

Choosing the Right Cisco Catalyst Center Deployment Model for Your Network

CISCO Live !

Adam Radford, Distinguished Solutions Engineer
@adamradford123

Lila Rousseaux, Principal Solutions Engineer
@lila_rousseau

Cisco Webex App

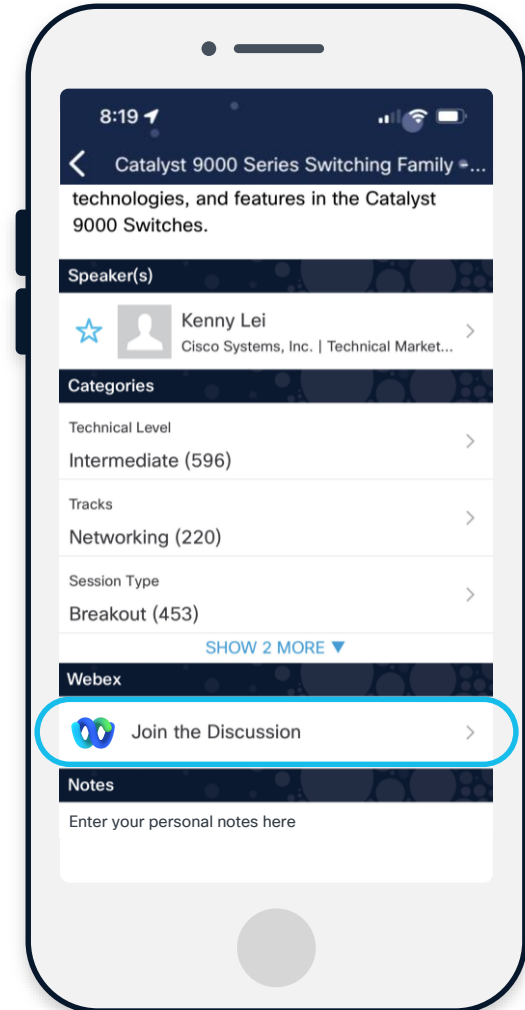
Questions?

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 June 13, 2025.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKOPS-2698>

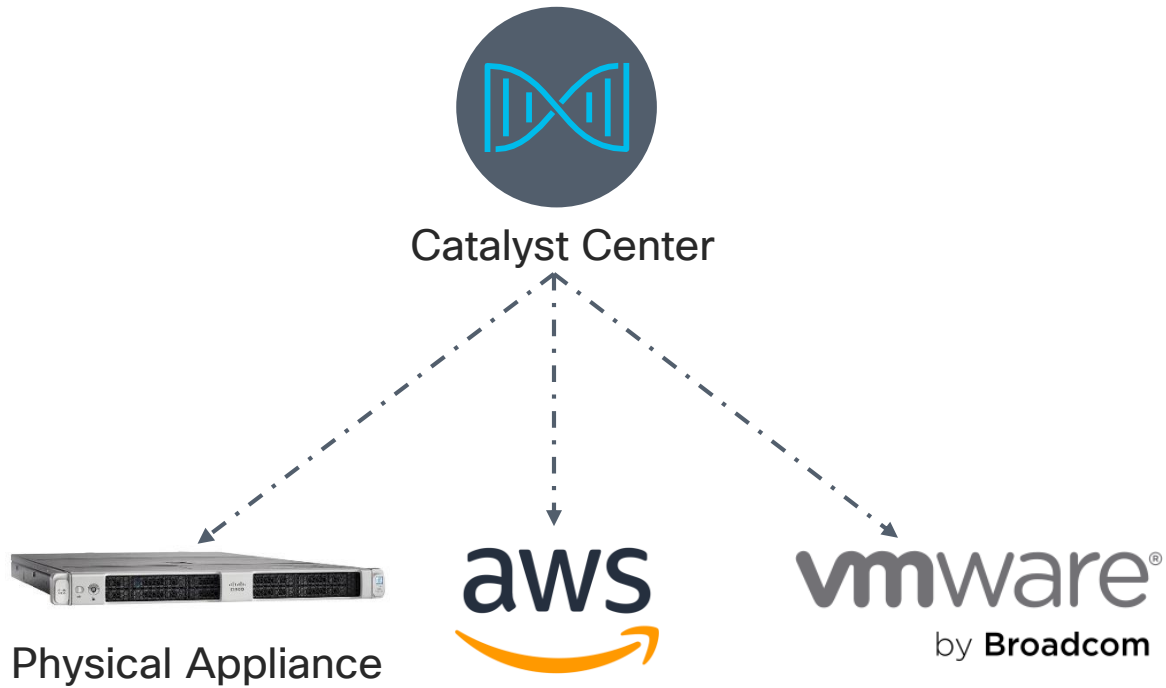
Agenda

- 01 Physical and virtual appliance options
- 02 Scaling considerations and capacity planning
- 03 High availability
- 04 Disaster Recovery
- 05 Backup and Restore
- 06 Catalyst Center Global Manager for multi-site management



Physical and Virtual Appliance Options

Catalyst Center- Form Factors



1

Virtual Appliance running on customer's ESXi

2

Feature Parity and Upgrade Process same as Physical Appliance

3

Cisco Catalyst Center VA Cost - \$0
TAC/CX Support (Optional) - \$5000/VA/Year

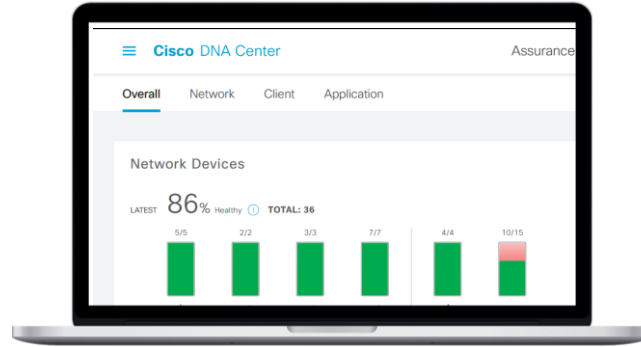
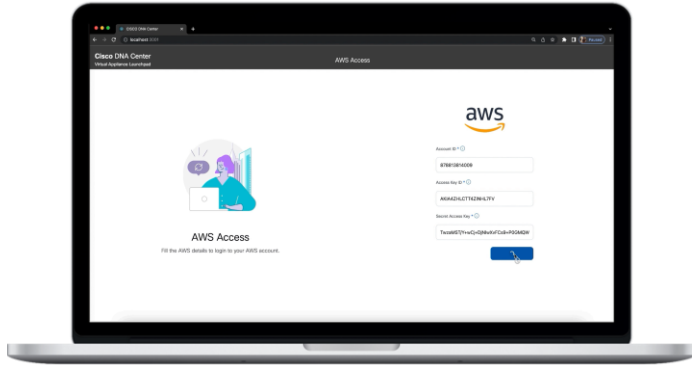
4

VMware Licensing (customer)

Catalyst Center Form Factors



*Azure - EFT



Physical Appliance



- Quicker time to value
Deploy in 90 min
- Supported worldwide
15 AWS regions supported; more coming!

No cost for software (\$0 PID)

- Optional support can be purchased

Scale parity with M-sized appliance

- 25K End points
- 1K switches
- 4K access points
- 1,500 sites
- Clustering instances not supported

M-L-XL appliances

- 25K-300K End points
- 5K-25K devices
- 1,500-10K sites
- HA and DR supported

DN2/DN3 Appliance Comparison



DN2-HW-APL (44C) ~1KW 1,236.10BTU/hr

- i6238 2x22C @2.1/3.7Ghz, 2x140W, 256G RAM



DN3-HW-APL (32C) ~1.1KW 1,428.31 BTU/hr

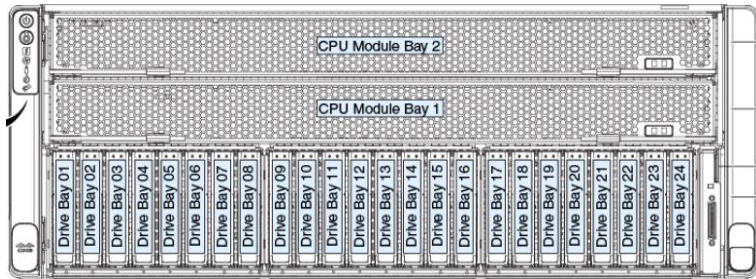
- i6326 2x16C @2.8/4Ghz, 2x185W, 256G RAM

DN2-HW-APL-L (56C) ~1.2KW 1,485.35BTU/hr

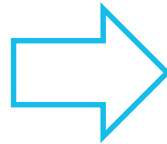
- i8280 2x28C@2.7/4Ghz, 2x205W, 384 RAM

DN3-HW_APL-L (56C) ~1.3KW 2,159.40 BTU/hr

- i6348 2x28C@2.7/4Ghz, 2x235W, 384G RAM



4U



2U



DN2-HW-APL-XL(112C) ~2KW 2,573.32 BTU/hr

- i8276 4x 28C@2.2/4Ghz, 4x165W, 768G RAM

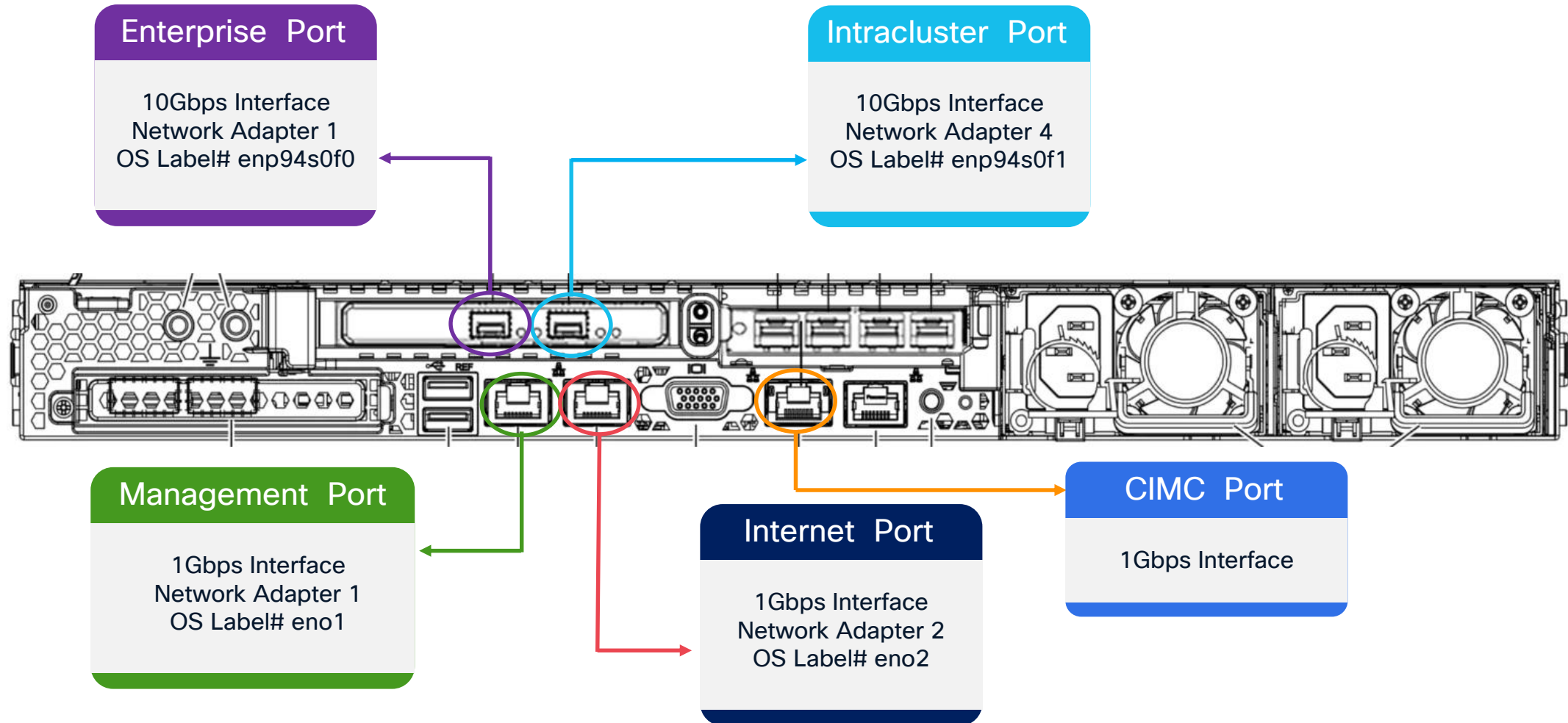
DN3-HW-APL-XL (80C) ~1.9KW 2,107.36BTU/hr

- i8380 2x40C @2.3/4Ghz, 2x270W, 768G RAM

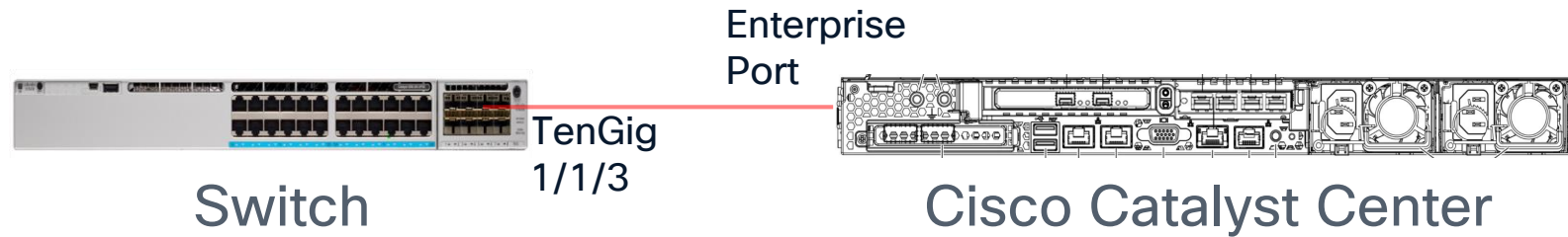
Note: There is no scale difference between DN2 & DN3 appliances

Power, BTU and space savings

Rack/Stack/Cable



Switch Configuration for Cisco Catalyst Center



```
dist-dc-01#config terminal
dist-dc-01(config)#interface tenGigabitEthernet 1/1/3
dist-dc-01(config-if)#switchport mode access
dist-dc-01(config-if)#switchport access vlan 99
dist-dc-01(config-if)#speed auto
dist-dc-01(config-if)#duplex full
dist-dc-01(config-if)#mtu 1500
dist-dc-01(config-if)#no shut
dist-dc-01(config-if)#end
dist-dc-01#copy running-config startup-config
```

Access VLAN

Speed Auto

Duplex Full

MTU 1500

Planning workflow

Step 1

Interface cable connections

Step 2

Required IP addresses and subnets

Step 3

Internet access for required resources

Step 4

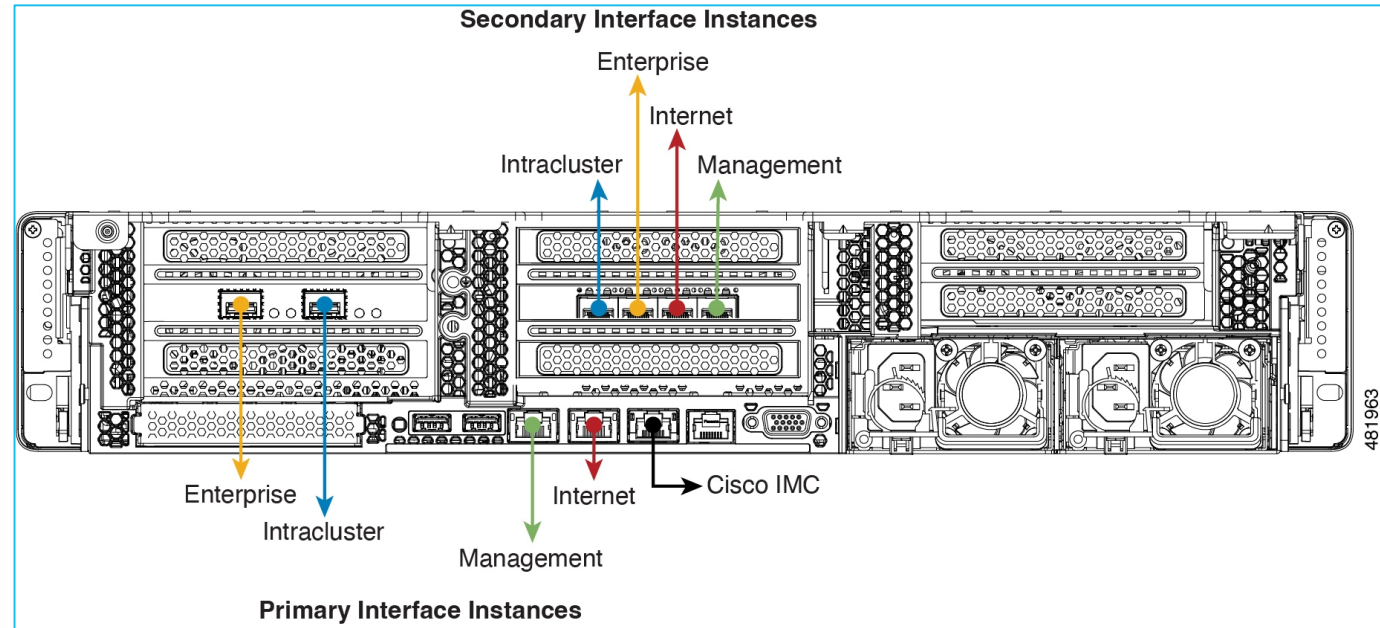
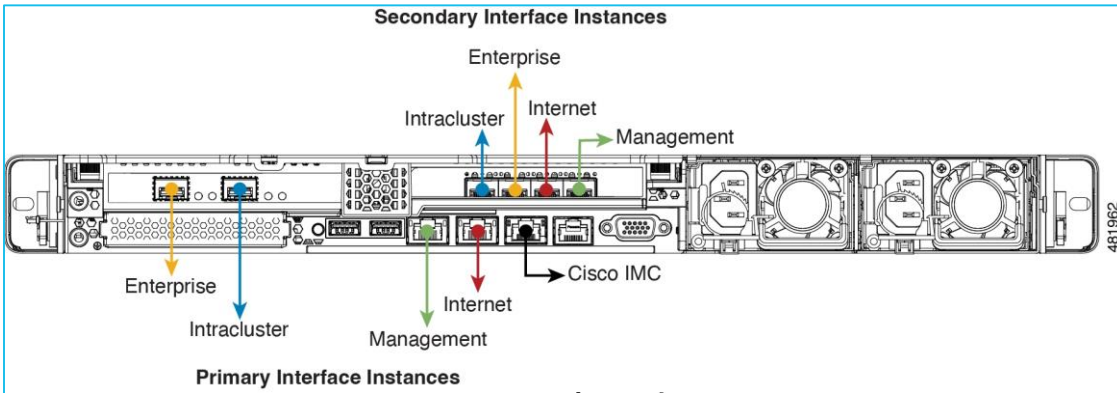
Required network ports and protocols

