

CISCO *Live!*

Let's go



The bridge to possible

# Understanding and Troubleshooting the Cisco Catalyst Center

Abhay Kaviya, Customer Success Specialist  
@abhaykaviya

# 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

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.

# Have you ever called TAC?



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



```
...n.lua:276: getma...
value: maglev-system.catalog
host: "172.20.99.10", referer: "ht...

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

3039660 [lua] auth.lua:276: getmatchifany(): Incom1
/v1/catalog/ value: maglev-system.catalog-api.default
HTTP/1.1", host: "172.20.99.10", referer: "https://

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

^lua] auth.lua:276: getmatchifan/
^lev/ value: maglev-system
host: "172.20.99.10", referer: "https://"
```

# 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

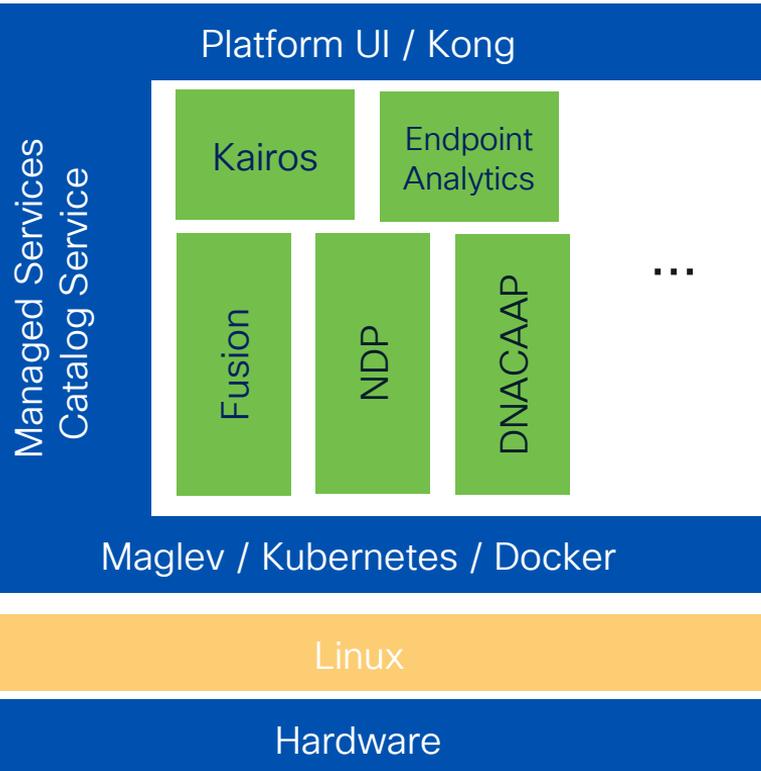
- Cisco Catalyst Center Architecture
- Cisco Catalyst Center Health
- Cisco Catalyst Center Inventory
- Cisco Catalyst Center SWIM
- Cisco Catalyst Center Assurance
- Cisco Catalyst Center Software Upgrades
- Cisco Catalyst Center Troubleshooting Tools (Reference Section)

# 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)

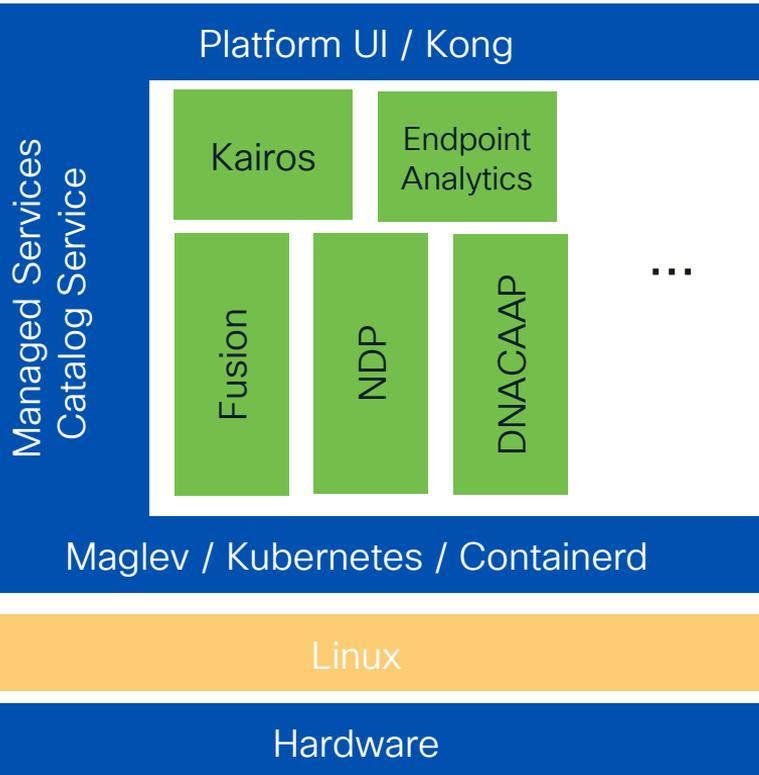
DN1 - 44 core (based on the Cisco UCS C220 M4)

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

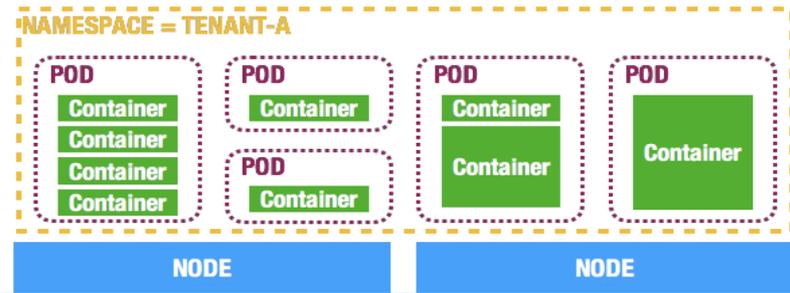
Maglev ~~v1.7~~ (v3.0)

- 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



<b>Container</b>	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.
<b>Pod</b>	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
<b>Namespace</b>	Namespaces are multiple virtual clusters backed by the same physical cluster
<b>Service</b>	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.
<b>Node</b>	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

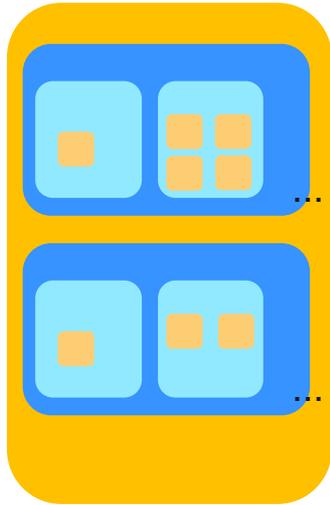


Appstack maps to K8s Namespace, is a virtual cluster within the K8s cluster. Administrative and resource controls are defined.

- 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.

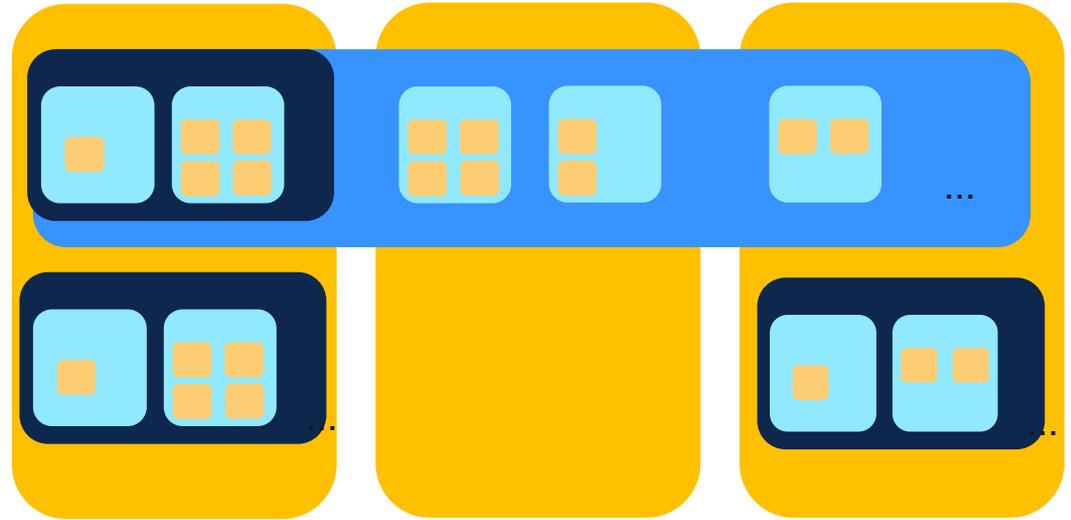
# Cisco Catalyst Center Architecture

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

System / System 360

## View Micro Services via UI

System 360 System Health Service Explorer

### System 360

Cluster

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

- 172.19.239.134
- 172.19.239.135
- 172.19.239.136

172.19.239.134  
Node Status: Healthy  
Services Status: Healthy

#### SERVICES (61)

As of: Jan 31, 2024 6:38 PM

EQ Find

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



# Cisco Catalyst Center System 360

# Catalyst Center UI: System 360

The screenshot displays the Catalyst Center interface. On the left, a dark sidebar contains a menu with icons and labels: Design, Policy, Provision, Assurance, Workflows, Tools, Platform, Activities, Reports, System, and Explore. The 'System' option is highlighted with a green box. A red box highlights the menu icon in the top left corner of the Catalyst Center header. The main content area shows the 'System 360' page, which includes a breadcrumb trail 'System / System 360' and a sub-header 'System 360'. Below this, there are three tabs: 'System 360', 'System Health', and 'Service Explorer'. The 'System 360' tab is active. The main content area is titled 'Cluster' and contains three cards: 'Hosts (1)' with a green status indicator and a 'View 135 Services' link; 'High Availability' with an orange status indicator and a 'View Guide' link; and 'Cluster Tools' with a green status indicator and two links: 'Monitoring' and 'Log Explorer'.

# System 360

## Cluster

### Hosts (1)

As of Jan 27, 2024 5:56 PM

● 192.168.210.53

[View 135 Services](#)

### High Availability

As of Jan 27, 2024 5:56 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 [🔗](#)

# System 360: Cluster Tools

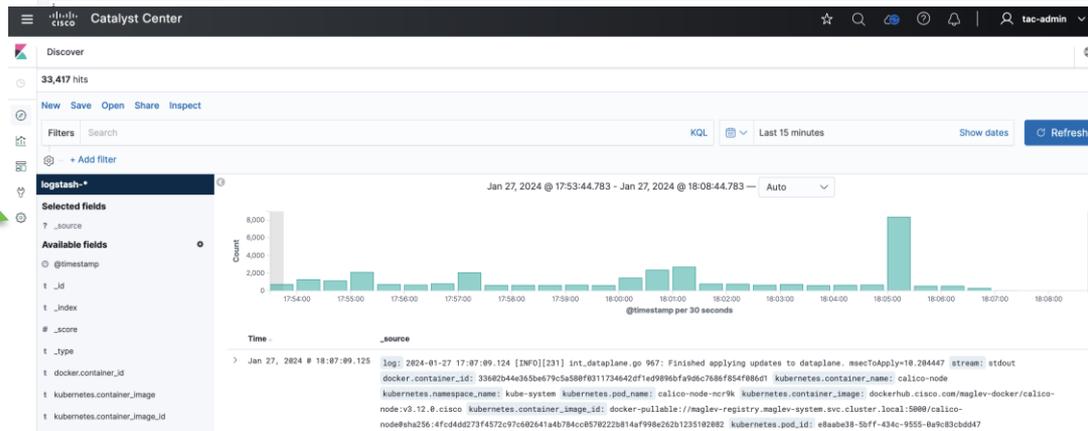
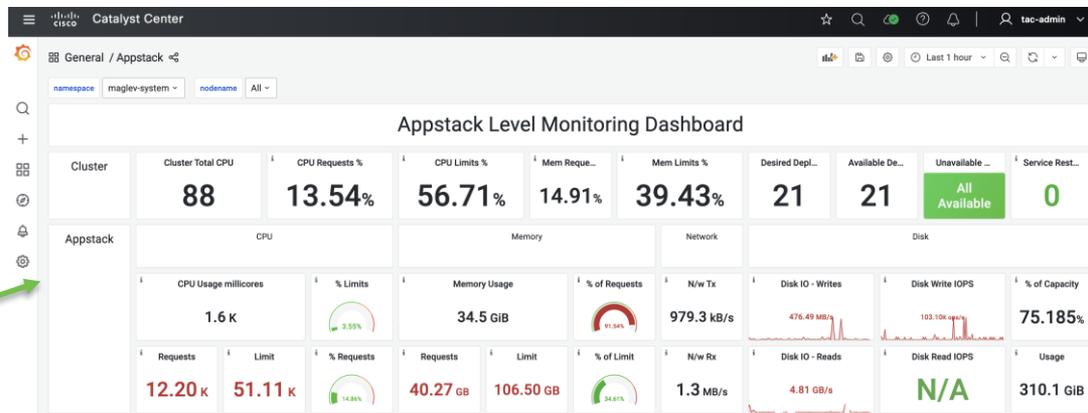
## Cluster Tools

