

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC



Deploying Nexus Dashboard in your Organisation

Matthias Wessendorf, Principal Technical Marketing Engineer
@matteq4er
BRKDCN-2914

Cisco Webex App

Questions?

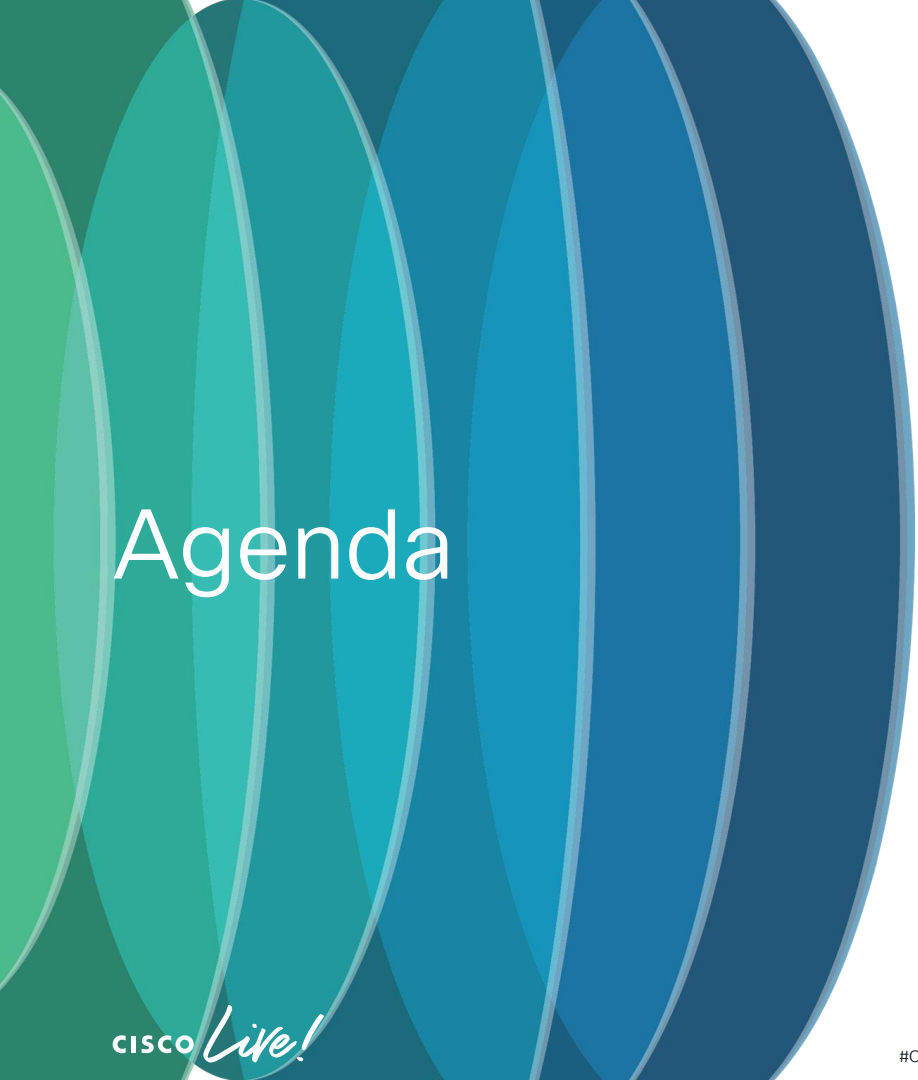
Use Cisco Webex App to chat with the speaker after the session

How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until November 15, 2024.





Agenda

- Introduction
- What is Nexus Dashboard?
A view under the hood
- Deploying Nexus Dashboard
- Operating Nexus Dashboard
- Summary

At the end of the session you will ...

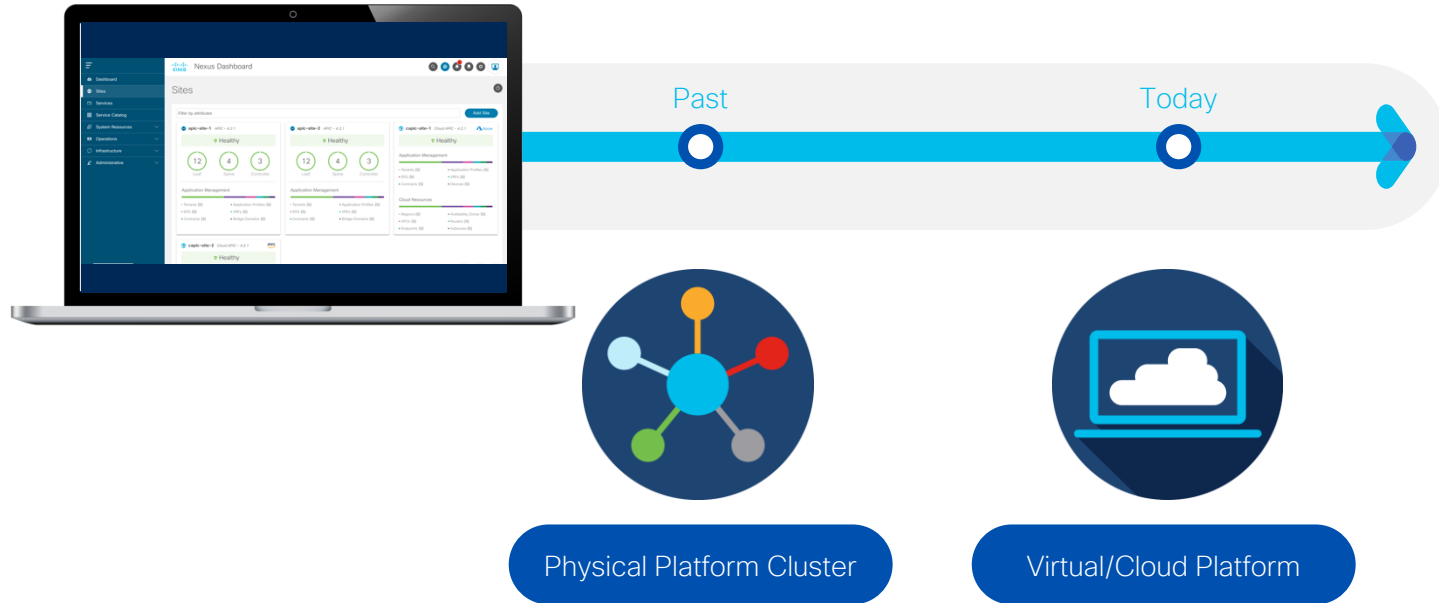
- Be able to define the requirements for deploying a Nexus Dashboard in your Organisation. By describing the
 - Deployment model, centralised vs. stretched
 - Network requirements and attachment to the network
 - Sizing a Nexus Dashboard for the different services.

Introduction



Nexus Dashboard

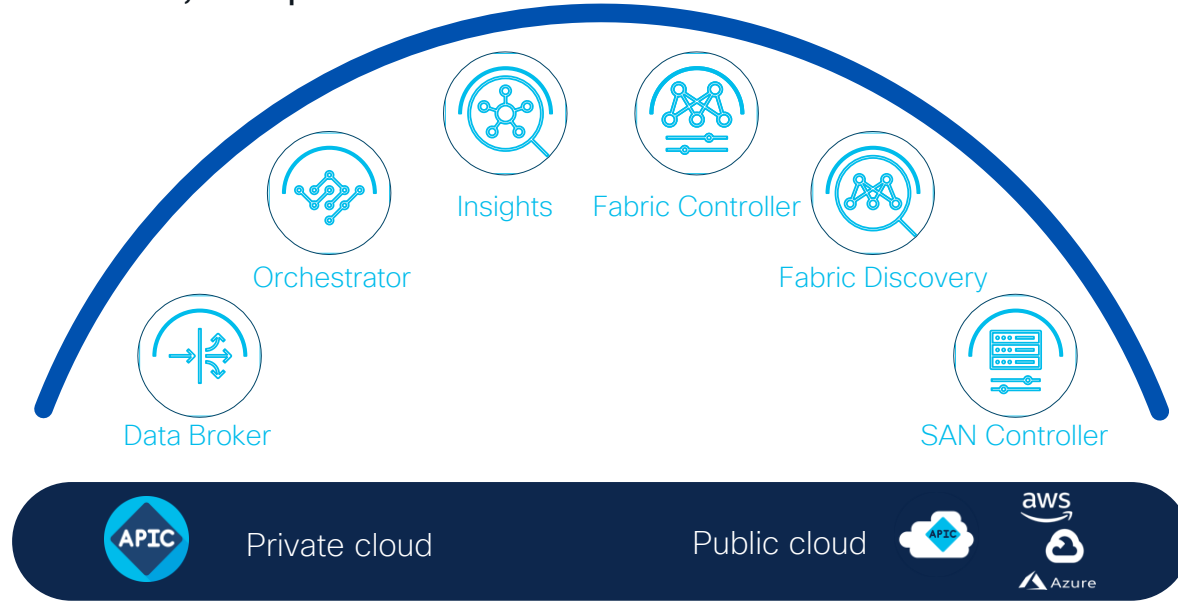
Deployment evolution



Nexus Dashboard

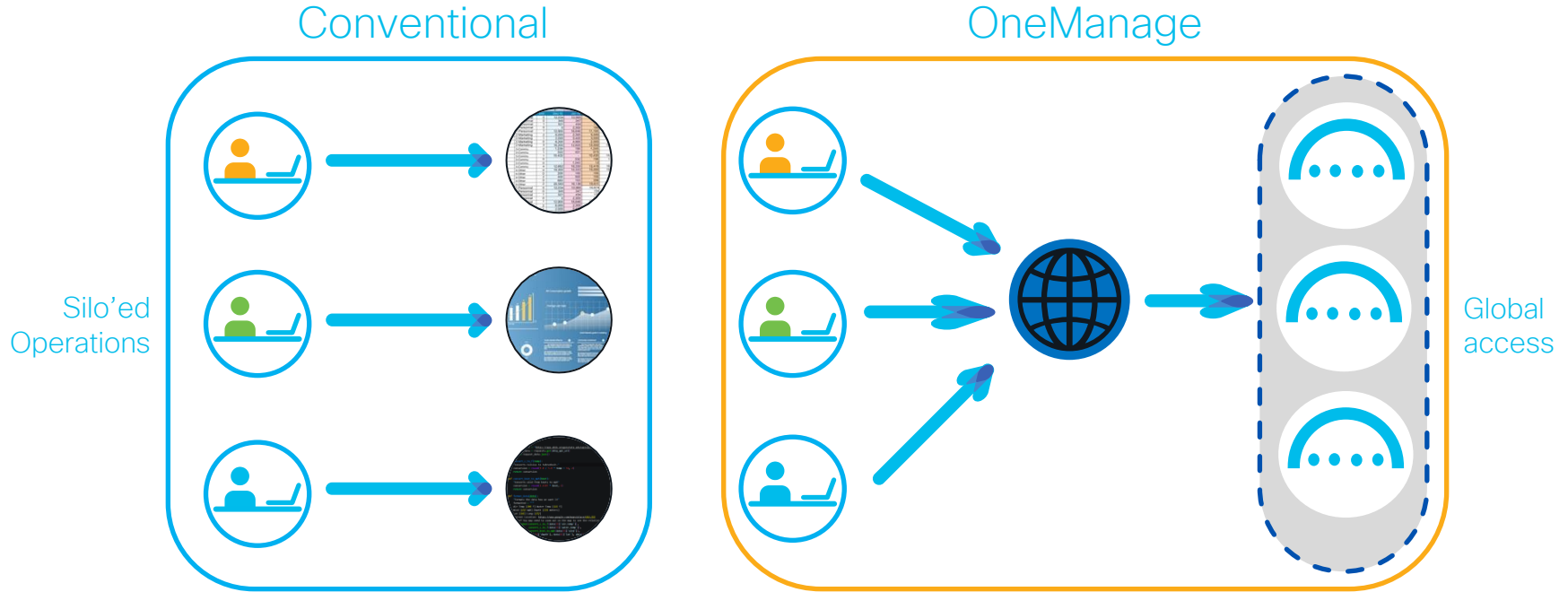
Simple to automate, simple to consume

Powering automation
Unified agile platform



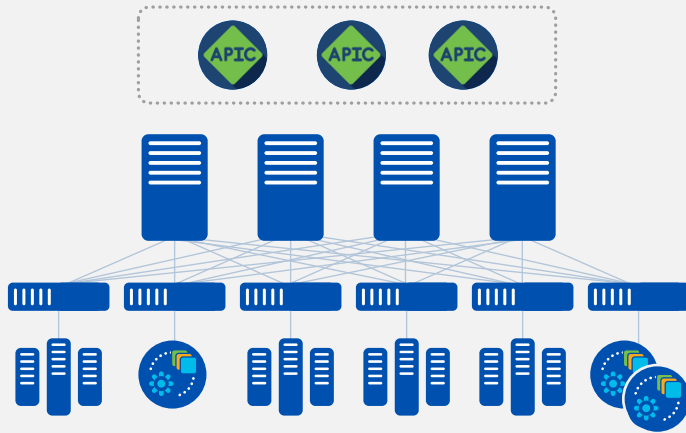
Consume all services in one place

Nexus Dashboard: OneManage



Cisco Nexus Dashboard Platform

Modern Scale-out application services stack to host data center operations applications



2.2 GHz(Node-G2) or 2.8Ghz(Node-G4) CPU x 2

256 GB memory

2.4 TB x 4 HDD

10G/25G/40G connect

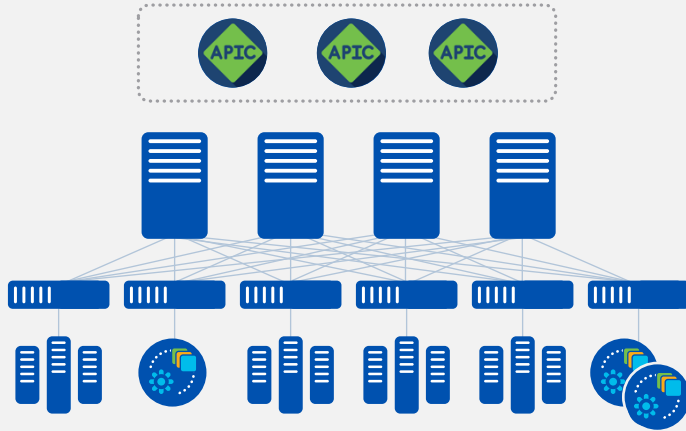
Network automation

Scale-out cluster

High Availability

Virtual Nexus Dashboard Platform

Virtual Platform to Support NDI ,NDO and NDFC in Production



Nexus
Dashboard
Insights



APP-Node

64 GB memory

550G/1536GB* SDD

16 vCPUs



Nexus
Dashboard
Orchestrator



Nexus
Dashboard
Fabric Controller



DATA-Node

128 GB memory

3TB SSD/NVMe

32 vCPUs

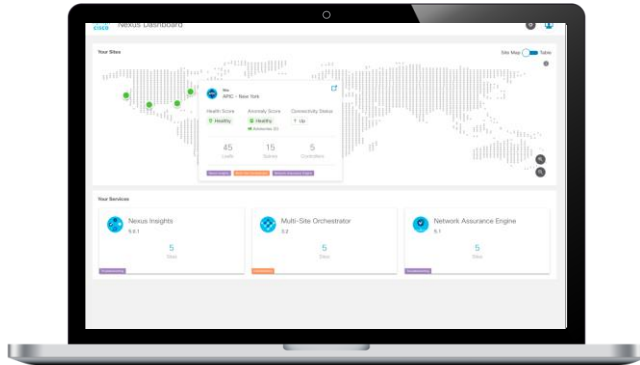
Available for

ESXi

KVM

Nexus Dashboard: A Unified Agile Platform

The operator view



Consume service(s) from single place

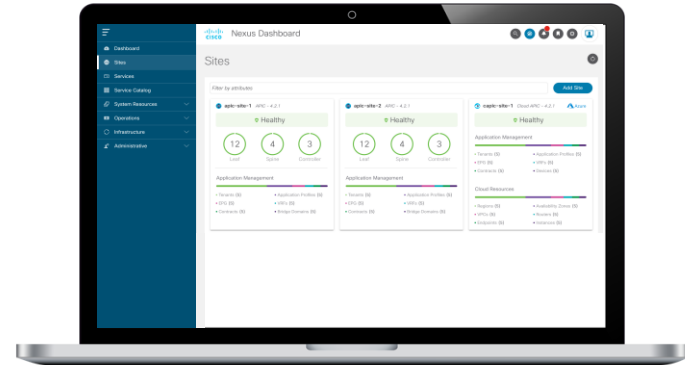


Frictionless navigation across multiple services and sites



Customise views and workflows

The admin view



Single dashboard for lifecycle management of services and Ops infra



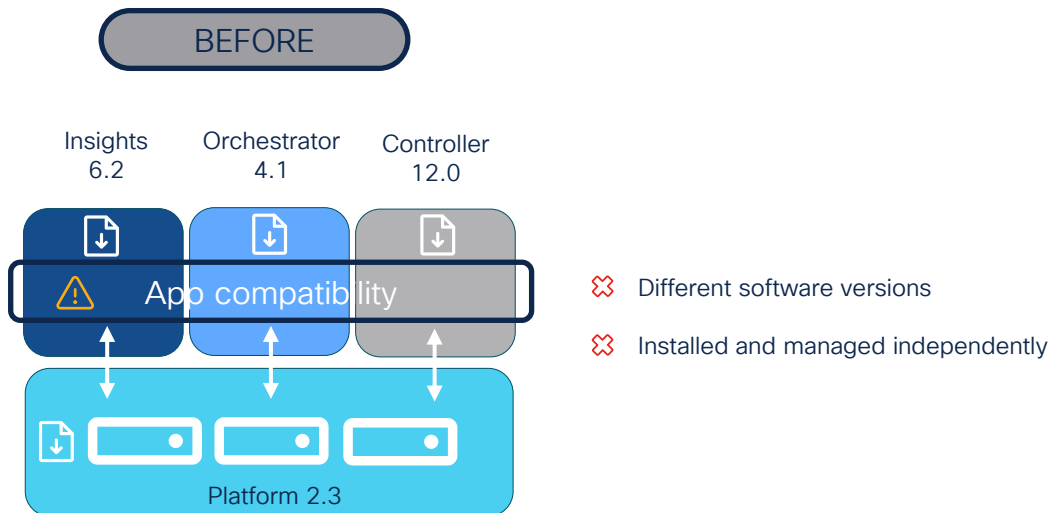
Consistent one-time onboarding of domains and services



