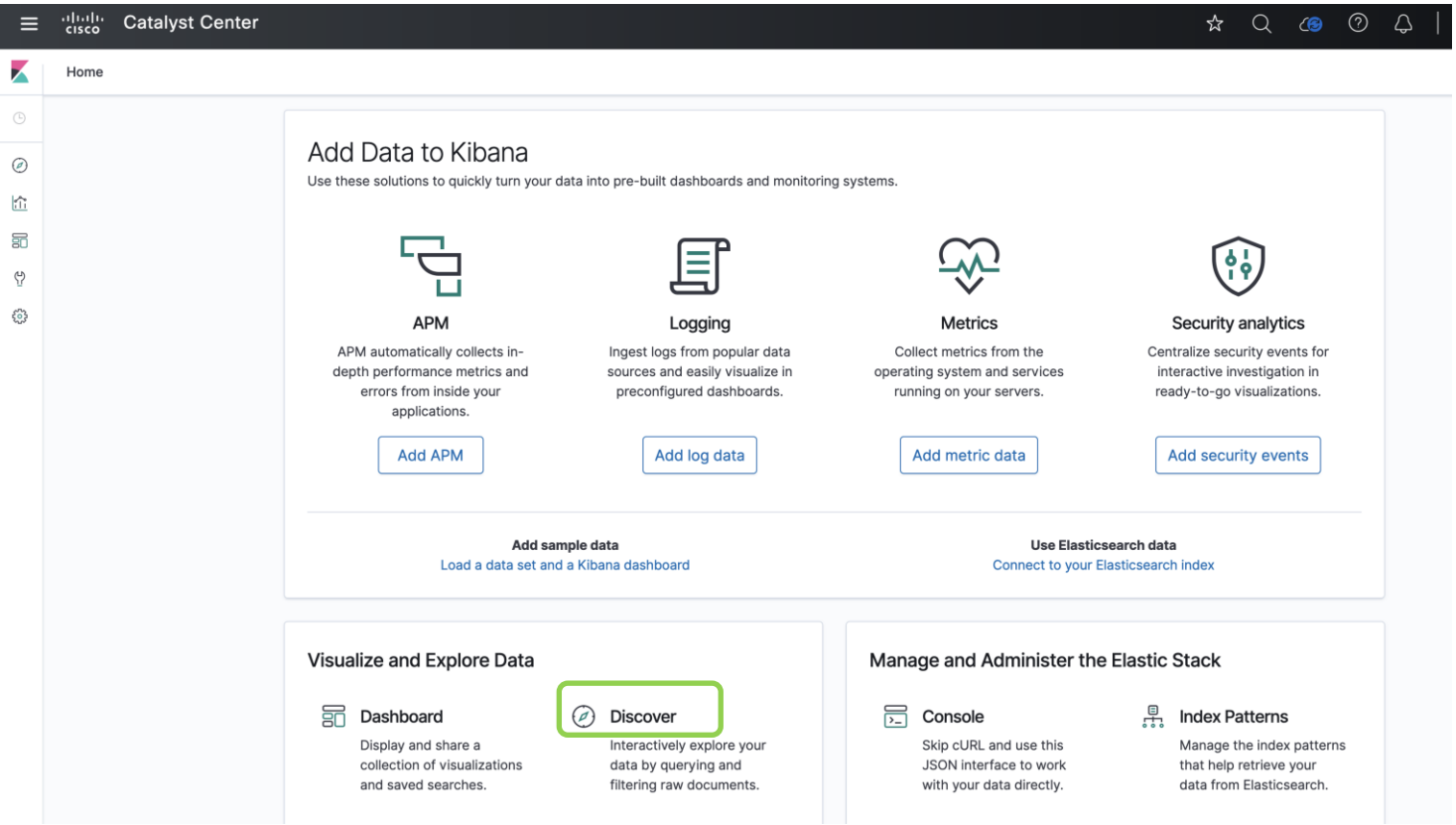
As of Jan 27, 2024 5:53 PM

Monitoring

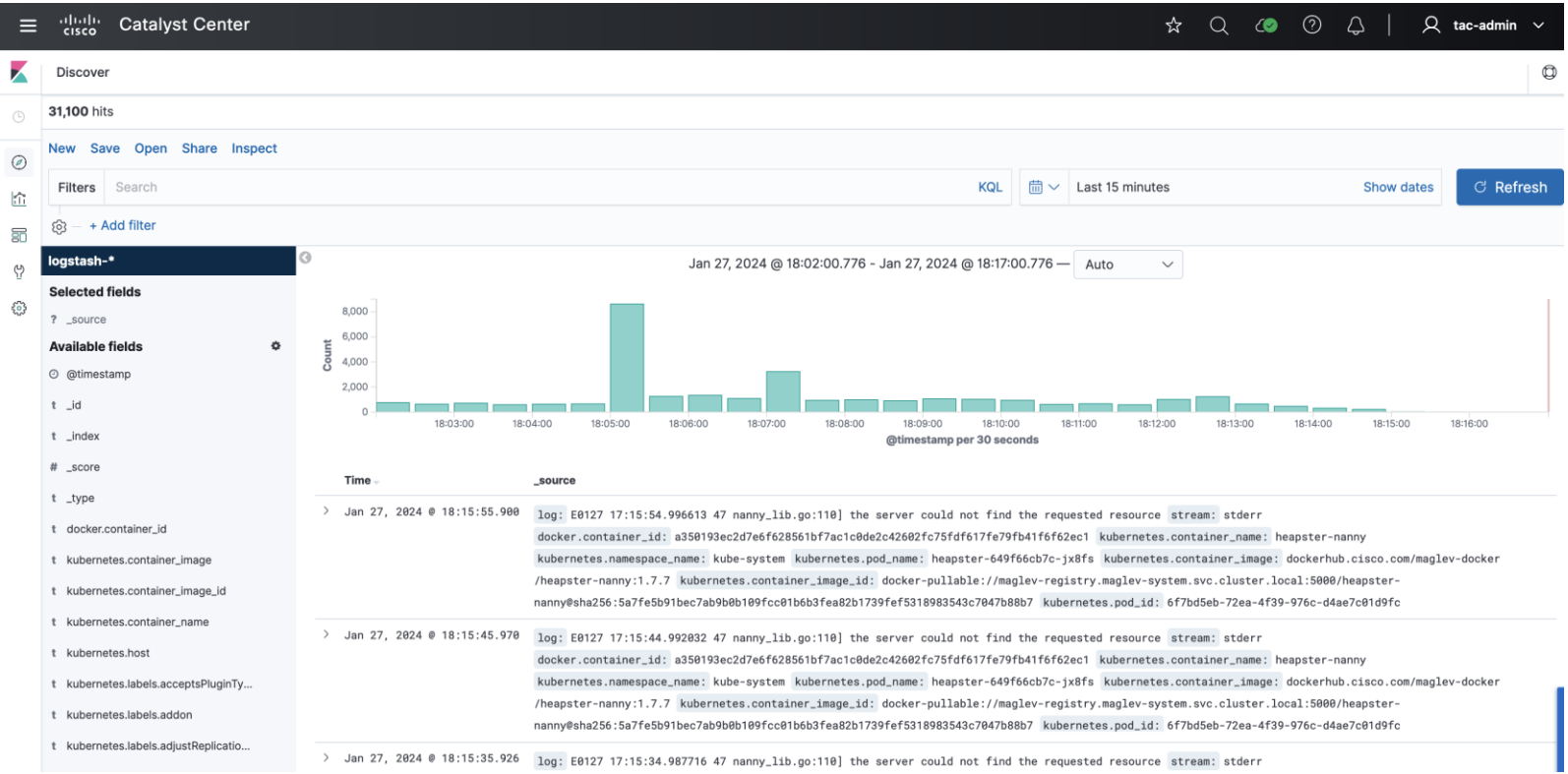
Log Explorer



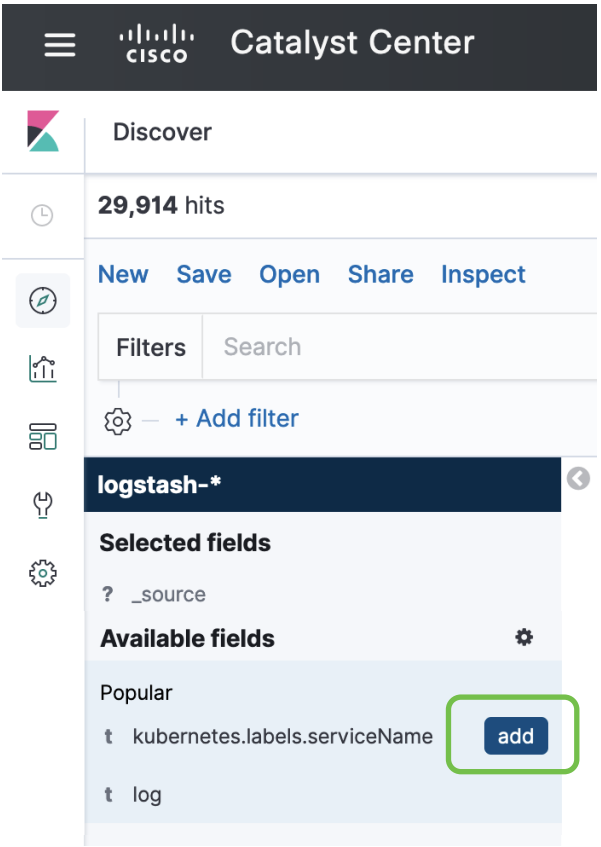
System 360: Cluster Tools – Log Explorer

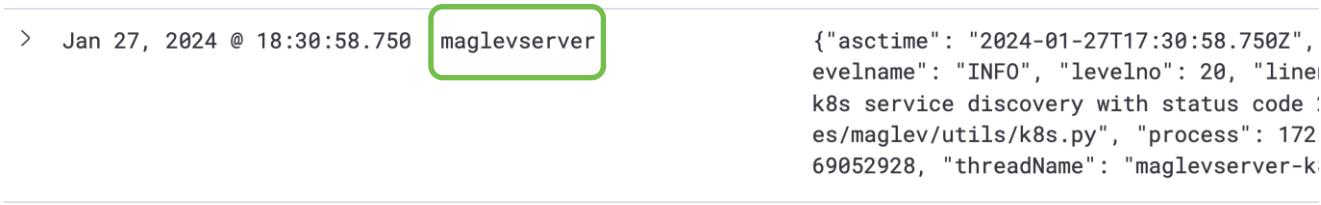


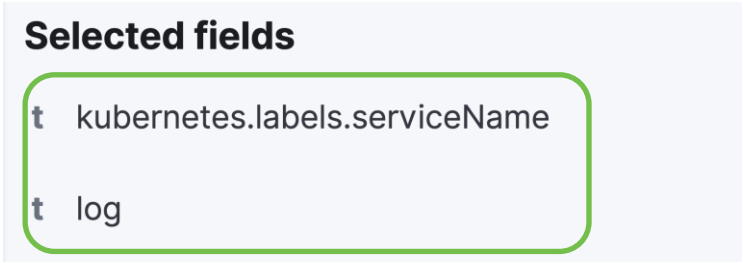
System 360: Cluster Tools – Log Explorer

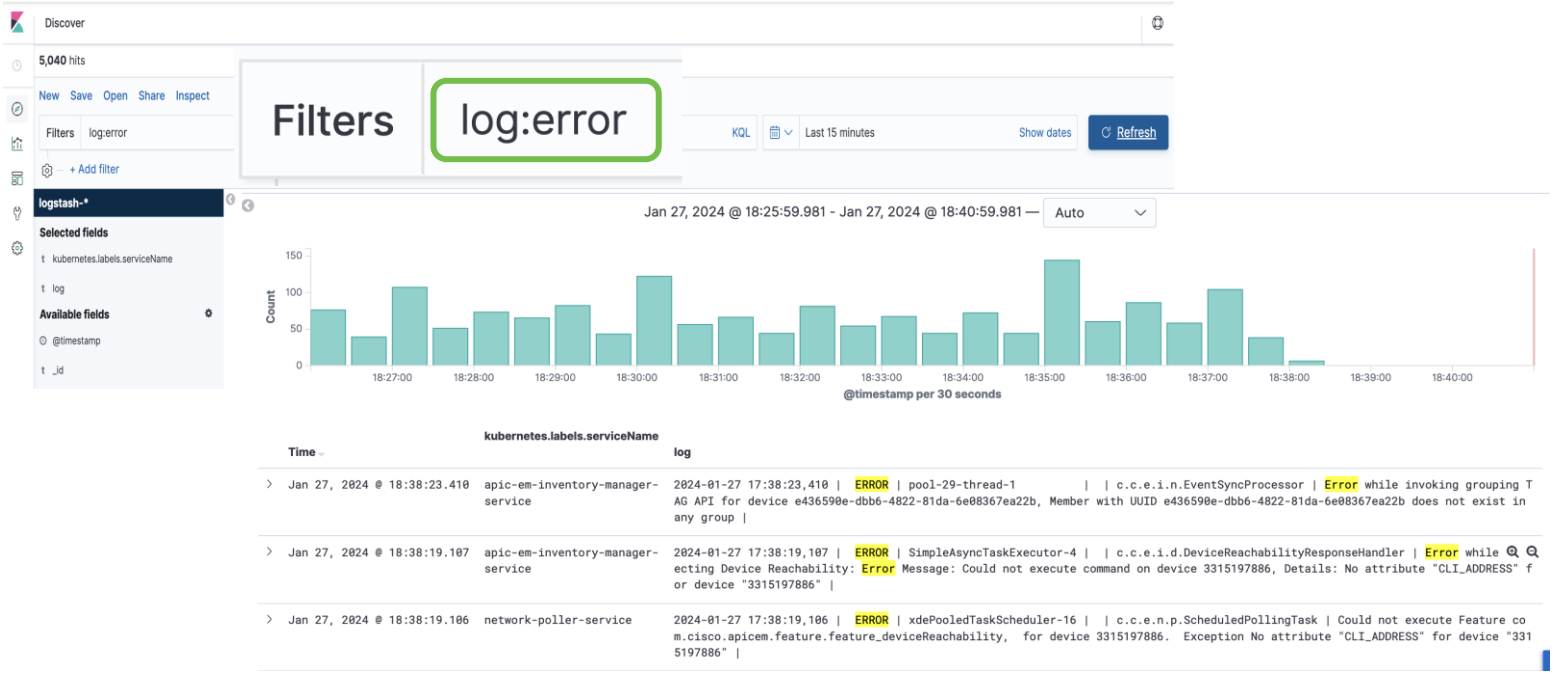


Sample use case





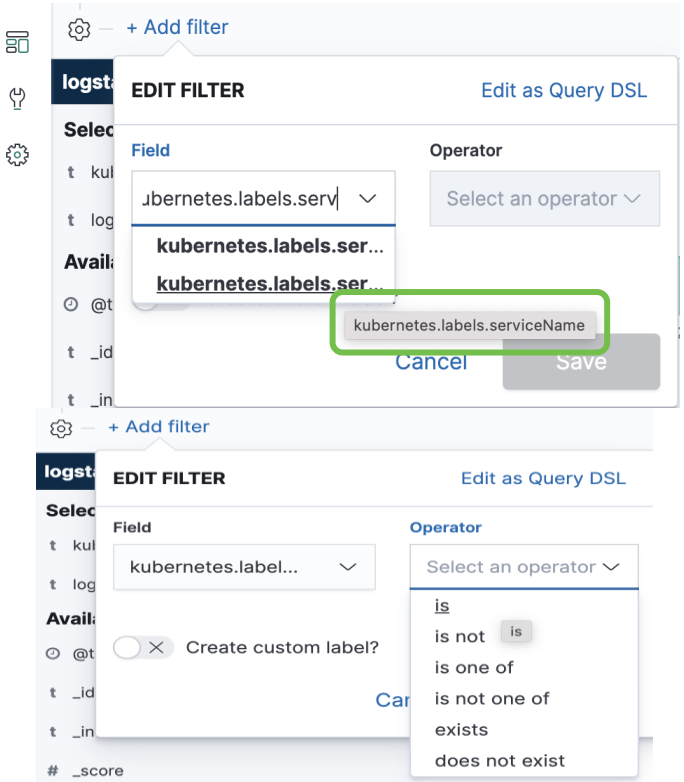


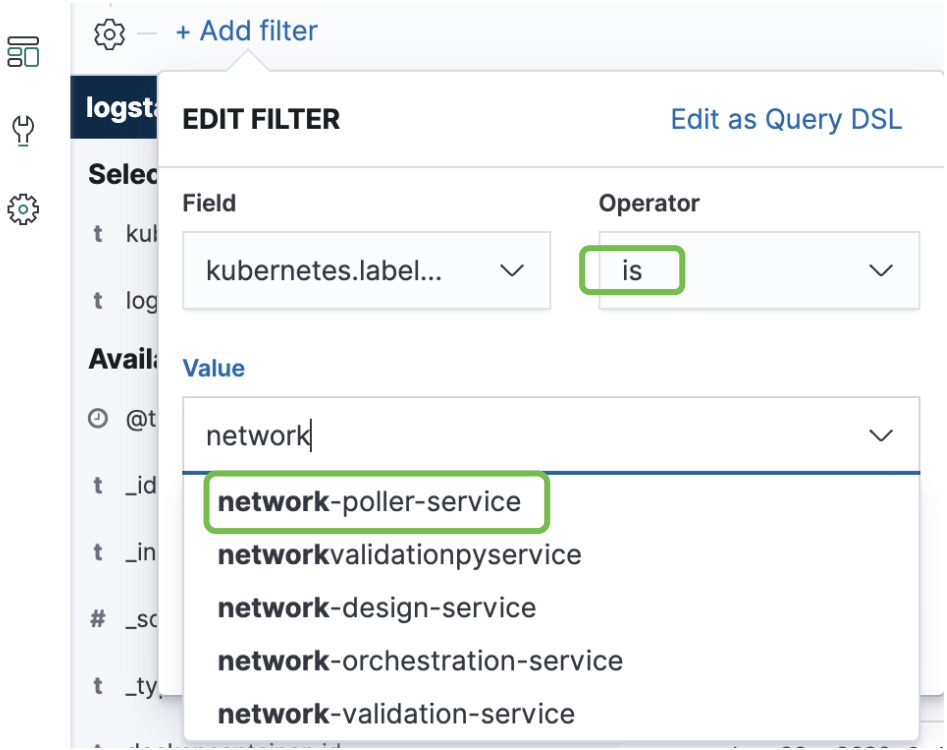


apic-em-inventory-manager-service

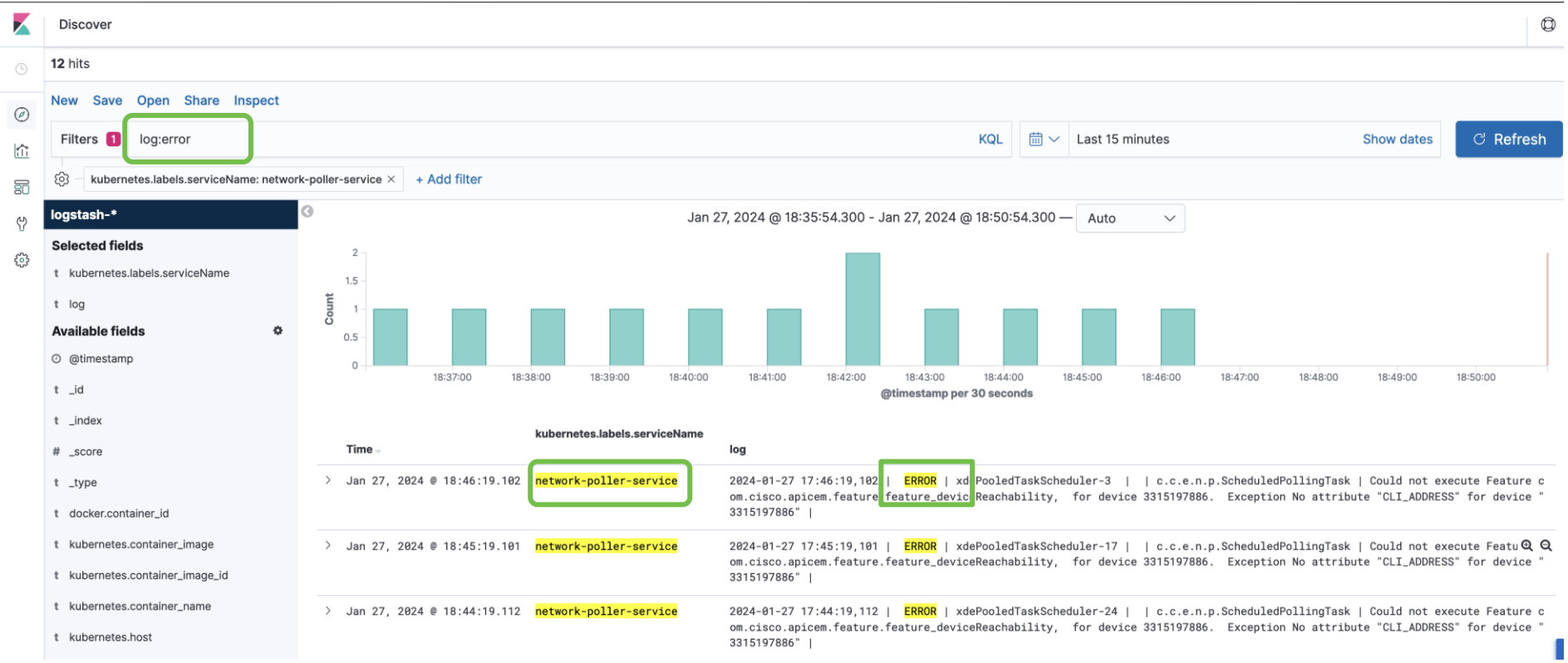
2024-01-27 17:38:19,107 | ERROR | SimpleAsyncTaskExecutor-4 | | c.c.e.i.d.DeviceReachabilityResponseHandler | Error while ecting Device Reachability: Error Message: Could not execute command on device 3315197886, Details: No attribute "CLI_ADDRESS" for device "3315197886" |

Sample use case with mix and match





Sample use case with Mix and Match



Microservices – Reference

Inventory

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

Provisioning

spf-service-manager
network-programmer
template-programmer
kong

ISE Integration

pki-broker
network-design
identity-manager-pxgrid
jboss-ejbca
kong

SWIM

swim
dna-common
network-design
network-programmer
kong

Upgrades

catalogserver
workflow-server
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

Release 2.3.x

Cisco Catalyst Center Restricted Shell

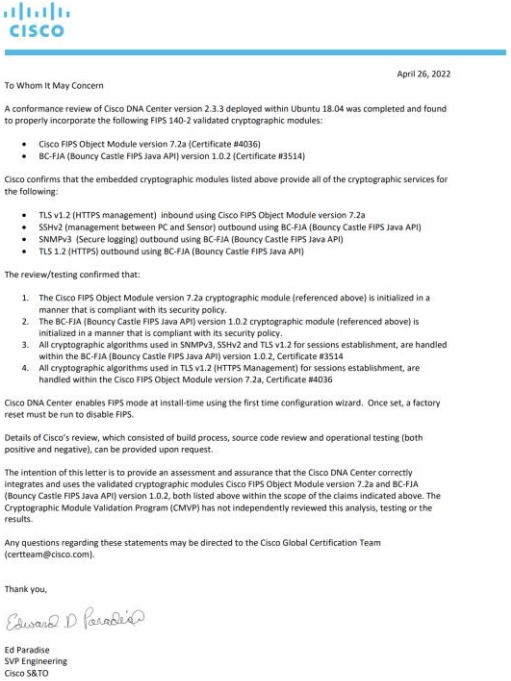
Description: For added security, the Cisco Catalyst Center is now FIPS 140-2 certified.

