cisco live!

Let's go

#CiscoLive



Deploying Nexus Dashboard in your Organization

Matthias Wessendorf, Principal Engineer @matteq4er BRKDCN-3914



#CiscoLive

Cisco Webex App

Questions?

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

How

- 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 June 9, 2023.

	8:19 7 Catalyst 9000 Series Switching Family * technologies, and features in the Catalyst 9000 Switches.
	Speaker(s)
	Kenny Lei Cisco Systems, Inc. Technical Market >
	Categories
	Technical Level
	Intermediate (596)
	Tracks
	Networking (220)
	Breakout (453)
	SHOW 2 MORE V
	Webex
(•	Join the Discussion
	Notes
	Enter your personal notes here
https://ciscoliv	e.ciscoevents.com/ciscolivebot/#BRKDCN



-3914

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, centralized vs. stretched
 - Network requirmenets 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

8



Consume all services in one place



Nexus Dashboard: One view

Conventional

One view



cisco live!

Cisco Nexus Dashboard Platform

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



Virtual Nexus Dashboard Platform

Virtual Platform to Support NDI ,NDO and NDFC in Production



Nexus Dashboard: A Unified Agile Platform

The operator view





Consume service(s) from single place



Frictionless navigation across multiple services and sites



Customize views and workflows

The admin view

		0	
Ŧ	disto Nexus Dashboard		0000
Cashboard Sites	Sites		0
Services Services	Filter by attributes		Add Ste
Ø System Resources	apic-site-1 APIC-42.1	epic-site-2 APO-4(2)	@ eastersite=1 Good APIC=4.2.1 Alare
III Operators 🗸 🗸	 Healthy 	 Healthy 	e Healthy
U Innanska ∨	Image: Second system Image: Second system Image: Second system Ima	Image: Constraint of the second se	Aptication State (Section 2014) - Section 2014 - Section 201



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 -

cisco live!



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 and NDO	NDFC***
Total number of nodes needed	6	3	6	3
Type of master nodes	DATA	APP	DATA	APP
Total number of DATA nodes needed	3	0	3	0
Total number of APP nodes needed	3	3	3	3

* 3 APP node PoC setup for NDI with reduced scale is available

** 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 DCNM Connectivity Considerations



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

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



vND Considerations for ND 2.2 or earlier

cisco live!

Attaching vND to the Network (via UCS FI or equivalent or direct)

- If you plan to leverage Persistent IPs for NDI or NDFC
 - Port-Group and virtual Switch, where the vND is connected to has to be:
 - Connected via PC or vPC
 - Connected via a single link
 - A/A without PC or vPC is not supported
 - A/S at Hypervisor level without PC or vPC is <u>not</u> supported
 - Interface failover at UCS level (or equivalent) without PC or vPC is supported
 - In a nutshell the virtual switch has to have a single logical uplink.
- This is addressed in ND 2.3 and later release.

Attaching vND to Network (via UCS FI or equivalent)



A/A uplinks of Port-Group/virtual Switch without PC or vPC



A/S uplinks of Port-Group /virtual Switch at Hypervisor level without PC or vPC







Single uplinks of Port-Group /virtual Switch



Attach vND to Network (directly)





Unsupported

A/A uplinks of Port-Group / virtual Switch with PC or vPC A/A uplinks of Port-Group / virtual Switch without PC or vPC A/S uplinks of Port-Group /virtual Switch at Hypervisor level without PC or vPC

Single uplink of Port-Group /virtual Switch

Supported

1000

أ¶

i.

Port-Channel used as uplink of Port-Group /virtual Switch

Supported

Ţ

j.

cisco / ile !

Persistent IPs and their usage



Important Requirement for NDI 5.1 and later for DCNM/NDFC and for NetFlow/SFlow

- 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
- Currently used by NDI 6.0, when monitoring DCNM based Sites or Netflow/Sflow collection used for ACI/DCNM
 - Only required for the Data Subnet of ND

Persistent IP Pool 2/2

Ŧ	cisco Nexus Dashboard		
Dashboard	Cluster Details		
G System Overview	Name se-ova	App Subnet 172.17.0.0/16	
Gites			
Evices V			
System Resources	Proxy Configuration		
Operations	-		
	Ignore Hosts		
Cluster Configuration			
Resource Utilization 6	Denter		
Intersight	-		
App Infra Services			
🖈 Administrative 🗸 🗸	External Service Pools		/
	Management Service IP Usage	Data Service IP Usage	
	0	0	
	Total	Total	
	Management Service IP's -		
	Data Service IP's		

External Service Pool	S		\times
Management Service IP's			
IP Usage	Assignment		
Add IP Address			
Data Service IP's			
IP Usage	Assignment		
Add IP Address			
Data Service IP's	+		
IP	Usage Assignmen	t	
192.168.6.10		~ ×	
	-		
External Service Pools			/
Management Service IP Usage	Data Service IP Usaç	ge	
0		Available (1)	
0			
Total	1 Total		
Total Management Service IP's	Total		
Total Management Service IP's	Total		
Total Management Service IP's - Data Service IP's	Total		
Total Management Service IP's - Data Service IP's IP	Usage	Assignment	



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 DCNM based Sites	L3 adjacent	L2 adjacent	6 IPs in data network (+1 for IPv6)	no
NDI for ACI based Sites	L3 adjacent	L3 adjacent	-/-	yes
NDI with SFLOW/Netflow function	L3 adjacent	L2 adjacent	6 IPs in data interface network*	no
NDO	L3 adjacent	L3 adjacent	-/-	yes

cisco live!