Physical vs Virtual

Recommended Cabling – DN3

32/56 core appliances

80 (112-dn2) core appliance



Legend

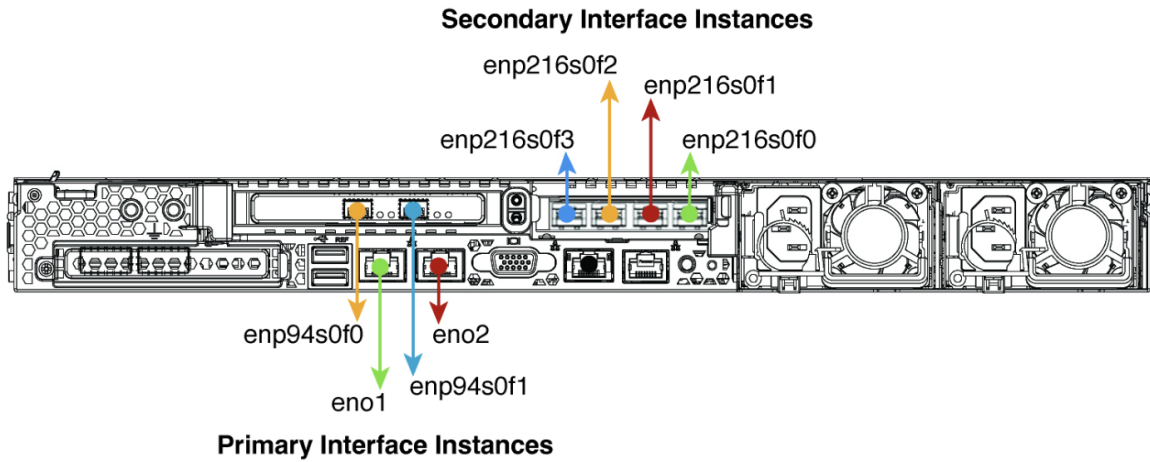
- 10-Gbps Enterprise Port (Network Adapter 1)
- 10-Gbps Intracluster Port (Network Adapter 2)
- 1-Gbps/10-Gbps Management Port (Network Adapter 3)
- 1-Gbps/10-Gbps Internet Port (Network Adapter 4)
- 1-Gbps Cisco IMC Port

DN1* Last date of Support HW from 30th June 2024 -> 31st March 2025**

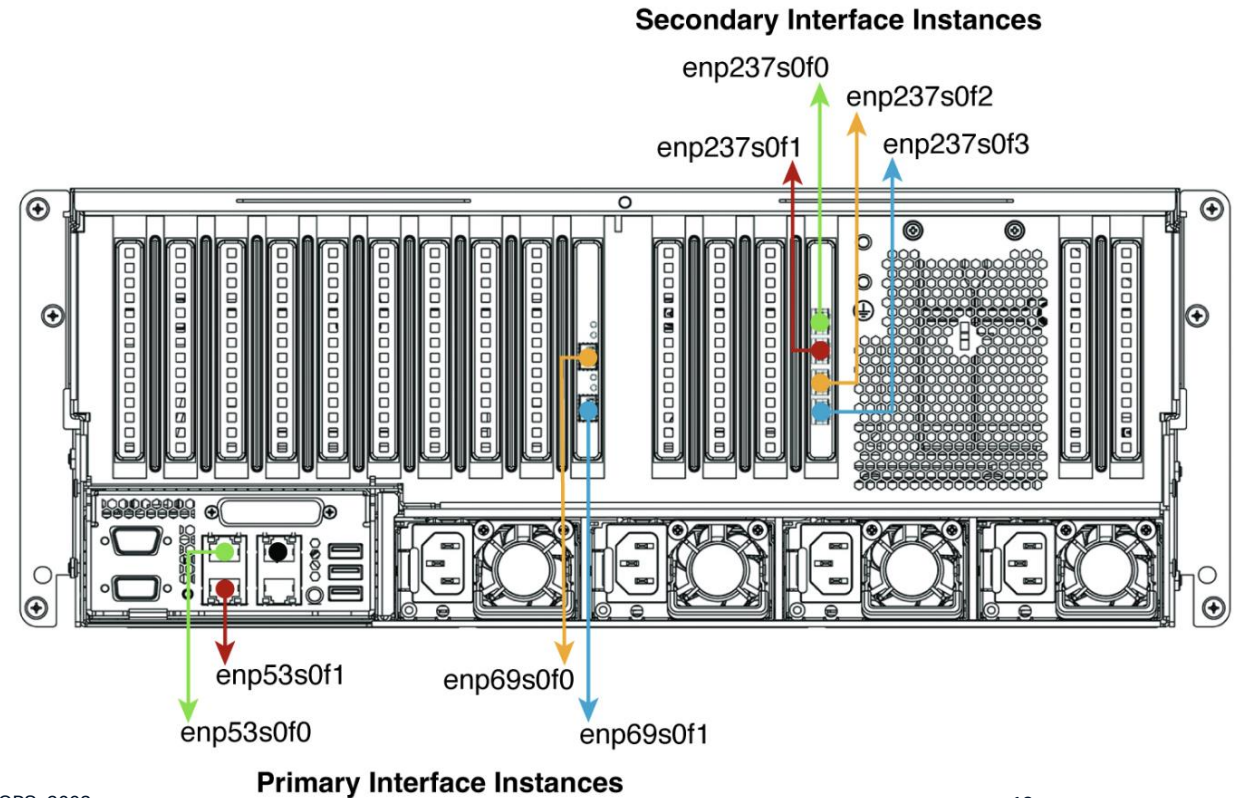
Recommended Cabling - DN2



Reference



- 10-Gbps Enterprise Port (Network Adapter 1)
- 10-Gbps Intracluster Port (Network Adapter 2)
- 1-Gbps/10-Gbps Management Port (Network Adapter 3)
- 1-Gbps/10-Gbps Internet Port (Network Adapter 4)
- 1-Gbps Cisco IMC Port

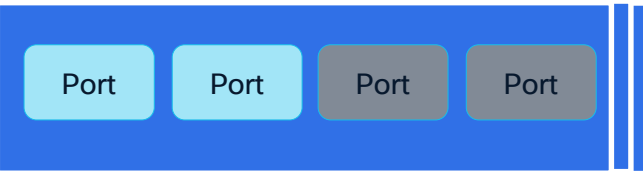


NIC Bonding

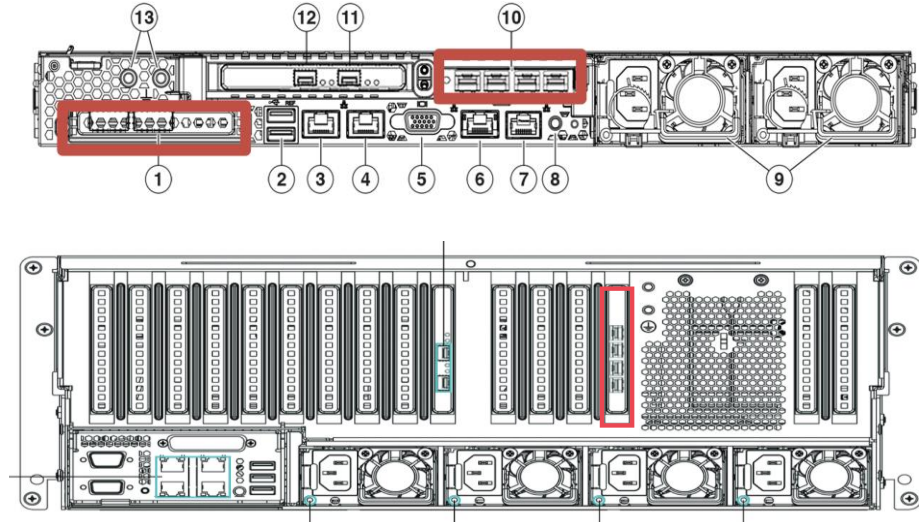


Reference

To external (enterprise network)



3-node cluster



```
OPTIONAL - NETWORK ADAPTER #3 (management)
-----
Host IPv4 Address:
  10.66.104.121
IPv4 Netmask:
  255.255.255.192
Default Gateway IPv4 Address:
  10.66.104.65
IPv4 DNS Servers:
  171.70.168.183
IPv4 Static Routes:

X Cluster Link
```

✓ Enabling two switch configurations for Cisco Catalyst Center Deployments

✓ DN2/3 support only

✓ Active/Active: Enterprise and Inter-cluster

✓ 802.3ad support

✓ Active/Standby: Management and Internet

If you have a new appliance with Cisco Catalyst Center 2.2.1.0 installed, this NIC is already configured for use. You do not need to complete this procedure.

If you are upgrading an appliance to Cisco Catalyst Center version 2.2.1.3, please follow the link [Enable NIC on an Upgraded Appliance](#).

NIC Bonding






DN2-HW-APL (M5-based)



Interface color: Green + Green and Orange + Orange
 Bonding type: Can be either LACP or Active Backup
 Interface type: SFP + SFP

single node and 3-node HA supported

Interface color: Yellow + Yellow and Purple + Purple
 Bonding type: Can be only active-backup
 Interface type: mix media RJ45 + SFP

-  CIMC (1G)
-  Enterprise (10G)
-  Cluster (10G)
-  Internet (1G/10G)
-  Management (1G/10G)

L3 port-channel



All DN2 Chassis comes with a four port SFP interface NIC which remains disabled. From 2.2.1.x release, this card will be enabled by default. Supported only with DN2* appliances

Maglev Config Wizard Steps

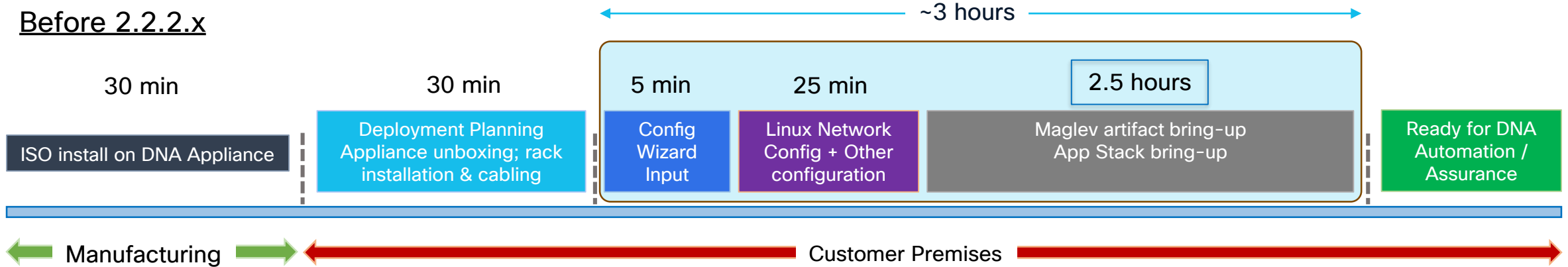
The image displays six overlapping screenshots of the Maglev Config Wizard interface, showing various configuration steps:

- STEP #3 NETWORK ADAPTER #1 (enterprise)**: Shows instructions for configuring the first network adapter (40:a6:b7:37:ff:fc - 10G - enterprise network). It lists recommended use, phy interfaces (enp94s0f0), and a warning to remove NFS mounts. Network settings include Host IPv4 Address (10.4.48.66), IPv4 Netmask (255.255.255.0), Default Gateway IPv4 Address, IPv4 DNS Servers (172.29.58.1), IPv4 Static Routes (10.4.0.0/255.254.0.0/10.4.48.1), and LACP Mode.
- OPTIONAL - NETWORK ADAPTER #2 (cluster)**: Shows instructions for configuring the second network adapter (40:a6:b7:37:ff:fd - 10G - intra-cluster link). It lists recommended use, phy interfaces (enp94s0f1), and a warning to remove NFS mounts. Network settings include Host IPv4 Address (169.254.6.66), IPv4 Netmask (255.255.255.128), Default Gateway IPv4 Address, IPv4 DNS Servers, IPv4 Static Routes, and LACP Mode.
- STEP #3 OPTIONAL - NETWORK ADAPTER #3 (management)**: Shows instructions for configuring the third network adapter (48:0b:0a:48:54:a2 - 1G - management network). It lists recommended use, phy interfaces (en01), and a warning to remove NFS mounts. Network settings include Host IPv4 Address (172.29.59.66), IPv4 Netmask (255.255.254.0), Default Gateway IPv4 Address (172.29.58.1), IPv4 DNS Servers (173.36.131.10), and IPv4 Static Routes.
- STEP #6 USER ACCOUNT SETTINGS**: Prompts for a new password for the 'maglev' user. It includes instructions on using SHIFT and CAPS LOCK, a note that asterisks indicate mandatory fields, and options to generate or use an auto-generated password. A caution advises remembering the password for future logins.
- MAGLEV CLUSTER DETAILS**: Shows fields for Cluster Virtual IP Address(s) and a note that it is a space-separated list of virtual IPs for each configured network interface.

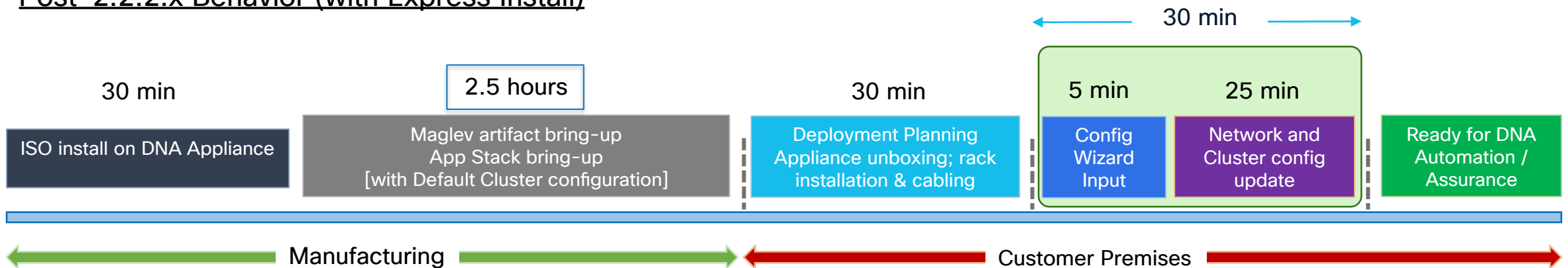
Express Install Experience



Reference



Post-2.2.2.x Behavior (with Express Install)



Two modes of Deploying- Catalyst Center on AWS

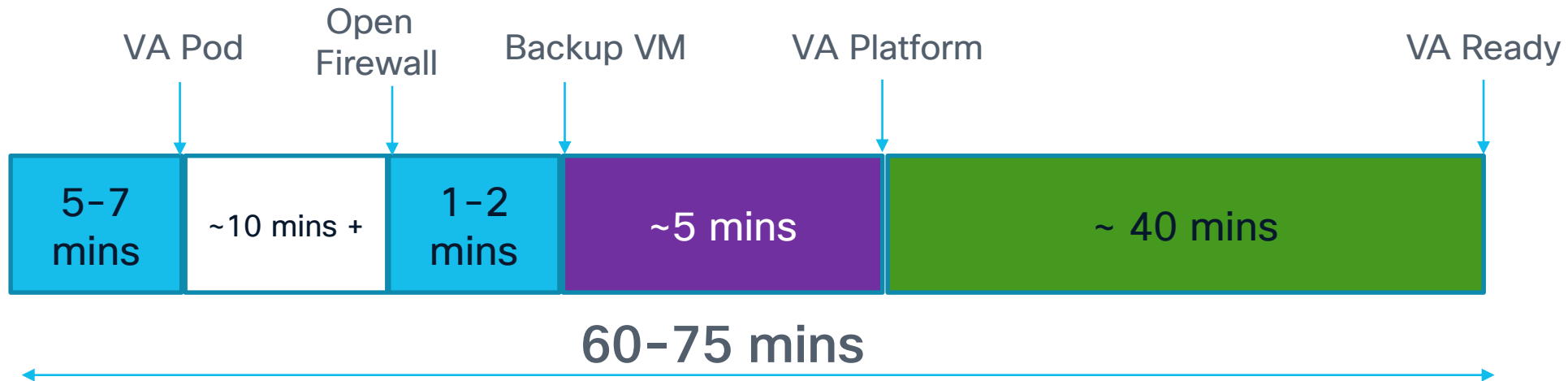
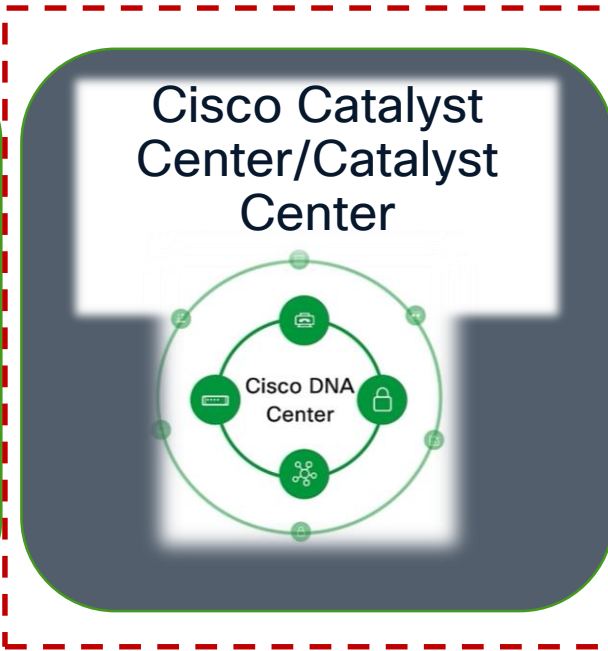
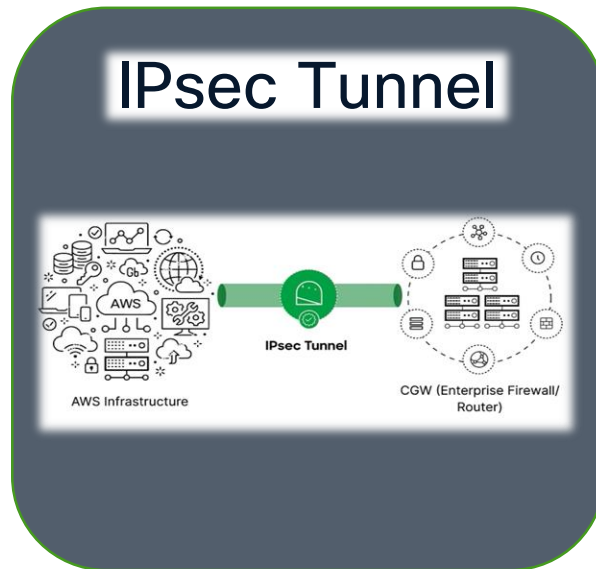
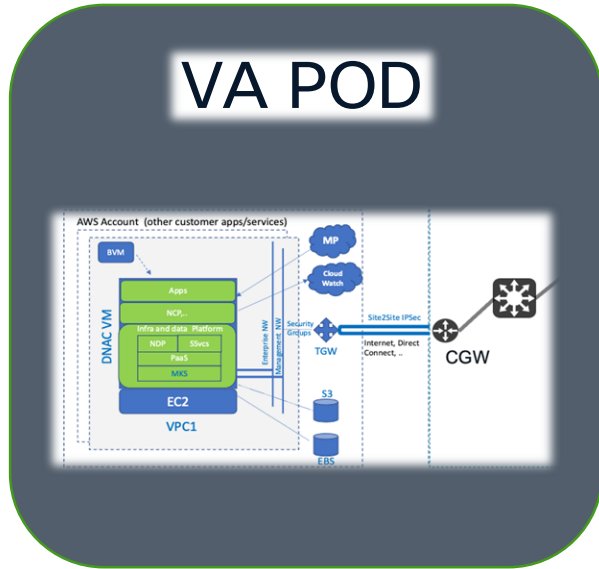
Manual Mode