As of Jan 27, 2024 5:53 PM

## Monitoring



## Log Explorer



# System 360: Cluster Tools – Log Explorer

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

- APM**  
APM automatically collects in-depth performance metrics and errors from inside your applications.  
[Add APM](#)
- Logging**  
Ingest logs from popular data sources and easily visualize in preconfigured dashboards.  
[Add log data](#)
- Metrics**  
Collect metrics from the operating system and services running on your servers.  
[Add metric data](#)
- Security analytics**  
Centralize security events for interactive investigation in ready-to-go visualizations.  
[Add security events](#)

**Add sample data**  
[Load a data set and a Kibana dashboard](#)

**Use Elasticsearch data**  
[Connect to your Elasticsearch index](#)

**Visualize and Explore Data**

- Dashboard**  
Display and share a collection of visualizations and saved searches.
- Discover**  
Interactively explore your data by querying and filtering raw documents.

**Manage and Administer the Elastic Stack**

- Console**  
Skip cURL and use this JSON interface to work with your data directly.
- Index Patterns**  
Manage the index patterns that help retrieve your data from Elasticsearch.

# System 360: Cluster Tools – Log Explorer

Catalyst Center

Discover

31,100 hits

New Save Open Share Inspect

Filters Search KQL Last 15 minutes Show dates Refresh

+ Add filter

logstash\*

Selected fields

? \_source

Available fields

@timestamp

t \_id

t \_index

# \_score

t \_type

t docker.container\_id

t kubernetes.container\_image

t kubernetes.container\_image\_id

t kubernetes.container\_name

t kubernetes.host

t kubernetes.labels.acceptsPluginTy...

t kubernetes.labels.addon

t kubernetes.labels.adjustReplicatio...

Jan 27, 2024 @ 18:02:00.776 - Jan 27, 2024 @ 18:17:00.776 — Auto

Count

@timestamp per 30 seconds

Time

\_source

> Jan 27, 2024 @ 18:15:55.980

```
log: E8127 17:15:54.996613 47 nanny_lib.go:110] the server could not find the requested resource stream: stderr
docker.container_id: a358193ec2d7e6f628561bf7ac1c8de2c42682fc75fdf617fe79fb41f6f62ec1 kubernetes.container_name: heapster-nanny
kubernetes.namespace_name: kube-system kubernetes.pod_name: heapster-649f66cb7c-jx8fs kubernetes.container_image: dockerhub.cisco.com/maglev-docker
/heapster-nanny:1.7.7 kubernetes.container_image_id: docker-pullable://maglev-registry.maglev-system.svc.cluster.local:5000/heapster-
nanny@sha256:5a7fe5b91bec7ab9b0b109fcc01b6b3fea82b1739fef5318983543c7047b88b7 kubernetes.pod_id: 6f7bd5eb-72ea-4f39-976c-d4ae7c01d9fc
```

> Jan 27, 2024 @ 18:15:45.978

```
log: E8127 17:15:44.992832 47 nanny_lib.go:110] the server could not find the requested resource stream: stderr
docker.container_id: a358193ec2d7e6f628561bf7ac1c8de2c42682fc75fdf617fe79fb41f6f62ec1 kubernetes.container_name: heapster-nanny
kubernetes.namespace_name: kube-system kubernetes.pod_name: heapster-649f66cb7c-jx8fs kubernetes.container_image: dockerhub.cisco.com/maglev-docker
/heapster-nanny:1.7.7 kubernetes.container_image_id: docker-pullable://maglev-registry.maglev-system.svc.cluster.local:5000/heapster-
nanny@sha256:5a7fe5b91bec7ab9b0b109fcc01b6b3fea82b1739fef5318983543c7047b88b7 kubernetes.pod_id: 6f7bd5eb-72ea-4f39-976c-d4ae7c01d9fc
```

> Jan 27, 2024 @ 18:15:35.926

```
log: E8127 17:15:34.987716 47 nanny_lib.go:110] the server could not find the requested resource stream: stderr
```

# Sample use case

The screenshot shows the Cisco Catalyst Center interface. At the top left, there is a navigation menu with a hamburger icon and the text 'Catalyst Center'. Below this, the 'Discover' section is active, showing '29,914 hits'. There are buttons for 'New', 'Save', 'Open', 'Share', and 'Inspect'. A search bar contains 'logstash-\*'. Below the search bar, there is a 'Filters' section with a search input and a '+ Add filter' button. The 'Selected fields' section shows a list of fields, including '\_source'. The 'Available fields' section shows a list of fields, including 'kubernetes.labels.serviceName' and 'log'. The 'add' button next to 'kubernetes.labels.serviceName' is highlighted with a green box.

> Jan 27, 2024 @ 18:30:58.750 **maglevserver**

```
{"asctime": "2024-01-27T17:30:58.750Z",  
  "levelname": "INFO", "levelno": 20, "lineno": 1,  
  "message": "k8s service discovery with status code 200",  
  "module": "es/maglev/utils/k8s.py", "process": 17269052928,  
  "threadName": "maglevserver-k8s-discovery"}
```

The screenshot shows the 'Selected fields' section of the interface. It contains a list of fields: 'kubernetes.labels.serviceName' and 'log'. Both fields are highlighted with a green box.

Discover

5,040 hits

New Save Open Share Inspect

Filters log:error

+ Add filter

**Filters** **log:error**

KQL [v] Last 15 minutes Show dates Refresh

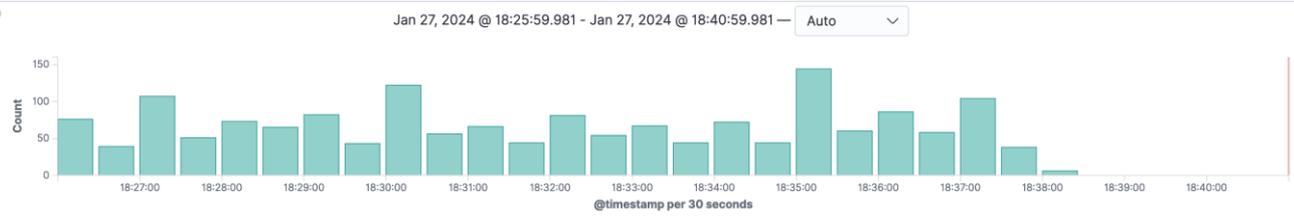
logstash-\*

Selected fields

- t\_kubernetes.labels.serviceName
- t\_log

Available fields

- @timestamp
- t\_id



Time	kubernetes.labels.serviceName	log
> Jan 27, 2024 @ 18:38:23.410	apic-em-inventory-manager-service	2024-01-27 17:38:23,410   <b>ERROR</b>   pool-29-thread-1     c.c.e.i.n.EventSyncProcessor   <b>Error</b> while invoking grouping T AG API for device e436590e-dbb6-4822-81da-6e08367ea22b, Member with UUID e436590e-dbb6-4822-81da-6e08367ea22b does not exist in any group
> Jan 27, 2024 @ 18:38:19.107	apic-em-inventory-manager-service	2024-01-27 17:38:19,107   <b>ERROR</b>   SimpleAsyncTaskExecutor-4     c.c.e.i.d.DeviceReachabilityResponseHandler   <b>Error</b> while selecting Device Reachability: <b>Error</b> Message: Could not execute command on device 3315197886, Details: No attribute "CLI_ADDRESS" for device "3315197886"
> Jan 27, 2024 @ 18:38:19.106	network-poller-service	2024-01-27 17:38:19,106   <b>ERROR</b>   xdePooledTaskScheduler-16     c.c.e.n.p.ScheduledPollingTask   Could not execute Feature com.cisco.apicem.feature.feature_deviceReachability, for device 3315197886. Exception No attribute "CLI_ADDRESS" for device "3315197886"

apic-em-inventory-manager-service 2024-01-27 17:38:19,107 | **ERROR** | SimpleAsyncTaskExecutor-4 | | c.c.e.i.d.DeviceReachabilityResponseHandler | **Error** while selecting 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

logst EDIT FILTER Edit as Query DSL

Select

Field Operator

t kul .kubernetes.labels.serv | Select an operator

t log

Available

kubernetes.labels.ser...

kubernetes.labels.ser...

kubernetes.labels.serviceName

Cancel Save

logst EDIT FILTER Edit as Query DSL

Select

Field Operator

t kul kubernetes.label... Select an operator

t log

Available

Create custom label?

is

is not is

is one of

is not one of

exists

does not exist

logst EDIT FILTER Edit as Query DSL

Select

Field Operator

t kul kubernetes.label... is

t log

Available

Value

@t network |

t \_id network-poller-service

t \_in networkvalidationpyservice

# \_sc network-design-service

t \_ty network-orchestration-service

network-validation-service

# Sample use case with Mix and Match

Discover

12 hits

New Save Open Share Inspect

Filters 1 log:error

kubernetes.labels.serviceName: network-poller-service x + Add filter

logstash-\*

Selected fields

- t\_kubernetes.labels.serviceName
- t\_log

Available fields

- @timestamp
- t\_id
- t\_index
- #\_score
- t\_type
- t\_docker.container\_id
- t\_kubernetes.container\_image
- t\_kubernetes.container\_image\_id
- t\_kubernetes.container\_name
- t\_kubernetes.host

Jan 27, 2024 @ 18:35:54.300 - Jan 27, 2024 @ 18:50:54.300 — Auto

Time	kubernetes.labels.serviceName	log
> Jan 27, 2024 @ 18:46:19.102	network-poller-service	2024-01-27 17:46:19,102   ERROR   xdePooledTaskScheduler-3     c.c.e.n.p.ScheduledPollingTask   Could not execute Feature com.cisco.apicem.feature.feature_deviceReachability, for device 3315197886. Exception No attribute "CLI_ADDRESS" for device "3315197886"
> Jan 27, 2024 @ 18:45:19.101	network-poller-service	2024-01-27 17:45:19,101   ERROR   xdePooledTaskScheduler-17     c.c.e.n.p.ScheduledPollingTask   Could not execute Feature com.cisco.apicem.feature.feature_deviceReachability, for device 3315197886. Exception No attribute "CLI_ADDRESS" for device "3315197886"
> Jan 27, 2024 @ 18:44:19.112	network-poller-service	2024-01-27 17:44:19,112   ERROR   xdePooledTaskScheduler-24     c.c.e.n.p.ScheduledPollingTask   Could not execute Feature com.cisco.apicem.feature.feature_deviceReachability, for device 3315197886. Exception No attribute "CLI_ADDRESS" for device "3315197886"



# 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

# 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



April 26, 2022

To Whom It May Concern

A performance 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,

Ed Paradise  
SVP Engineering  
Cisco S&TO

# 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

- 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):
```

```
*****
```

```
Br00aAAAAQUBAAQAAAABAqAEAAAAAMACAAAAAABAAQ32GC3XwzhRKcsMilrzAzhAUABAAAFoAGAARETkFDBwAMTUFHU0hfTExfQ1...
```

```
*****
```

```
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.