* 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



- 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
- Persitent 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



ND Cluster attached to ACI Fabric



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

Pro	Contra
 Easy connection between ND and Inband Management of ACI fabric 	 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	Contra
 ND Cluster is not tied to any ACI Fabric Same communication paths between all sites. 	 All communications between ACI Apps on ND need to go via L3out

cisco lile

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.


Placement of Master/Standby Nodes for Distribute/Stretched ND Clusters (recommended for NDO)

Number of Sites	1	2	3	4	5
1	M1, M2, M3				
2	M1,M2	M3,S1			
3	M1	M2	M3		
4	M1	M2	M3	S1	
5	M1	M2	M3	S1	

M1, M2, M3 : ND Master Nodes

S1 : ND Standby Node

cisco live!

When Centralized or Distributed/Stretched Cluster

Centralized		Distributed/Stretched		
- With NDI	/NDFC deployed	- For redundancy/DR for NDO		
 NDI do n redundar clusters. cluster to with a dis 	ot gain any better ncy with distribute/stretched You more likely expose the p interconnection failures stributed/stretched cluster			
 Synchror between telemetry WAN 	hization traffic is kept the ND nodes and only / traffic is streamed via			
 Same tra site 	ffic path for reaching each			
Recommended for NDI/NDFC Recommended for NDO				

#CiscoLive BRKDCN-3914 © 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public 38

Deployment Options for ND

cisco ive!

Definition Terms and Assumptions/Requirements

- <u>Site</u>: geographical datacenter location with 1 or more fabrics
- RTT requirements for:
 - ND: between ND nodes <150ms
 - NDO : to APIC <500ms, to DCNM <50ms, between ND/NDO nodes <150ms
 - NDI: between ND/NDI nodes <50ms, to APIC/Fabric <50ms
 - NDFC: between ND/NDI 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)!
 - For NDI being hosted on ND2.1 or later for DCNM/NDFC based fabrics, you need to have the Data Interfaces of the ND nodes L2 adjacent or eBGP enabled and provide persistant IPs!
 - For NDI being hosted on ND2.1 or later leveraging Netflow/Sflow, you need to have the Data Interfaces of the ND nodes L2 adjacent and provide persistant IPs!
 - When deploying NDFC on ND2.1 or later the Management Interfaces of ND nodes have to be L2 adjacent. Also Data Interfaces of the ND nodes have to be L2 adjacent.

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

HA/Redundancy with Stretched ND clusters

- 2 ND master nodes are always needed to keep the ND cluster operational. If you deploy a stretched cluster across 2 sites, you SHOULD deploy in the site with a single ND master node, a ND standby node.
- In case of a failure of 2 ND master nodes, you have to manual promote the standby to master to replace a failed master.
 - NDO/NDFC are the only apps surviving this.
 - When the failed master needs to be wiped and re-added as standby node.



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



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

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

Not recommended as NDO is not distributed















Site 1 Fabric 1



Cisco Nexus Dashboard cluster 1





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

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

Operating Nexus Dashboard



OneView aka as ND Federation



Overview

- ND Federation 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
- <u>Remote User is required to setup and use ND Federation</u>

Federation 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.

APIGW



cisco live!

Onboard Clusters (Federation Configuration)

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

Co Overview		Cluster Configuration
Gites		Cluster Conliguration
Services		General Multi Cluster Connectivity
2 System Resources	~	
Operations	~	
C Infrastructure	^	
Cluster Configuration		
Resource Utilization 🧔		
Intersight		
App Infra Services		
🗴 Administrative	~	
		No Clusters Connected
		Connect to another Nexus Dashboard cluster for a single pane of glass view into all clusters' sites and services Connect Cluster



Onboard Clusters (Federation Configuration)

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

Connect Cluster		⊸ ×
General		
Host Name/ IP Address *		
172.25.124.164		
User Name *		
admin		
Password *		
*****	•	
Login Domain		
Select an Option	\sim	
Geographical Location - Drop	pin to locate your cluster	

ノロのひゃいで - 日 J P - 日 G B ワ -	300000000° // // // // 30000000000000000
	#0000000000000000000000000000000000000
	/000000/*´ // //////////////////////////
/^************************************	
· _ + + + + + + + + + + + + + + + + + +	
	177 IAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
100 100 100 100 100 100 100 100 100 100	· · · · · · · · · · · · · · · · · · ·
8700000 11	
1. 00000 V/ /	
1 20001	
000	
30000	
· ` ` • = = • `	
	(Capcel) Save
	(Oalicel) 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 selecta specific cluster
- Central Dashboard is added to the header bar
- Local cluster and FM are marked in the list