- Power user of AWS
- Using CloudFormation Template
- Cisco Catalyst Center/Catalyst Center VA only
- Security perimeter needs to be configured manually
 - Security Group update manually
- Backup/Restore – Need to be deployed Manually

Auto Mode

- Minimal knowledge of AWS
- Using Launchpad VA Application
- AWS Infrastructure and Cisco Catalyst Center VA
- Security perimeter
 - CloudWatch alerts
 - Security Group
 - VPN Gateway
- Backup/Restore – Cloud NFS

Steps to Deploying Cisco Catalyst Center/Catalyst Center VA on AWS



Two modes of Deploying- Catalyst Center on ESXi

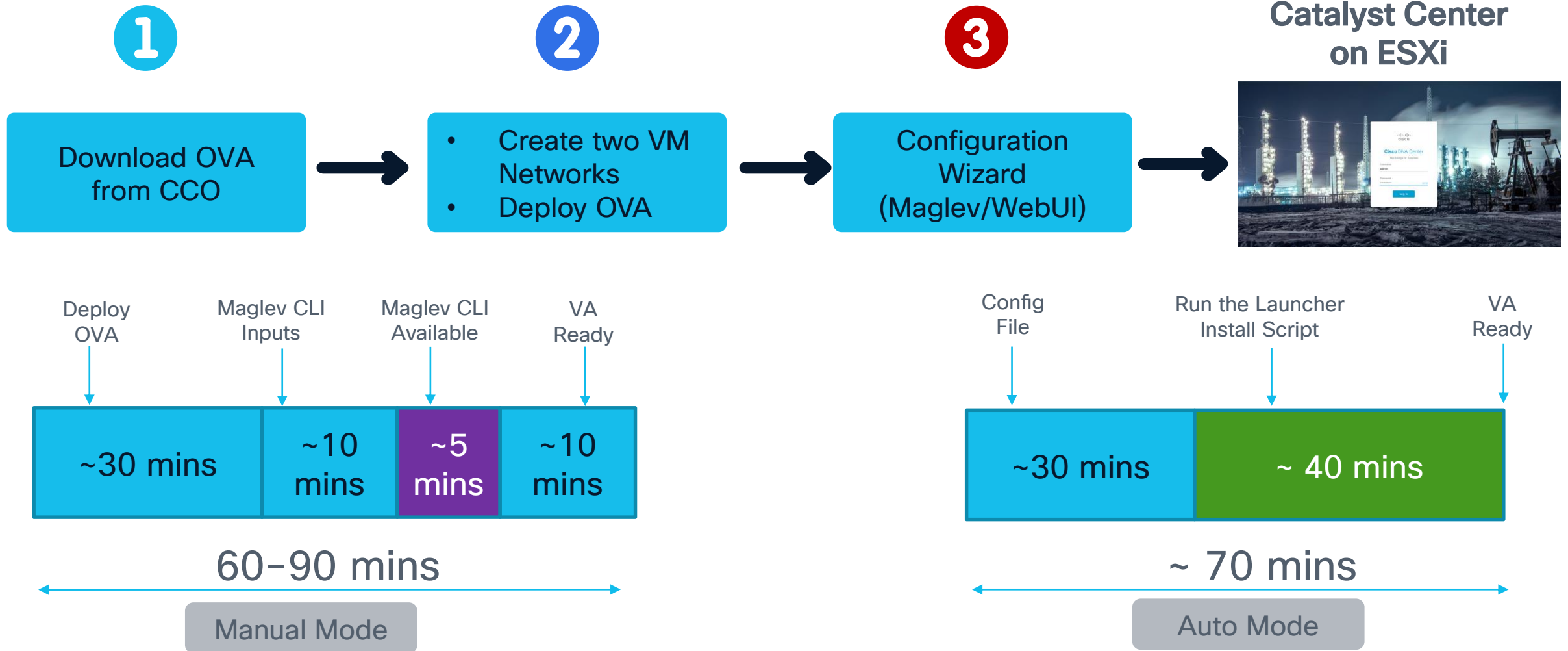
Traditional Way

- Deploy OVA and power on
- WebUI/CLI Maglev workflow

Launcher Mode

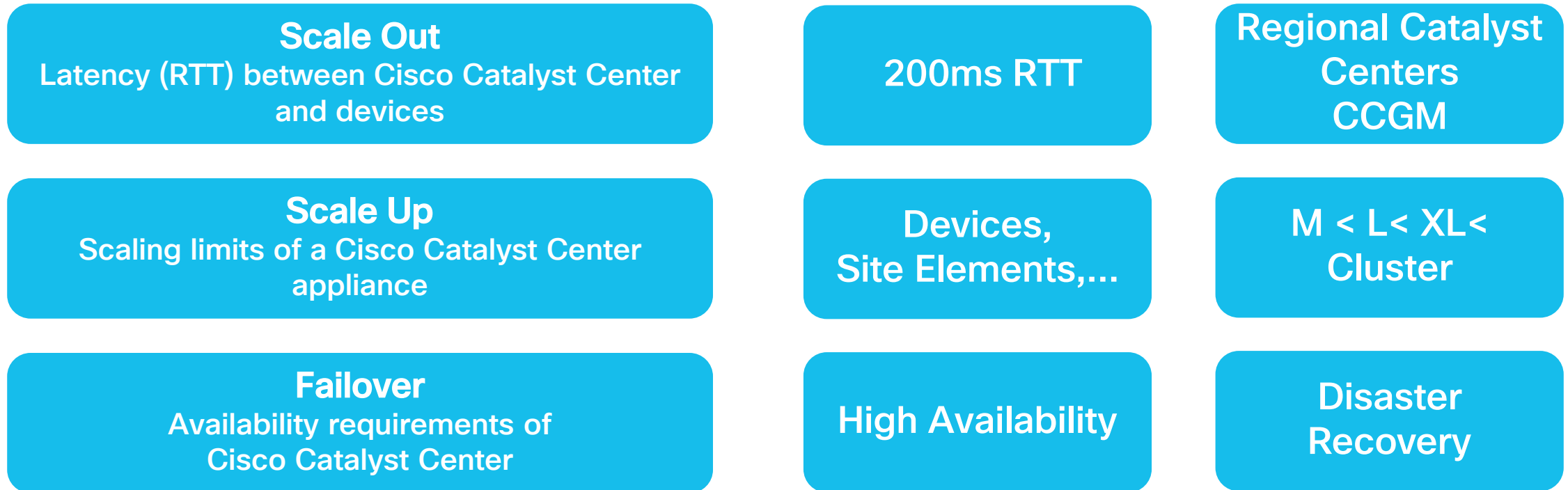
- One step to deploy
- Headless deployment
- No WebUI/CLI maglev

Steps to Deploy Catalyst Center VA on ESXi



Scaling Considerations and Capacity Planning

Which Catalyst Center Appliance do I need and how many?



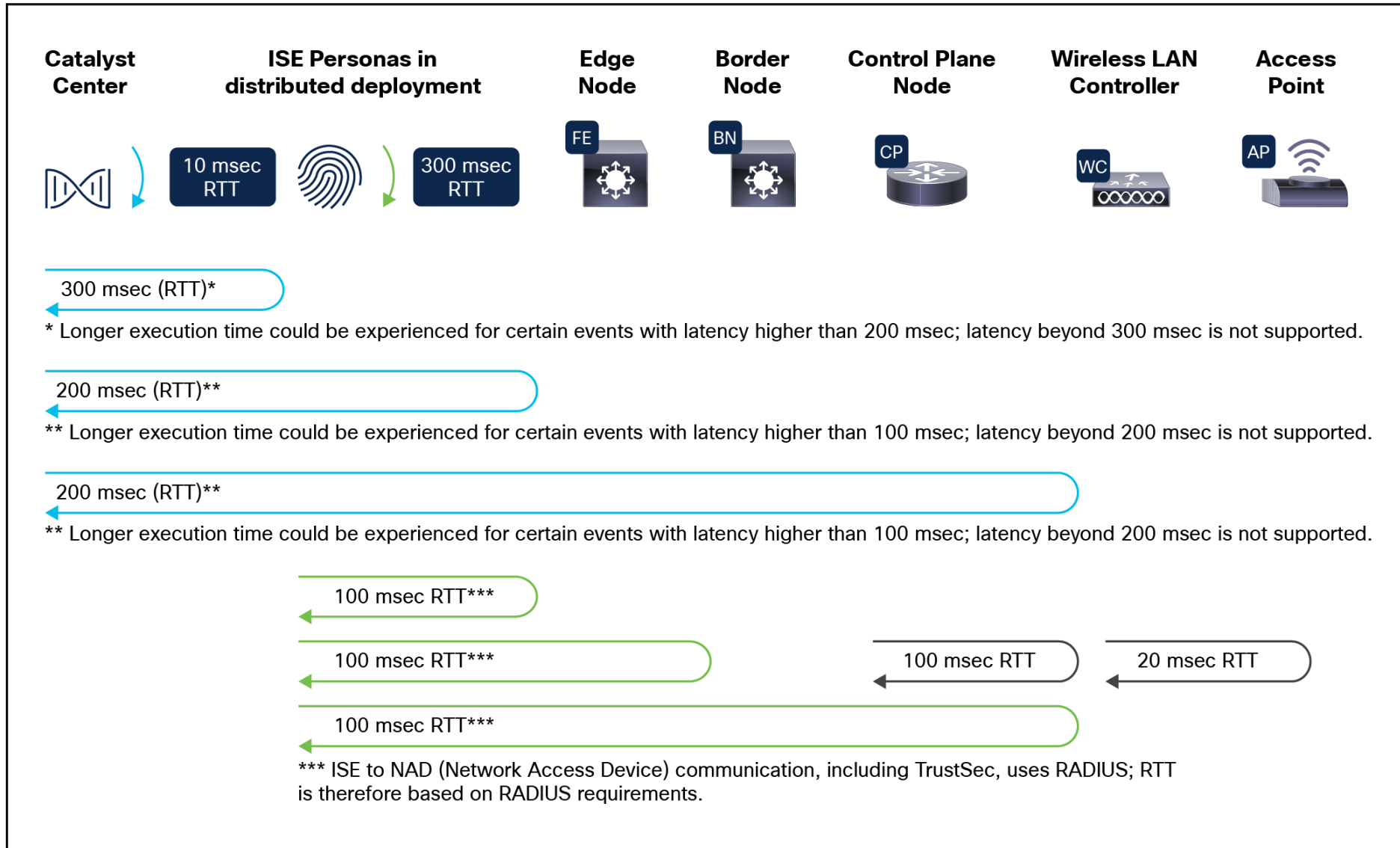
IMPORTANT NOTE:

Cisco Catalyst Center is **NOT part of the network data plane**

Maximum latency supported, roundtrip time.



Reference



Catalyst Center platform system scale

As of 2.3.7.x

Description	Medium appliance DN3-HW-APL	Large appliance DN3-HW-APL-L	Extra large appliance DN3-HW-APL-XL	3 XL cluster	Virtual Appliances
Endpoints (concurrent)	25,000	40,000	100,000	300,000	25,000
Network devices	5,000	8,000	25,000	35,000	5,000
APs	4,000	6,000	13,000	25,000	4,000
Sites	2,500	5,000	10,000	10,000	2,500
Access control policies	25,000	25,000	25,000	25,000	25,000
Access contracts	500	500	500	500	500
Per fabric site scale					
Fabric nodes	500	600	1,200	1,200	500
VNs	64	128	256	256	64
IP pools	100	300	1,000	1,000	100

← Latency between Catalyst Center to device: 200ms (RTT) →

<https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/dna-center/nb-06-dna-center-data-sheet-cte-en.html>



Trials and demos

Search

Products & Services / Cloud and Systems Management / Cisco Catalyst Center / Data Sheets /

Cisco Catalyst Center 2.3.7 Data Sheet

Updated: April 30, 2025

Bias-Free Language

Data Sheet

- Table of Contents
- Table of Contents
- Introduction
- Licensing
- Introduction to Smart Licensing
- Automation features
- Assurance features
- SD-Access features
- System and platform capabilities
- Latency requirements
- SD-Access platform scale
- Meraki integration
- Appliance scale
- Hardware appliance specificati...
- Virtual appliance requirements



Cisco Certified Remanufactured Equipment for Networking
Upgrade at deeply discounted prices to help ensure secure network transformation.

[See offer](#)







Save Translations Download Print

Introduction

Cisco Catalyst™ Center, formerly Cisco DNA Center, is a powerful network controller and management dashboard that empowers you to take charge of your network, optimize your Cisco investment, and lower your IT spending. Catalyst Center provides a single dashboard for every fundamental management task to simplify running your network. With this platform, IT can respond to changes and challenges faster and more intelligently.

Design: Design your network using intuitive workflows, starting with locations where your network devices will be deployed. Users of

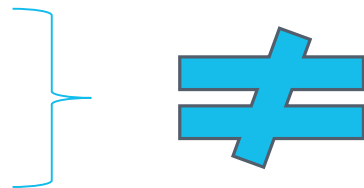
Reference plan for platform selection

-  **Determine architecture** – Is the deployment model fabric or non-fabric?
-  **Evaluate distribution** – Choose between distributed or consolidated model based on latency and regional needs
-  **Identify scale driver** – Pinpoint the main contributor influencing scalability
-  **Quantify scaling** – Provide scaling metrics for the primary contributor
-  **Account for growth** – Factor in expected future growth
-  **Validate form factor** – Ensure the form factor fits secondary contributors as well

How to start scale planning for Catalyst Center



- Fabric or non-fabric deployment model
- Preference to distribute or consolidate (regional models, latency)
- Identify the main contributor for scale decisions. Typically
 - # devices
 - # AP's
 - # endpoints
 - # site elements
 - # fabric sites
- Provide scale numbers for the main contributors
- Factor potential growth



Example -

Financial institution with headquarters in the US, large presence in Canada

- Fabric or non-fabric deployment model **Non fabric**
- Preference to distribute or consolidate (regional models, latency) **Consolidate**
Less than 200msec RTT
- Identify the main contributor for scale decisions. Typically
 - # devices **Main contributor**
 - # AP's **Main contributor**
 - # endpoints **Probably Not**
 - # site elements **Main contributor**
 - # fabric sites **Not relevant**
- Provide scale numbers for the main contributors **Provided next**
- Factor potential growth **Not available now**

Example -

Financial institution with headquarters in the US, large presence in Canada

Location	Branches / Offices	Switches	Stacks	Members / Stack	AP's
US Offices	30	2,564			3,393
US Branches	960		1	2	3
Canada Offices	20	1,518			2,288
Canada Branches	680		1	2	3

Example -

Financial institution with headquarters in the US, large presence in Canada

Location	Branches / Offices
US Offices	30
US Branches	960
Canada Offices	20
Canada Branches	680

Distributed Environment typically requires many site elements

Example -

Financial institution with headquarters in the US, large presence in Canada

How to Estimate Site elements

Location	Branches / Offices
US Offices	30
US Branches	960
Canada Offices	20
Canada Branches	680

- Devices need to be assigned to buildings or floors
- AP's need to be assigned to floors

- For estimate of minimum site elements:
 - Offices -
 - 1 x site element for the building
 - Average 25 floors per building
 - Branches -
 - 1 x site element for the branch building
 - 1 x site element for the branch floor

- For more accurate calculation:
 - Actual floors per building, consider country, province/state, city, etc

Example -

Financial institution with headquarters in the US, large presence in Canada

Large number of site elements identified!