The screenshot shows the System 360 dashboard. At the top, an orange banner displays a warning: "Automation and Assurance services have been temporarily disrupted. The system is working to restore this functionality." A "More Info" link is highlighted in the banner. Below the banner, the page title is "System / System 360". The left sidebar shows "System 360" selected, with "System Health" and "Service Explorer" as sub-headers. The main content area shows the "System 360" overview, including a cluster of hosts and a list of 62 services. The service "apic-em-inventory-manager-service" is highlighted as "Restarting". A "Tools" menu is visible for the selected service, containing "Metrics" and "Logs" links. A blue arrow points from the "More Info" link in the banner to the text "Click here to view which Service(s) is affected".

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
- 172.19.239.135
- 172.19.239.136

[View 62 Services](#)  
[View 68 Services](#)  
[View 70 Services](#)

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

SERVICES (62)  
As of: Feb 3, 2024 6:08 PM

[Filter](#)

Name	Appstack	Health	Version	Tools
apic-em-inventory-manager-service	fusion	Restarting ⓘ	7.1.714.60631	<a href="#">Metrics</a>   <a href="#">Logs</a>
agent	maglev-system	Up ⓘ	1.7.1105	<a href="#">Metrics</a>   <a href="#">Logs</a>
catalogserver	maglev-system	Up ⓘ	1.7.134	<a href="#">Metrics</a>   <a href="#">Logs</a>
cnsr-reasoner	fusion	Up ⓘ	7.28.714.210081	<a href="#">Metrics</a>   <a href="#">Logs</a>

Click here to view which Service(s) is affected

# System in Self Monitoring Mode

## Software Services

Catalyst Center System / System 360

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 Services](#)
- 172.19.239.135 [View 68 Services](#)
- 172.19.239.136 [View 71 Services](#)

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**

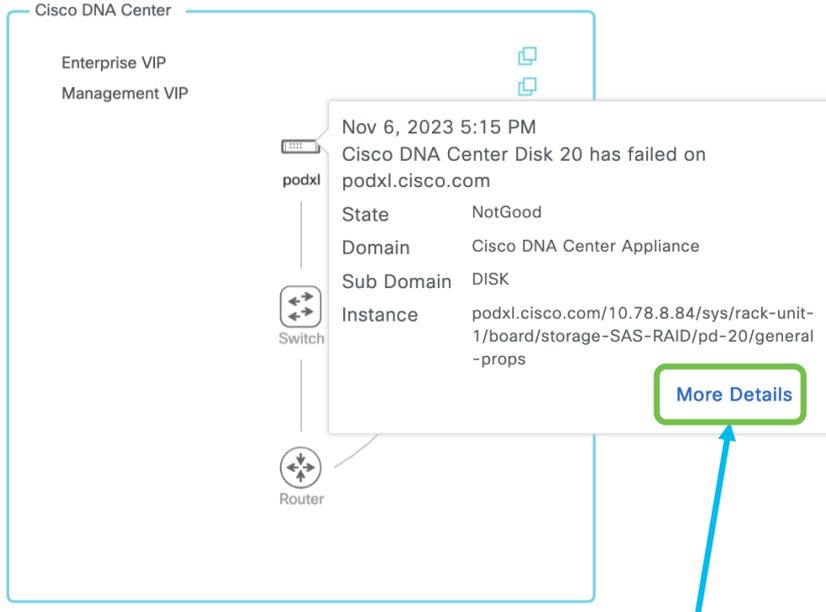
SERVICES (61) As of: Jan 31, 2024 6:38 PM

Filter

Name	Appstack	Health	Version	Tools
agent	maglev-system	Up	1.7.1105	<a href="#">Metrics</a>   <a href="#">Logs</a>
catalogserver	maglev-system	Up	1.7.134	<a href="#">Metrics</a>   <a href="#">Logs</a>
cnsr-reasoner	fusion	Up	7.28.714.210081	<a href="#">Metrics</a>   <a href="#">Logs</a>
collector-iosxe-db	assurance-backend	Up	2.3.7.4138	<a href="#">Metrics</a>   <a href="#">Logs</a>
collector-manager	ndp	Up	5.0.60	<a href="#">Metrics</a>   <a href="#">Logs</a>
connection-manager-service	fusion	Up	2.1.714.60631	<a href="#">Metrics</a>   <a href="#">Logs</a>
contextcache	ndp	Up	5.3.7	<a href="#">Metrics</a>   <a href="#">Logs</a>
credentialmanager	maglev-system	Up	1.7.64	<a href="#">Metrics</a>   <a href="#">Logs</a>
daas-runtime	dnacaap	Up	1.13.247.0	<a href="#">Metrics</a>   <a href="#">Logs</a>
data-cob	fusion	Up	7.1.714.60631	<a href="#">Metrics</a>   <a href="#">Logs</a>

# 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



Cisco DNA Center

1

System / Settings



EQ 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

- **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 dnaac\_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
<b>91</b>	<b>8</b>	<b>16</b>

#### Cisco DNA Center & Device Assurance Results:

Checks Executed	Errors Found	Warnings Found
<b>12</b>	<b>0</b>	<b>0</b>

#### Cisco DNA Center & Device Upgrade Readiness Results:

Checks Executed	Errors Found	Warnings Found
<b>39</b>	<b>2</b>	<b>2</b>

#### Cisco DNA Center SD-Access Health Results:

Checks Executed	Errors Found	Warnings Found
<b>5</b>	<b>2</b>	<b>2</b>

#### Cisco DNA Center Scale Limit Check Results:

Checks Executed	Errors Found	Warnings Found
<b>18</b>	<b>0</b>	<b>0</b>

# Validation Tool

## • 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

### Network Ping

### Validation Tool

### System Analyzer

### 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

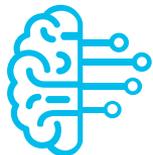
## Automation Capabilities from Inventory Page

### 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)



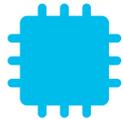
- Data collection via SNMP, CLI or Netconf
- Reports reachability & manageability status
- Convert data to database objects

# 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

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	Unmanaged Device Unreac...

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

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
POD5-WLC	172.16.53.11	Wireless Controller	Reachable

### 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

Scan Failed [CLI Authentica...](#) Error

Not Scanned Managed

More details on clicking the error message

## Provision / Inventory

### 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?"

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

Step 1. Select device IP

Step 2. Select 'Key logs' to view Service logs

The screenshot shows the Inventory Grafana Dashboard interface. At the top, there are filters for Log Pattern, Log Level (set to ERROR), Device IP (192.5.200.245), and Device Id (13661649). Below these filters is a table with columns: id, hostname, type, collectionstatus, reachabilitystatus, inventorystatusdetail, errorcode, devicesupportlevel, collectioninterv, and serialnum. The first row shows a Cisco Catalyst 9500 Switch with collectionstatus 'In Progress' and reachabilitystatus 'Reachable'. Below the table are sections for Basic Stats, Stats, and Device Syncs Stats. The 'Key logs - 13661649 (192.5.200.245)' section is highlighted, showing a list of logs for the device. The logs include messages such as 'SSH2 authentication failure : SSH\_MSG\_USERAUTH\_FAILURE' with error codes like 'ERROR\_LOGIN\_PASSWORD' and error names like 'palConnectionError'.

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

**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: Oct 16, 2022    Oct 31, 2022

**Timestamp** (indicated by a blue arrow pointing to the chart)

Config Drift Version: **October 30, 2022 9:48 PM**    **October 30, 2022 10:58 PM**

Running Config (1619 Lines)    Running Config (1620 Lines)

```

211 erredisable recovery cause psp
212 erredisable 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
  
```

**Configuration Diff** (indicated by a blue arrow pointing to the diff)

```

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
  
```



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** ▾

Q Filter devices

0 Selected **+** Add Device Tag Actions ▾ ⓘ

<input type="checkbox"/>	Device Name ▲	IP Address	Device Family	Reachability ⓘ
<input type="checkbox"/>	BLR_BORDER.cisco.com Main Hub	192.5.101.65	Switches and Hubs (WLC Capable)	Reachable
<input type="checkbox"/>	BLR-EDGE-1.cisco.com	192.5.101.68	Switches and Hubs (WLC Capable)	Reachable
<input type="checkbox"/>	CHN_BORDER.cisco.com	192.5.200.245	Switches and Hubs (WLC Capable)	Reachable
<input type="checkbox"/>	POD5-WLC	172.16.53.11	Wireless Controller	Reachable
<input type="checkbox"/>	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



Customer Voice

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



## Verify Credentials

## Provision / Inventory

### Step 1. Select device in Inventory

Devices (4) Focus: Inventory

Filter devices

1 Selected + Add Device Tag Actions

Device Name	Inventory	Software Image	Provision	Actions
POD5-WLC				<ul style="list-style-type: none"> <li>Edit Device</li> <li>Resync Device</li> </ul>

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

### Edit Device

Credentials Management IP

Type Network Device

### Step 3. Click Validate

Credentials **Validate**

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

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

Credentials Validating...

Note: CLI and SNMP credentials are r 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

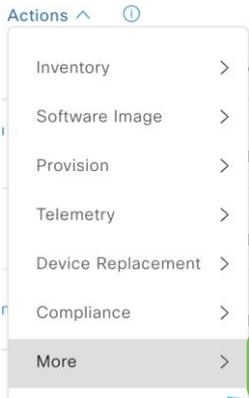
Q2: “Why is my device in an unmanaged or constant syncing or errored state?”



## Check device reachability from Cisco Catalyst Center

```

Command Runner
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 and 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>
  
```



Customer Voice

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



Resync the device

Devices (4) Focus: Inventory

Filter devices

1 Selected

+ Add Device

Tag

Actions



Device Name

Inventory



Edit Device



POD5-WLC

Software Image



Resync Device

Provision



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.  <b>Note</b> 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.  <b>Note</b> 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](https://www.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: <ul style="list-style-type: none"> <li>• Read the device configuration for discovery.</li> <li>• Make configuration changes.</li> </ul> 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: <ul style="list-style-type: none"> <li>• The managed network</li> <li>• Cisco ISE</li> </ul>
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: <a href="http://www.cisco.com/security/pki/">http://www.cisco.com/security/pki/</a>
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.

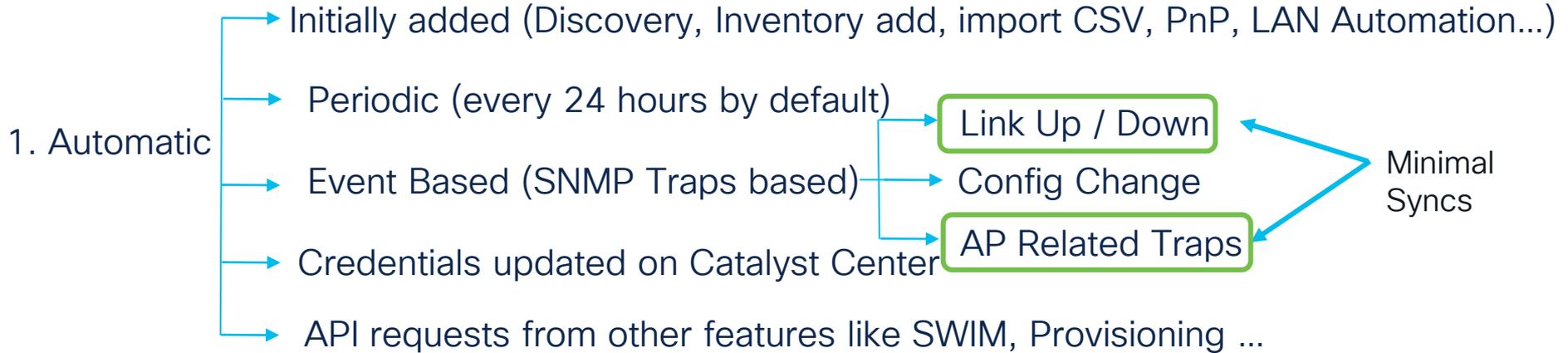
[\\*from Cisco.com](http://www.cisco.com)

**CISCO** Live!



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

- 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://crl.quovadisglobal.com/*)
- [http://\\*.identrust.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](#)

The screenshot shows the Cisco DNA Center interface. The breadcrumb navigation is "Design / Image Repository / Imported Image Family". The page title is "Recent Tasks (Last 50)". There is a "Task Status" dropdown menu and a "Last updated: 7:58 AM" timestamp. The main content area displays a table of tasks. The first task is "nxos64-cs.10.4.1.F.bin" with a red error icon, "Start Time: Sep 13, 2023 7:58 AM", "Duration: Less than 5 seconds", and "Type: IMPORT". A tooltip is visible over this task, containing the text "Invalid Image File. Image file has incorrect header." and a "See Why?" link. The second task is also "nxos64-cs.10.4.1.F.bin" with a "Start Time: 7:46 AM", "Duration: Less than 5 seconds", and "Type: IMPORT". A blue arrow points from the text below to the error message tooltip.