Consistent user management and access control

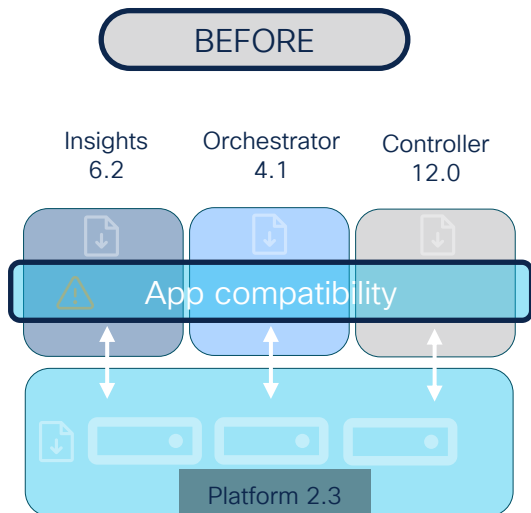
Nexus Dashboard

Unified Image

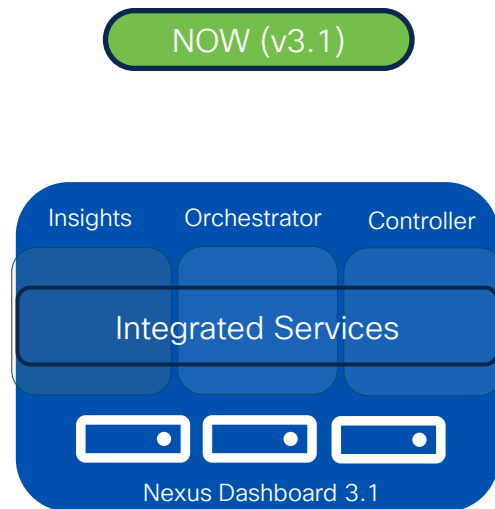


Nexus Dashboard

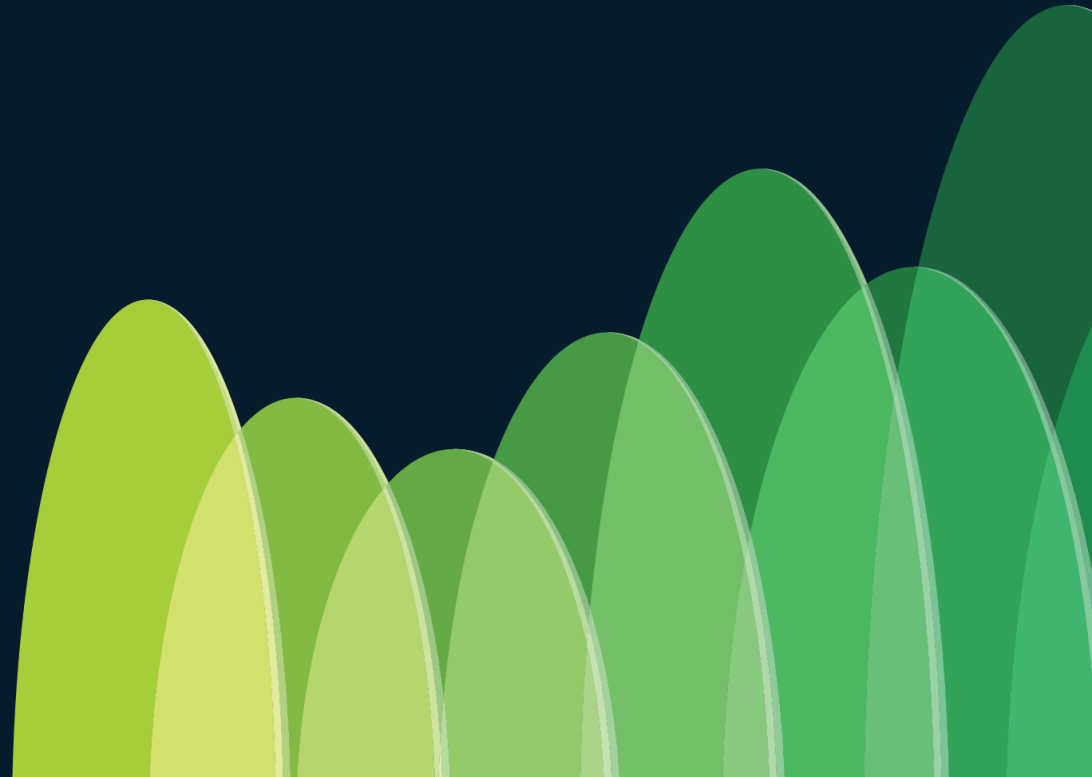
Unified Image



- ✓ Single .iso or .ova includes all services
- ✓ Direct upgrade from previous versions²



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 redundancyOr
 - 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

Nexus Dashboard Interfaces

Data Interface

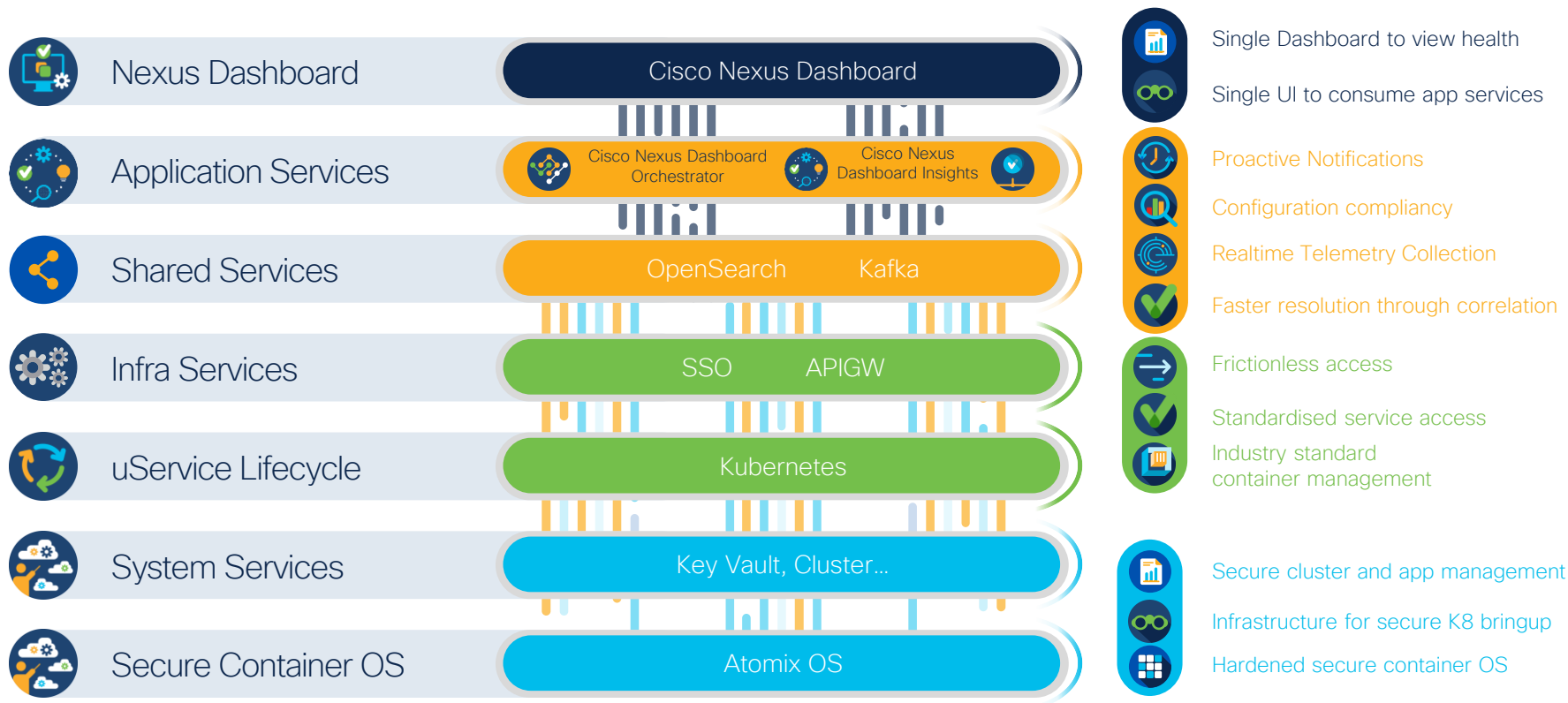


Used for Intra Cluster Communication
Used for Telemetry Collection

Mgmt Interface

Used for Mgmt/API Access to Cluster
Used for Syslog, AAA, Proxy, DNS communication

Nexus Dashboard Platform—Under the Hood



Deployment Model

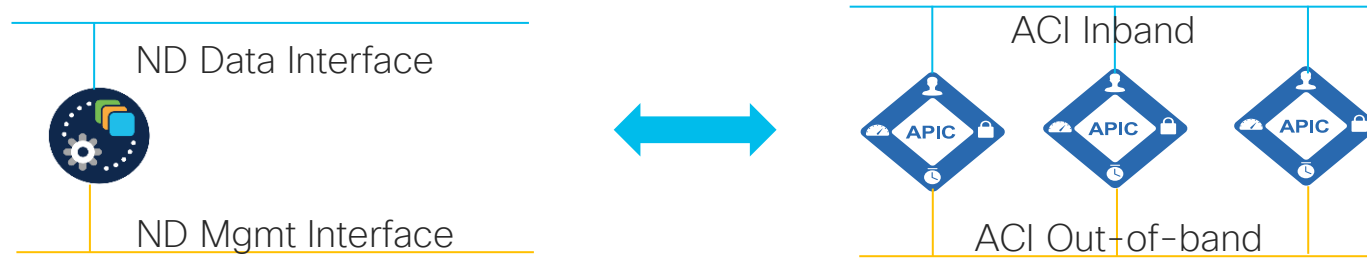
- Depending on the services (NDI/NDO) being deployed on top of vND the number of required nodes and which node type must be deployed as master is changing
- Scale numbers are documented in the ND cluster sizing [tool](#)

Deployed Services	NDI	NDO**	NDI	NDFC***
Total number of nodes needed	3	3	6	3
Type of master nodes	App	APP	DATA	APP
Total number of DATA nodes needed	0	0	3	0
Total number of APP nodes needed	3	3	3	3

** 1 APP node PoC setup for NDO with reduced scale is available

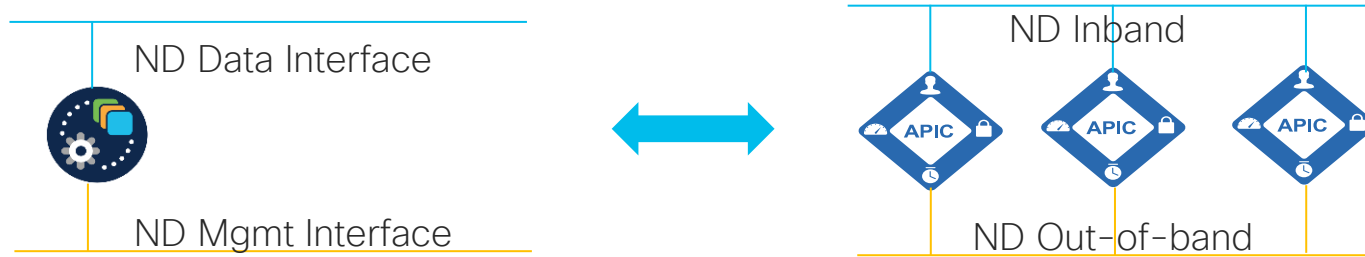
*** 1 APP node PoC setup for NDFC with reduced scale is available

ND to APIC Connectivity Considerations



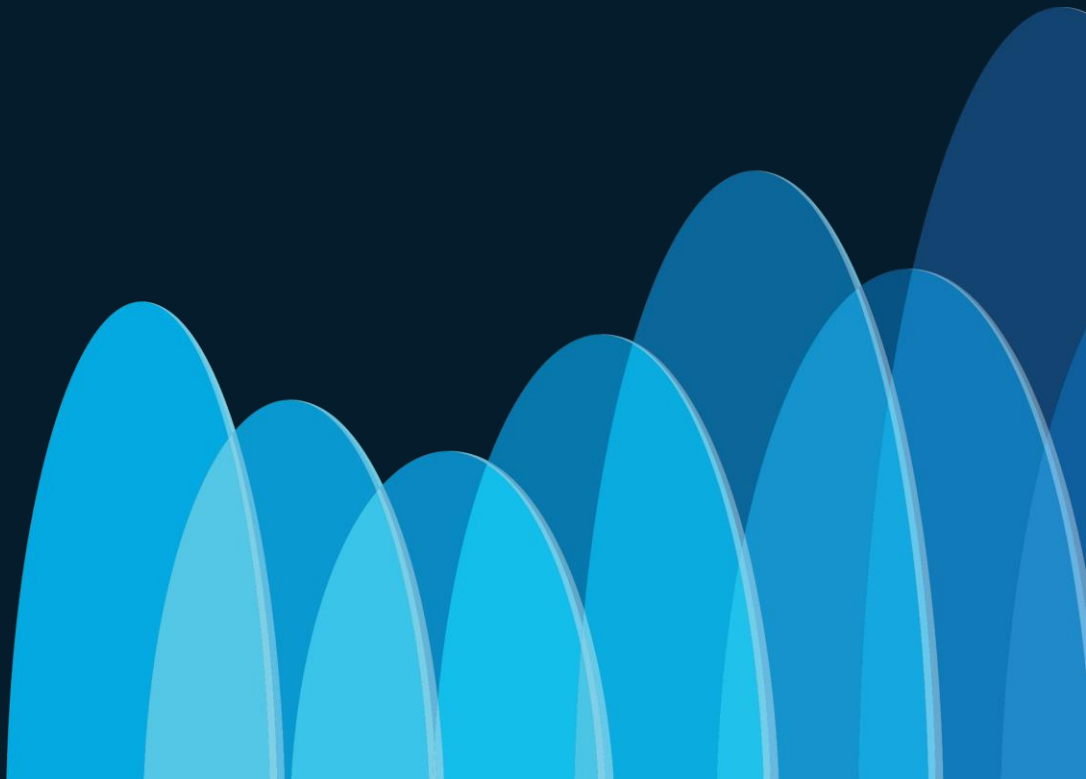
- An ACI fabric is onboarded on ND by specifying the IP address of one of the nodes of the APIC cluster
 - This can be either the APIC's IB or OOB address. In case of the usage of NDI it must be the APIC's IB address
- ND uses the Data Interface to establish the initial connection to that APIC's IP address
 - If the connection is successful, ND discovers all the OOB and IB IP addresses for the other nodes in the APIC cluster

ND to NDFC Connectivity Considerations



- An NDFC site is onboarded on ND by specifying the Inband IP address of the ND hosting the NDFC, no other IP is supported
- ND uses the Data Interface to establish the initial and ongoing connection to that ND Data IP address hosting NDFC