Location	Branches / Offices
US Offices	30
US Branches	960
Canada Offices	20
Canada Branches	680

Offices -> $30 + 20 = 50$

Average of 25 floors

1 x site elements for building + 25 x site elements for floors = 26 site elements

$50 * 26 = 1,300$ **site elements for offices**

Branches -> $960 + 680 = 1,640$

1 x site element for branch + 1 x site element for floor = 2 site elements

$1,640 * 2 = 3,280$ **site elements for branches**

Total ->

$1,300 + 3,280 = 4,580$ **site elements minimum**

Table 14. Scale and hardware specifications

SKU	DN-SW-APL	DN3-HW-APL	DN3-HW-APL-L	DN3-HW-APL-XL
Description	Catalyst Center Virtual Appliance	Cisco UCS® C220 M6 Rack Server 32 cores	Cisco UCS C220 M6 Rack Server 56 cores	Cisco UCS C480 M6 Rack Server 80 cores
Catalyst Center system scale				
Site elements	2500	2500	5000	10,000
Canada Branches	680			

site elements

$1,640 * 2 = 3,280$ site elements for branches

Total ->

$1,300 + 3,280 = 4,580$ site elements minimum

Example -

Financial institution with headquarters in the US, large presence in Canada

Location	Branches / Offices	AP's
US Offices	30	3,393
US Branches	960 - 3 per branch	2,880
Canada Offices	20	2,288
Canada Branches	680 - 3 per branch	2,040

AP's

Total ->

$$3,393 + 2,880 + 2,288 + 2,040 = \mathbf{10,601 \text{ AP's}}$$

Updated Datasheet Device Scale 2.3.7.9

SKU	DN-SW-APL	DN3-HW-APL	DN3-HW-APL-L	DN3-HW-APL-XL
Description	Catalyst Center Virtual Appliance	Cisco UCS® C220 M6 Rack Server 32 cores	Cisco UCS C220 M6 Rack Server 56 cores	Cisco UCS C240 M6 Rack Server 80 cores

Catalyst Center system scale

Total Network Devices (not to exceed)	5000	5000	8,000	18,000
M Scale Profile 1 (Fabric and Non-fabric)	1000 (Switch, Router, WLC) + 4000 APs		Intentionally Left Blank	Intentionally Left Blank
M Scale Profile 2 (Fabric and Non-fabric)	2000 (Switch, Router, WLC) + 3000 APs		Intentionally Left Blank	Intentionally Left Blank
L and XL Scale Non-fabric	Intentionally Left Blank	Intentionally Left Blank	2000 (Switch, Router, WLC) + 6000 APs	5000 (Switch, Router, WLC) + 13000 APs
L and XL Scale Fabric	Intentionally Left Blank	Intentionally Left Blank	4000 (SW, Router, WLC) + 4000 APs	8000 (SW, Router, WLC) + 10000 APs

Updated Datasheet Device Scale 2.3.7.9

SKU	DN-SW-APL	DN3-HW-APL	DN3-HW-APL-L	DN3-HW-APL-XL
Description	Catalyst Center Virtual Appliance	Cisco UCS® C220 M6 Rack Server 32 cores	Cisco UCS C220 M6 Rack Server 56 cores	Cisco UCS C240 M6 Rack Server 80 cores
Catalyst Center system scale				
Total Network Devices (not to exceed)	5000	5000	8,000	18,000
M Scale Profile 1 (Fabric and Non-fabric)	1000 (Switch, Router, WLC) + 4000 APs		Intentionally Left Blank	Intentionally Left Blank
M Scale Profile 2 (Fabric and Non-fabric)	2000 (Switch, Router, WLC) + 3000 APs		Intentionally Left Blank	Intentionally Left Blank
L and XL Scale Non-fabric	Intentionally Left Blank	Intentionally Left Blank	2000 (Switch, Router, WLC) + 6000 APs	5000 (Switch, Router, WLC) + 13000 APs
L and XL Scale Fabric	Intentionally Left Blank	Intentionally Left Blank	4000 (SW, Router, WLC) + 4000 APs	8000 (SW, Router, WLC) + 10000 APs

Example -

Financial institution w

Canada

SKU	DN-SW-APL	DN3-HW-APL	DN3-HW-APL-L	DN3-HW-APL-XL
Description	Catalyst Center Virtual Appliance	Cisco UCS® C220 M6 Rack Server 32 cores	Cisco UCS C220 M6 Rack Server 56 cores	Cisco UCS C240 M6 Rack Server 80 cores

Location	Branches / Offices	
US Offices	30	
US Branches	960 - 3 per branch	
Canada Offices	20	
Canada Branches	680 - 3 per branch	2,040

Catalyst Center system scale				
M Scale Profile 1 (Fabric and Non-fabric)	1000 (Switch, Router, WLC) + 4000 APs	Intentionally Left Blank	Intentionally Left Blank	
M Scale Profile 2 (Fabric and Non-fabric)	2000 (Switch, Router, WLC) + 3000 APs	Intentionally Left Blank	Intentionally Left Blank	
L and XL Scale Non-fabric	Intentionally Left Blank	Intentionally Left Blank	2000 (Switch, Router, WLC) + 6000 APs	5000 (Switch, Router, WLC) + 13000 APs

Total ->

$$3,393 + 2,880 + 2,288 + 2,040 = 10,601 \text{ AP's}$$

Example -

Financial institution with headquarters in the US, large presence in Canada

Location	Branches / Offices	Stacks
US Offices	30	2,564
US Branches	960 - avg 1x 2- member stack	960
Canada Offices	20	1,518
Canada Branches	680 - avg 1x 2- member stack	680

- For device count, WLC's are not main contributors in this customer design
- Stacks count as single device

Switch Stacks

Total ->

$$2,564 + 960 + 1,518 + 680 = \mathbf{5,722 \text{ Switch Stacks}}$$

Example -

Financial institution

in Canada

Location	Branches / Offices	Configuration
US Offices	30	Catalyst Center system scale
US Branches	960 1x member stack	M Scale Profile 1 (Fabric and Non-fabric)
		M Scale Profile 2 (Fabric and Non-fabric)
Canada Offices	20	L and XL Scale Non-fabric
Canada Branches	680 - avg 1x 2-member stack	680

SKU	DN-SW-APL	DN3-HW-APL	DN3-HW-APL-L	DN3-HW-APL-XL
Description	Catalyst Center Virtual Appliance	Cisco UCS® C220 M6 Rack Server 32 cores	Cisco UCS C220 M6 Rack Server 56 cores	Cisco UCS C240 M6 Rack Server 80 cores
Catalyst Center system scale				
M Scale Profile 1 (Fabric and Non-fabric)	1000 (Switch, Router, WLC) + 4000 APs	Intentionally Left Blank	Intentionally Left Blank	Intentionally Left Blank
M Scale Profile 2 (Fabric and Non-fabric)	2000 (Switch, Router, WLC) + 3000 APs	Intentionally Left Blank	Intentionally Left Blank	Intentionally Left Blank
L and XL Scale Non-fabric	Intentionally Left Blank	Intentionally Left Blank	2000 (Switch, Router, WLC) + 6000 APs	5000 (Switch, Router, WLC) + 13000 APs

Total ->

$$2,564 + 960 + 1,518 + 680 = \mathbf{5,722 \text{ Switch Stacks}}$$

Example -

Financial institution with headquarters in the US, large presence in Canada

Location	Branches / Offices	Stacks
US Offices	30	2,564
US Branches	960 - avg 1x 2- member stack	960
Canada Offices	20	1,518
Canada Branches	680 - avg 1x 2- member stack	680

Table 15. Scale for 3-node DN3-HW-APL-XL cluster

Description	Supported scale
Devices ¹ (switch, router, wireless controller)	10,000

Total ->
 $2,564 + 960 + 1,518 + 680 = 5,722$ **Switch Stacks**

Validate the Selected Form Factor



- Validate the non main contributor factors
- If # switches is main contributor or if very large stacks or chassis, check the number of interfaces supported
- If Catalyst Center is managing a wireless environment, validate the number of WLC's

Validate the Selected Form Factor



- Validate the non main contributor factors
- If # switches is main contributor or if very large stacks or chassis, check the number of interfaces supported
- If Catalyst Center is main contributor, check the number of WLC's

SKU	DN-SW-APL	DN3-HW-APL	DN3-HW-APL-L	DN3-HW-APL-XL
Description	Catalyst Center Virtual Appliance	Cisco UCS [®] C220 M6 Rack Server 32 cores	Cisco UCS C220 M6 Rack Server 56 cores	Cisco UCS C480 M6 Rack Server 80 cores
Catalyst Center system scale				
Wireless controllers	500	500	1000	2000

Validate the Selected Form Factor



- Validate the non main contributor factors
- If # switches is main contributor or if very large stacks or chassis, check the number of interfaces supported
- If Catalyst Center is managing a wireless environment, validate the number of WLC's
 - Especially important in environments with distributed WLC's like FIAB+W

Validate the Selected Form Factor



- Validate the non main contributor factors
- If # switches is not 1, check the number of WLCs
- If Catalyst Center is not 1, check the number of WLCs
- Especially important for FIAB+W

SKU	DN-SW-APL	DN3-HW-APL	DN3-HW-APL-L	DN3-HW-APL-XL
Description	Catalyst Center Virtual Appliance	Cisco UCS [®] C220 M6 Rack Server 32 cores	Cisco UCS C220 M6 Rack Server 56 cores	Cisco UCS C480 M6 Rack Server 80 cores
Catalyst Center system scale				
Wireless controllers	500	500	1000	2000
Catalyst Center SD-Access scale				
Fabric sites ³	500	500	1000	2000

Example -

Financial institution with headquarters in the US, large presence in Canada

- Shared with the customer scale for:

of WLC's

Informed

Concurrent Clients

Informed

Transient Clients

Informed

SKU	DN-SW-APL	DN3-HW-APL	DN3-HW-APL-L	DN3-HW-APL-XL
Description	Catalyst Center Virtual Appliance	Cisco UCS® C220 M6 Rack Server 32 cores	Cisco UCS C220 M6 Rack Server 56 cores	Cisco UCS C480 M6 Rack Server 80 cores

Description	Supported scale
Concurrent endpoints	300,000
Transient endpoints (over 14-day period)	750,000

Example -

Financial institution with headquarters in the US, large presence in Canada

Switch Ports

Offices -> $2,564 + 1,518 = 4,082$

Half 24-port and Half 48-port

$2,041 * 24 + 2,041 * 48 = 146,952$ physical ports in offices

Branches -> $960 + 680 = 1,640$

1 x 2-member stack; All 48-ports

$1,640 * 2 * 48 = 157,440$ physical ports in branches

Total ->

$146,952 + 157,440 = 304,392$ physical ports

Example -

Financial institution with headquarters in the US, large presence in Canada

Switch Ports

Offices -> 2,564 + 1,518
Half 24-port and Half 48-
 $2,041 * 24 + 2,041 * 48 =$

Branches -> 960 + 680 =
1 x 2-member stack; All 48-ports
 $1,640 * 2 * 48 =$ **157,440 physical ports in branches**

Total ->
 $146,952 + 157,440 =$ **304,392 physical ports**

Table 15. Scale for 3-node DN3-HW-APL-XL cluster

Description	Supported scale
Physical ports ²	768,000

Validate the selected form factor



- Consider checking all other scale factors: Netflow, logical ports, etc
- For SD-Access validate architecture specific parameters like # of L3 VN's, #L2 VN's, # devices per fabric site, IP pools, etc

SKU	DN-SW-APL	DN3-HW-APL	DN3-HW-APL-L	DN3-HW-APL-XL
Description	Catalyst Center Virtual Appliance	Cisco UCS® C220 M6 Rack Server 32 cores	Cisco UCS C220 M6 Rack Server 56 cores	Cisco UCS C480 M6 Rack Server 80 cores
Catalyst Center scale per fabric site				
Layer 3 Virtual Networks	64/site	64/site	128/site	256/site
Fabric devices	500/site	500/site	600/site	1200/site
Scalable groups	4000	4000	4000	4000
Access contracts	500	500	500	500
Group-based policies	25,000	25,000	25,000	25,000
IP pools ⁴	100 ⁵	100 ⁵	300 ⁶	1000 ⁷
Layer 2 Virtual Networks ⁴	200 ⁵	200 ⁵	600 ⁶	1000 ⁷







If Required Scale Exceeds the 3-Node XL Scale?

- Consider Regional Catalyst Center Instances
 - For SD-Access, consider using the “Multiple Catalyst Center Solution” (a.k.a mDNAC) to leverage the same ISE cluster with multiple Catalyst Center Clusters
- Consider Catalyst Center Global Manager - CCGM

Reference Plan for Platform Selection



Reference

-  **Determine architecture** – Is the deployment model fabric or non-fabric?
-  **Evaluate distribution** – Choose between distributed or consolidated model based on latency and regional needs
-  **Identify scale driver** – Pinpoint the main contributor influencing scalability
-  **Quantify scaling** – Provide scaling metrics for the primary contributor
-  **Account for growth** – Factor in expected future growth
-  **Validate form factor** – Ensure the form factor fits secondary contributors as well

System Notifications When Capacity is Exceeded

✓  Mar 24, 2025 4:09 PM

Transient client count is 1055654 (exceeds 95% of capacity limit 250000).

State	NOTOK
Domain	System
Sub Domain	System Scale Limits

Scale Validation Tool

System Health / Validation Tool

No Validation Runs Available

Use the "New Validation Run" button below to schedule a new Validation Run

New Validation Run

New Validation Run

Triggering a Validation Run can be a combination of multiple validation sets or at least one validation set.

Name*

May12_2025

Description

Scale Validation

Validation Set(s) Selection*

Appliance Infrastructure Status

Appliance Scale

- Total device count
- Wired device (switches and hubs + routers + wireless controllers) count
- Wireless device (access Points + sensors) count
- Physical port count
- Interface count
- Total client count (concurrent)
- Wired client count (concurrent)
- Wireless client count (concurrent)
- Transient client count
- Site count
- IP pool count
- Netflows count
- Policies count
- Security groups count

Cancel Run

Scale Validation Tool

The screenshot displays the Cisco Catalyst Center interface for the Scale Validation Tool. The left sidebar shows a list of validation runs with one record selected: 'May12_2025' for 'Scale Validation'. The main panel, titled 'Validation Run Details', shows the run's name, description, and status (Critical). Below this, the 'Result' section is expanded to show 'APPLIANCE SCALE' with a filter for 'Info' messages. A table of results is displayed, detailing various validation metrics such as device counts, port counts, and client counts, all with an 'Info' status.

Validation Run Details

Name: May12_2025
Description: Scale Validation
Status: Critical

Result

APPLIANCE SCALE

Filter: All | Info | Warning | Critical | In Progress

Validation	Status	Duration	Message
Total device count	Info	198 ms	Total device count is 38.
Wired device (switches and hubs + routers + wireless controllers) count	Info	199 ms	Wired device (switches and hubs + routers + wireless controllers) count is 31.
Wireless device (access Points + sensors) count	Info	200 ms	Wireless device (access Points + sensors) count is 7.
Physical port count	Info	109 ms	Physical port count is 1279.
Interface count	Info	112 ms	Interface count is 1565.
Total client count (concurrent)	Info	302 ms	Total concurrent client count is 1.
Wired client count (concurrent)	Info	201 ms	Wired concurrent client count is 1.

Scale Validation Tool

Cisco Catalyst Center

Detailed Validation Results

Appliance Scale

Number	Validation	Message	Status
1	Total device count	Total device count is 38.	Info
2	Wired device (switches and hubs + routers + wireless controllers) count	Wired device (switches and hubs + routers + wireless controllers) count is 31.	Info
3	Wireless device (access Points + sensors) count	Wireless device (access Points + sensors) count is 7.	Info
4	Physical port count	Physical port count is 1279.	Info
5	Interface count	Interface count is 1565.	Info
6	Total client count (concurrent)	Total concurrent client count is 1.	Info
7	Wired client count (concurrent)	Wired concurrent client count is 1.	Info
8	Wireless client count (concurrent)	Wireless concurrent client count is 0.	Info
9	Transient client count	Transient client count is 2.	Info
10	Site count	Site count is 65.	Info
11	IP pool count	IP Address Pools count is 82.	Info
12	Netflows count	Netflows count is 0.	Info
13	Policies count	Policies count is 8.	Info
14	Security groups count	Security groups count is 21.	Info

Run Results

Found 1 critical issue and 0 warning.

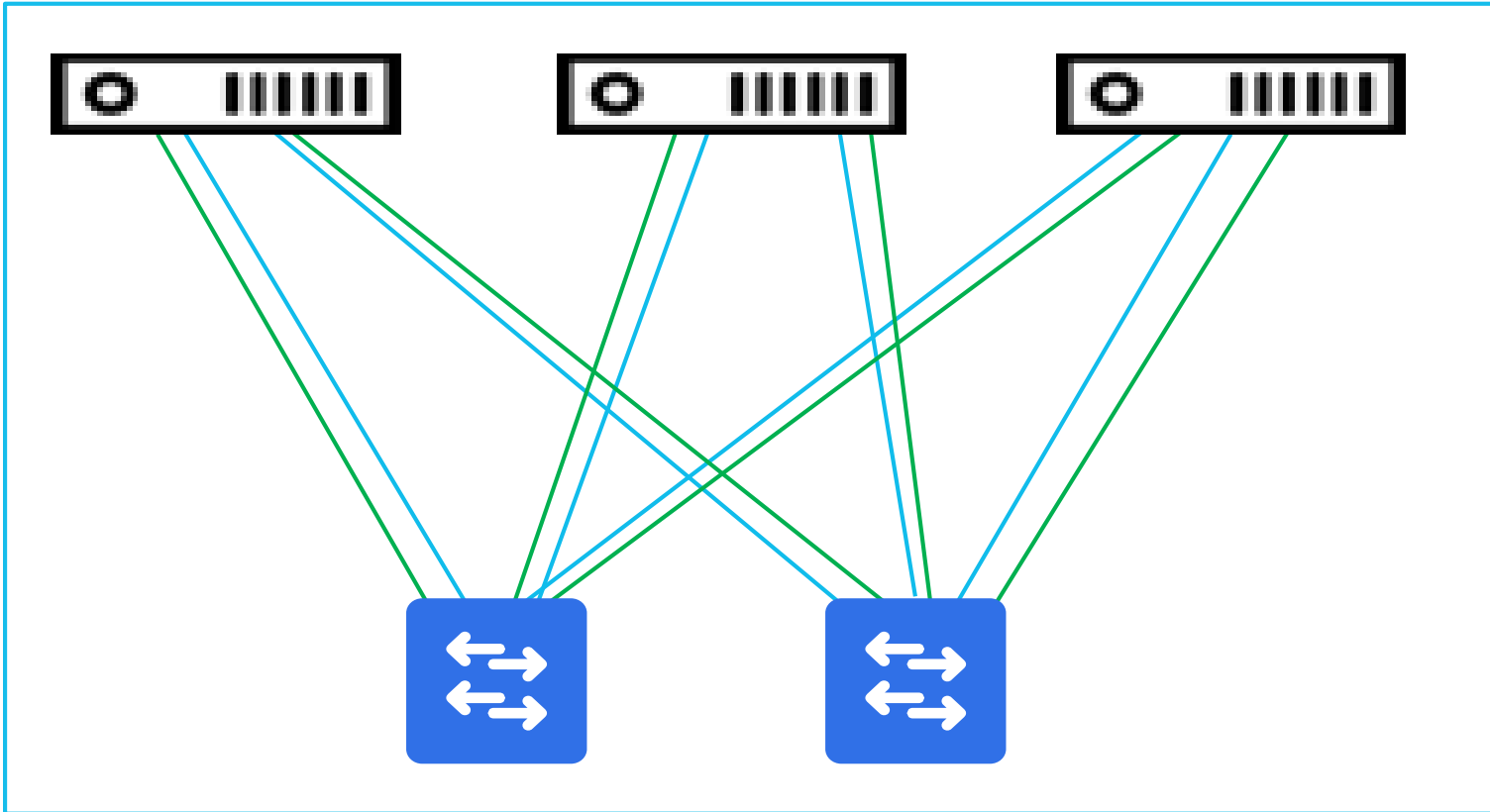
Issues	Critical	Warnings	Info	Skipped
	1	0	17	0