FIPS compliance disables access to the root shell (by default) and introduces a restricted shell (Magshell) in 2.3.x which can cause a challenge to troubleshooting in some scenarios.

Consent Token Authorization process enabled in 2.3.5.x.

Challenges:

- Restricted set of commands
- No access to native Linux Bash shell
- Troubleshooting tools like AURA will not work
- Required to contact TAC support to access the Linux Bash shell through a Consent Token Authorization process



cisco

April 26, 2022

To Whom It May Concern

A conformance review of Cisco DNA Center version 2.3.3 deployed within Ubuntu 18.04 was completed and found to properly incorporate the following FIPS 140-2 validated cryptographic modules:

- Cisco FIPS Object Module version 7.2a (Certificate #4036)
- BC-FJA (Bouncy Castle FIPS Java API) version 1.0.2 (Certificate #3514)

Cisco confirms that the embedded cryptographic modules listed above provide all of the cryptographic services for the following:

- TLS v1.2 (HTTPS management) inbound using Cisco FIPS Object Module version 7.2a
- SSHv2 (management between PC and Sensor) outbound using BC-FJA (Bouncy Castle FIPS Java API)
- SNMPv3 (Secure logging) outbound using BC-FJA (Bouncy Castle FIPS Java API)
- TLS 1.2 (HTTPS) outbound using BC-FJA (Bouncy Castle FIPS Java API)

The review/testing confirmed that:

1. The Cisco FIPS Object Module version 7.2a cryptographic module (referenced above) is initialized in a manner that is compliant with its security policy.
2. The BC-FJA (Bouncy Castle FIPS Java API) version 1.0.2 cryptographic module (referenced above) is initialized in a manner that is compliant with its security policy.
3. All cryptographic algorithms used in SNMPv3, SSHv2 and TLS v1.2 for sessions establishment, are handled within the BC-FJA (Bouncy Castle FIPS Java API) version 1.0.2, Certificate #3514
4. All cryptographic algorithms used in TLS v1.2 (HTTPS Management) for sessions establishment, are handled within the Cisco FIPS Object Module version 7.2a, Certificate #4036

Cisco DNA Center enables FIPS mode at install-time using the first time configuration wizard. Once set, a factory reset must be run to disable FIPS.

Details of Cisco's review, which consisted of build process, source code review and operational testing (both positive and negative), can be provided upon request.

The intention of this letter is to provide an assessment and assurance that the Cisco DNA Center correctly integrates and uses the validated cryptographic modules Cisco FIPS Object Module version 7.2a and BC-FJA (Bouncy Castle FIPS Java API) version 1.0.2, both listed above within the scope of the claims indicated above. The Cryptographic Module Validation Program (CMVP) has not independently reviewed this analysis, testing or the results.

Any questions regarding these statements may be directed to the Cisco Global Certification Team (certteam@cisco.com).

Thank you,

Edward D Paradise

Ed Paradise
SVP Engineering
Cisco S&TO

Release 2.3.3.x

Cisco Catalyst Center Restricted Shell

- Commands to disable / enable root access from CLI

Command to enable the BASH shell

```
$ _shell -c 'sudo magctl ssh shell bash'
Password:
Warning! Activity within this shell can jeopardize the functioning of the system!
[sudo] password for maglev:
Successfully enabled bash for user, will be effective from next login.

$
```

Command to disable the BASH shell

```
$ sudo magctl ssh shell magshell
[sudo] password for maglev:
Successfully enabled magshell for user, will be effective from next login.

$
```

Cisco Catalyst Center Restricted Shell

Release 2.3.5.x onwards

- Consent Token

1. Command '_shell' to generate the challenge string

2. Specify the time-out (default is 4 days)

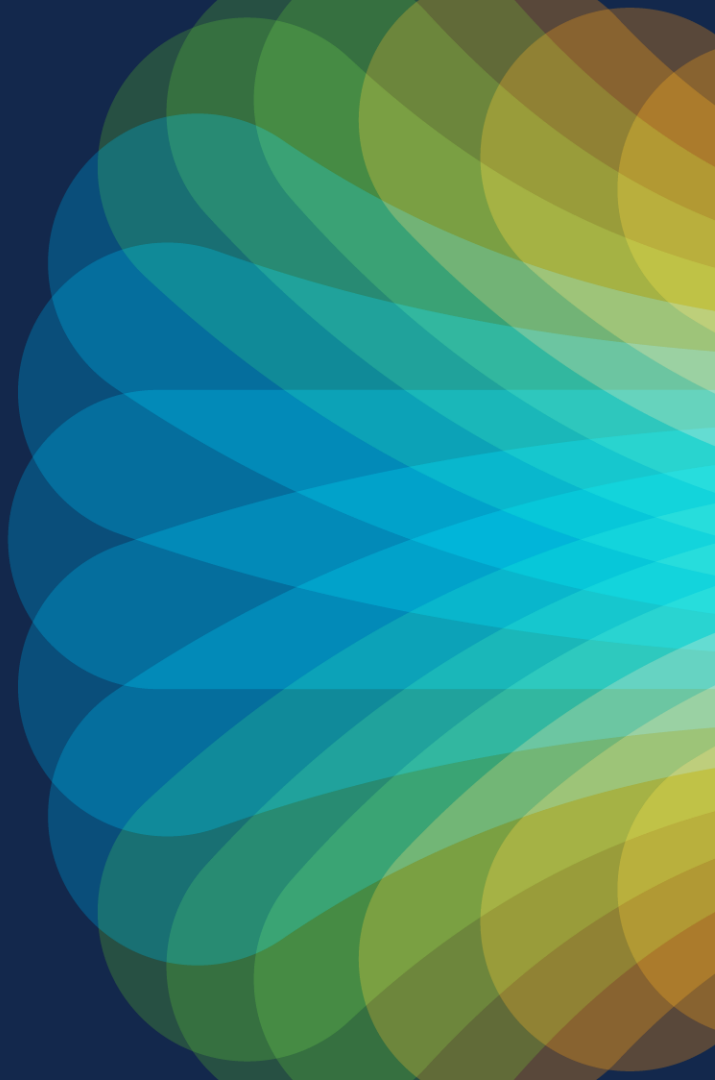
```
$ _shell
Please secure authentication via request of a consent token for bash shell-access.
Proceed to generate a challenge? [y/n] : y
Enter authentication time-out(in minutes - max 10080[default 4 days]) :
Generating Challenge.....................................
Challenge String (Please copy everything between the asterisk lines exclusively):
********************************************************************************************
BrQOaAAAAQUBAAQAAAABAgAEAAAAAAMACAAAAAAAAAAABAAQ32GC3XwzhRKcsMilrzAzhAUABAAAFoAGAARETkFDBwAMTUFHU0hFTExfQ1...
********************************************************************************************
Validate the generated challenge using [_shell -v] command for bash shell-access.
[Thursday Aug 11 15:51:40 UTC] maglev@40.0.0.171 (maglev-master-40-0-0-171)
```

3. Share the Challenge String with the TAC engineer

4. Command '_shell -v' to enter the response token received from TAC

```
$ shell -v rQj8PQAAAQUBAAQ…
Warning! Activity within this shell can jeopardize the functioning of the system!
maglev@maglev-master-172-16-52-11:~$
```

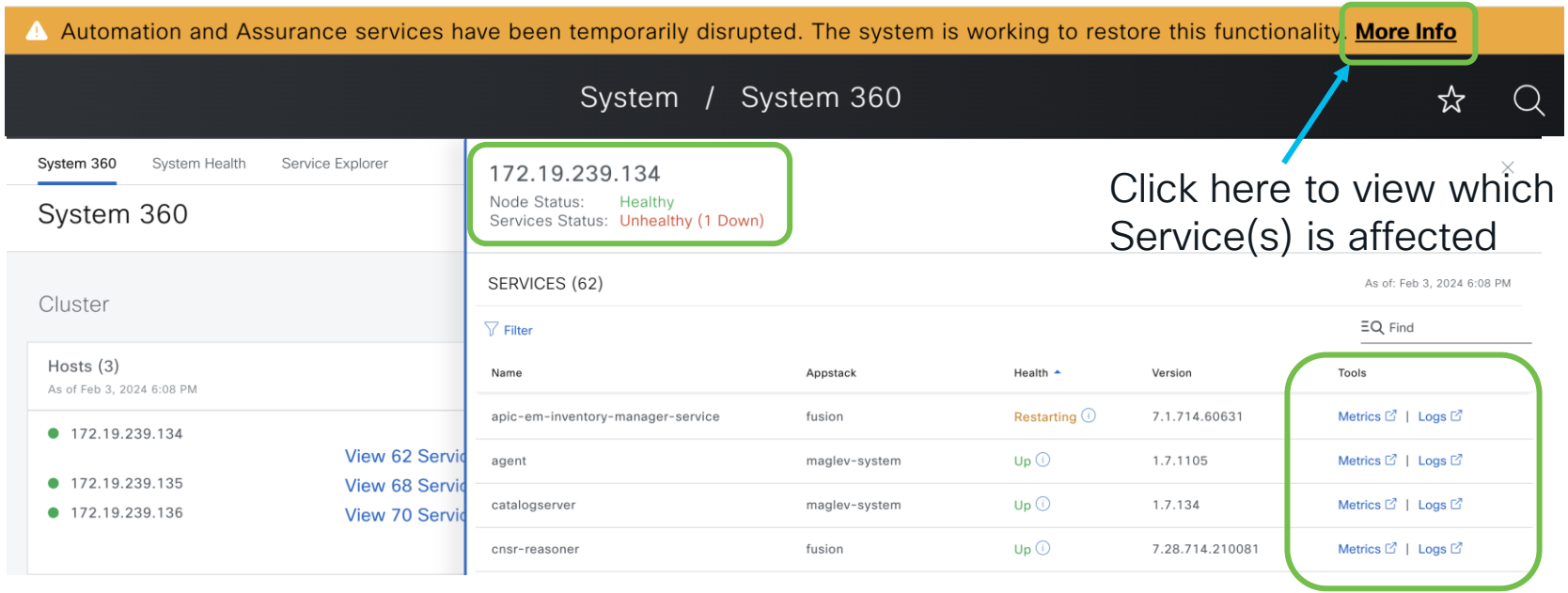
Cisco Catalyst Center Health



System in Self Monitoring Mode
Software Services

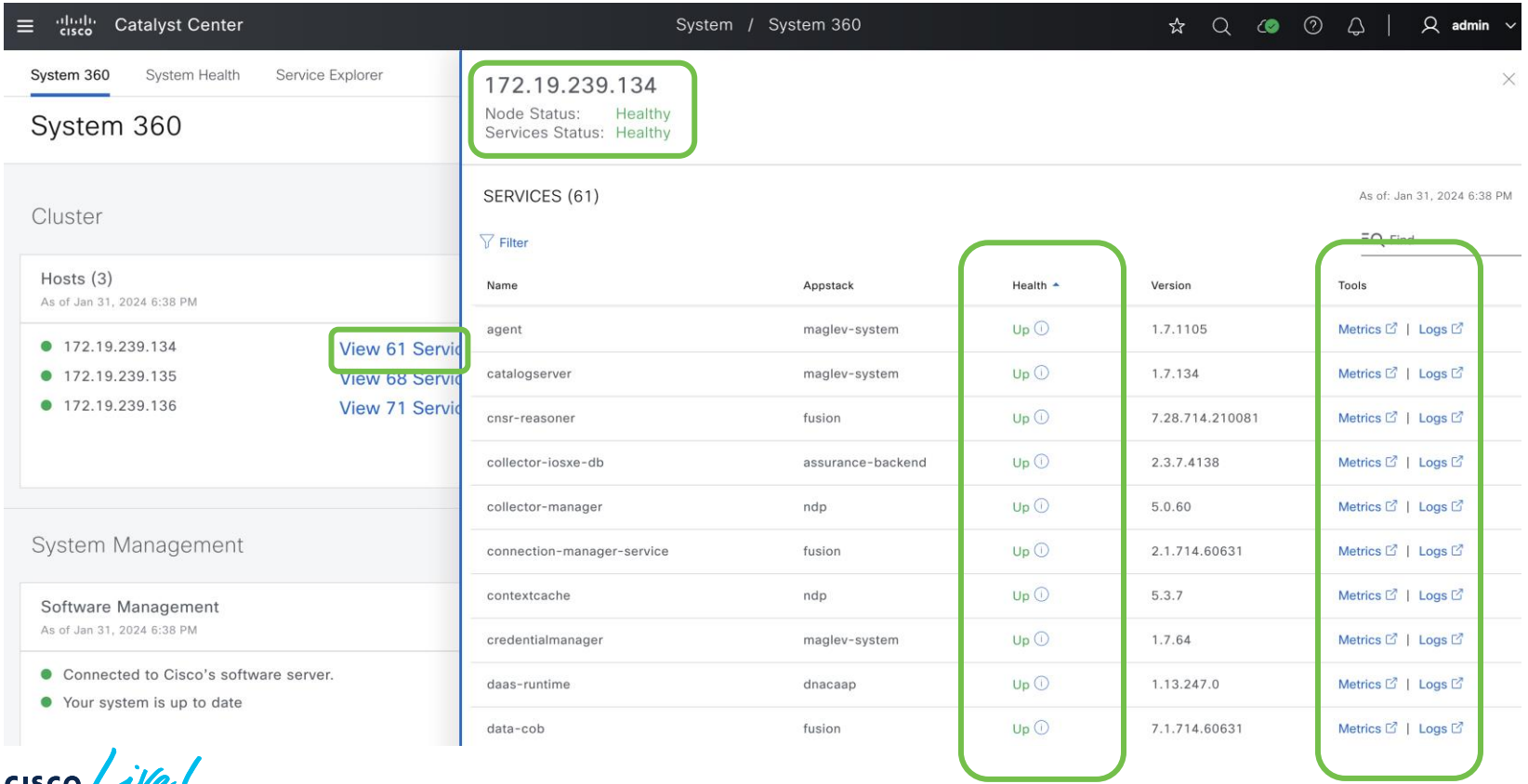
Release 2.2.x Onwards

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



Release 2.2.x Onwards

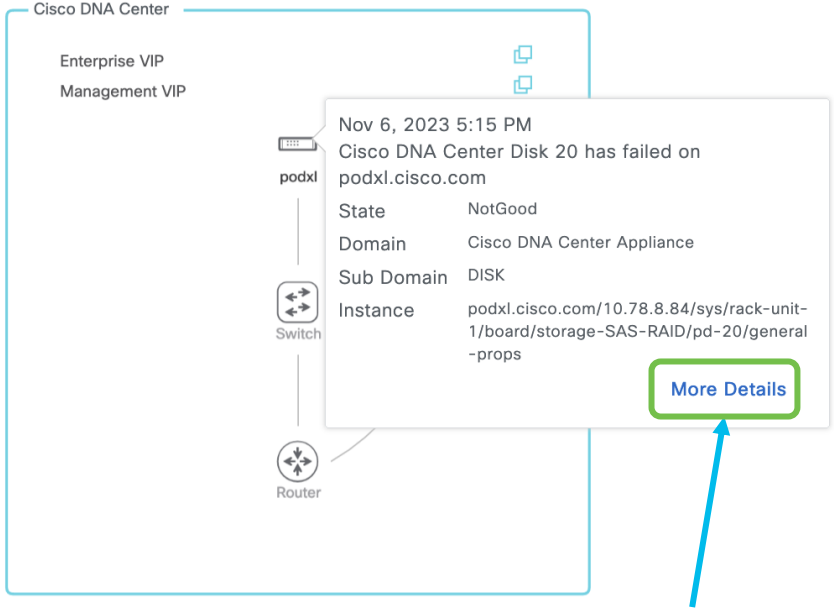
System in Self Monitoring Mode
Software Services



Release 2.3.5.x Onwards

System in Self Monitoring Mode

Hardware Health



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 in Self Monitoring Mode

Hardware Health

Release 2.3.5.x Onwards

Cisco DNA Center

1 System / Settings

Search Settings

- Cisco Accounts
- Device Settings
- External Services
- System Configuration
  - Debugging Logs
  - Proxy
  - High Availability
  - Integration Settings
  - System Health (2)
  - Login Message
- Terms and Conditions
- Trust & Privacy

Settings / System Configuration

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 Cisco DNA Center hardware.

Cisco DNA Center Address	Cisco IMC Address
10.105.192.135 (3)	NA

Edit Cisco DNA Center Server Configuration

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

Cisco DNA Center Address
10.105.192.135

4

Cisco IMC Address*

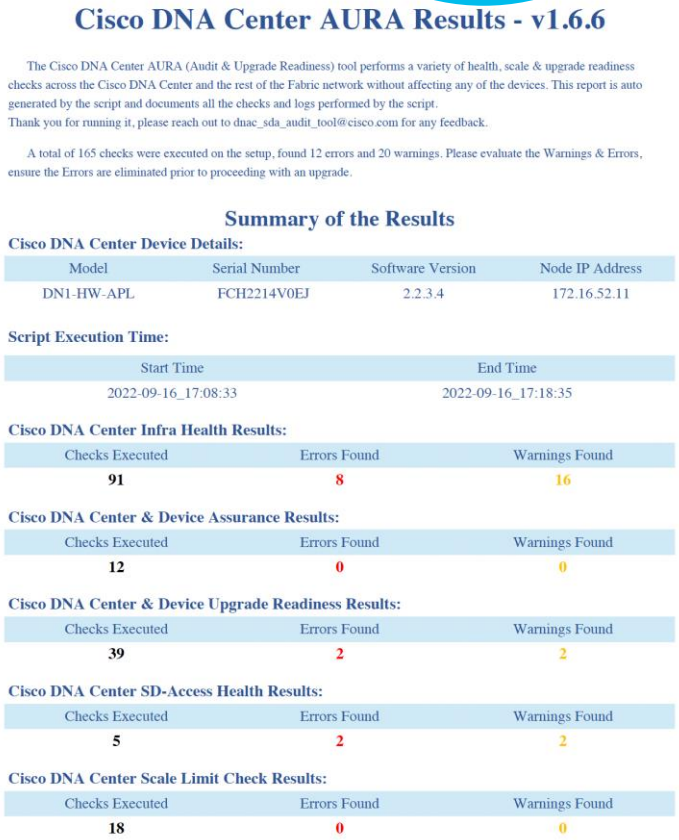
Cisco IMC Username*

Cisco IMC Password*

AURA – Health Checker Tool

Release 1.2.8 Onwards

- 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

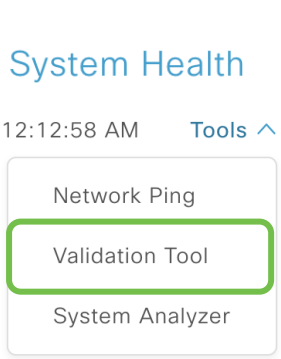
Cisco DNA Center SD-Access Health Results:

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

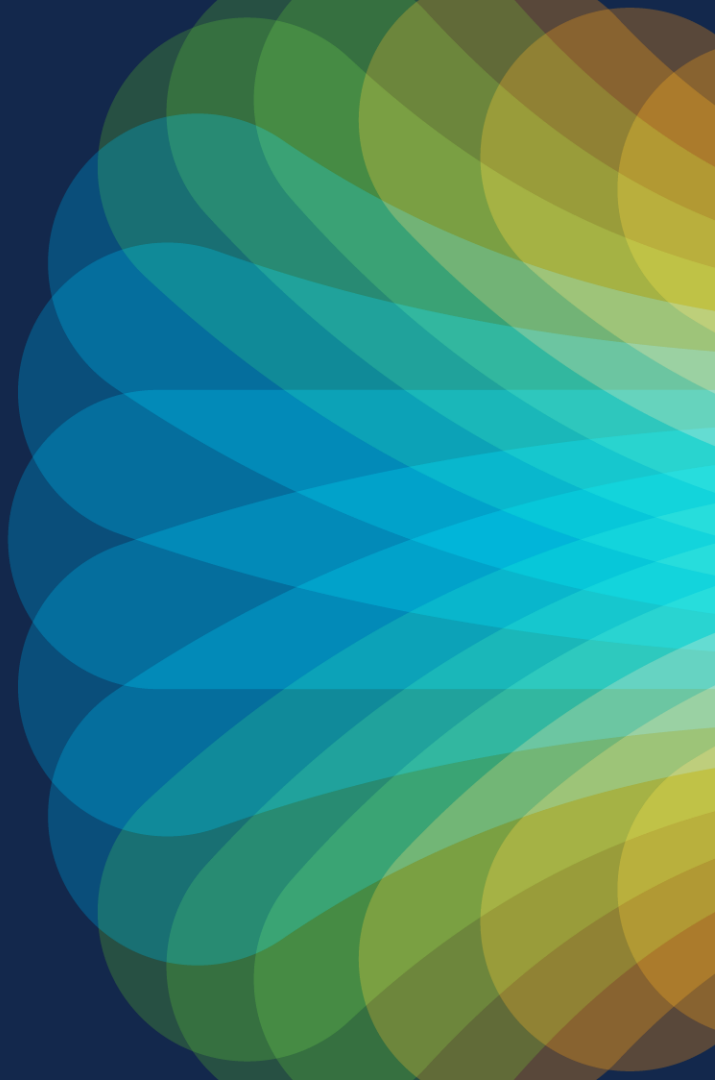
Cisco ISE Health and Cisco DNA Center Role

- 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

Cisco Catalyst Center Inventory



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
- LAN Automation
- RMA
- Run Commands …

Main Role of Inventory

Inventory Collection (Sync)

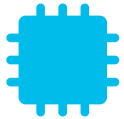
- Data collection via SNMP, CLI or Netconf
- Reports reachability & manageability status
- Convert data to database objects

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...)