n diale Nexus Dashi	board			Feedback Help ~	admin \sim
	C ND21-QA-FED >			Central Dashboard) 🏟
G Overview	Cluster Configuration		`		0
Sites	oldster oornigdration				•
E Services	General Multi Cluster Connectivity				
System Resources					
Operations	Filter by attributes				
C Infrastructure	Connectivity Status	Name	URL		
Cluster Configuration	↑ Up	IFAV201-ND-CLUSTER	10.193.81.22 Show 2 more >>		
Resource Utilization 🌀			10 105 011 105		
Intersight	↓ Down	Scale-vND-cluster	Show 2 more ~		
App Infra Services	↓ Down	Scale-pND-cluster1	10.195.211.128 Show 2 more ∨		
E vonuniso auve 🗸	T Up	ND21-QA-FED Local	10.49.153.62 Show 2 more ↓		
	↑ Up	ND-SYD	10.67.185.6 Show 2 more ∨		
	↑ Up	ifav22-cluster	172.23.49.116 Show 2 more ~		
	↑ Up	ifav40-vnd-cluster	172.23.50.148 Show 2 more ∨		
ttps://10.43.151.60/4./ResourceUtilization	↑ Up	spog-cluster Primer	172.28.243.126 Show 2 more ∨		



Central Dashboard



cisco / ile !

OneView across all Clusters



cisco live

Switch Cluster

- Switch to another cluster without reloading the UI entirely
- Click on the cluster name from the header bar to select a cluster to switch to
- Click on a cluster and click
 Select





Public API



Overview

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

cisco ile

API UI



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

What's new in 2.1.1a?

Watch an Overview View Release Notes







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 (Worker or Standby)
- Worker Node is for horizontal Scaling
- Standby Node is increasing HA as it can replace a failed Master
- 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





cisco ile

Adding a new Node

Add Node				
CIMC Details				
IP Address *	Username •			
Password *				
•	Venty			
Node Details Name *	Serial Number +			
Turne				
Worker V				
Management Network				
IP Address •	Gateway *			
Data Network				
IP Address •	Gateway *			
VLAN				

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

cisco /

Replace a failed Master with Standby Node



cisco live!

Failover to Standby

	Fail Over	×
Actions >	Select Standby Node Data Network IP Address. Standby Node	
Register	ins15-dev4-sn6	
Replace		
Reboot		
Delete		
Fail Over		
Select failed Master and click	Fail Over	Save

Select Standby to replace failed Master

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

Manual Recovery of 2 failed Masters





Recovery Process if 2 Masters are down 1/3

- 2 Master Nodes are failed
- 1 Standby Nodes are required to get the system back online
- Log in to the remaining master
 - Run "acs failover" command to failover one of failed master to standby

```
acs failover --failedIP <master-to-failover> \
```

```
--failedIP <other-failed-master> \
```

```
--standbyIP <standby-ip>
```

```
Note: Use inband ipaddress for above parameters
```

Recovery Process if 2 Masters are down 2/3

• acs cluster masters will show 1 Active Master and 2 Inactive Masters

[rescue-user@ndsim ~]\$ acs cluster get masters				
ATTRIBUTES	INS15-PROD2-SN1	INS15-PROD2-SN2	INS15-PROD2-SN6	
CleanReboot	true	true	true	
FirmwareVersion	2.0.0.63	2.0.0.63	2.0.0.63	
FirstMaster	true	false	false	
ID	6954c2f3-e827-46e7-a03d-4a1ea8720a0f	2681befb-e7fc-45d5-8889-91193caca48b	b3d9e566-4d8a-44d2-82f2-13c74ca762b9	
InbandNetwork GatewayIP	192.192.1.1	192.192.1.1	192.192.1.1	
InbandNetwork Iface	bond0br4001	bond0br4001	bond0br4001	
InbandNetwork IfaceIP InbandNetwork Subnet Labels	192.192.1.101 192.192.1.101/24	192.192.1.102 192.192.1.102/24	192.192.1.106 192.192.1.106/24	
Model	SE-NODE-G2	SE-NODE-G2	SE-NODE-G2	
Name	ins15-prod2-sn1	ins15-prod2-sn2	ins15-prod2-sn6	
OobNetwork GatewayIP	10.195.219.1	10.195.219.1	10.195.219.1	
OobNetwork Iface	bond1br	bond1br	bond1br	
OobNetwork IfaceIP	10.195.219.69	10.195.219.71	10.195.219.79	
OobNetwork Subnet	10.195.219.69/24	10.195.219.71/24	10.195.219.79/24	
Role	Master	Master	Master	
SecondaryStatus	Alive	Failed	Failed	
Self	true	false	false	
Status	Active	Inactive	Inactive	

Recovery Process if 2 Masters are down 3/3

• Command (both failed Masters needs to be entered):

acs failover -- failedIP 192.192.1.102

--failedIP 192.192.1.106

--standbyIP 192.192.1.105

[rescue-user@ndsim ~] # acs failover --failedIP 192.192.1.102 --failedIP 192.192.1.106 --standbyIP 192.192.1.105
Warning: Failover can be a disruptive operation and should only
be performed as last resort option to recover cluster from disasters using standby
where two master nodes have lost their state due to hardware faults. Proceed? (y/n): y
Connection to ins15-prod2 closed by remote host.
Connection to ins15-prod2 closed.