Version
2.3.7.9-70301

End Time
Mon, 12 May 2025 15:05:40 UTC

High Availability

Physical Appliance High Availability with Clustering

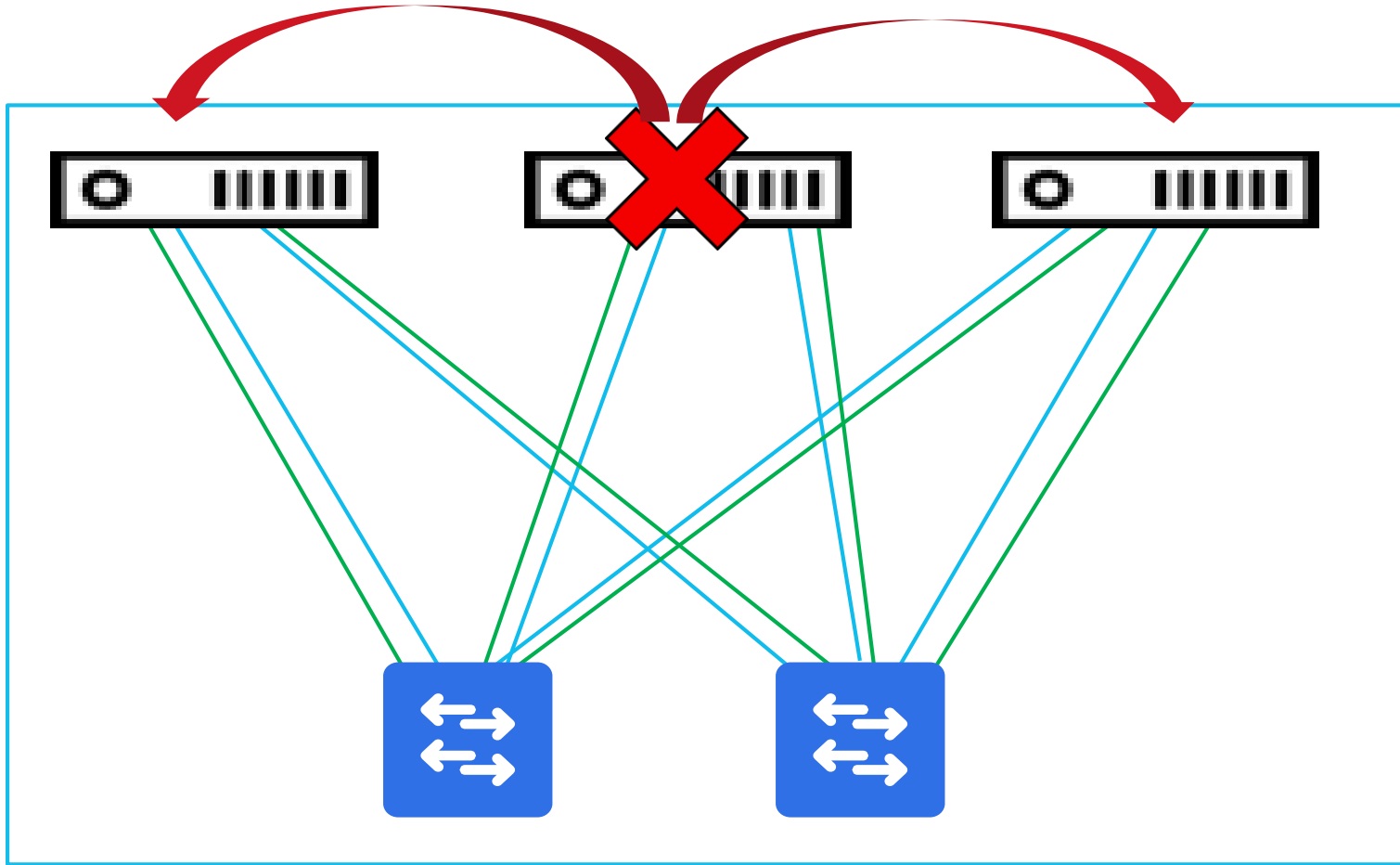


- ✓ 3-node cluster
- ✓ Software or Hardware Failure
- ✓ Active/Active
- ✓ Near Real-Time Synchronization
- ✓ Automation & Assurance Data Protected

IMPORTANT NOTE:

Cisco Catalyst Center is **NOT** part of the network data plane

Physical Appliance High Availability with clustering

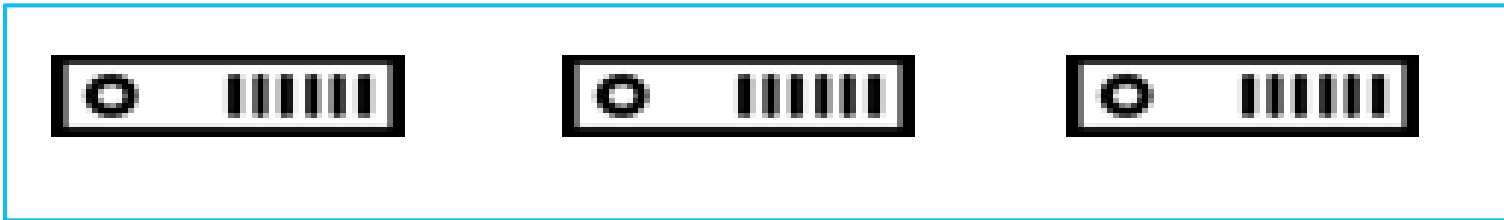


- ✓ Automatic service redistribution upon failure
- ✓ Remaining cluster continues to manage the network
- ✓ No protection of node failure with 2-nodes

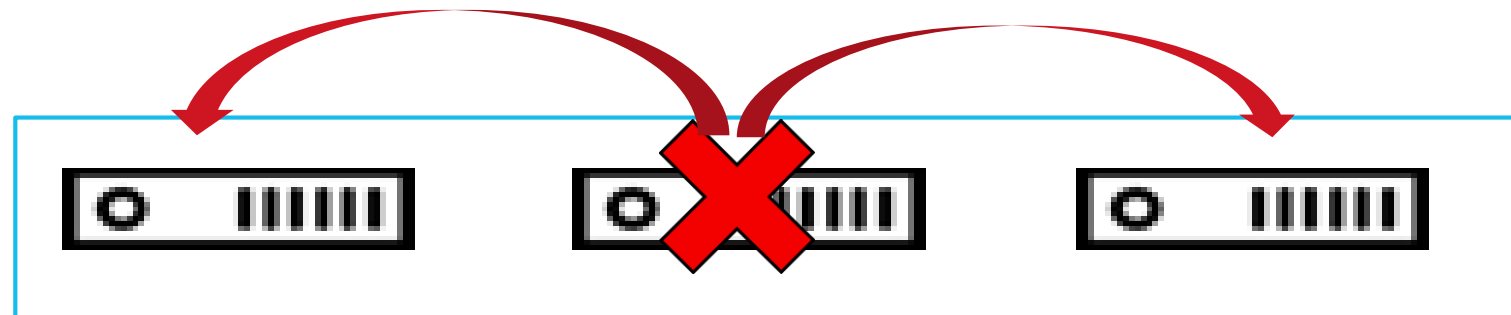
Protection Against Node Failure



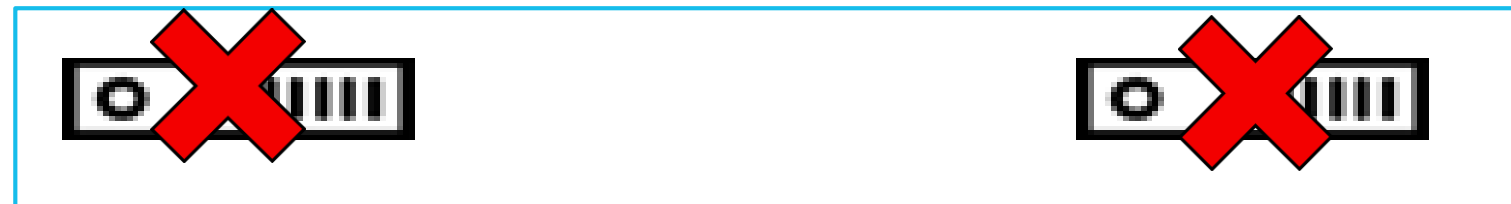
Physical Appliance



- Three node cluster: full clustering. Protection against node failure

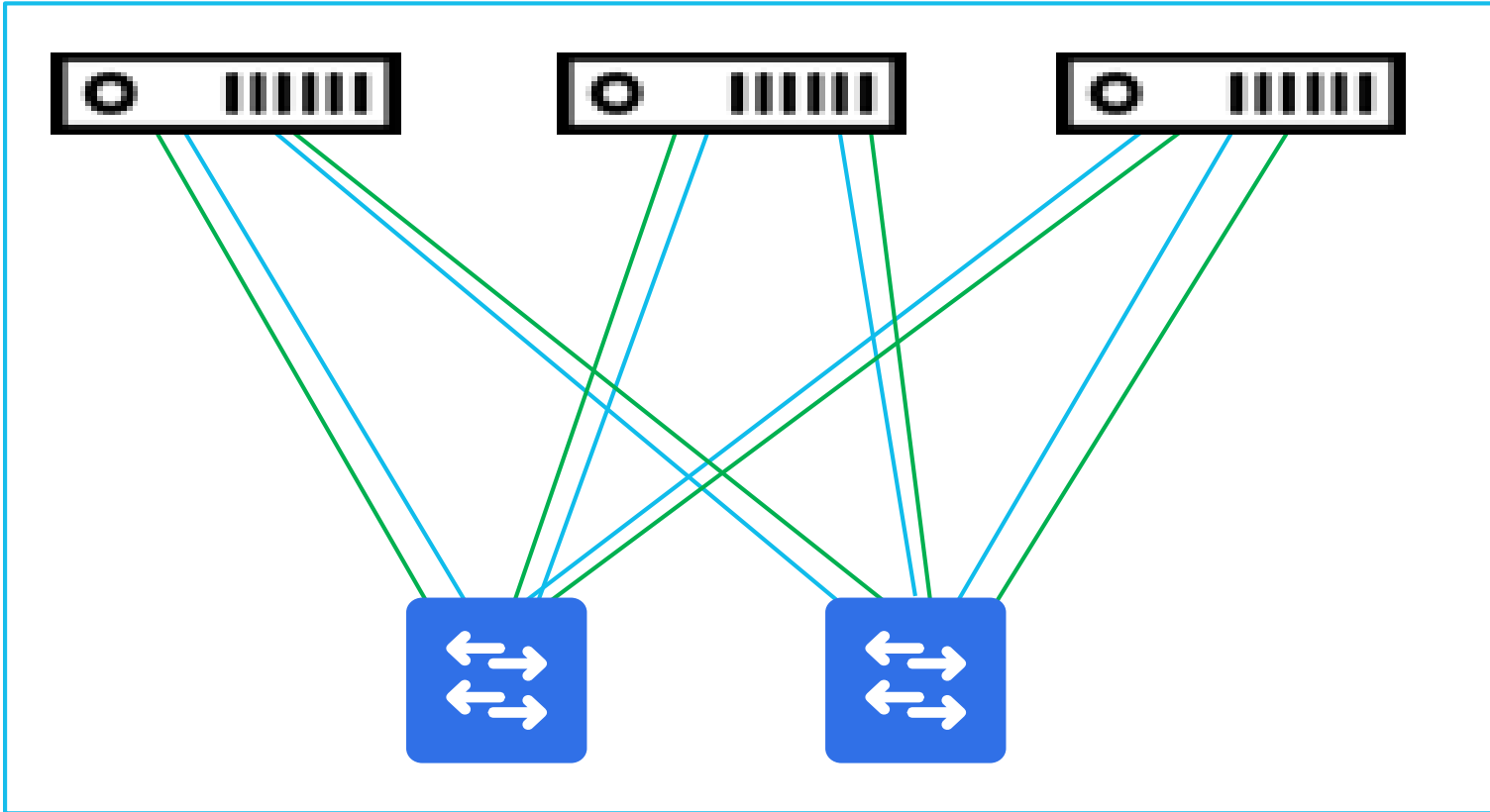


- Two node cluster: Management available but no protection from node failure



- Two node cluster: One node failure will lead to stall of the other node

Physical Appliance High Availability with Clustering



Considerations

- ✓ **Hardware Appliance size needs to match**
- ✓ **3-node cluster in same network, same site**
- ✓ **DN2 + DN3 mixed clusters 2.3.7.9**

Cisco Catalyst Center- 3 Node Cluster Bring-up Best Practices



Physical Appliance

- Bring up first node: choose “create a cluster”

Node 1 bring up

Single node cluster:
validate configuration

```
Welcome to the Maglev Configuration Wizard!
```

```
The wizard will walk you through the steps to configure this host. Select one of the options below to specify how you would like to configure this host:
```

```
Start a Cisco DNA Center Cluster
```

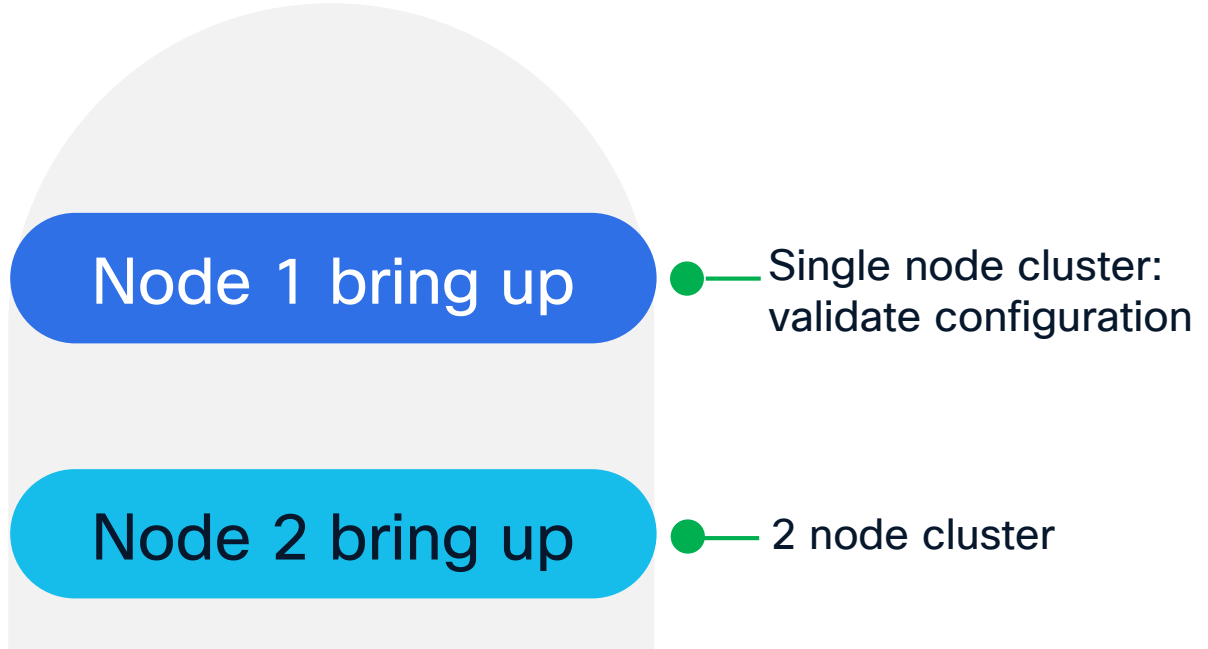
```
Join a Cisco DNA Center Cluster
```

Cisco Catalyst Center- 3 Node Cluster Bring-up Best Practices



Physical Appliance

- Bring up first node: choose “create a cluster”
- Bring up the second node (“join cluster”)



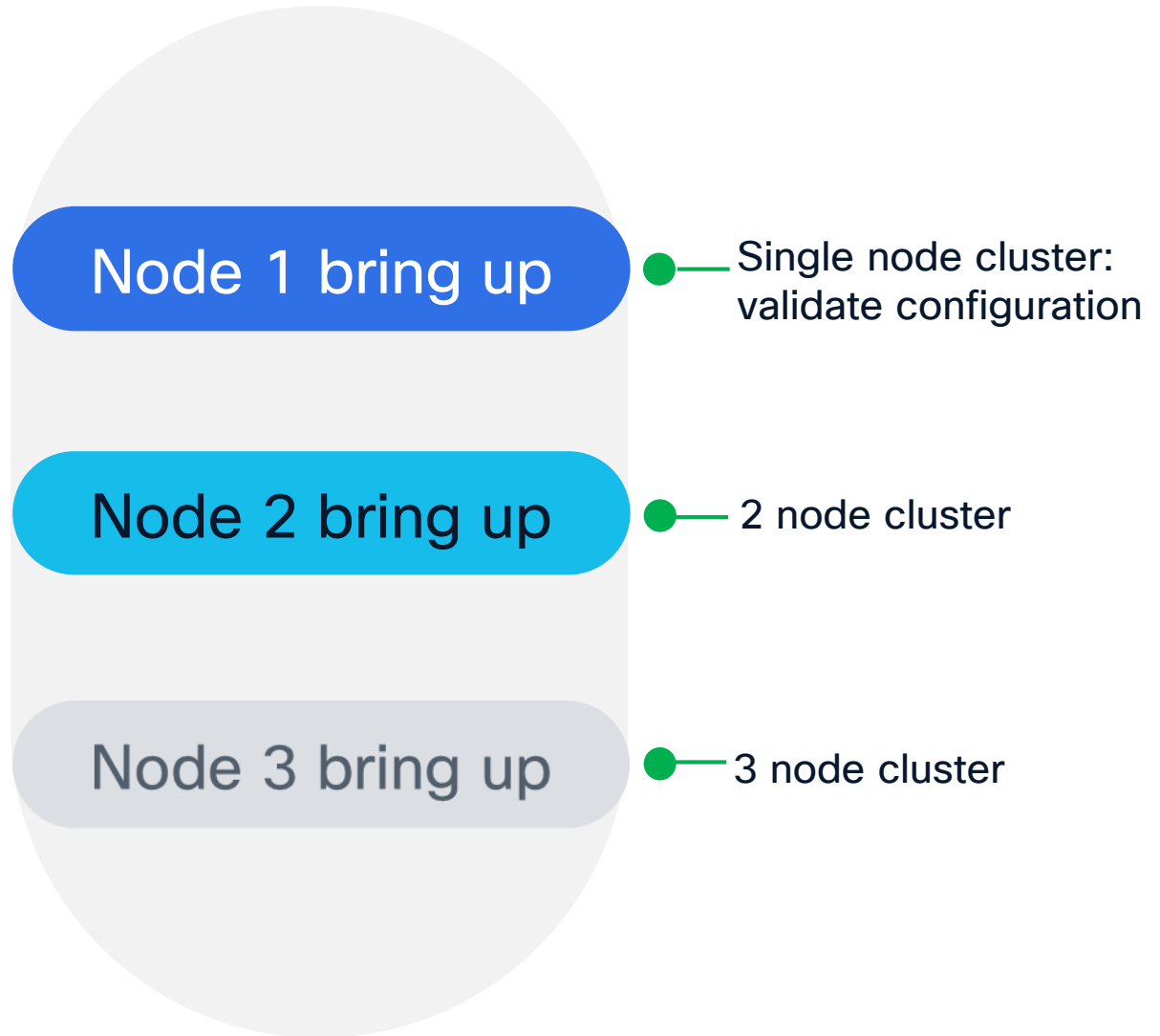
```
Welcome to the Maglev Configuration Wizard!  
  
The wizard will walk you through the steps to configure this host. Select one of the options below to specify how you would like to configure this host:  
  
Start a Cisco DNA Center Cluster  
Join a Cisco DNA Center Cluster
```

Cisco Catalyst Center- 3 Node Cluster Bring-up Best Practices



Physical Appliance

- Bring up first node: choose “create a cluster”
- Bring up the second node (“join cluster”)
- Bring up the third (“join cluster”)



Activate HA in Catalyst Center

▲ High availability is currently unavailable. Visit [System Settings](#) to enable.

Catalyst Center System / System 360

System 360 System Health Service Explorer

System 360

Cluster

Hosts (3)

As of Jan 7, 2025 9:39 AM

- 169.254.65.11
- 169.254.65.12
- 169.254.65.13

[View 123 Services](#)

High Availability

As of Jan 7, 2025 9:39 AM

● Your system meets the requirements for High Availability.