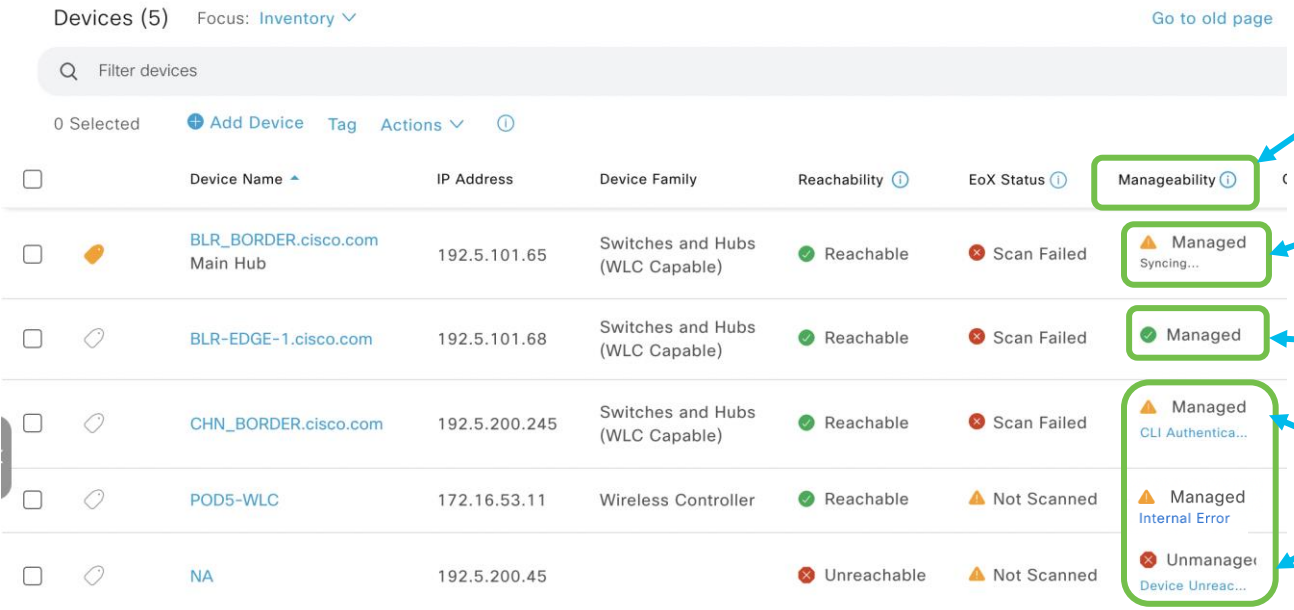
Multiple Memory Optimizations (shorter sync times especially for scaled setups, prevention of out of memory / crashes)

Grafana Inventory Dashboard (additional visibility and troubleshooting)

Visibility into Sync Errors (no more Partial Collection Failures)

Customer Voice

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



Whether the device is managed by Cisco Catalyst Center or not

Sync in progress

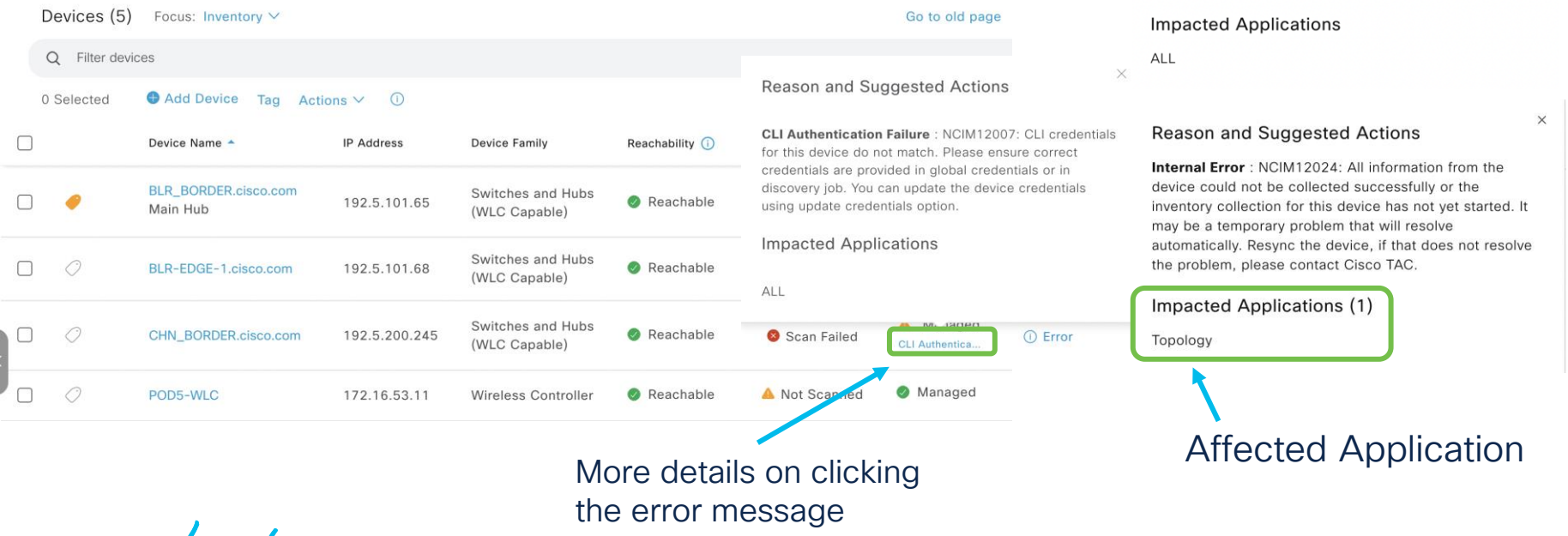
Successfully Managed

Errors

Customer Voice

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

Reason and Suggested Actions menu



More details on clicking the error message

Affected Application

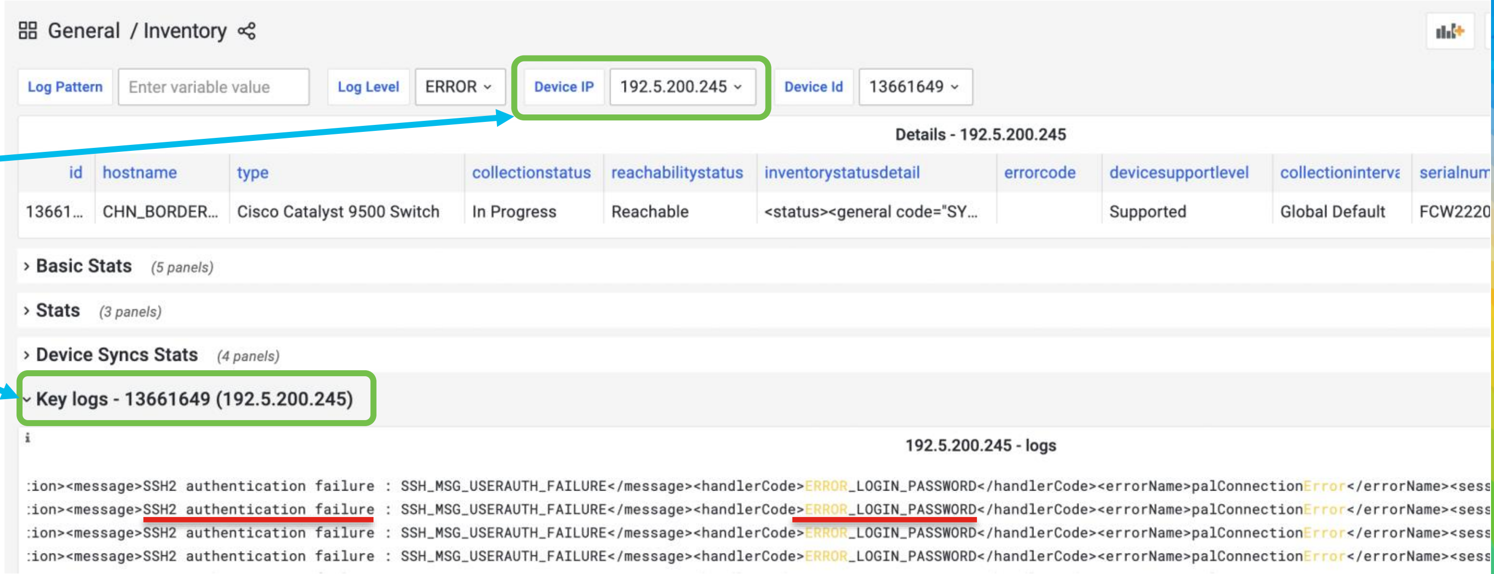
Customer Voice

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



Most useful in an XL or Cluster setup where multiple Inventory instances exist
Contact TAC to enable (disabled by default)

Customer Voice

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

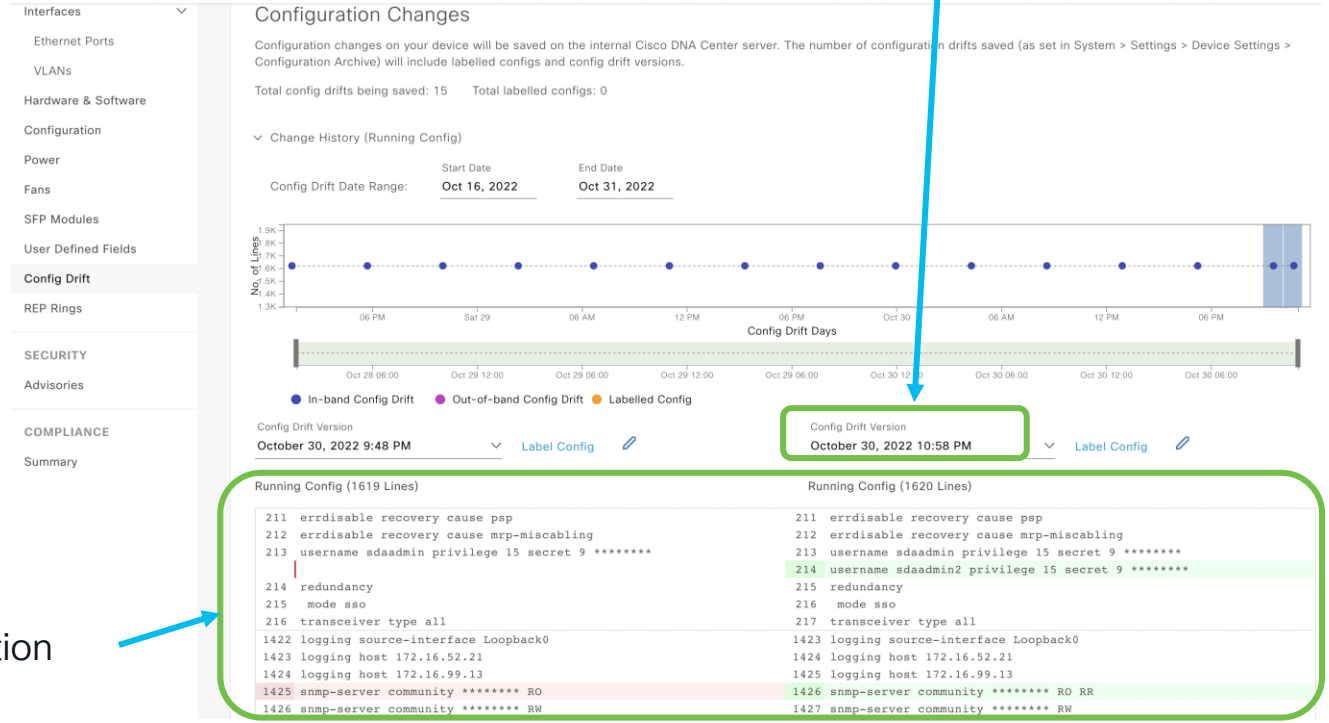
Provision / Inventory

View Device Details

Check for configuration changes
- Config Drift
- Device CLI

Changes to
- SNMP
- AAA
- HTTPS
- Netconf
- Certificates

Timestamp

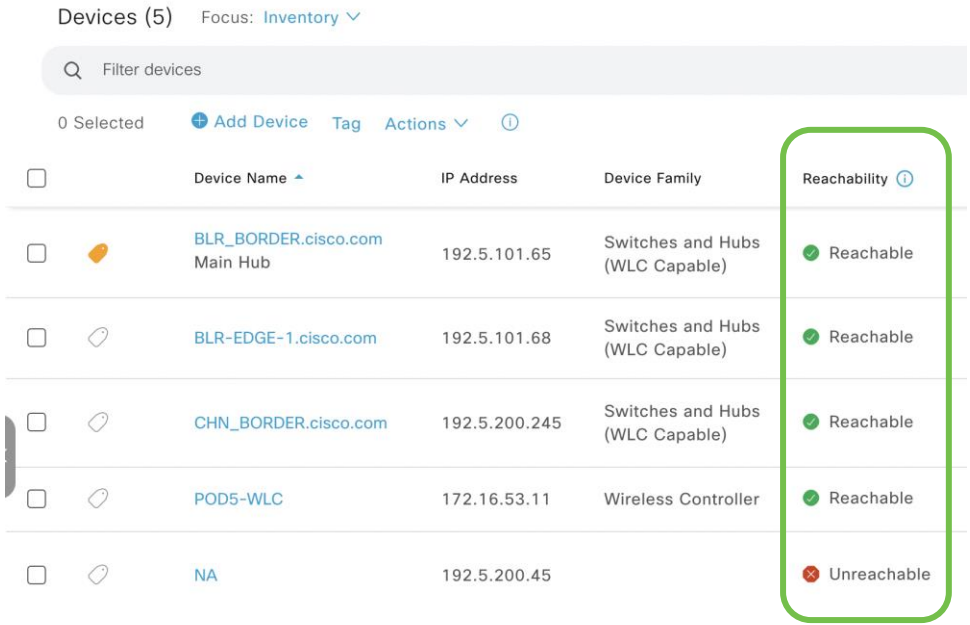


Configuration Diff

Customer Voice

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

Check 'Reachability' column to determine reachability



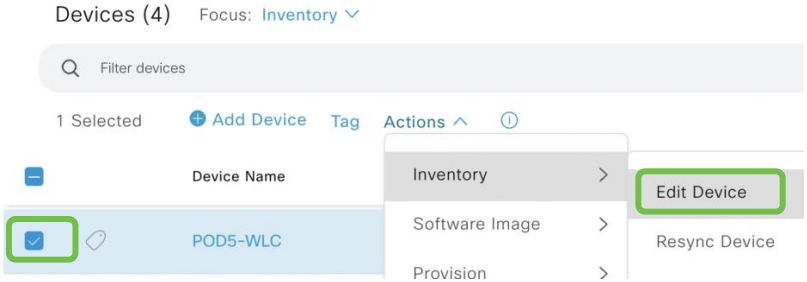
Status	Reachability
Reachable	Reachable via all mandatory protocols
Ping Reachable	Reachable via ICMP
Unreachable	Unreachable via all mandatory protocols

Customer Voice

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

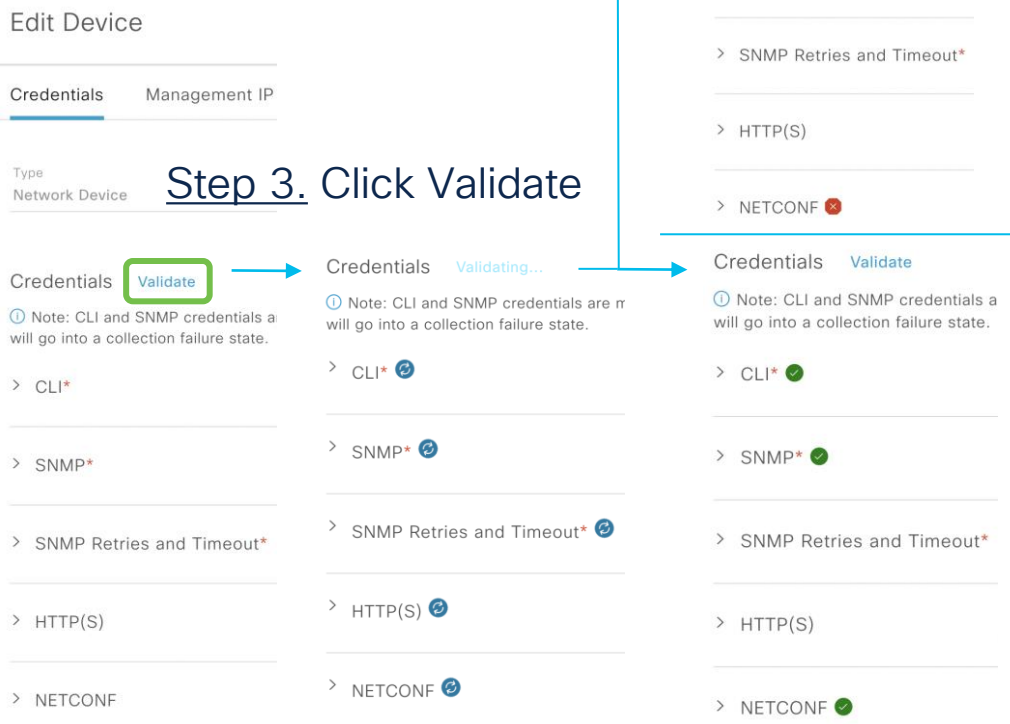
Verify Credentials

Step 1. Select device in Inventory



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

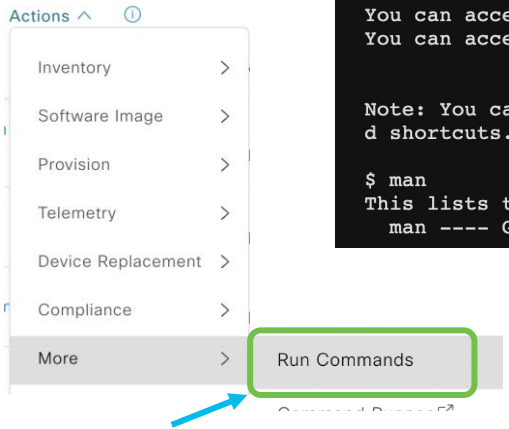
Step 3. Click Validate



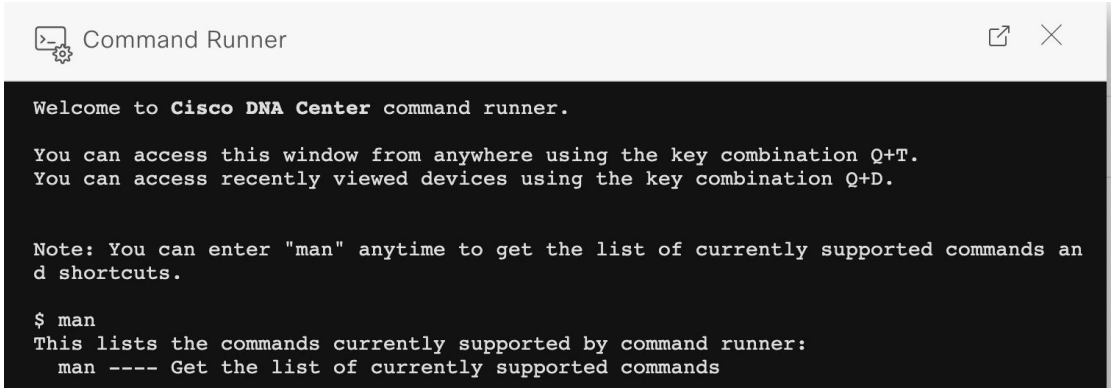
Customer Voice

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

Check device reachability from Cisco Catalyst Center



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>

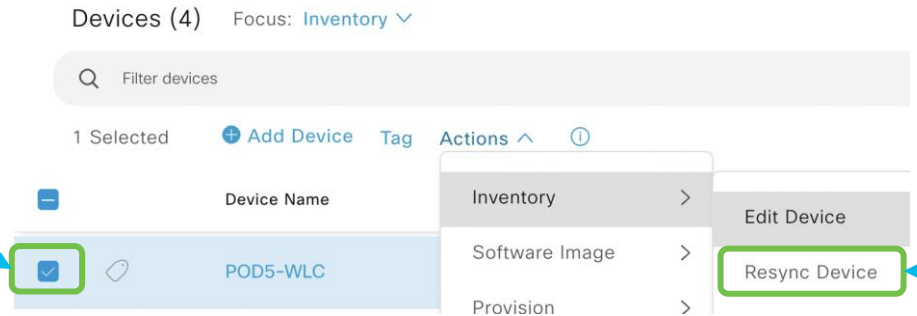
Netconf connectivity

ssh -p 830 <username>@<IP address>

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

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

Customer Voice

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

- Ensure no firewall blocking necessary ports

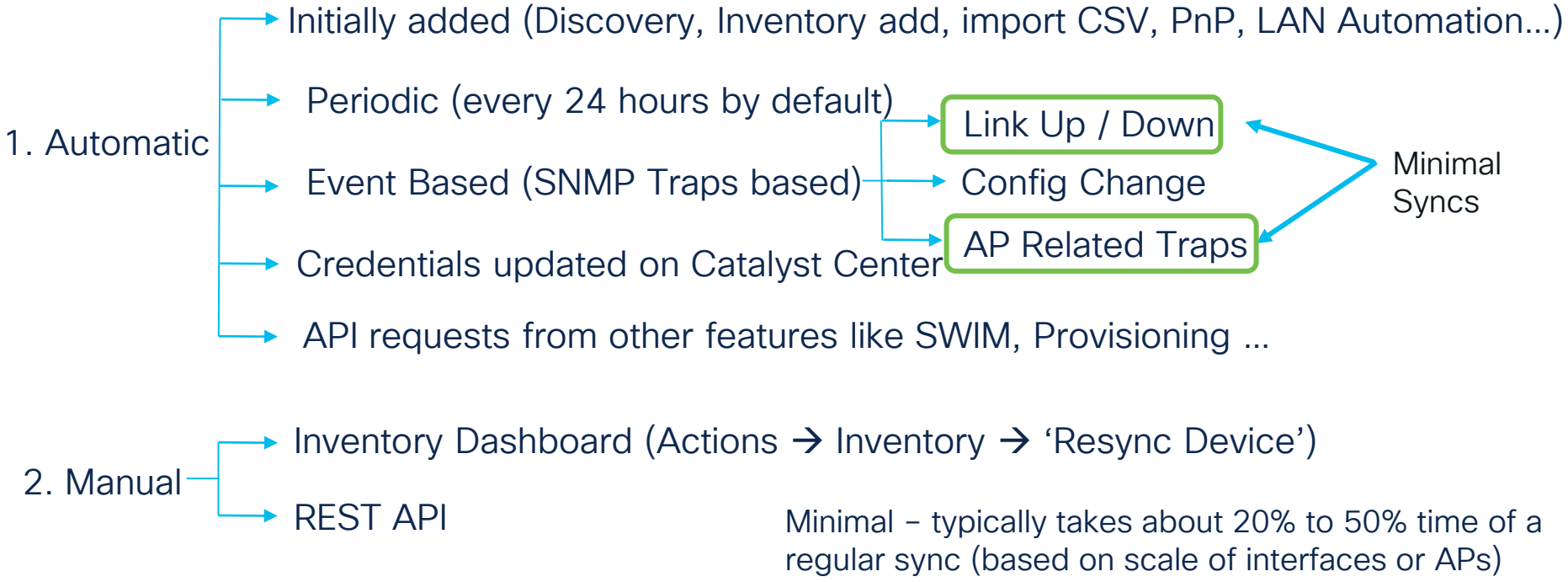
Cisco Catalyst Center to device **outbound** ports to be kept open

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

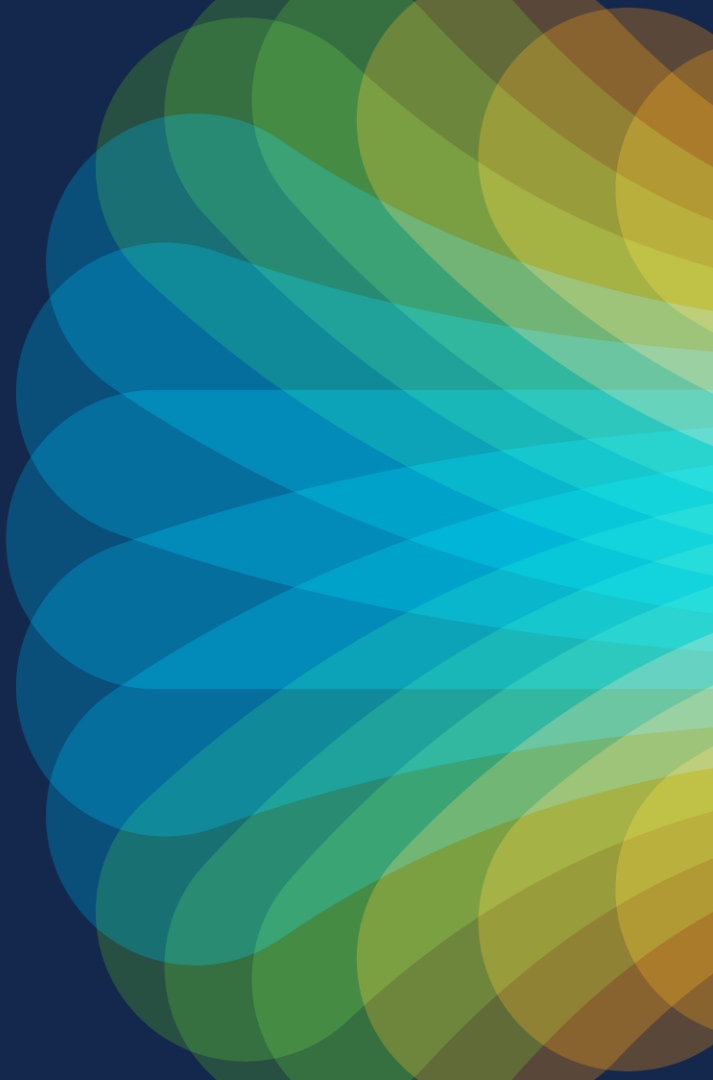
Customer Voice

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



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

Cisco Catalyst Center SWIM



SWIM Recap

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

2.3.7

Design > Image Repository	Inventory (Software Images focus)	System > Settings	Workflows (Image Update)
• Imports / stores the required images & patches (SMU) • Marking the images as Golden • Import the ISSU Compatibility Matrix	• Provisioning software images to the devices (Distribution + Activation) • Check Image update status • Perform Image update readiness	• Configure up to 3 external image distribution servers • Change the protocol order of an image distribution server	• 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

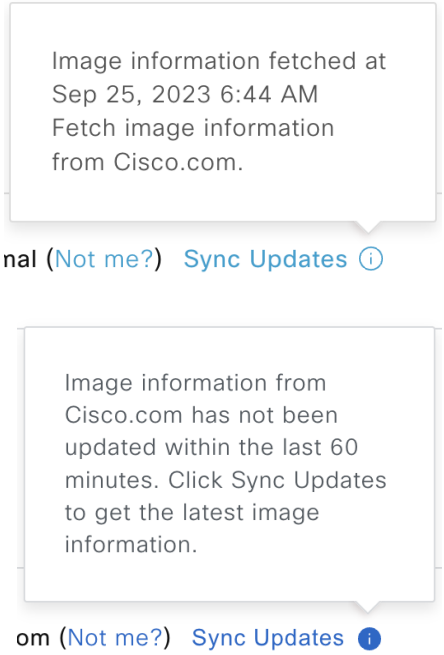
install activate <image name>

install commit

*Moved from Activate step to Distribute.