- State will be copied from remaining Master to Standby node
- Both nodes will reboot
- Standby node will reboot and come up as Master
Firmware Upgrade

cisco live!

Click in Images first to upload a firmware image

n dudu Nexus Dasht	board			Feedback Help \sim ndadmin \sim
	G ND21-QA-FED >			Multi-Cluster Deshboard 🌘 😳
Overview Sites Services	Firmware Management			Modify Details O
System Resources V Operations Firmware Management	Node Details Current Firmware Version 2.1.1a	Number Of Nodes 3	Last Update 2021-09-06, 20:59:31	
Tech Support Audit Logs Backup & Restore Infrastructure & Administrative	Last Update Status Overall Status ⊘ Done	Status Breakdown 3 · Done (3)	Target Firmware Version 2.1.1a	Update Start Time 2021-09-06, 21:48:52

cisco ive!

				Click Add Image		
Ŧ	Cisco Nexus Dashboard				0(3 💶
Dashboard	—					
C System Overview	Firmware Management					Ø
Gites	Updates Images					
Service Catalog						
System Resources	Filter by attributes					tions ^
Operations ^	File Name	Status		Version	Add Image	9
Firmware Management					Delete Ima	ige
Tech Support						
Audit Logs						
Backup & Restore						
⊖ Infrastructure ∨						
🖍 Administrative 🗸			No rows found			
	10 V Rows				Page 1 of 1 ◀ ◀ 0-0 of	10 > >

cisco ive

• 2 Options supported either via remote (http server) or local

Add Firmware Image		×
Location Remote Local		
http://192.168.10.12/IMG/case-dk9.1.1.2.152.iso		
		e.g.: protoco://iv-[.port//path/filename
	Add Firmware Image	
	Location Remote Local Choose File No file chosen	



Application Services Engine		00
Firmware Management		0
Updates Images		
Filter by attributes		Actions >
File Name	Status	Version
apic-se-dk9.1.1.2.152.iso	⊘ Downloaded	1.1.2.152
10 V Rows		Page 1 of 1 ◀ ◀ 1-1 of 1 ▶ ▶

cisco live!

Setup Firmware Upgrade

Ŧ	Application Services Engine		
Dashboard			
Apps	Firmware Management		
System Resources			
Operations ^			
Firmware Management	Node Details		
Tech Support	Current Firmware Version 1.1.2.144	Number Of Nodes 1	Last Update 2020-04-29, 12:50:35
Audit Logs			
Backup & Restore			
Sites			
Cluster Configuration	Click to Set	tup an Upgrade	**
Intersight			
🖍 Administrative 🗸			Thora are no Firmware Undates
			There are no Finnware Opdates
			Please use the wizard to setup a firmware update.
			Setup Update



Select Firmware

Firmware Update		×
	Setup Matuli @ Activate @ Complete	
	O O O O	
	Pick a firmware version for this update.	
	Available Target Forware Ventions * terms toxin 1.1.2.152	
		Previous Next

cisco live!

Current Cluster Setup is validated

Firmware Update			8 8	💿 — 🗙
✿ Setup 🗕 🗄	Validate ± Install	⊙ Activate ⊘ Complet	te	
This is to validate the firmware and ex	amine the current cluster state before installing the	firmware. Once the validation passes the update	ate will be 'Ready to Install'.	
Update Details Overall Status	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	\checkmark		
Nodes' Health	Verifying nodes' states	~		
Disk Utilization	Verifying nodes' disk utilization	~		
	·····	······································		

cisco live!