[Activate HA](#)

Cluster Tools

As of Jan 7, 2025 9:38 AM

- Monitoring [↗](#)
- Log Explorer [↗](#)

System Management

Software Management

As of Jan 7, 2025 9:39 AM

- Connected to Cisco's software server.
- Your system is up to date
- 12 applications are available for download

[View](#)

Backups

As of Jan 7, 2025 9:39 AM

● No backups server configured

[Configure](#)

Application Health

As of Jan 7, 2025 9:39 AM

- Automation
- Assurance

Windows App

Catalyst Center HA settings

⚠ High availability is currently unavailable. Visit [System Settings](#) to enable.

System / Settings

Catalyst Center

Search: high

System Configuration




High Availability

Settings / System Configuration

High Availability

Activate High Availability to reduce your system's downtime and distribute risk of failure across multiple hosts.

Status **Inactive**

		
169.254.65.11	169.254.65.12	169.254.65.13

[Activate High Availability](#)

Catalyst Center HA settings

The screenshot shows the Catalyst Center interface for High Availability settings. The breadcrumb trail is 'Settings / System Configuration'. The page title is 'High Availability' with a sub-description: 'Activate High Availability to reduce your system's downtime and distribute risk of failure across multiple hosts.' A blue box highlights the 'Status Active' section, which displays three hosts with green status indicators and IP addresses: 169.254.65.11, 169.254.65.12, and 169.254.65.13.

High Availability in Virtual Appliances

Clustering is not supported with ESXi VM and AWS VA

High Availability is delivered using the hosting infrastructure HA features

Edit Cluster Settings | danc-cluster

vSphere HA

Failures and responses | Admission Control | Heartbeat Datastores | Advanced Options

You can configure how vSphere HA responds to the failure conditions on this cluster. The following failure conditions are supported: host, host isolation, VM component protection (datastore with PDL and APD), VM and application.

Enable Host Monitoring ⓘ

> Host Failure Response	Restart VMs ▾
> Response for Host Isolation	Disabled ▾
> Datastore with PDL	Power off and restart VMs ▾
> Datastore with APD	Power off and restart VMs - Conservative restart policy ▾
> VM Monitoring	Disabled ▾

High Availability in ESXi VA

ESXi High Availability delivered via VMware vSphere's HA functionality

If a host failure occurs, the virtual machines restart on alternate hosts

At least two hosts must have the unreserved CPU/Memory resources required for ESXi VM

The screenshot shows the 'Edit Cluster Settings' window for a cluster named 'danc-cluster'. The 'vSphere HA' toggle is turned on. The 'Failures and responses' tab is selected, showing a list of failure conditions and their corresponding actions. The 'Enable Host Monitoring' toggle is also turned on. At the bottom right, there are 'CANCEL' and 'OK' buttons.

Failure Condition	Action
Host Failure Response	Restart VMs
Response for Host Isolation	Disabled
Datastore with PDL	Power off and restart VMs
Datastore with APD	Power off and restart VMs - Conservative restart policy
VM Monitoring	Disabled

High Availability in AWS VA



If a Catalyst Center EC2 (*) instance crashes, AWS brings up another instance automatically

Single-node EC2 HA within an Availability Zone (AZ) is enabled by default.

The screenshot shows the AWS IAM console interface for creating an access key. It features the AWS logo at the top, followed by three input fields: 'AWS Account ID * ⓘ' containing the value '878813814009', 'Access Key ID * ⓘ' which is currently empty, and 'Secret Access Key * ⓘ' which is also empty. A blue button with a circular arrow icon is positioned at the bottom right of the form.

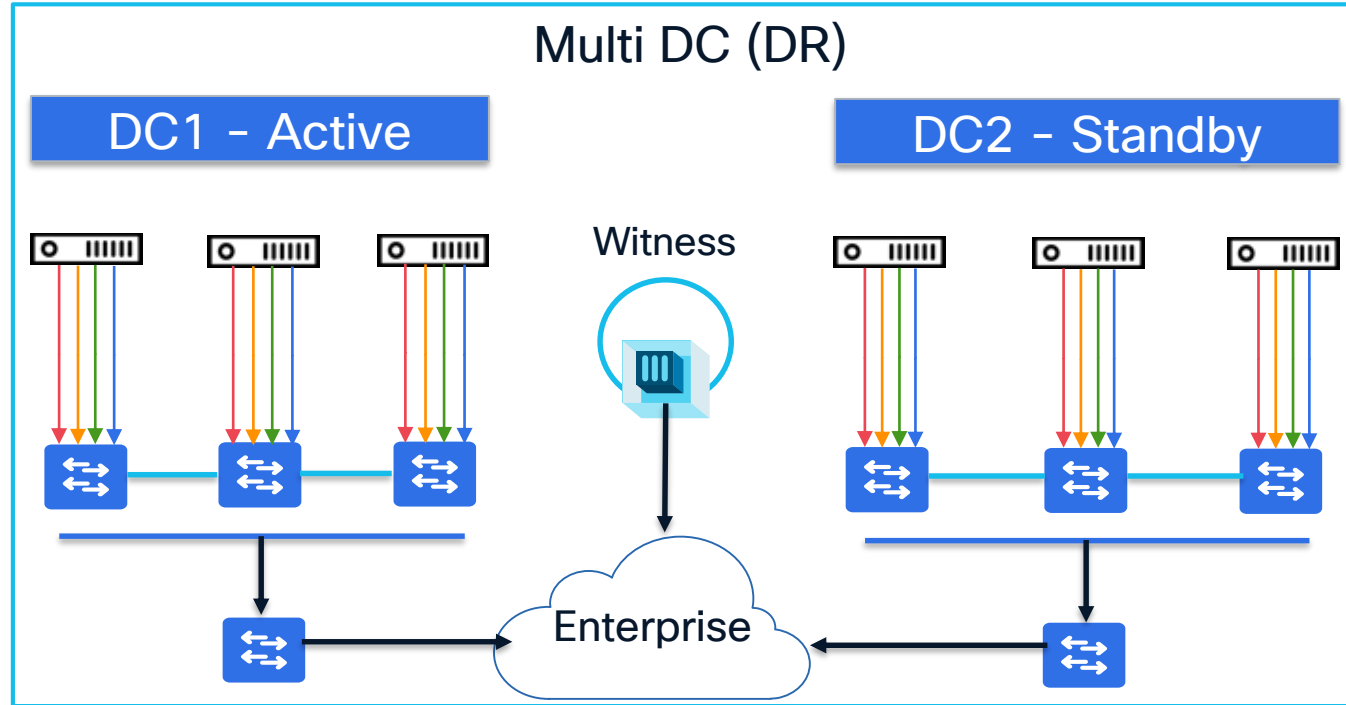
(*) Amazon EC2: Amazon Elastic Compute Cloud

Disaster Recovery

Physical Appliance Disaster Recovery



Physical Appliance



✓ Resiliency in Site failure

✓ Active/Standby

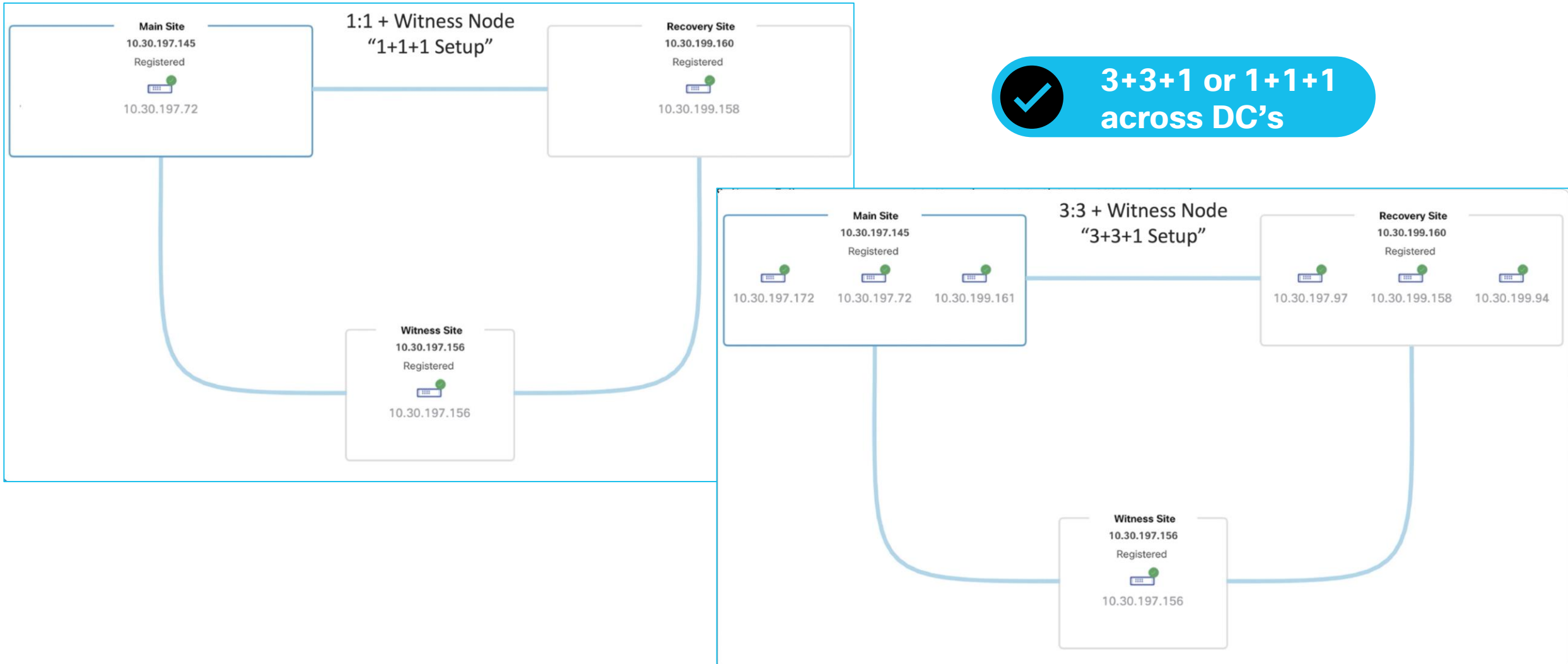
✓ Not all data gets replicated

✓ 3+3+1 or 1+1+1 across DC's

Physical Appliance Disaster Recovery



Physical Appliance

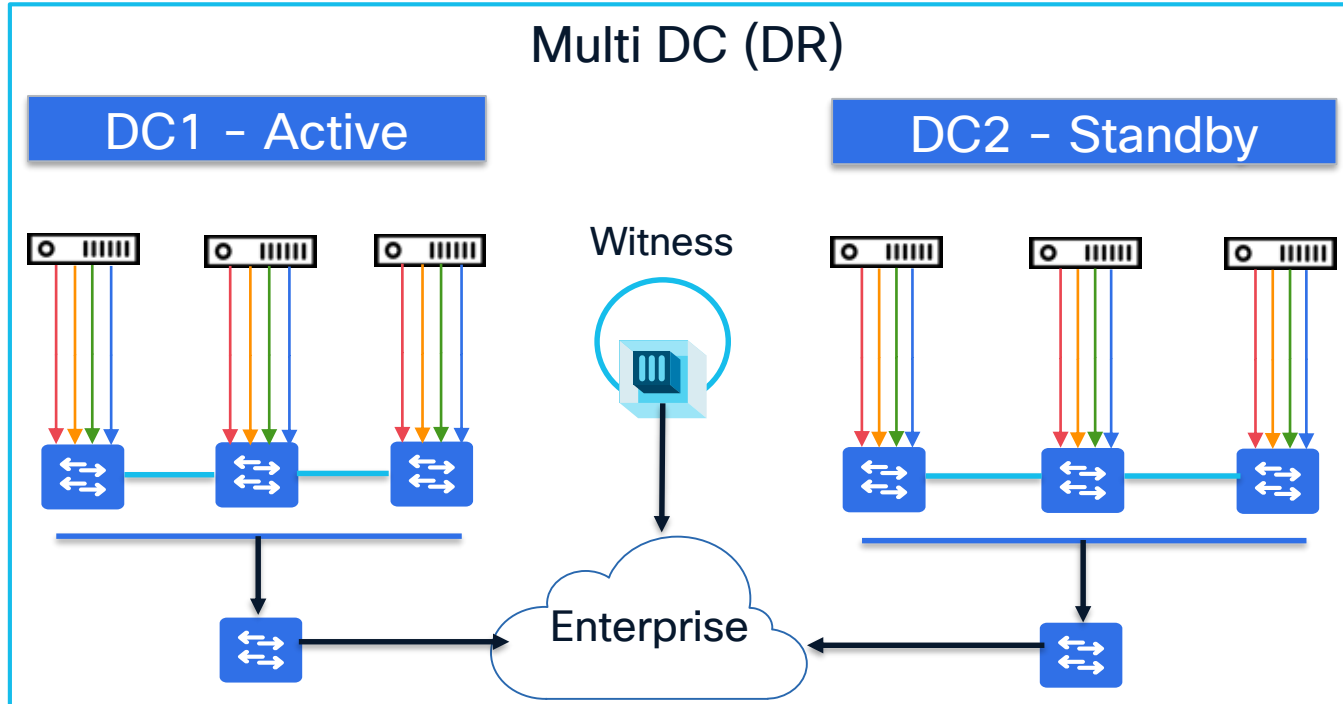


Physical Appliance Disaster Recovery



Physical Appliance

Considerations



Identical third-party certificates on both DR clusters. Don't use self-signed certs



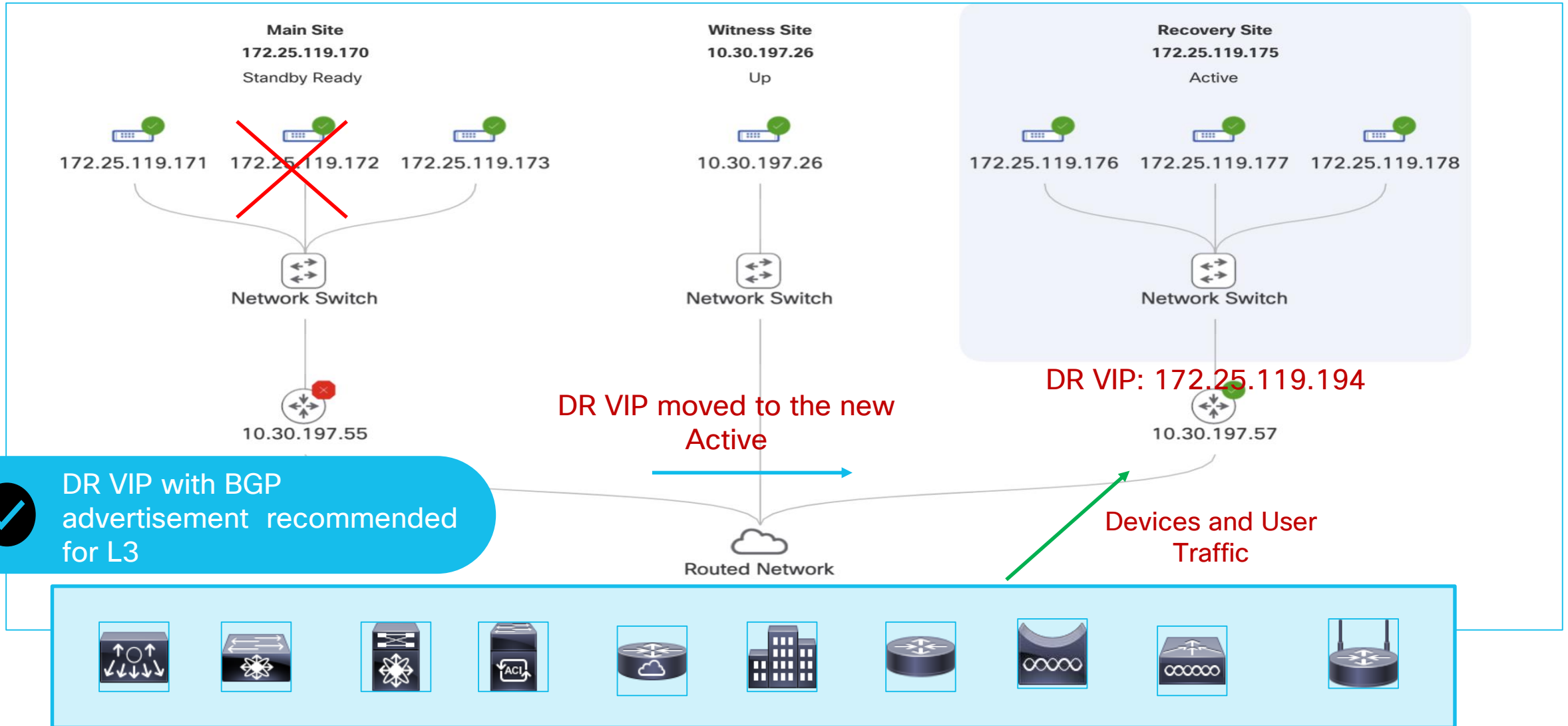
Deploy witness in a third location



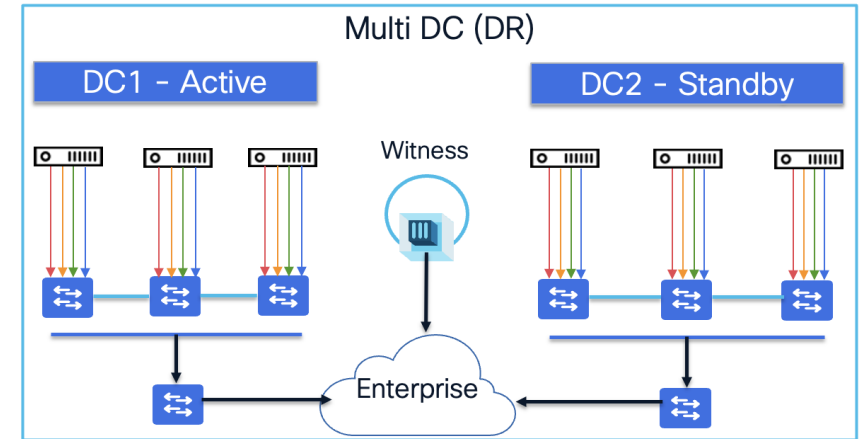
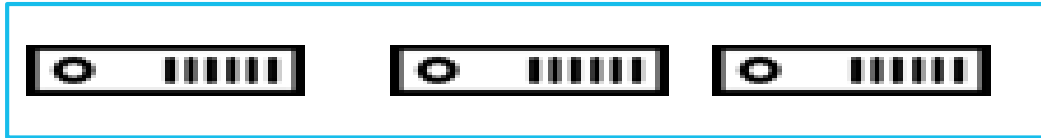
DR VIP with BGP advertisement
** recommended for L3

How to Configure Disaster Recovery: https://youtu.be/PVQi_9h8iSg?si=g02hVlwJzDGBIZOT

Physical Appliance Disaster Recovery



Implications of DR VIP on Firewall Rules



HA Mode:

- Outbound traffic sourced from real IP of the Appliance
- Inbound traffic sent to VIP for HA