Common SWIM Issues – Image Repository

Issue 1. – Image information has not been updated



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.

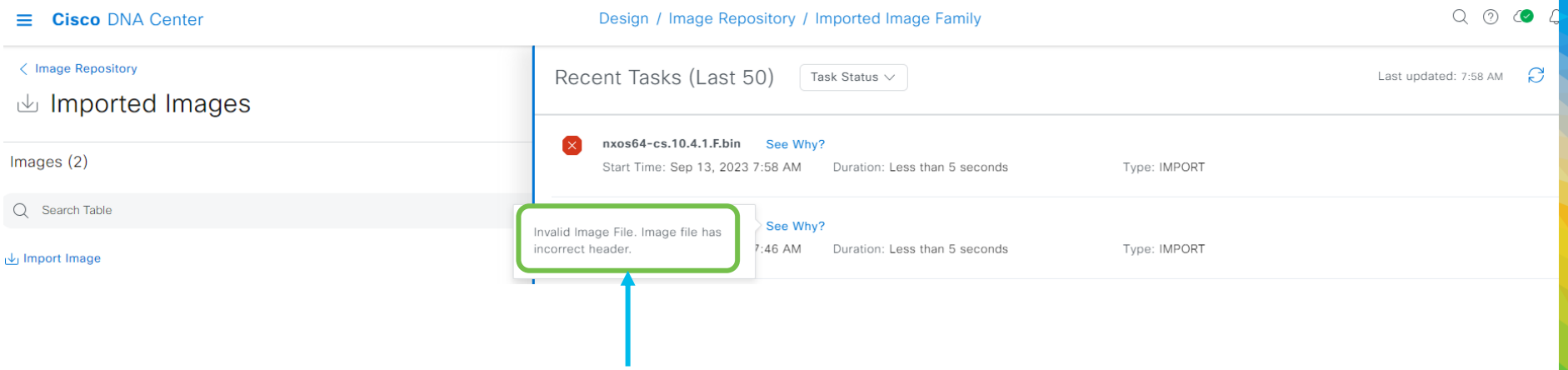
- http://ocsp.quovadisglobal.com
- http://crl.quovadisglobal.com/*
- http://*.identrust.com

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



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 Re-Execute Checks

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

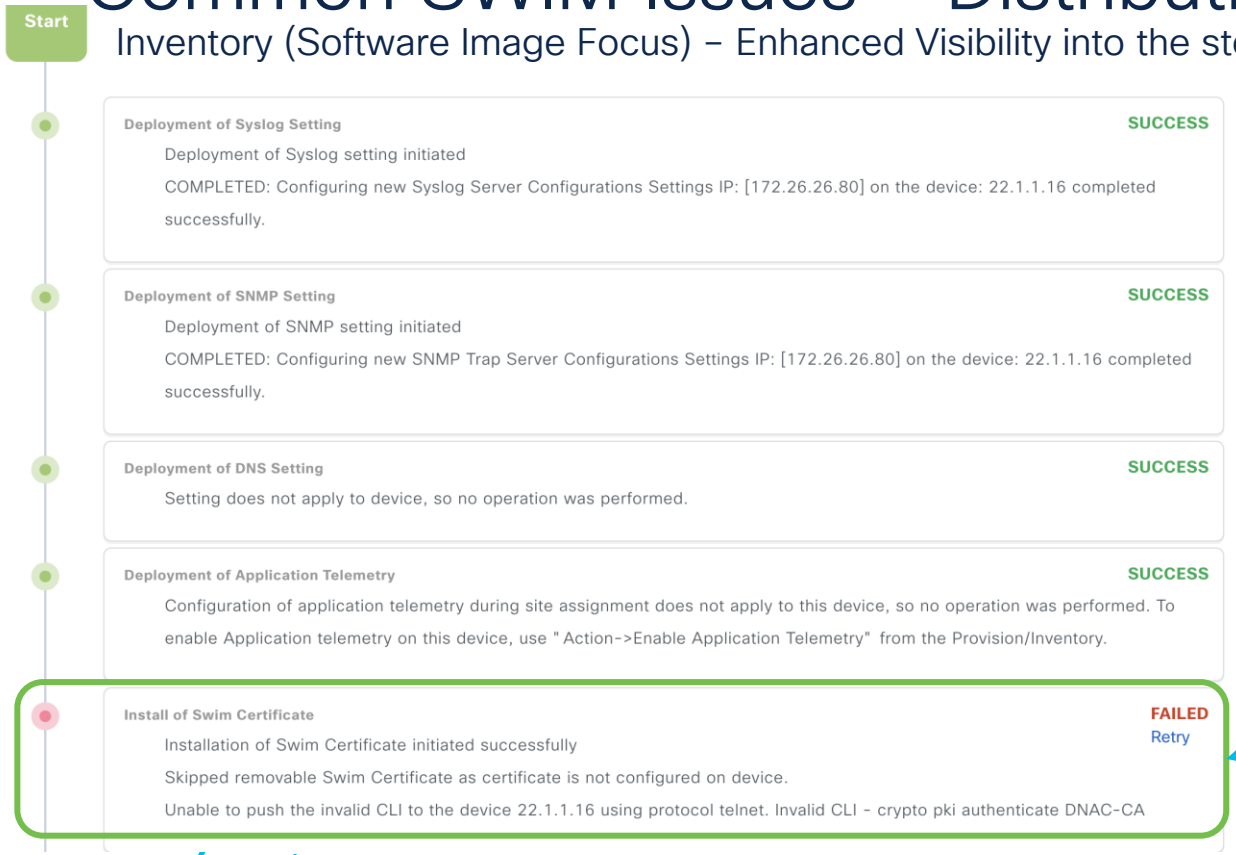
1. Device needs to be Managed & Reachable

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

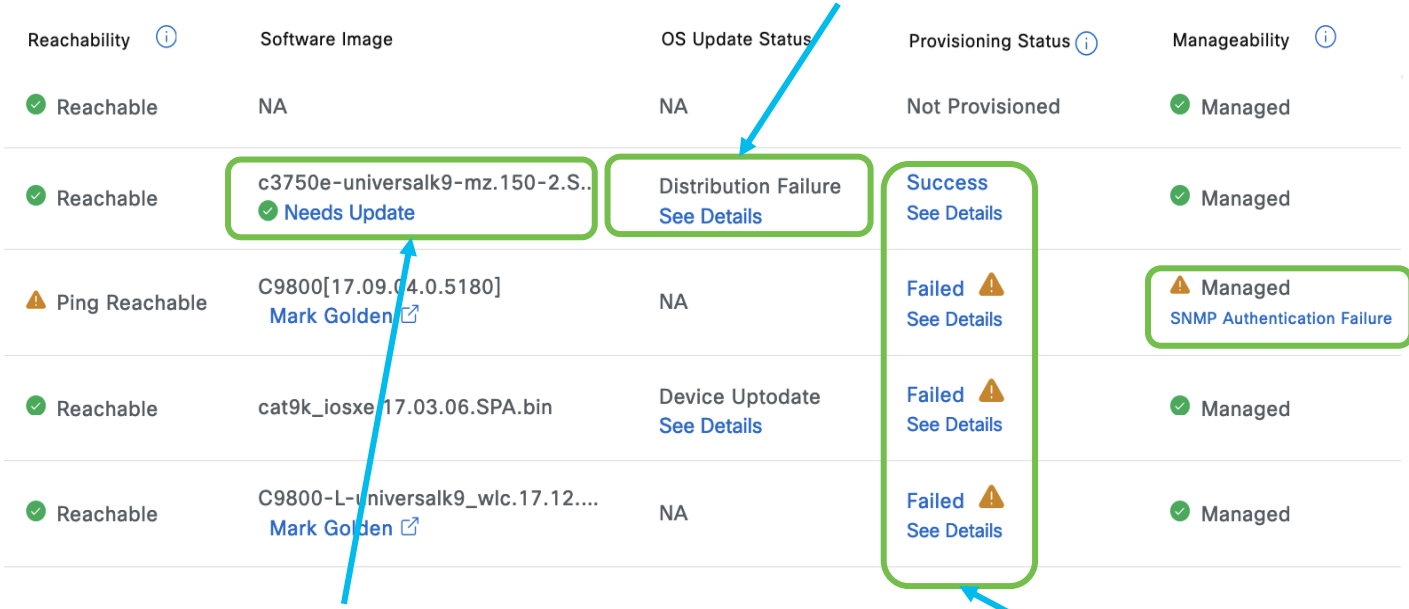


Example of a Failure

Common SWIM Issues – Distribution + Activation

Inventory (Software Image Focus)

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



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

Operations | Checks

Distribution — 4 minutes 40 seconds

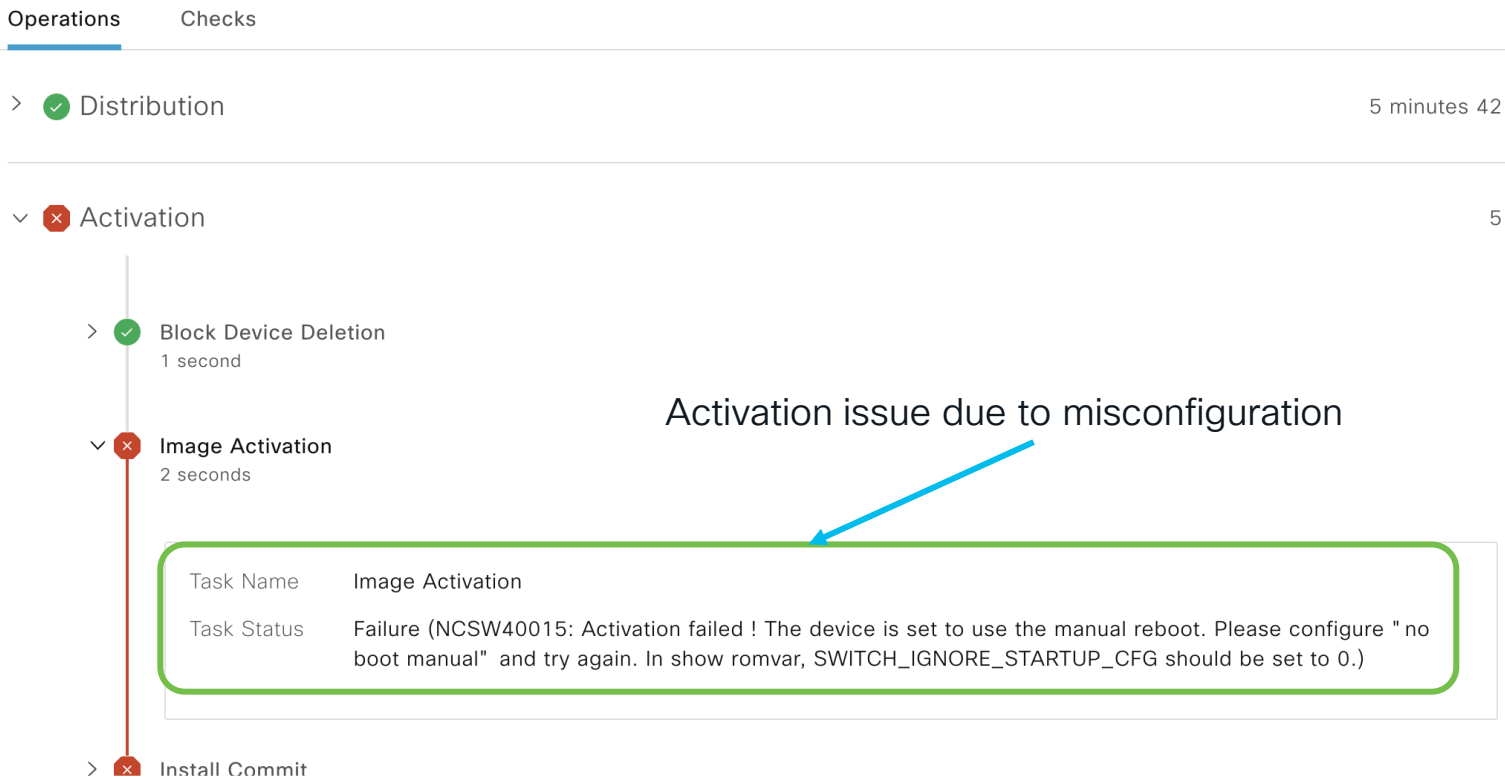
NCSW32001: Distribution failed using protocol: SCP. Distribution of image: c3750e-universalk9-tar.152-4.E10.tar on device. with protocol: SCP . Failed! Distribution of image: c3750e-universalk9-tar.152-4.E10.tar on device. with protocol: SCP . Flash Validation successfully completed. No Sufficient free 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**

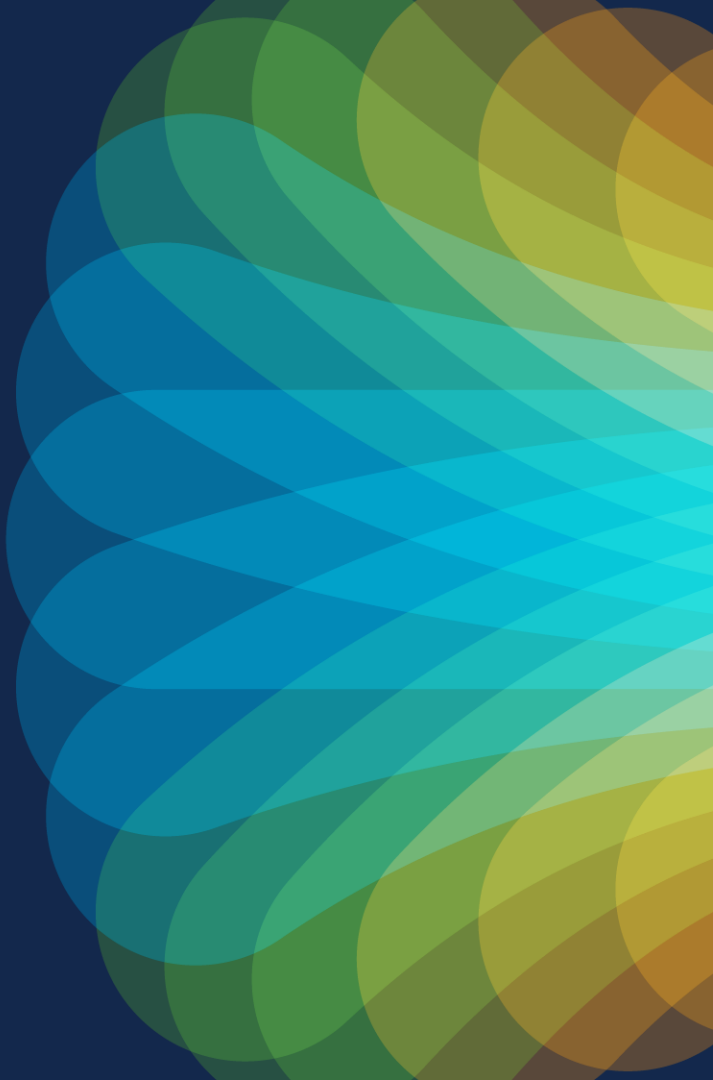
Distribution issue due to insufficient space in flash

Common SWIM Issues – Distribution + Activation

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



Cisco Catalyst Center Assurance



Assurance an End-to-End Visibility and Insights

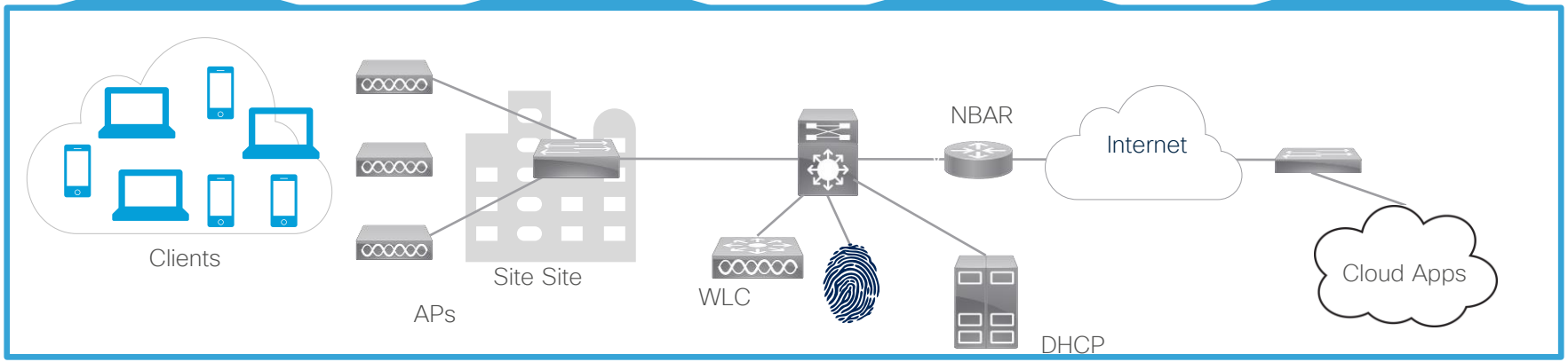
2.2.3

End user Client health and visibility

Network & Services health

Application visibility and performance

SD-Access health and status



Assurance 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

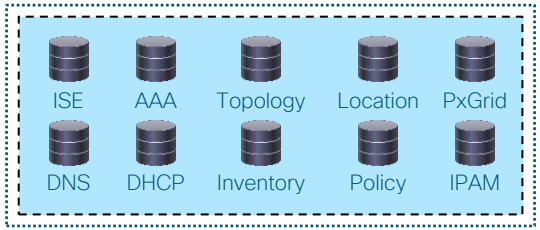
- Ensure Catalyst Center is set for SNMP trap server, Syslog server & Netflow collector server
- For Assurance from Wired clients, ensure “Cisco Catalyst Center Wired Endpoint Data Collection At This Site” is enabled
- For Wireless Assurance, ensure “Wireless Telemetry” is enabled