Install Firmware to Nodes

Setup Ativate O complete O	Setup install Activate Ormete Tenson Selection Confirmation Rease confirm the configuration information below. Once install begins, all nodes will begin to download firmware image immediately. After the installation process is Value Value Number of Nodes 20.07 ib Setup Value Number of Nodes 20.07 ib Number of Nodes 20.07 ib 20.07 ib Number of Nodes 20.07 ib Number of Nodes 20.07 ib Node Type Number of Nodes 20.07 ib Number of Nodes 20.07 ib Number of Nodes 20.07 ib Number of Nodes 20.07 ib Number of Nodes 20.07 ib Node 10 Node 20.07 ib 10 Node 20.07 ib 10 Node 20.07 ib 10 20.07 ib 20.07 ib 20.07 ib 20.07 ib <t< th=""><th>rmware Update</th><th>e</th><th></th><th></th><th></th><th></th></t<>	rmware Update	e				
Version Stetchin Confirmation Desce confirm the configuration information below. Once install begins, all nodes will begin to download firmware lunge immediately. After the installation process is Version Selection Version Selection Version Selection Target Firmware Version 2:0.0.71a Target Firmware Version 2:0.0.71b 3 Number Of Nodes Last Update 2:0.0.71a 2:0.0.71b Node Type Number Of Nodes Last Update 2:0.0.71a 2:0.0.71b Node Type Number Of Nodes Last Update 2:0.0.71b 3 Node Type Version Selection Last Update Version Selection Node Version Selection Note Version Selection Node Version Selection Node Version S	Vision Selection Confirmation Descendent the configuration information below. Once install begins, all nodes will begin to download firmware image immediately. After the installation process is Participation Target Firmware Version 2.0.71b 3 Descendent the installation process is Descendent the installation process is <		🌣 Setup	Install Activate	⊘ Complete		
Visite Detail Target Firmware Version Target Firmware Version Number Of Nodes Last Update 2.0.71a 2.0.71b 3 2020-10-02, 14.40.19 Node Type Status Last Update VEP23340A7P N02 Master © Active 2020-10-02, 14.40.19 VEP23340A7P N03 Master © Active 2020-10-02, 14.40.19 VEP23340A7X N01 Master © Active 2020-10-02, 14.40.20 10 Rotes 2020-10-02, 14.40.20 1.0	Period but into a data but but into a but in the unit bud into a data but bud into a data bud into data bud into a data bud into a data bud in		Version Selection Confirmation	balau Oasa jastall basiga all pedea will be	sin to download firmware image immediately	After the installation process is	
Vipdate Detail Target Firmware Version Number Of Nodes Last Update Las	Number Of Nodes Saturbate Enrowate Version Durant Firmwate Version Target Firmwate Version Number Of Nodes Saturbate Exclose Second Saturbate Saturbate Mode Tope Saturbate Casturbate Viet Saturbate Ondes Saturbate Viet Node Tope Saturbate Viet Node Ondes Saturbate Viet Node Nodes Casturbate Viet Nodes Saturbate Saturbate Viet Nodes Nodes Saturbate Viet Node Nodes Outboat Viet Nodes Nodes Outboat Viet Nodes Outboat Outboat Viet Nodes Outboat Outboat Viet Nodes Outboat Outboat Viet Nodes Outboat Outboat <td></td> <td>complete, you can start activation of downloa</td> <td>ded image!</td> <td>an o download in nivare mage minociatory</td> <td>, Arter the installation process is</td> <td></td>		complete, you can start activation of downloa	ded image!	an o download in nivare mage minociatory	, Arter the installation process is	
Serial Number Node Type Status Lat Update VZP23340A7P ND2 Master © Active 2020-10-02,14.40.19 VZP23340A7Q ND3 Master © Active 2020-10-02,14.40.19 VZP23340A7Q ND1 Master © Active 2020-10-02,14.40.20 VZP23340A7X ND1 Master © Active 200-10-02,14.40.20 10 v Rovis VZP0100000000000000000000000000000000000	Serial Number Node Type Statis Las Update VZP23340A7P ND2 Mater O Active 2020-10-02, 14:01 9 VZP23340A7Q ND3 Mater O Active 2020-10-02, 14:01 9 VZP23340A7Q ND3 Mater O Active 2020-10-02, 14:01 9 VZP23340A7X ND1 Mater O Active 2020-10-02, 14:01 9 10 Rows		Update Detail Current Firmware Version 2.0.0.71a	Target Firmware Version 2.0.0.71b	Number Of Nodes 3	L 2	ast Update 020-10-02, 14:40:19
Serial Number Node Type Status Last Update VZP23340A7P ND2 Master O Active 2020-10-02, 14.00.19 VZP23340A7Q ND3 Master O Active 2020-10-02, 14.00.19 VZP23340A7Q ND1 Master O Active 2020-10-02, 14.00.29 VZP23340A7X ND1 Master O Active 2020-10-02, 14.00.29 10 v Rovis VZP004 VZP014 VZP014 VZP014	Serial Number Node Type Status Last Update WZP23340A7P ND2 Mater O Active 2020-10-02, 14:40:19 WZP23340A7Q ND3 Mater O Active 2020-10-02, 14:40:29 WZP23340A7Q ND1 Mater O Active 2020-10-02, 14:40:20 WZP23340A7X ND1 Mater O Active 2020-10-02, 14:40:20 10 v Rows France V Rows V Rows V Rows V Rows		Nodes				
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 v< Rows	WZP23340A7P ND2 Master O. Active 2020-10-02, 14.40.19 WZP23340A7Q ND3 Master O. Active 2020-10-02, 14.40.19 WZP23340A7X ND1 Master O. Active 2020-10-02, 14.40.20 10 v< Rows		Serial Number	Node	Туре	Status	Last Update
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 [4 ≤ 1-3 of 3 ▶ ▶]	WZ223340A7Q ND3 Master O Active 2020-10-02, 14:39:37 WZ223340A7X ND1 Master O Active 2020-10-02, 14:40:20 10 Rows Page 1 of 1 I 4 4 1-3 of 3 > >I		WZP23340A7P	ND2	Master	 Active 	2020-10-02, 14:40:19
WZP23340A7X ND1 Master O Active 2020-10-02, 14.40.20 10 Rows Page 1 of 1 [4 4 1-3 of 3 b b]	WZP23340A7X ND1 Master © Active 2020-10-02, 14:40.20 10 Rows Page 1 of 1 1 4 4 1-3 of 3 > >>		WZP23340A7Q	ND3	Master	Active	2020-10-02, 14:39:37
10 V Rows Page 1 of 1 (4 4 1-3 of 3 + >1	10 ∨ Rows Page 1 of 1 4 < 1-3 of 3 ▶ ▶		WZP23340A7X	ND1	Master	Active	2020-10-02, 14:40:20
			10 🗸 Rows				Page 1 of 1 ◀ ◀ 1-3 of 3 ▶ ▶

cisco ive!