Task Name	Start Time	Duration	Type
nxos64-cs.10.4.1.F.bin	Sep 13, 2023 7:58 AM	Less than 5 seconds	IMPORT
nxos64-cs.10.4.1.F.bin	7:46 AM	Less than 5 seconds	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’.

Check Type	Description	Status
Startup config check	Startup configuration exist for this device	✓
Config register check	Config-register verified successfully <b>Expected:</b> 0xF,0x2102,0x102 <b>Actual:</b> 0xF <b>Action:</b> No action required	✓
Flash check	Image Size is larger than free space <b>Expected:</b> 29 MB Available Free space is: 33 MB <b>Actual:</b> fstage: 6 MB <b>Action:</b> 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 <b>Expected:</b> Cisco DNA Center certificate has to be installed successfully and Device should be able to reach DNAC (10.78.8.83) via HTTPS. <b>Action:</b> 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[17.09.0...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

Start

## 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

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 . 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 again.

- > ✔ 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

Operations Checks

>  Distribution

5 minutes 42 seconds

∨  Activation

5 seconds

>  Block Device Deletion  
1 second

∨  Image Activation  
2 seconds

Activation issue due to misconfiguration

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

# Cisco Catalyst Center Assurance



# Assurance an End-to-End Visibility and Insights



End user **Client** health and visibility



**Network & Services** health

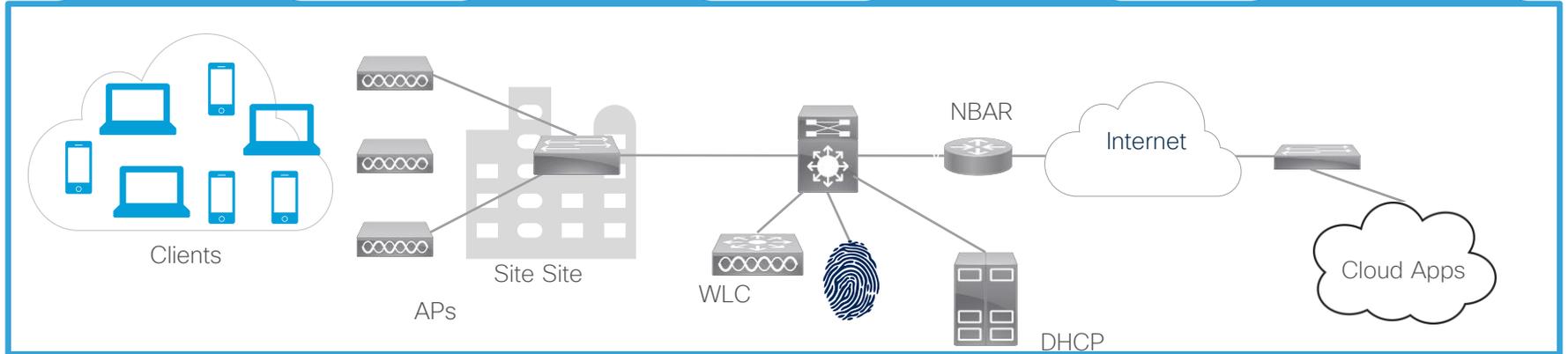


**Application** visibility and performance



**SD-Access** health and status

2.2.3



# 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



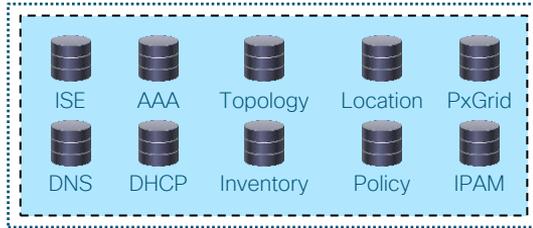
Choose Design > Network Settings > Telemetry

- 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

Device Name	IP Address	Device Family	Site	Reachability	Most recent operation
9500-1.dr.com	172.19.100.3	(WLC Capable)	.../Bangalore/BGL14	Reachable	Device Provisioning
AP006B.F125.F052	12.12.12.11	Unified AP	.../BGL14/F4	Reachable	Success
fusion-1.dr.com	172.19.100.2	Routers	.../Bangalore/BGL14	Reachable	Success
fusion-2.dr.com	172.19.100.10	Routers	.../Bangalore/BGL17	Reachable	Device Controllability and Telemetry
pod7-6500-2.dns-blr1.cisco.com	172.19.100.8	Switches and Hubs	.../Bangalore/BGL14	Reachable	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'

DEVICES (10)  
FOCUS: Provision

Filter | Add Device | Tag | Actions | Take a Tour | 2 Selected

Device Name	Device Family	Site
9500-1.dr.com	(WLC Capable)	.../Bangal
AP006B.F125.F052	Unified AP	.../BGL14
fusion-1.dr.com	Enable Application Telemetry	
fusion-2.dr.com	Disable Application Telemetry	
pod7-6500-2.dns-blr1.c	Switches and Hubs	.../Bangal
pod7-9200-1.cisco.com	Switches and Hubs	.../Bangal
pod7-9200-2.dr.com	Switches and Hubs	.../Bangal

Actions menu items: Inventory, Software Image, Provision, Telemetry, Device Replacement, Others, Compliance. 'Update Telemetry Settings' is highlighted in a green box.

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

### Update Telemetry Settings

Force Configuration Push

GLOBAL/INDIA/BANGALORE/BGL14

Device	Configuration
pod7-9200-1.cisco.com	Syslog Server: Cisco DNA Center
pod7-9200-1.cisco.com	Netflow Collector: Cisco DNA Center
pod7-9200-2.dr.com	Wired Endpoint Data Collection: Yes
pod7-9200-2.dr.com	Cisco TrustSec (CTS) Credentials: Yes
pod7-9200-2.dr.com	SNMP Trap Receiver: Cisco DNA Center
pod7-9200-2.dr.com	Cisco TrustSec (CTS) Credentials: Yes
pod7-9200-2.dr.com	Syslog Level: 6 - Information Messages
pod7-9200-2.dr.com	Controller Certificates: Yes

Step 3. Click Next

Cancel | Next

# Device Checks

## Configurations and Certificates

Release 2.3.3.x  
onwards

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

**Start**

**Deployment of syslog setting** SUCCESS  
No change in setting, so no operation was performed

**Deployment of snmp setting** SUCCESS  
Deployment of snmp setting initiated  
COMPLETED: Deconfiguring old SNMP Trap Server Configurations Settings IP: [100.100.100.16] on the device: 172.200.200.1 completed successfully.  
COMPLETED: Configuring new SNMP Trap Server Configurations Settings IP: [100.100.100.16] on the device: 172.200.200.1 completed successfully.

**Deployment of dns setting** SUCCESS  
DNS Configurations pushed successfully  
Process success on all devices.

**Deployment of netflow setting** SUCCESS  
No change in setting, so no operation was performed

**Application telemetry** SUCCESS  
Configuration of application telemetry is only applicable upon enable/disable application telemetry action, so no operation was performed

**Install of Swim Certificate** SUCCESS  
Installation of SWIM Certificate initiated successfully  
SWIM Certificate installed successfully

**Deployment of WSA certificate** SUCCESS  
Cleaning up exiting network-assurance Configuration on the device  
Cleaned up existing network-assurance configuration successfully  
Starting network-assurance Configuration on the device  
ICAP port and Assurance WSA Configuration pushed successfully  
WSA Certificate was pushed successfully

**Deployment of DTLS Ciphersuites** SUCCESS  
Skip DTLS Ciphersuite Config

**Deployment of Wireless AP Join Certificate** SUCCESS  
Setting does not apply to device, so no operation was performed

**Deployment of PKCS12 certificate** SUCCESS  
Started process: Pkcs12 Internal Certificate Install  
Cisco DNA Center 100.100.100.16 is reachable from device 172.200.200.1  
Cleaned up PKI configurations successfully  
Reachable DNAC IP:100.100.100.16  
PKI Configurations pushed successfully  
PKCS12 Certificate process completed successfully

**i** This difference view represents the configuration changes performed by all the actions (Provisioning, Telemetry, etc.) within a 5 minutes window.

Show only differences  Show entire configs

Running Config (1232 Lines)

Collected at: Oct 5, 2023 2:48 PM

```
80 source interface Vlan200
81 crypto pki trustpoint sdn-network-infra-ivan
82 enrollment url http://100.100.100.16:80/eyJbcA/publicw
b/apply/acep/adsncep
83 fqdn WLC
84 subject-name CN=C9800-40-K9_TTH224105MS_sdn-network-in
fra-ivan
85 revocation-check crl
86 source interface Vlan200
87 rsakeypair sdn-network-infra-ivan
88 output-field 7
89 field cts_rolebased_policy.num_of_sgacl
898 output-field 8
899 field cts_rolebased_policy.policy_life_time
1000 output-field 9
```

Showing Lines 1000 - 1234

```
1 field cts_rolebased_policy.last_updated_time
2 specified
3 wireless aaa policy default-aaa-policy
```

Running Config (1233 Lines)

Collected at: Oct 10, 2023 11:41 PM

```
80 source interface Vlan200
81 crypto pki trustpoint sdn-network-infra-ivan
82 enrollment url http://100.100.100.16:80/eyJbcA/publicw
b/apply/acep/adsncep
83 fqdn WLC.dr.com
84 subject-name CN=C9800-40-K9_TTH224105MS_sdn-network-in
fra-ivan
85 subject-alt-name WLC.dr.com
86 revocation-check crl
87 source interface Vlan200
88 rsakeypair sdn-network-infra-ivan
89 output-field 7
898 field cts_rolebased_policy.num_of_sgacl
899 output-field 8
1000 field cts_rolebased_policy.policy_life_time
```

```
1 output-field 9
2 field cts_rolebased_policy.last_updated_time
3 specified
4 wireless aaa policy default-aaa-policy
```

# Device Checks

## Verification Routines using the Network Reasoner

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

### Assurance Telemetry Analysis

---

Perform detailed Assurance telemetry analysis of the device.