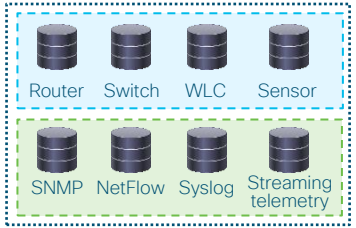
Assurance System Flow

Network

Contextual data

Network telemetry data





Device Checks

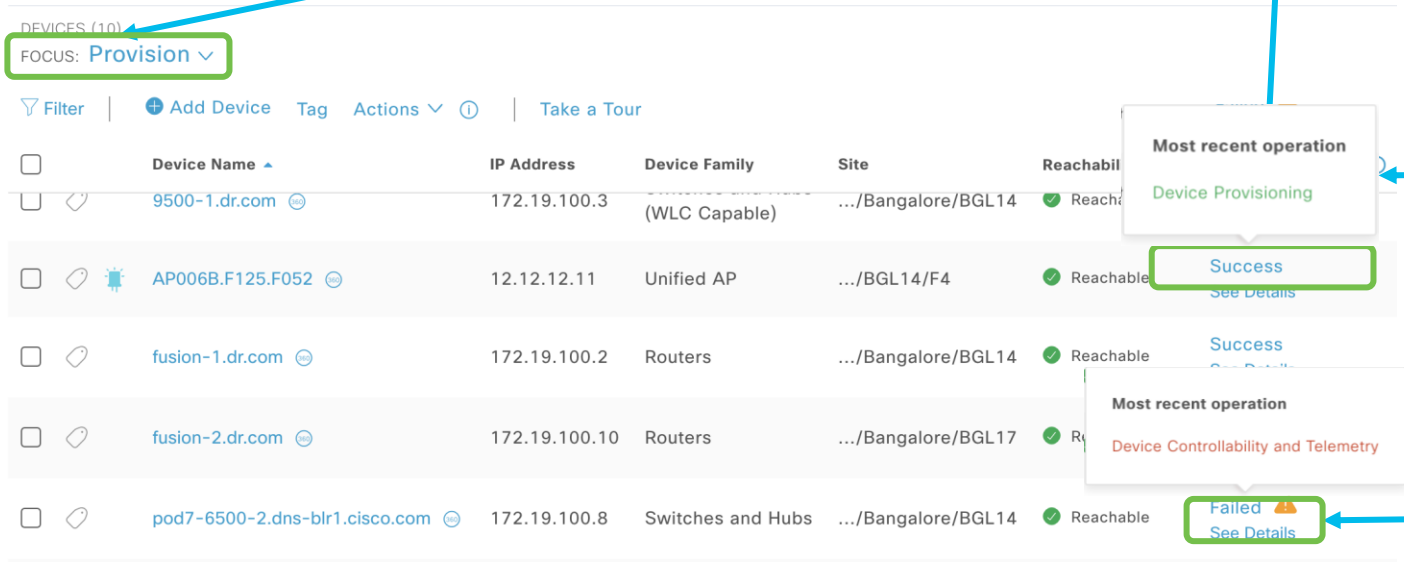
Configurations and Certificates

Release 2.3.3.x onwards

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



Success Scenario

Failure Scenario

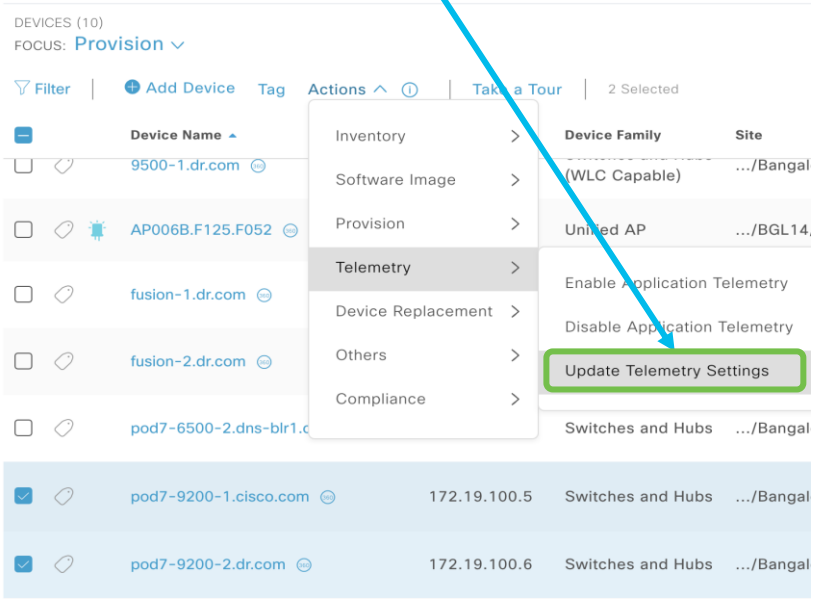
Step 3. Click to see configuration details in both scenarios

Device Checks
Configurations and Certificates

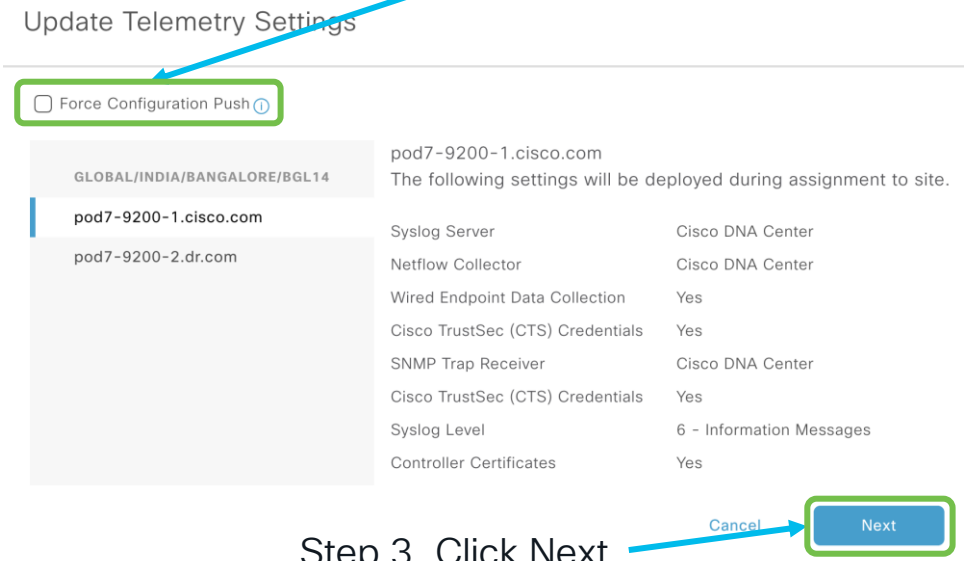
Release 2.3.3.x onwards

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’

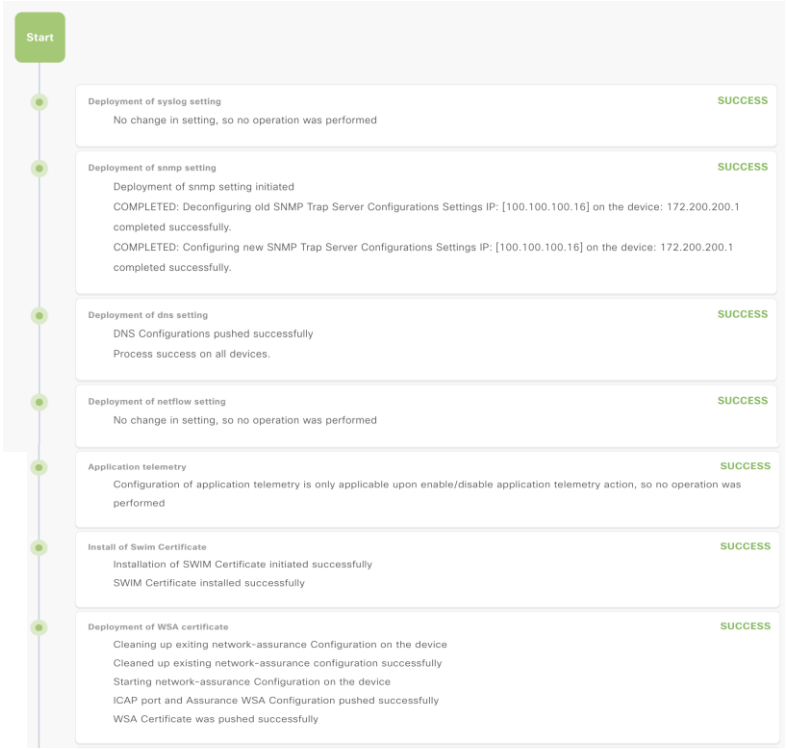


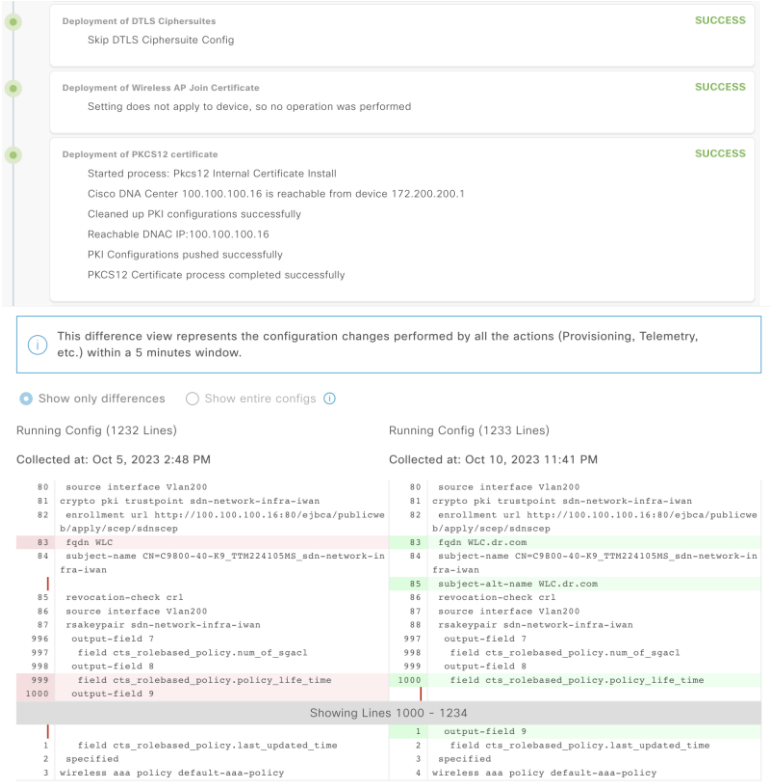
Step 3. Click Next

Device Checks
Configurations and Certificates

Release 2.3.3.x onwards

Details of configurations pushed and diff can be seen in the details





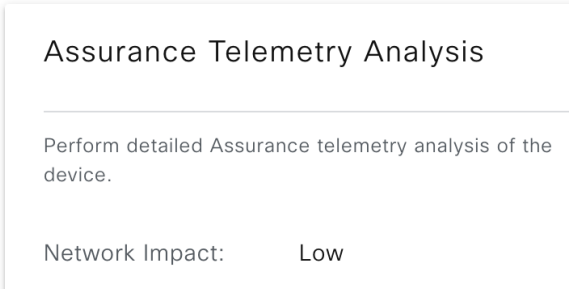
Device Checks

Verification Routines using the Network Reasoner

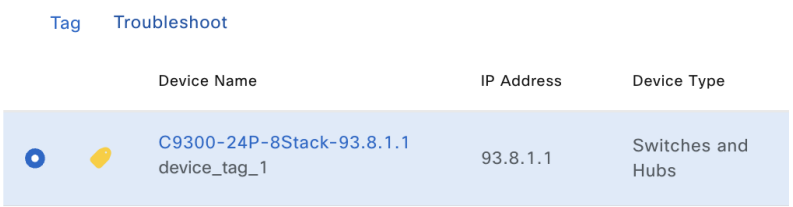
Release 2.3.5.x onwards

A sequence of network machine reasoning steps related to Assurance for various configuration/settings related issues in the network and the Catalyst Center.

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



Step 2. Choose one device & click on Troubleshoot



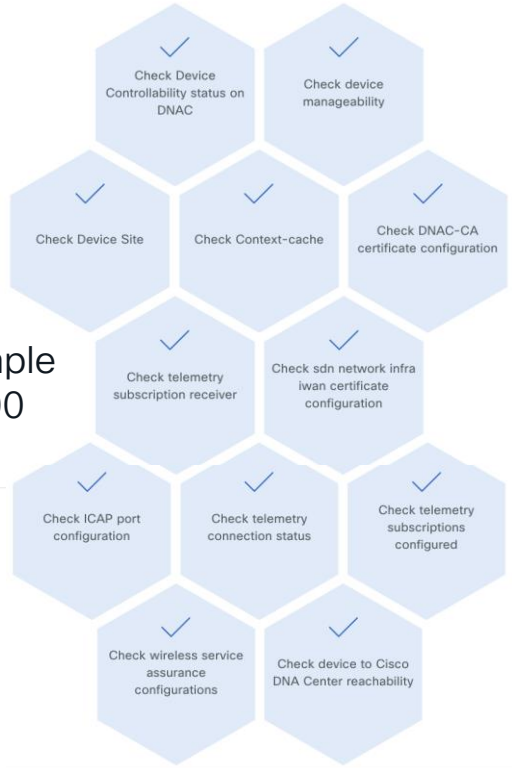
Device Checks

Verification Routines using the Network Reasoner

Release 2.3.5.x onwards

Example 1. Sample output for a 9800 WLC

Example 2. Sample output for a 9300 switch



Device Checks

Verification Routines using the Network Reasoner

Release 2.3.5.x onwards

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

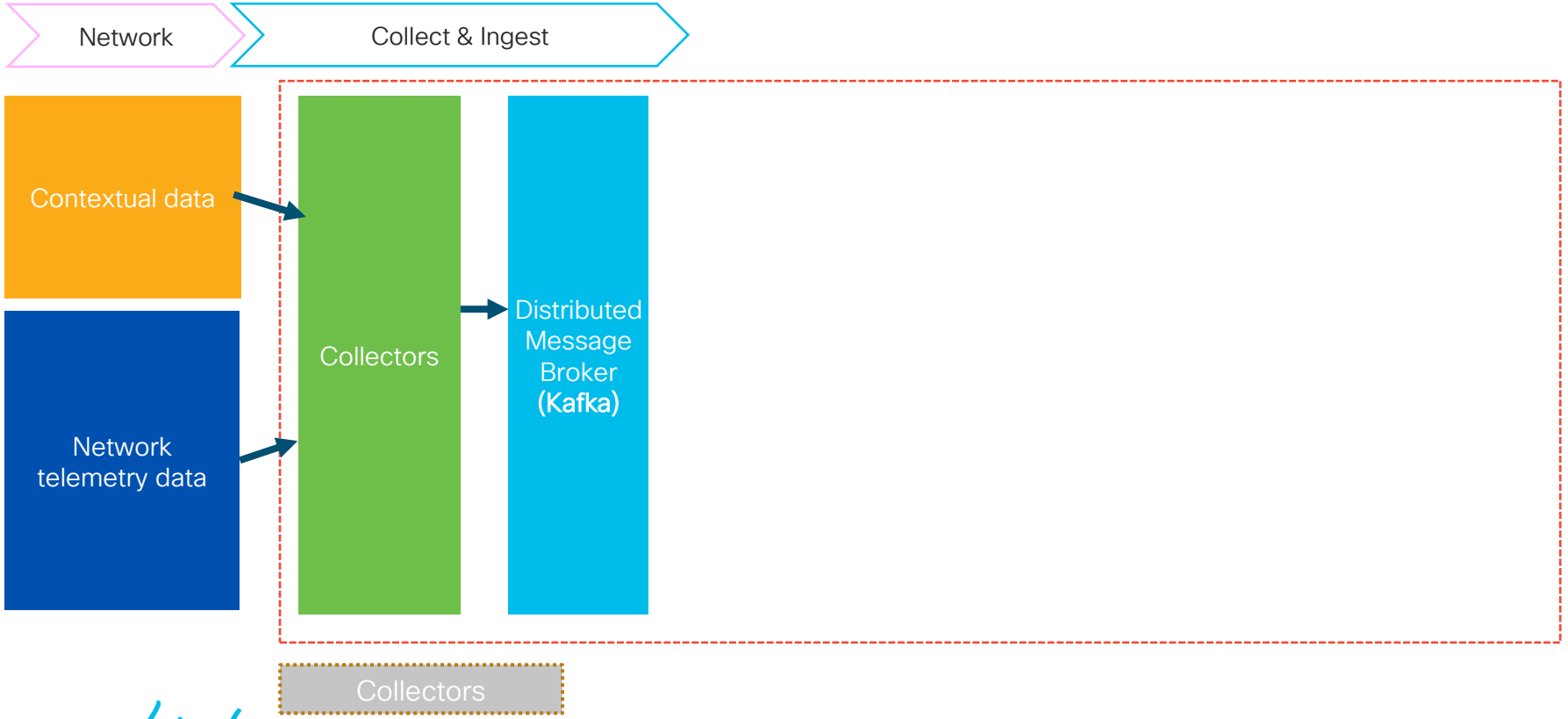
Telemetry subscription receiver configured correctly.
View Relevant Activities

Telemetry Subscriptions present are as follows:

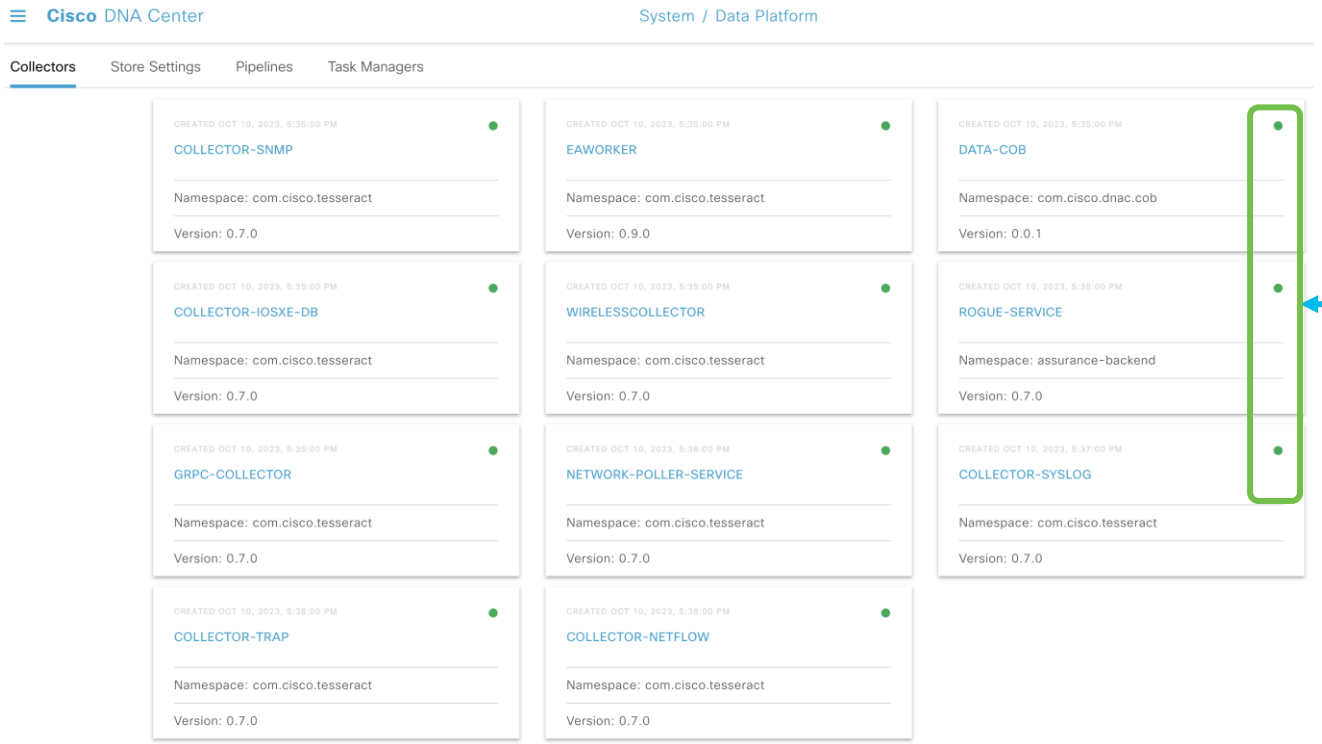
Subscription Id ▲	Value
750	/services;serviceName=ios_emul_oper/environment_sensor
1011	/services;serviceName=ewlc/wlan_config

WSA enabled and configured correctly.
View Relevant Activities

Assurance System Flow



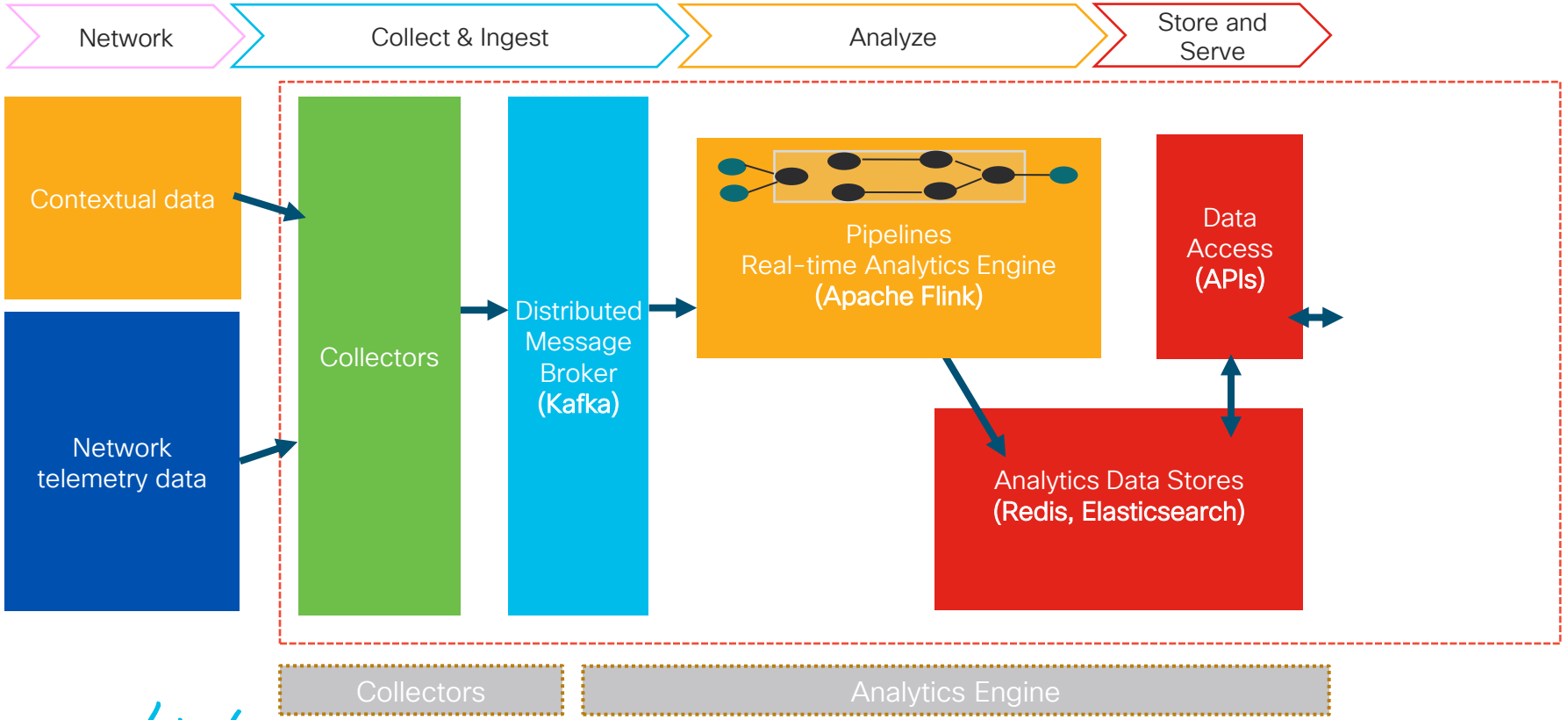
Assurance Collectors Check



Status of the Collectors

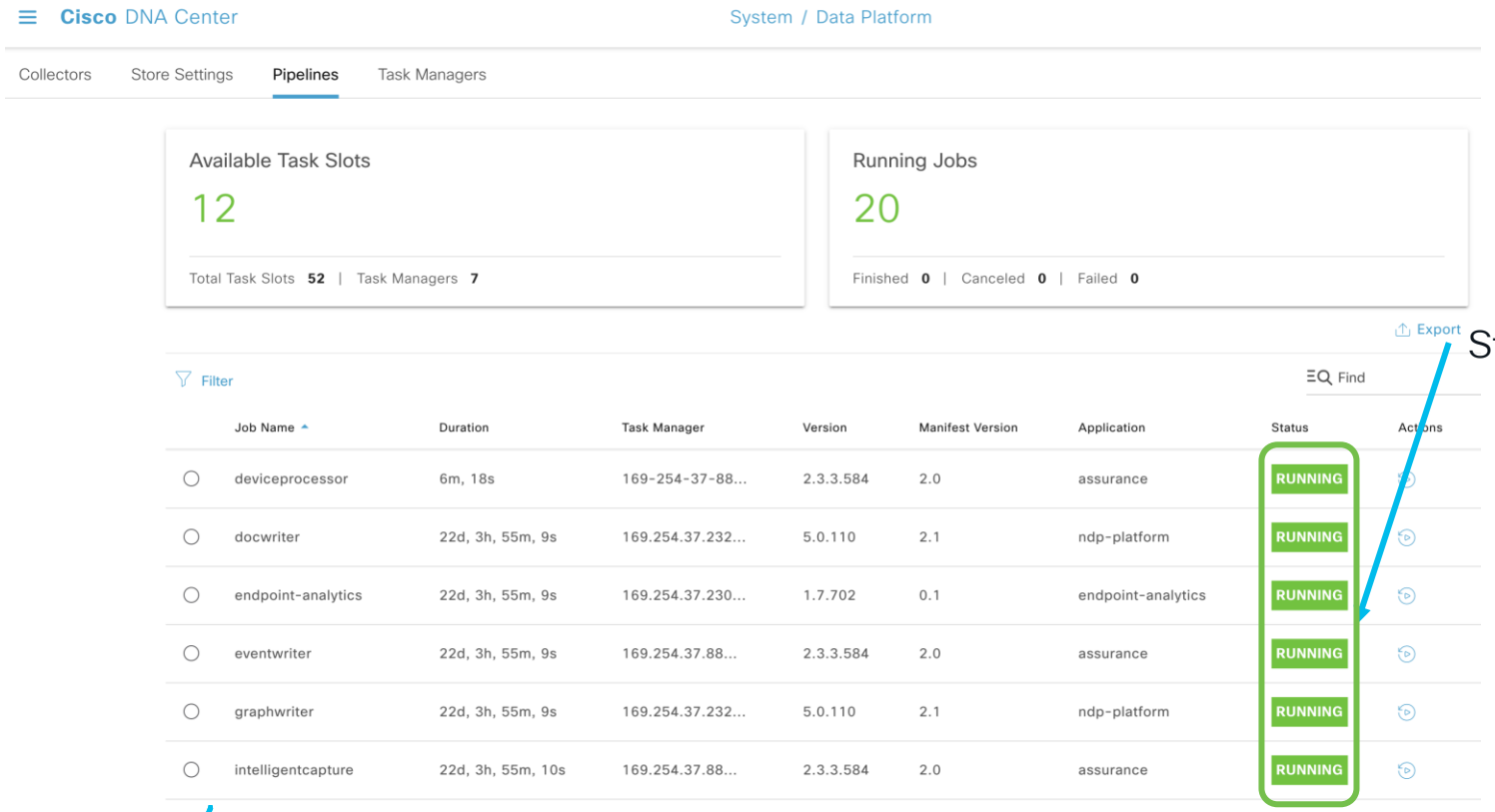
Click on a Collector to view the status and configurations