Installing Firmware to Nodes

Firmware Update							×
	Setup This update is in the 'Pre-Installing' s	Install O Activate tage of the update process. Once the firmware has	Complete Pre-installed to each node, the update will be	"Ready to install".			
	Update Status Overali Status ⊘ Running	Status Breakdown 3 Bunning	Update Details Current Firmware Version 1,1.2.144	Target Firmware Version 1.1.2.152	Number Of Nodes	Last Update 2020-94-30, 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 This update is in the 'Pre-Installing'	Install stage of the update process, 6	Activate O C Once the firmware has pre-installe	Complete ed to each node, the update will be '	Ready to Activate'.					
	Update Status Overall Status Ready to Activate	Status Breakdown 3 • Done (3)	Update D Current Fi 1.1.2.160	Vetails ismware Version)	Target Firmware Version 1.1.3c	Number Of Nodes		Last Update 2020-05-04, 14:15:18	Edit Details	
	Nodes									
	Node		In-Band Management IP Address		Status		Last Install			
	ServiceNode?		192 168 6 173		(a) Done (100%)		2020-05-18, 18:18:00			
	ServiceNode3		192.168.6.174		(g Done (100%)		2020-05-18, 18:18:02			
										_
										(Retry A) Activate

cisco life!

Activation Progress

irmware Update					
	o Setup	Activate O Complete			
This is	the final stage of the update process. Once activation ha	is finished, the update will be complete!			
Update St Overall St ⊘ Runnin	Ratus Intus Status Breakdown Ng 3 • Exercise (1) Exercise (1)	Update Details Current Firmware Version 1.1.2.160	Target Fernivare Version 1.1.3c	Number Of Nodes Last Update 3 • Matter (3) 2020-05-04, 14.15.18	
Nodes					
Node		In-Band Management IP Address	Status	Last Install	
Service	eNode1	192.168.6.172	O Running (25%)	2020-05-18, 18:18:57	
Service	eNode2	192.168.6.173	Ø Done (12%)	2020-05-18, 18:18:56	
Service	eNode3	192.168.6.174	O Done (12%)	2020-05-18, 18:18:56	

cisco live!

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:

	Firmware Management				O
	Updates Images				
	Node Details Current Firmware Version 2.0.0.71a	Number Of Nodes 3	Last Update 2020-10-02, 14:40:19		
• Node	Last Update Status Overall Status Running Running running activate stage for host 192.168.6.172	Status Breakdown	Target Firmware Version 2.0.0.71b	Update Start Time 2020-10-05, 12:10:15	View Details

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

cisco / ile

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



cisco ive

Create a Login Domain

Ŧ	cisco Nexus Dashboard				2 3 🔽
Dashboard					
G System Overview	Authentication				^(C)
③ Sites	Login Domains				
Service Catalog					
🕼 System Resources 🗸 🗸	Default Authentication				/
Operations	Login Domain local				
C Infrastructure ∨					
▲ Administrative ∧	Filter by attributes				Actions ^
Authentication		Description	Dealer	Descrident	Create Login Domain
Users	Name	Description	Realm	Providers	Delete Login Domain
		No rows	found		
		140 10493	Iouna		
	10 X Pours			Page 1	of 1 4 4 0-0 of 0 >>

Create a Login Domain

te Login Domain				
Name •				
Least				
Ldap				
Radius	×			
Radius /	<u></u>			
Providers Name Description	Authentication Port	Timeout	Retries	
Add Provider				

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.

dd Provider		
General		
Host Name/IP Address .		
Description		
Settings		
Authorization Protocol		
PAP CHAP MS-CHAP		
Port 1812		
Key •		
Confirm Key •		
Timeout (sec)		
Retrine		
1		
Server Monitoring		
Disabled Enabled		
/alidation		
Username •		
Password *		



Change Default Authentication for Login

Ŧ	Nexus Dashboard	2 🕸 💶
Dashboard		
System Overview	Authentication	Ø
Sites	Login Domains	
Service Catalog		
🕼 System Resources 🗸 🗸	Default Authentication	/
Operations	Login Domain local	_
◯ Infrastructure ∨		

Default Authentication



Login Screen with Login Domain



cisco live

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		\sim		
Roles				
Name	Read Privilege	Write Privilege	Service	Details
Administrator			Nexus Dashboard	(i)
Approver			Nexus Dashboard	(i)
Dashboard User	\checkmark		Nexus Dashboard	(i)
Deployer			Nexus Dashboard	(i)
Policy Manager			Nexus Dashboard	(j)
Site Administrator			Nexus Dashboard	(j)
Site Manager			Nexus Dashboard	(j)
Tenant Manager			Nexus Dashboard	(i)
User Manager			Nexus Dashboard	()

cisco ive

Configurable Security Settings

cisco ive!



