

Deploying Nexus Dashboard in your Organization

cisco Live !

Matthias Wessendorf
Principal Technical Marketing Engineer
@matteq4er

Agenda

- 01 Introduction
- 02 What is Nexus Dashboard?
- 03 A view under the hood
- 04 Deploying Nexus Dashboard
- 05 Operating Nexus Dashboard
- 06 Summary

Before we start!

- This presentation is focusing on the Unified Nexus Dashboard Release 4.1
- We are covering the infra part and not the functionality details of Orchestrator, Telemetry or Controller

At the end of the session you will ...

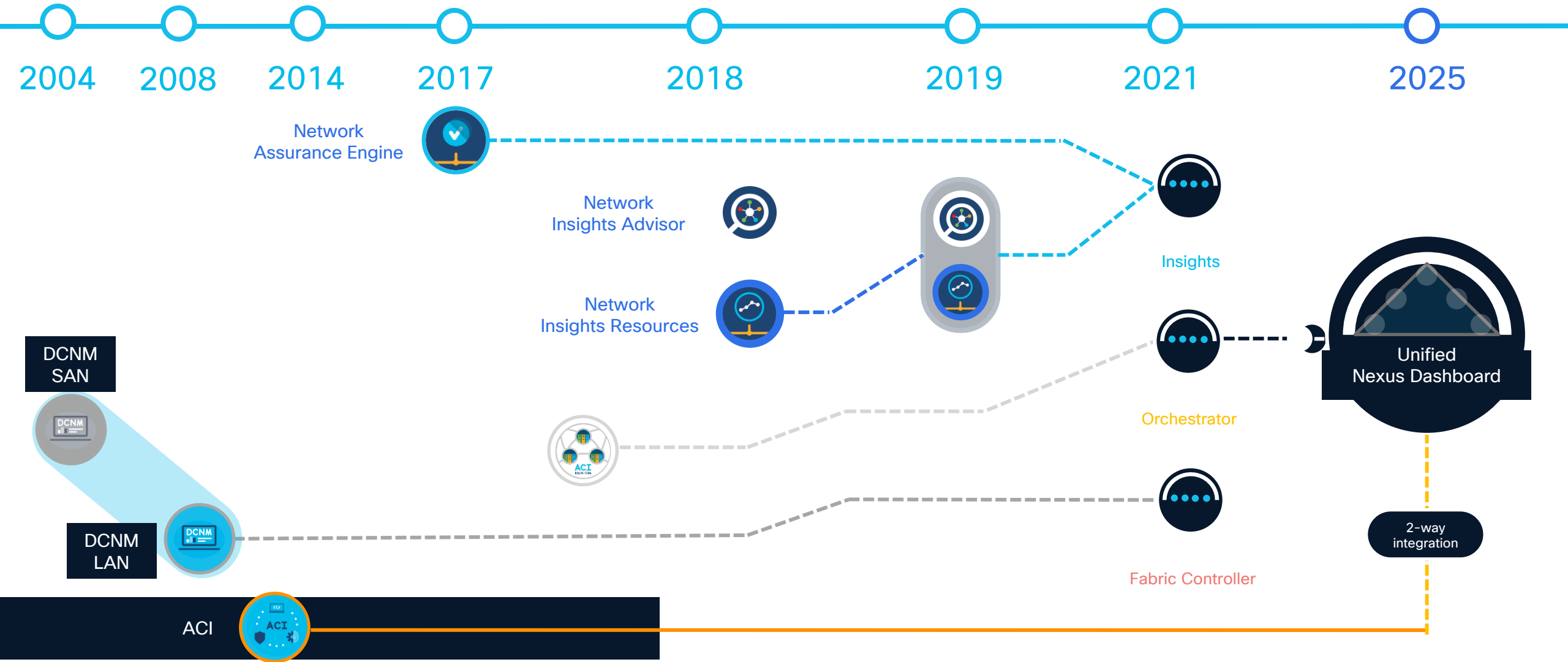
- Be able to define the requirements for deploying a Nexus Dashboard in your Organisation. By describing the
 - Deployment model, HA and DR
 - Network requirements and attachment to the network
 - Sizing a Nexus Dashboard for the different services.

Introduction

We have embarked on a journey

Towards simplification and unification

 Products have evolved through the years with microservices-based architectures & other enhancements



Which leads us here...

Unified Nexus Dashboard

Provisioning



Operations

Access to Nexus Dashboard services/features is based on the Cisco Nexus 9000 [switch license tier](#)

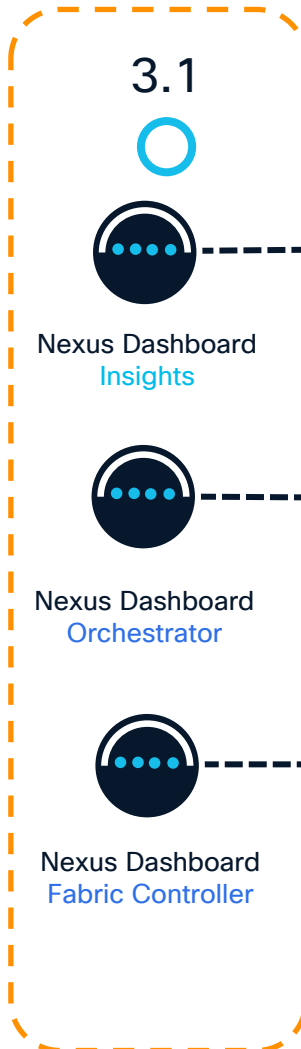
Nexus Dashboard – Unified What?

A journey of combining six products into one

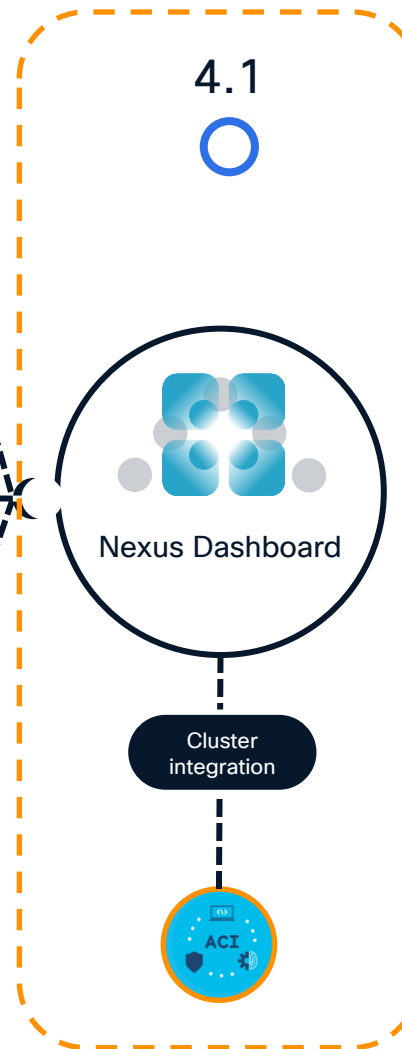
Unified Image

- Single Image Installation
- All Services pre-installed (NDO/NDI/NDFC)
- Service versions bound to ND version

Unified Image



Unified Product

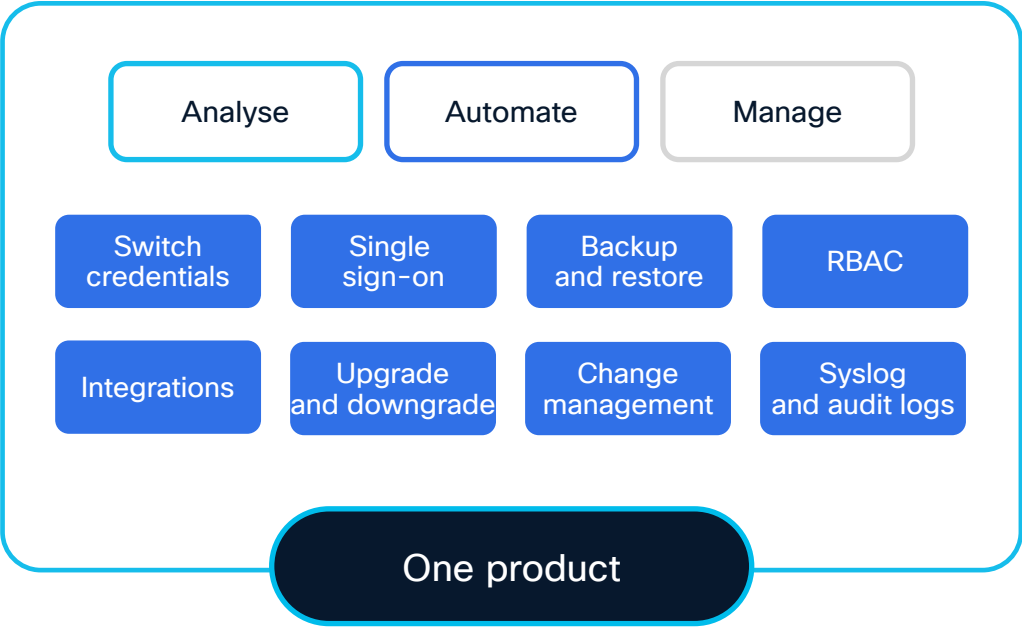
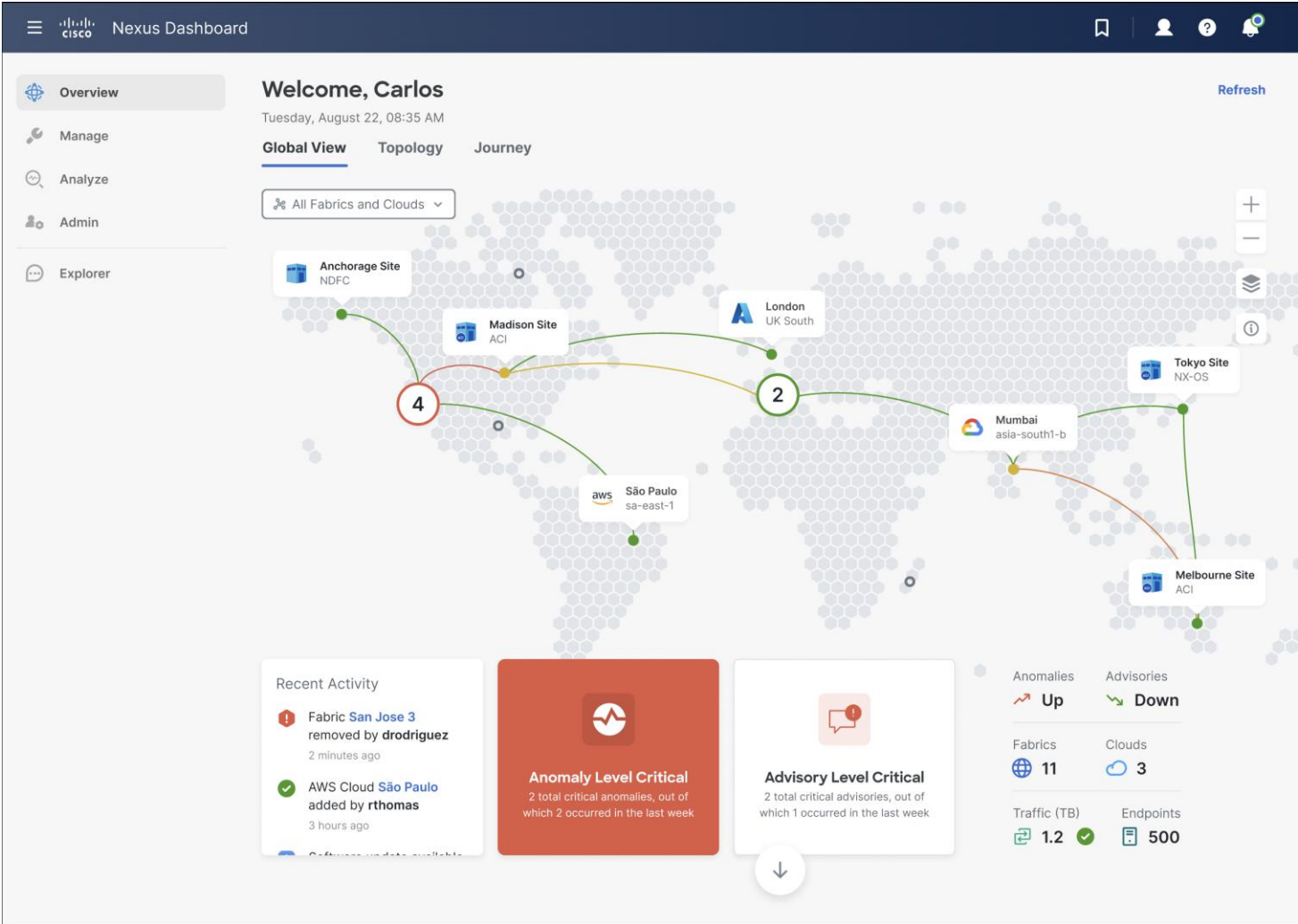


Unified Product

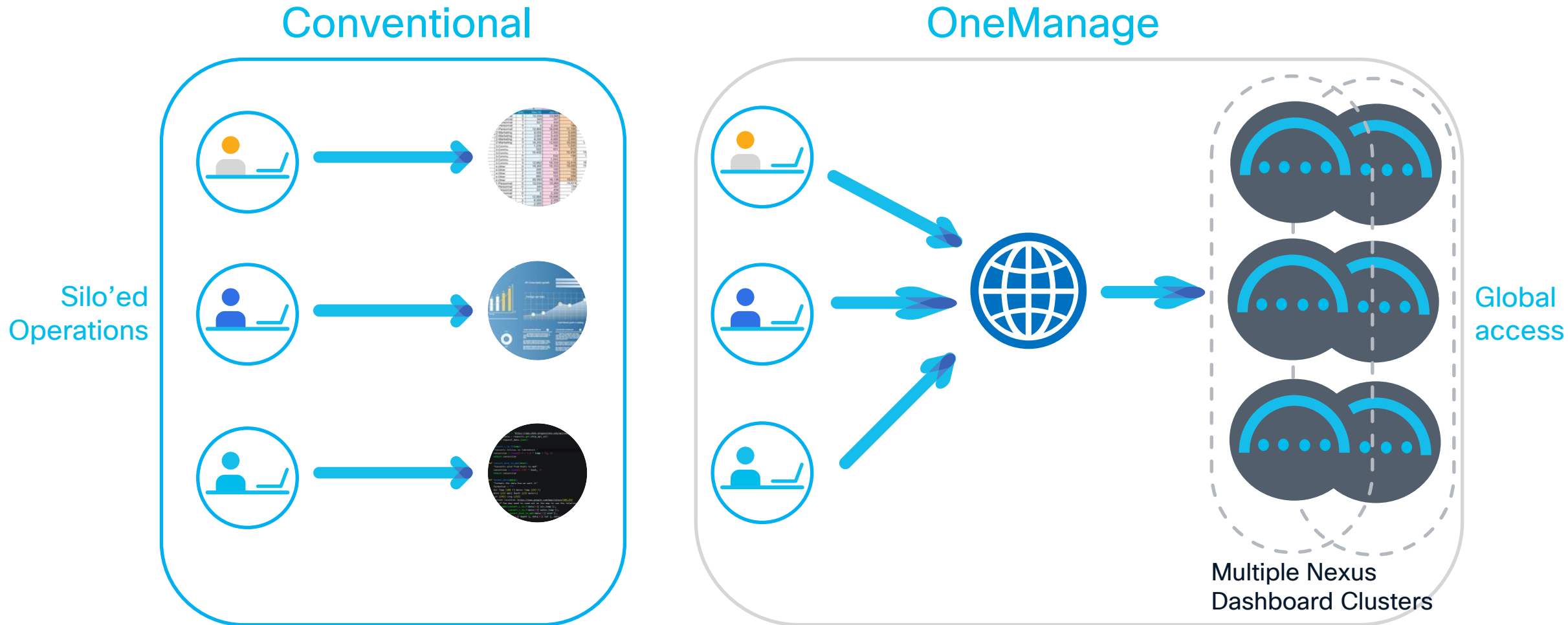
- Single Image Installation
- Services merged into base OS
- Services now == ND Capabilities
Automation Orchestration Telemetry

Which leads us here...

Unified Nexus Dashboard

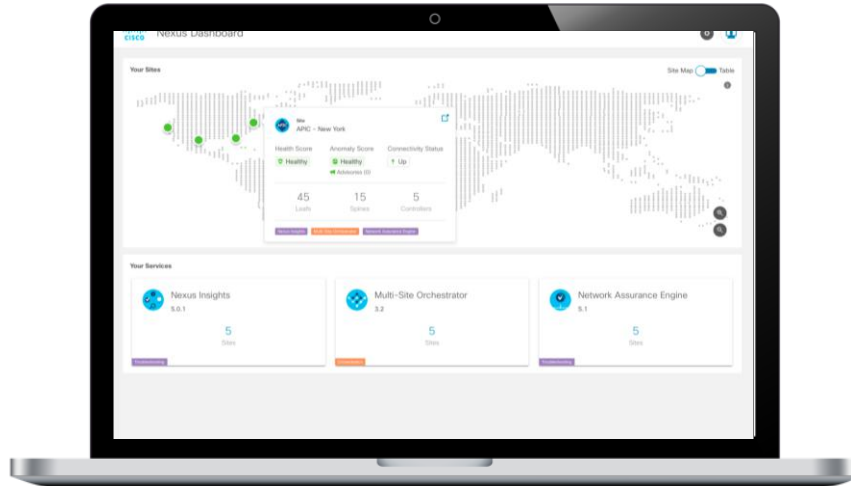


Nexus Dashboard: OneManage



Nexus Dashboard: A Unified Agile Platform

The operator view



Consume service(s) from single place

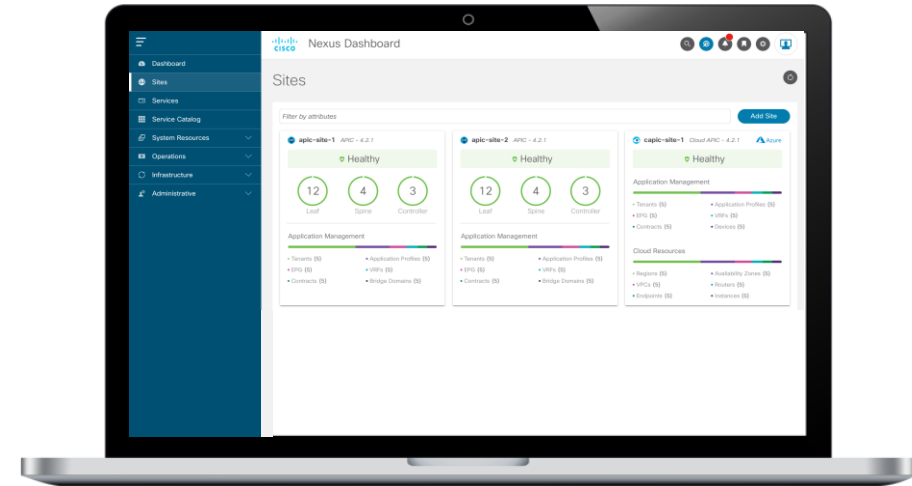


Frictionless navigation across multiple services and sites



Customise views and workflows

The admin view



Single dashboard for lifecycle management of services and Ops infra



Consistent one-time onboarding of domains and services



Consistent user management and access control

What is Nexus Dashboard?