Network Impact:      Low

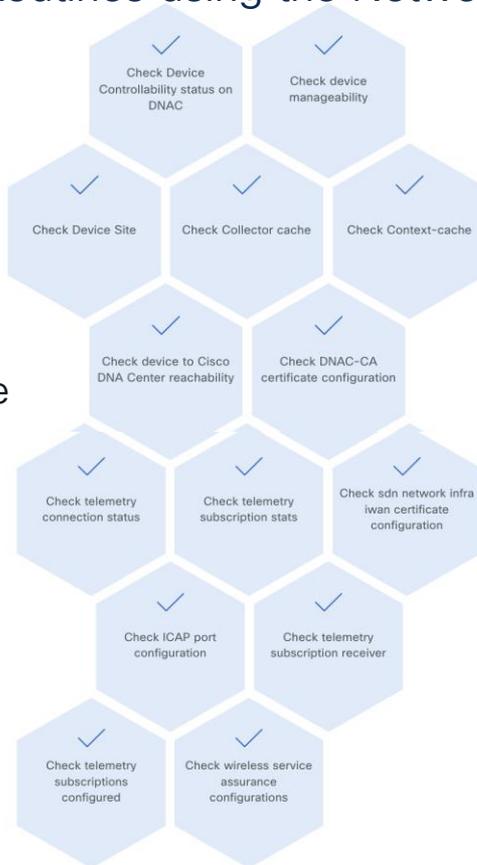
Step 2. Choose one device & click on Troubleshoot

Tag	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

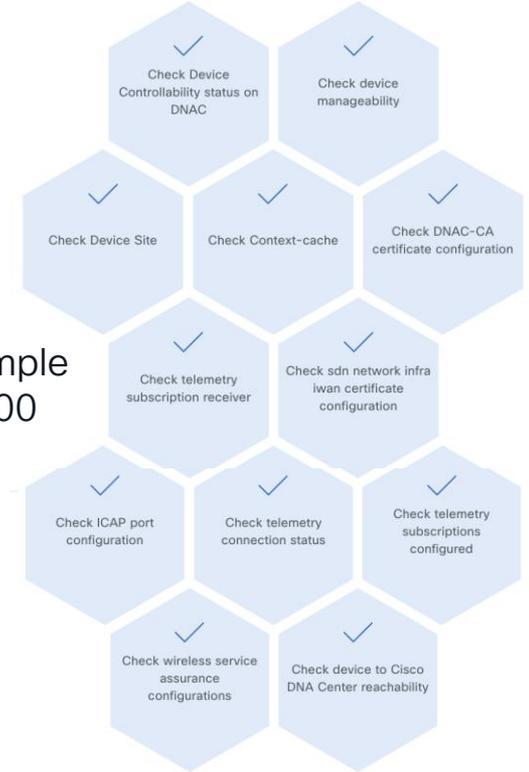
## Verification Routines using the Network Reasoner

Release 2.3.5.x  
onwards



Example 1. Sample output for a 9800 WLC

Example 2. Sample output for a 9300 switch



# Device Checks

## Verification Routines using the Network Reasoner

ⓘ 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](#)

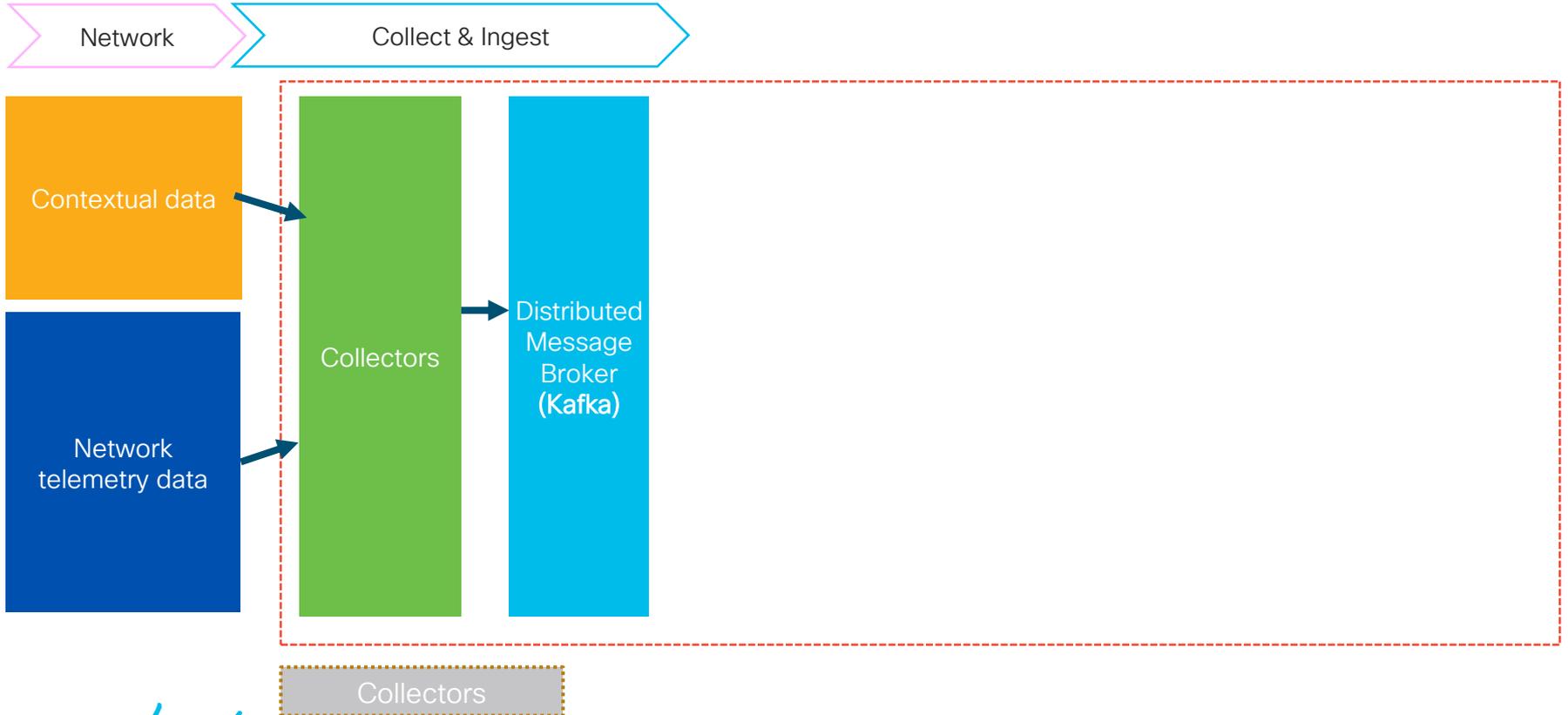
ⓘ Telemetry Subscriptions present are as follows:

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

ⓘ WSA enabled and configured correctly.

[View Relevant Activities](#)

# Assurance System Flow



# Assurance Collectors Check

Cisco DNA Center

System / Data Platform

Collectors Store Settings Pipelines Task Managers

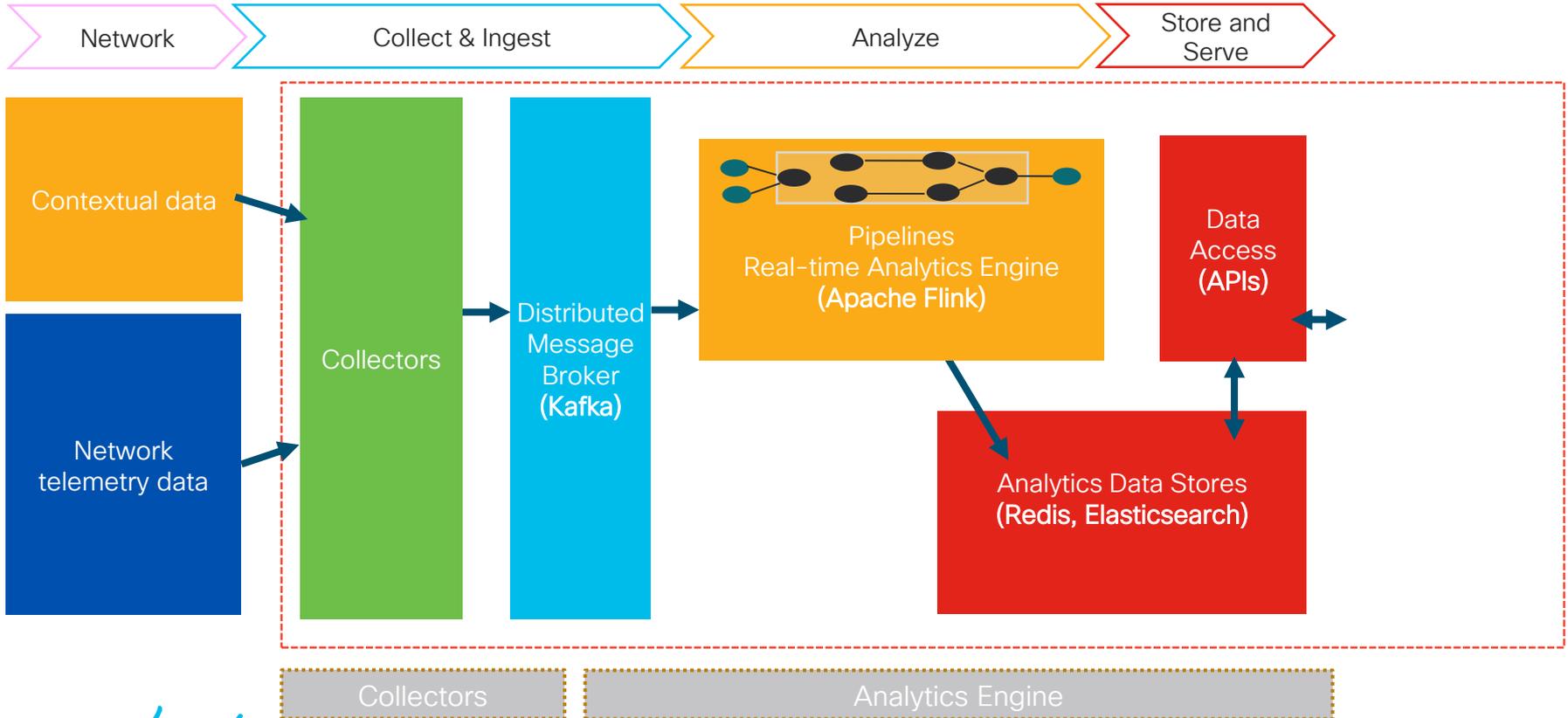
<p>CREATED OCT 10, 2023, 5:35:00 PM</p> <p><b>COLLECTOR-SNMP</b></p> <hr/> <p>Namespace: com.cisco.tesseract</p> <hr/> <p>Version: 0.7.0</p>	<p>CREATED OCT 10, 2023, 5:35:00 PM</p> <p><b>EAWORKER</b></p> <hr/> <p>Namespace: com.cisco.tesseract</p> <hr/> <p>Version: 0.9.0</p>	<p>CREATED OCT 10, 2023, 5:35:00 PM</p> <p><b>DATA-COB</b></p> <hr/> <p>Namespace: com.cisco.dnac.cob</p> <hr/> <p>Version: 0.0.1</p>
<p>CREATED OCT 10, 2023, 5:35:00 PM</p> <p><b>COLLECTOR-IOSXE-DB</b></p> <hr/> <p>Namespace: com.cisco.tesseract</p> <hr/> <p>Version: 0.7.0</p>	<p>CREATED OCT 10, 2023, 5:35:00 PM</p> <p><b>WIRELESSCOLLECTOR</b></p> <hr/> <p>Namespace: com.cisco.tesseract</p> <hr/> <p>Version: 0.7.0</p>	<p>CREATED OCT 10, 2023, 5:35:00 PM</p> <p><b>ROGUE-SERVICE</b></p> <hr/> <p>Namespace: assurance-backend</p> <hr/> <p>Version: 0.7.0</p>
<p>CREATED OCT 10, 2023, 5:35:00 PM</p> <p><b>GRPC-COLLECTOR</b></p> <hr/> <p>Namespace: com.cisco.tesseract</p> <hr/> <p>Version: 0.7.0</p>	<p>CREATED OCT 10, 2023, 5:36:00 PM</p> <p><b>NETWORK-POLLER-SERVICE</b></p> <hr/> <p>Namespace: com.cisco.tesseract</p> <hr/> <p>Version: 0.7.0</p>	<p>CREATED OCT 10, 2023, 5:37:00 PM</p> <p><b>COLLECTOR-SYSLOG</b></p> <hr/> <p>Namespace: com.cisco.tesseract</p> <hr/> <p>Version: 0.7.0</p>
<p>CREATED OCT 10, 2023, 5:36:00 PM</p> <p><b>COLLECTOR-TRAP</b></p> <hr/> <p>Namespace: com.cisco.tesseract</p> <hr/> <p>Version: 0.7.0</p>	<p>CREATED OCT 10, 2023, 5:38:00 PM</p> <p><b>COLLECTOR-NETFLOW</b></p> <hr/> <p>Namespace: com.cisco.tesseract</p> <hr/> <p>Version: 0.7.0</p>	