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 you can have ND verify the Certificates of the onboarded Site-Controller before onboarding



Configure Security Settings

	Ŧ	Cisco Nexus Dashboard		00 💶
	Dashboard	Sociurity		0
	System Overview	Security		0
	Sites			
	Service Catalog	Security Configuration Session Timeout (seconds) Idle Timeout (seconds)	Domain Name	
	🗗 System Resources 🛛 🗸	1200 3600	*	
	Operations	RSA Certificate Root CertificateBEGIN CERTIFICATE	Intermediate Certificate -	
	C Infrastructure V	MIIDozCCAougAwiBAgilL4sty5ocYGwwDQYJKoZIhvcNAQELB BhMCVVMxCzAJBgNVBAgTAkNBMRUwEwYDVQQKEwxDaXN BhMCVVMxCzAJBgNVBAgTAkNBMRUwEwYDVQQKEwxDaX	L N	
	_£° Administrative ∧	BAMTD0FDSSBQbGF0Zm9ybSBDQTAeFw0yMDExMTYw0DM MzBaMBMxETAPBgNVBAMTCHNuLWFwaWd3MilBiJANBgkqh MjBaMEsxCzAJBgNVBAYTAIVTMQswCQYDVQQIEwJDQTEV	M	
	Authentication	MIIBCgKCAQEAoKtdWsT7nT3VncnVX2g1oTSdXZBIF48GQKvI U3lzdGVtMRgwFgYDVQQDEw9BQ0kgUGxhdGZvcm0gQ0Ev Exj5GTNdhqSNtvF+RjSngyxPm8KEuZ1C0HeLGmWArYaegN0 AQUAA4IBDwAwggEKAoIBAQDNpdkkW4smnX2A42Gb5a8	/g	
<	Security	dPQpL+7SbRjJ0n4oOzO9ygjf8Xrrq1H3I4xX1cplt9vBEdODn4s 1YWGCgXKOniJI2GXUrMAIKSypdiczcYtruUJMKN2cBLG9M1y 0BytuwnaxzeWWi8OKC/JacFg5AT7nTlj5sMJsELs2t3OyYzM	Yh K+	
	Users	bFwTYu79ycczqaSBx4A7A0w/SUn+0Kv7RR+ConU8206PRZb *XUSaM1a+t-KItG32VLcSVQRBODcdfuGqeGcX3xX3KGF33 7vebovrf8wgg2DB3ehp1G706kDntz97WdQIDAQABo4HCMIG 11/AU55BMINEARggPLkkD028BFDg78sFSmlSB74tbx8v21 CCsGAQUF5WMCBgrgbEFBQcDATAMBgNVFMRBA7E6JAA 11/AU55BMINEARggPLkkD028BFDg78sFSmlSB74tbx8v21 QmbHbArYTNeg7IXKtch+1a+ahhWU535JcCzWCjArBgNVHS 11/AU55BMINEARggPLkkD028BFDg2BsFSmlSB74tbx8v21 20b6D0xKZemcQw4scm042D/whebr0PKzA4BgNVHEEZMT AVH/BAUwAKEBJXA2BgNVHQ4EIgQg16iAmi9/p8zm1s5i35 Zm0ELy9wbGPCZmV2YeVXPX2cv2K8DD2Av2QE8DD2A2Q MOH/BAUwAKEBJXADg8NVHQ4EIgQg16iAmi9/p8zm1s5i35 BQADggEBAKid3N8C+qpWE2QP2cAzqRPGaGMEUhKHsigS3T MOH/BAUwAKEBJSBENFVOHiltqd1o9u*mq52872FNVJ32BBN 9zChdSzqmOqLVGmHce/ffUqkipjeJTWRAZ9irTWRndNoHV VyuYKLkHimOCC9VkDyNbcaLkdS1jQtMUWhe68UCo8fMD VolVbgjSxUvzncTjzUwijaowFCXC+qoRoAUAQF4psSjp4EvUb YVFUI29nkMCADwTaSTmPAhmrdoHXVW33eMXfKRexoYBkG Vn1n7g3XugHdnKh4pxUYrkhRmJJ+YY=END CERTIFICATE	л Э З Ч Ц R J J А га	

cisco live!

Configure Security Settings





Save

```
[rescue-user@ND2 ~]$ openssl reg -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 ~]$ 🗌
```

cisco ile

Resource Monitoring

cisco live!