Persistent IPs and their usage



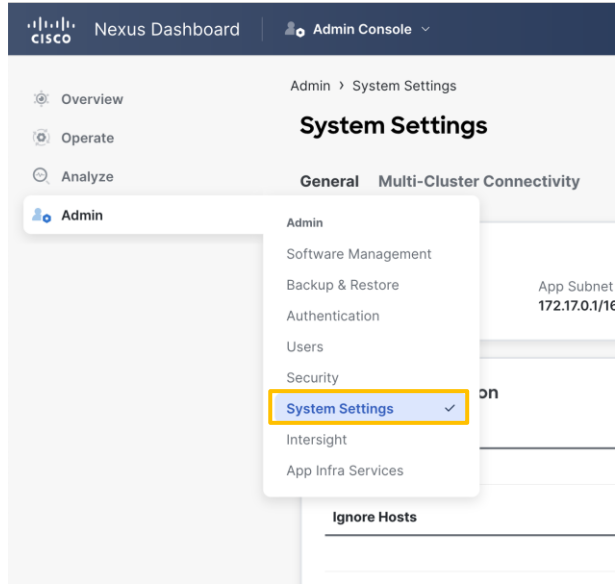
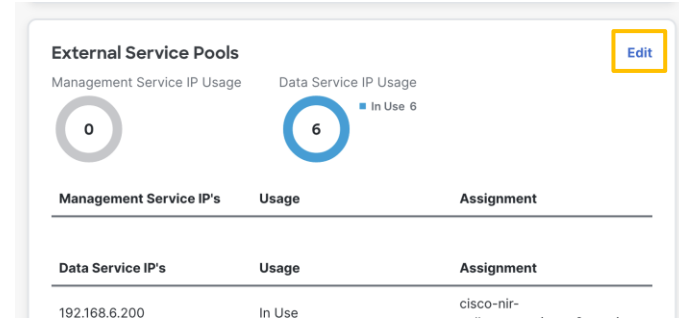
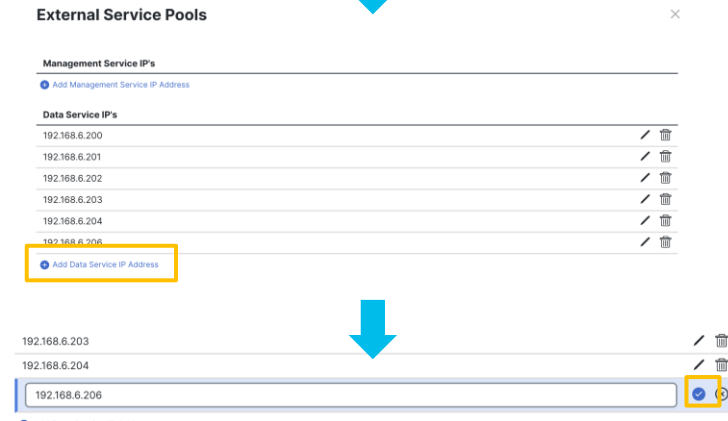
Requirement for persistent IPs

- Nexus Dashboard Cluster Nodes need to be Layer-2 Adjacent on Data Interface
- IPv4 requirements:
 - You need to assign 6 IPs, out of the range of the Data Interface Subnet, Nexus Dashboard Cluster. 3 IP are needed for SW Telemetry receiver and 3 for HW Telemetry.
- IPv6 requirements:
 - You need to assign 7 IPs, out of the range of the Data Interface Subnet, Nexus Dashboard Cluster. 3 IP are needed for SW Telemetry receiver, 3 for HW Telemetry and 1 for Assurance Collector

Persistent IP Pool 1/2

- Is needed to assign persistent IPs to Services/Apps
- These IPs are staying the same even the Service/App is moved to another ND Node
- Are entered as host IP addresses under Cluster Configuration->External Service Pools
- Used by NDI and NDFC
 - Only required for the Data Subnet of ND

Persistent IP Pool 2/2



Apps	Mgmt Interface	Data Interface	Persistent IPs	Support for Data and Mgmt in the same Subnet**
NDFC	L2 adjacent	L2 adjacent / L3 adjacent with L3 HA	2 IPs in mgmt network (for default settings) or 2 IPs data network (for POAP etc. via data network) + 1 IP per fabric for EPL in data network	no
NDI for NDFC based Sites	L3 adjacent	L2 adjacent	6 IPs in data network (+1 for IPv6)	no
NDI for ACI based Sites	L3 adjacent	L2 Adjacent	-/-	yes
NDI with SFLOW/Netflow function	L3 adjacent	L2 adjacent	6 IPs in data interface network*	no
NDO	L3 adjacent	L3 adjacent	-/-	yes

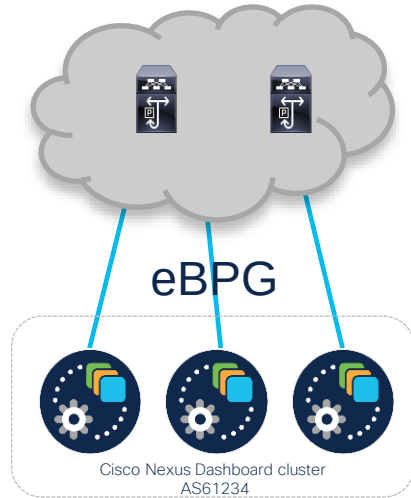
* if NDI is for DCNM no additional IPs are needed.

** supported but not recommended

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

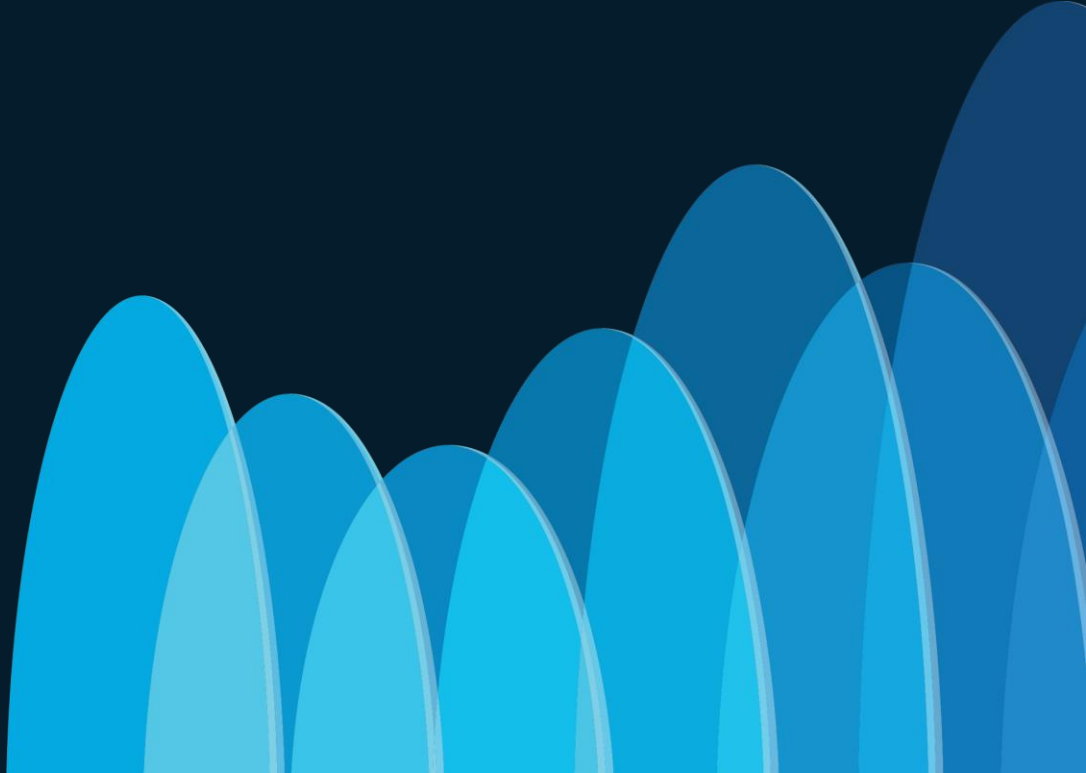
eBGP Peering with Network



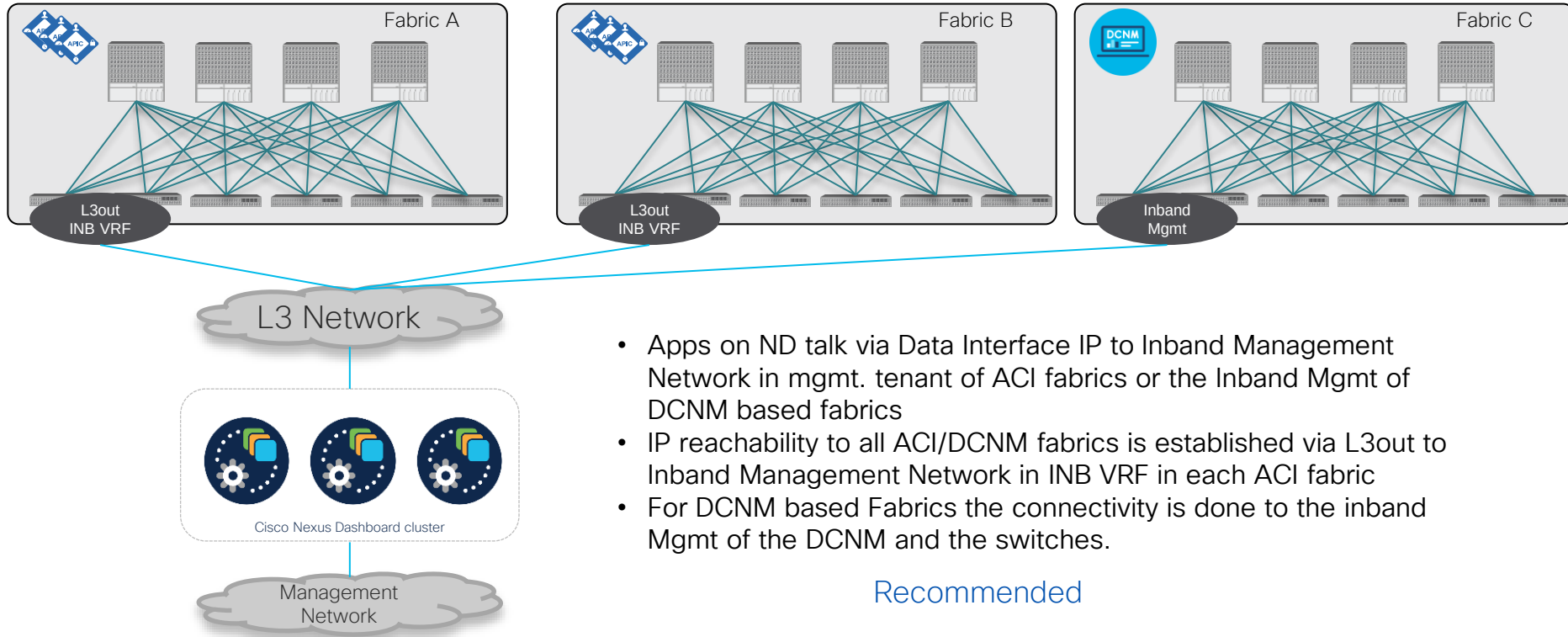
↑
Reachability of
Persistent IPs per
ND Node

- 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.

Attaching ND to your Network



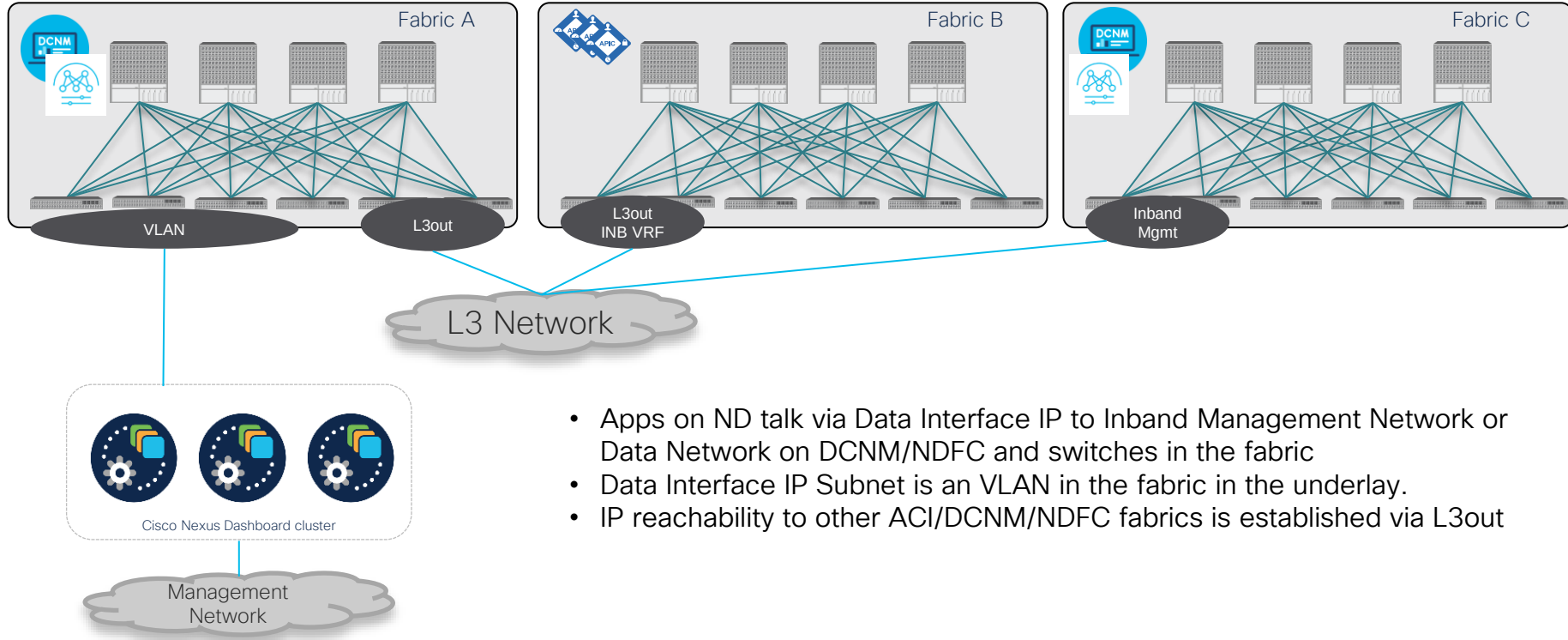
ND Cluster attached to any Networking Infra



- 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.

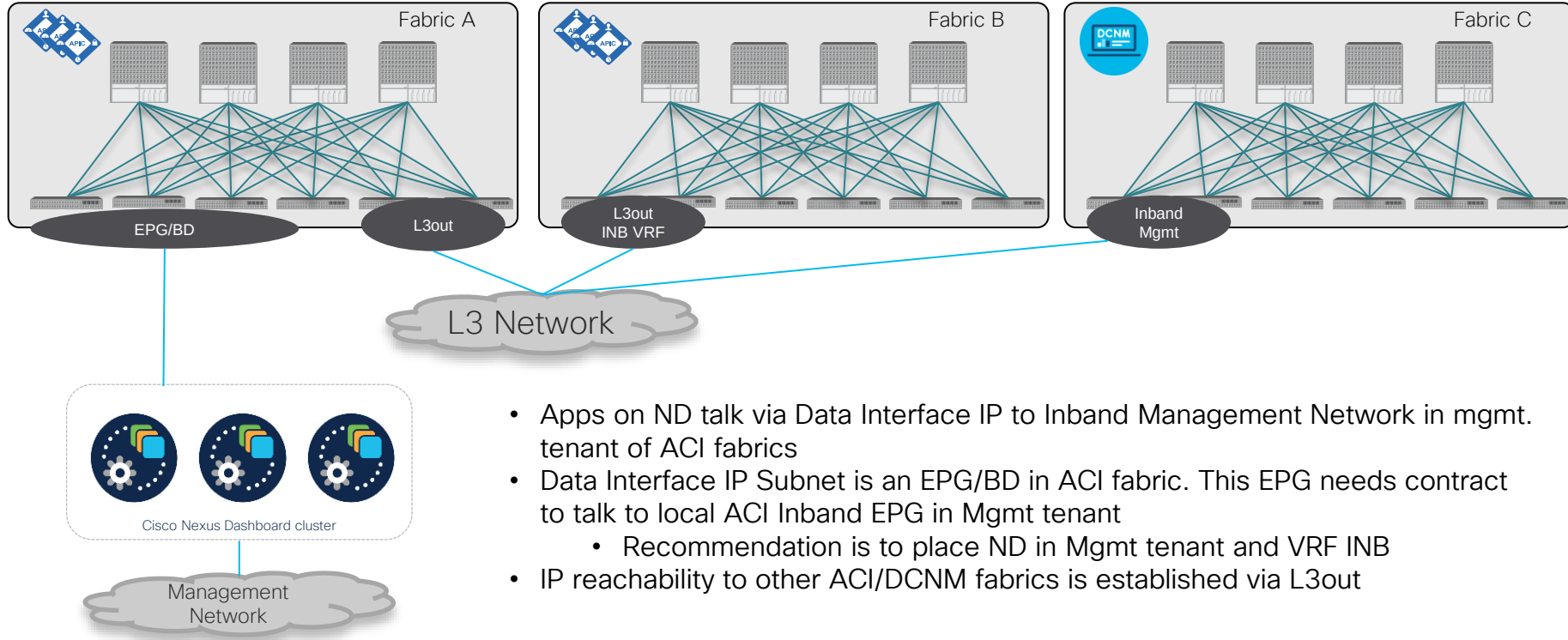
Recommended

ND Cluster attached to DCNM/NDFC based Fabric



- Apps on ND talk via Data Interface IP to Inband Management Network or Data Network on DCNM/NDFC and switches in the fabric
- Data Interface IP Subnet is an VLAN in the fabric in the underlay.
- IP reachability to other ACI/DCNM/NDFC fabrics is established via L3out