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

Collectors Store Settings **Pipelines** Task Managers

System / Data Platform

Available Task Slots

12

Total Task Slots 52 | Task Managers 7

Running Jobs

20

Finished 0 | Canceled 0 | Failed 0

Export

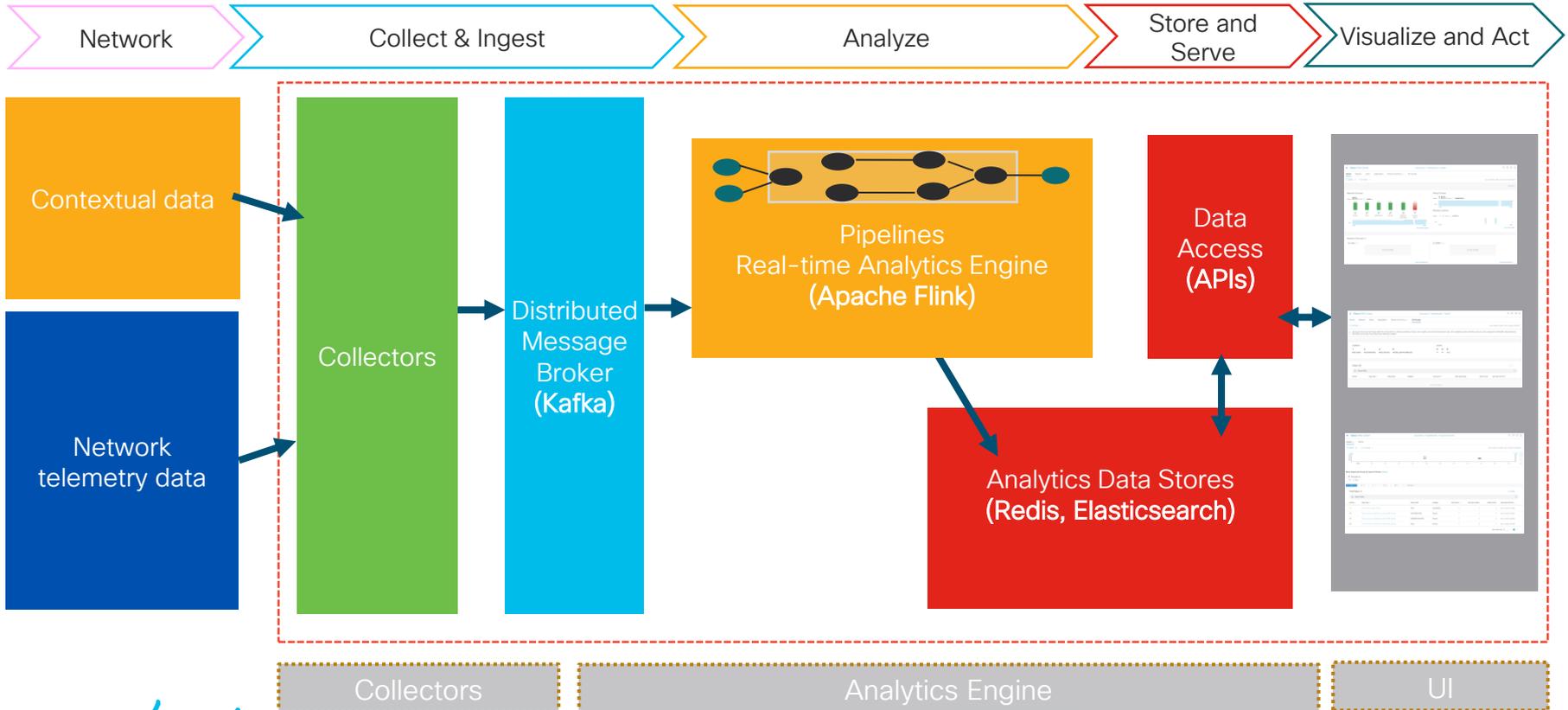
Status of the Pipelines

Filter

Find

Job Name	Duration	Task Manager	Version	Manifest Version	Application	Status	Actions
deviceprocessor	6m, 18s	169-254-37-88...	2.3.3.584	2.0	assurance	RUNNING	
docwriter	22d, 3h, 55m, 9s	169.254.37.232...	5.0.110	2.1	ndp-platform	RUNNING	
endpoint-analytics	22d, 3h, 55m, 9s	169.254.37.230...	1.7.702	0.1	endpoint-analytics	RUNNING	
eventwriter	22d, 3h, 55m, 9s	169.254.37.88...	2.3.3.584	2.0	assurance	RUNNING	
graphwriter	22d, 3h, 55m, 9s	169.254.37.232...	5.0.110	2.1	ndp-platform	RUNNING	
intelligentcapture	22d, 3h, 55m, 10s	169.254.37.88...	2.3.3.584	2.0	assurance	RUNNING	

# Assurance System Flow



# Assurance – Network Health

## Validation Tool – (System → System Health → Tools)

### 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

Choose your target release version

Installed version: 2.3.3.7-72328

- Go green! Configure AP power profiles.

**SecOps**

- Enhance security by automatically remediating rogue access points.

For additional details, please see the [Cisco DNA Center 2.3.5.x](#)

Release 2.3.3.7-72328-HF4

**\*\*ATTENTION:\*\*** The updated version of 2.3.3.7 is available for new and existing customers. All 2.3.2.1 customers, follow the instructions in [Upgrade from Release 2.3.2.1 to Release 2.3.3.7](#)

This release offers new features to improve operational efficiency and enhance the experience of network users, including:

**AIOps and Analytics**

- Identify and correlate issues using the new global assurance event viewer.
- Get deeper insights into wireless client behavior with Intel Connectivity Analytics.

Cancel

Select

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

# Catalyst Center Software Version

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
<a href="#">CSCwe15923</a>	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.
<a href="#">CSCwh81546</a>	An internally autogenerated etcd certificate is not activated after upgrade. This problem occurs in the following scenario: <ol style="list-style-type: none"> <li>Cisco DNA Center is freshly installed using 2.3.5.3, or is upgraded to 2.3.5.3.</li> <li>The etcd certificate renews, but is not activated (etcd keeps using the old certificate).</li> <li>Cisco DNA Center is upgraded to 2.3.5.4.</li> <li>After the upgrade, the old certificate is still used. The system is expected to experience an outage when the certificate expires.</li> </ol>

# 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

System / Software Management

System / Software Management

Installed Version: 2.3.3.7-72328

Currently Installed Applications

Release 2.3.5.4-70852 is available

The latest Cisco DNA Center release includes new use cases to increase IT team agility and provide a consistent end user experience. Some of the key highlights include:

#### AIOps and Analytics

- Speed up troubleshooting with the client DNS service dashboard.

#### NetOps

- Go green! Configure AP power profiles.

#### SecOps

- Enhance security by automatically remediating rogue access points.

For additional details, please see the [Cisco DNA Center 2.3.5.x Release](#)

Read More

Download now

Looking for other releases

[Click here](#)

New applications are available to download

[View available downloads](#)

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

### Choose your target release version

Installed version: 2.3.3.7-72328

Release 2.3.5.4-70852 **LATEST**

The latest Cisco DNA Center release includes new use cases to increase IT team agility and provide a consistent end user experience. Some of the key highlights include:

#### AIOps and Analytics

- Speed up troubleshooting with the client DNS service dashboard.

#### NetOps

- Go green! Configure AP power profiles.

#### SecOps

- Enhance security by automatically remediating rogue access points.

For additional details, please see the [Cisco DNA Center 2.3.5.x Release](#)

Release 2.3.5.3-70194

The latest Cisco DNA Center release includes new use cases to increase IT team agility and provide a consistent end user experience. Some of

Cancel

Select

### Choose your target release version

Installed version: 2.3.3.7-72328

- Go green! Configure AP power profiles.

#### SecOps

- Enhance security by automatically remediating rogue access points.

For additional details, please see the [Cisco DNA Center 2.3.5.x Release](#)

Release 2.3.3.7-72328-HF4

**\*\*ATTENTION:\*\*** The updated version of 2.3.3.7 is available for new and existing customers. All 2.3.2.1 customers, follow the instructions in [Upgrade from Release 2.3.2.1 to Release 2.3.3.7](#)

This release offers new features to improve operational efficiency and enhance the experience of network users, including:

#### AIOps and Analytics

- Identify and correlate issues using the new global assurance event viewer.
- Get deeper insights into wireless client behavior with Intel Connectivity Analytics.

Cancel

Select

# 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: 2.3.3.7-72328 [Currently Installed Applications](#)

## Release 2.3.5.4-70852 is available

The latest Cisco DNA Center release includes new use cases to increase IT team agility and provide a consistent end user experience. Some of the key highlights include:

### AIOps and Analytics

- Speed up troubleshooting with the client DNS service dashboard.

### NetOps

- Go green! Configure AP power profiles.

### SecOps

- Enhance security by automatically remediating rogue access points.

For additional details, please see the [Cisco DNA Center 2.3.5.x Release Notes](#).

[Read More](#)

[Download now](#)

The screenshot shows the Cisco DNA Center 'System / Software Management' page. It displays the current installed version (2.3.3.7-72328) and a notification for a new release (2.3.5.4-70852). The notification lists key highlights under three categories: AIOps and Analytics, NetOps, and SecOps. Below the notification are 'Read More' and 'Download now' buttons. A modal dialog box titled 'Preparing 2.3.5.4-70852 for download' is open, showing a green checkmark and the message 'Download Prechecks Completed Successfully'. The dialog also lists the checks performed: External connectivity, certificate validation, proxy validation, and disk space. At the bottom of the dialog are 'Cancel' and 'Download' buttons.

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

# The Upgrade Process

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

System and Applications packages downloaded in the same step

System / Software Management

Installed Version: 2.3.3.4-72142    Currently Installed Applications

Release 2.3.4.0-70523 is available

[Read More](#)    [Install now](#)

Downloading release 2.3.4.0-70523 . Downloaded (27/45) [More details](#)

63%

Downloading release 2.3.4.0-70523 applications

The applications below are being downloaded to your system

Application Name	Version	Size	Status
Automation - Intelligent Capture	2.1.560.60835	11.27 MB	Downloaded
Automation - Sensor	2.1.560.60835	200.96 MB	75%
Machine Reasoning	2.1.560.210319	179.57 MB	Downloaded
Path Trace	2.1.560.60835	580.68 MB	Downloaded
Rogue and aWIPS	2.6.0.36	9.51 MB	75%
PROGRAMMABILITY AND INTEGRATIONS			
Application Name	Version	Size	Status
Cisco DNA Center Platform	1.9.1.78	2.05 GB	100%
POLICY APPLICATIONS			
Application Name	Version	Size	Status
Access Control Application	2.1.560.60835	157.79 MB	75%
AI Endpoint Analytics	1.8.525	159.60 MB	75%
Group-Based Policy Analytics	2.3.4.17	181.12 MB	75%
SYSTEM			
Application Name	Version	Size	Status
catalogserver	1.7.774	N/A	Downloaded
main-system-package	1.7.774	N/A	Downloaded
system-updater	1.7.774	N/A	Downloaded

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

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

☰ Cisco DNA Center

Currently Installed Applications

Release 2.3.3.4-72142 is available

**\*\*ATTENTION:\*\*** All 2.3.2.1 customers, follow the instructions in [Upgrade from Release 2.3.2.1 to Release 2.3.3.4](#)

This release offers new features to improve operational efficiency and enhance the experience of network users, including:

#### AIOps and Analytics

- Identify and correlate issues using the new global assurance event viewer.
- Get deeper insights into wireless client behavior with Intel Connectivity Analytics.
- View client location in 3D maps for improved visibility troubleshooting.

Read More

Download now

☰ Cisco DNA Center

Currently Installed Applications

Release 2.3.3.4-72142 is available

**\*\*ATTENTION:\*\*** All 2.3.2.1 customers, follow the instructions in [Upgrade from Release 2.3.2.1 to Release 2.3.3.4](#)

This release offers new features to improve operational efficiency and enhance the experience of network users, including:

#### AIOps and Analytics

- Identify and correlate issues using the new global assurance event viewer.
- Get deeper insights into wireless client behavior with Intel Connectivity Analytics.
- View client location in 3D maps for improved visibility troubleshooting.