Resource Monitoring

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

cisco ile

Resource Monitoring on Node and Cluster Level

Nexus Dashboard Feedback Â Help \lor admin 🗸 Ŧ Admin Console C ND22-TME ð ඉ Overview **Resource** Utilization C Sites III Services 器 Node Resource 🗠 ④ Last 12 hours ∨ ⊖ ⊖ 30s ∨ System Resources Host nd-1 ~ NIC All ~ =Dashboards Operations CPU% Basic Firmware Management Uptime: 19... Memory Basic CPU Busy 25% 279 GiB 100% Tech Support 11 week 14.0% 233 GiB 20% 75% Backup & Restore 186 GiB Used RAM Memory 15% 140 GiB 50% CPU Cores... and an an a thigh beautiful as a black a second and والمعادية والمتحد والمعاد Event Analytics 10% 🕌 33.6% 93 GiB 25% 5% ○ Infrastructure 47 GiB 40 Used Max Mount(/da.. 0 R 0% Cluster Configuration 04:00 06:00 08:00 10:00 12:00 14:00 04:00 10:00 12:00 14:00 12.7% Total RAM current Resource Utilization 🧑 Used SWAP Total 13.80% 22.07% 15.25% 14.00% Total 251 31 GIR 251 31 GIB 251.31 GiB 251 Use 0.36% 9.51% Avaliab 166.79 GiB Intersight GiB System 1.76% 2.28% 1.83% 1.79% Used 94 25 Gil 86 77 GiB 94 49 CiR 84.56 GiB App Infra Services Disk Space Used Basic(EXT?/XFS) Disk Space Used% Basic 1º Administrative Filesyst Mounted on Used 100% Device ext4 976 885.1 75% /dev/mapper/atom0-aaamgr.log.aaamgr /logs/k8_infra/aaamgr 2.6% MiB MiB 50% ext4 93 85.8 /dev/mapper/atom0-appsshd_logs /logs/appsshd 0.1% MiB MiB 0% 976 854.8 ext4 04.00 06:00 08:00 10.00 12.00 14.00 /dev/mapper/atom0-authy.log.authy /logs/k8_infra/authy 5.9% MiB MiB /logs/k8_infra/mongodb 52 ext4 976 843.1 /data/services/app_logs/cisco-appcenter-logger /dev/mapper/atom0-cisco.appcenter.logger 7.2% /logs/k8_infra/kafka MiB MiB 34

cisco ilei

Event Analytic



Event Analytic

A state of the state of th							
Admin Console	G se-physical						ی 🔕
Corview	Event A	polytice					0
Sites	EVENIA	larytics					0
E Services	Events Audit	Logs					
System Resources	Filter by attribut	les					
Operations ^					a sorres		Lawrence 1
Firmware Management	Severity	Life Cycle	Name	Domain	Age	Description	Acknowledged
Tech Support	Critical	Cleared	Cluster CPU Usage	server	21h35m	Cluster CPU usage greater than 80%	Yes
Backup & Restore							
Event Analytics							
⊖ Infrastructure ∨							
🖍 Administrative 🗸							

Event Analytics enables easy access your Nexus Dashboard's events and audit logs. In addition to viewing the events and logs directly in the Nexus Dashboard GUI, you can also configure the cluster to stream the events to an external syslog server

#CiscoLive BRKDCN-3914 © 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public 105

Events

- Cluster-wide events like:
 - CPU usage above 80%
 - Memory usage above 80%
 - Storage usage above 80%

cisco (

Configuring Syslog Servers 1/3

n dudu Nexus Dashb	board			Feedback	Help \checkmark	ndadmin \sim
	O ND-DCNM				9	۲
G Overview	Cluster Configuration					0
Gites	Claster Comigaration					•
Services	General Multi-Cluster Connectivity					
System Resources						
Operations	Cluster Details Name	App Subnet	Sei	rvice Subnet		
🔿 Infrastructure 🔨 🔨	ND-DCNM	172.17.0.0/16	10	0.80.0.0/16		
Cluster Configuration						
Resource Utilization 🧑	Proxy Configuration	/	NTP			/
Intersight	Servers		IP Addresses 192.168.10.120			
App Infra Services	Ignore Hosts					
🖍 Administrative 🗸	-		DNS			/
	Routes Management Network Routes 10.49.153.0/24 192.168.8.0/24 192.168.10.0/24 Data Network Routes	/	Domains ND-DCNM.case.local Search Domains Syslog Remote Destinations -	Providers IP Addresses 192.168.10.10		/



Configuring Syslog Servers 2/3

S	Syslog				\times
	Remote Destinations				
	Address	Enabled	Transport	Port	
L	Add Remote Destinations				
н.					
2					
					Save

Syslog				
Remote Destinations				
Address	Enabled	Transport	Port	
	Select an Option V	Select an Option		~ ×
		TCP		
		LIDD		

Remote Destinations				
Address	Enabled	Transport	Port	
192.168.10.120	true	VUDP	614	~ X


Configuring Syslog Servers 3/3

Syslog					\times
Remote Destinations Address	Enabled	Transport	Port		
192.168.10.120	true	UDP	614	/	1
Add Remote Destinations					
					Save

Syslog			/
Remote Destinations			
Address	Enabled	Transport	Port
192.168.10.120	true	UDP	614

cisco live!

Conclusion

cisco live!

Take Away

- Better visibility with real time analysis
- Meaningful, actionable anomalies
- Root Cause is a few clicks away
- Assurance for your configuration intent

Fill out your session surveys!



Attendees who fill out a minimum of four session surveys and the overall event survey will get **Cisco Live-branded socks** (while supplies last)!



Attendees will also earn 100 points in the **Cisco Live Challenge** for every survey completed.



These points help you get on the leaderboard and increase your chances of winning daily and grand prizes

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at <u>www.CiscoLive.com/on-demand</u>



Thank you



#CiscoLive

Cisco Live Challenge

Gamify your Cisco Live experience! Get points for attending this session!

How:



cisco / illen

- Open the Cisco Events App.
- Click on 'Cisco Live Challenge' in the side menu.
- Click on View Your Badges at the top.







cisco live!

Let's go

#CiscoLive