- a view under the hood -**

Nexus Dashboard Node Roles

Each node in Nexus Dashboard Cluster can have either one of these roles:

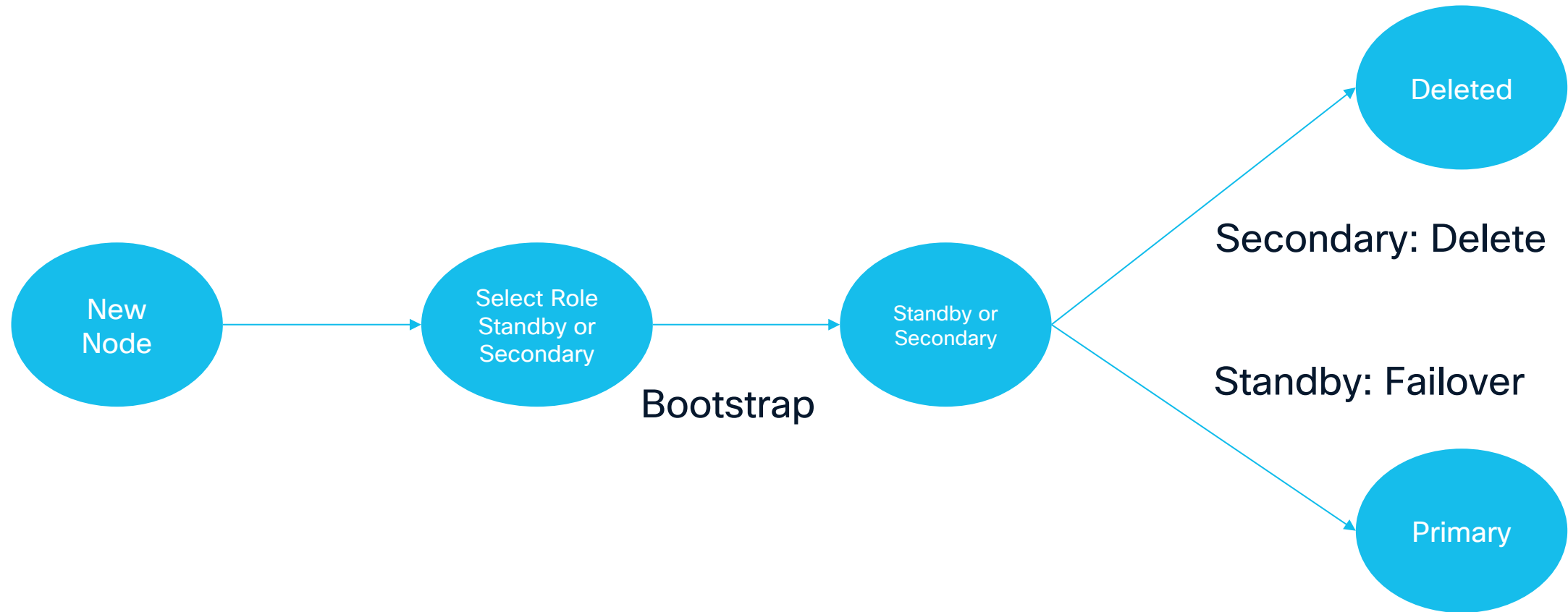
- Primary
 - Used to control the cluster and provide compute for workload
- Secondary
 - Used to add additional compute to cluster for workload
- Standby
 - Not actively participating in cluster, only to replaced failed Primary

Parts of Nexus Dashboard Cluster

- A Nexus Dashboard Cluster either consist out of
 - 3 Primary Nodes for full redundancy
- Or
- 1 Primary Node
- For redundancy reason you can add up to 2 Standby Nodes, which can replace a failed Primary Node
- For horizontal scale-out for workload, you can add up to 3 Secondary Nodes

Secondary and Standby Nodes are only supported with 3 Primary Node Cluster

Lifecycle of non-Primary Nodes



Nexus Dashboard Interfaces

Data Interface



Mgmt Interface

- Node clustering
 - Service to service communication
 - Communication to fabrics and controller
 - Telemetry traffic for switches and on-boarded fabrics
-
- Used for Mgmt/API Access to Cluster via CLI/GUI
 - Used for Syslog, AAA, Proxy, DNS communication

Nexus Dashboard Platform–Under the Hood



Nexus Dashboard



Functions



Shared Services



Infra Services



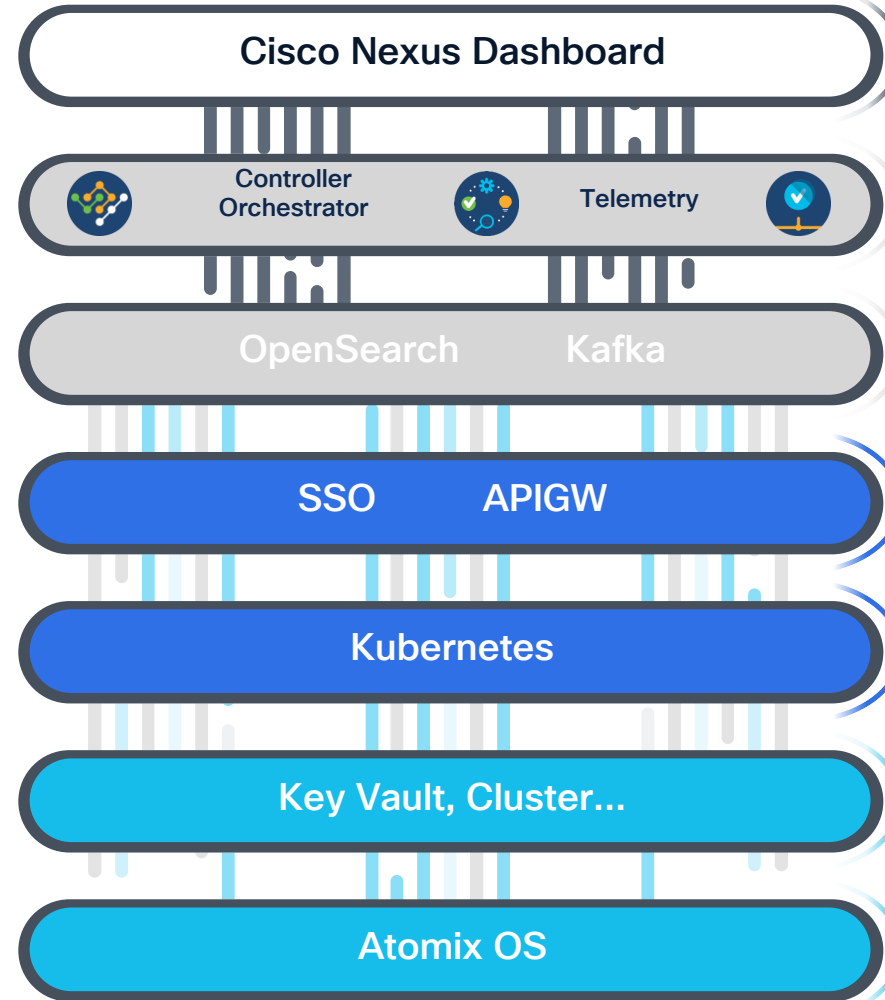
uService Lifecycle



System Services



Secure Container OS



Single Dashboard to view health



Single UI to consume app services



Proactive Notifications



Configuration compliancy



Realtime Telemetry Collection



Faster resolution through correlation



Frictionless access



Standardized service access

Industry standard container management



Secure cluster and app management



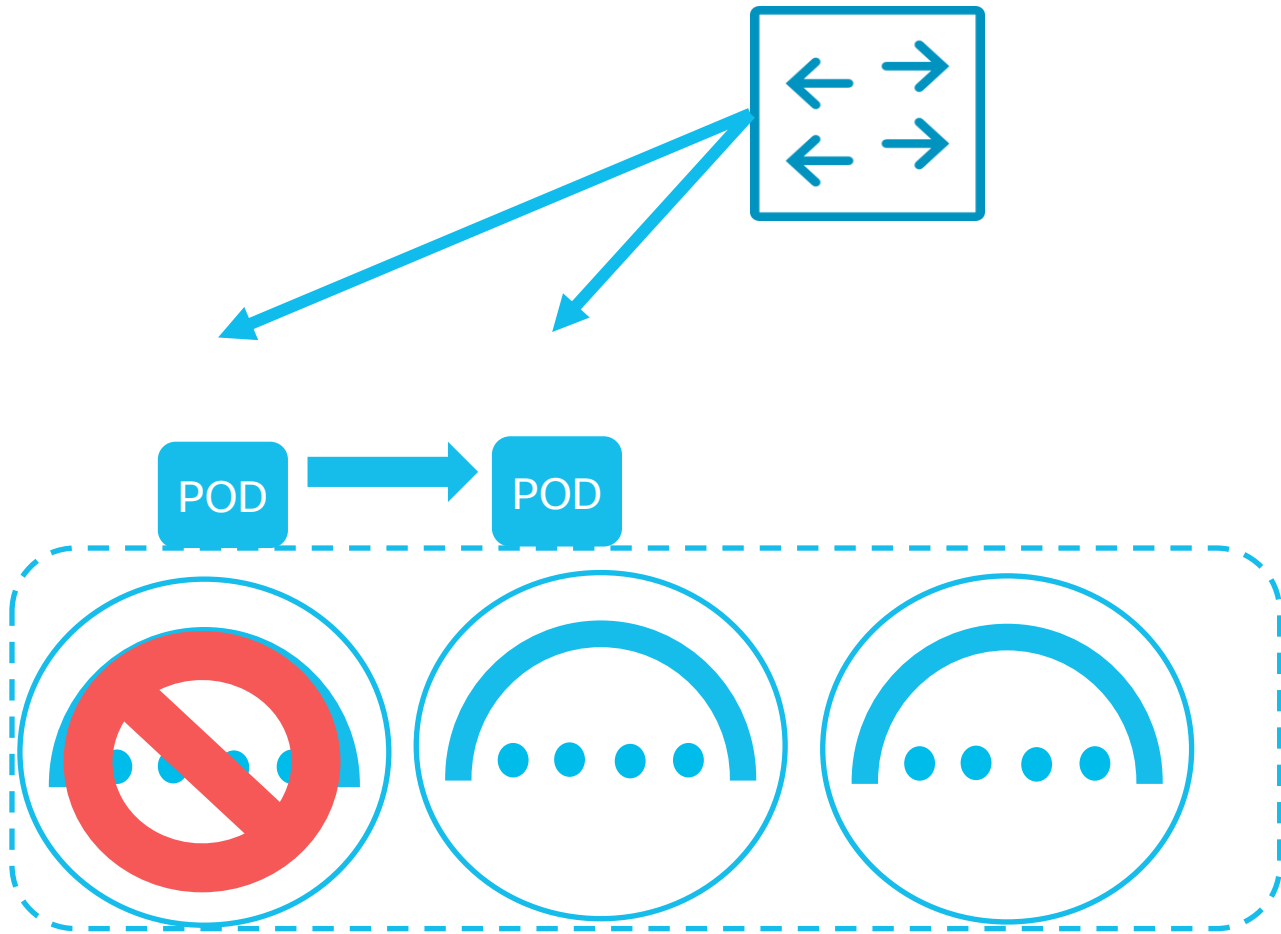
Infrastructure for secure K8 bringup



Hardened secure container OS

Persistent IPs and their usage

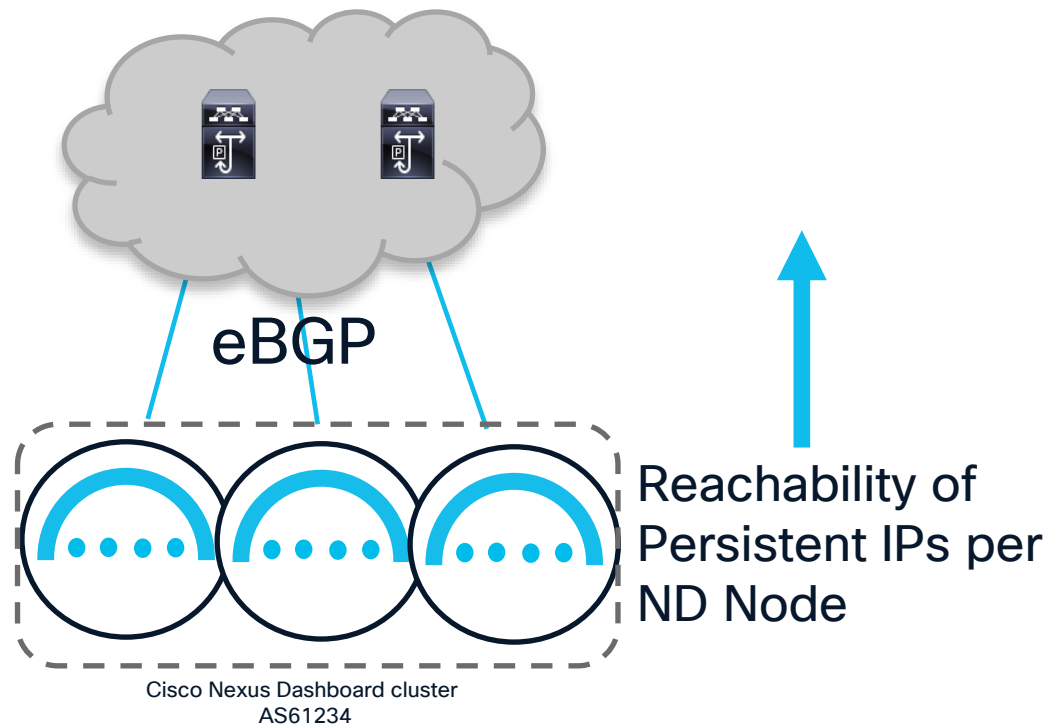
What are Persistent IPs?



ND L3 peering / L3 HA

- For use of persistent IPs, there are now 2 choices:
 - 1. L2
 - All ND data interfaces are in the same subnet/L2 Domain and Persistent IPs are out of the same Network
 - 2. L3
 - All ND data interfaces can be in different subnets and have a BGP peering towards the network. Persistent IPs must not be out of any of these subnets.
 - ND nodes will only update the external peer with persistent IPs and not learn any prefixes. The local routing table will still be honored
 - Only supported on ND Data Interface

eBGP Peering with Network



- Each ND node can be a separate AS or all in a single AS
- Multi-hop BGP peering is not supported
- Each ND node can peer to multiple Nodes (max 2) via IPv4 or IPv6
- Can be configured during bootstrap or added later
- Persistent IPs have to be out of an IP subnet not overlapping with any ND local IP.

Requirement for persistent IPs

If you use L2 HA mode:

Nexus Dashboard Cluster Nodes need to be Layer-2 Adjacent on Data Interface

- IPv4 requirements:
 - You need to assign 5 IPs, out of the range of the Data Interface Subnet, per Nexus Dashboard Cluster.
- IPv6 requirements:
 - You need to assign 5 IPs, out of the range of the Data Interface Subnet, per Nexus Dashboard Cluster.

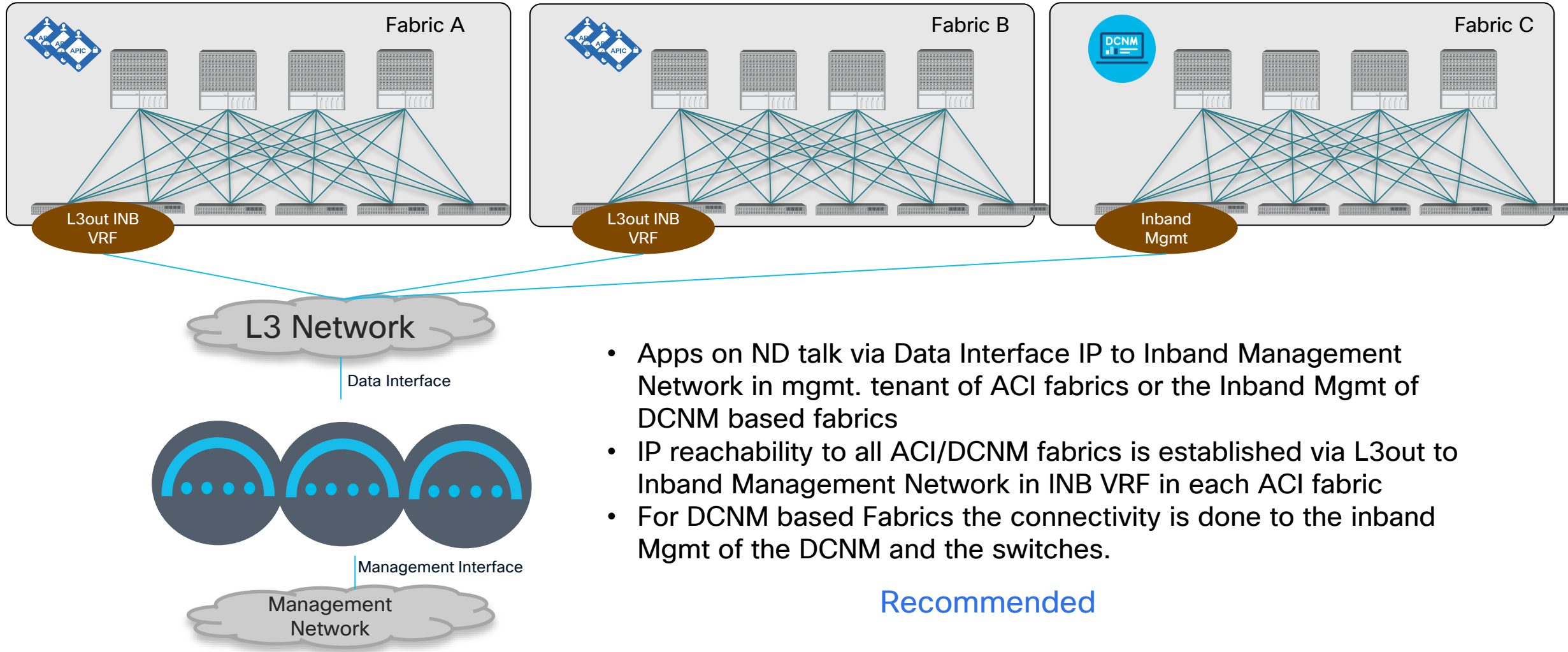
If you use L3 HA mode:

Nexus Dashboard Cluster Nodes need to be Layer-2 Adjacent on Data Interface

- IPv4 requirements:
 - You need to assign 5 IPs, out of the range of the Data Interface Subnet, per Nexus Dashboard Cluster.
- IPv6 requirements:
 - You need to assign 5 IPs, out of the range of the Data Interface Subnet, per Nexus Dashboard Cluster.

Attaching ND to your Network

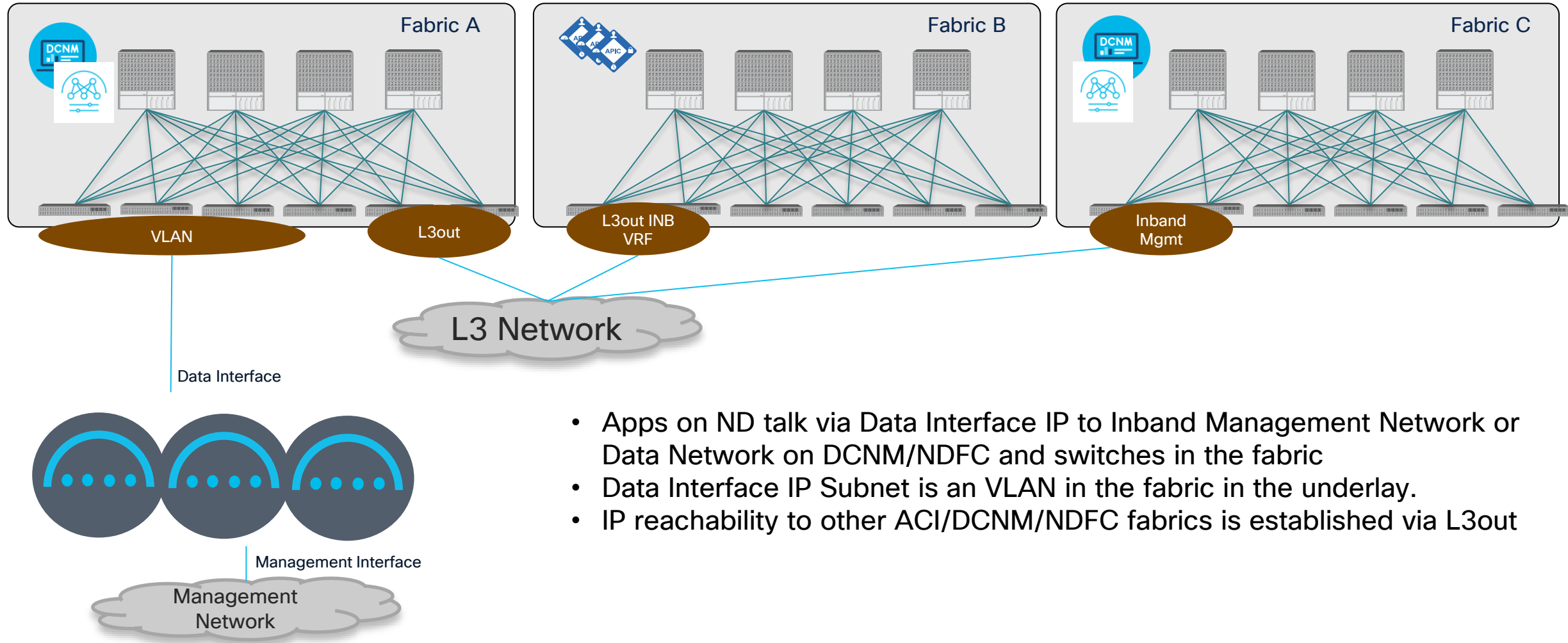
ND Cluster attached to any Networking Infra



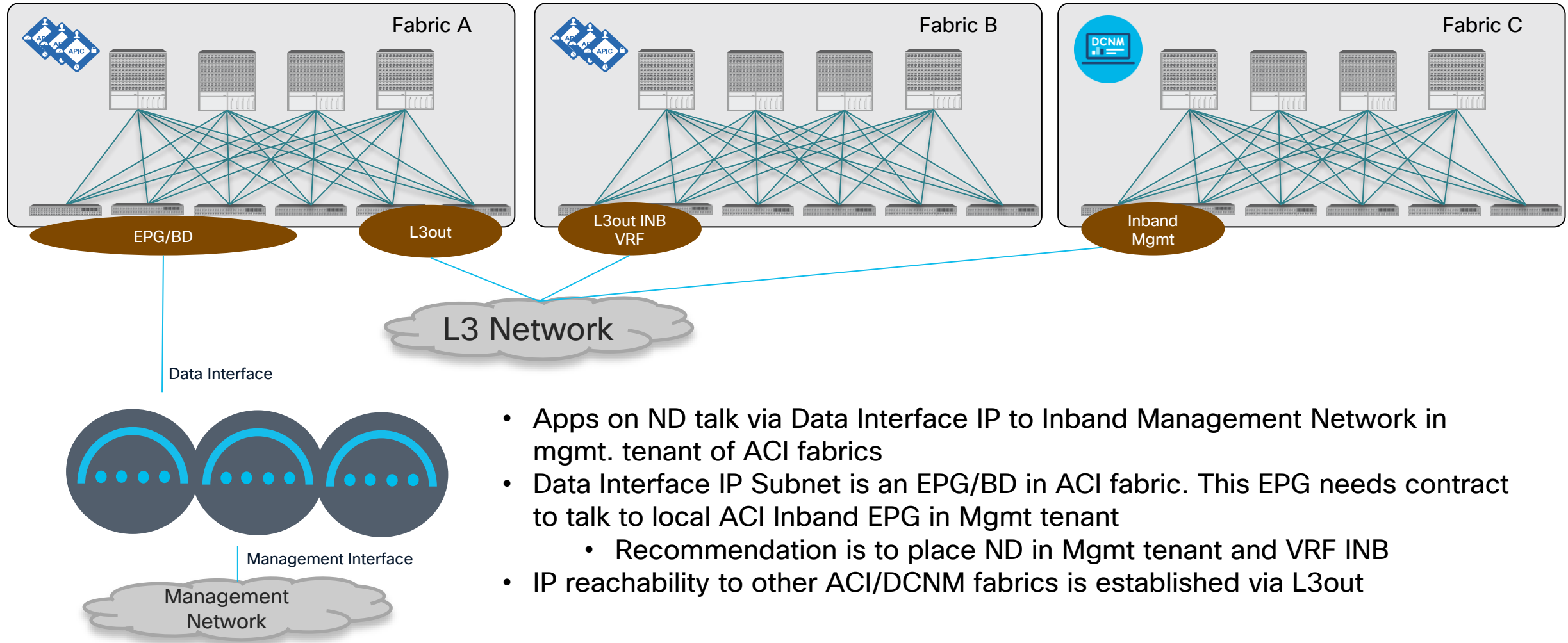
- Apps on ND talk via Data Interface IP to Inband Management Network in mgmt. tenant of ACI fabrics or the Inband Mgmt of DCNM based fabrics
- IP reachability to all ACI/DCNM fabrics is established via L3out to Inband Management Network in INB VRF in each ACI fabric
- For DCNM based Fabrics the connectivity is done to the inband Mgmt of the DCNM and the switches.