DR Mode:

- Outbound traffic sourced from DR VIP
- Inbound traffic sent to DR VIP

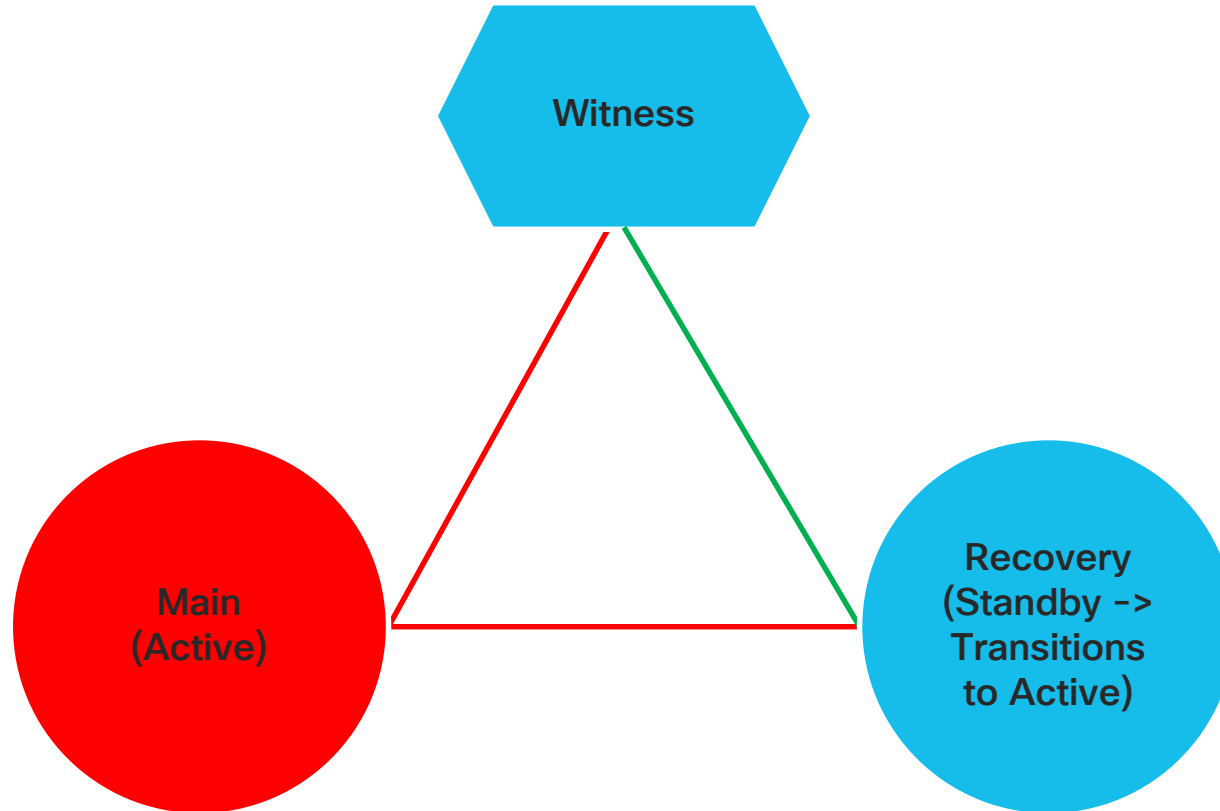
Careful with FW rules e.g. internet access during upgrade (pause DR)

Physical Appliance Disaster Recovery



Physical Appliance

Main Failure Scenarios: **Active is down**



Quorum between passive and witness.

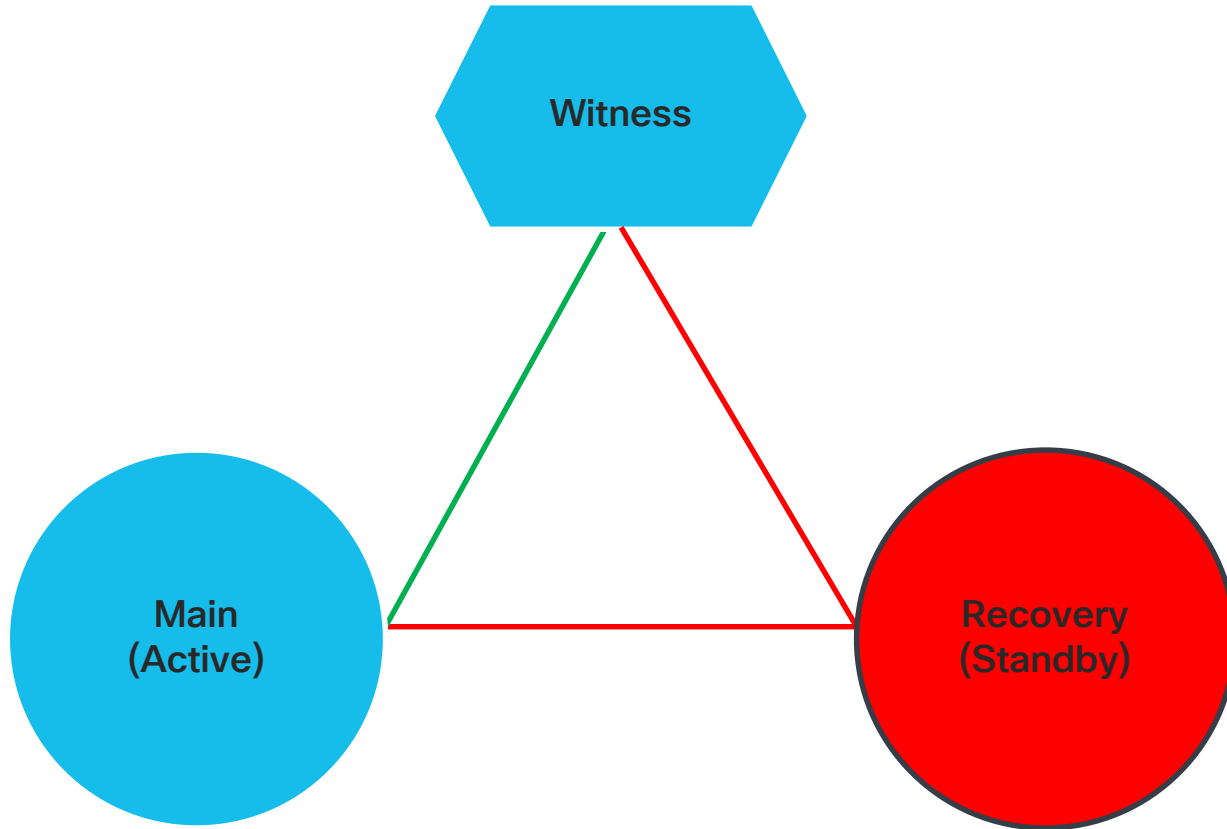
Standby will failover to active and become active, and active will be isolated

Physical Appliance Disaster Recovery



Physical Appliance

Main Failure Scenarios: **Standby is down**



Active and witness still have a quorum. There is no real activity so there's no failover. The active remains active.

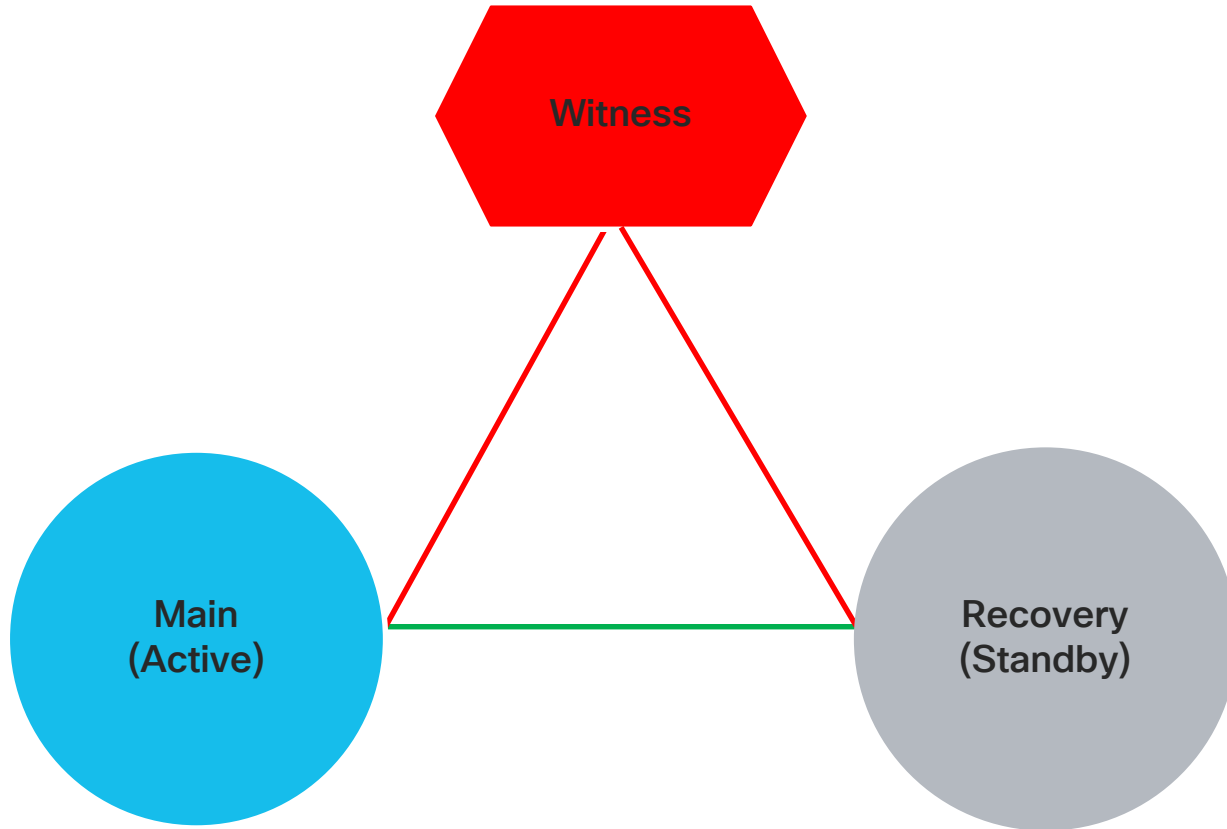
Once the standby comes back up, Standby will need to rejoin DR once back in network

Physical Appliance Disaster Recovery



Physical Appliance

Main Failure Scenarios: **Witness is down**



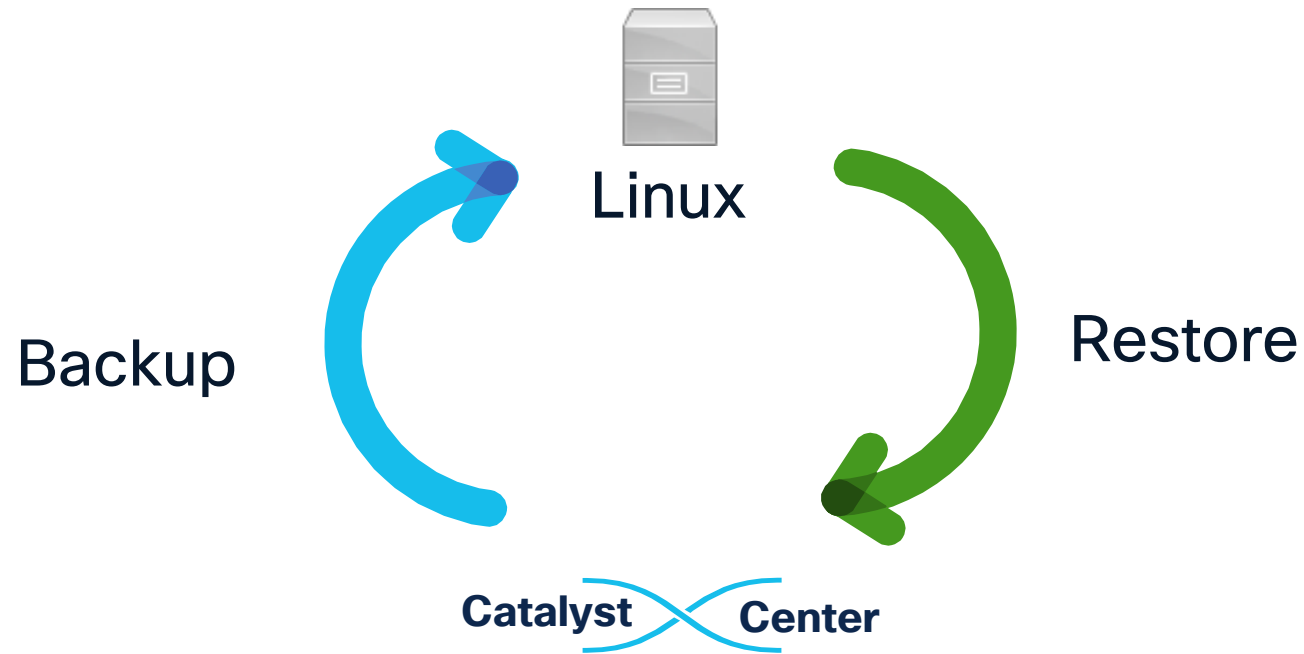
No possibility for quorum, auto-failover is disabled

When witness comes back up, there's no need for manual re-join, it will come back up in the DR system

Backup & Restore

Backup & Restore

- Make a copy of your automation and assurance data
- Restore Catalyst Center back to its previous state
- Migrate data from one of type of server to another



Backup and Restore - Appliance, AWS VA, ESXi VA

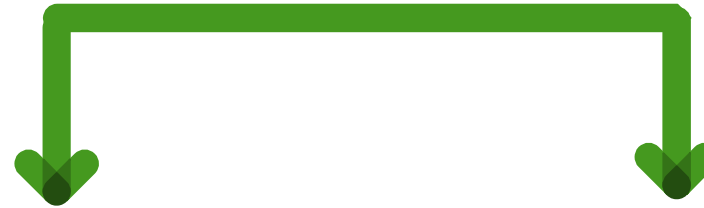


Physical Appliance


vmware[®]
by Broadcom



↓ Types of backup



 System and network automation ★

 System, network automation and assurance

Backups can be On-Demand or Scheduled

Backup and Restore - Appliance, AWS VA, ESXi VA



Physical Appliance



↓ Types of backup

Create Backup

BASICS

Backup Name*
10oct2023

Create now Schedule daily Schedule weekly

Repeat weekly on:

S M T W T F S

At this time:
🔒
12 : 00 : AM

SCOPE

Cisco DNA Center (All data) ⓘ
 Cisco DNA Center (without Assurance data) ⓘ

Use this option to back up only automation data. With this option, Assurance data is not backed up.

Create Backup

BASICS

Backup Name*
10oct2023

Create now Schedule daily Schedule weekly

Repeat weekly on:

S M T

At this time:
🔒
12 : 00

SCOPE

Cisco DNA Center (All data) ⓘ
 Cisco DNA Center (without Assurance data) ⓘ

Use this option to back up automation and Assurance data. You must have two backup directories:

- One backup location is an external NFS server for Assurance data;
- One backup location is an external remote sync (rsync) target location for automation and system data;

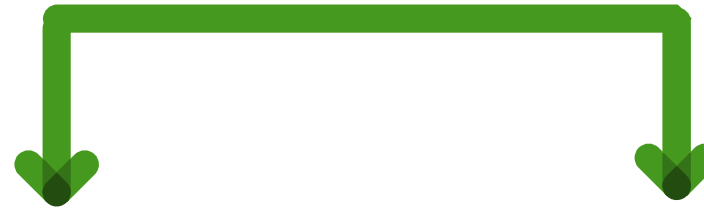
Backup and Restore - Appliance, AWS VA




Physical Appliance

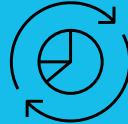


Backup Destinations



 RSYNC for Automation Backup



 Linux-based NFS server for Assurance Backup

Backup and Restore - Appliance, AWS VA



Physical Appliance



Navigation: System / Backup & Restore

Backup & Restore

Backups Schedule Activity **Configure**

Cisco DNA Center (Remote Host) *i* Cisco DNA Center (NFS) *i*

Configured

SSH IP Address*
10.85.54.179

SSH Port*
22 [Hint](#)

Server Path*
/home/netadmin/TRN6_DNAC_Backups/

Username*
netadmin

Password*

Encryption Passphrase* [Hint](#)

Navigation: System / Backup & Restore

Backup & Restore

Backups Schedule Activity **Configure**

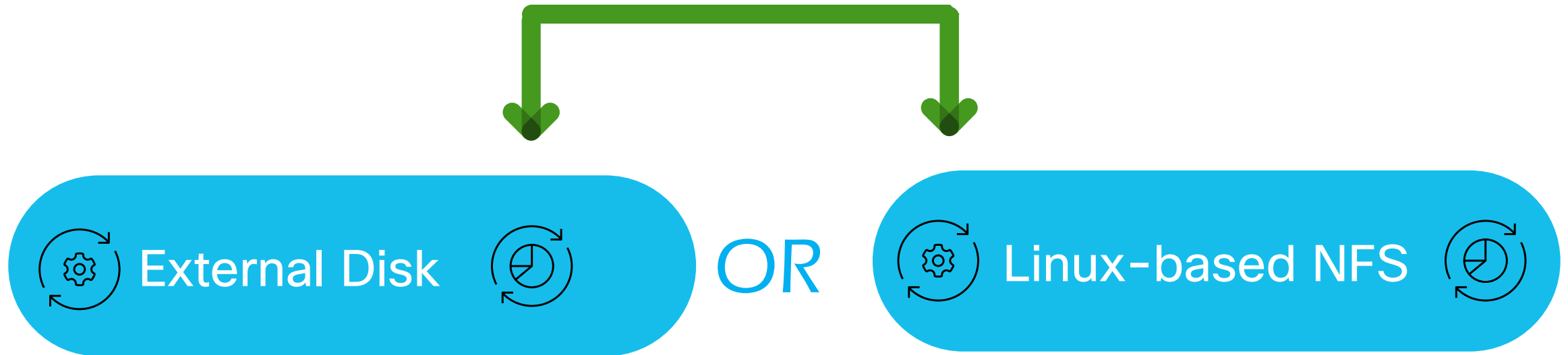
Cisco DNA Center (Remote Host) *i* Cisco DNA Center (NFS) *i*

Configured

Host*
10.85.54.179

Server Path*
/home/netadmin/TRN6_DNAC_Backups/

Backup Destinations



Single destination for System, Automation and Assurance & ability to schedule data retention