Assurance System Flow



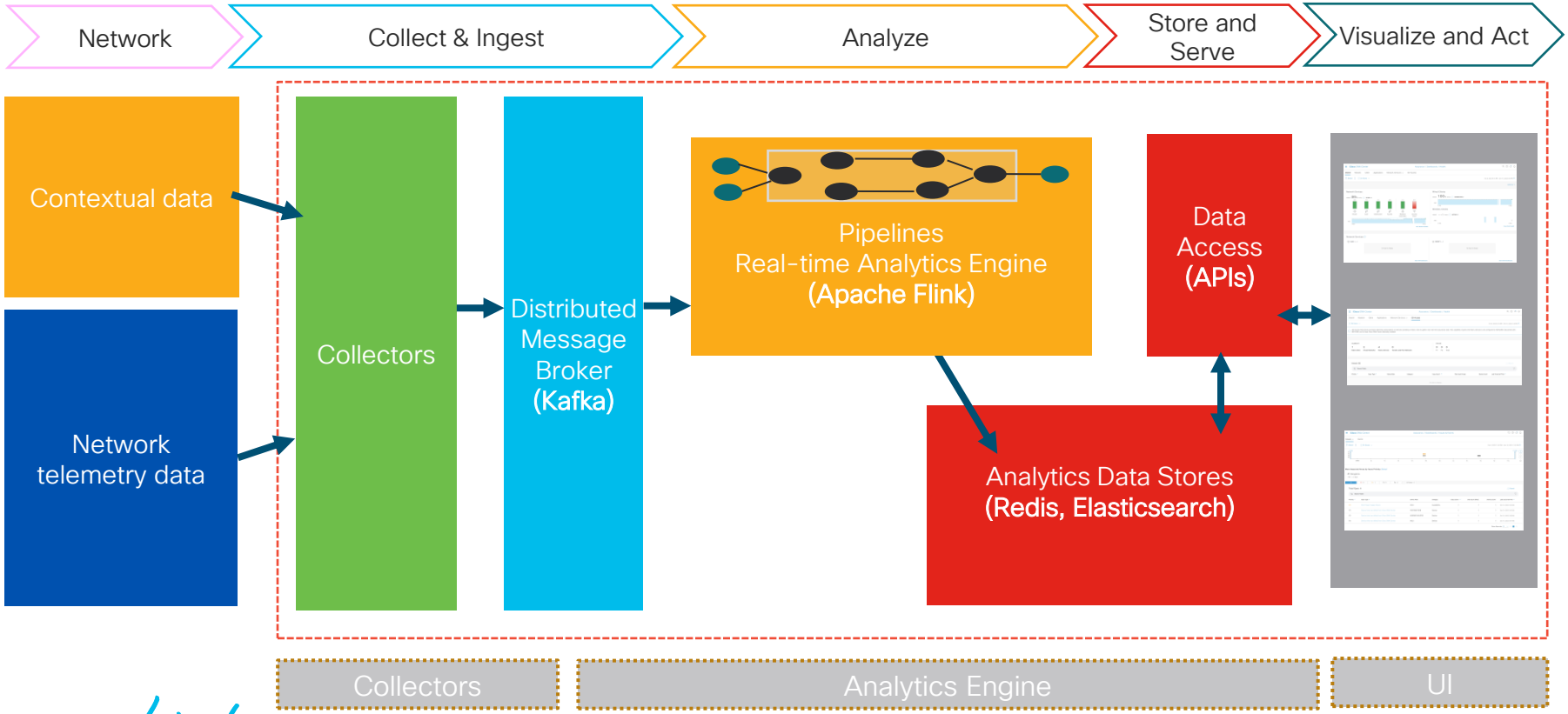
Assurance Pipelines Check

Click on a Pipeline to view the metrics, configurations & any exceptions



Status of the Pipelines

Assurance System Flow



Assurance – Network Health

Validation Tool – (System → System Health → Tools)

Release 2.3.5.x onwards

Validation Run Details

Name	assurance_test
Description	test
Status	Warning

Result

Export Copy

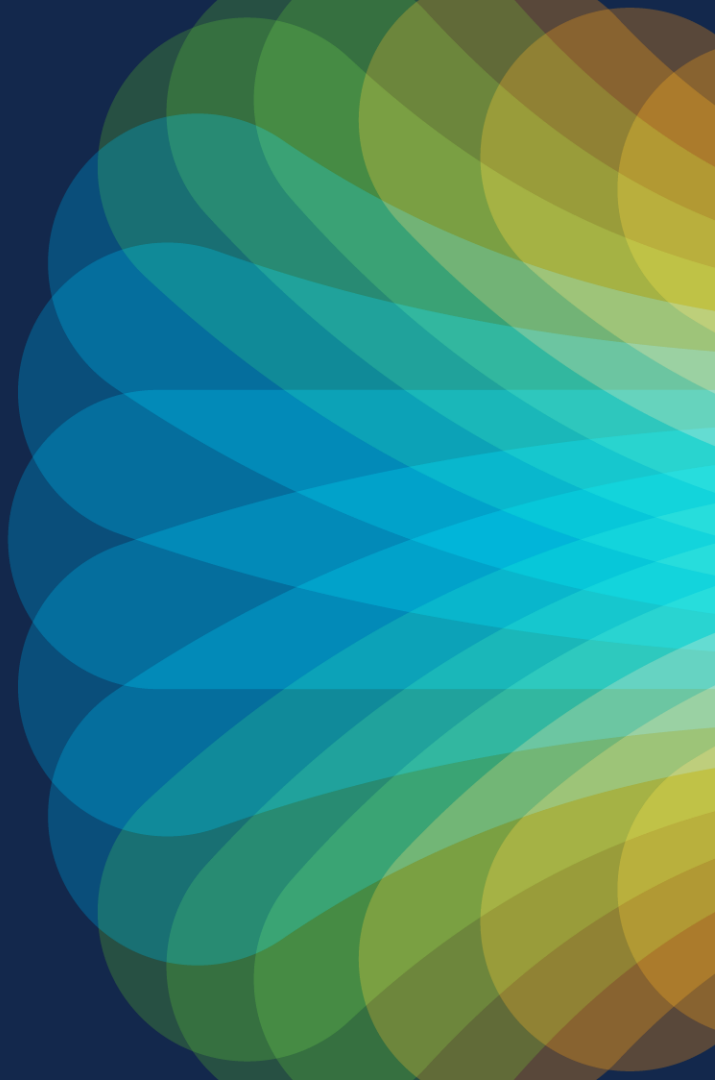
ASSURANCE HEALTH

All | Info | Warning | Critical | In Progress

Search Table

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

Cisco Catalyst Center Software Upgrades



Catalyst Center Software Version

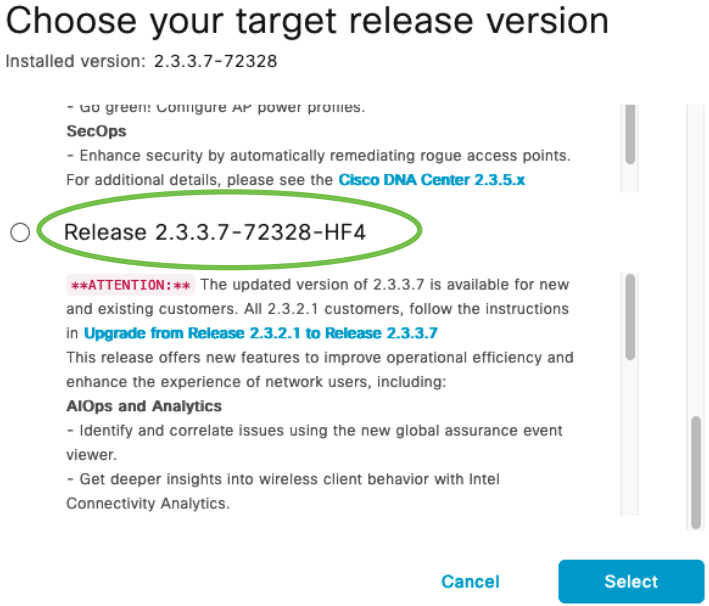
Release 2.3.3.x onwards

a.b.c.d-e

major.minor.minor-minor.patch-release

a.b.c.d-e-HFf

major.minor.minor-minor.patch-release-hotfix



From the Release Notes

Package Name	Release 2.3.3.7				Release 2.3.3.6	Release 2.3.3.5	Release 2.3.3.4	Release 2.3.3.3	Release 2.3.3.1	Release 2.3.3.0
Release Build Version										
Release Version	2.3.3.7-72328-HF5	2.3.3.7-72328-HF4	2.3.3.7.72328	2.3.3.7.72323	2.3.3.6.70045	2.3.3.5.70134	2.3.3.4.72142	2.3.3.3.72139	2.3.3.1.72077	2.3.3.0.70399

*Release Notes

Catalyst Center Software Version

Release 2.3.3.x onwards

Hot fix addresses critical customer issue(s) and is cumulative of all prior hot fixes of that patch release. Only visible for that patch release.

In 2023, 2.3.3.7 > HF4/HF5, 2.3.5.3 > HF5 & 2.3.5.4 > HF3.

Resolved Bugs

Cisco DNA Center 2.3.5.4-70852-HF3 Hot Fix

The following table lists the resolved bugs in the Cisco DNA Center 2.3.5.4-70852-HF3 hot fix.

Note

- To obtain the hot fix, go to the **Software Management** window in the Cisco DNA Center GUI and install the 2.3.5.4-70852-HF3 hot fix. If you don't see it, scroll down and click "Looking for other releases? **Click here**."
- The 2.3.5.4-70852-HF3 hot fix is visible only if you have 2.3.5.4 installed.

Bug Identifier	Headline
CSCwe15923	Under some conditions, a newly installed, autogenerated etcd certificate in Cisco DNA Center does not get activated. When the etcd certificate does not get activated, the system might become unresponsive and inaccessible through the GUI, ultimately discarding network telemetry and losing the management capability of Cisco DNA Center. CSCwe15923 is resolved in 2.3.5.4. If you upgraded from 2.3.5.3 to 2.3.5.4 before 2023-10-12, install the 2.3.5.4.70852-HF3 hot fix atop 2.3.5.4.
CSCwh81546	An internally autogenerated etcd certificate is not activated after upgrade. This problem occurs in the following scenario: a. Cisco DNA Center is freshly installed using 2.3.5.3, or is upgraded to 2.3.5.3. b. The etcd certificate renews, but is not activated (etcd keeps using the old certificate). c. Cisco DNA Center is upgraded to 2.3.5.4. d. After the upgrade, the old certificate is still used. The system is expected to experience an outage when the certificate expires.

Choosing a Target Release

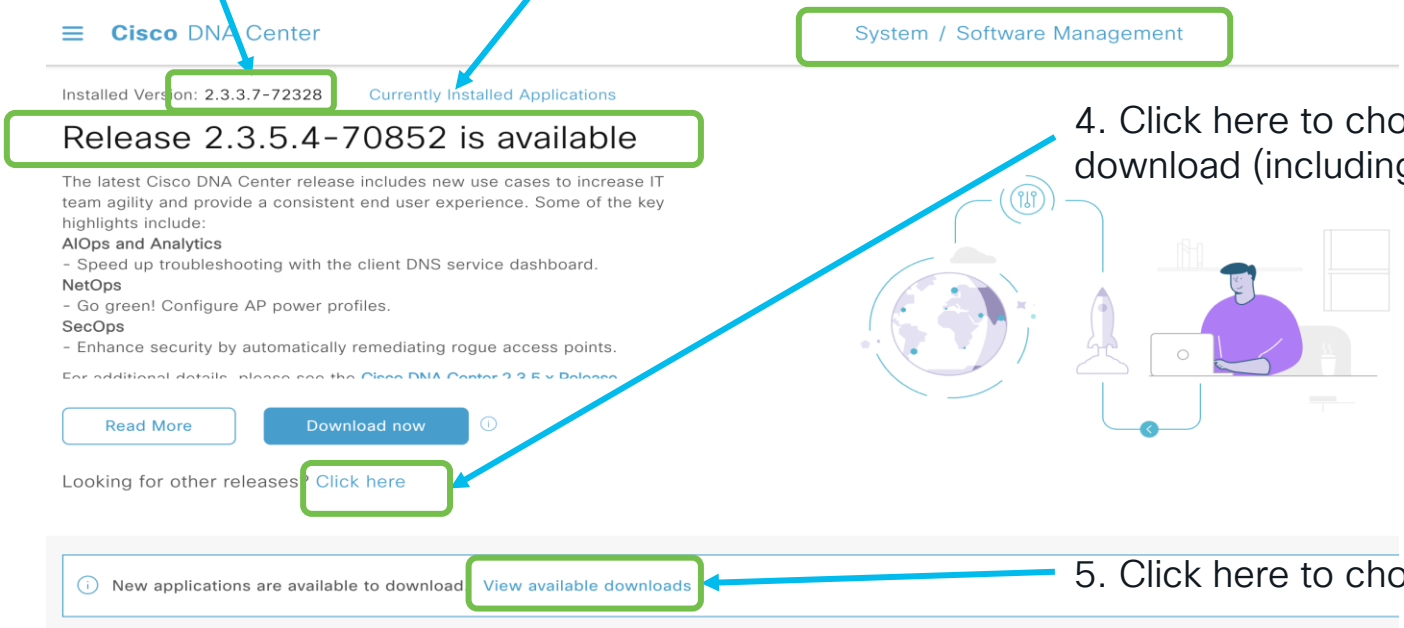
The New Way - Simplified

Release 2.3.x.x onwards

1. The current version

2. The latest available option (by default)

3. Software Update is now Software Management



4. Click here to choose a different release to download (including latest patch release)

5. Click here to choose new applications

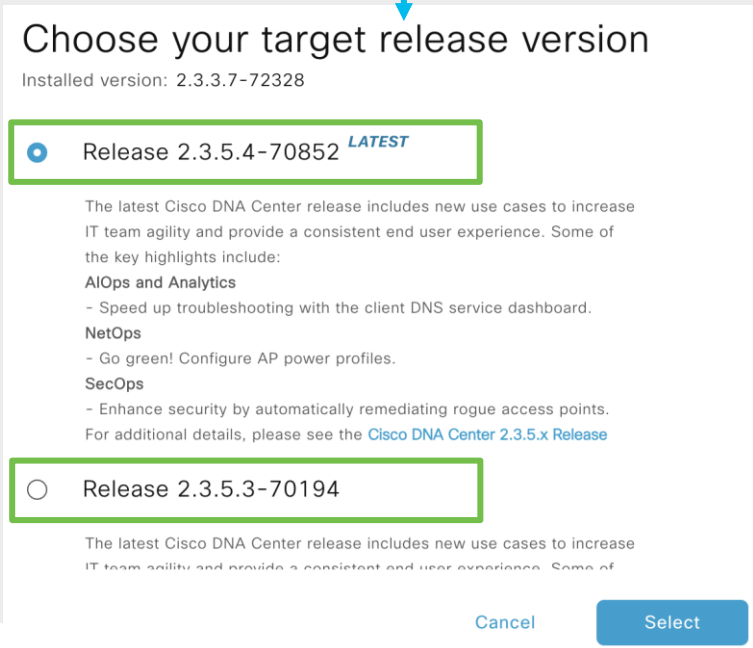
Choosing a Target Release

The New Way – Multiple Options

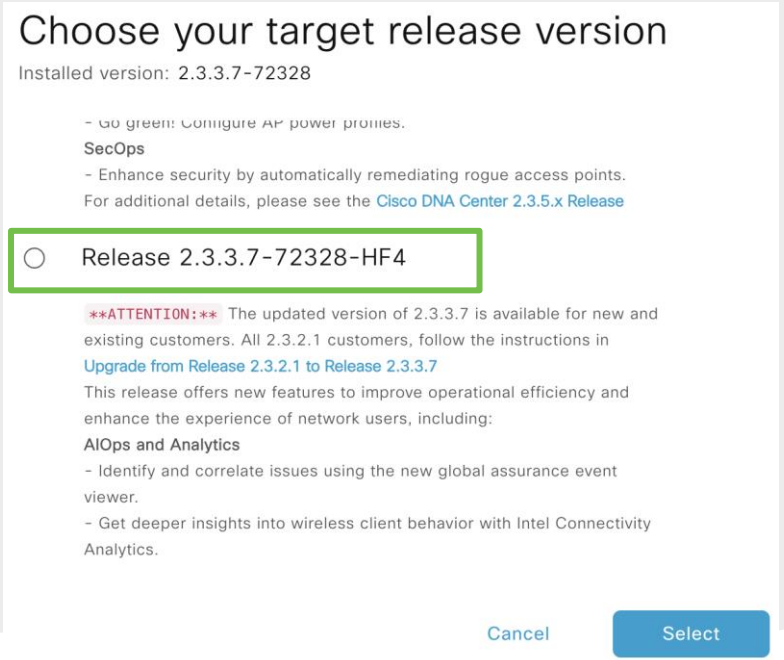
Release 2.3.x.x onwards

Looking for other releases? Click here

Pop-up window ...



...

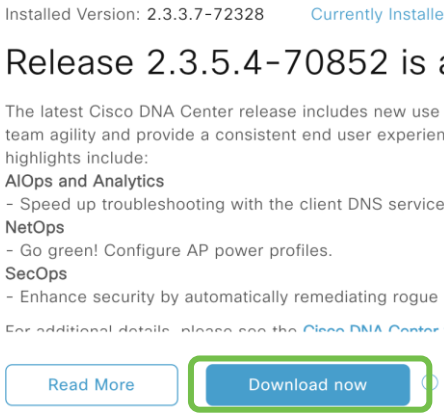


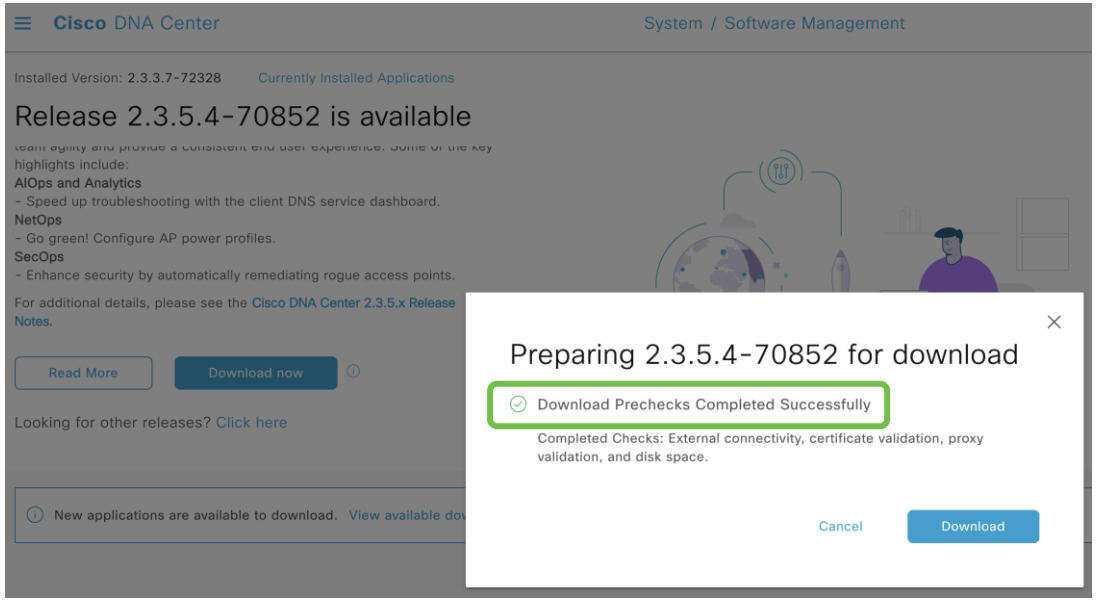
The Upgrade Process

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





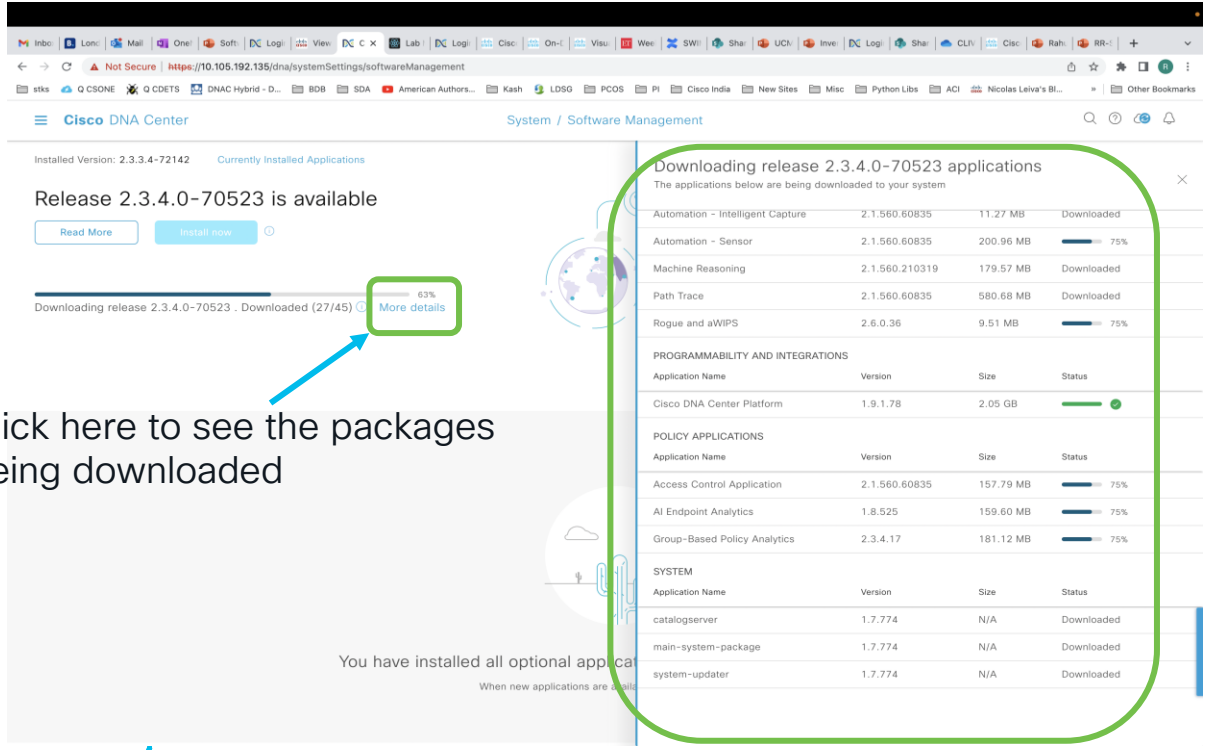
System and Applications packages **downloaded** in the same step