Recommended

ND Cluster attached to DCNM/NDFC based Fabric



ND Cluster attached to ACI Fabric



Pro/Contra of connecting to an ACI/NDFC/DCNM fabric

Pro	Contra
<ul style="list-style-type: none">- Easy connection between ND and Inband Management of ACI fabric or NXOS fabric	<ul style="list-style-type: none">- ND cluster is tied to a single fabric- Reachability to other sites/fabrics has to go via L3out- ND cluster relies on single ACI/NXOS fabric

Pro/Contra of connecting to any Networking Infra

Pro

- ND Cluster is not tied to any ACI/NXOS Fabric
- Same communication paths between all sites.

Contra

- All communications between ACI/NXOS fabric and ND need to go via L3out

Recommendations/Best Practice

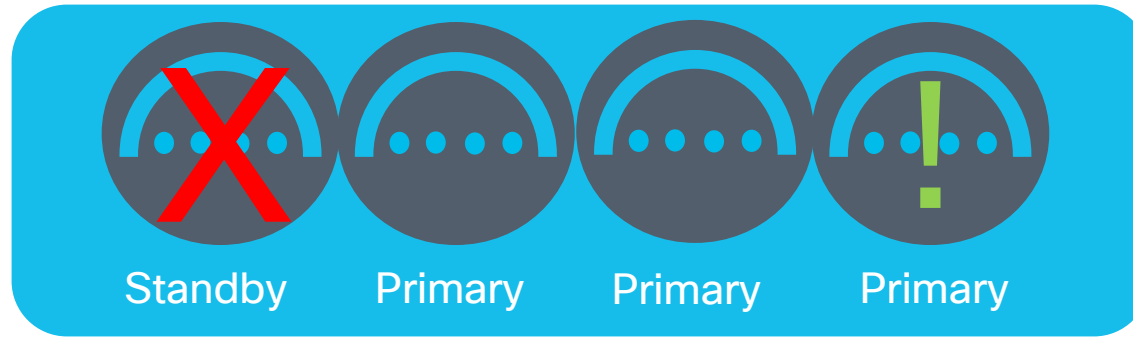
- Do not connect whenever possible to an ACI Fabric/NXOS based Fabric directly:
 - ND cluster is relying on correct functioning of the fabric, could be impacting during outages or maintenance
 - If you monitor multiple sites the ND cluster does not depend on a single site
- If a ND cluster is connected to a single fabric:
 - Fully supported/working BUT keep in mind
 - Issues in the fabric may impact the function of the ND cluster and the apps as they share fate.

DR/HA Considerations

HA/Redundancy with Stretched ND clusters

- 2 ND Primary nodes are always needed to keep the ND cluster operational. If you deploy a stretched cluster across more 3 sites, you SHOULD deploy a Standby Node in a quorum site.
- In case of a failure of 2 ND primary nodes, you have to re-install the ND cluster.
- For distributed cluster in the case of telemetry keep in mind that there is a lot of traffic flowing between ND nodes for the distribute computing.

DR and HA, Failure Scenarios



1. Primary Node fails
2. Standby Node is promoted to Primary
3. Failed Primary Node is coming back or is replaced
4. Node is re-installed as Standby Node

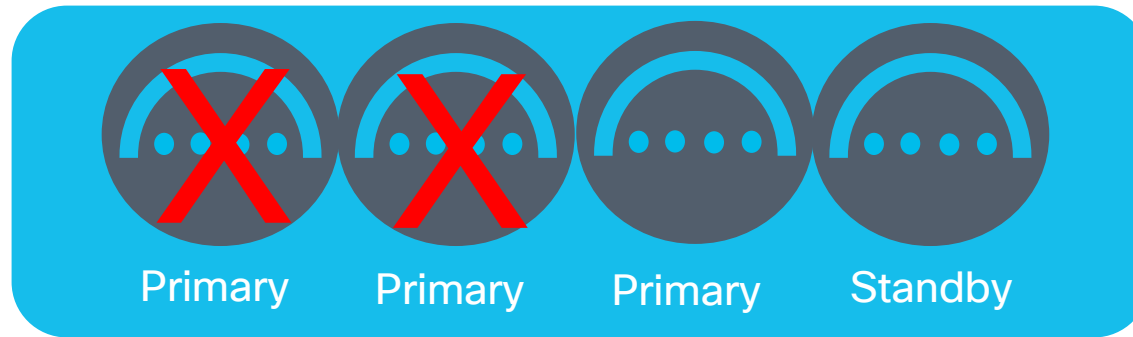
DR and HA, DR Recovery



In case of productive ND cluster in Site 1 goes down (DR Case):

1. ND cluster on DR site is brought up (either physical ND or virtual ND, needs to match same scale)
2. Latest Backup is applied
3. Sites need to be synchronized

DR and HA, Failure Scenarios



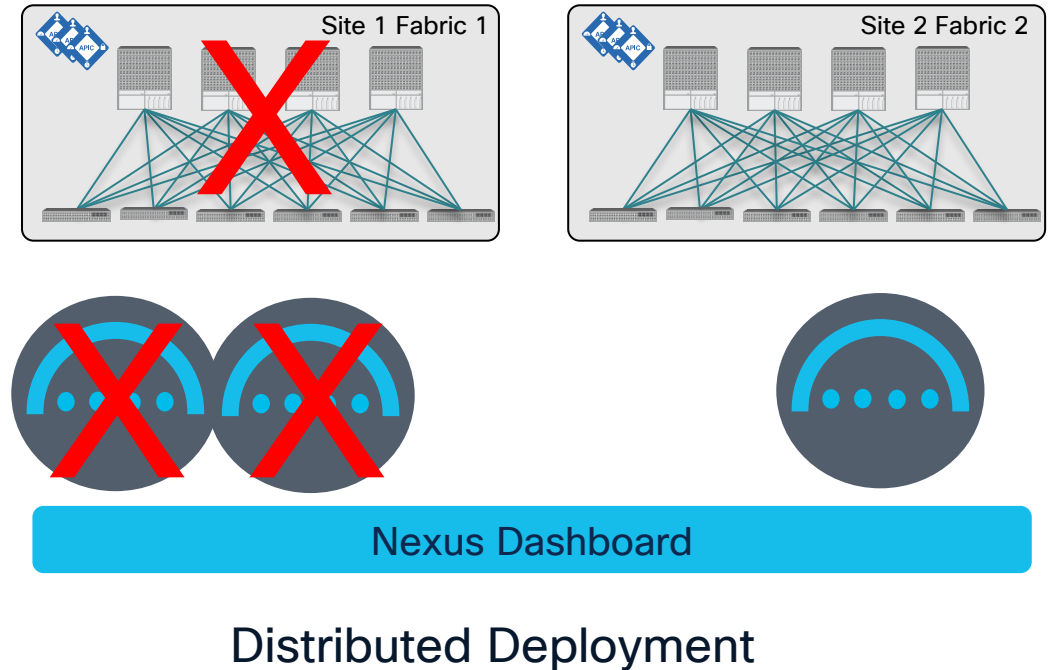
1. 2 Primary Nodes fail
2. Cluster becomes non-operational
3. Standby can't be promoted to Primary
4. Cluster needs to be re-deployed and a backup needs to be restored

Centralized vs Distributed Deployment

Distributing my Nodes across multiple Sites will increase my resiliency!

Keep in Mind!!!

- DR event in a Site will also bring down the cluster
- Issue within the interconnect network of ND nodes will impact the cluster operations

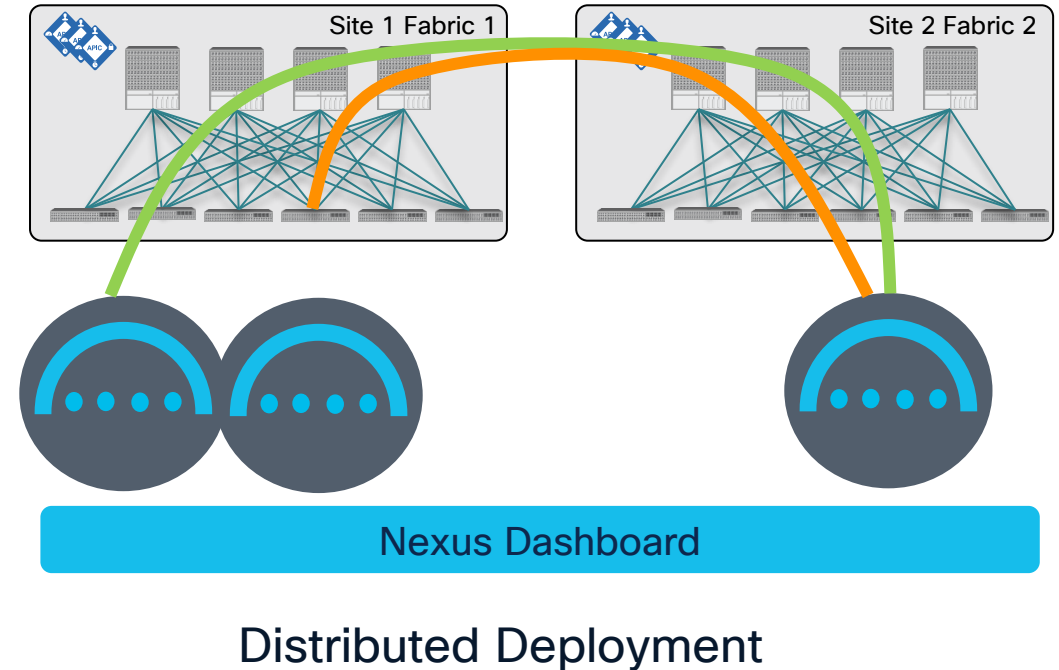


Centralized vs Distributed Deployment

Distributing my Nodes across multiple Sites will improve my performance!

Keep in Mind!!!

- ND to ND latency will impact performance
- ND to ND traffic will consume bandwidth (more than Network to ND)
- Network to ND traffic is not localized



Deployment Options for ND

Definition Terms and Assumptions/Requirements

- [Site](#): Geographical datacenter location with 1 or more fabrics
- RTT requirements for:
 - ND: between ND nodes in the same cluster <50ms
 - ND: between ND nodes in different clusters <500ms
 - ND: to switches <150ms
- Reachability between Nexus Dashboard nodes
 - Layer 2 Adjacency (same subnet)
 - Layer 3 Adjacency (different subnets)
 - Requires BGP support on upstream router
 - 1500 bytes MTU on the ports, 1504 if ND is configured with trunk interfaces

Deployment Requirements

- Customer has more than 1 Site
 - Number of ND clusters is driven by number of switches and combination of functions
 - Please check the sizing calculator for ND scale on CCO
 - <https://www.cisco.com/c/dam/en/us/td/docs/dcn/tools/nd-sizing/index.html>

Some Deployment Considerations 1/2

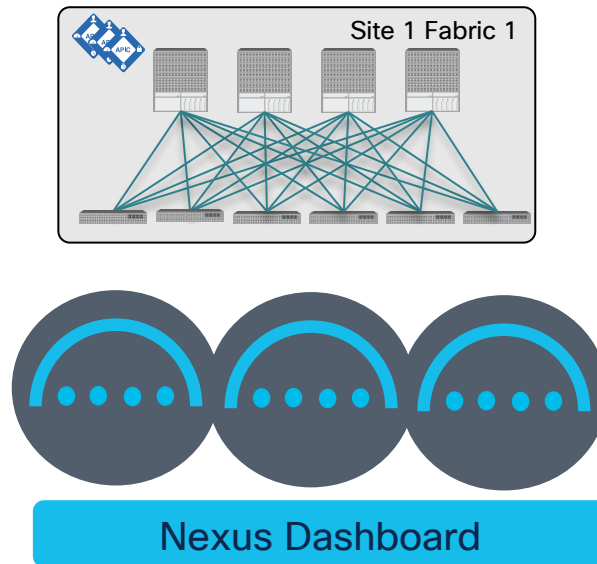
- Try to keep the potential points of failure for reachability between the ND nodes as low as possible.
- When distributing a ND cluster
 - ND Data and Mgmt interface of ND nodes can be in different subnets. Only IP connectivity is needed. (Please allow ports listed in documentation)! This requires L3 HA!
 - Keep traffic between ND nodes in mind, especially if Telemetry is used.

Some Deployment Considerations 2/2

- In MPOD, ACI is taking care of the reachability, Keep in mind loosing IPN connectivity will e.g. break NDI
- In MSITE communication can not happen via ISN. It has to go via L3OUT in each site. Telemetry is sent via INB EPG in Mgmt Tenant, this is not managed by Orchestrator!
- Data Interface IPs, have to be different from INB EPG subnet of ACI, when ND cluster is connected to ACI fabric
- All communication of functions on ND towards the fabrics is initiated via Data Interface IPs

Option 1: 1 Site/Fabric (below 500 nodes)

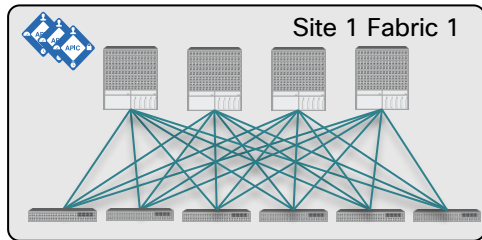
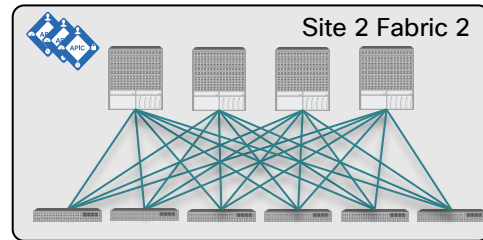
- Single cluster (x number of nodes, cluster connected to either ACI fabric or legacy infra with IP reachability)



Option 2: 1+ Site (below 500 nodes)

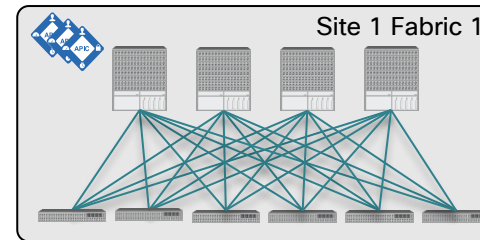
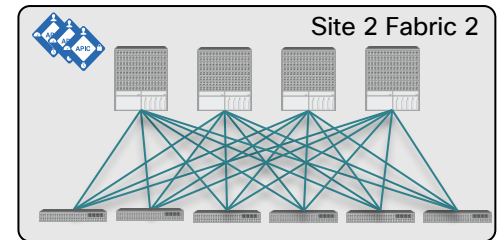
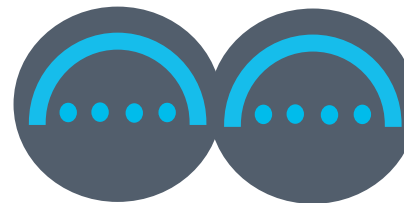
- Single cluster (x number of nodes, cluster connected to either ACI fabric or legacy infra with IP reachability, Cluster can be stretched or local to a site)

Recommended



Nexus Dashboard

Central deployment

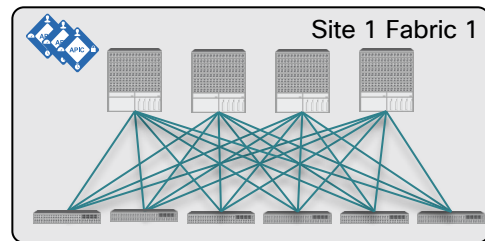
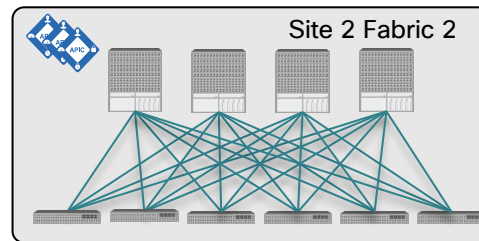


Nexus Dashboard

Distributed Deployment

Option 3a: 1+ Site (below 500 nodes)

- Single ND cluster for NDI (x number of nodes, cluster connected to either ACI fabric or legacy infra with IP reachability)
- Single additional virtual ND cluster for Orchestrator to meet HA/DR requirements



Recommended



ND Cluster #1
Telemetry



ND Cluster #2
Orchestrator



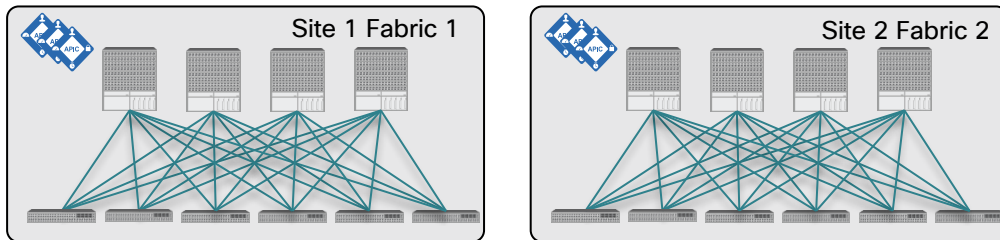
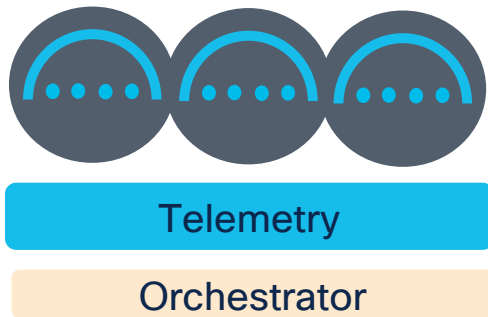
ND Cluster #3
Orchestrator

Standby cluster

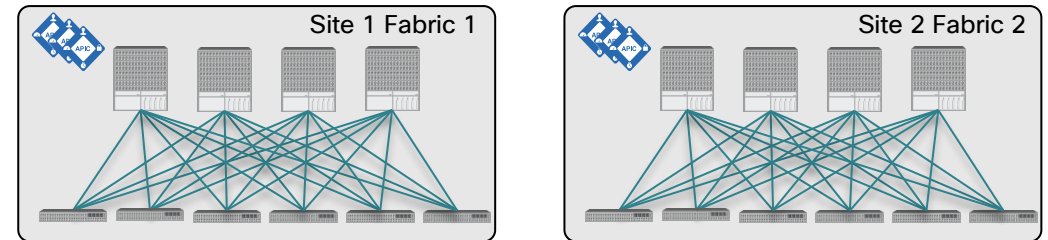
Option 3b: 1+ Site (below 500 nodes) NDI and NDO

- Single ND cluster (x number of nodes, cluster connected to either ACI fabric or legacy infra with IP reachability)

Not recommended as Orchestrator is not distributed

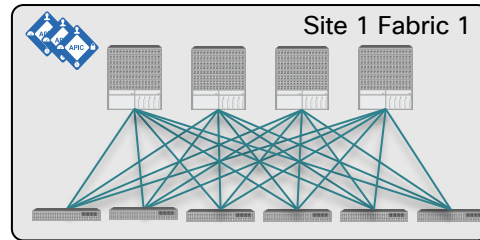
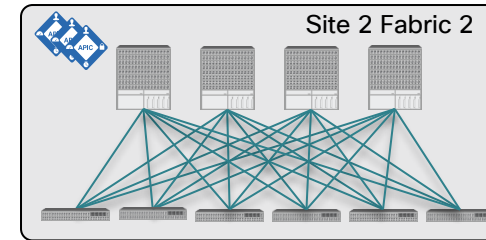


Not recommended



Option 4: 1+ Site (above 500 nodes)

- Multiple ND cluster (x number of nodes, cluster connected to either ACI fabric or legacy infra with IP reachability) and connected via Federation