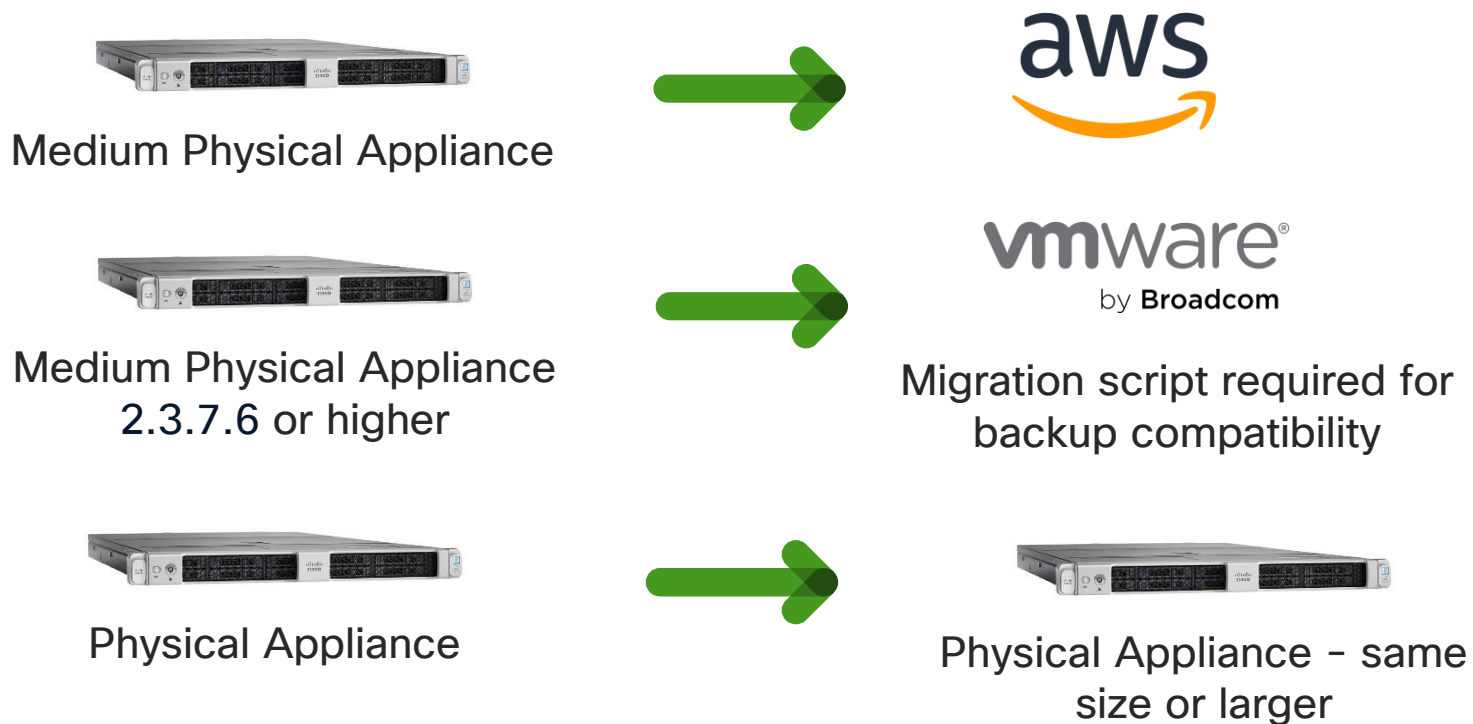
Backup and Restore - ESXi Virtual Appliance

The screenshot shows the Cisco DNA Center interface. The main page is titled "Backup Configuration" under "System / Settings". It features a sidebar with navigation options like "System Configuration", "Backup Configuration", and "Trust & Privacy". The main content area includes a "Physical Disk" section and a "Network File System (NFS)" section. The NFS section is active, showing a "Mount Path" of "nfs://nfs-e51b0f72-fb9b-5b09-b7a5-95c6d8b62419" and an "Encryption passphrase" field. A dialog box titled "Add NFS" is open on the right, with fields for "Server Host*" (10.106.172.227), "Source Path*" (/var/share/storage-1), "NFS Version*" (NFS 4), "Port" (2050), and "Port Mapper" (111). At the bottom of the dialog are "Cancel" and "Save" buttons. A blue box highlights the "Backup Retention" field, which is set to "14", and the "Reset" and "Submit" buttons.

Migration

Physical Appliance to Physical Appliance or AWS VA

- Migration is based on B&R
- Supports migration from: physical to physical or physical to virtual



Restore

- **Software version:**
 - **For Physical Appliance and AWS VA restore works on exact same software version of Catalyst Center**
 - **For ESXi VA can be restored on the same or later Catalyst Center software version**

What if You Don't Know the Backup Version

- In backup folder, there will be backup-metadata:
- Open the latest .json file
- Match packages from release notes

```
netadmin@DNAC-Backup-Server:~$ ls TRN6_DNAC_Backups/
app-hosting.postgres  fusion.postgres  maglev-system.credentialmanager  maglev-system.mongodb  ndp.elasticsearch
backup-metadata       maglev-system    maglev-system.glusterfs          ndp                       ndp.redis
netadmin@DNAC-Backup-Server:~$
```

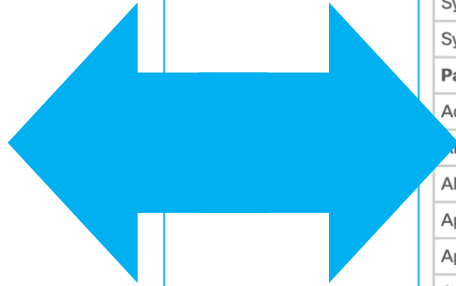
```
netadmin@DNAC-Backup-Server:~$ ls -la TRN6_DNAC_Backups/backup-metadata
total 164
drwxr-xr-x  2 netadmin netadmin  4096 Mar 13 08:30 .
drwxrwxrwx 12 netadmin netadmin  4096 Feb 27 09:16 ..
-rw-rw-r--  1 netadmin netadmin 51048 Dec  2 11:28 5e7f902f-3766-4590-a056-07df18467765.json
-rw-rw-r--  1 netadmin netadmin 51056 Jan 24 16:48 9a18b64a-675f-4416-b76e-9382bc0361ef.json
-rw-rw-r--  1 netadmin netadmin 51055 Feb 27 11:33 f43ae636-f47f-4faf-ba65-7045eb2b1aaf.json
```

Compare Metadata file with Release Notes

```

file:///Users/lila/f43ae636-f47f-4faf-ba65-7045eb2b1aaf.json
pretty print
{
  "_id": "67c088c2220b563a73ca1920",
  "backup_id": "f43ae636-f47f-4faf-ba65-7045eb2b1aaf",
  "operation": "BACKUP",
  "service_fqn": "fusion:postgres",
  "_version": 4,
  "backup_size": 8138475258,
  "description": "27feb2025",
  "fips_enabled": "false",
  "id": "5f82b794-ad17-423f-9f83-df1deb8bdfc2",
  "last_modified": 1740673958.60146,
  "maglev_address_family": "ipv4",
  "start_time": "2025-02-27 15:46:10",
  "start_timestamp": 1740671170.71485,
  "status": "completed",
  "target_node": "192.168.12.25",
  "tenantId": "SYS0",
  "versions": [
    "ise-bridge:2.1.716.90701",
    "ndp-ui:1.9.5001",
    "catalyst-center-api-catalog:1.15.69",
    "cloud-connectivity-data-hub:1.15.57",
    "ai-network-analytics:3.1.41.389",
    "cloud-connectivity-tethering:2.36.1.47",
    "cloud-connectivity-contextual-content:2.11.2.542",
    "dnac-search:1.15.1.12",
    "system-remediation:1.4.0",
    "wide-area-bonjour:2.4.718.75196",
    "app-hosting:2.3.12406270628",
    "system:1.8.232",
    "platform-ui:1.7.7.71",
    "dnac-platform:1.15.96.0",
    "ndp-platform:1.9.5055",
    "ndp-base-analytics:2.3.7.750049",
    "assurance:2.3.7.7004",
    "ncp-system:2.1.720.60128",
    "automation-core:2.1.720.60128",
    "machine-reasoning:2.1.720.210013",
    "network-visibility:2.1.720.60128",
    "rbac-extensions:2.1.720.1900009",
    "cisco-dna-docs:2.1.720.60128",
    "path-trace:2.1.720.60128",
    "command-runner:2.1.720.60128",
    "appsvc-remediation:1.1.30",
    "access-control-application:2.1.720.60128",
    "sd-access:2.1.720.60128",
    "application-registry:2.1.720.117227",
    "application-policy:2.1.720.117227",
    "ssa:2.1.720.1090100",
    "system-commons:2.1.720.60128",
    "disaster-recovery:2.1.720.360029",
    "dna-core-apps:2.1.720.60128",
    "image-management:2.1.720.60128",
    "device-onboarding:2.1.720.60128",
    "base-provision-core:2.1.720.60128",
    "sensor-automation:2.1.720.60128",
    "sensor-assurance:2.3.7.7003",
    "rogue-management:2.9.0.653",
  ]
}

```



Package versions in Catalyst Center

To download Catalyst Center software, go to <https://software.cisco.com/download/home/286316341/type>.

Package Name	Release 2.3.7.9	Release 2.3.7.7	Release 2.3.7.6	Release 2.3.7.5	Release 2.3.7.4
Release Build Version					
Release Version	2.3.7.9.70301	2.3.7.7-70047-CSCwn89323.SMU	2.3.7.7.70047	2.3.7.6.70319	2.3.7.5.70434
System Updates					
System	1.8.409	1.8.232	1.8.222	1.8.114	1.7.1105
System Commons	2.1.722.60901	2.1.720.61514	2.1.720.60128	2.1.718.60779	2.1.715.60719
Package Updates					
Access Control Application	2.1.722.60901	2.1.720.61514	2.1.720.60128	2.1.718.60779	2.1.715.60719
Endpoint Analytics	1.11.1325	1.11.1185	1.11.1180	1.11.1166	1.11.938
AI Network Analytics	3.3.59.23	3.3.58.21	3.1.41.389	3.1.39.362	3.1.30.335
Application Hosting	2.3.22412090506	2.3.12406270628	2.3.12406270628	2.3.12402020457	2.3.12311300818
Application Policy	2.1.722.117743	2.1.720.117227	2.1.718.117586	2.1.715.117447	2.1.714.117457
Application Registry	2.1.722.117743	2.1.720.117227	2.1.718.117586	2.1.715.117447	2.1.714.117457
Application Visibility Service	2.1.722.117743	2.1.720.117227	2.1.718.117586	2.1.715.117447	2.1.714.117457
Application and Service Remediation	1.2.1009	1.1.32	1.1.30	1.1.27	-
Assurance - Base	2.3.7.9226	2.3.7.7006	2.3.7.7004	2.3.7.6236	2.3.7.5165
Assurance - Sensor	2.3.7.9163	2.3.7.7003	2.3.7.6206	2.3.7.5122	2.3.7.4139
Automation - Base	2.1.722.60901	2.1.720.61514	2.1.720.60128	2.1.718.60779	2.1.715.60719
Automation - Intelligent Capture	2.1.722.60901	2.1.720.60128	2.1.718.60779	2.1.715.60719	2.1.714.60631
Automation - Sensor	2.1.722.60901	2.1.720.60128	2.1.718.60779	2.1.715.60719	2.1.714.60631
Catalyst Center API Catalog	1.16.95.0	1.15.69	1.15.69	-	-

Catalyst Center Global Manager for multi-site management

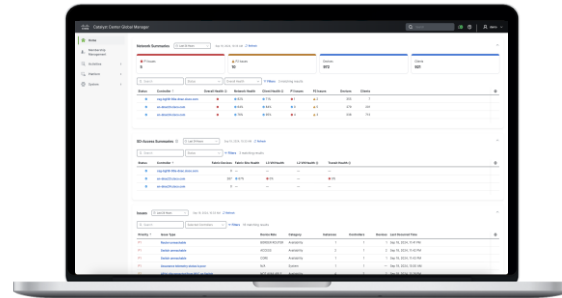
Why Catalyst Center Global Manager (CCGM)?

Single Pane of Glass



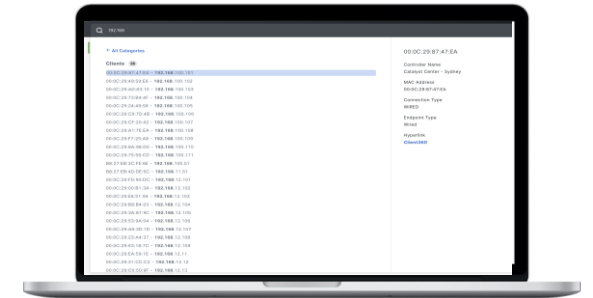
- Catalyst Center
- Unified View
- Enhanced Administrative Efficiency

Issue Monitoring +



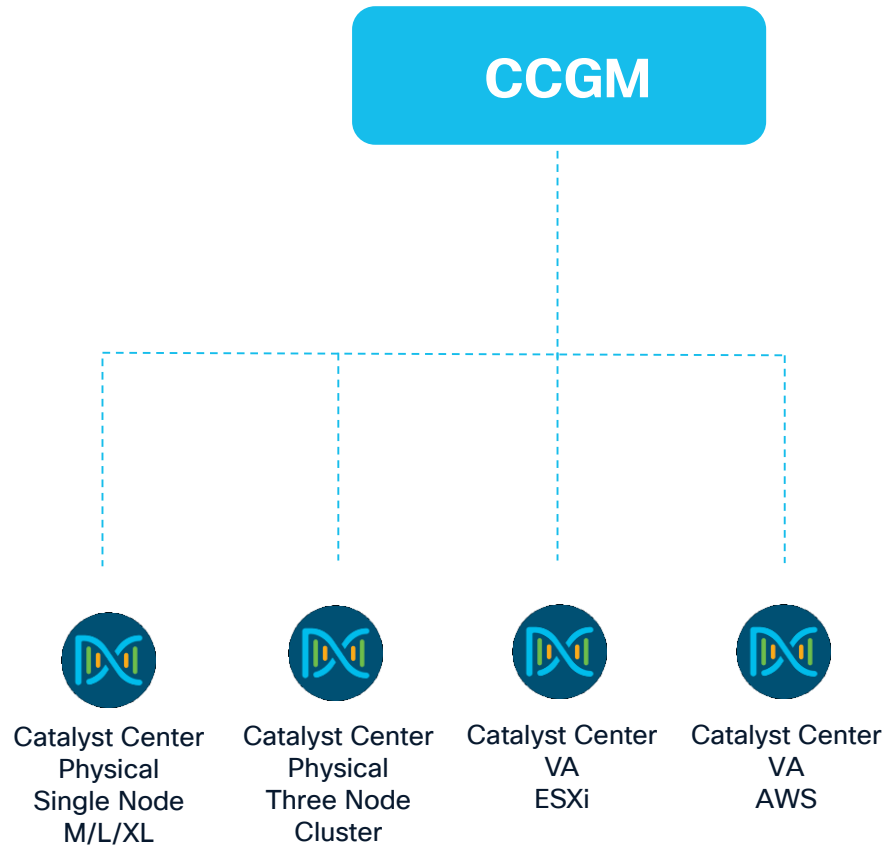
- Monitors Network, Client, Devices Health
- Monitors SD-Access Fabric Health.
- Reports P1/P2/P3 issues from any Catalyst Center
- Cross-launch without requiring additional username and password authentication.

Global Search



- Global search to clients and network devices via IP Address, Hostname, MAC address, Software version, and other metadata.
- Cross-launch into 360 view of the client/device

CCGM Requirements



- vCenter and ESXi host running 7.0.x or higher

- 16 vCPU,
- 32GB RAM
- 100 GB + 550GB SSD HDD

- 25 Controllers (Catalyst Centers 2.3.7.9+) can be added to CCGM

- 350 msec Latency

- Smart Account and Virtual Account Created for Catalyst Center registration with CCGM

Home page

The screenshot displays the Cisco Catalyst Center Global Manager interface. The top navigation bar includes the Cisco logo, the title 'Catalyst Center Global Manager', a search bar, and a user profile for 'adam'. A left-hand sidebar contains navigation options: Home, Membership Management, Workflows, Activities, Platform, and System.

The main content area is divided into three sections:

- Network Summary:** Shows a time filter for 'Last 24 Hours' and a refresh button. It features four summary cards: 'P1 Issues' (1), 'P2 Issues' (0), 'Devices' (20), and 'Clients' (4). Below these is a table with 3 matching results, filtered by 'Overall Health'.

Status	Controller	Overall Health	Network Health	Client Health	P1 Issues	P2 Issues	Devices	Clients
●	172.29.76.152	●	—	—	—	—	—	—
●	adamlab.cisco.com	●	● 33%	—	● 0	● 0	3	0
●	pnpserver.adamlab.cisco.com	●	● 88%	● 75%	● 1	● 0	17	4
- SDA Summary:** Also shows a time filter for 'Last 24 Hours' and a refresh button. It includes a table with 3 matching results, filtered by 'Status'.

Status	Controller	Fabric Devices	Fabric Site Health	L3 VN Health	L2 VN Health	Transit Health
●	172.29.76.152	— —	—	—	—	—
●	adamlab.cisco.com	0 —	—	—	—	—
●	pnpserver.adamlab.cisco.com	0 ● 0%	● 0%	—	—	—
- Issues:** Shows a filter for 'Controller Error' and a time filter for 'Last 24 Hours'. It includes a table with 5 matching results, filtered by 'Selected Controllers'.





Catalyst Center CCGM integration

The screenshot shows the Catalyst Center web interface. The top navigation bar includes the Cisco logo, the text 'Catalyst Center', and 'System / Settings'. A left sidebar contains a search bar and a list of menu items: PnP Device Authorization, Device Controllability, Network Resync Interval, SNMP, ICMP Ping, Device EULA Acceptance, PnP AP Location, Device Prompts, Configuration Archive, External Services (with a dropdown arrow), and Cisco AI Analytics. The main content area is titled 'Global Manager Integration' and includes a breadcrumb 'Settings / External Services'. Below the title is a descriptive paragraph: 'Use this page to integrate your Catalyst Center to the centralized Catalyst Center Global Manager for simplified network management. Monitor and manage your network from one location for seamless operation.' The status section shows 'Connected To' as '10.66.104.107' and 'Enrollment Status' as 'Enrolled' with a green checkmark icon. A blue 'Unenroll' button is present. A note at the bottom states: 'Click 'Unenroll' to unlink this Catalyst Center from your Catalyst Center Global Manager.'

Closing and Q&A

Today's Mission: Architect Catalyst Center to Scale, Adapt, and Endure

Guiding Questions from this session:

-  **What form factor best fits our needs based on our scale requirements?**
-  **Is a distributed environment necessary? How would we manage it?**
-  **Do we need resiliency? How do we design for resiliency and recovery?**
-  **How do we future-proof growth – horizontally or vertically?**

Complete your session evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to win 1 of 5 full conference passes to Cisco Live 2026.



Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.



Level up and earn exclusive prizes!



Complete your surveys in the Cisco Live mobile app.

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 www.CiscoLive.com/on-demand

Contact me at: cisco.com/go/catalyst-center / cs.co/dnac-resources

The logo for Cisco Live! is displayed in a white rectangular box. It features the word "CISCO" in a bold, black, sans-serif font, followed by the word "Live" in a lighter weight of the same font, and a large, bold exclamation point. The background of the slide is a vibrant blue with dynamic, flowing light trails that create a sense of motion and energy.

CISCO Live !