ND Cluster attached to ACI Fabric



- Apps on ND talk via Data Interface IP to Inband Management Network in mgmt. tenant of ACI fabrics
- Data Interface IP Subnet is an EPG/BD in ACI fabric. This EPG needs contract to talk to local ACI Inband EPG in Mgmt tenant
 - Recommendation is to place ND in Mgmt tenant and VRF INB
- IP reachability to other ACI/DCNM fabrics is established via L3out

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

Pro

- Easy connection between ND and Inband Management of ACI fabric

Contra

- ND cluster is tied to a single fabric
- Reachability to other sites/fabrics has to go via L3out
- ND cluster relies on single ACI fabric

Pro/Contra of connecting to any Networking Infra

Pro

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

Contra

- All communications between ACI Apps on ND need to go via L3out

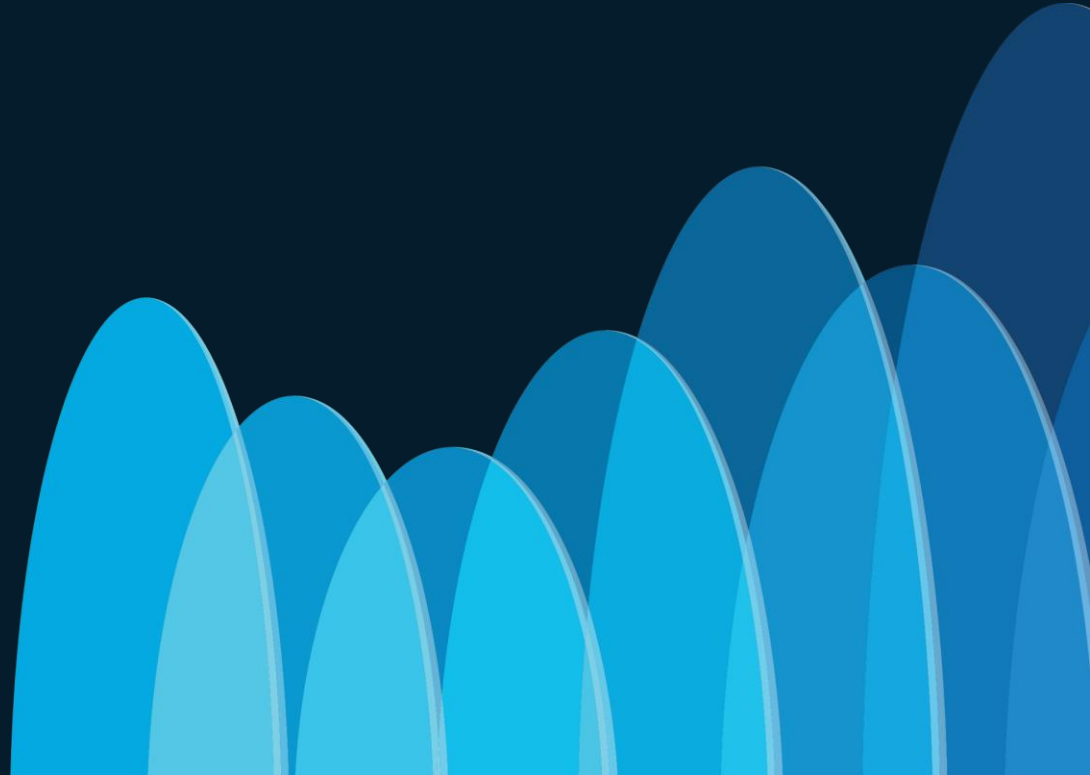
When Centralised or Distributed/Stretched Cluster

Centralised	Distributed/Stretched
<ul style="list-style-type: none">- With NDI/NDFC deployed	<ul style="list-style-type: none">- For redundancy/DR for NDO
<ul style="list-style-type: none">- NDI do not gain any better redundancy with distribute/stretched clusters. You more likely expose the cluster to interconnection failures with a distributed/stretched cluster	
<ul style="list-style-type: none">- Synchronisation traffic is kept between the ND nodes and only telemetry traffic is streamed via WAN	
<ul style="list-style-type: none">- Same traffic path for reaching each site	

Recommendations/Best Practice

- Do not connect whenever possible to an ACI Fabric/DCNM based Fabric directly:
 - ND and Apps are relying on a functioning of the fabric, could be impacting during outages or maintenance
 - If you monitor multiple sites the ND cluster is 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 master nodes, you have to re-install the ND cluster.

Placement of Master/Standby Nodes for Distribute/Stretched ND Clusters

(recommended for NDO)

Number of Sites	1	2	3	4	5
1	P1, P2, P3, S1				
2	P1,P2,P3	P1',P2',P3'			
3	P1	P2	P3		
4	P1	P2	P3	S1	
5	P1	P2	P3	S1	

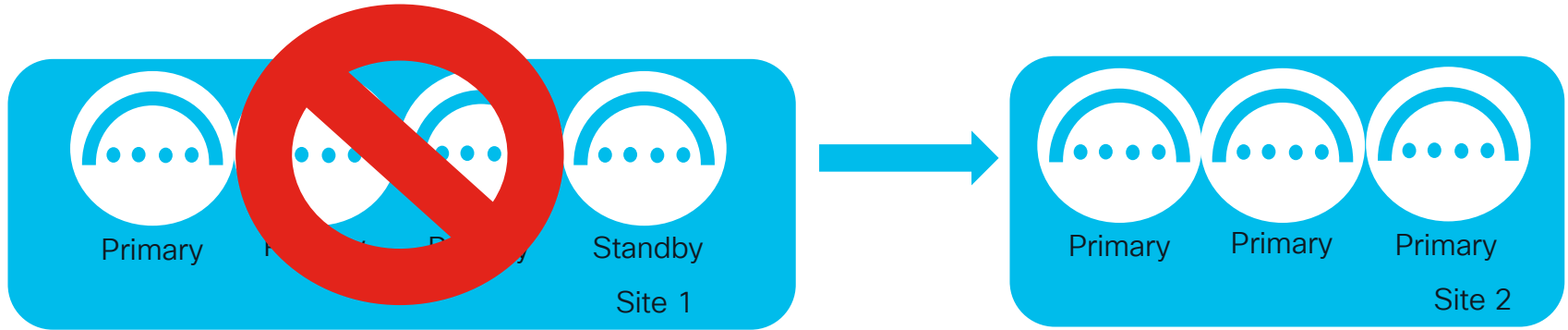
P1, P2, P3
S1

: ND Primary Nodes
: ND Standby Node

P1', P2', P3'

: ND Primary Nodes in a “standby” Cluster

DR and HA for 2 Sites



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

1. Customer brings up ND cluster (either physical ND or virtual ND, needs to match same scale)
2. Applies latest Backup
3. Synchronises Sites

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 <50ms
 - NDO : to APIC <500ms, to DCNM <50ms, between ND/NDO nodes <50ms
 - NDI: between ND/NDI nodes <50ms, to APIC/Fabric <50ms
 - NDFC: between ND/NDFC nodes <50ms, to Fabric <50ms (<200ms if no PoAP is used)
- Always select the lowest common denominator.
 - E.g. NDI and NDO co-hosted : between ND nodes <50ms, to APIC/Fabric <50ms

Deployment Requirements

- Customer has more than 1 Site
 - Number of ND clusters is driven by number of switches and combination of apps
 - Location of the ND clusters is driven by type of the apps:
 - NDO: cluster should be distributed for HA/DR reasons
 - NDI, NAE: cluster can be distributed, but should be placed close to source of telemetry data
 - Always keep virtual ND for NDO in consideration, to satisfy the HA/DR requirement
 - Please check the sizing calculator for ND for the supported apps and scale on CCO

Some Deployment Considerations 1/2

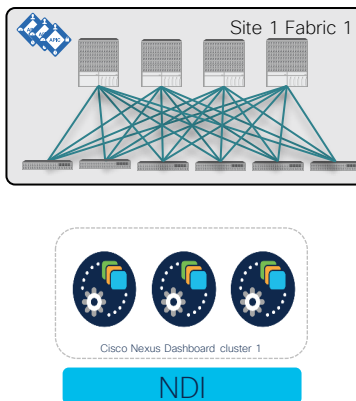
- Try to keep the potential points of failure for reachability between the ND nodes as low as possible.
- When distributing a ND cluster
 - ND Data and Mgmt interface of ND nodes can be in different subnets. Only IP connectivity is needed. (Please allow ports listed in documentation)!
 - L2 adjacency is needed for NDI

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 NDO!
- Data Interface IPs, have to be different from INB EPG subnet of ACI, when ND cluster is connected to ACI fabric
- All communication of Apps hosted on ND is initiated via Data Interface IPs

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

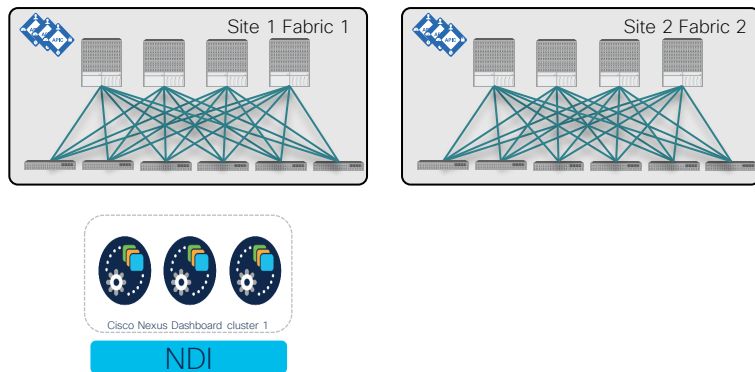
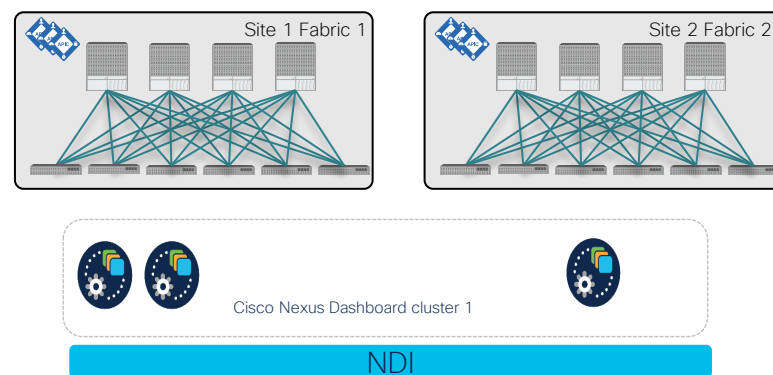
- Single cluster (x number of nodes, cluster connected to either ACI fabric or legacy infra with IP reachability)



Option 2: 1+ Site (below 500 nodes) NDI

- 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)

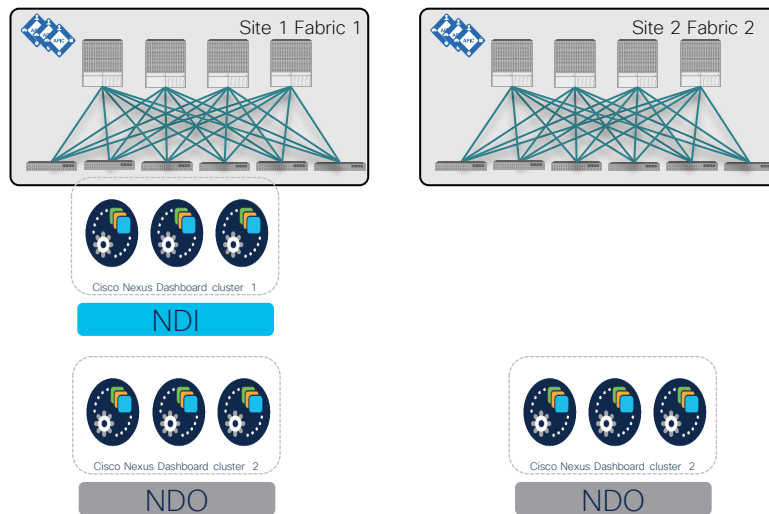
Recommended



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

- 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 NDO to meet HA/DR requirements

Recommended

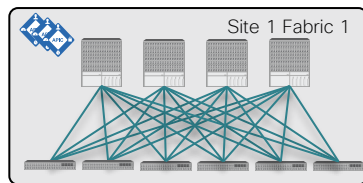
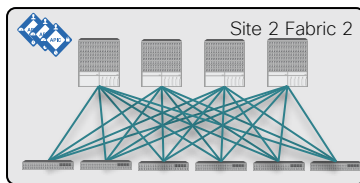


Standby cluster

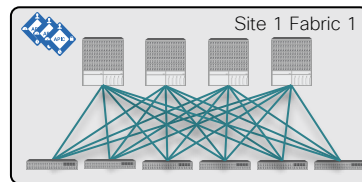
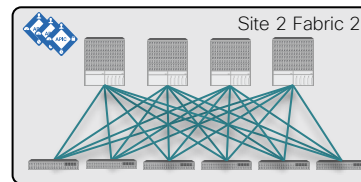
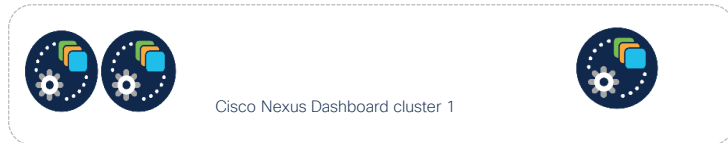
Option 3b: 1+ Site (below 500 nodes) NDI and NDO

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

Not recommended as NDI is distributed, consider vND for NDO (Option 3a)

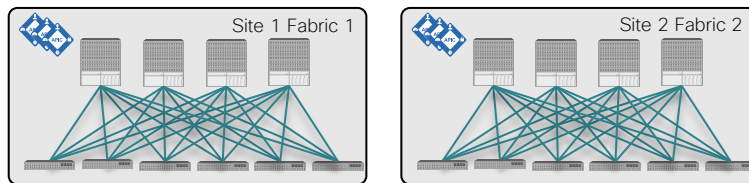


Standby



Option 4: 1+ Site (above 500 nodes) NDI and NDO

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



Recommended



Cisco Nexus Dashboard cluster 1

NDI



Cisco Nexus Dashboard cluster 2

NDI



Cisco Nexus Dashboard cluster 3

NDO



Cisco Nexus Dashboard cluster 4

NDO

Standby

Operating Nexus Dashboard



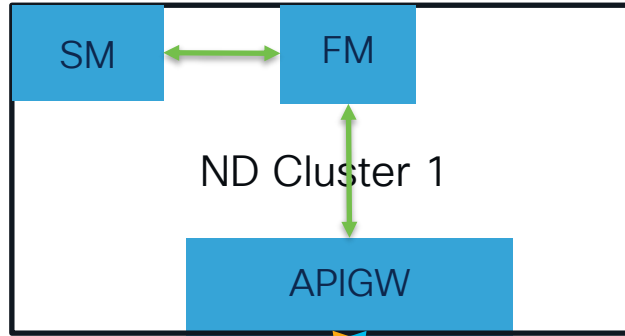
OneManage aka as ND Federation

Overview

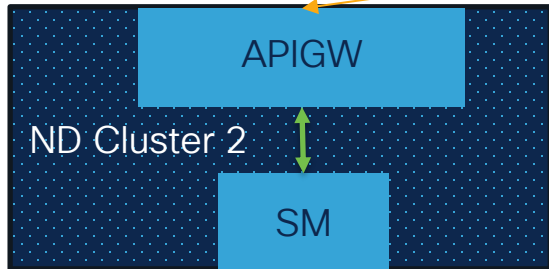
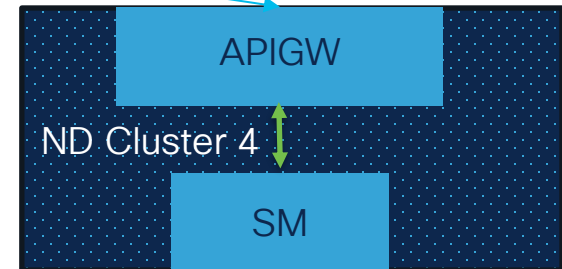
- ND OneManage is an association of several ND clusters that allows working across with them as if they were a single entity and simplify the consumption of their resources
- ND clusters onboard other ND clusters creating a trusted environment which allows to learn about those clusters and to communicate 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.
- Apps can query for information related to other clusters in the federation for purposes such as onboarding (for eg NDI/Sites) or grouping
- [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.