Recommended



Operating Nexus Dashboard

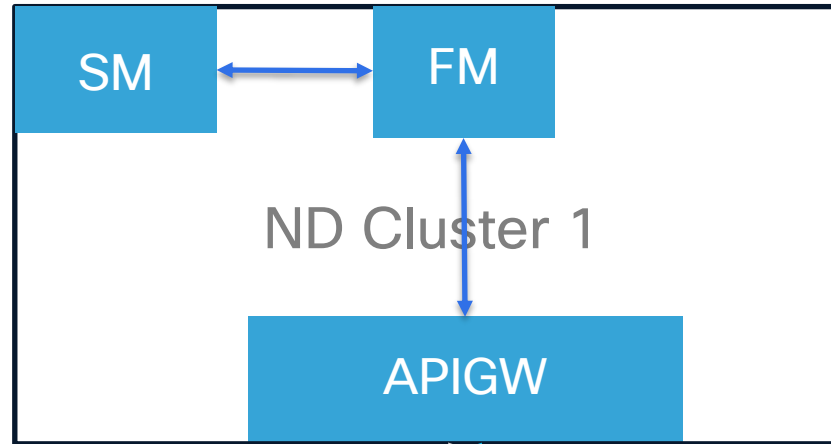
OneManage aka as ND Federation

Overview

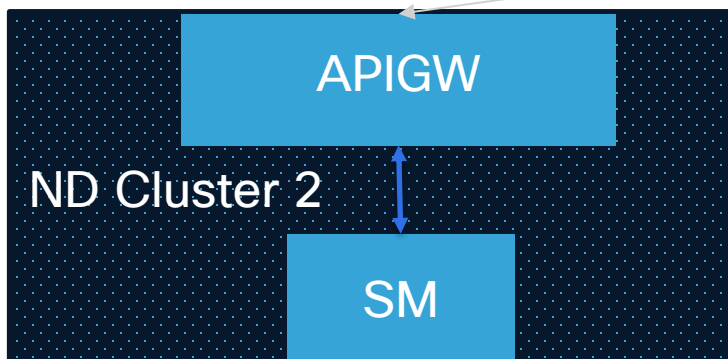
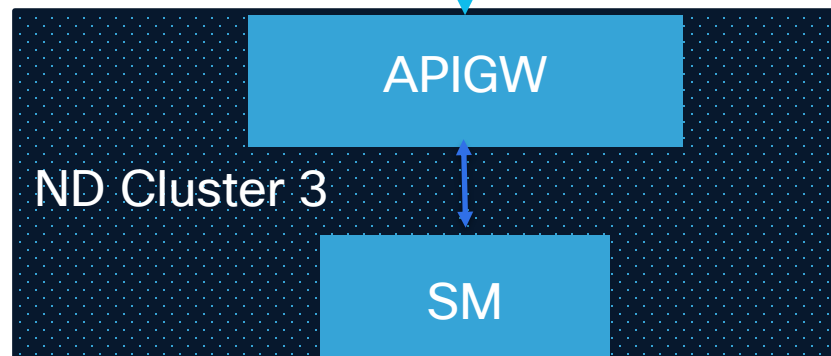
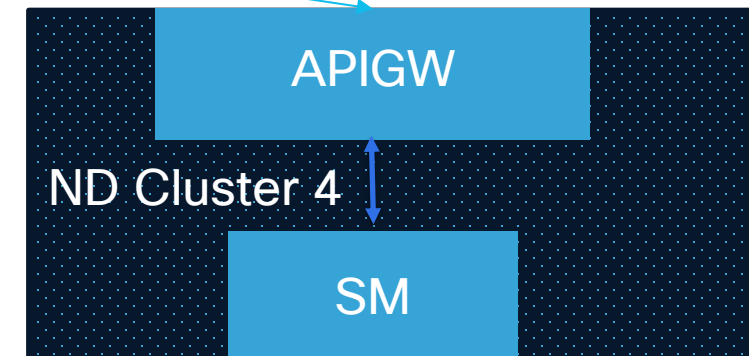
- ND OneManage is an association of several ND clusters that allows working across with them as if they were a single entity and simplify the consumption of their resources
- ND clusters onboard other ND clusters creating a trusted environment which allows to learn about those clusters and to communicate and share information with each other
- Information shared between clusters is visible on each cluster being part of that federation. Also this data is accessible from each cluster.
- Remote User is required to setup and use ND Federation

OneManage Architecture

- User configures an ND cluster as Federation manager (FM) and connects it to other ND clusters
- FM manages the federation keeping track of member cluster reachability, node status, sites. etc.



- FM uses Site Managers (SM) on all ND clusters to replicate this information for local queries/display
- APIGW is used to sync keys (for accessing data) between federation members



Onboard Clusters (OneManage Configuration)

Nexus Dashboard

vND

Home

Manage

Analyze

Admin

System Settings

General

Fabric management

Multi-cluster connectivity

Flow collection

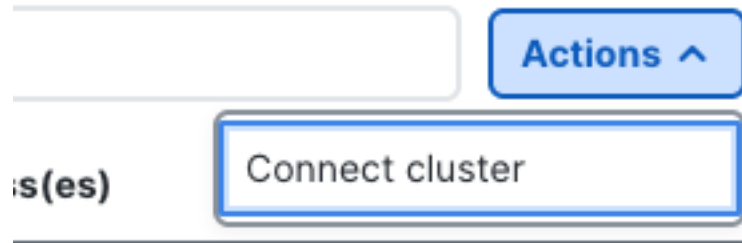
Create a single point of management by connecting multiple Nexus Dashboard and/or ACI Clusters together.

Filter by attributes

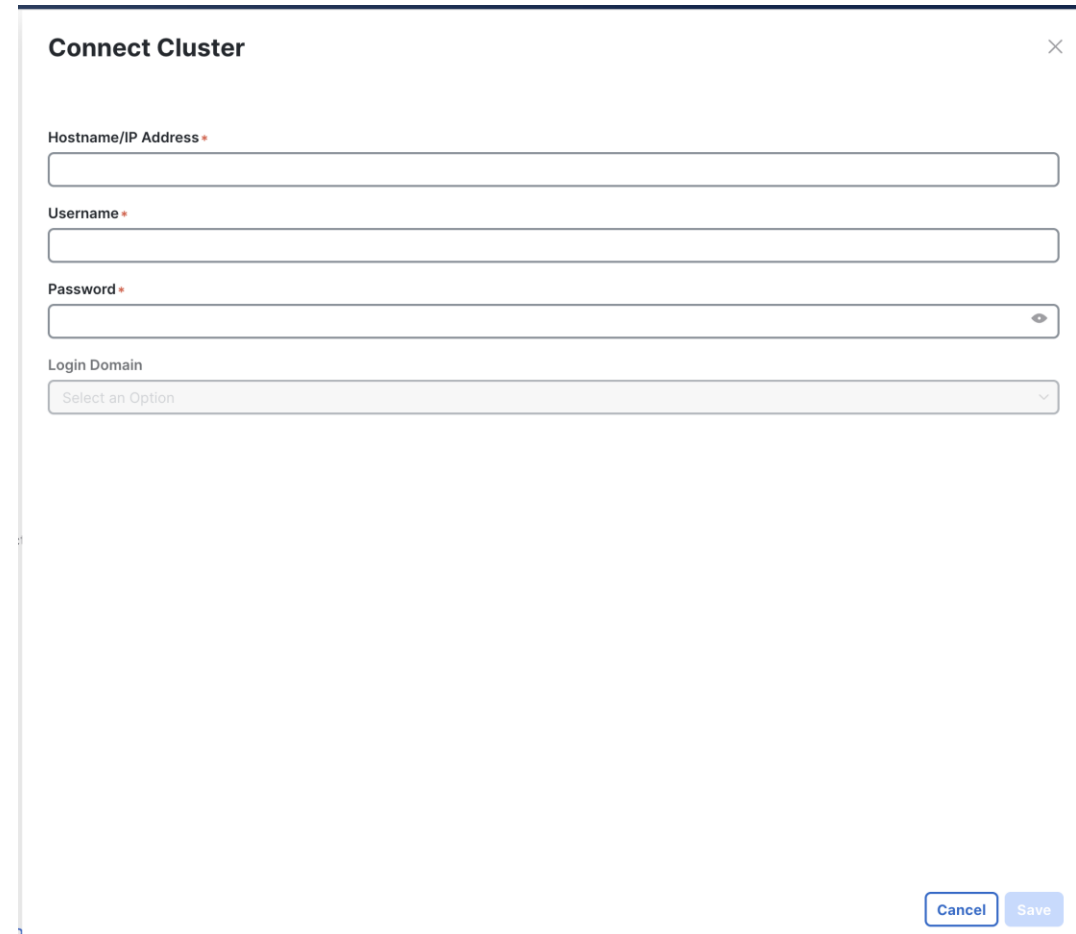
Name	Connectivity status	Version
☐ ACI-Site1	 Up	6.1(1f)
☐ ACIPreProd	 Up	6.1(1f)
<div>vND</div> <div>☐ <div>Primary</div><div>Local</div></div>	 Up	4.1.0.122
☐ vNDO	 Up	4.1.0.122

Onboard Clusters (OneManage Configuration)

- Complete the target cluster information (IP of Mgmt Interface of remote cluster)
- Click save



A partial view of a table interface. The table has a header row with a text input field and a blue button labeled "Actions ^". Below the header, a row contains the text "s(es)" and a button labeled "Connect cluster", which is highlighted with a blue border.



A screenshot of a "Connect Cluster" dialog box. The dialog has a title bar with a close button (X). It contains four input fields: "Hostname/IP Address", "Username", "Password" (with a toggle icon), and "Login Domain" (a dropdown menu with "Select an Option" selected). At the bottom right, there are "Cancel" and "Save" buttons.

← System Settings

Connect Cluster

1 Select type

2 Settings

3 Summary

Select type



Nexus Dashboard

Unified platform to transform data-ce



ACI

Centralized controller for automation

Viewing Connected Clusters' Information

- After connecting a cluster, it will show up on the Multi Cluster Connectivity table
- User would be able to connect more clusters or disconnect clusters from the table
- The cluster name on the header bar becomes a link to select a specific cluster
- Central Dashboard is added to the header bar
- Local cluster and Federation Manager are marked in the list (no extra cluster needed for this)

Central Dashboards

All Clusters

Home

Manage

Admin

Welcome, tme

Overview

Topology

All Clusters at a glance

Anomaly level

1 N/A

No anomalies found

Critical 7

Major 25

Minor 0

Warning 19

Advisory level

No advisories found

All Clusters

Home

Manage

Admin

System Status

Overview

Nodes

Nodes by status

Active 2

Filter by attributes

Name	Cluster	Serial
<div><div></div><div>vNDO</div></div>	vNDO	93B2E8F43CB7
<div><div></div><div>vND</div></div>	vND	E4A61BC4DF7F

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

BRKDCN-2914

Registering Nodes to existing Cluster and Standby Node

Register new Nodes and Standby

- New nodes are discovered via CIMC (reachability from MGMT Network is required) and bootstrapped
- During registration Role is selected (Secondary or Standby)
- Secondary Node is for horizontal Scaling
- Standby Node is increasing HA as it can replace a failed Primary
- Difference between Replace and Standby is, that Replace is a RMA workflow where the new node is installed and brought up. Standby is replacing a failed master with an already bootstrapped node
- Secondaries can only be replaced by delete and re-add

Adding a new Node

Add node×

Deployment details

CIMC IP Address *

Username *

Password *

Show

Validate

General

Name *

Serial number *

Type *

Secondary

1. Provide CIMC details to discover node
2. Fill in node details
3. Node is bootstrapped and registered
4. Node status will change from “unregistered” to “discovering” to “active”

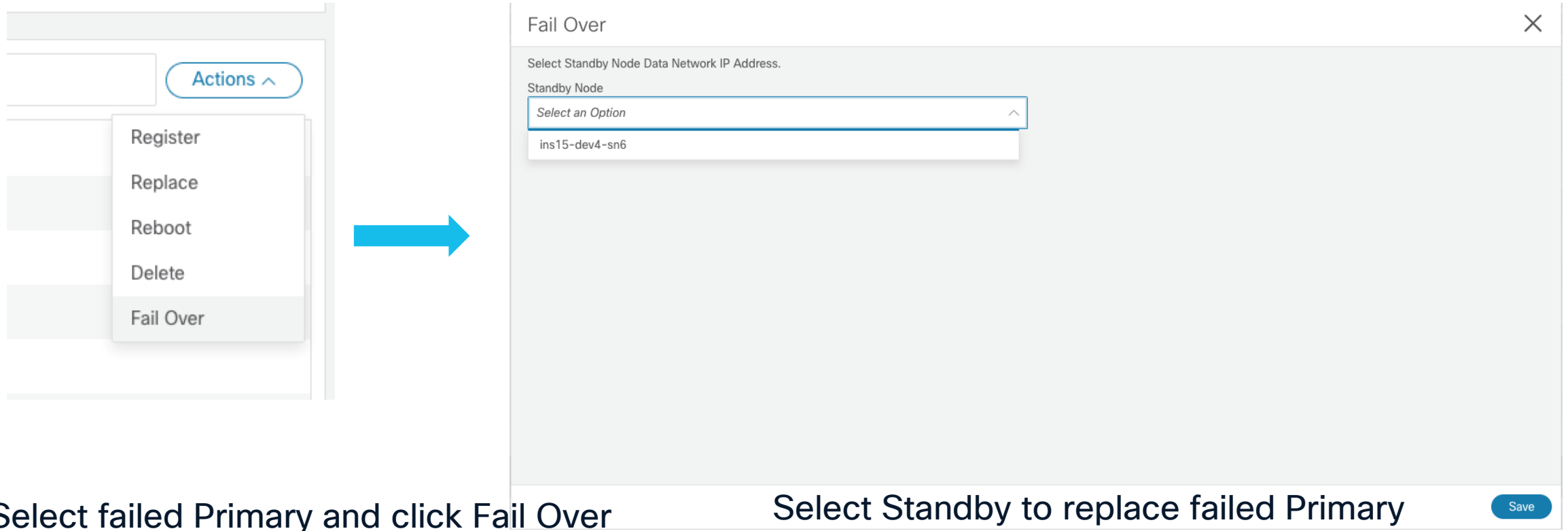
Replace a failed Primary with Standby Node

Primary is failed

Name	Serial	Data network address (IPv4)	Management network address (IPv4)	Data network address (IPv6)	Management network address (IPv6)	Status	Role	
ND4	WMP2512014R	192.168.6.175/24	10.49.153.175/24	-	-	Active	Primary	...
ND6	WZP2728084E	192.168.6.135/24	10.49.153.135/24	-	-	Active	Primary	...
ND7	WZP27280849	192.168.6.136/24	10.49.153.136/24	-	-	Inactive	Primary	...
vND	E4A61BC4DF7F	192.168.0.30/24	10.48.169.107/24	-	-	Active	Standby	

Standby Node is part of Cluster

Failover to Standby



The diagram illustrates the failover process in two steps. On the left, a list of actions (Register, Replace, Reboot, Delete, Fail Over) is shown, with 'Fail Over' selected. A blue arrow points to the right, where a 'Fail Over' dialog box is displayed. The dialog box contains a dropdown menu for 'Standby Node' with the option 'ins15-dev4-sn6' selected. Below the dialog box, the text 'Select Standby to replace failed Primary' is visible, followed by a 'Save' button.

Actions ^

- Register
- Replace
- Reboot
- Delete
- Fail Over

Fail Over

Select Standby Node Data Network IP Address.

Standby Node

Select an Option ^

ins15-dev4-sn6

Select failed Primary and click Fail Over

Select Standby to replace failed Primary

Save

If you receive a replacement for the failed node, you can register it as a Standby node

Recovery Process of a virtual ND

Recovery Process of a virtual ND

- Ensure that the failed node's VM is powered down.
- Ensure new VM is deployed and powered on.
- Use the Replace workflow for the inactive node.

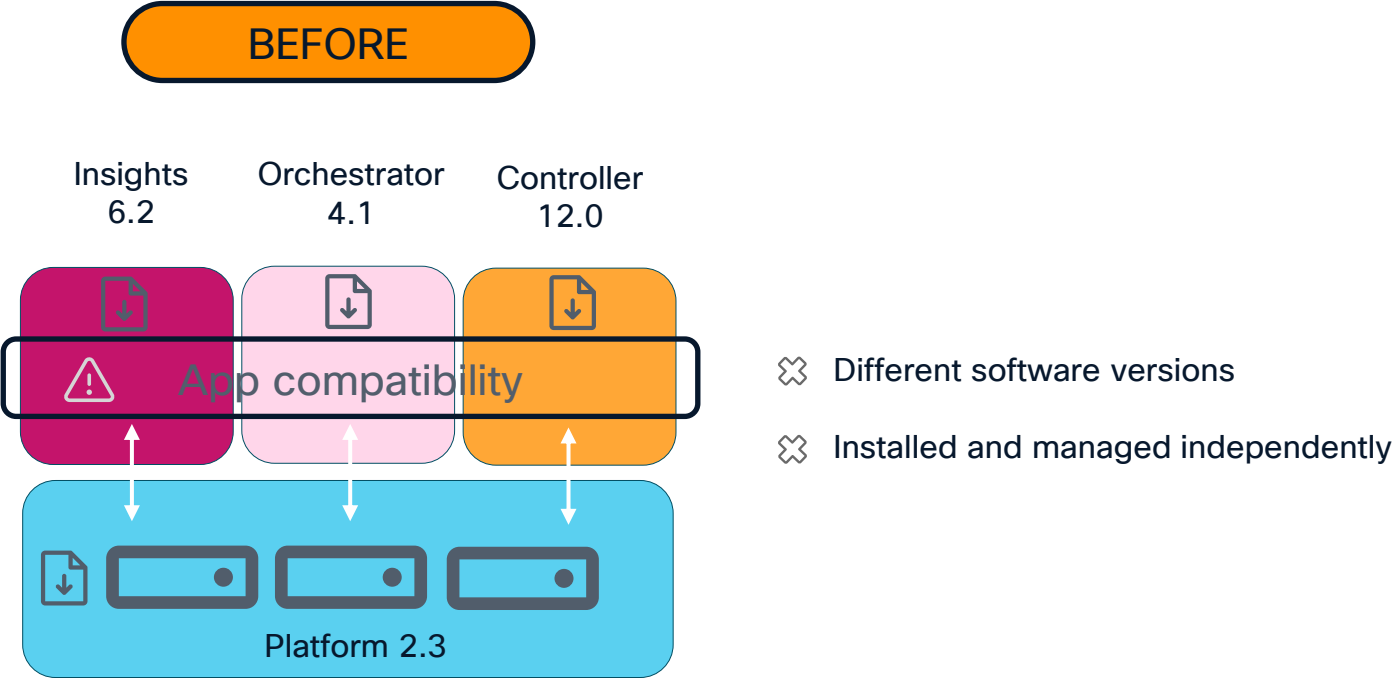
Firmware Upgrade

Unified Firmware Upgrade

- Single Image for all Services and Infrastructure
- Upgrade at Cluster Level, but a rolling upgrade per ND Node
- Verification is done before Upgrade

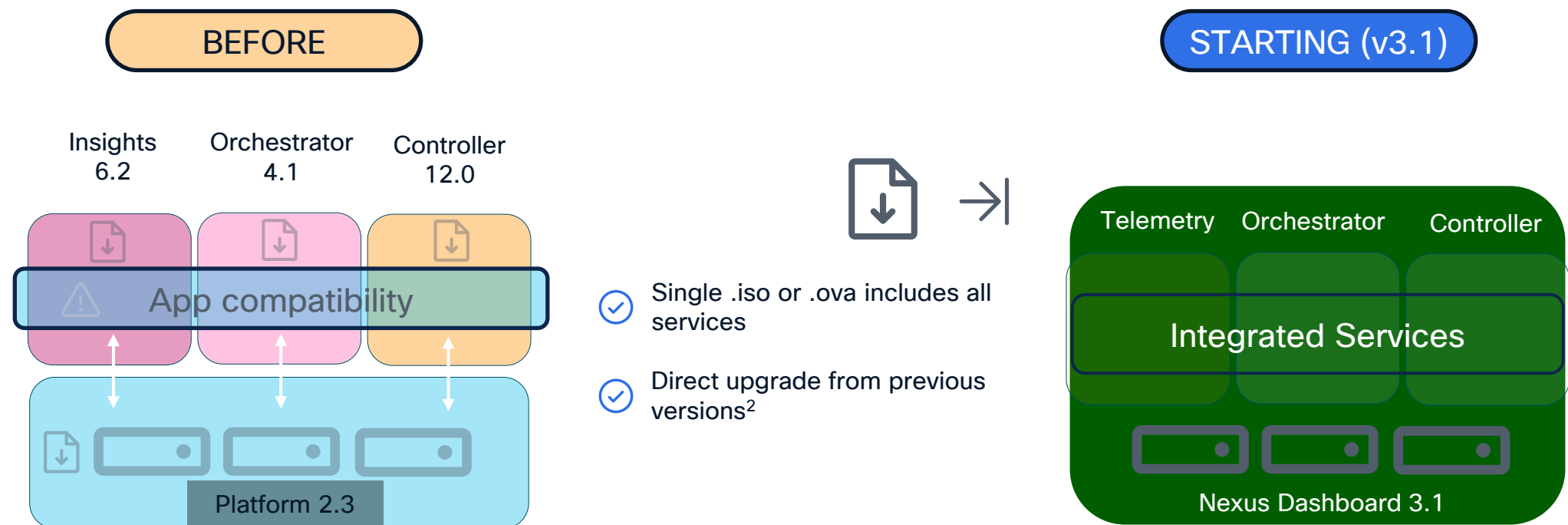
Nexus Dashboard

Unified Image



Nexus Dashboard

Unified Image



Firmware Upload

Cisco

Nexus Dashboard

ND-Denali

Admin

Nexus Dashboard Management

System Status

System Software

Nexus Dashboard Releases

4.0.1iRunning

[What's new?](#) [Release details](#)

Cluster Software

Current Software Version
4.0.1i

Nodes

Primary 3

Last Update
February 04, 2025, 09:10:33 PM
[View History and Logs](#)

Authentication and more

Users and Security

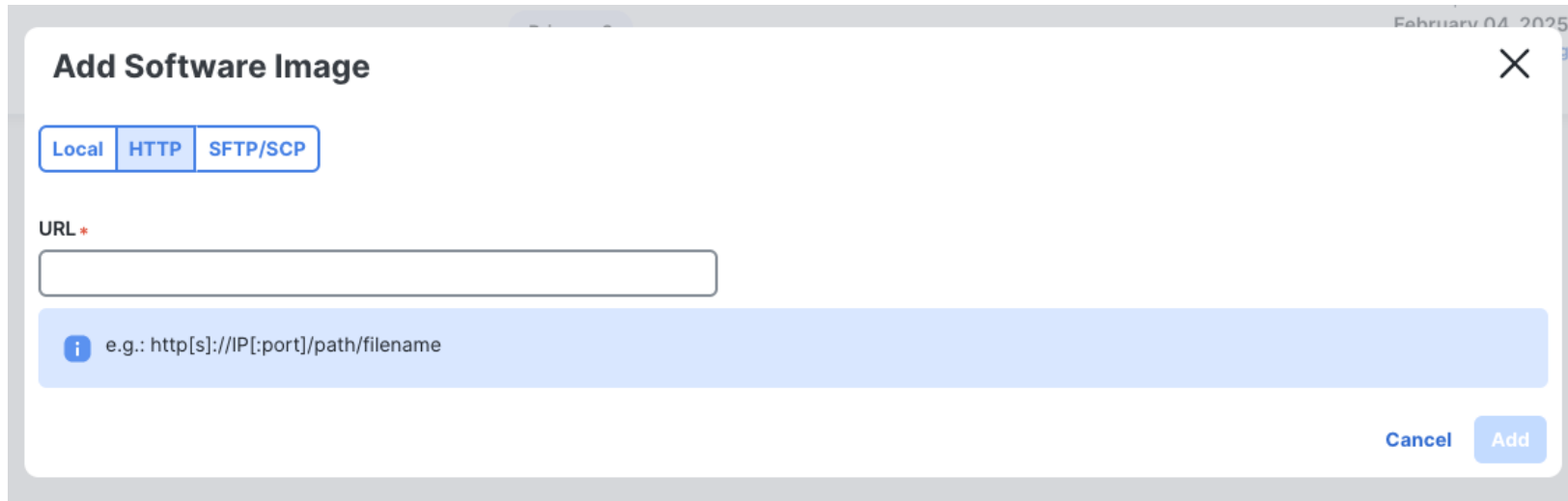
Certificate Management

Click in Images first to upload a firmware image

Add Image

Firmware Upload

- 3 Options supported either via remote (WEB server/SCP) or local
- Remote upload is recommended



The screenshot shows a dialog box titled "Add Software Image" with a close button (X) in the top right corner. Below the title, there are three tabs: "Local", "HTTP", and "SFTP/SCP". The "HTTP" tab is currently selected. Under the tabs, there is a label "URL *" followed by an empty text input field. Below the input field, there is a light blue informational banner with an information icon (i) and the text "e.g.: http[s]://IP[:port]/path/filename". At the bottom right of the dialog, there are two buttons: "Cancel" and "Add".