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



Click here to see the packages being downloaded

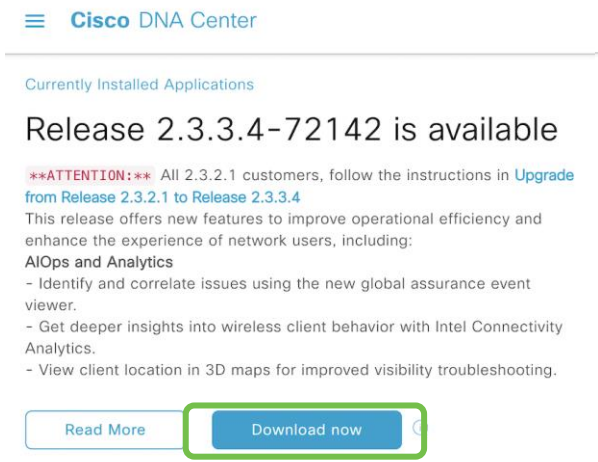
- Visibility into the packages being downloaded and overall downloaded percent
- The Cisco Catalyst Center is not locked during this step

The Upgrade Process

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

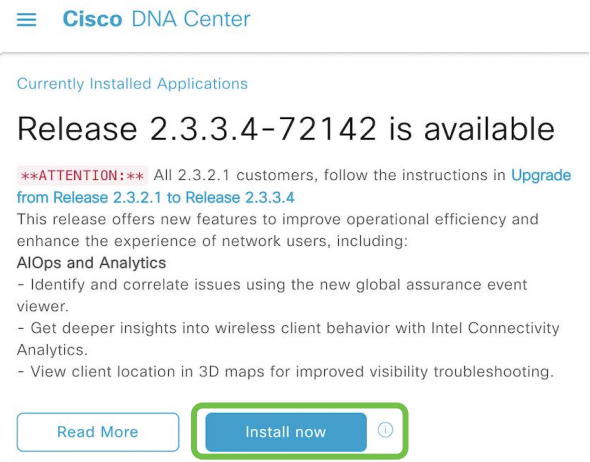
Release 2.3.x.x onwards

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

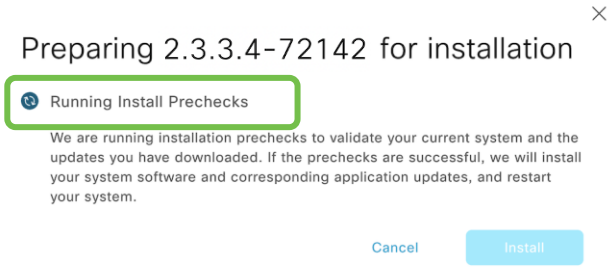


System and Applications packages **downloaded** in the same step

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



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

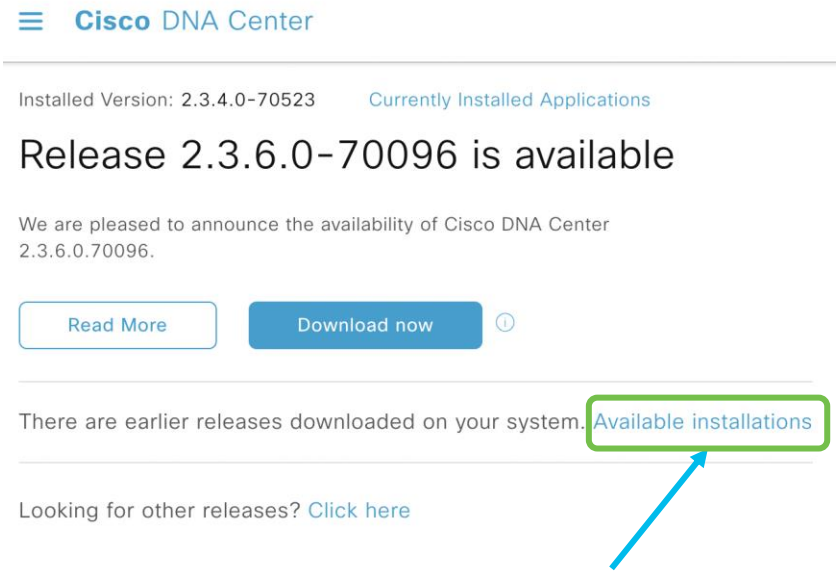


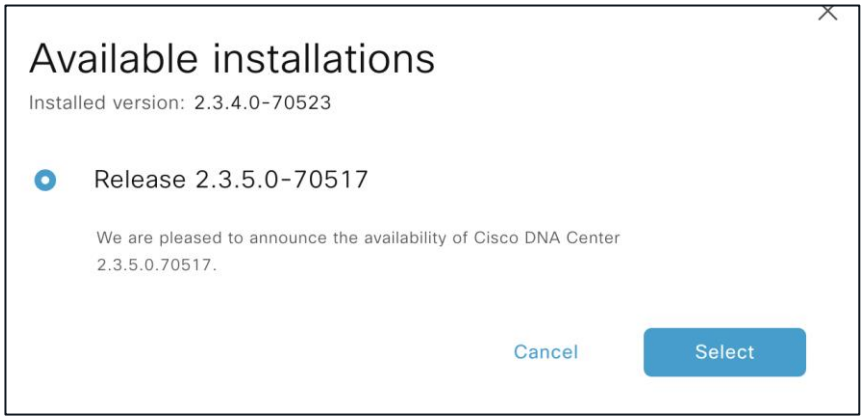
The Upgrade Process

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

Release 2.3.x.x onwards

System and Applications packages installed in the same step





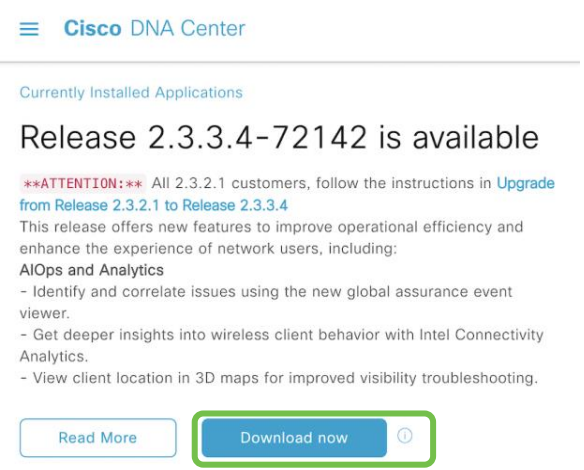
Click to see previously downloaded releases

The Upgrade Process

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

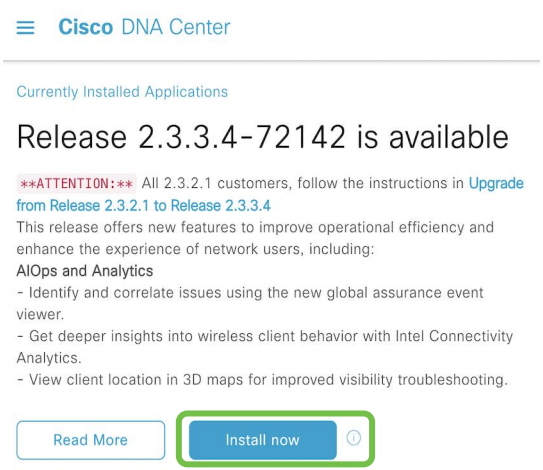
Release 2.3.x.x onwards

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



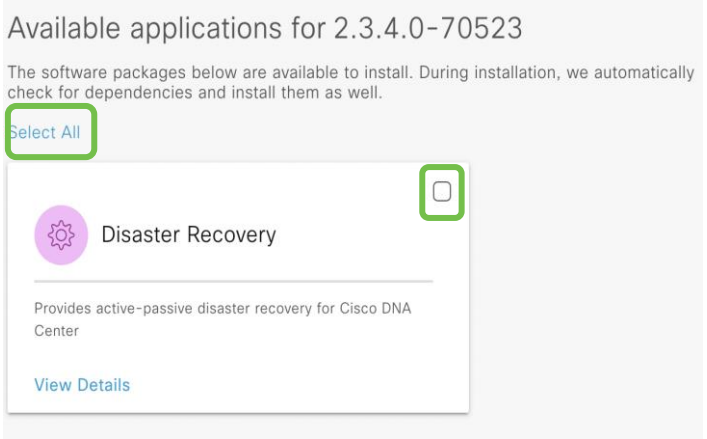
System and Applications packages **downloaded** in the same step

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



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

Step 3 (optional). Install Optional Application packages



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

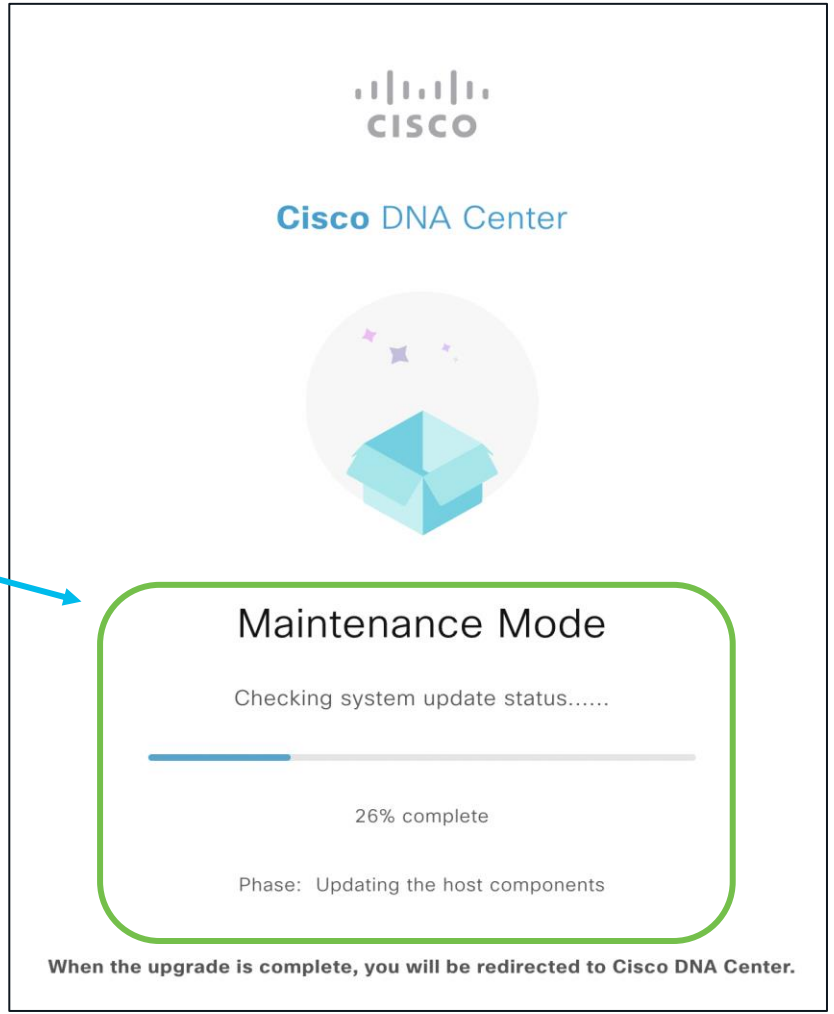
Software Upgrade Process Enhancements

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)	<u>3 Steps</u> 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	<u>2 Steps</u> 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 and Troubleshooting

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



Its Monday morning and you are still stuck in maintenance mode

The Upgrade Process

Monitoring and Troubleshooting System Upgrade

1. System Upgrade

2. Applications Upgrade

Monitoring the System Upgrade progress

```
$ maglev system_update progress
```

New commands from 2.3.x

```
INSTALLED_VERSION     CURRENTLY_PROCESSED_VERSION     CURRENT_PHASE
UPDATE_PROGRESS_PERCENT    CURRENT_PHASE_DETAILS
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
1.7.774               1.7.774                         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 : 1.7.774

  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

Step 1. Maintenance mode, System update hooks downloading and installation (0-1%)

```
$ maglev system_updater update_info
System update status:
  Version successfully installed : 1.6.424
  Version currently processed    : 1.6.594
    Update phase                 : Installing System updater pre update
hooks
    Update details               : Deploying hooks for pre system update
    Progress                     : 1%

  Updater State:
    Currently processed version  : 1.6.594
    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

Typically, connectivity issues seen, required FQDNs, ports blocked for a node or all nodes, proxy settings …

Logs

- magctl service logs -r system-updater
- magctl service logs -r catalogserver

Step 2. Download & upgrade of Services catalogserver, systemupdater (2% - 6%)

```
$ maglev catalog system_update_package display

maglev-1 [main - https://kong-frontend.maglev-system.svc.cluster.local:443]

NAME                    VERSION   REQUIRES_PULL  STATE   MESSAGE
-------------------------------------------------------------------------
catalogserver           1.6.718   False          READY   Successfully pulled
main-system-package     1.6.718   False          READY   Successfully pulled
system-updater          1.6.718   False          READY   Successfully pulled

$ maglev catalog system_update_package display

maglev-1 [main - https://kong-frontend.maglev-system.svc.cluster.local:443]

NAME                    VERSION   REQUIRES_PULL  STATE   MESSAGE
-------------------------------------------------------------------------
catalogserver           1.6.718   False          PARTIAL   Error response
from daemon: Get https://registry.ciscoconnectdna.com/v1/_ping: x509:
certificate signed by unknown authority
main-system-package     1.6.718   False          PARTIAL Needs to be
downloaded
system-updater          1.6.718   False          PARTIAL Needs to be
downloaded
```

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

Typically, connectivity issues seen, required FQDNs, ports blocked for a node or all nodes, proxy settings …

Step 2. Download & upgrade of Services catalogserver, systemupdater (2% - 6%)

```
$ maglev system_updater update_info
System update status:
  Version successfully installed : 1.6.424
  Version currently processed    : 1.6.594
    Update phase                 : failed
    Update details               : ERROR: Downloading update package
catalogserver:1.6.718 failed (Downloading systemUpdatePackage
catalogserver:1.6.718 failed)
    Progress                     : 2%

  Updater State:
    Currently processed version  : 1.6.594
    State                        : FAILED
    Sub-State                    : DOWNLOADED_CATALOG
    Details                      : Downloading systemUpdatePackage
catalogserver:1.6.718 failed
    Source                       : system-updater
    Abort pending                : False
```

Logs

- magctl service logs -r system-updater
- magctl service logs -r catalogserver

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

Step 3. Download packages to the Nodes (7% - 30%)

```
$ maglev system_updater update_info
System update status:
  Version successfully installed : 1.6.424
  Version currently processed    : 1.6.594
    Update phase                 : Downloading the host update packages
    Update details               : Copying the host packages to all the
nodes
    Progress                     : 7%

  Updater State:
    Currently processed version  : 1.6.594
    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

Step 4. Applications are shut down (31%)

```
$ maglev system_updater update_info
System update status:
  Version successfully installed : 1.6.424
  Version currently processed    : 1.6.594
    Update phase                 : Disabling the applications
    Update details               : Disabling user applications
    Progress                     : 31%

  Updater State:
    Currently processed version  : 1.6.594
    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

Upgrading the Nodes one by one

```
$ maglev system_updater update_info
System update status:
  Version successfully installed : 1.6.424
  Version currently processed    : 1.6.594
    Update phase                 : failed
    Update details               : Updating node 10.10.10.10 failed
    Progress                     : 34%

  Updater State:
    Currently processed version  : 1.6.594
    State                        : FAILED
    Sub-State                    : INSTALLED_HOST_COMPONENTS
    Details                      : Updating node 10.10.10.10 failed
    Source                       : system-updater
    Abort pending                : False
```

Logs

- magctl service logs -r system-updater
- sudo journalctl -u maglev-node-updater

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 : 1.6.594

  Updater State:
    Currently processed version  : 1.6.594
    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

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

```
sudo journalctl -u maglev-node-updater
sudo journalctl -u maglev-hook-installer
```

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]
```

Node Agnostic

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

The Upgrade Process (Prerequisites)

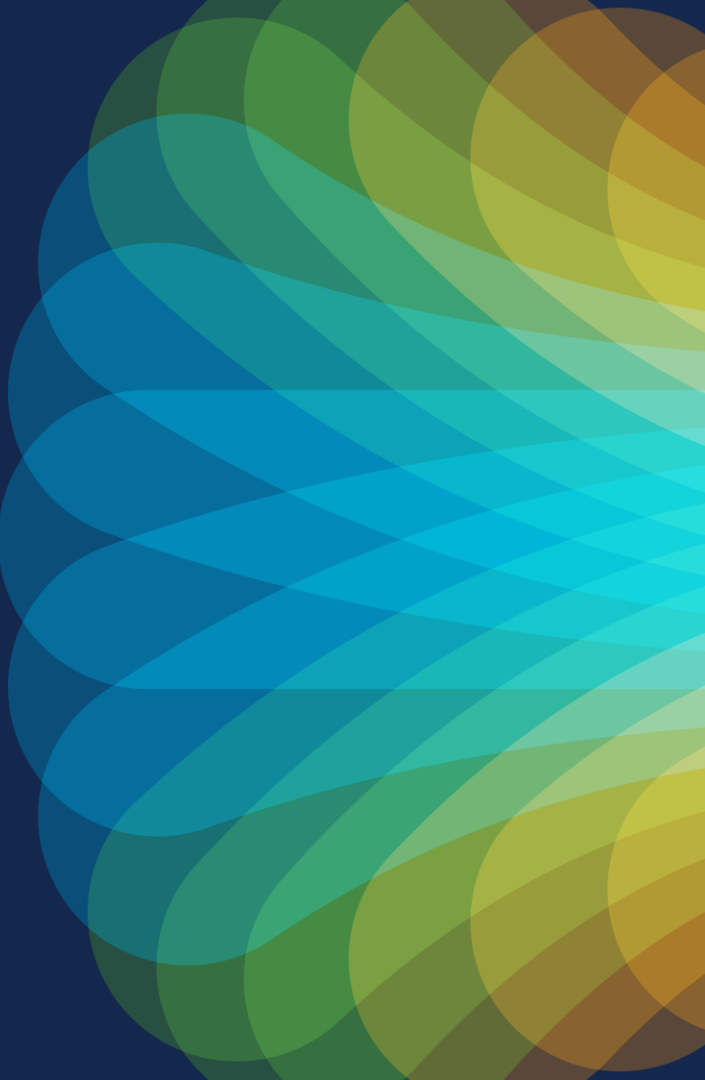
- Healthy Backup
- Healthy Hardware
- Open required ports on the Firewall
- Prechecks:
  - 1.2.8 to 2.3.3.x > AURA from every node OR
  - 2.3.5.x > Validation Tool

(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

Cisco Catalyst Center Troubleshooting Tools & Other Services

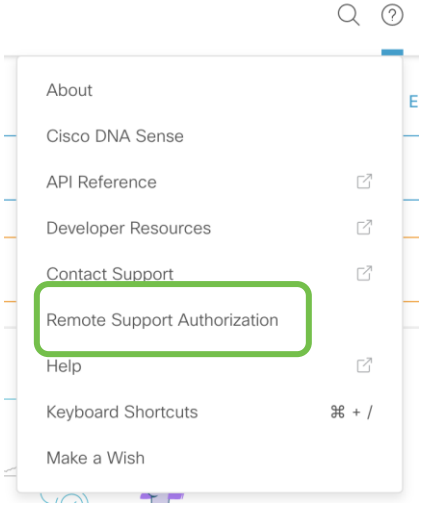


Collecting Logs for Troubleshooting

- 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.

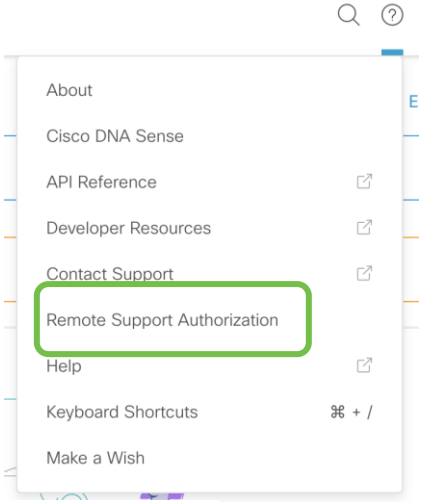


For more details reach out to us at the RADKit Community Page

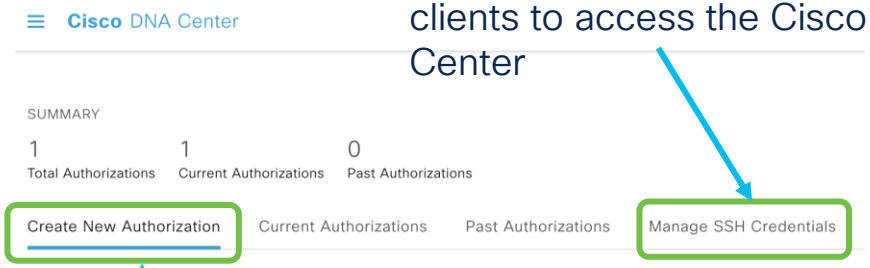
Collecting Logs for Troubleshooting

- Remote Support Authorization using RADKit

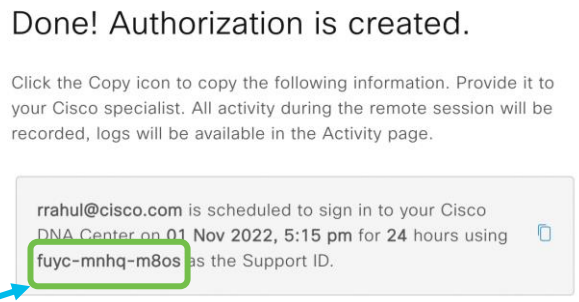
Customer View is **UI** based and authorizes a Cisco TAC Engineer in **2 steps** via the Remote Support Authorization Dashboard.



Step 1. Provide password for RADKit clients to access the Cisco Catalyst Center



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



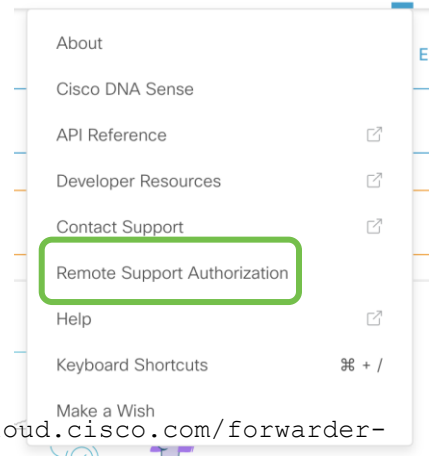
Step 3. Share the support ID with the TAC engineer.

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

- 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/

Collecting Logs for Troubleshooting

- Logs from CLI for any Service

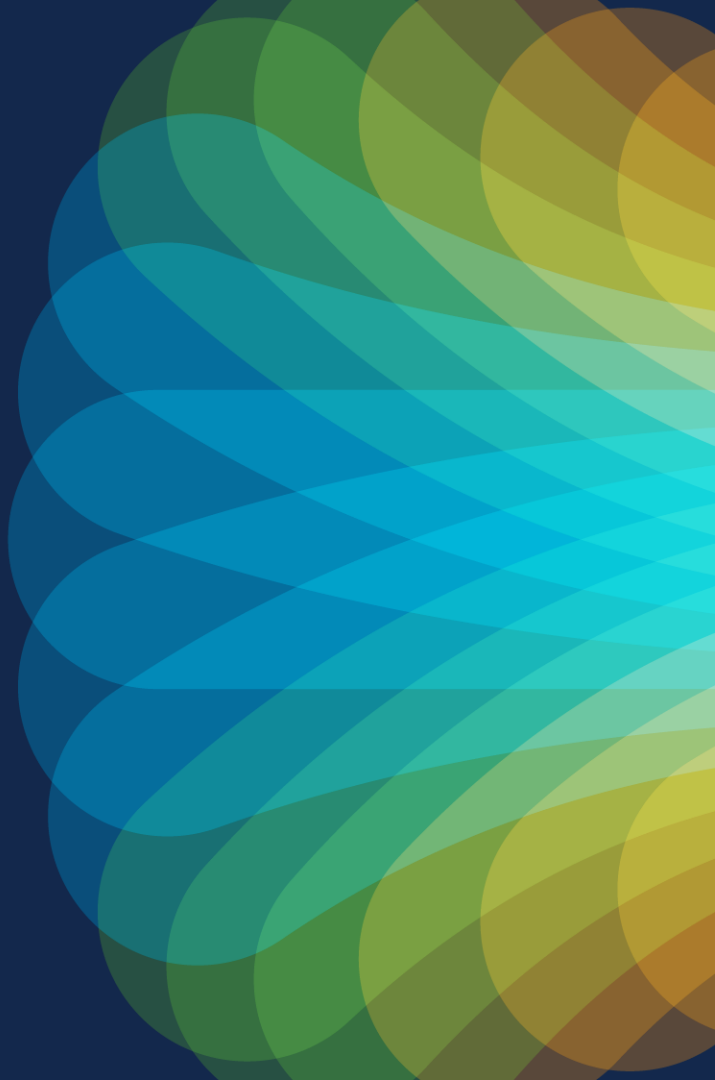
```
$ magctl service logs --help
Usage: magctl service logs [OPTIONS] SERVICE