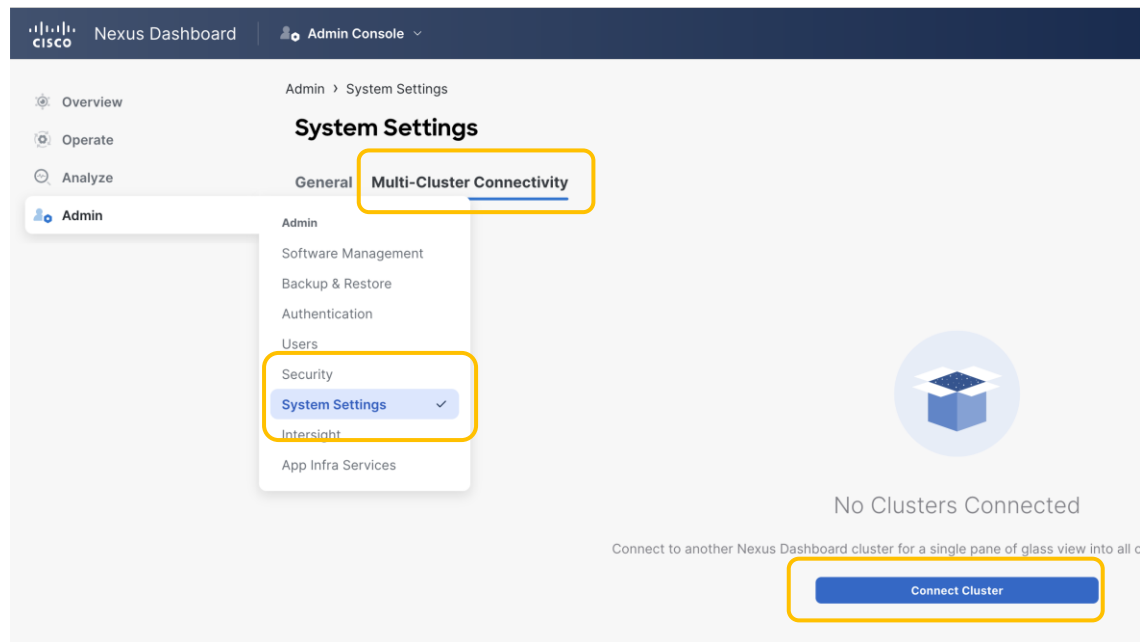


- FM uses Site Managers (SM) on all ND clusters to replicate this information for local queries/display
- APIGW is used to sync keys (for accessing data) between federation members



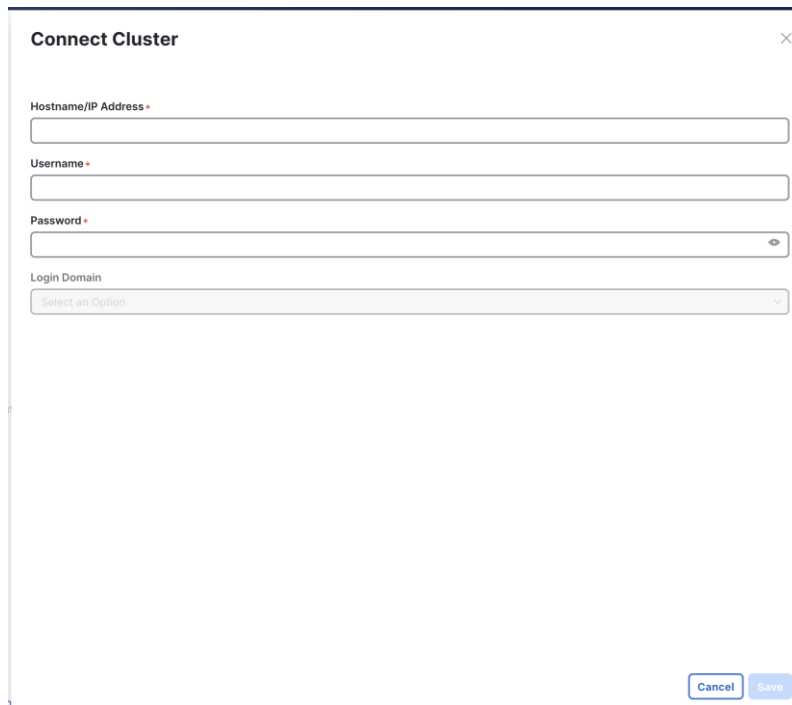
Onboard Clusters (OneManage Configuration)

- Expand the Infrastructure menu
- Select Cluster Configuration
- Go to the Multi Cluster Connectivity tab
- Click “Connect Cluster”



Onboard Clusters (OneManage Configuration)

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



The screenshot shows a web-based configuration window titled "Connect Cluster" with a close button (X) in the top right corner. The window contains four input fields: "Hostname/IP Address", "Username", "Password" (with a toggle icon), and "Login Domain" (a dropdown menu). At the bottom right, there are "Cancel" and "Save" buttons.

Connect Cluster ✕

Hostname/IP Address *

Username *

Password *

Login Domain

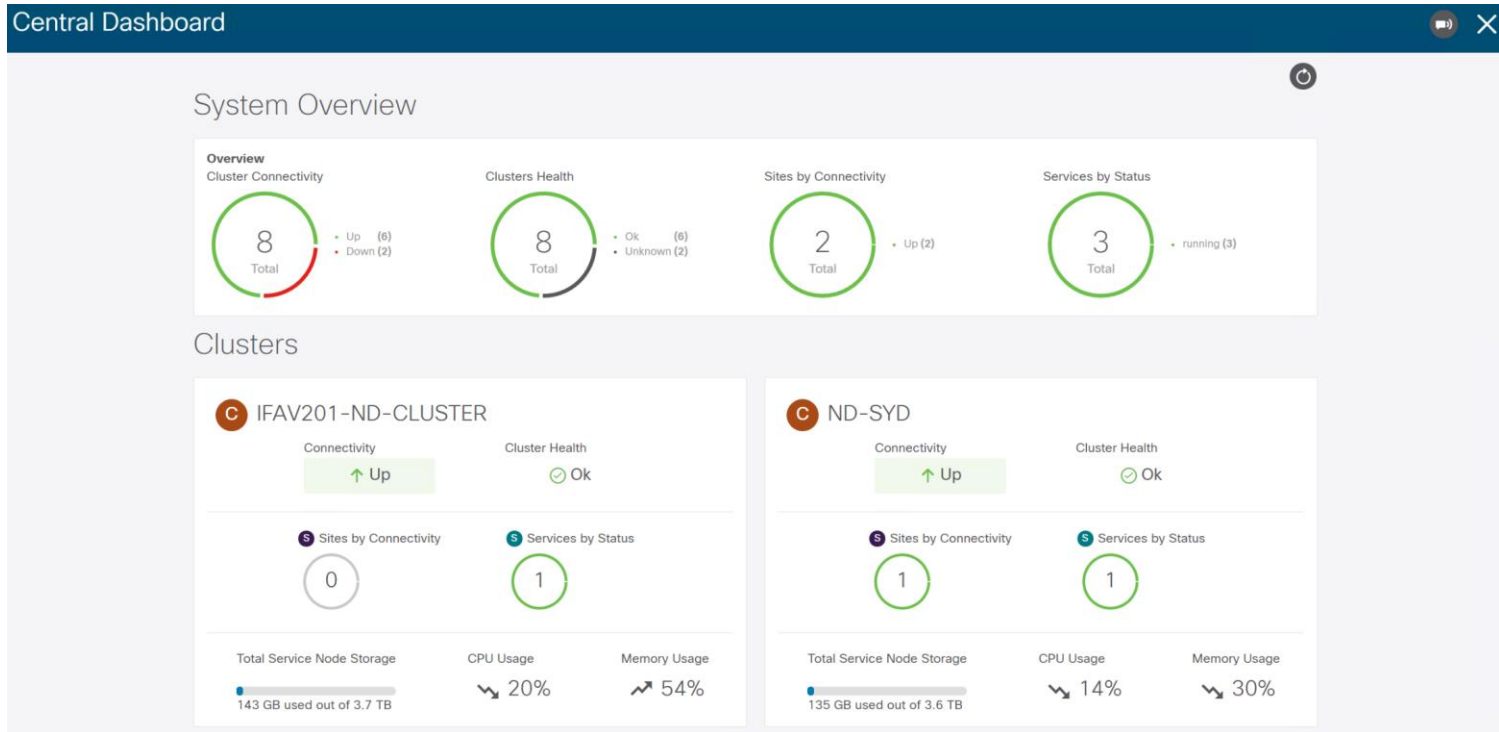
Select an Option

Cancel Save

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 FM are marked in the list

Central Dashboard

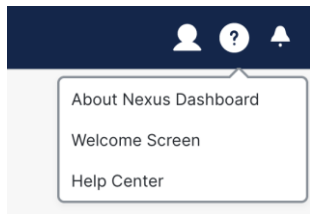


Public API

Overview

- API publicly available
- Swagger built-in
- Apps onboarded to ND populate their APIs there as well (e.g. NDI)

API UI



Learn, explore, and find the links to resources for Nexus Dashboard

What's New in 3.0(1)?

[View Release Notes](#)

Deployment

After your cluster is up and running, check out some of the resources to prepare for when it's time for the next upgrade.

[Rare Setup Guide for UCS C220 M5](#)

[Rare Setup Guide for UCS C225 M6](#)

[Deployment Guide](#)

[Capacity Planning Tool](#)

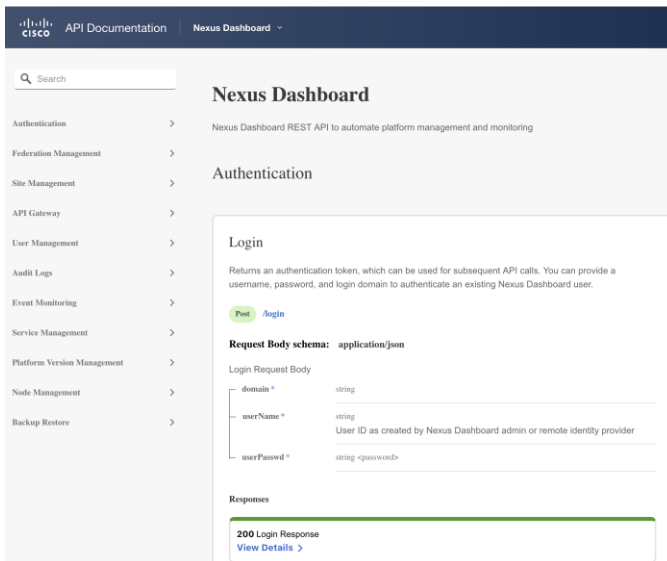
[Hardware Compatibility Matrix](#)

Programming

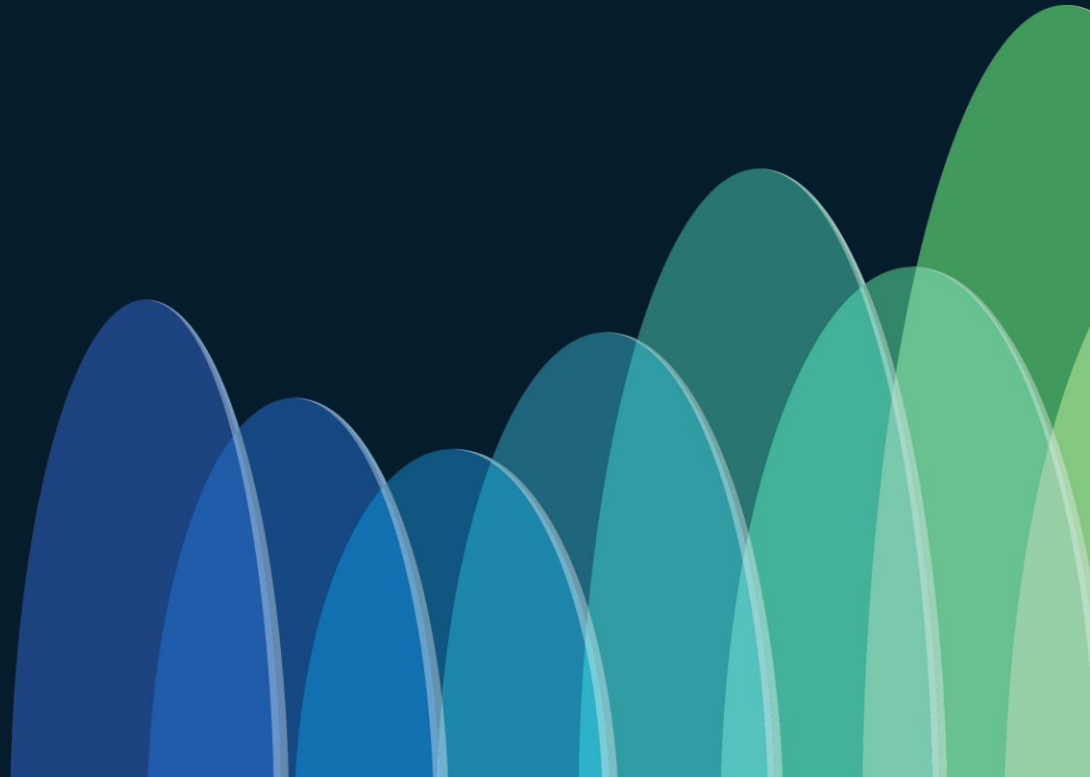
Want to standardize, streamline, and automate deployments at a large scale? The development resources will introduce you to our APIs, object model, and provide simple examples so you can write your own integrations.

[REST API](#)

[Developer Guide](#)



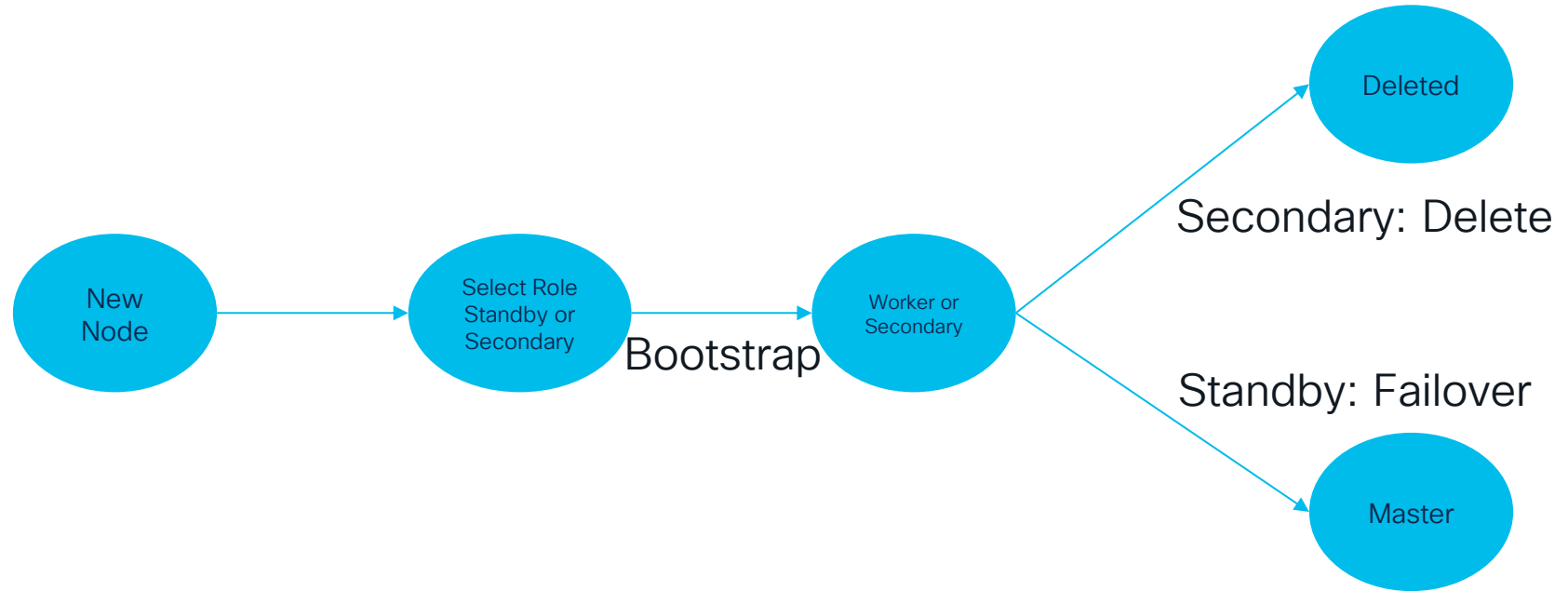
Registering Nodes to existing Cluster and Standby Node



Register new Nodes and Standby Master

- New nodes are discovered via CIMC 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
- Workers can only be replaced by delete and re-add

Lifecycle of non-Primary Nodes



Adding a new Node

Add Node

Deployment Details

CIMC IP Address * ⓘ

Username *

Password *
 [Validate](#)