Select Firmware

Firmware Update

⚙️ Setup

⬇️ Install

⌚ Activate

⌚ Complete

1

2

Version Selection

Confirmation

Pick a firmware version for this update.

Available Target Firmware Versions *

Service Node

1.1.2.152

Previous

Next

Current Cluster Setup is validated

Firmware Update

Setup

Validate

Install

Activate

Complete

This is to validate the firmware and examine the current cluster state before installing the firmware. Once the validation passes the update will be 'Ready to Install'.

Update Details

Overall Status

Running

Current Firmware Version

2.2.2d

Target Firmware Version

2.3.0.85

Last Update

2022-09-07, 14:41:59

Image Preparation

✓

Loading target image information

▼

Cluster Networking

✓

Verifying reachability to other cluster nodes

▼

Platform Services' Health

✓

Verifying critical services' status

▼

Kubernetes Health

✓

Checking K8s cluster reachability

▼

Nodes' Health

✓

Verifying nodes' states

▼

Disk Utilization

✓

Verifying nodes' disk utilization

▼

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

BRKDCN-2914



Install Firmware to Nodes

Firmware Update

Setup

Install

Activate

Complete

1

2

Version Selection

Confirmation

Please confirm the configuration information below. Once install begins, all nodes will begin to download firmware image immediately. After the installation process is complete, you can start activation of downloaded image!

Update Detail

Current Firmware Version

2.0.0.71a

Target Firmware Version

2.0.0.71b

Number Of Nodes

3

Last Update

2020-10-02, 14:40:19

Nodes

Serial Number	Node	Type	Status	Last Update
WZP23340A7P	ND2	Master	Active	2020-10-02, 14:40:19
WZP23340A7Q	ND3	Master	Active	2020-10-02, 14:39:37
WZP23340A7X	ND1	Master	Active	2020-10-02, 14:40:20

10

Rows

Page 1 of 1

1-3 of 3

Previous

Begin Install

Installing Firmware to Nodes

Firmware Update

⚙ Setup

⬇ Install

⌛ Activate

✅ Complete

This update is in the 'Pre-Installing' stage of the update process. Once the firmware has pre-installed to each node, the update will be 'Ready to Install'.

Update Status

Overall Status

🟢 Running

Status Breakdown

3

Total

Running

Update Details

Current Firmware Version

1.1.2.144

Target Firmware Version

1.1.2.152

Number Of Nodes

3

Total

Master

Last Update

2020-04-30, 12:30:56

Nodes

Node	Status	Last Install
192.168.6.172	🟢 Running	2020-04-30, 19:31:33
192.168.6.173	🟢 Running	2020-04-30, 19:31:33
192.168.6.174	🟢 Install: Running	2020-04-30, 19:31:30

Start Over

Activate

Once Install is done Click Activate

Firmware Update

⚙ Setup

↓ Install

⌂ Activate

⌂ Complete

This update is in the 'Pre-Installing' stage of the update process. Once the firmware has pre-installed to each node, the update will be 'Ready to Activate'.

Update Status

Overall Status

🟡 Ready to Activate

Status Breakdown

3
Total

• Done (3)

Update Details

Current Firmware Version

1.1.2.160

Target Firmware Version

1.1.3c

Number Of Nodes

3
Total

• Master (3)

Last Update

2020-05-04, 14:15:18

Edit Details

Nodes

Node	In-Band Management IP Address	Status	Last Install
ServiceNode1	192.168.6.172	🟢 Done (100%)	2020-05-18, 18:17:59
ServiceNode2	192.168.6.173	🟢 Done (100%)	2020-05-18, 18:18:00
ServiceNode3	192.168.6.174	🟢 Done (100%)	2020-05-18, 18:18:02

Retry All

Activate

Activation Progress

Firmware Update

Setup

Install

Activate

Complete

This is the final stage of the update process. Once activation has finished, the update will be complete!

Update Status

Overall Status

Running

Status Breakdown

3

Running (1)

Done (2)

Update Details

Current Firmware Version

1.1.2.160

Target Firmware Version

1.1.3c

Number Of Nodes

3

Master (3)

Last Update

2020-05-04, 14:15:18

Nodes

Node	In-Band Management IP Address	Status	Last Install
ServiceNode1	192.168.6.172	Running (25%)	2020-05-18, 18:18:57
ServiceNode2	192.168.6.173	Done (12%)	2020-05-18, 18:18:56
ServiceNode3	192.168.6.174	Done (12%)	2020-05-18, 18:18:56

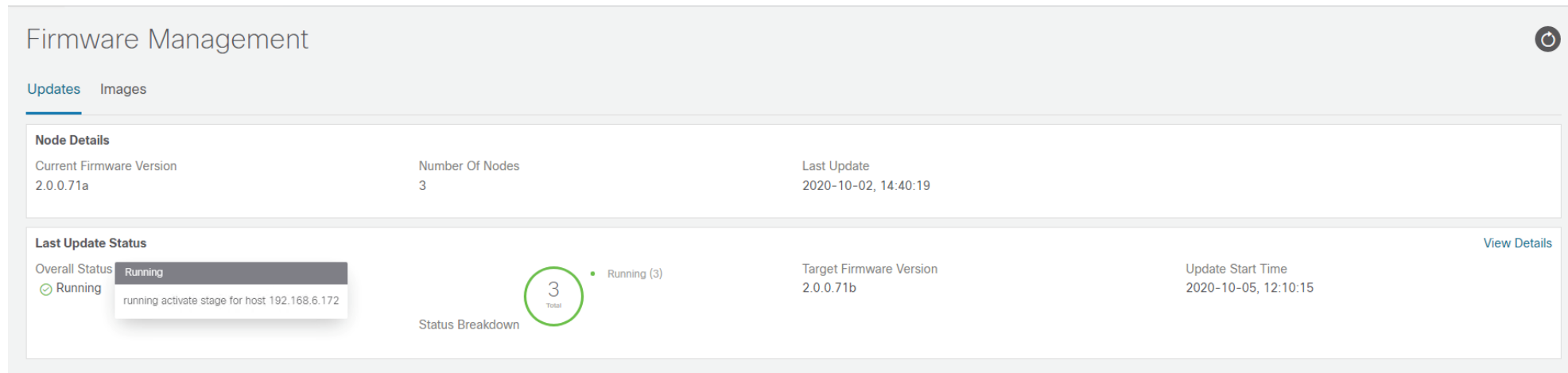
Retry All

Done



Monitoring Firmware Upgrade

- When the node you are connected to is activating, it will disconnect you. Please connect to another ND node. Check status via:

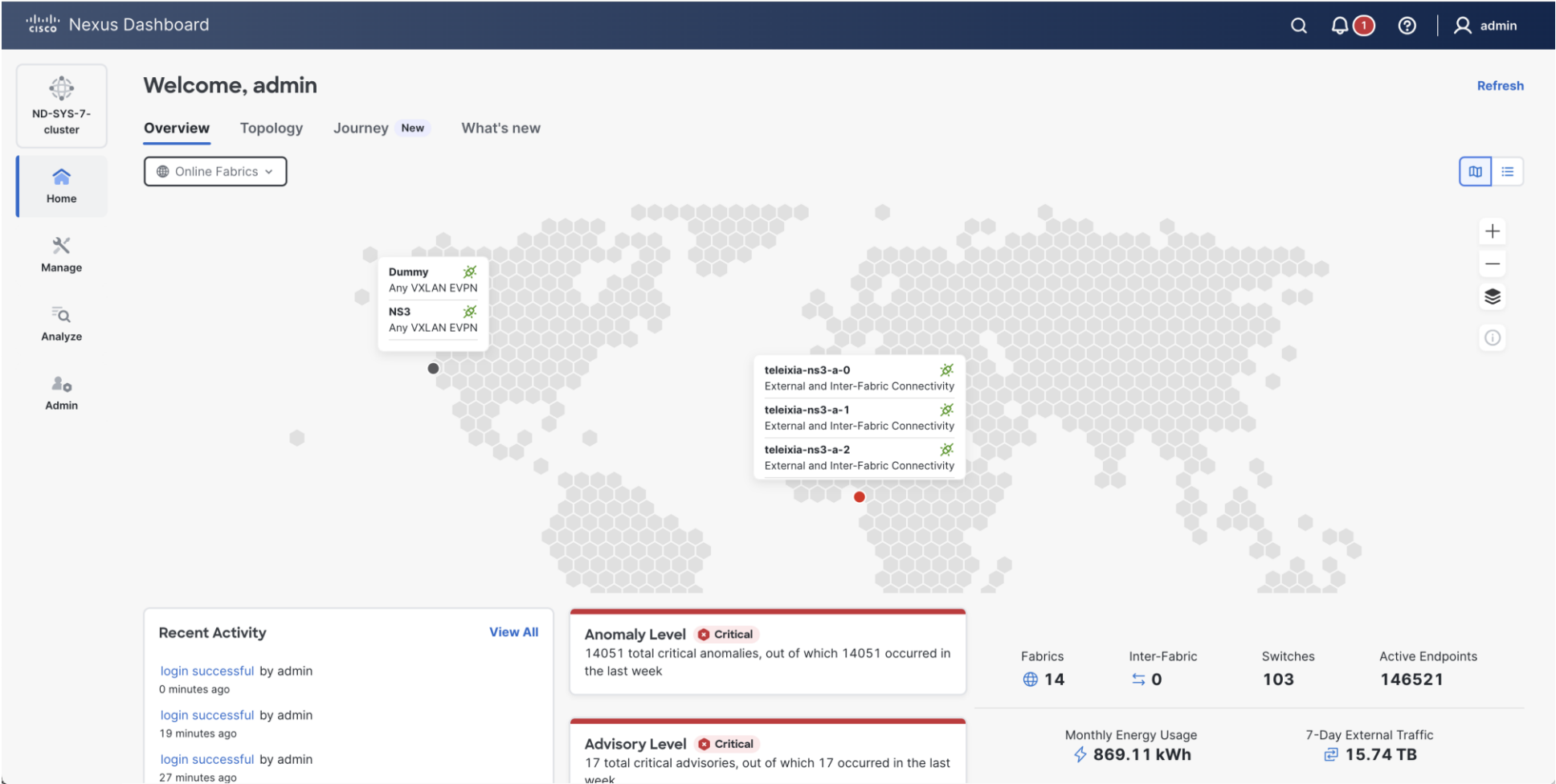


- Node going through an update will display:

Current node is going through upgrade, any configuration change during upgrade will not work. [More Info](#)

API and RBAC in 4.1

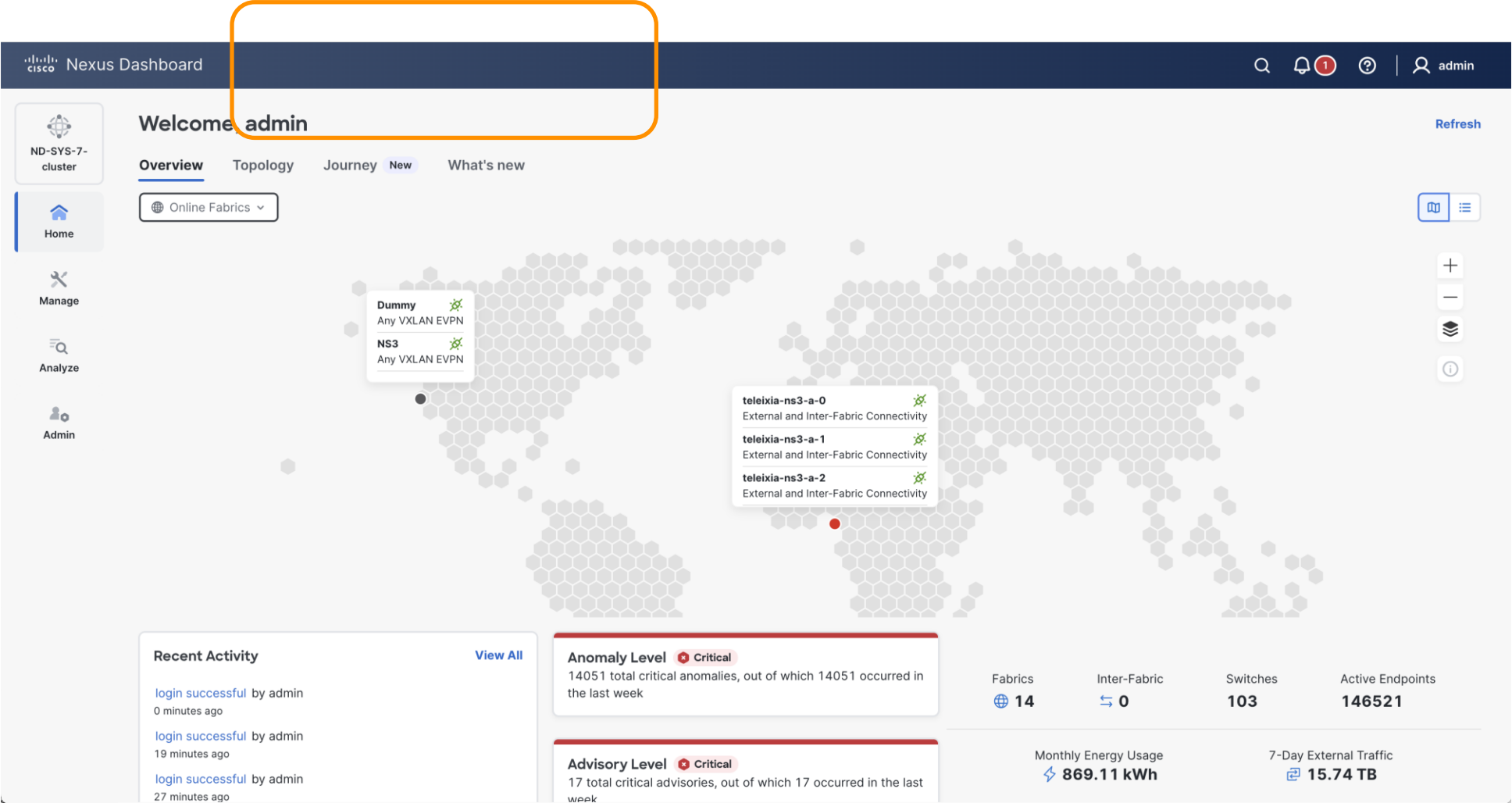
Unification



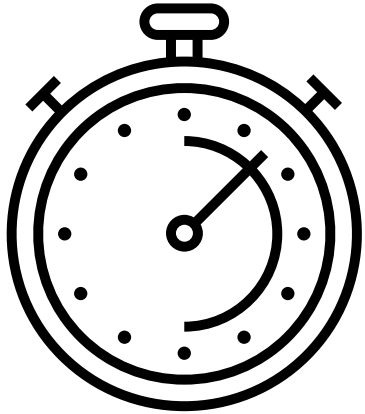
Unification

APIs

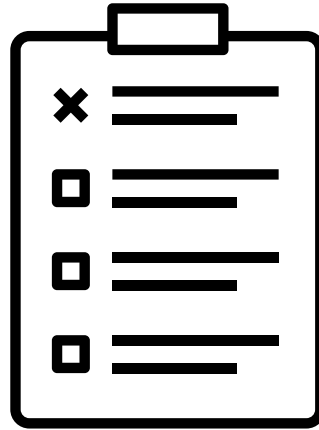
RBAC



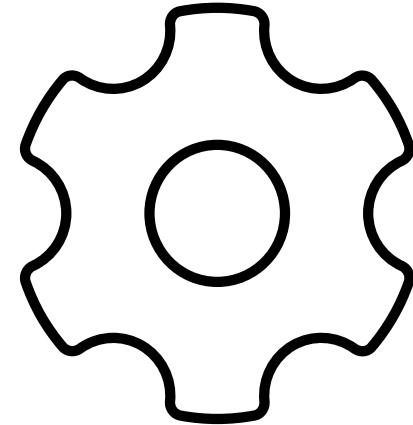
API Lessons Learned



APIs have a
lifespan

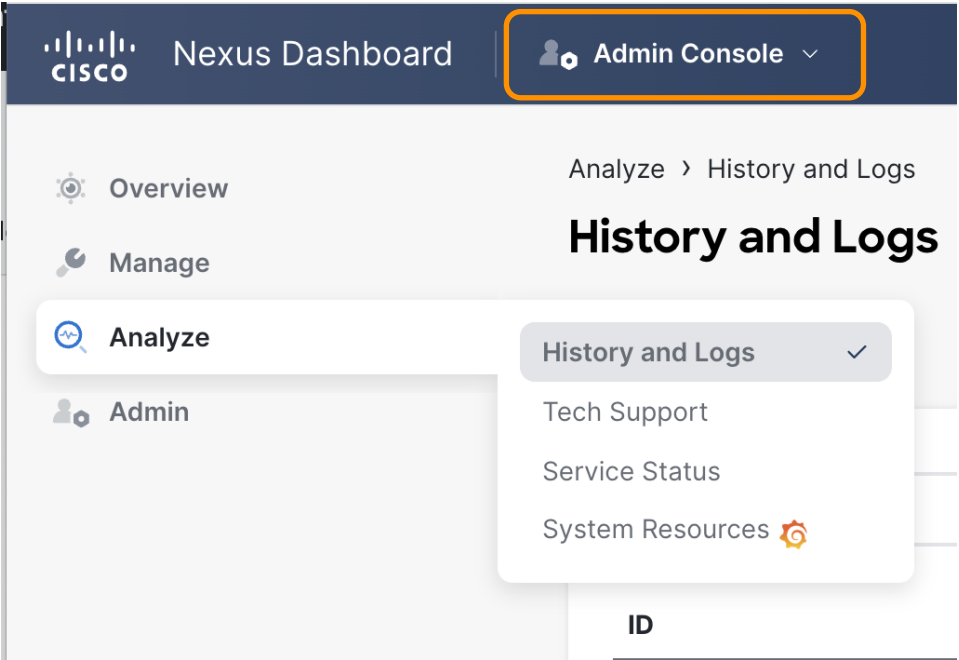


Cisco
guideline
development

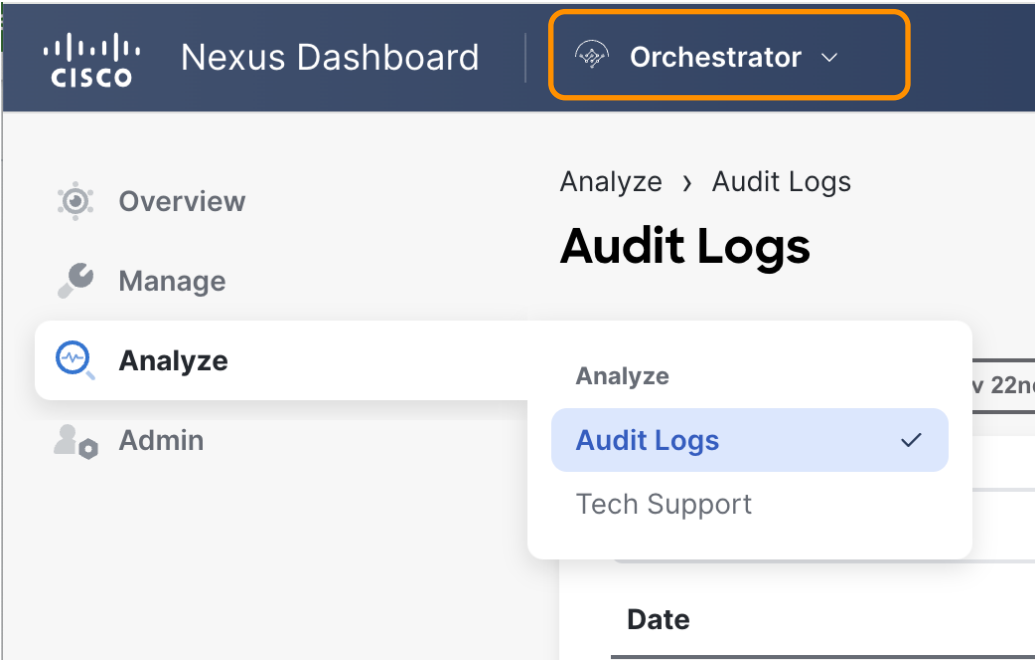


Automation
contracts

Resource Unification Example: Audit



ND



NDO

Resource Unification Example: Audit

Nexus Dashboard

Fabric Controller

Fabric FABRIC-1

Critical

Alarms(400)