Read More

Install now

Preparing 2.3.3.4-72142 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.

Cancel

Install

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

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

CISCO *Live!*

# 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

☰ Cisco DNA Center

System / Software Management

Installed Version: 2.3.4.0-70523 [Currently Installed Applications](#)

### Release 2.3.6.0-70096 is available

We are pleased to announce the availability of Cisco DNA Center 2.3.6.0.70096.

[Read More](#)

[Download now](#)



There are earlier releases downloaded on your system. [Available installations](#)

Looking for other releases? [Click here](#)

Available installations

Installed version: 2.3.4.0-70523

- Release 2.3.5.0-70517

We are pleased to announce the availability of Cisco DNA Center 2.3.5.0.70517.

[Cancel](#) [Select](#)

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

Step 3 (optional). Install Optional Application packages

☰ Cisco DNA Center

Currently Installed Applications

Release 2.3.3.4-72142 is available

**\*\*ATTENTION:\*\*** All 2.3.2.1 customers, follow the instructions in [Upgrade from Release 2.3.2.1 to Release 2.3.3.4](#)

This release offers new features to improve operational efficiency and enhance the experience of network users, including:

#### AIOps and Analytics

- Identify and correlate issues using the new global assurance event viewer.
- Get deeper insights into wireless client behavior with Intel Connectivity Analytics.
- View client location in 3D maps for improved visibility troubleshooting.

[Read More](#)

[Download now](#)

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

**CISCO** Live!

☰ Cisco DNA Center

Currently Installed Applications

Release 2.3.3.4-72142 is available

**\*\*ATTENTION:\*\*** All 2.3.2.1 customers, follow the instructions in [Upgrade from Release 2.3.2.1 to Release 2.3.3.4](#)

This release offers new features to improve operational efficiency and enhance the experience of network users, including:

#### AIOps and Analytics

- Identify and correlate issues using the new global assurance event viewer.
- Get deeper insights into wireless client behavior with Intel Connectivity Analytics.
- View client location in 3D maps for improved visibility troubleshooting.

[Read More](#)

[Install now](#)

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

Available applications for 2.3.4.0-70523

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

[Select All](#)



Disaster Recovery



Provides active-passive disaster recovery for Cisco DNA Center

[View Details](#)

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

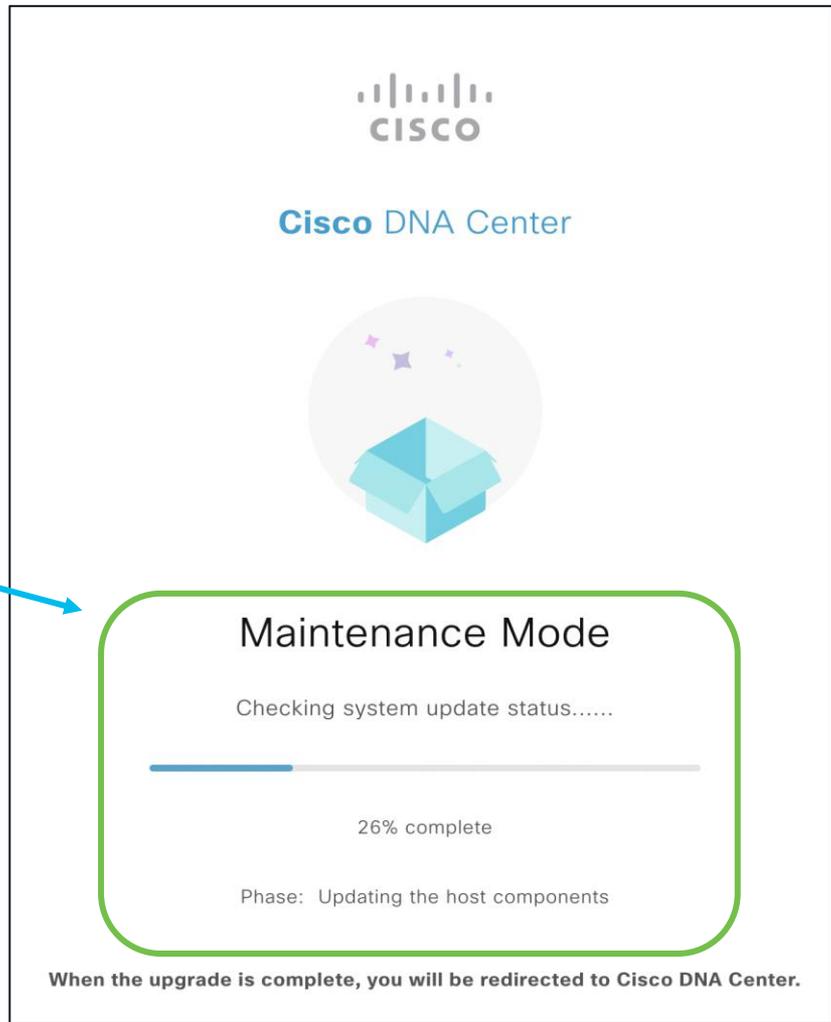
# Software Upgrade Process Enhancements

Changes	2.2.x and below	Introduced in 2.3.x
Choosing a Target Release	<ul style="list-style-type: none"> <li>• Either the latest patch release or the next available release</li> <li>• Can be confusing</li> </ul>	<ul style="list-style-type: none"> <li>• Multiple options</li> <li>• Easy to understand single drop down window</li> </ul>
Upgrade Process (compulsory steps)	<p><u>3 Steps</u></p> <ol style="list-style-type: none"> <li>1. Click 'Update' to upgrade the System packages</li> <li>2. Click 'Download All' to download the Applications packages</li> <li>3. Click 'Update All' to upgrade the Applications packages</li> </ol>	<p><u>2 Steps</u></p> <ol style="list-style-type: none"> <li>1. Click 'Download' to download all packages (System + Applications)</li> <li>2. Click 'Install' to install all packages (System + Applications)</li> </ol>
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

CISCO *Live!*



# The Upgrade Process

## Monitoring and Troubleshooting System Upgrade

### 1. System 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

### 2. Applications Upgrade

```
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	<b>Error response from daemon: Get https://registry.ciscoconnectdna.com/v1/_ping: x509: certificate signed by unknown authority</b>
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 ...

Logs

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

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
```

# 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%)

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

### 2. Applications Upgrade

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

} Node Agnostic  
} 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

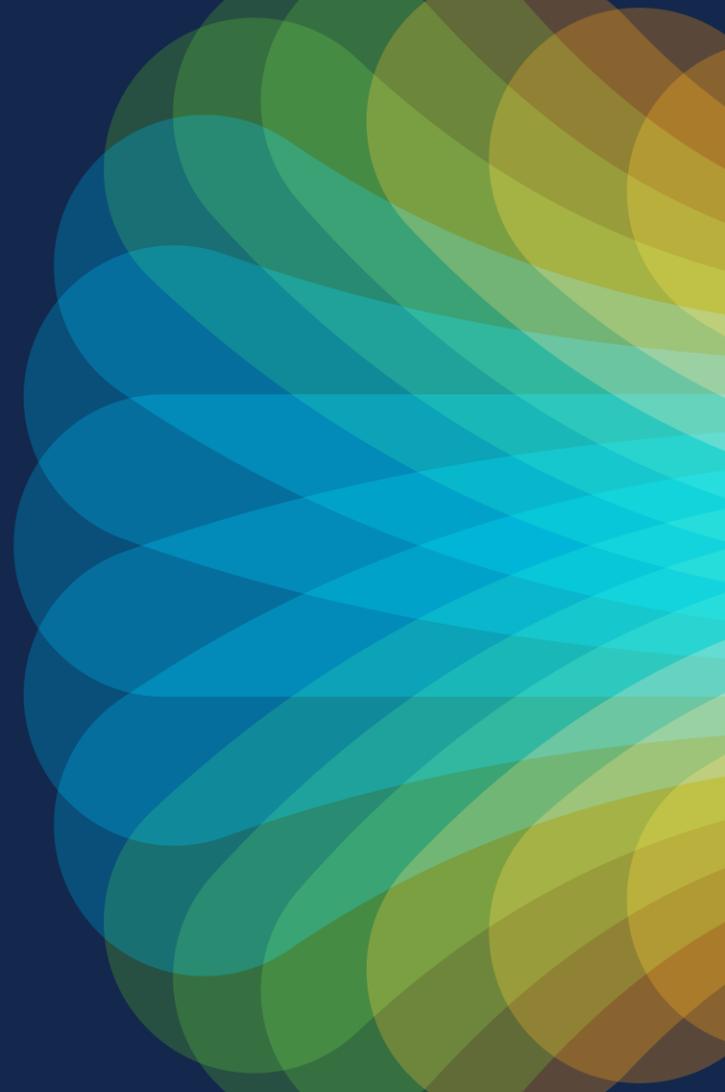
# The Upgrade Process (Prerequisites)

- 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
- 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

(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 ...)

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

# Cisco Catalyst Center Troubleshooting Tools & Other Services

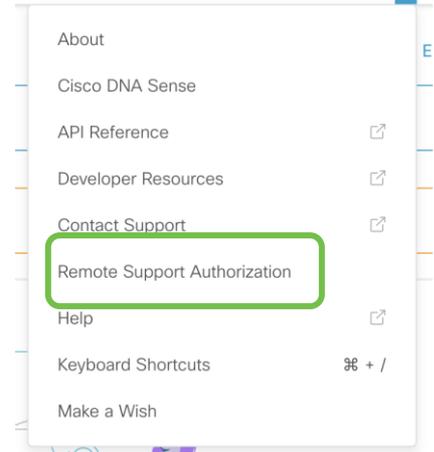


# Collecting Logs for Troubleshooting

- 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.

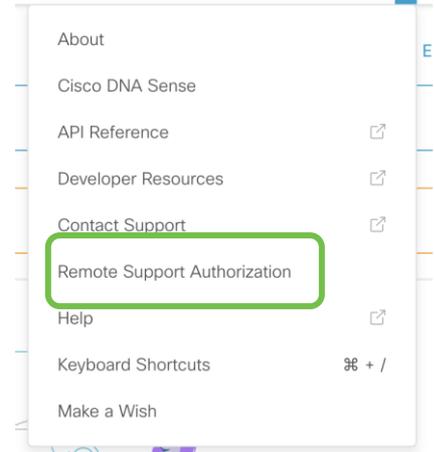


For more details reach out to us at the [RADKit Community Page](#)

# 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.

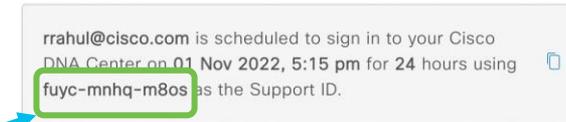


Step 1. Provide password for RADKit clients to access the Cisco Catalyst Center



Done! Authorization is created.

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.



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

For more details reach out to us at the [RADKit Community Page](#)

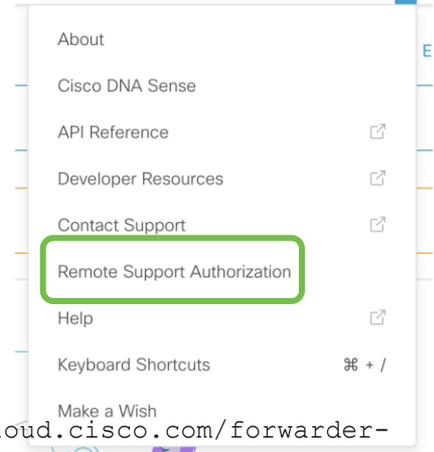
Step 2. Schedule access for 24 hours (default) for a specific Cisco email id.