General

Name *

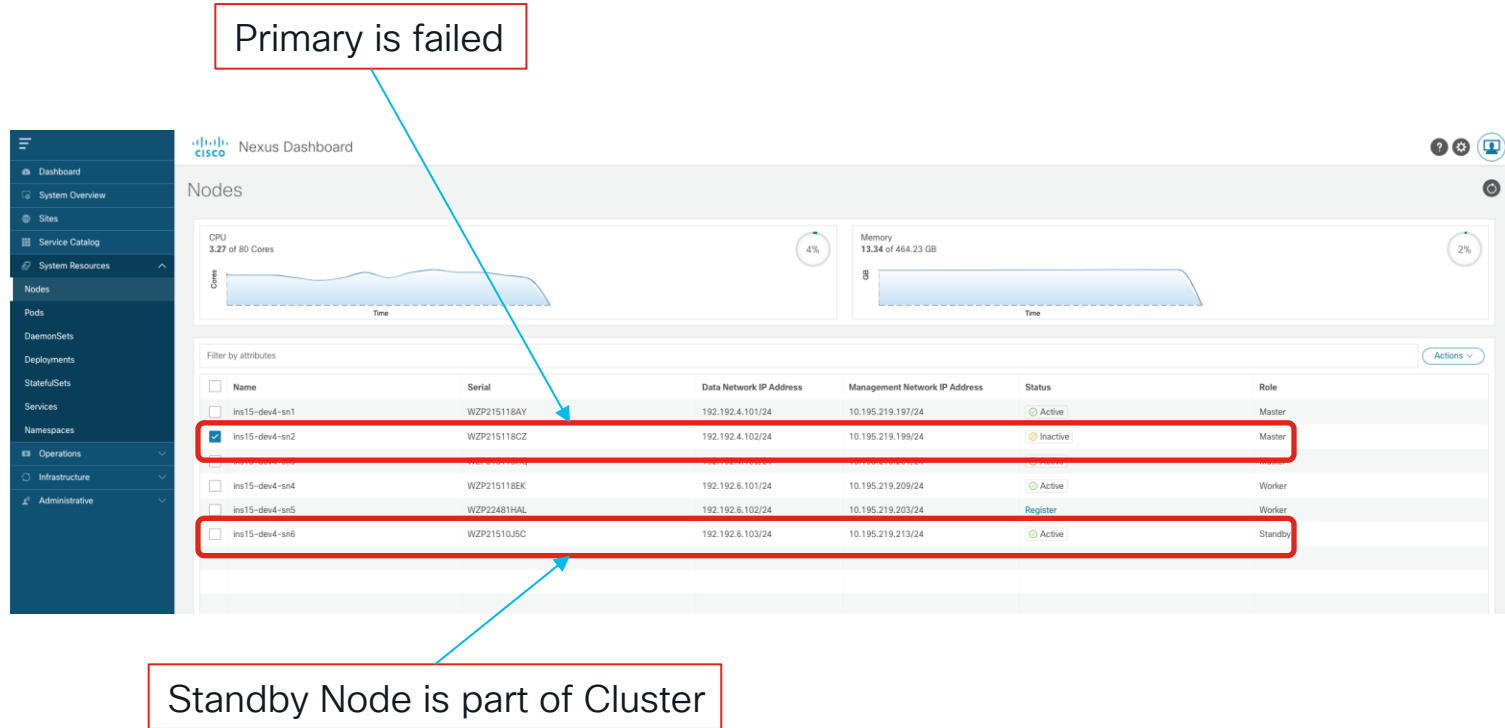
Serial Number *

Type

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



Nodes

CPU 3.27 of 80 Cores 4%

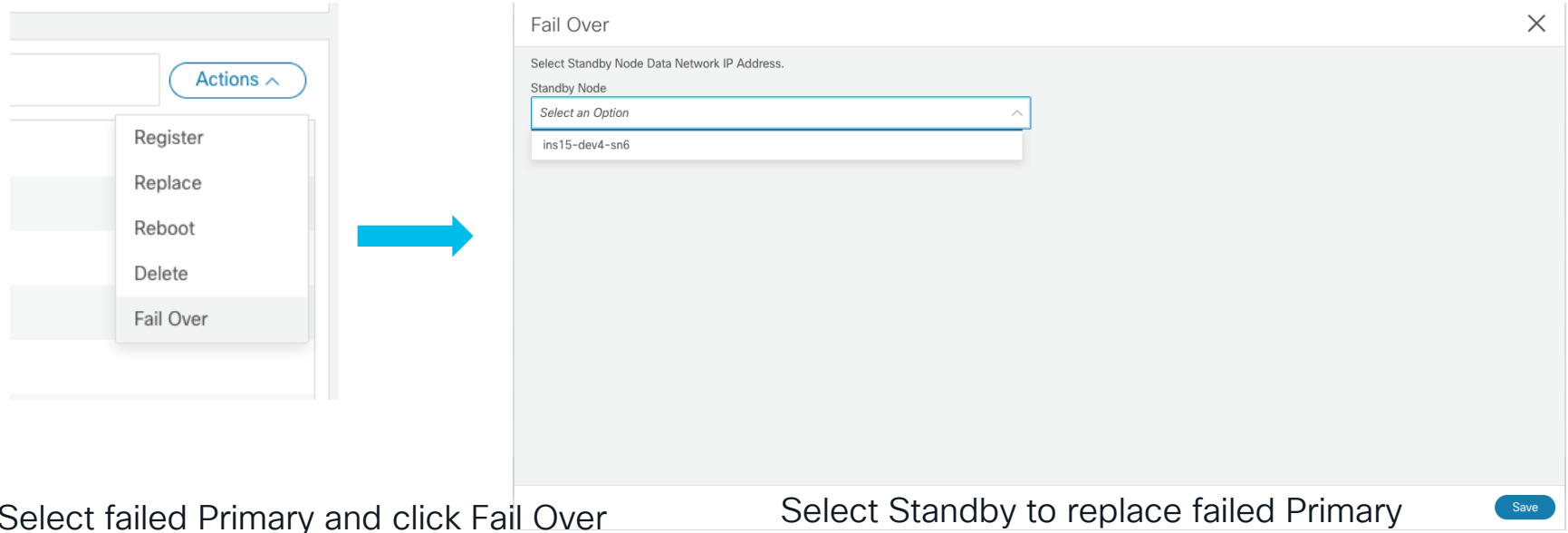
Memory 13.34 of 464.23 GB 2%

Filter by attributes

Name	Serial	Data Network IP Address	Management Network IP Address	Status	Role
☐ Ins15-dev4-sn1	WZP215118AY	192.192.4.101/24	10.195.219.197/24	Active	Master
☒ Ins15-dev4-sn2	WZP215118CZ	192.192.4.102/24	10.195.219.199/24	Inactive	Master
☐ Ins15-dev4-sn3	WZP215118EK	192.192.6.101/24	10.195.219.209/24	Active	Worker
☐ Ins15-dev4-sn4	WZP215118EK	192.192.6.101/24	10.195.219.209/24	Active	Worker
☐ Ins15-dev4-sn5	WZP22481HAL	192.192.6.102/24	10.195.219.203/24	Register	Worker
☐ Ins15-dev4-sn6	WZP215110JC	192.192.6.103/24	10.195.219.213/24	Active	Standby

Standby Node is part of Cluster

Failover to Standby



The diagram illustrates the failover process in two steps. On the left, a menu with the title 'Actions ^' contains the options: Register, Replace, Reboot, Delete, and Fail Over. A blue arrow points from the 'Fail Over' option to a 'Fail Over' configuration window on the right. The window has a title bar with a close button (X) and a subtitle 'Select Standby Node Data Network IP Address.' Below this, there is a 'Standby Node' section with a dropdown menu. The dropdown menu is open, showing 'Select an Option' at the top and 'ins15-dev4-sn6' as the selected option. At the bottom right of the window is a blue 'Save' button.

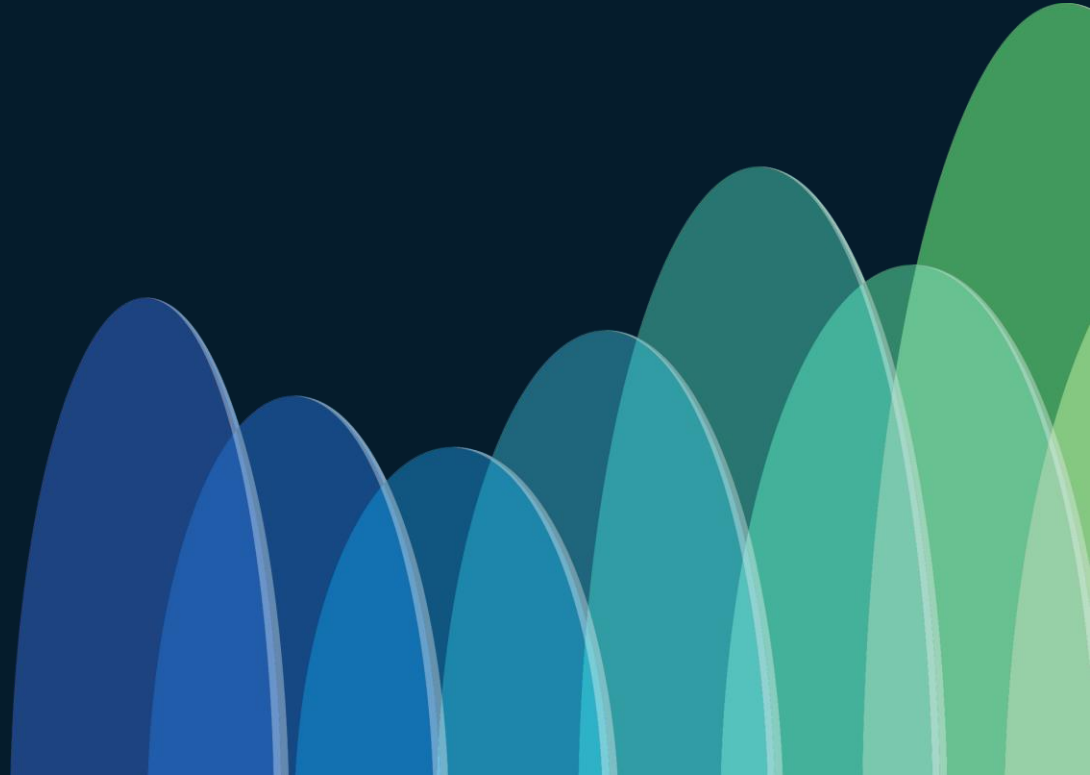
Select failed Primary and click Fail Over

Select Standby to replace failed Primary

Save

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

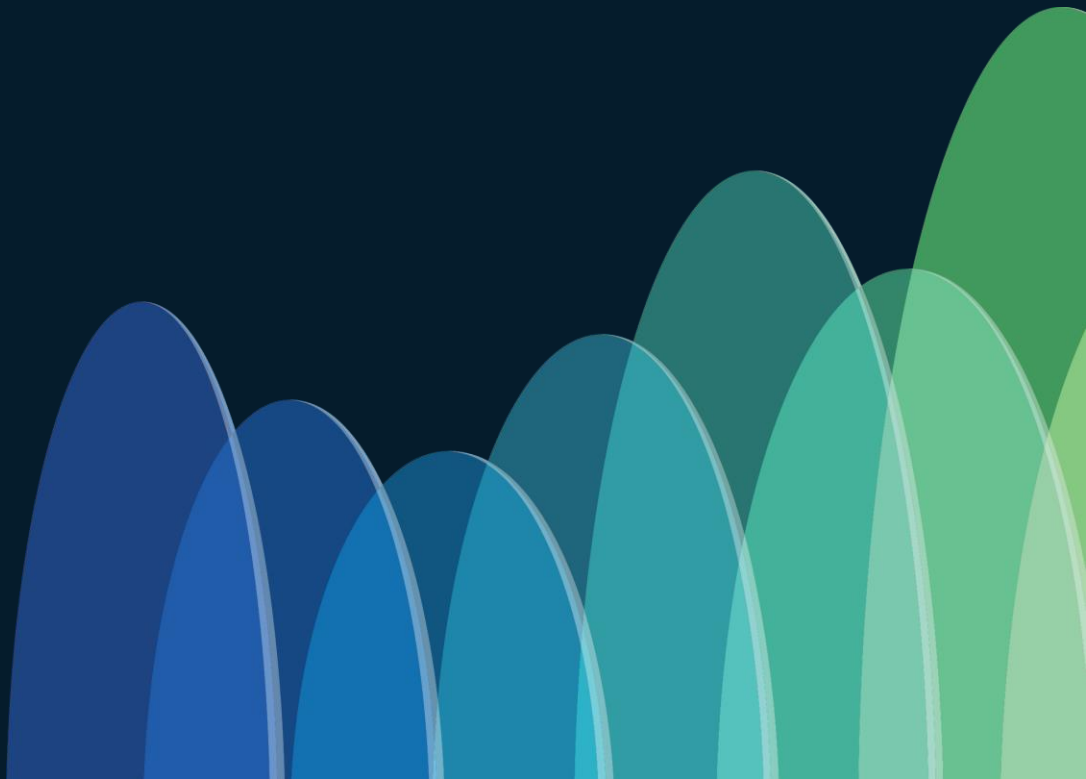
Recovery Process of a virtual ND



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



Firmware Upload

The screenshot shows the Cisco Nexus Dashboard Admin Console. The top navigation bar includes the Cisco logo, 'Nexus Dashboard', and 'Admin Console'. The left sidebar has tabs for 'Overview', 'Operate', 'Analyze', and 'Admin'. The 'Admin' tab is selected, and a dropdown menu is open, showing 'Software Management' as the active item. The main content area is titled 'Software Management' and has a sub-tab 'Images' which is highlighted with a red box. A red arrow points from a text box above to the 'Images' tab. The text box contains the instruction: 'Click in Images first to upload a firmware'. Below the 'Images' tab, there is a table with columns 'Number of Nodes' and 'Last Update'. The 'Number of Nodes' column shows the value '5'. The 'Last Update' column shows the date and time '2023-09-26, 05:35:33'. A 'Refresh' button is located in the top right corner of the main content area.

Click in Images first to upload a firmware

Nexus Dashboard | Admin Console

Admin > Software Management

Software Management

Updates Images

Admin

Software Management ✓

Backup & Restore

Authentication

Users

Security

System Settings

Intersight

App Infra Services

Number of Nodes

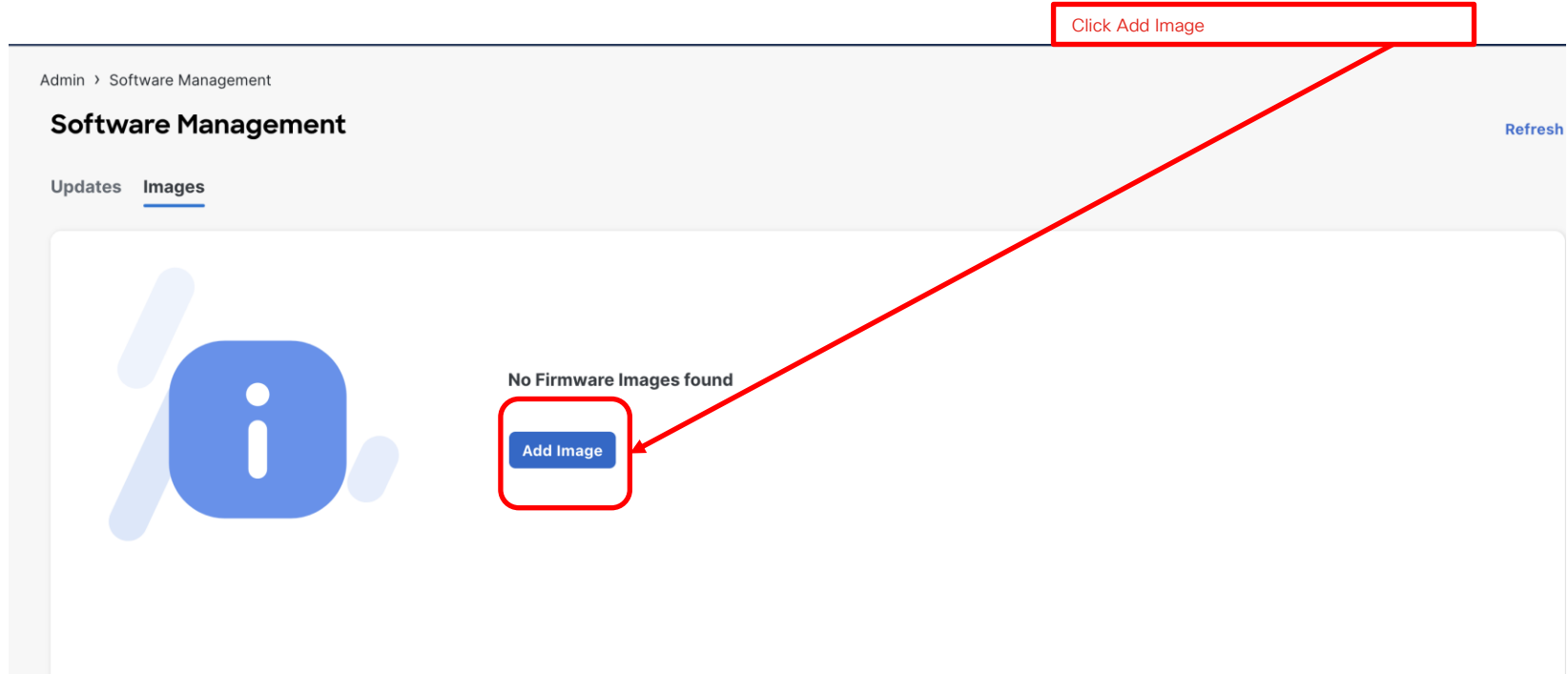
5

Last Update

2023-09-26, 05:35:33

Refresh

Firmware Upload



Firmware Upload

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

The image shows a 'Firmware Upload' interface with two overlapping 'ADD SOFTWARE IMAGE' dialog boxes. The background dialog box has the 'Remote' tab selected, showing a 'URL *' field with a placeholder example: 'e.g.: http[s]://IP[:port]/path/filename'. The foreground dialog box has the 'Local' tab selected, showing a 'Browse...' button and the text 'No file selected.'.