8critical

42major

349minor

1warning

Fabric Controller

Overview

Manage

Analyze

Admin

Filter by attributes

Fabric Name

msd-test

Hide child Fa

NDFC

Fabric Overview - FABRIC-1

Overview

Switches

Links

Interfaces

Interface Groups

Policies

Networks

VRFs

Services

Security

Event Analytics

History

Deployment History

Policy Change History

Resource Organization: /api/v1



infra



manage



analyze



oneManage

Resource Organization: /api/v1



infra

auditRecords

clusters

integrations

certificates



manage

fabrics

switches

anomalyRules

changeControl



analyze

advisories

anomalies

connectivity

reports



oneManage

fabrics

links

clusters

Resource Unification: Audit

Nexus Dashboard

admin

cohost-pnd39

Home Manage Analyze Admin

Admin

Current ▾

Refresh

Nexus Dashboard Management

- System Status
- System Settings
- Licensing
- Integrations
- Intersight

Maintenance and Troubleshooting

- System Software
- Backup and Restore
- History and Logs** ✓
- Tech support

Authentication and more

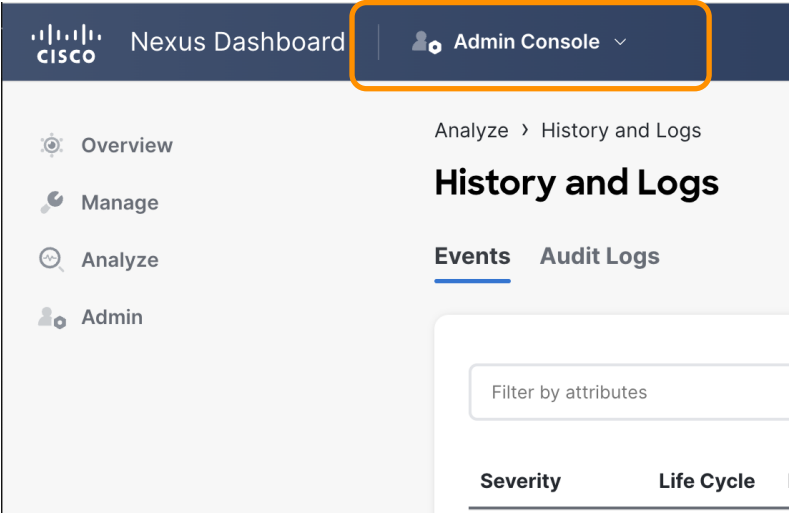
- Users and Security
- Certificate Management

User	Resource	Action performed	Description	Fabric name
admin	local	login	login successful	-
admin	local	login	login successful	-
adminwrite	clusters	delete	Delete cluster CS1	-
adminwrite	clusters	delete	Delete cluster CS1	-
adminwrite	radius	login	login successful	-
system	nodemgr	modify	modify User preference: remote-adminwrite	-
system	nodemgr	modify	modify Remote users: adminwrite	-
admin	radius	login	login failed	-
admin	radius	login	login failed	-

Download ▾

```
/api/v1/infra/auditRecords
```

Resource Unification Example2: Anomalies



Resource Unification Example2: Anomalies

Nexus Dashboard

Admin Console ▾

Overview

Manage

Analyze

Admin

Analyze > History and Logs

History and Logs

Events

Audit Logs

Filter by attributes

Severity

Life Cycle

Nexus Dashboard

Fabric Controller ▾

Fabric Controller

Overview

Manage

Analyze

Admin

Analyze > Event Analytics

Event Analytics

Learn More

Alarms

Events

Accounting

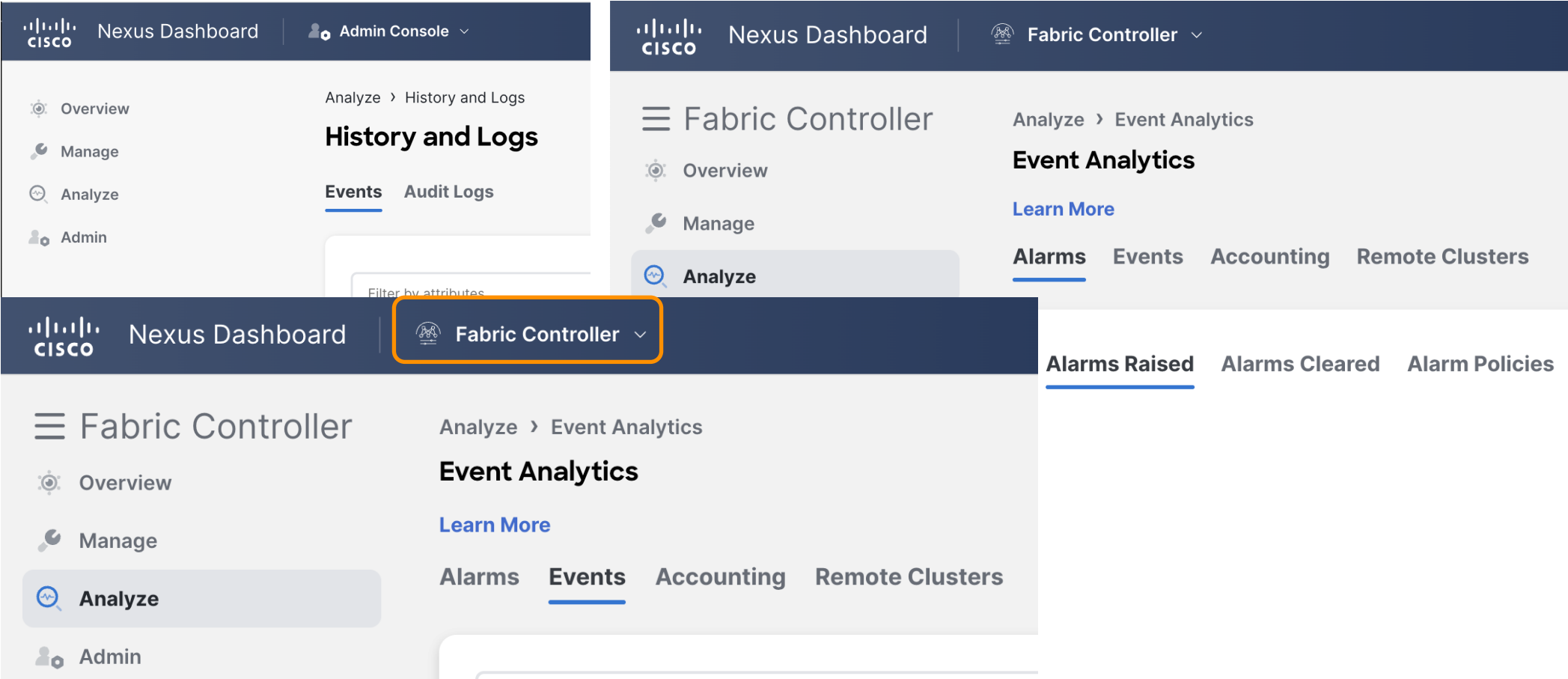
Remote Clusters

Alarms Raised

Alarms Cleared

Alarm Policies

Resource Unification Example2: Anomalies



Resource Unification Example2: Anomalies

The image illustrates the navigation path to the Anomalies page in the Cisco Nexus Dashboard. The top screenshot shows the 'Admin Console' view with 'History and Logs' selected. The middle screenshot shows the 'Fabric Controller' view with 'Event Analytics' selected. The bottom screenshot shows the 'Insights' view with 'Anomalies' selected. The 'Anomalies' page displays a donut chart for 'Anomaly Level' (1.4K total) and a table for 'Category'.

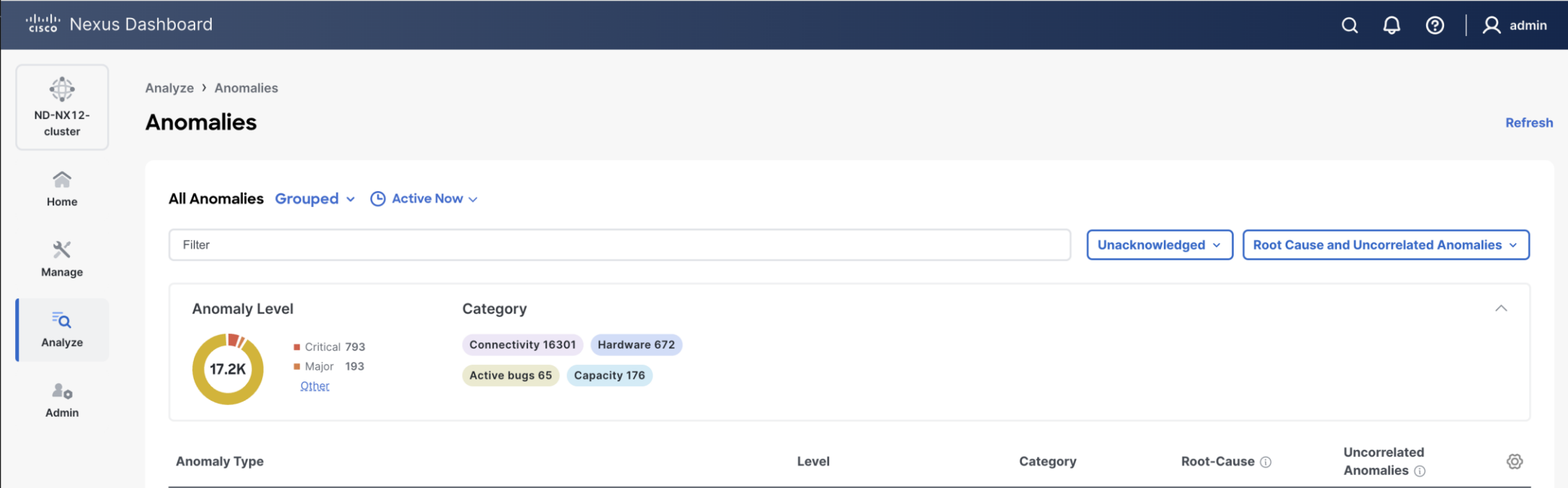
Anomaly Level

Anomaly Level	Count
Critical	563
Major	131
Other	1.4K

Category

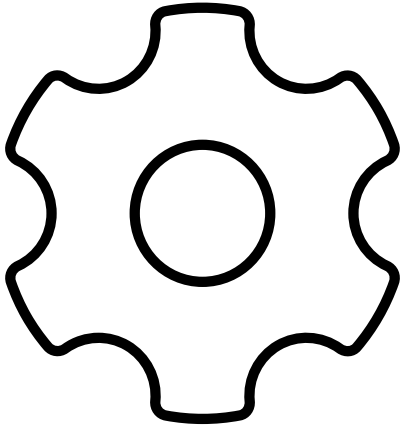
Category	Count
Configuration	998
Connectivity	357
Active bugs	12
Hardware	76

Resource Unification Example2: Anomalies



/api/v1/analyze/anomalies

4.1 API Workflow Impact



- Cluster Bootstrapping
- Cluster Settings
- Fabric Onboarding
- Federation Management
- Anomaly Management
 - Infra Events mapped
 - Controller Alarms mapped

4.1 API Summary

- Cisco-DevNet Standards -> consistency across platforms
- Nexus Dashboard Guidelines -> consistency across Nexus Dashboard features
- Backward Compatibility -> consistency across releases
- Legacy Commitment (now & future) -> evolution planning

4.1 API Summary

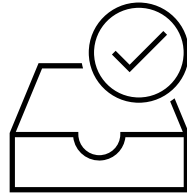
- Cisco-DevNet Standards -> consistency across platforms
- Nexus Dashboard Guidelines -> consistency across Nexus Dashboard features
- Backward Compatibility -> consistency across releases
- Legacy Commitment (now & future) -> evolution planning
- [API as a Product](#)

RBAC

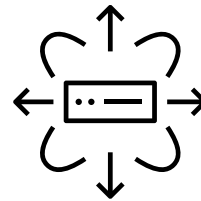
RBAC Simplification



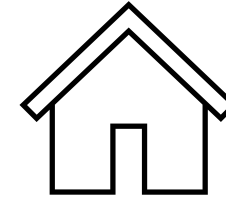
User has
Role(s)



Performs
Action



On
Resource(s)



In a Security
Domain

Roles pre-4.X

ND/NDO Roles	NDFC Roles
Administrator User Manager Power User	
Site Administrator Site Admin	Network Admin Device Upgrade Admin Access Admin
Dashboard User Admin (read-only)	Network Operator
Deployer	Change Deployer
Approver	Change Approver
Tenant Manager Site Manager	Network Stager

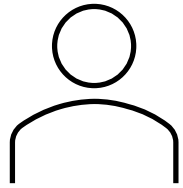
Roles in 4.0

ND/NDO Roles	NDFC Roles	4.X Roles
Administrator User Manager Power User		super-admin
Site Administrator Site Admin	Network Admin Device Upgrade Admin Access Admin	fabric-admin
Dashboard User Admin (read-only)	Network Operator	observer
Deployer	Change Deployer	support-engineer
Approver	Change Approver	approver
Tenant Manager Site Manager	Network Stager	designer

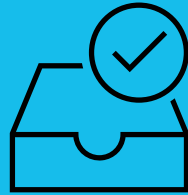
Role Descriptions

Description	4.X Roles
Unlimited access role	super-admin
Fabric ownership and management	fabric-admin
View-only	observer
Role for troubleshooting and general operations	support-engineer
Configuration change reviewer	approver
Configuration intent creator	designer

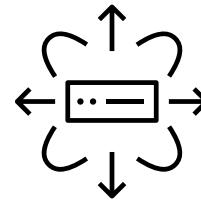
RBAC Simplification



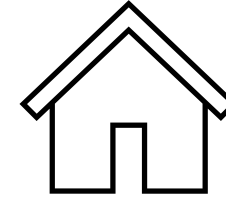
User has
Role(s)



Performs
Action



On
Resource(s)



In a Security
Domain

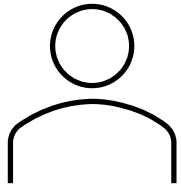
Actions

- Standard REST methods: Post, Delete, Get, Put, (Patch)
- Role access is conveyed in our OAS definitions.

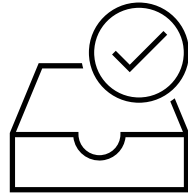
```
paths:
  /auditRecords: ...
  /cluster/config:
    get:
      Scan | Try it | Audit
      operationId: getClusterConfig
      responses: ...
      security:
        - OAuth2:
            - super-admin
            - observer
            - fabric-admin
            - support-engineer
            - approver
            - designer
```

```
paths:
  /auditRecords: ...
  /cluster/config:
    get: ...
    post:
      Scan | Try it | Audit
      description: Trigger cluster bootstrapping
      operationId: createCluster
      requestBody: ...
      responses: ...
      security:
        - OAuth2:
            - super-admin
```

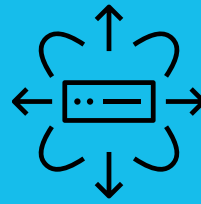
RBAC Simplification



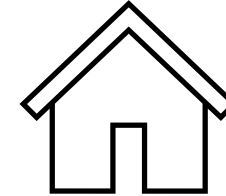
User has
Role(s)



Performs
Action



On
Resource(s)



In a Security
Domain

Resource Organization



/api/v1/**infra**



/api/v1/**analyze**

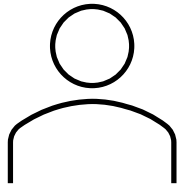


/api/v1/**manage**

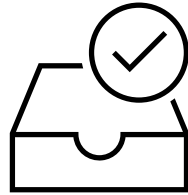


/api/v1/**oneManage**

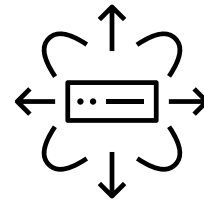
RBAC Simplification



User has
Role(s)



Performs
Action

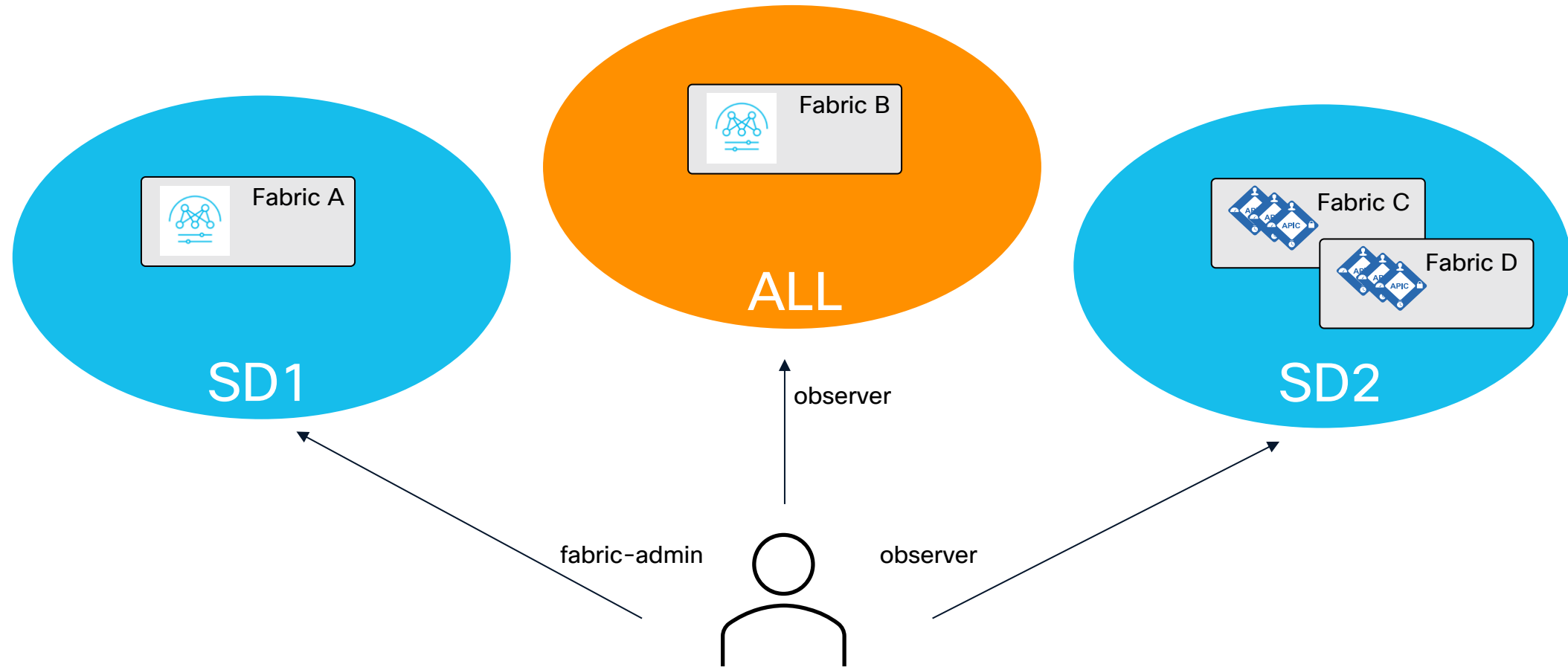


On
Resource(s)

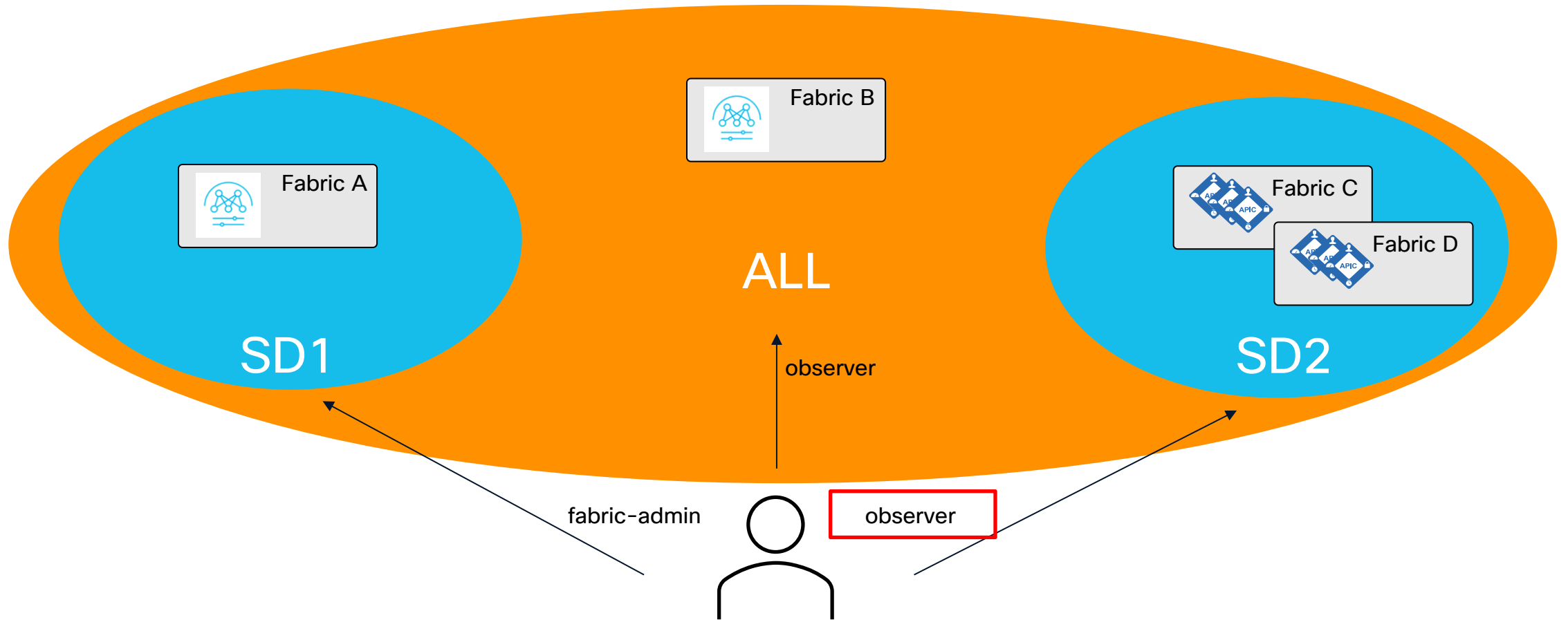


In a Security
Domain

Security Domains pre-4.0



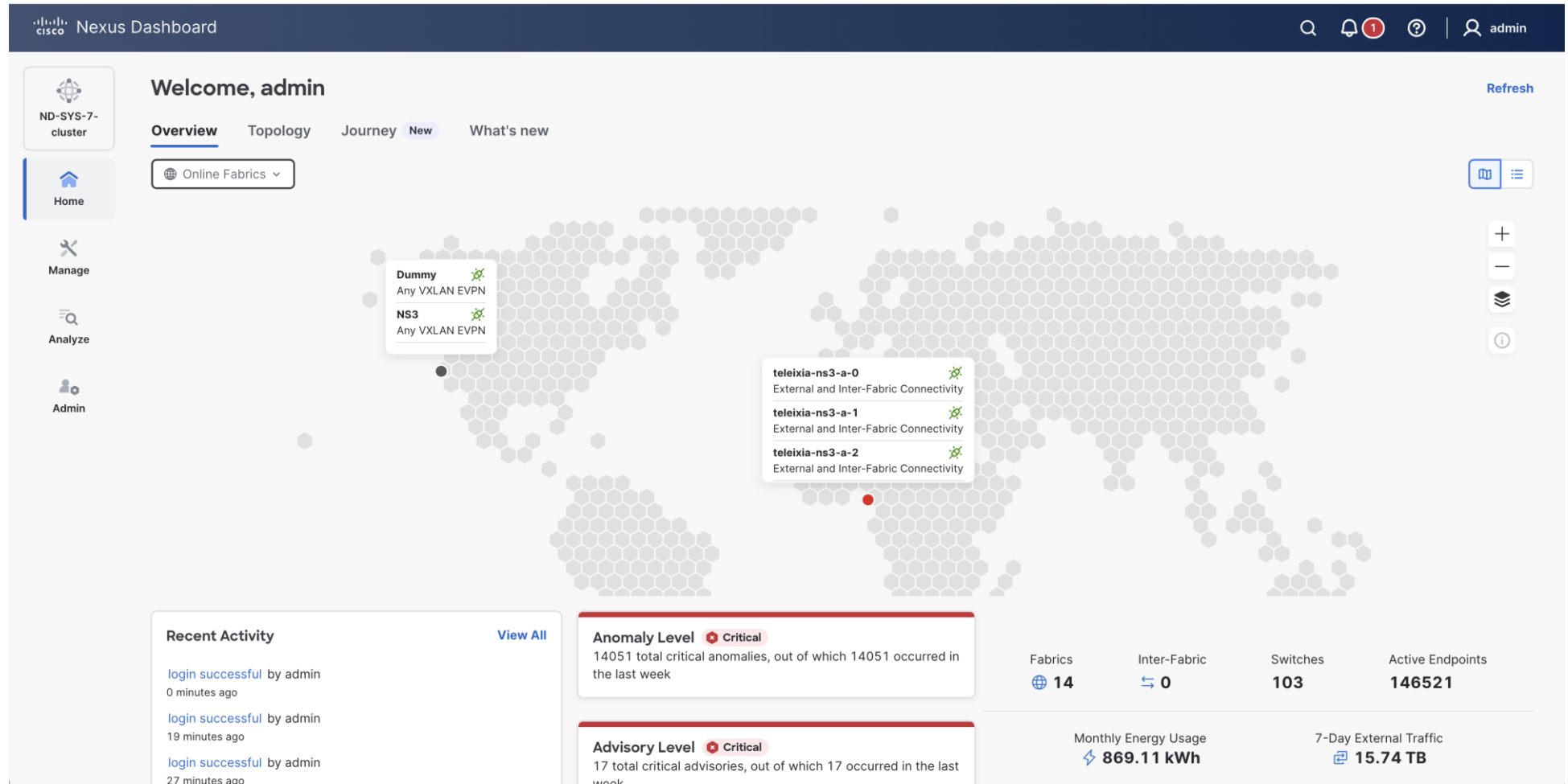
Security Domains 4.0 (NEW)



Unification in 4.1

APIs
Product
4 Umbrellas
Legacy
Run

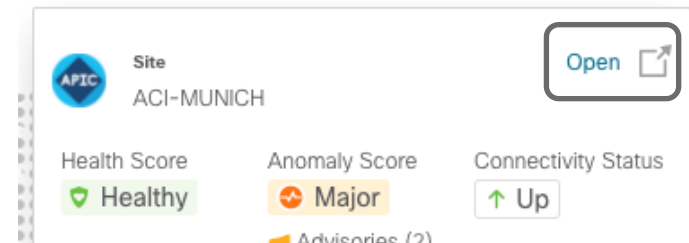
RBAC
6 Roles
ALL =
union



Remote Authentication

Remote Authentication

- ND adds support for following authentication providers
 - LDAP
 - TACACS
 - RADIUS
- RBAC is supported via cisco-avpair
- Is used for SSO, if the remote user has access rights to APIC, the user is automatically signed into APIC UI (4.2.6, 5.1 and later) and DCNM 11.5, when cross launching the UI. This is assuming the same auth. domain is used.



Login without and with enabled Login Domain





Welcome to
Nexus Dashboard
Version 4.1.0.122

Username

Password
 [Show](#)

Login

[Help Center](#) [Terms](#) [Privacy](#) [Cookies](#) ©2023 Cisco Systems, Inc.





Welcome to
Nexus Dashboard
Version 4.1.0.122

Username

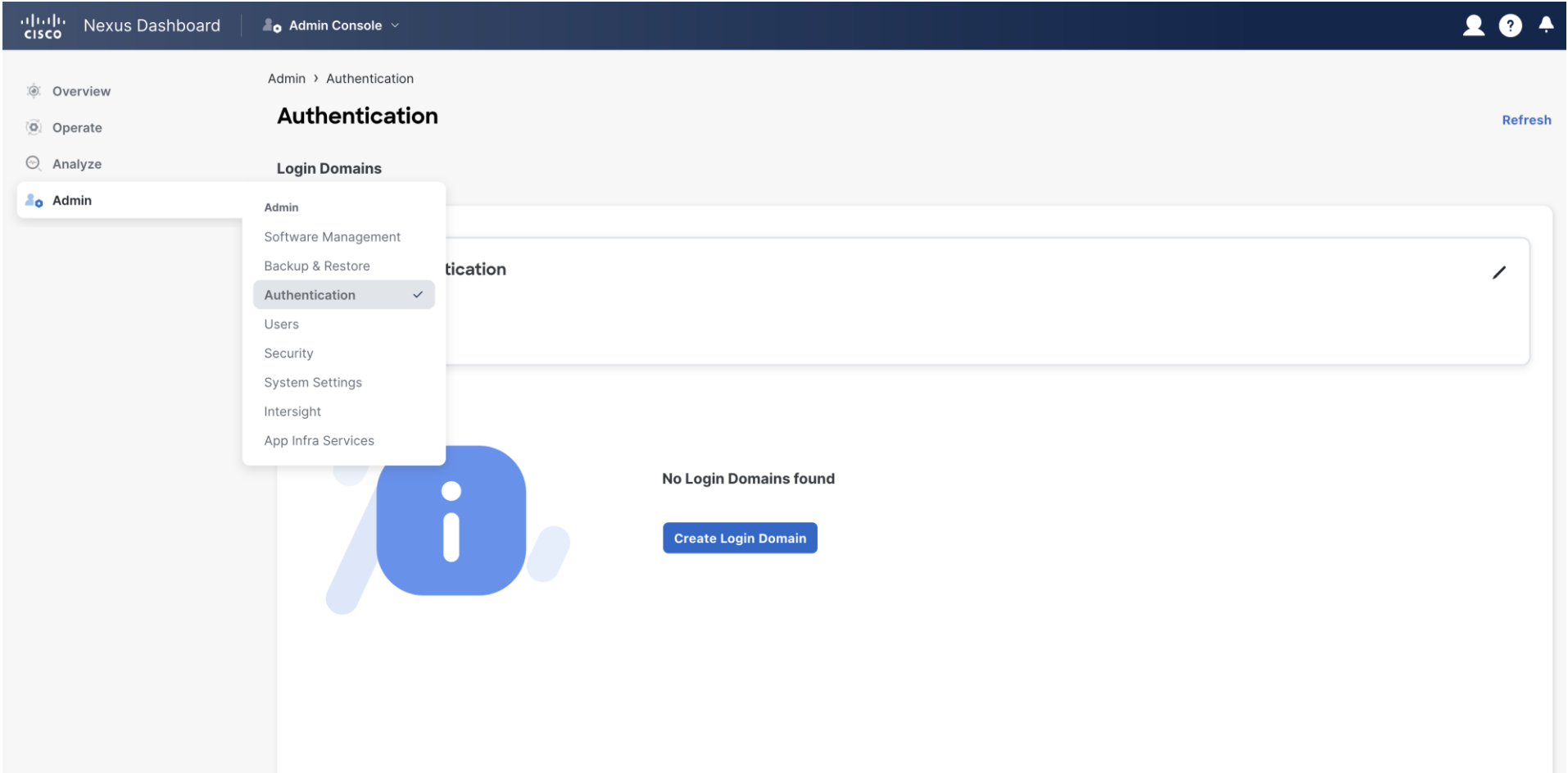
Password
 [Show](#)

Login domain
 [X](#) [v](#)

Login

[Help Center](#) [Terms](#) [Privacy](#) [Cookies](#) ©2023 Cisco Systems, Inc.

Create a Login Domain



Create a Login Domain

Create Login Domain

Name *

RADIUS

Description

Realm

RADIUS

Providers

Name	Description	Authentication Port
+ Add Provider		

ADD PROVIDER

General

Hostname/IP Address *

Description

Settings

Authorization Protocol

PAP CHAP MS-CHAP

Port

1812

Priority

0

Key *

Confirm Key *

Timeout (sec)

5

Retries

[Cancel](#) [Save](#)

Need to have a valid remote user to add provider –
backend will query the remote auth server with provider
info and user/pass before it can be added.

Change Default Authentication for Login

Admin > Authentication

Authentication

Refresh

Login Domains

Default Authentication

Login Domain
local

Filter by attributes

Create Login Domain

Default Authentication

Login Domain

local

RADIUS

local

Login Screen with Login Domain



Welcome to
Nexus Dashboard

Version 4.1.0.122

Username

Password

Show

Login domain



Login

[Help Center](#) [Terms](#) [Privacy](#) [Cookies](#)

©2023 Cisco Systems, Inc.

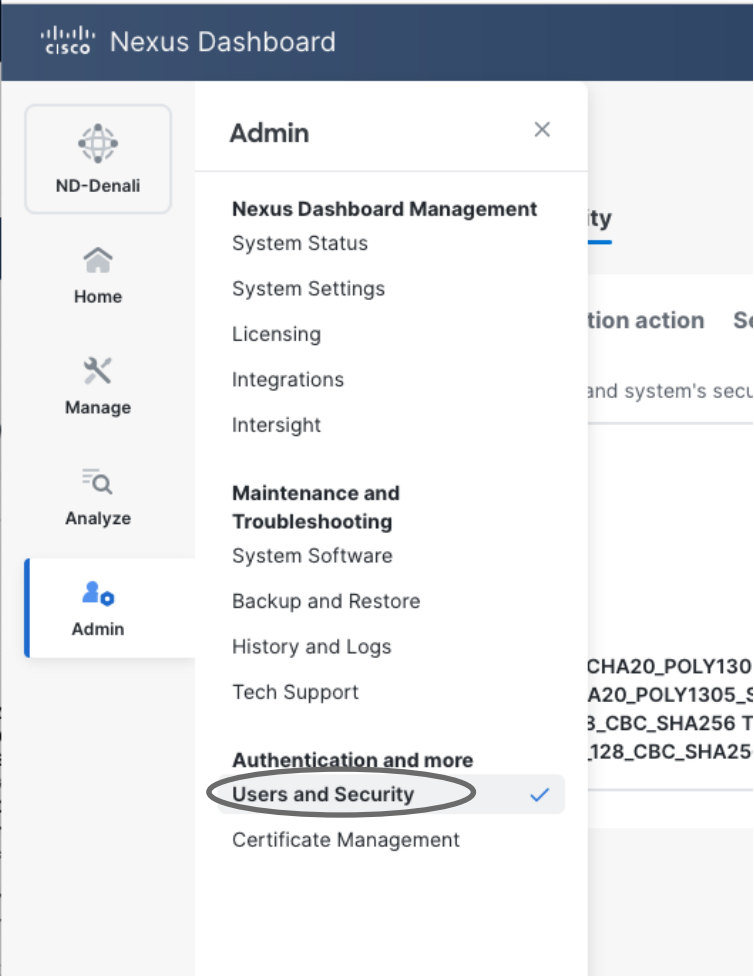
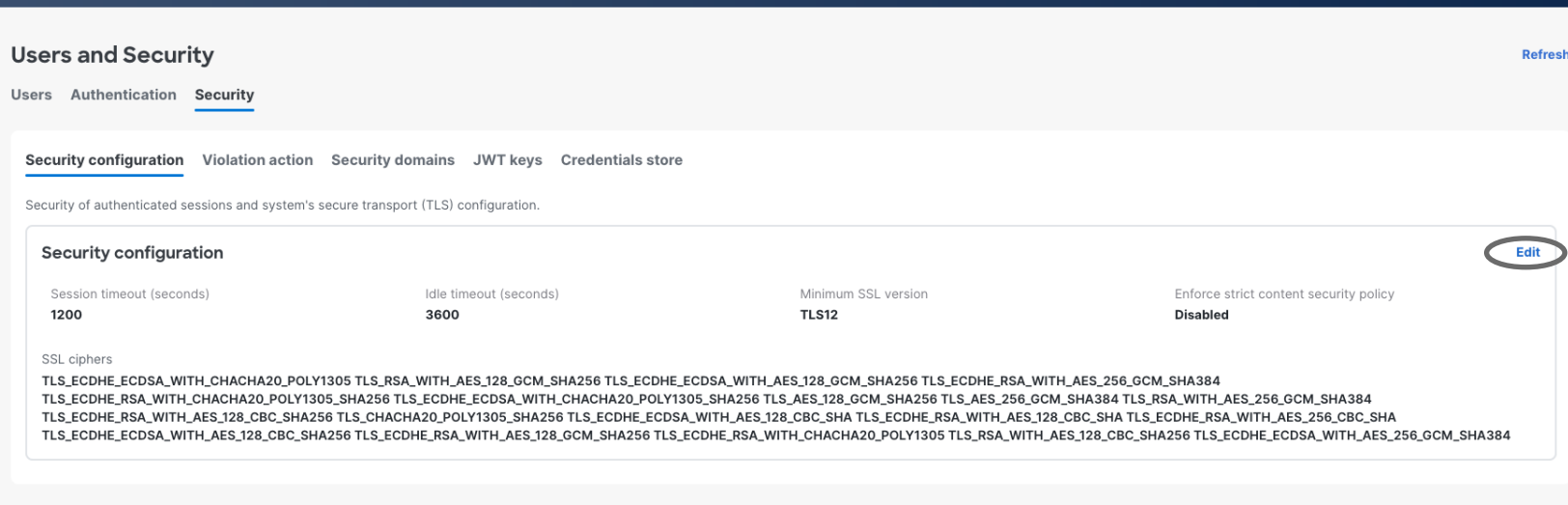


Configurable Security Settings

Configurable Security Settings

- Idle and Session Timeout is configurable
- Custom Certificates can be used
 - User needs to provide valid cert chain – backend does the validation before applying custom certs.
- Also with ND 2.3 and later you can have ND verify the Certificates of the onboarded Site-Controller before onboarding
- With 4.1 we support CyberARK as a credentials store

Configure Security Settings



Configure Security Settings

Session and Idle Timeout in Seconds

enabled SSL Chiphers etc.

Edit security configuration ✕

Session timeout (seconds)
1200

Idle timeout (seconds)
3600

Domain name
*

Minimum TLS version ⓘ
☐ TLSV1.3
☐ Enable enforce strict content security policy

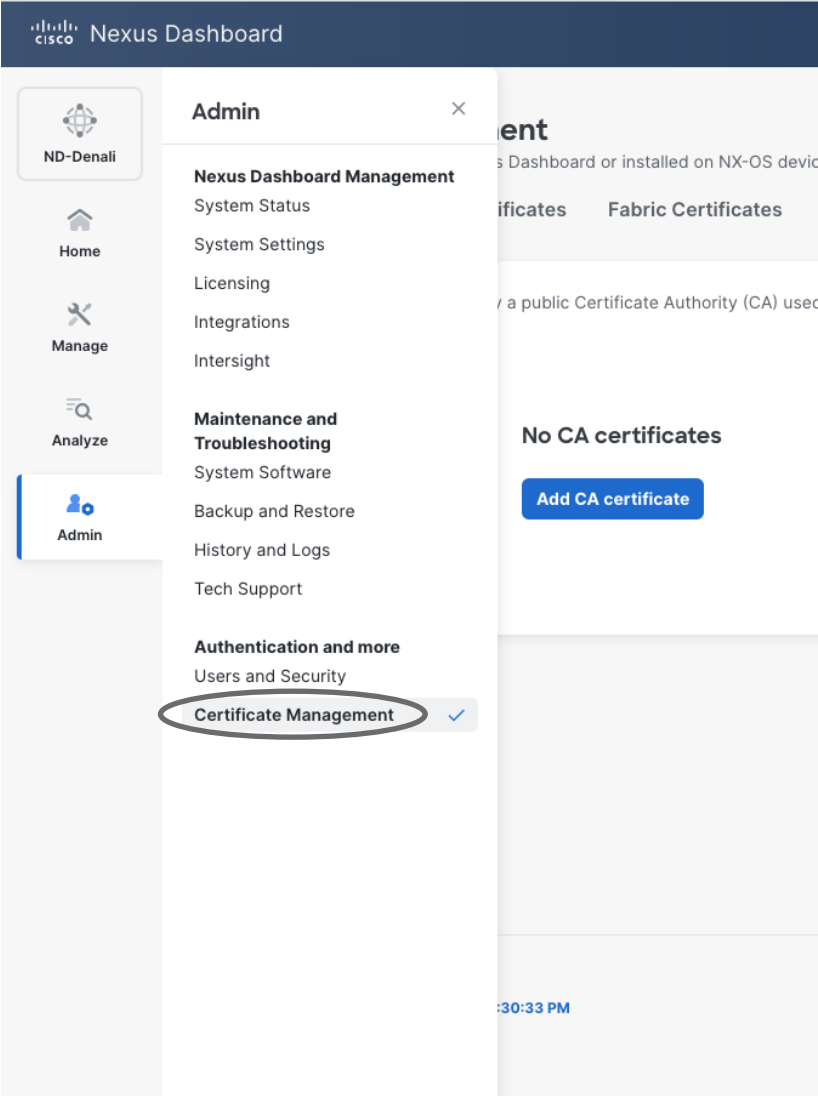
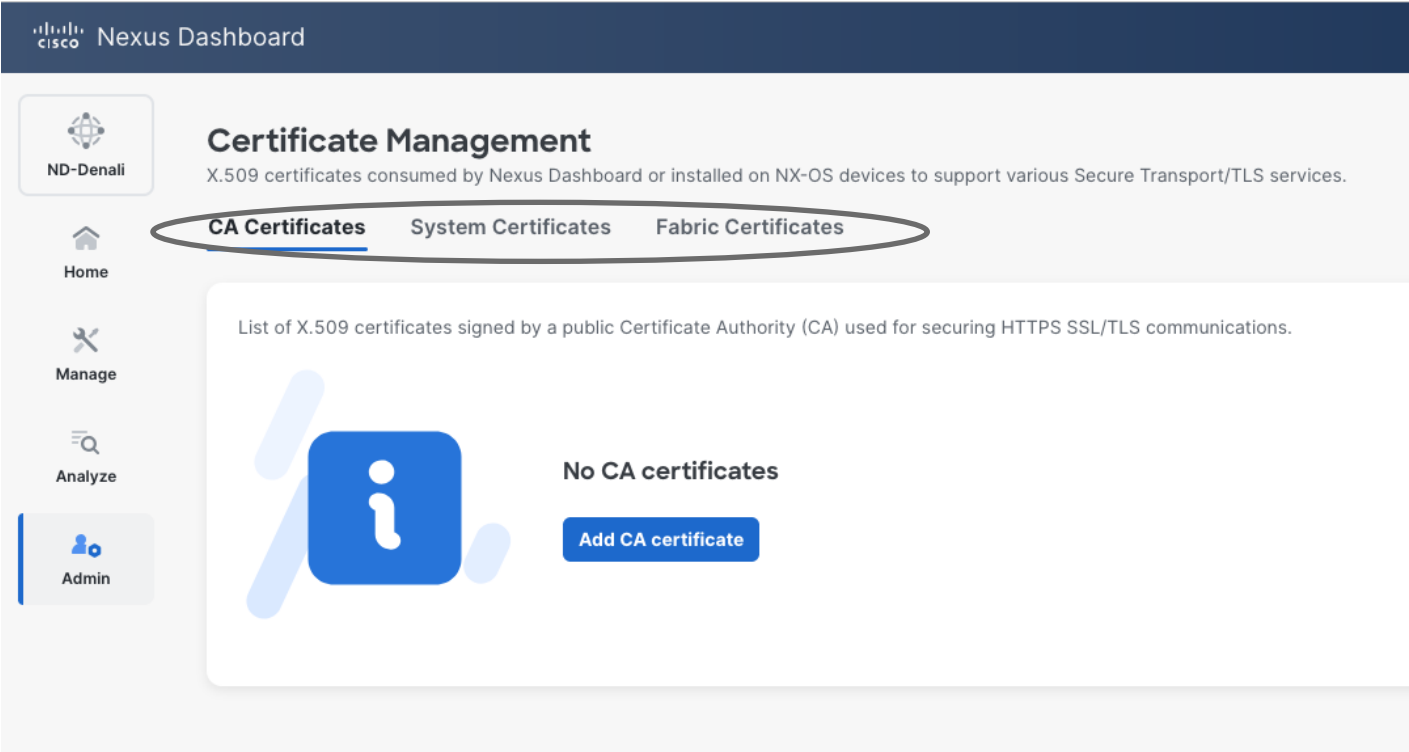
SSL ciphers

TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305 ✕
TLS_RSA_WITH_AES_128_GCM_SHA256 ✕
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ✕
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ✕
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 ✕
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 ✕
TLS_AES_128_GCM_SHA256 TLS_AES_256_GCM_SHA384
TLS_RSA_WITH_AES_256_GCM_SHA384 ✕
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ✕
TLS_CHACHA20_POLY1305_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ✕
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ✕

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

BRKDCN-2914

Configure Security Settings



```
[rescue-user@ND2 ~]$ openssl req -new -x509 -keyout cert.pem -out cert.pem -days 28 -nodes
Generating a RSA private key
.....
.....
writing new private key to 'cert.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:DE
State or Province Name (full name) []:Germany
Locality Name (eg, city) [Default City]:Munich
Organization Name (eg, company) [Default Company Ltd]:Cisco
Organizational Unit Name (eg, section) []:INSBU
Common Name (eg, your name or your server's hostname) []:*.tme-lab.local
Email Address []:insbu-muc@cisco.com
[rescue-user@ND2 ~]$
```

Unified Backup and Restore

Guidelines and Limitations

- Centrally-managed Remote Locations (SCP/SFTP)
- Multiple backup schedulers for Periodic Backups (remote location only)
- Persistent local backups
- Config-only/Full backups
- Fully encrypted backup files
- Backup/Restore is supported between vND and pND
- Backup & Restore functionality is not meant to be used as a mechanism for upgrading:
 - backup taken on version 3.2, will not be restored on version 4.0, 4.1, etc.

Creating a Backup

Create Backup

Settings

Name *

clus2025

Type ⓘ

Config-Only

Full

Destination

Local Download

Encryption Key *

.....

Backup And Restore

Backups

History

Backups

Backup Schedules

Filter by attributes

☐	Name	Type	St
☐	clus2025	Config-Only	2022

1 items found

Backup In Progress

Overall Progress

27%

Progress Details

Type	Description	Progress
> Orchestrator		<div></div> 0%
> Controller		<div></div> 0%
> Telemetry		<div></div> 10%
> Core		<div></div> ✓

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

BRKDCN-2914

Creating Periodic Upgrades

Create backup schedule

Settings

Name *

Type ⓘ

Config-Only

Full

Remote Storage Location

[View Details](#)

Remote path * ⓘ

Encryption Key *

Scheduler

Frequency *

Every day

Backups History

Backups Backup Schedules

Filter by attributes

Name	Type	Destination	Start time
daily-config	Config-Only	scp-server	2024-09-07, 17:00:20

1 items found

Restoring a Backup 1/2

2 Ways of restoring a backup. Either via a local available file or from a remote location or upload a file

Admin > Backup & Restore

Backup And Restore

Refresh

Restore

Create Backu

Backups

History

Backups

Backup Schedules

Filter by attributes

☐	Name	Type	Start time	End time	Status	Destination	User	Schedule
☐	backup1	Config-Only	2024-09-06, 16:52:52	2024-09-06, 16:54:08	<div><div></div>Success<div>View Details</div></div>	backup1.tar.gz	admin	-

1 items found

Rows per page

10

Delete

Download

Restore

Restoring a Backup 2/2

Restore

Source

Upload Configuration Backup File

Upload Configuration Backup File

Remote Storage Location

Accepted files: .tgz .tar.gz

Drag & Drop your files or [Browse](#)

Encryption Key *

Validation *

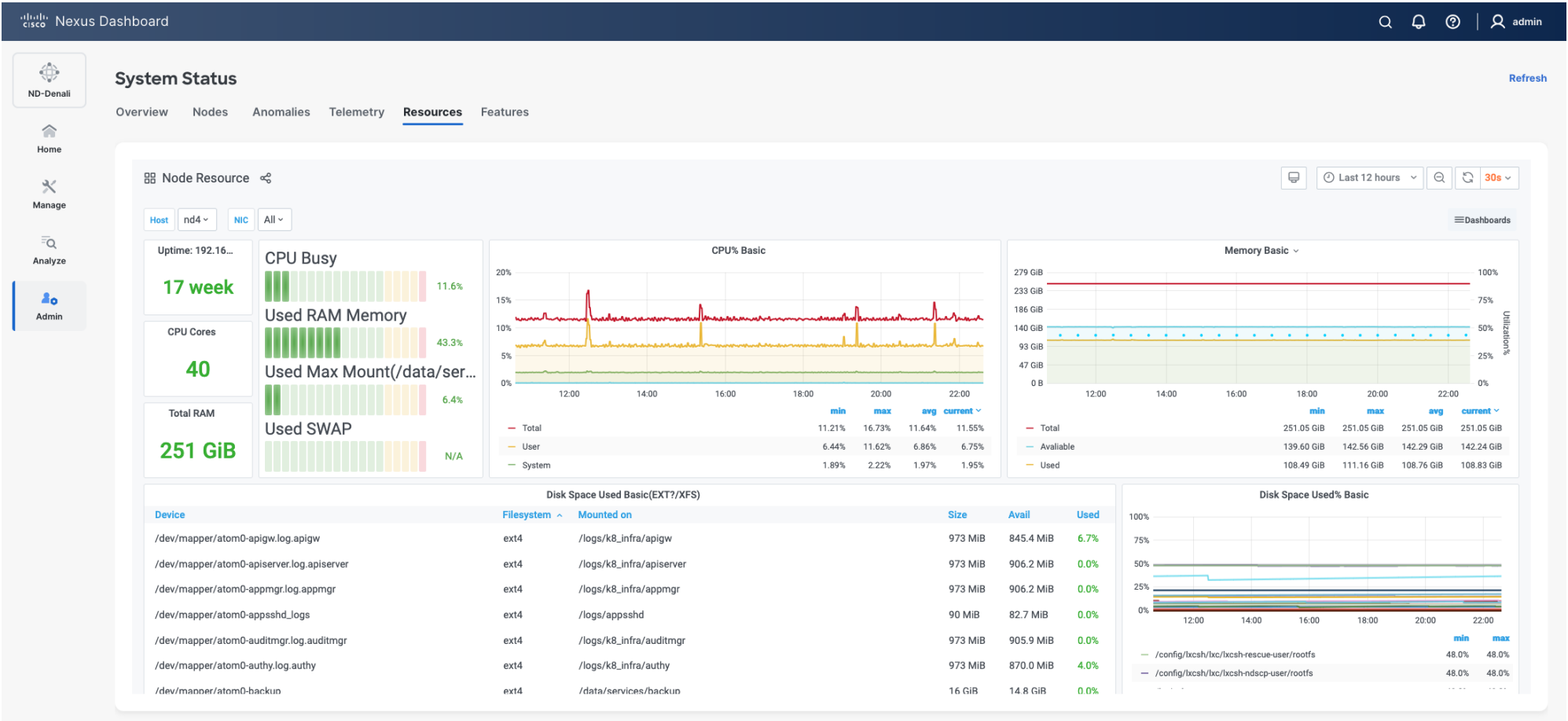
File Name	Progress
-	<div>Validate and Upload</div> <div></div>

Resource Monitoring

Resource Monitoring

- Provides Monitoring on
 - CPU
 - RAM
 - I/O Disk
 - I/O Network
- Node or Cluster level View
- Namespaces View

Resource Monitoring on Node and Cluster Level



Event Analytic

Overview

- Provides periodic monitoring of ND Cluster at platform level
- Generates critical, major and minor alerts for ND Cluster
- Optional these can be streamed via syslog (TCP/UDP)

Monitored Entities of ND Cluster (1/2)

- Node CPU Usage: determines if ND node level CPU usage crosses 80%
- Node Memory Usage: determines if ND node level memory usage crosses 80%
- Node Disk Usage: determines if ND node level disk usage crosses 80%
- Node not reachable: determines if the ND node is not reachable
- Node rebooted: determines if an ND node has been rebooted
- Node NTP sync state: determines whether ND node ntp is synchronised
- Node BGP Peer Health: determines whether ND node bgp peers are established
- etcd cluster health: determines whether ND node etcd endpoints are healthy

Monitored Entities of ND Cluster (2/2)

- Kubelet software fault: determines ND node level kubelet health
- Apps degraded: determines whether the app (NDI/NDFC/NDO) state is degraded
- Network link health: determines whether network devices (data) are down
- DNS health: determines whether DNS servers are reachable
- Cluster Health: if the cluster is not healthy with a detailed description
- Backup Schedule Config Health: determines if ND backup schedules are configured
- Scheduled Backup Health: determines if ND lates backup schedules are successful

Examples of Generated Events


Nexus Dashboard


ND-Denali


Home


Manage


Analyze


Admin

Admin

Nexus Dashboard Management

System Status

System Settings

Licensing

Integrations

Intersight

Maintenance and Troubleshooting

System Software

Backup and Restore

History and Logs

System Status

Overview
Nodes
Anomalies
Telemetry
Resources
Features

Filter

Anomaly Level

Category


Critical 4


System 4

ND Node Network Link Health Event Analytics

Overview
Event Records

General


Critical Severity

Detection Time
2024-08-28, 17:20:20

Cleared Time
-

Description
Network device mgmt1 in node nd-node3 is down

Fault Domain
server

Last Updated
2024-09-06, 16:09:04

Syslog

Status
Completed

Timestamp
2024-08-28, 17:20:19

Configuring Syslog Servers 1/2

ND-Denali

Home

Manage

Analyze

Admin

Nexus Dashboard

admin

System Settings

Refresh

General

Fabric management

Multi-cluster connectivity

Flow collection

Cluster details

Name

App subnet

Service subnet

ND-Denali

172.17.0.1/16

100.80.0.0/16

DNS

Edit

Domains

nd-denali.case.local

Providers IP addresses

10.49.153.3

Search domains

tme-lab.local

Remote storage

Edit

Name

IP address

Protocol

Status

scp-server

192.168.10.12

SFTP

N/A

Remote streaming servers

Edit

Name

Server type

Protocol

Host

Port

No remote streaming servers added

History and logs settings

Edit

Audit logs streaming



Configuring Syslog Servers 2/2

← Remote streaming servers

Add Server

Service

Splunk

Syslog

Protocol

TCP

UDP

Name *

syslog-1

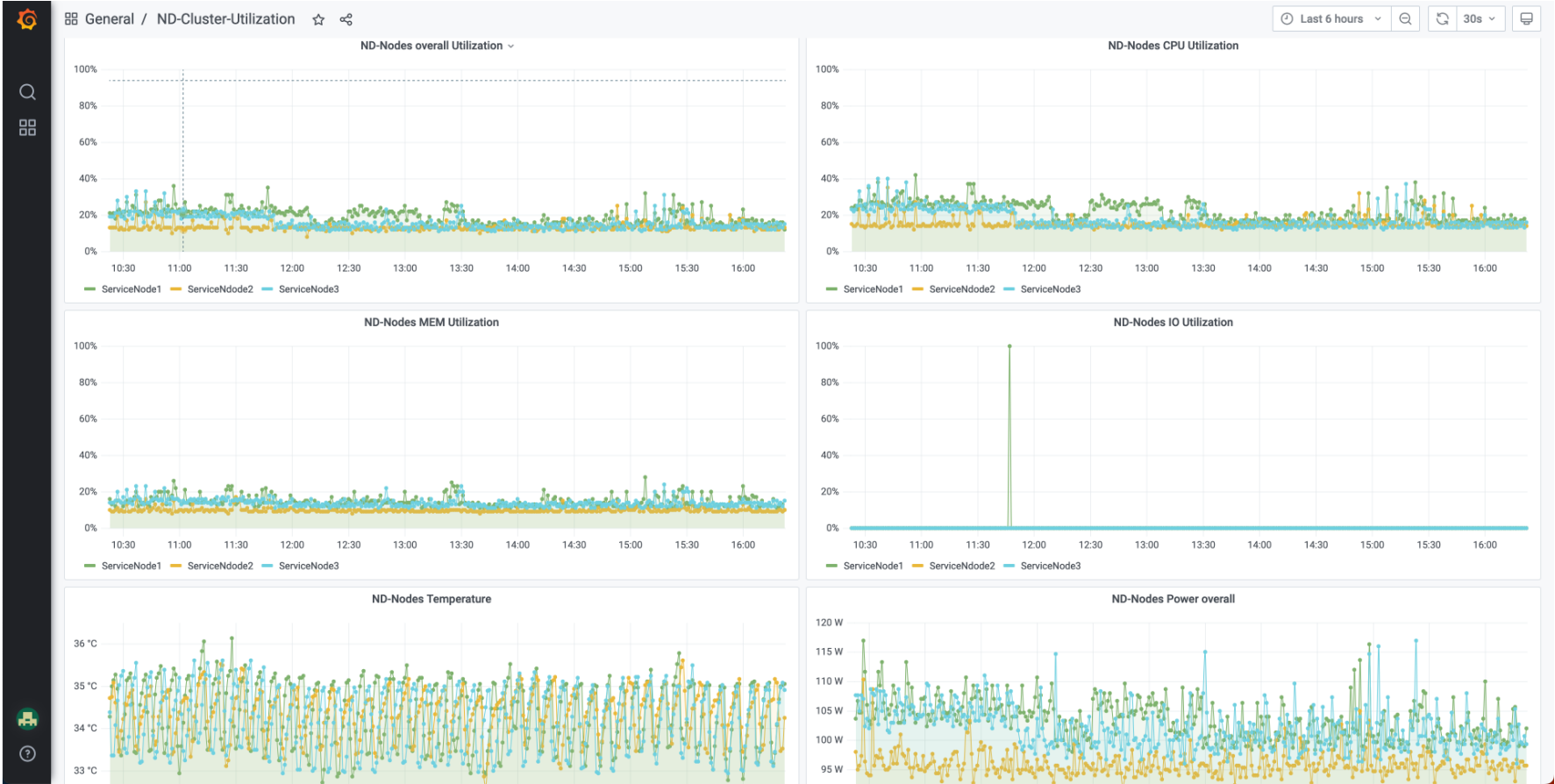
Hostname/IP address *

192.168.10.12

Port *

614

Hardware Monitoring of ND via CIMC



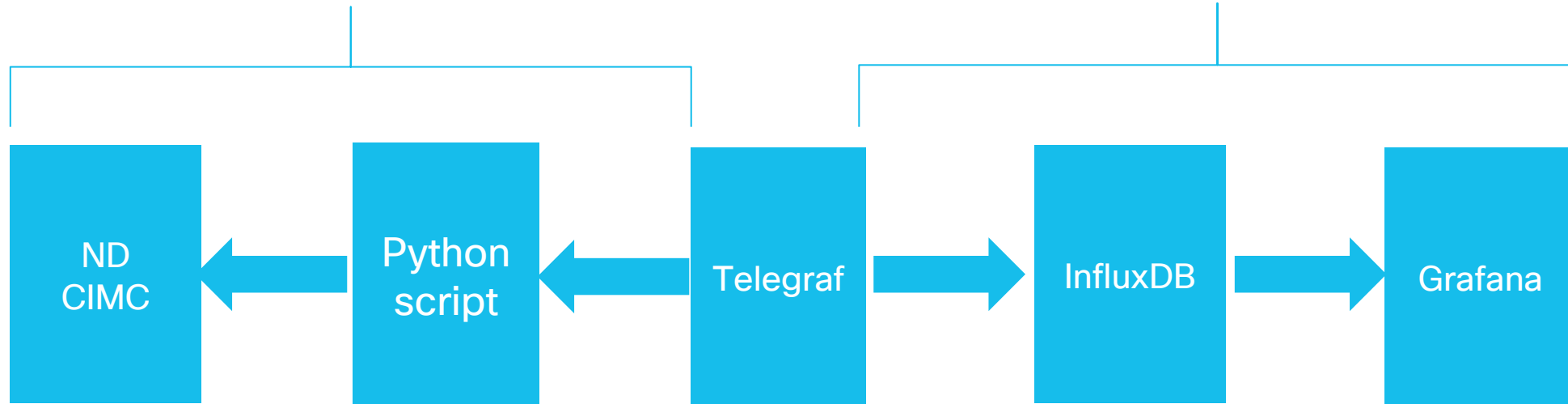
Hardware Monitoring of ND via CIMC

- Leveraging REST-API of CIMC to get:
 - Power draw
 - Temperature
 - CPU, I/O and RAM Utilisation
- Querying the following dns:
 - CPU, I/O and RAM : dn="sys/rack-unit-1/utilisation"
 - Temperature: dn=="sys/rack-unit-1/temperature"
 - Power: dn="sys/rack-unit-1/pwrmonitor-Platform"

SW Stack Example

Telegraf calling a Python script to collect periodically data from CIMC

Telegraf storing data as timeseries in InfluxDB.
Grafana visualizes the data



Basic Troubleshooting

Basic Troubleshooting

- Accessing ND Console, only via “rescue-user” with “admin” password
- Usage of ACS

```
rescue-user@ND-Node1:~$ acs
usage: [-h] [-v] {debug-token,passphrase,version,system-config,verify,
: error: the following arguments are required: which
rescue-user@ND-Node1:~$ acs health
All components are healthy
rescue-user@ND-Node1:~$
```

Basic Troubleshooting

Usage of Kubectl to get information of the K8S

```
rescue-user@ND-Node1:~$ kubectl get pods --all-namespaces
```

NAMESPACE	NAME	READY	STATUS	RESTARTS	AGE
aaamgr	aaamgr-5979845989-jmjbd	1/1	Running	0	57d
authy-oidc	authy-oidc-58bb444797-54qnn	1/1	Running	4 (57d ago)	57d
authy	authy-585955bc5f-jz9lz	3/3	Running	0	57d
authy	authy-585955bc5f-nwfgt	3/3	Running	0	57d
authy	authy-585955bc5f-zh5md	3/3	Running	0	57d
cisco-appcenter	apiserver-77b8dc6c65-t8xm6	1/1	Running	0	57d
cisco-appcenter	appcenterconnector-89d74b88b-ww6fv	1/1	Running	0	57d
cisco-appcenter	appsync-856f8f57b8-7bg77	1/1	Running	0	57d
cisco-appcenter	store-58f8fff84-nhkjz	1/1	Running	0	57d
cisco-intersightdc	deviceconnector-cjhnp	1/1	Running	0	57d
cisco-intersightdc	deviceconnector-kbjqv	1/1	Running	0	57d
cisco-intersightdc	deviceconnector-nj8c9	1/1	Running	0	57d

Conclusion

Conclusion

- Nexus Dashboard is now a Unified Product, offering all the Services
- Make a detailed Planning of HA/DR
- After Deployment, Services can be consumed on an as needed Basis

Complete your session evaluations



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



Earn up to 800 points by completing all surveys and climb the Cisco Live Challenge leaderboard.



Level up and earn exclusive prizes!



Complete your surveys in the Cisco Live Events app.

Continue your education



Visit the Cisco Stand for related demos



Book your one-on-one Meet the Expert meeting



Attend the interactive education with Capture the Flag, and Walk-in Labs



Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Thank you

CISCO Live !