# 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.
```

\* Works with Magshell

## Commonly used

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

# Collecting Audit Logs for Troubleshooting

# Collecting Logs for Troubleshooting

Audit Logs

Tasks

Work Items

- Audit Logs

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

Time	Description	Category	Severity	User
Filter				
Today <span style="float: right;">10 of 10</span>				
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.

# Collecting Logs for Troubleshooting

- Audit Logs

## 5 Filters available on the top left corner

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

The screenshot shows the Audit Logs interface. At the top, there is a date range filter: "By Date" (dropdown), "Sep 22, 2021 10:03 PM - Sep 21, 2022 10:03 PM" (text), and a refresh icon. Below this is a "SUMMARY" section with a "Severity (3)" dropdown and three checkboxes: "Critical Issue", "Warning", and "Info". A "Filter" dropdown is open, showing three input fields: "User Id", "Log Id", and "Description". At the bottom of the filter dropdown are "Cancel" and "Apply" buttons. The main content area shows a timeline view with a "10:03p" label and a bar chart with markers for "10/1", "11/1", and "12/1".

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

Syslog Server(s): 

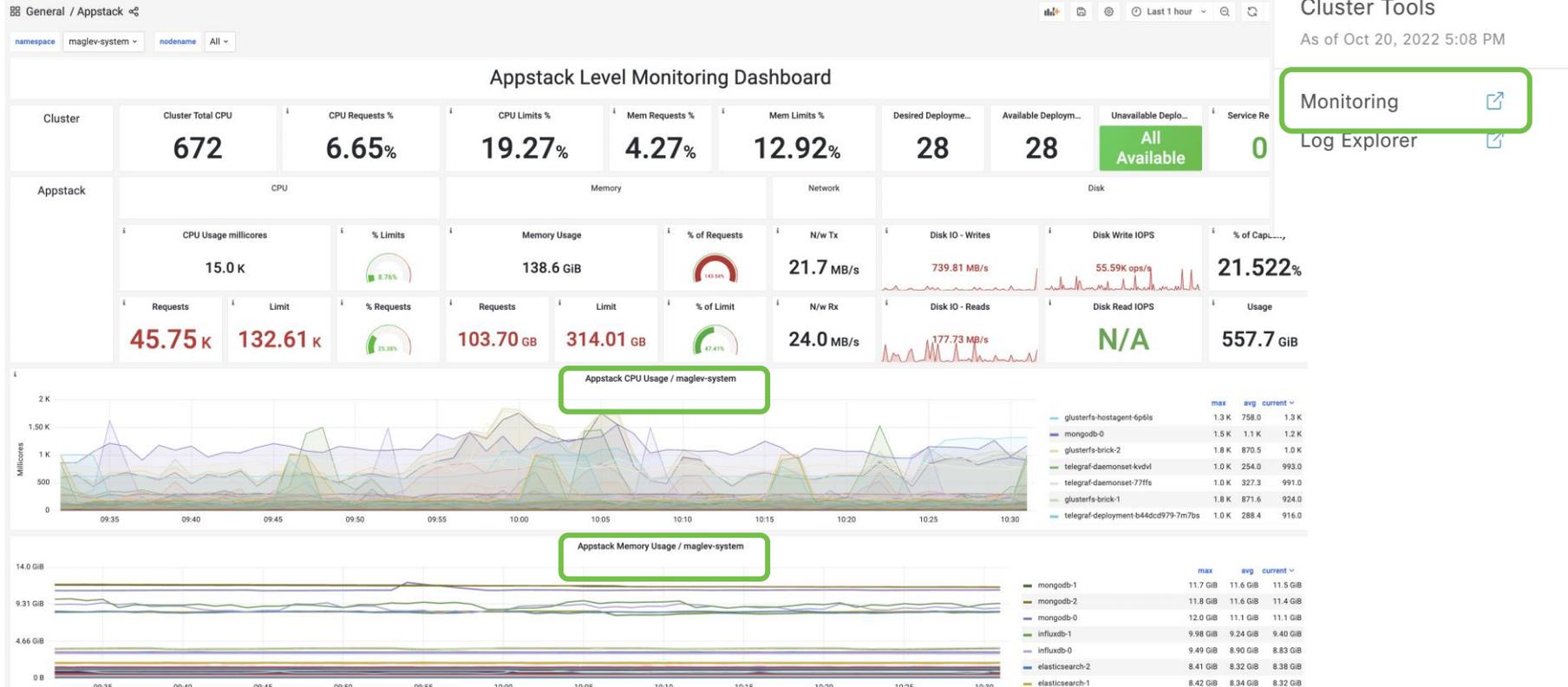
# Monitoring Service Statistics



# Grafana Dashboards

System / System 360

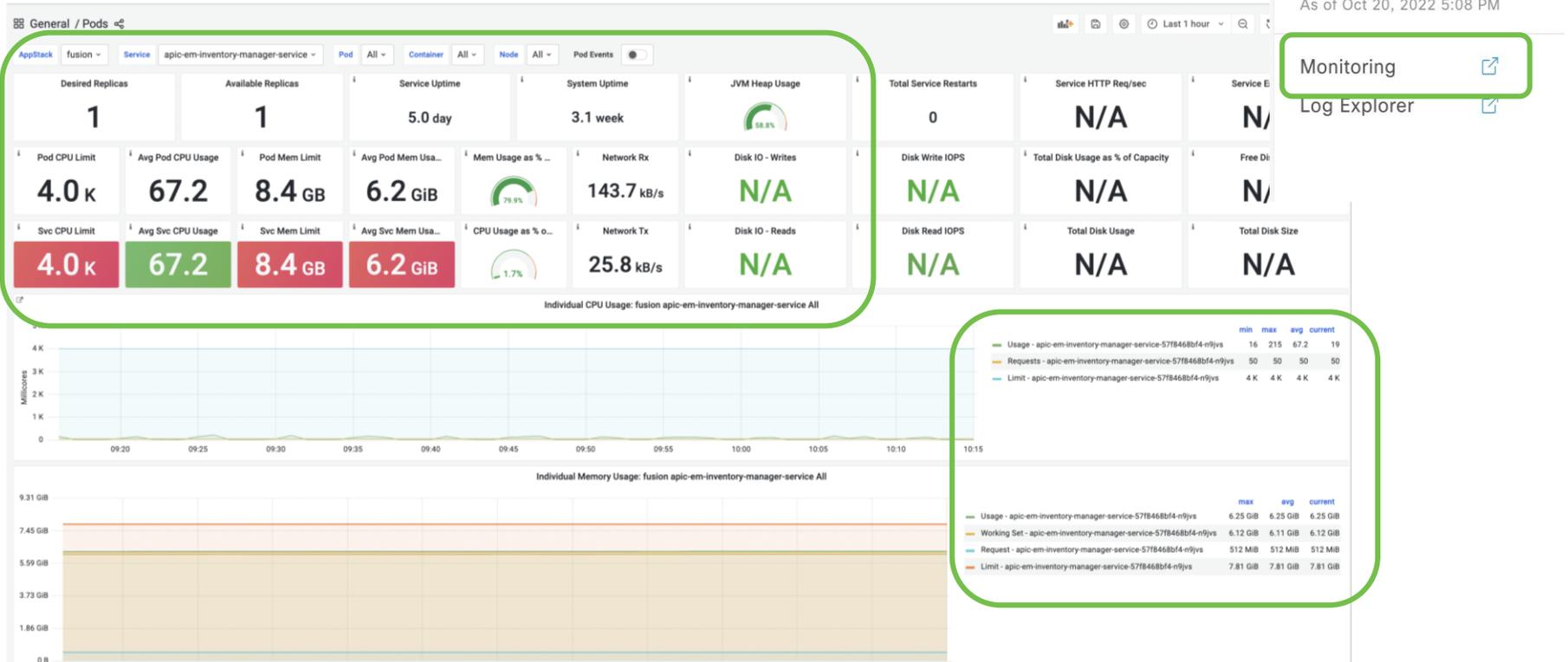
## • Appstack Level Dashboard (default)



# Grafana Dashboards

System / System 360

- Monitoring Service level Memory and CPU requirements (Live)



# Grafana Dashboards

- Monitoring JVM Metrics per Service (Live)

System / System 360

## Cluster Tools

As of Oct 20, 2022 5:08 PM

Monitoring [↗](#)

Log Explorer [↗](#)

General / JVM Metrics

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

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



📊 📄 ⚙️ 🕒 Last :

Heap Memory Used	2.26			
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)

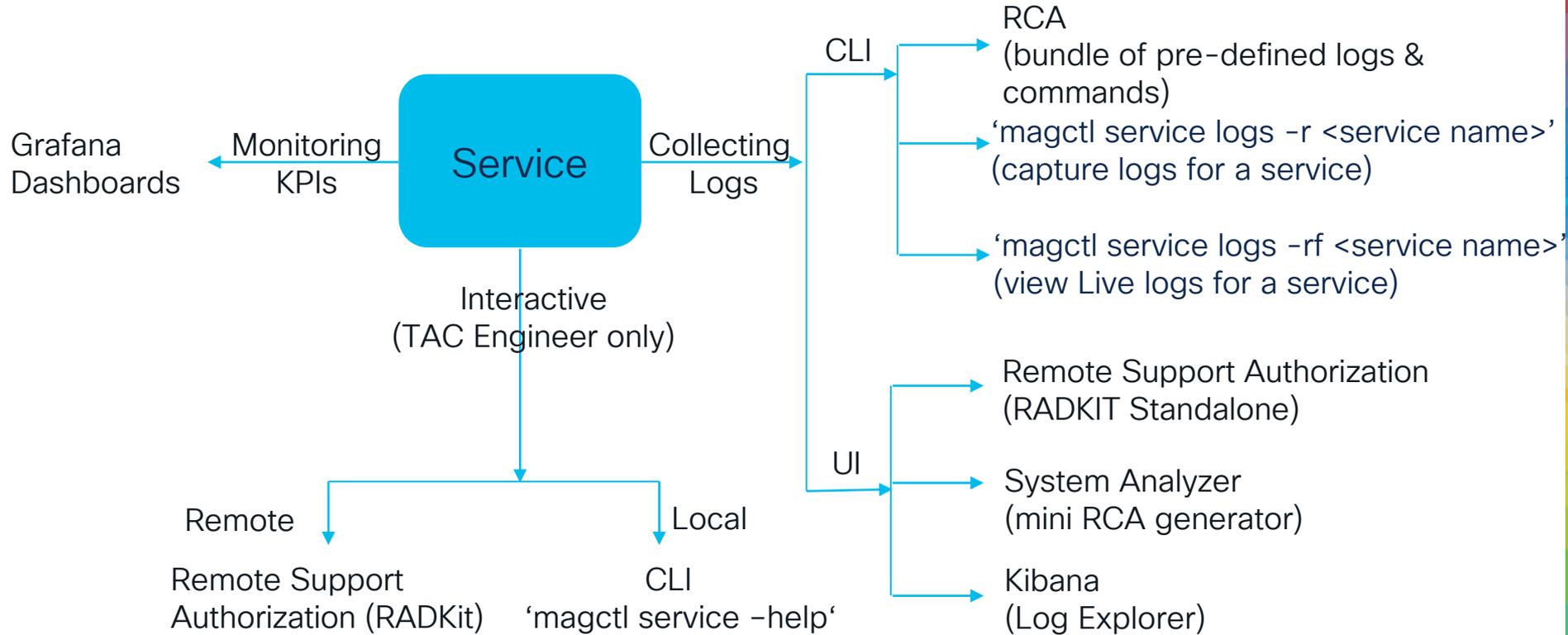


	max	avg	current
Total	425	416	419
blocked	0	0	0
daemon	102	93	94
deadlock	0	0	0
new	0	0	0
runnable	48	44	45
terminated	0	0	0

\*Most Services are Java based



# Troubleshooting Services – Cheat sheet



# 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](http://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!*



The Cisco Live! logo features the word "CISCO" in a bold, black, sans-serif font, followed by "Live!" in a black, cursive script font. The background of the entire image is a vibrant, multi-colored abstract pattern of overlapping, wavy bands in shades of red, orange, yellow, green, and blue, creating a sense of motion and energy.

CISCO *Live!*

Let's go