ADD SOFTWARE IMAGE [X]

Location

Remote Local

URL *

i e.g.: http[s]://IP[:port]/path/filename

ADD SOFTWARE IMAGE [X]

Location

Remote Local

Browse... No file selected.

Firmware Upload

The screenshot shows the Cisco Nexus Dashboard Admin Console. The top header includes the Cisco logo, 'Nexus Dashboard', and 'Admin Console'. The sidebar on the left has navigation links: Overview, Operate, Analyze, and Admin. The main content area is titled 'Software Management' and has tabs for 'Updates' and 'Images'. The 'Images' tab is active, showing a table of software images. The table has columns for 'File Name', 'Status', and 'Version'. One image is listed: 'nd-dk9.3.0.1i.iso' with a status of 'Downloaded' and version '3.0(1i)'. There are buttons for 'Filter by attributes', 'Add Image', 'Modify Details', and 'Refresh'.

File Name	Status	Version
nd-dk9.3.0.1i.iso	Downloaded	3.0(1i)

Setup Firmware Upgrade

The screenshot shows the Cisco Admin Console interface for Software Management. The top navigation bar includes 'Admin Console' and user icons. The breadcrumb trail is 'Admin > Software Management'. The main heading is 'Software Management' with a 'Refresh' button. Below this are tabs for 'Updates' (selected) and 'Images'. The 'Node Details' section displays a table with the following data:

Current Firmware Version	Number of Nodes	Last Update
3.0(1i)	5	2023-09-26, 05:35:33

Below the table, a message states 'There are no Firmware Updates'. A red box highlights the text 'Click to Setup an Upgrade' with a red arrow pointing to a button labeled 'Use the wizard to setup a firmware update.' Below this button is a blue button labeled 'Setup Update'.

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

▼

Install Firmware to Nodes

Firmware Update

Setup

Install

Activate

Complete

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	Target Firmware Version	Number Of Nodes	Last Update
2.0.0.71a	2.0.0.71b	3	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

Running

Update Details

Current Firmware Version

1.1.2.144

Target Firmware Version

1.1.2.152

Number Of Nodes

3

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

Cancel

Once Install is done Click Activate

The screenshot shows the 'Firmware Update' interface with a progress bar at the top indicating the stages: Setup, Install (active), Activate, and Complete. Below the progress bar, a message states: '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'.'

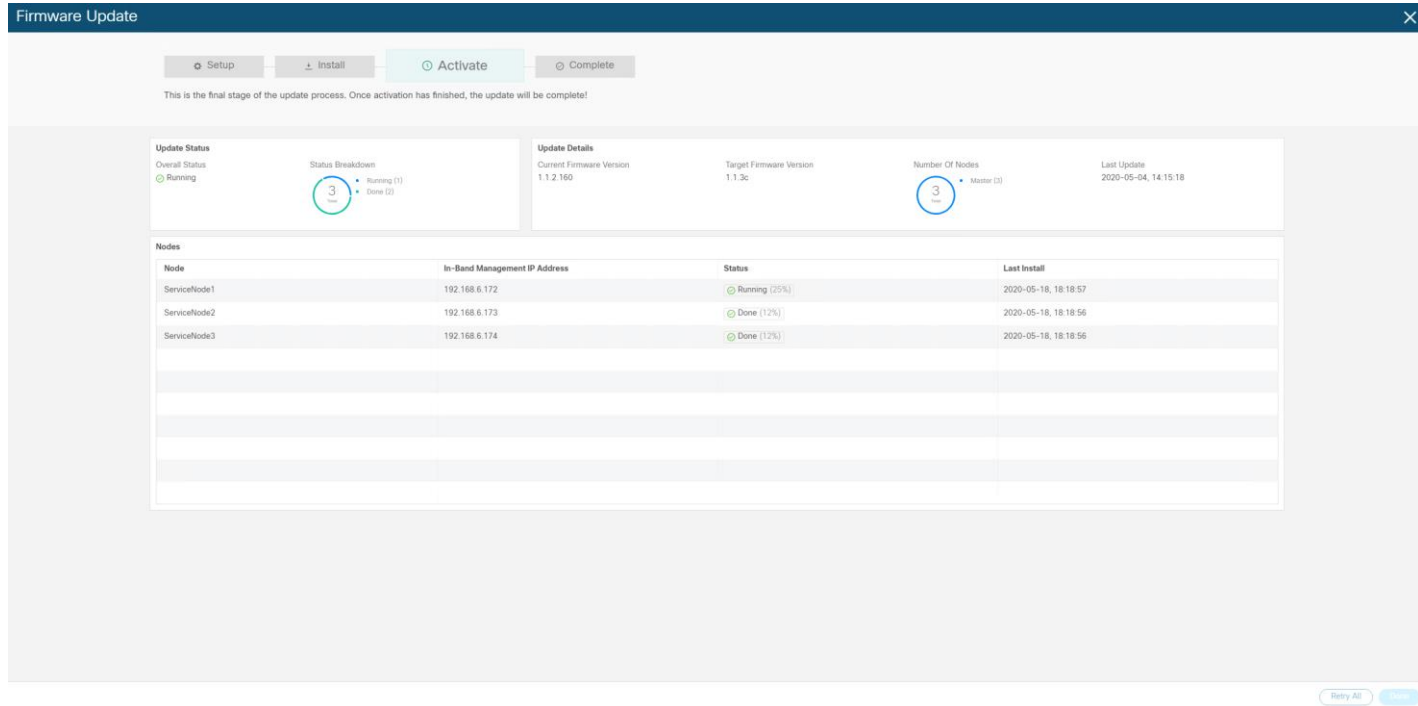
The 'Update Status' section shows the overall status as 'Ready to Activate' and a status breakdown of 3 nodes, all 'Done (3)'. The 'Update Details' section shows the current firmware version as 1.1.2.160 and the target firmware version as 1.1.3c. The number of nodes is 3, with 3 Master nodes. The last update was on 2020-05-04, 14:15:18.

The 'Nodes' table lists the nodes and their status:

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

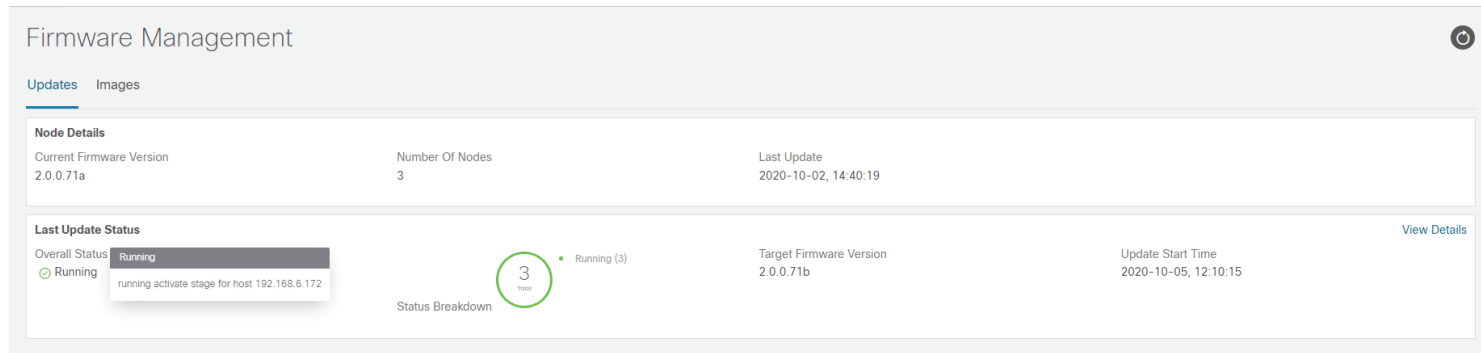
At the bottom right, there is a 'Retry All' button and an 'Activate' button, which is highlighted with a red box.

Activation Progress



Monitoring Firmware Upgrade

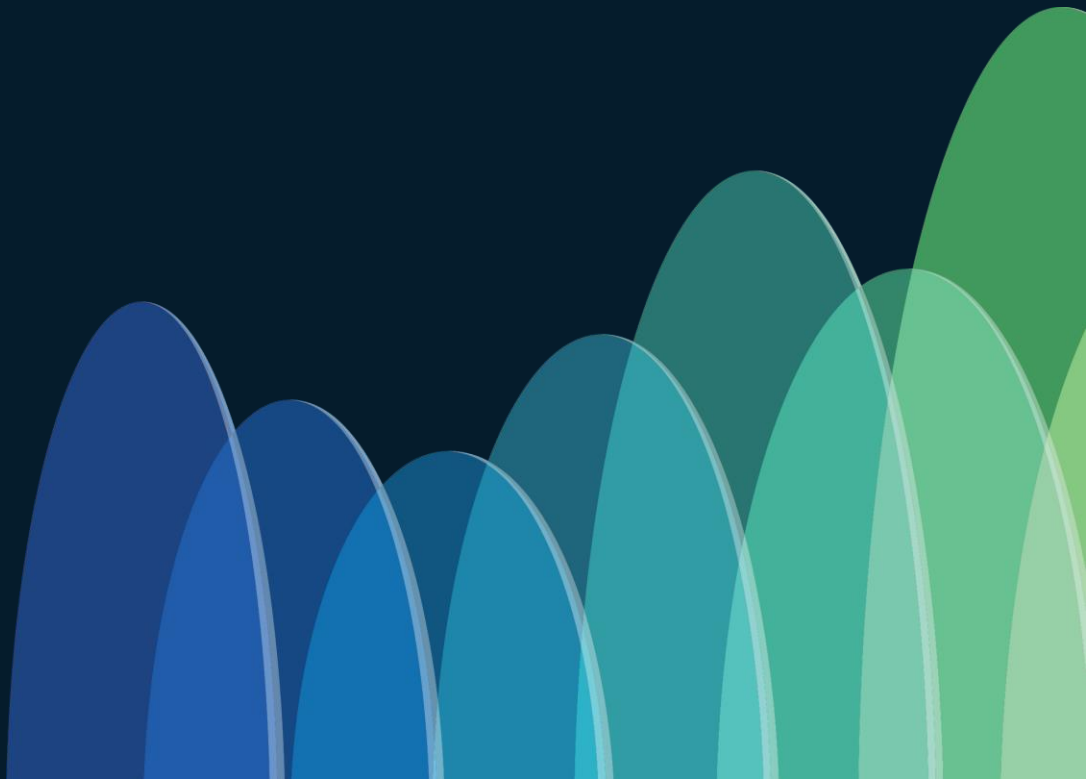
- When the node you are connected to is activating, it will disconnect you. Please connect to another SE node. Check status via:



- Node going through an update will display:

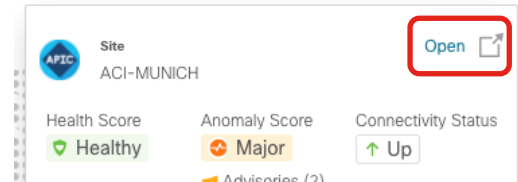
① Current node is going through upgrade, any configuration change during upgrade will not work. [More Info](#)

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 and later, 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 3.0(1)

Username

Password

Login

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

©2023 Cisco Systems, Inc.



Welcome to Nexus Dashboard

Version 3.0(1)

Username

Password

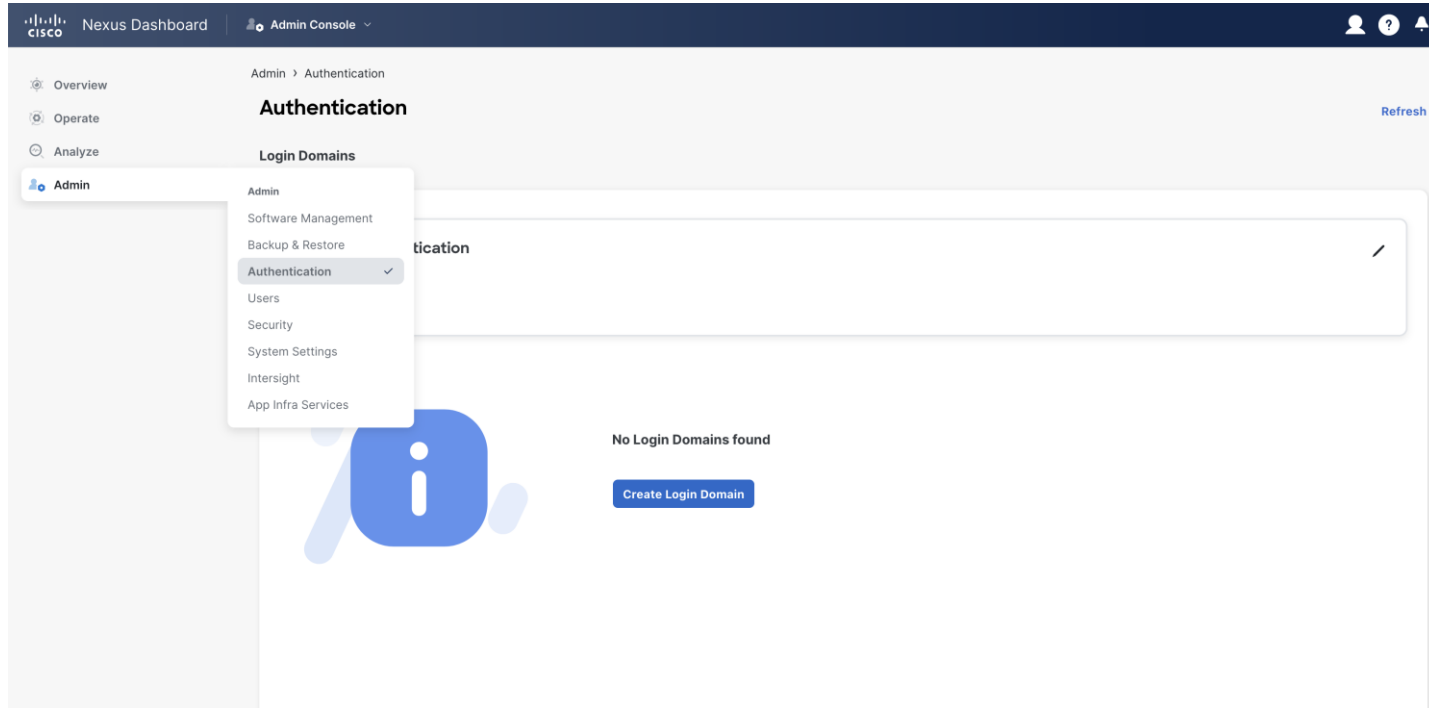
Login Domain

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 3.0(1i)

Username

Password

Login Domain

Login

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

©2023 Cisco Systems, Inc.

RBAC and User Roles 1/2

Administrator — allows access to all objects and configurations. (Dashboard role)

- AV Pair Value: admin

User Manager — allows access to users and authentication configurations. (Dashboard role)

- AV Pair Value: aaa

Dashboard User — allows access only to the Dashboard view and launching applications; does not allow any changes to the Nexus Dashboard configurations. (Dashboard role)

- AV Pair Value: app-user

Site Administrator — allows access to configurations related to the sites on-boarding and configuration. (Dashboard role)

- AV Pair Value: site-admin

Site Manager — allows application user to manage the sites used by that application. (NDO App role)

- AV Pair Value: config-manager

Policy Manager — allows application user to view policy objects. (NDO App role)

- AV Pair Value: site-policy

Tenant Manager — allows application user to view tenants (NDO App role)

- AV Pair Value: tenant-policy

RBAC and User Roles 2/2

- Cisco-avpair is used for RBAC via remote Auth
- AVPAIR format
 - shell:domains=<domain>/<writerole>|<writerole2>/<readrole>|<readrole2>
 - Example
 - All admin access: shell:domains=all/admin/
 - Tenant Mgr, Site Mgr and readonly AAA: shell:domains=all/tenant-policy|site-admin/aaa
- Local Users can be assigned to User roles as well while creating the User

User Roles for Local Users

Add Security Domain and Roles

Domain

Select an Option

Roles

Name	Read Privilege	Write Privilege	Service	Details
Administrator	☐	☐	Nexus Dashboard	i
Approver	☐	☐	Nexus Dashboard	i
Dashboard User	☒	☐	Nexus Dashboard	i
Deployer	☐	☐	Nexus Dashboard	i
Policy Manager	☐	☐	Nexus Dashboard	i
Site Administrator	☐	☐	Nexus Dashboard	i
Site Manager	☐	☐	Nexus Dashboard	i
Tenant Manager	☐	☐	Nexus Dashboard	i
User Manager	☐	☐	Nexus Dashboard	i

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

CISCO *Live!*



Configure Security Settings

Session and Idle Timeout in Seconds

Customer Certificate and Root Certificate, enabled SSL Chiphers etc.