  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

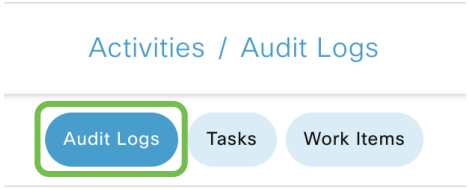
```
magctl service logs -r <service name>
magctl service logs -rf <service name>
magctl service logs -rt 10 <service name>
```

* Works with Magshell

Collecting Audit Logs for Troubleshooting

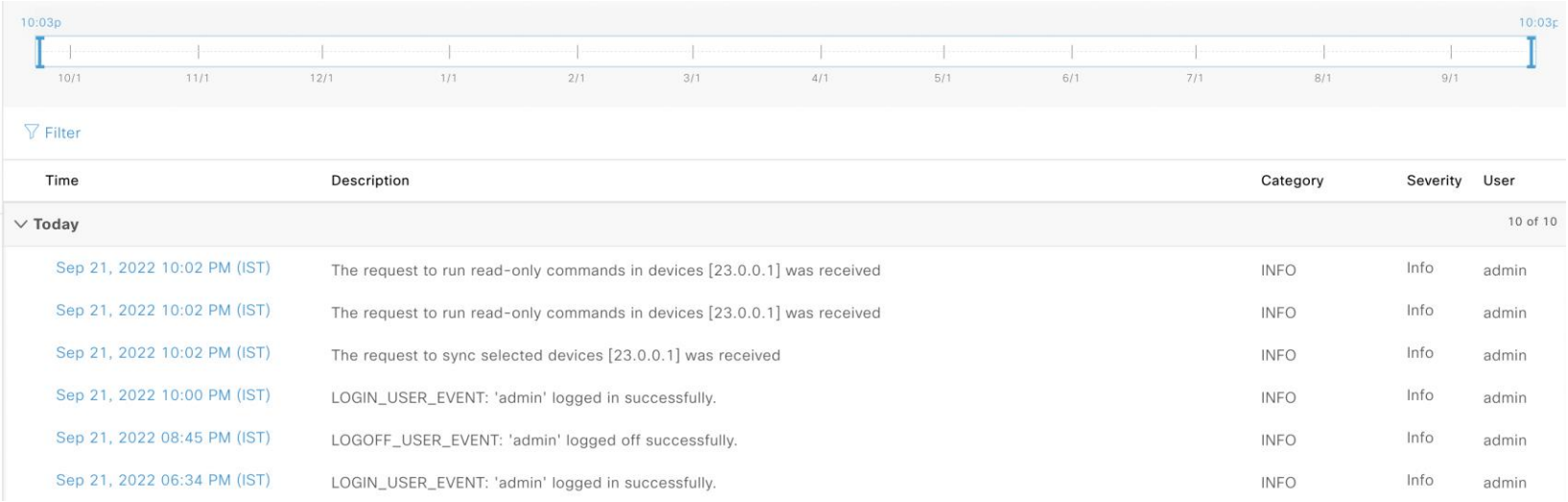


Collecting Logs for Troubleshooting



- Audit Logs

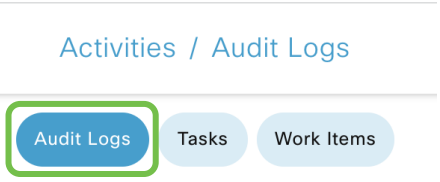
Audit logs captures all critical events/activities on the Cisco Catalyst Center



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

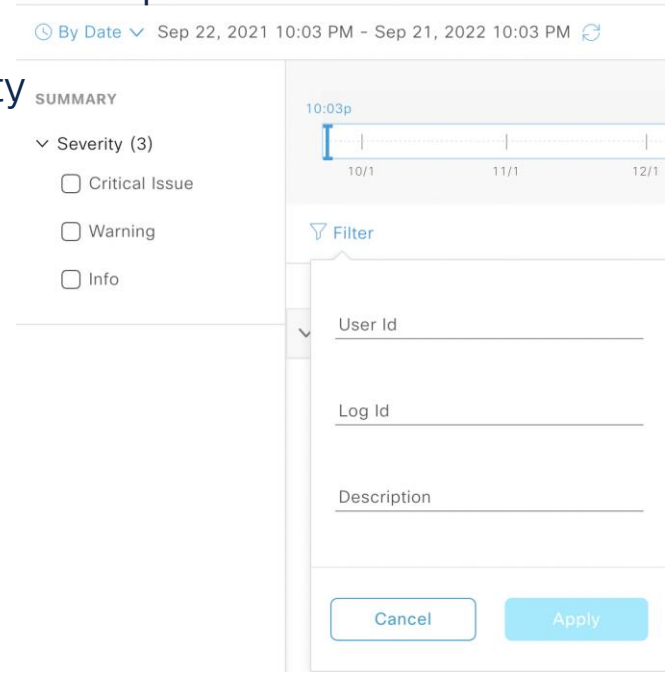
Collecting Logs for Troubleshooting

- Audit Logs

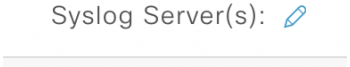


5 Filters available on the top left corner

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



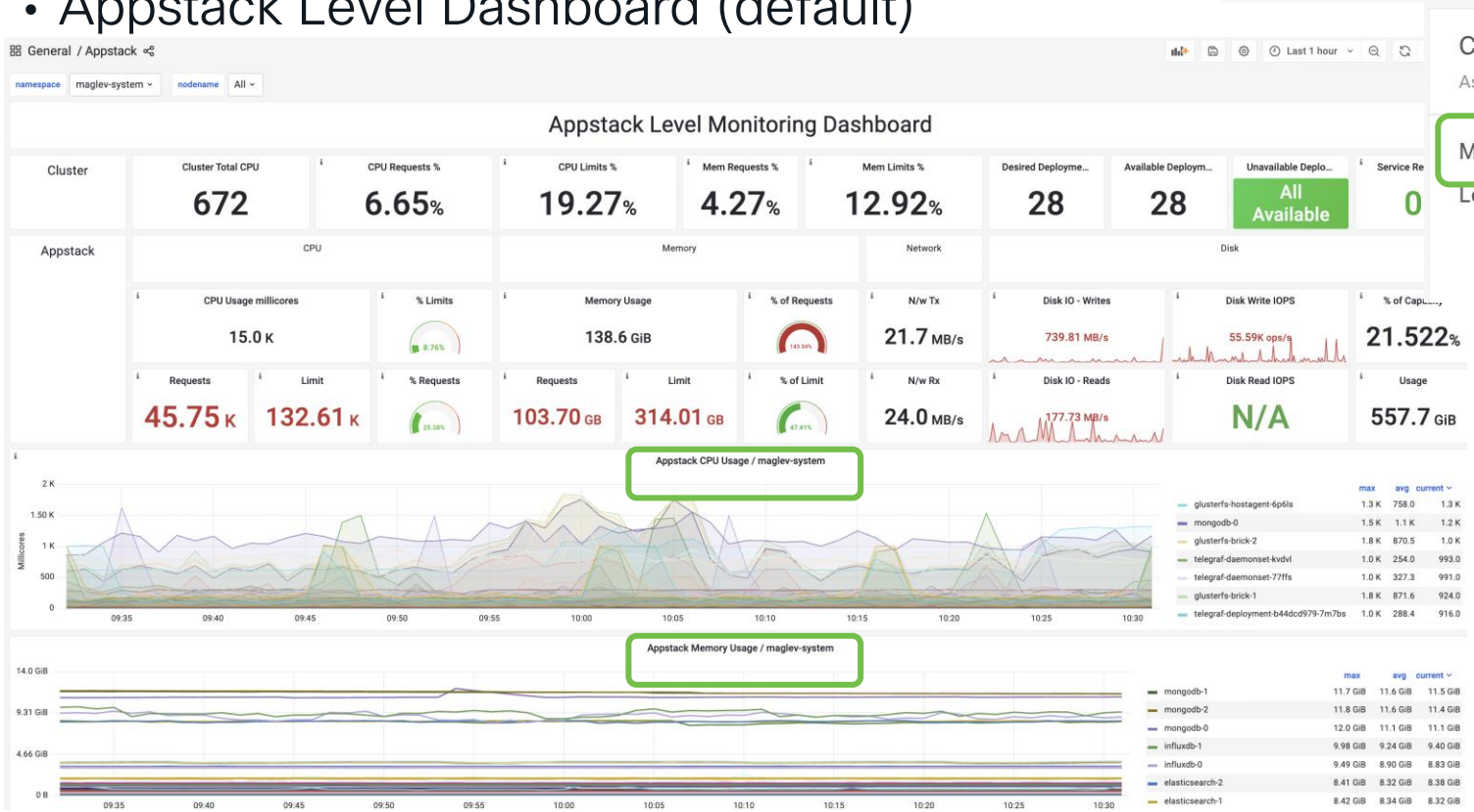
Option on the top right corner to export logs to a syslog server



Monitoring Service Statistics

Grafana Dashboards

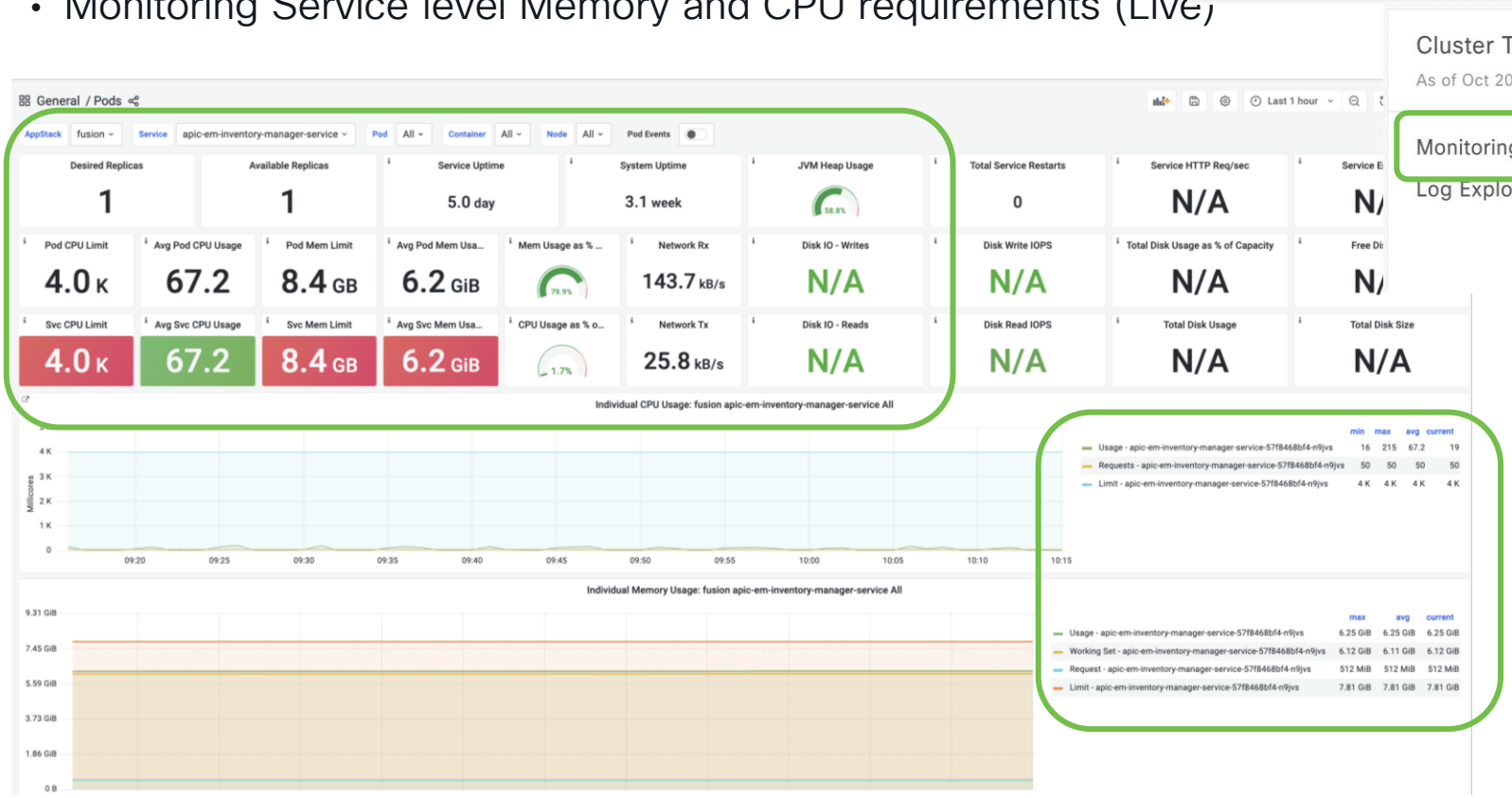
- Appstack Level Dashboard (default)



Grafana Dashboards

System / System 360

- Monitoring Service level Memory and CPU requirements (Live)

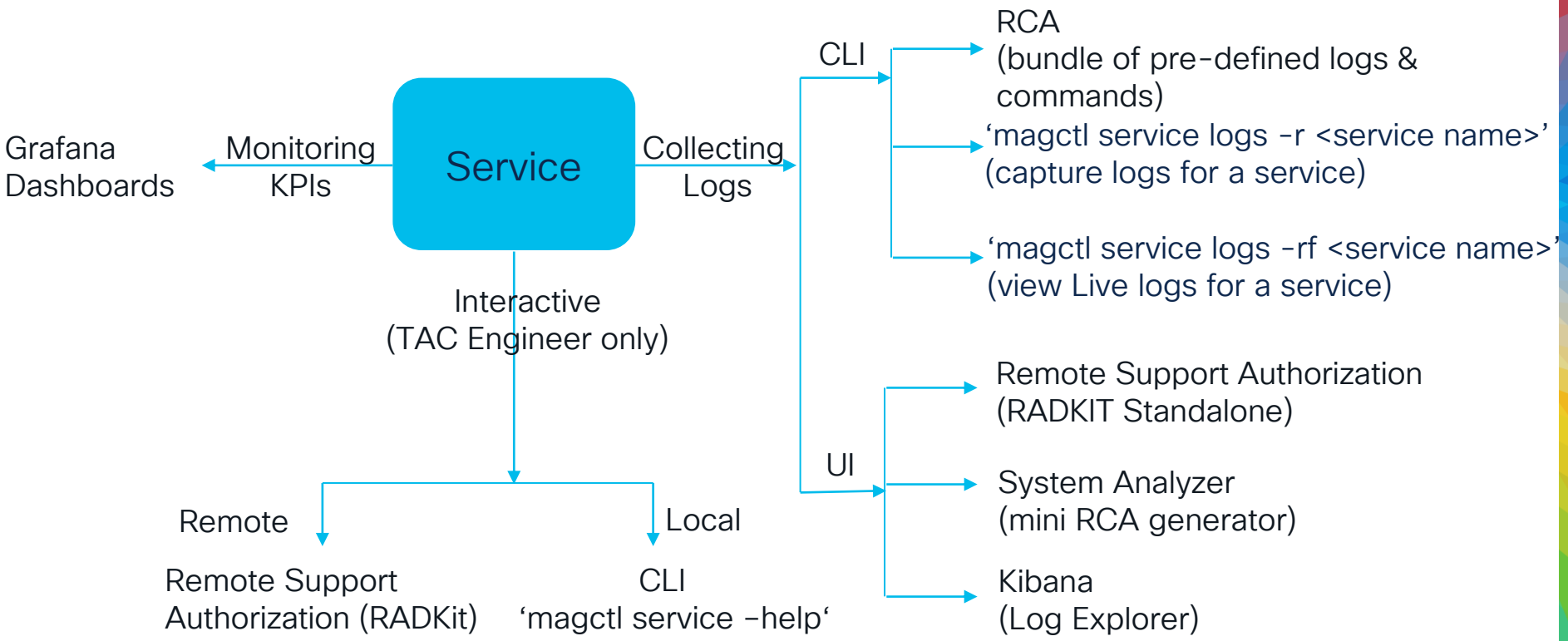


Grafana Dashboards

- Monitoring JVM Metrics per Service (Live)

*Most Services are Java based

Troubleshooting Services – Cheat sheet



Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.

Learn

Cisco U.
IT learning hub that guides teams and learners toward their goals

Cisco Digital Learning
Subscription-based product, technology, and certification training

Cisco Modeling Labs
Network simulation platform for design, testing, and troubleshooting

Cisco Learning Network
Resource community portal for certifications and learning

Train

Cisco Training Bootcamps
Intensive team & individual automation and technology training programs

Cisco Learning Partner Program
Authorized training partners supporting Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training
Accelerated curriculum of product, technology, and certification courses

Certify

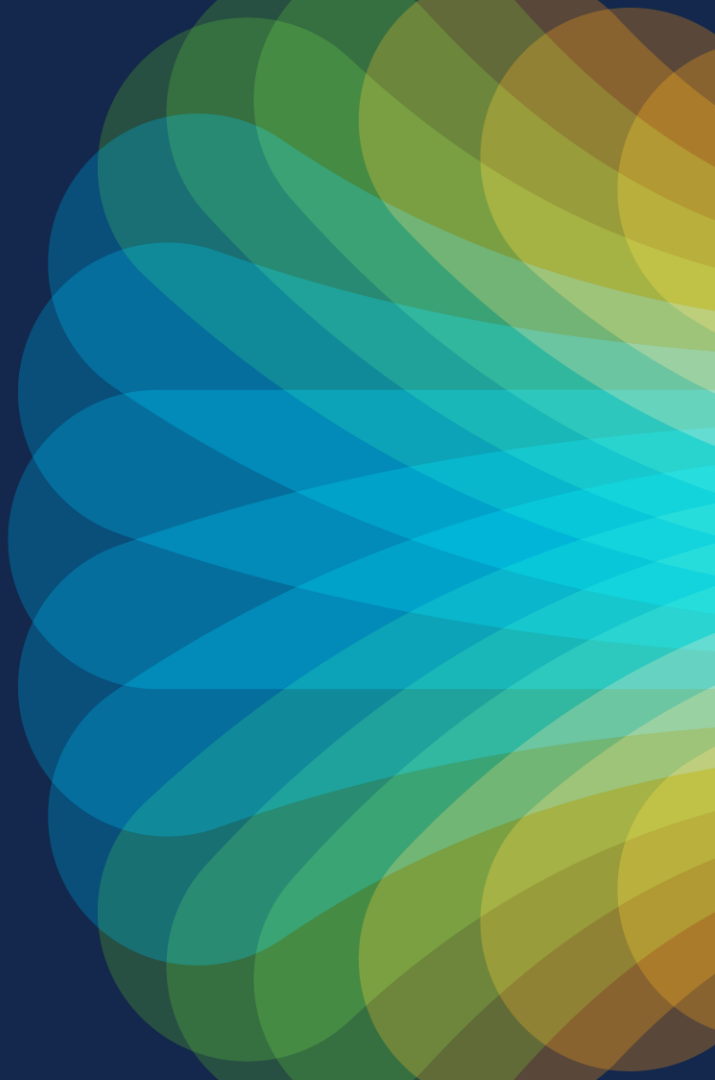
Cisco Certifications and Specialist Certifications
Award-winning certification program empowers students and IT Professionals to advance their technical careers

Cisco Guided Study Groups
180-day certification prep program with learning and support

Cisco Continuing Education Program
Recertification training options for Cisco certified individuals

The bridge to possible

Thank you



cisco Live!


cisco Live!
Let's go