Security Configuration

Timers

Session Timeout (seconds)

1200

Idle Timeout (seconds)

3600

Certificate

Domain Name

*

SSL Chiphers

TLS_ECDHE_RSA_WITH_AES_128_C... X

TLS_ECDHE_RSA_WITH_AES_256_G... X

TLS_ECDHE_ECDSA_WITH_AES_256... X

Cancel

Save

```
[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

Current Deployment Mode



Insights

Settings

Name *

backup1

Type

Config-Only

Full

Destination

Local Download

Local Download

Remote Storage Location

Backups History

Backups Backup Schedules

Filter by attributes

☐	Name	Type	Start time	End time
☐	backup1	Config-Only	2024-09-06, 16:52:52	-

1 items found

Backup Completed

Overall Progress

Progress Details

Type	Description	Progress
Insights		
Backup started		
Elastic backup		
Mongo backup		
Creating backup file		
Backup Complete		
Backup file uploaded	NDI Backup successful	
nd-core		
confd		
federation		
licensemgr		
system		

Creating Periodic Upgrades

Create Backup Schedule



Settings

Name *

daily-config

Type ⓘ

Config-Only Full

Remote Storage Location

scp-server

[View Details](#)

Remote Path Filename * ⓘ

/tmp

Encryption Key *

.....

Scheduler

09/07/24 05:00 pm



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 1/3

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 Backup

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 View Details</div>	backup1.tar.gz	admin	-

1 items found

Rows per page 10

- Delete
- Download
- Restore

Restoring a Backup 2/3

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

[Validate and Upload](#)



Restore a Backup 3/3

Restore from backup1

Source

Upload Configuration Backup File

Encryption Key *

.....

Validation *

File Name

backup1

Progress

[Validate a](#)

Restore

Current Deployment Mode

Insights

Post Restore Deployment Mode

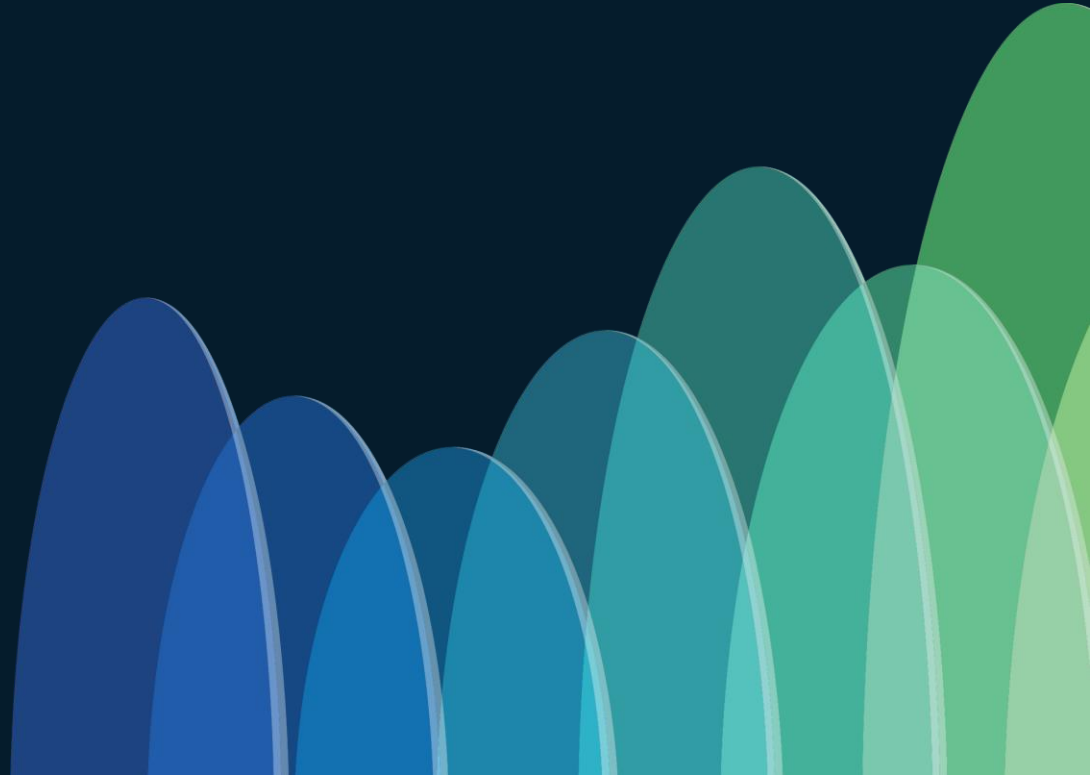
Insights

Type

Config-Only Full

☐ Ignore External Service IP Configuration

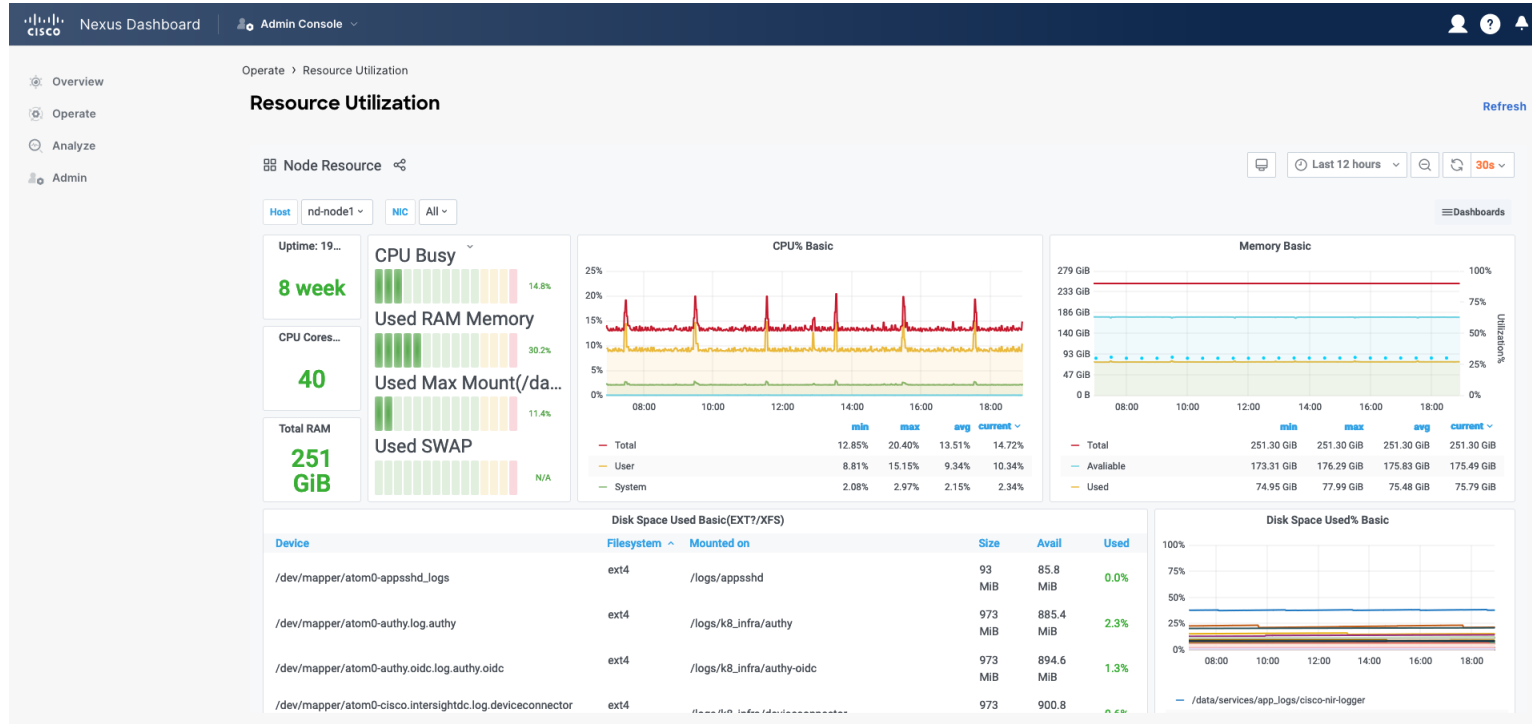
Resource Monitoring



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)

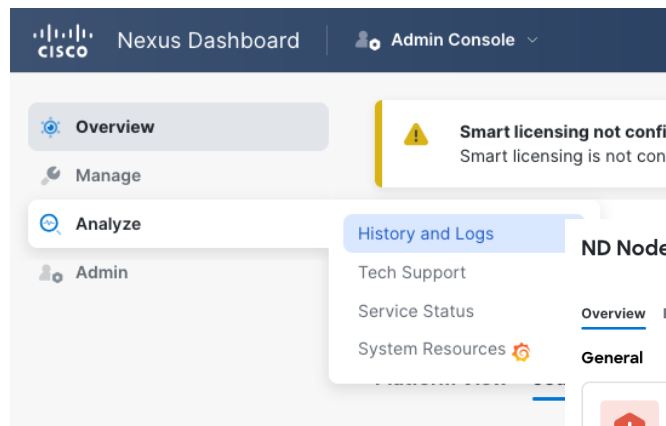
Monitored Entities of ND Cluster (1/2)

- 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 & mgmt) 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



Analyze > History and Logs

History and Logs

Events Audit Logs

Filter by attributes

Severity	Life Cycle	Name	Fault Domain	Age	Description
		backuprestore		30d23h	No backup schedule configured
		server		11d12h	Network device mgmt1 in node nd-node2 is down
		server		8d22h	Network device mgmt1 in node nd-node3 is down
		server		30d23h	Network device mgmt1 in node nd-node1 is down

ND Node Network Link Health Event Analytics

Overview Event Records

General



Critical Severity

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

Fault Domain
server

Cleared Time
-

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

Description
Network device mgmt1 in node nd-node3 is down

Syslog

Status
Completed

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

Configuring Syslog Servers 1/2

 Nexus Dashboard

Admin Console



Overview

Operate

Analyze

Admin

Admin > System Settings

System Settings

Refresh

General

Multi-Cluster Connectivity

Cluster Details

Name

TME-MUC

App Subnet

172.17.0.1/16

Service Subnet

100.80.0.0/16

Proxy Configuration

Edit

Type

Server

Ignore Hosts

Routes

Edit

Management Network Routes

Data Network Routes

Network Scale

Edit

Number of Sites

Number of Switches

Flows per second

NTP

Edit

Key

NTP Host Name/IP Address

192.168.10.120

DNS

Edit

Domain Name

tme-muc.case.local

Providers IP Addresses

10.49.153.3

Syslog

Edit

Remote Destinations

192.168.10.122

CISCO Live!

#CiscoLiveAPJC

BRKDCN-2914

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

115

Configuring Syslog Servers 2/2

Admin > System Settings

System Settings

General

Multi-Cluster Connectivity

Cluster Details

Name

TME-MUC

App Subnet

172.17.0.1/16

Proxy Configuration

Type

Server

Syslog

Address	Enabled	Transport	Port	
192.168.10.122	true	UDP	6514	 
+ Add Remote Destination IP Address				

Admin > System Settings

System Settings

General

Multi-Cluster Connectivity

Cluster Details

Name

TME-MUC

App Subnet

172.17.0.1/16

Syslog

Address	Enabled	Transport	Port	
192.168.10.122	true	UDP	6514	 
<input type="text" value="192.168.10.12"/>	☒	<input type="text" value="UDP"/>	<input type="text" value="614"/>	 

Hardware Monitoring of ND via CIMC



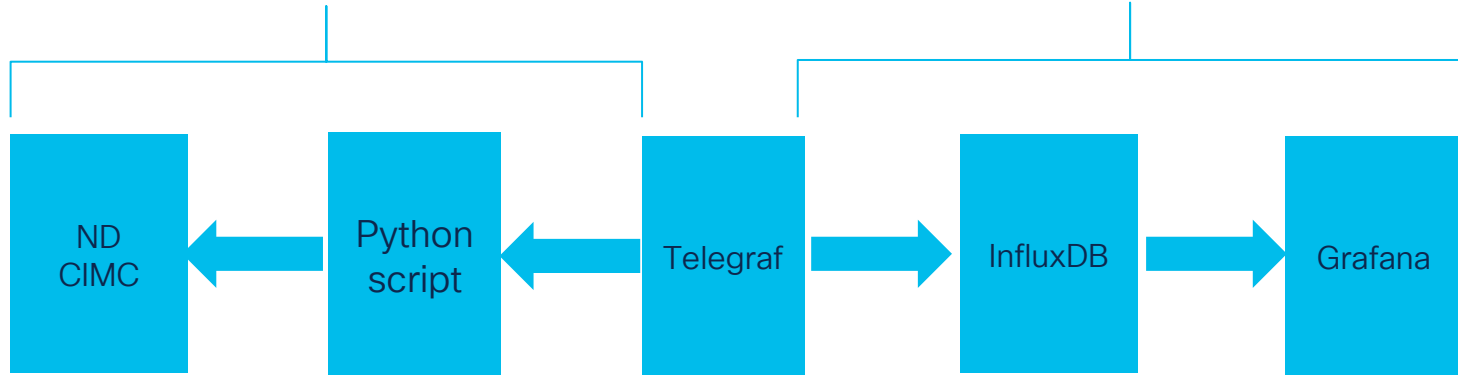
Hardware Monitoring of ND via CIMC

- 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"

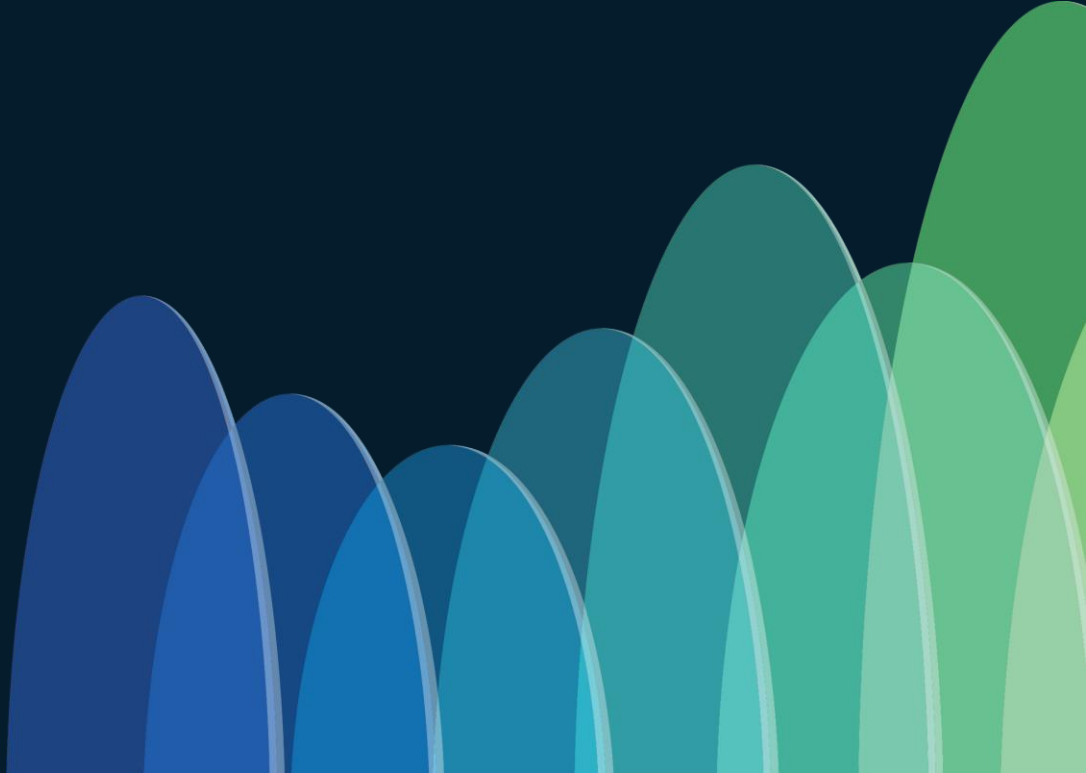
SW Stack Example

Telegraf calling a Python script to collect periodically data from CIMC

Telegraf storing data as timeseries in InfluxDB.
Grafana visualises 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

Complete Your Session Evaluations



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



Complete your surveys in the **Cisco Live mobile 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 DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand



Thank you



#CiscoLiveAPJC

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC