
cisco Live!
Let's go

Please read

This presentation template uses the CiscoSans TT ExtraLight font. If the text in these two columns does not match, please take a moment to install the font. Otherwise, your presentation will not display correctly.

Please download the fonts from Brand Exchange here. The font can also be found in the zipped folder. Double-click the font file and click “Install” in the window that appears.

This presentation template uses the CiscoSans TT ExtraLight font. If the text in these two columns does not match, please take a moment to install the font. Otherwise, your presentation will not display correctly.

Please download the fonts from Brand Exchange here. The font can also be found in the zipped folder. Double-click the font file and click “Install” in the window that appears.

The bridge to possible

Data Center Operations Maintenance and Migration Best Practices

Anis Edavalath
Principal Architect , Cisco CX

cisco Live!

BRKDCN-2958

Anis Edavalath

- 11 years with Cisco Customer Experience (CX)
- Focused in Strategizing and implementing Digital Transformation including Security , Observability and Hybrid Cloud
- Enterprise Campus and Datacenter across different verticals
- Worked 10 years with BU engineering groups in Security , switching, datacenter and Network Management products
- Design and deployment of Next Gen Data center architecture enterprise and cloud customers
- AS team lead for ACI, VxLAN, Tetration, SDA (uniform policy)
- Worked with major telecom vendors and Cloud providers prior to Cisco
- CCIE Datacenter # 48152

Contributor: Arvind Durai - Director , Cisco Cx

Support:Carlos Campos Torres - Director Product management, Cisco

Course Objective and Goal

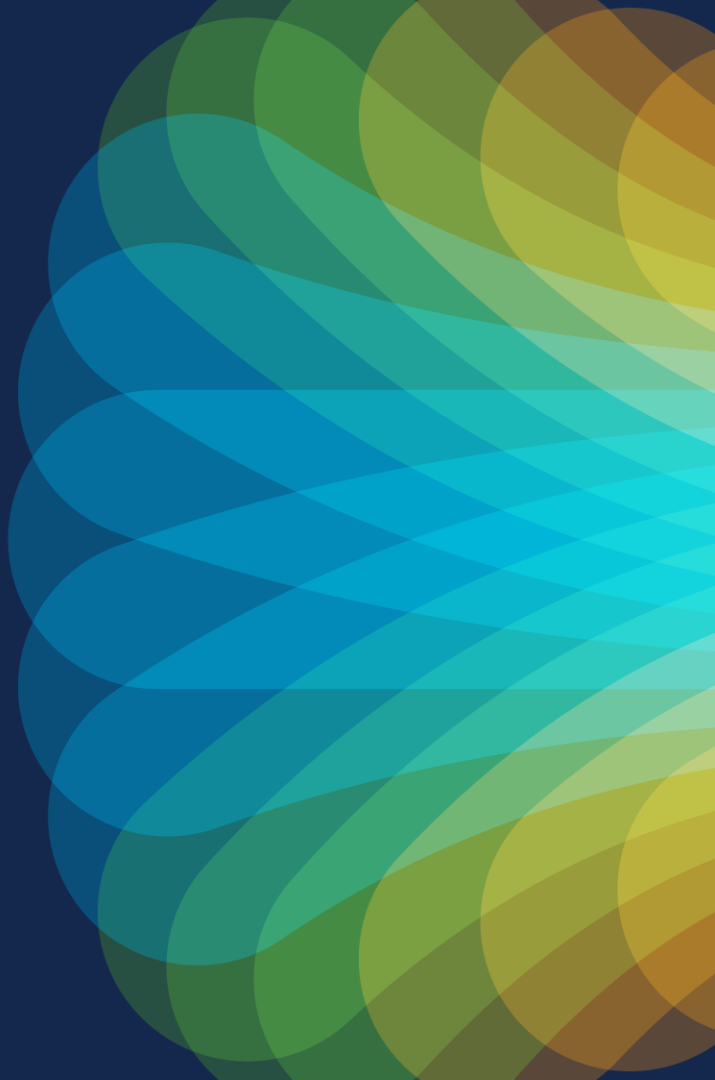
- To help Data Center operations and engineering staff understand the change management best practice to maintain a datacenter environment or migrate a legacy environment to next gen Cisco Nexus data center network deployment.

- Attendees should leave the session with a firm understanding of
  - Baseline – Fabric best practices
  - Operational Best Practices
  - Features and Tools used to manage DC fabric
  - Migration – Features and Tools (controllers)
  - Migration Methodology

Agenda

- Baseline
  - VPC, VxLAN & ACI Refresher
  - Change Management best practices
- Features and Tools
  - Graceful insertion and removal
  - Fabric controllers and Nexus
- Migration Methodology
  - Five key Use cases
- Change Window Best Practices

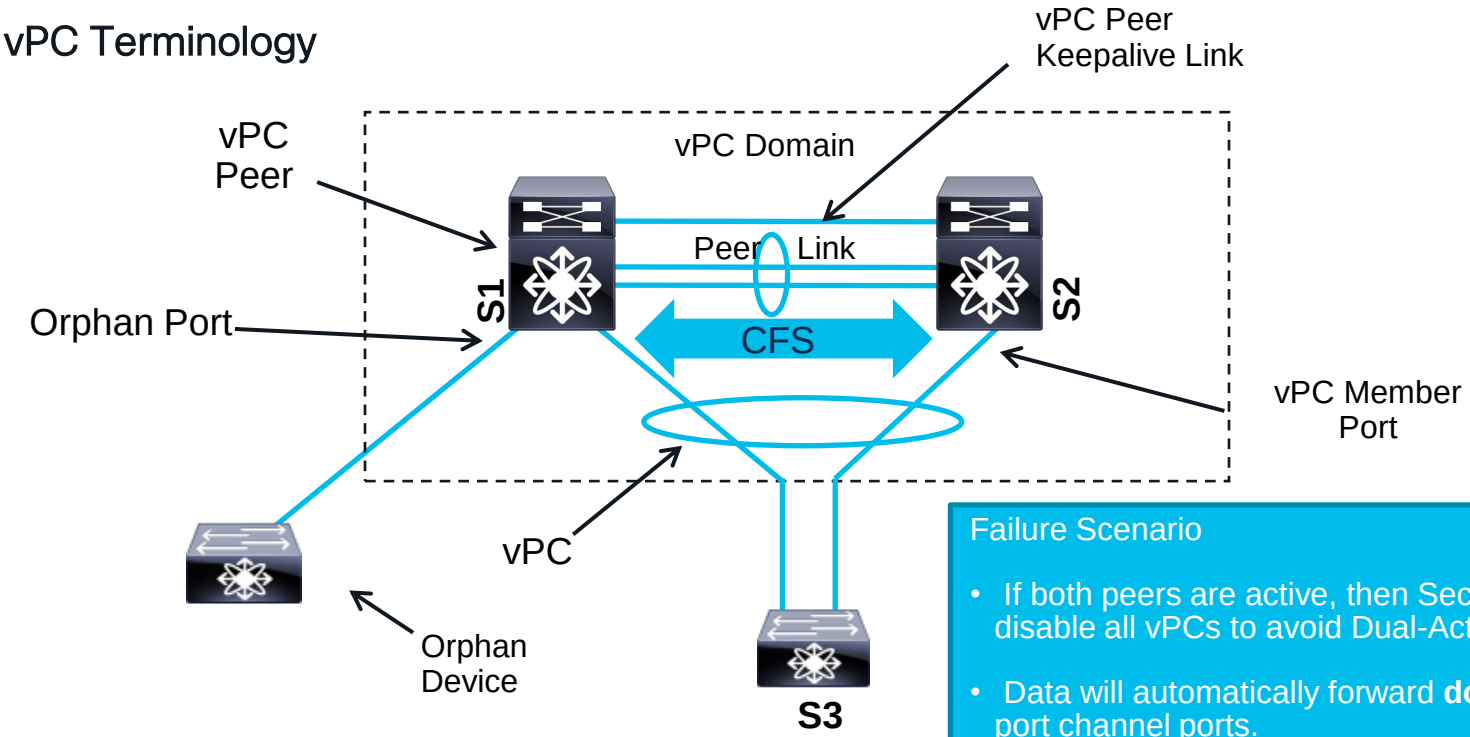
DC Baseline Refresher



vPC Feature Overview

For Your Reference

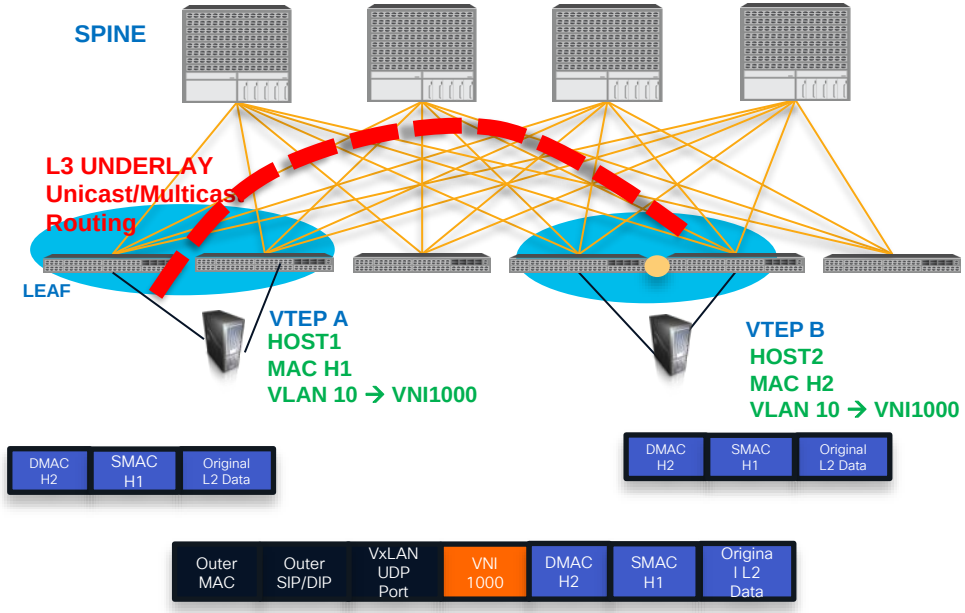
vPC Terminology



Failure Scenario

- If both peers are active, then Secondary vPC peer will disable all vPCs to avoid Dual-Active.
- Data will automatically forward **down** remaining active port channel ports.
- Loss of in-flight packets will depend on deployment of vPC best practice.

VXLAN Overview



VTEP A or VTEP B in deployment will be a pair, and this pair will provide host redundancy for Layer 2 via VPC.

VPC is still NEEDED and VTEP will represent the VPC pair!

Layer 2 overlay on top of your Layer 3 underlay

- Each VXLAN Segment is identified by a unique 24-bit segment ID called a VXLAN Network Identifier (VNI)
- Only hosts on the same VNI are allowed to communicate with each other
- Original L2 packet is encapsulated with VXLAN header in a UDP->IP->Ethernet

Overcome 4094 VLAN Scale Limitation

- VLANs use a 10-bit VLAN ID

Better utilization of available network paths

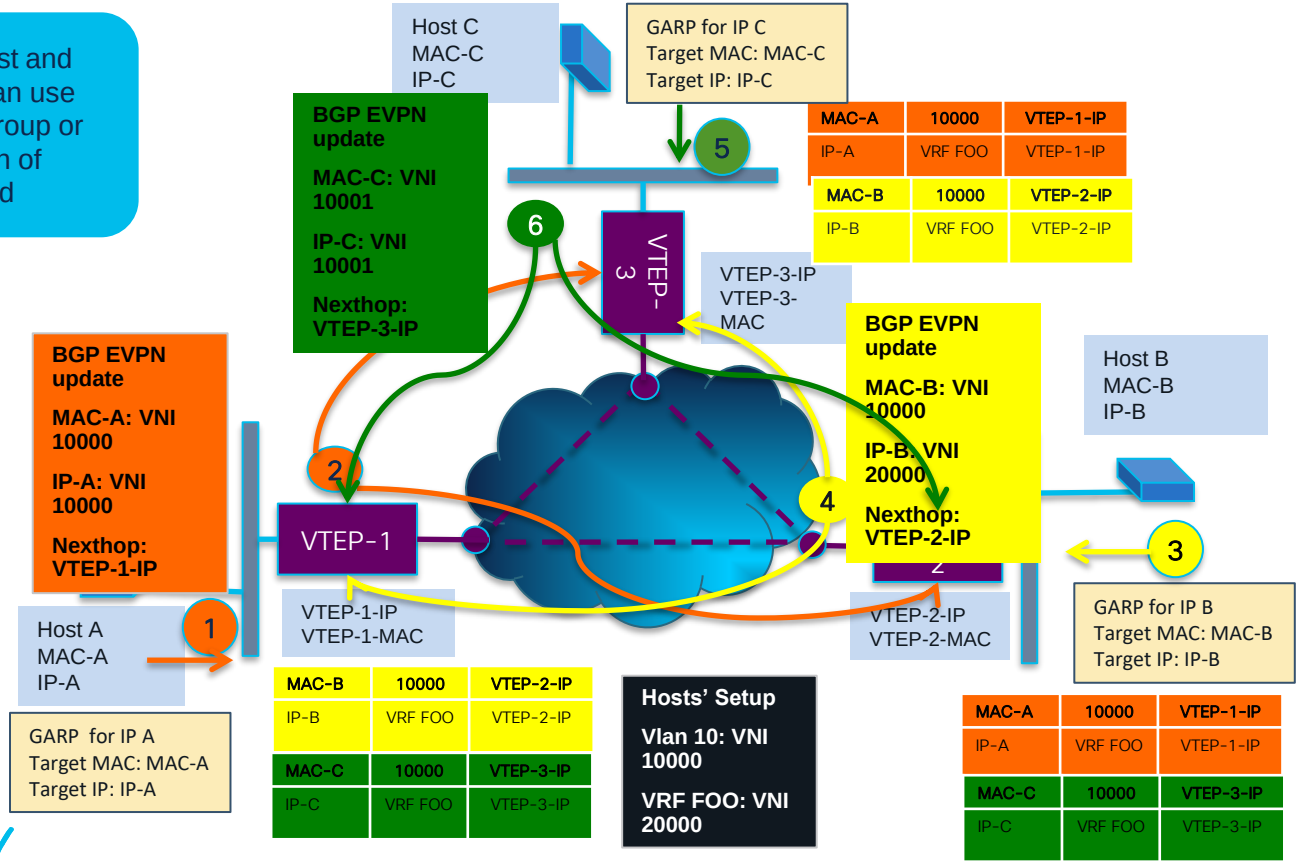
- No need of Spanning Tree (blocks paths)
- Utilize L3 underlay network (ECMP, Link Agg,…)

Multi-Tenant with virtualization

- Isolation of network traffic by a tenant and reusability of networking taxonomy for tenancy

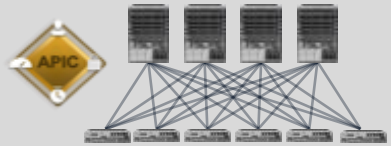
VxLAN Refresher With BGP EVPN Address Learning

Broadcast, Unicast and Multicast traffic can use either Multicast group or Ingress replication of traffic- not covered



SDN ‘with’ FCAPS ‘and’ Automation

Application Centric Infrastructure



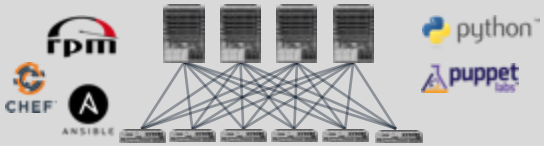
Turnkey integrated solution with security, centralized management, compliance and scale

Automated application centric-policy model with embedded security

Broad and deep ecosystem

Integrated Toolset

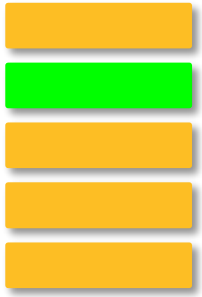
Programmable EVPN Fabric



Modern NX-OS with enhanced NX-APIs

DevOps toolset used for Network Management
(Puppet, Chef, Ansible etc.)

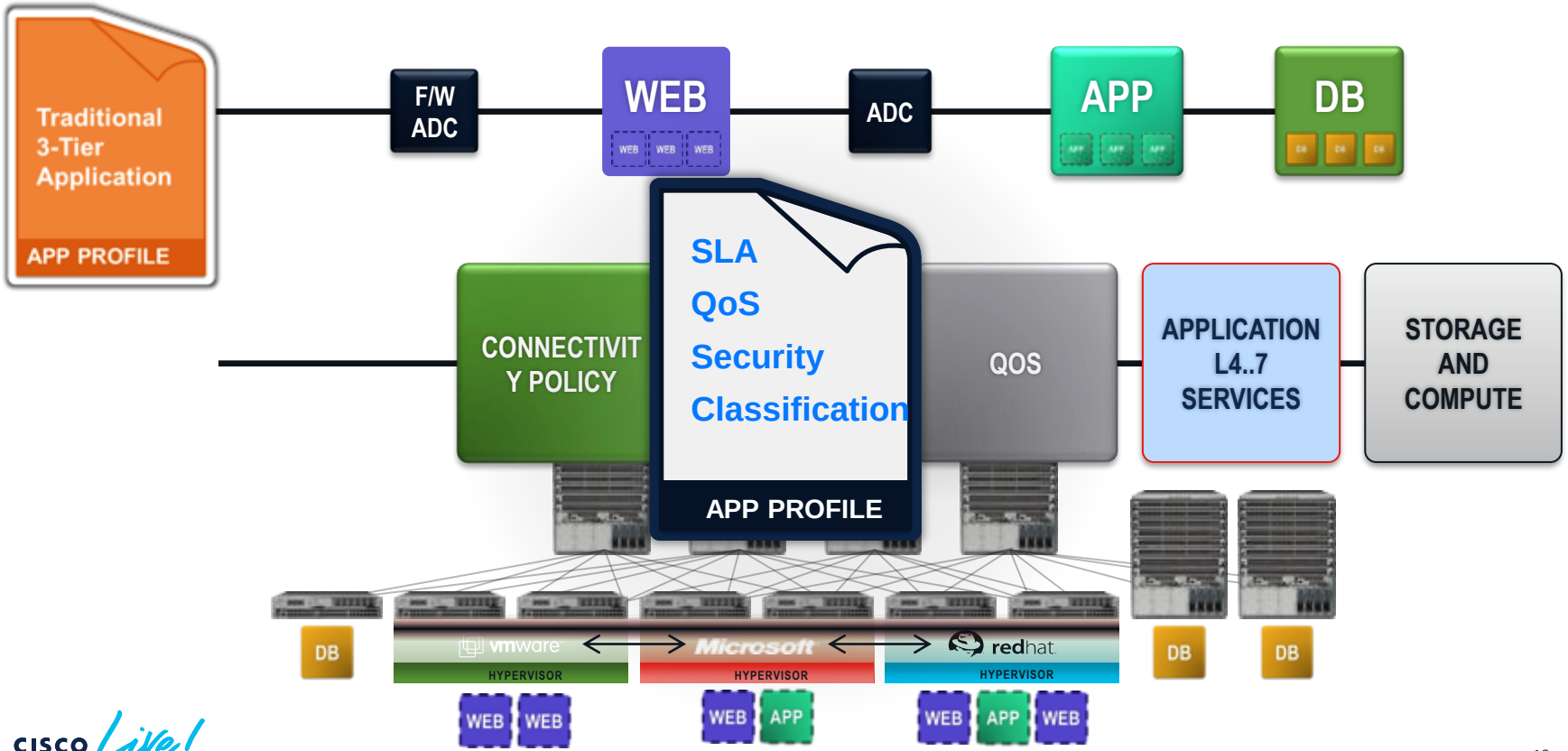
Custom Script based Operations and Workflows



External Tools

NDFC

Application Network Profiles (ANP) & ACI: how it works?

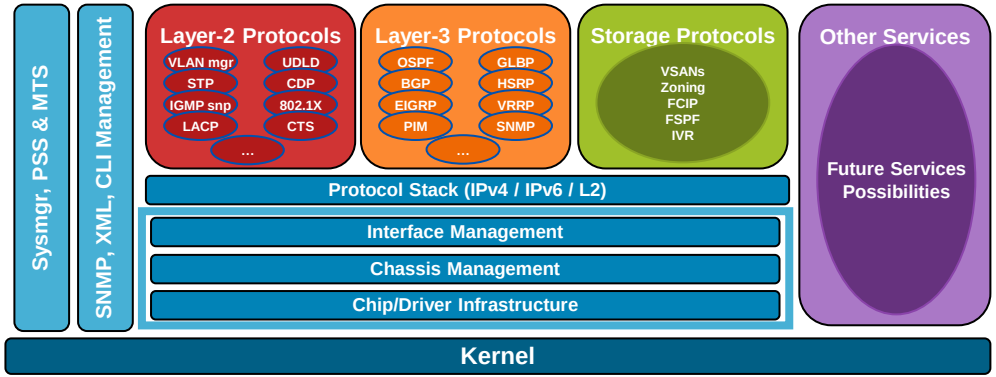


Operational Best Practices

NX-OS High Availability

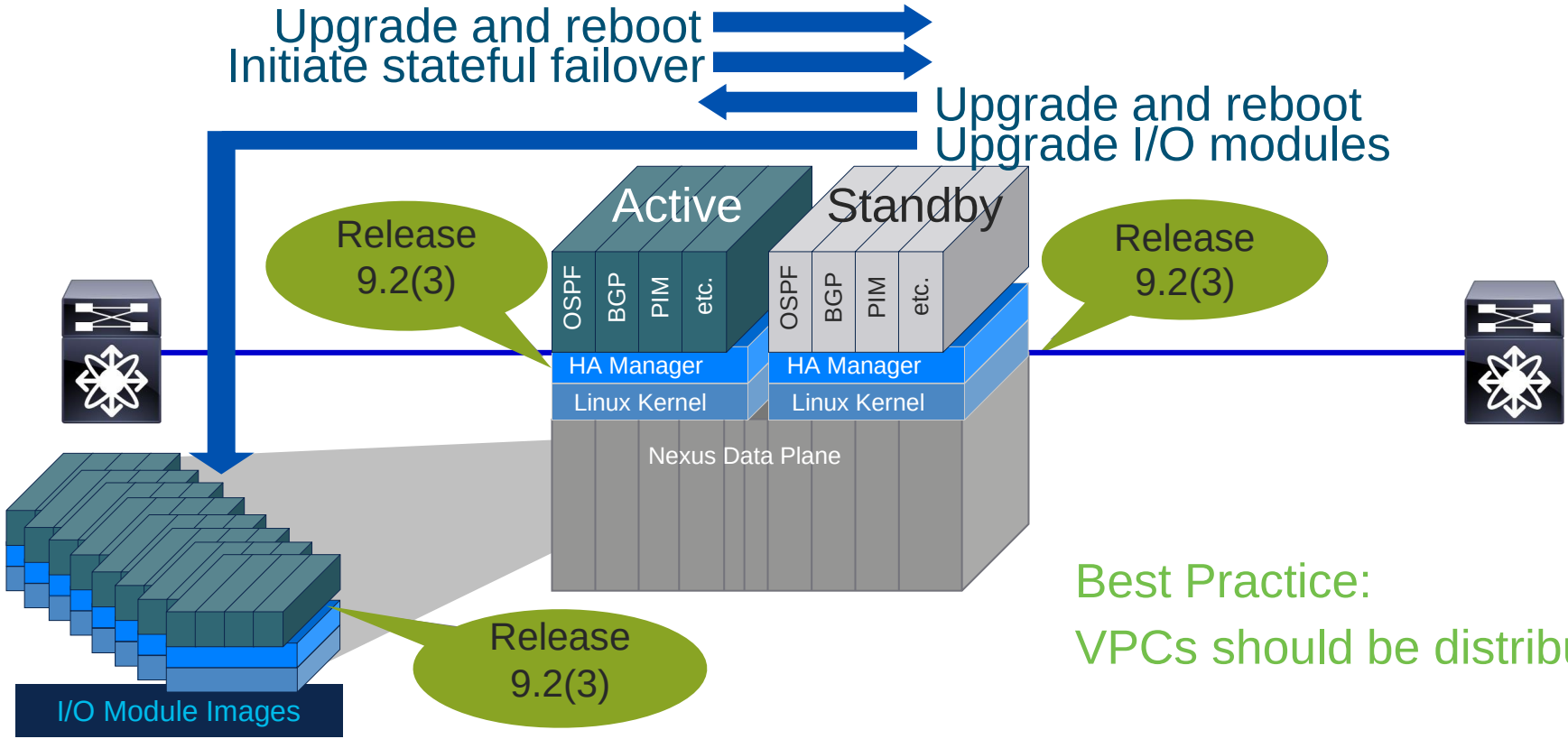
Process Modularity

- Independent memory-protected restart-able processes
- Service Restart-ability
  - Stateful Restart with Persistent Storage Service (PSS)
    - Checkpoints states to PSS
    - Recover states from PSS upon restart.
  - Stateful Restart with Graceful Restart
    - Recover states based on information from other services and/or network.
    - Mainly Routing Protocols
  - Stateless Restart
    - Fresh start, no trace of former instantiation.



In-Service Software Upgrade

```
Nexus# install all nxos bootflash:nxos.9.2.3.bin
```



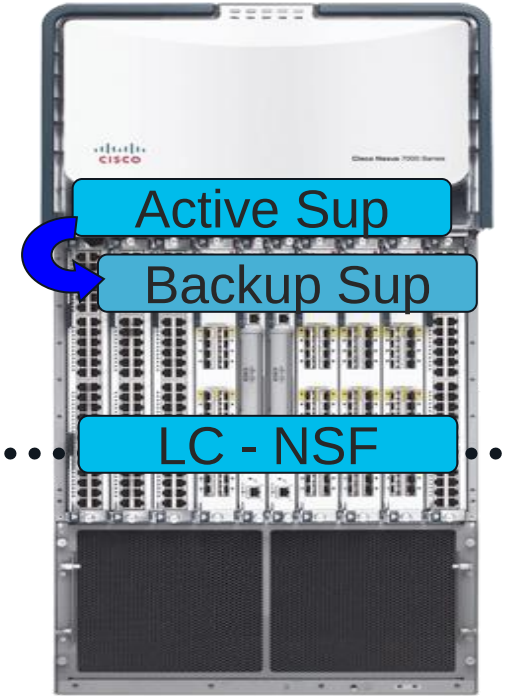
Best Practice:

VPCs should be distributed.

NX-OS High Availability

Supervisor Switchover

- Stateful Switchover (SSO)
  - Active-backup supervisors synchronized at all times
- Routing Protocols: → PSS Stateful Restart
  → NSF Graceful Restart failover
- Other components: → PSS Stateful Restart
- Triggers:
  - HA Policy Initiated – e.g. 3 component crashes → SSO
  - User Initiated – system switchover
  - ISSU initiated SSO



Defect Impact

TAC: You've encountered defect CSCxy12345. It's operationally impacting and, I'm sorry to say, there's no workaround. You'll need to **upgrade**.

Belay my last. We have a SMU for that.

You: Fine. Let's just get it fixed.

Bill, start up a war room.

John, get our AS NCE on the phone.

Sally, schedule testers in two hours.

Where's my $#@! coffee?

What?

Gesundheit.

Sally: You know how Richard gets when we call him at 2 AM...

Software Patching in NX-OS

Who's familiar with Software Maintenance Updates (SMU)?

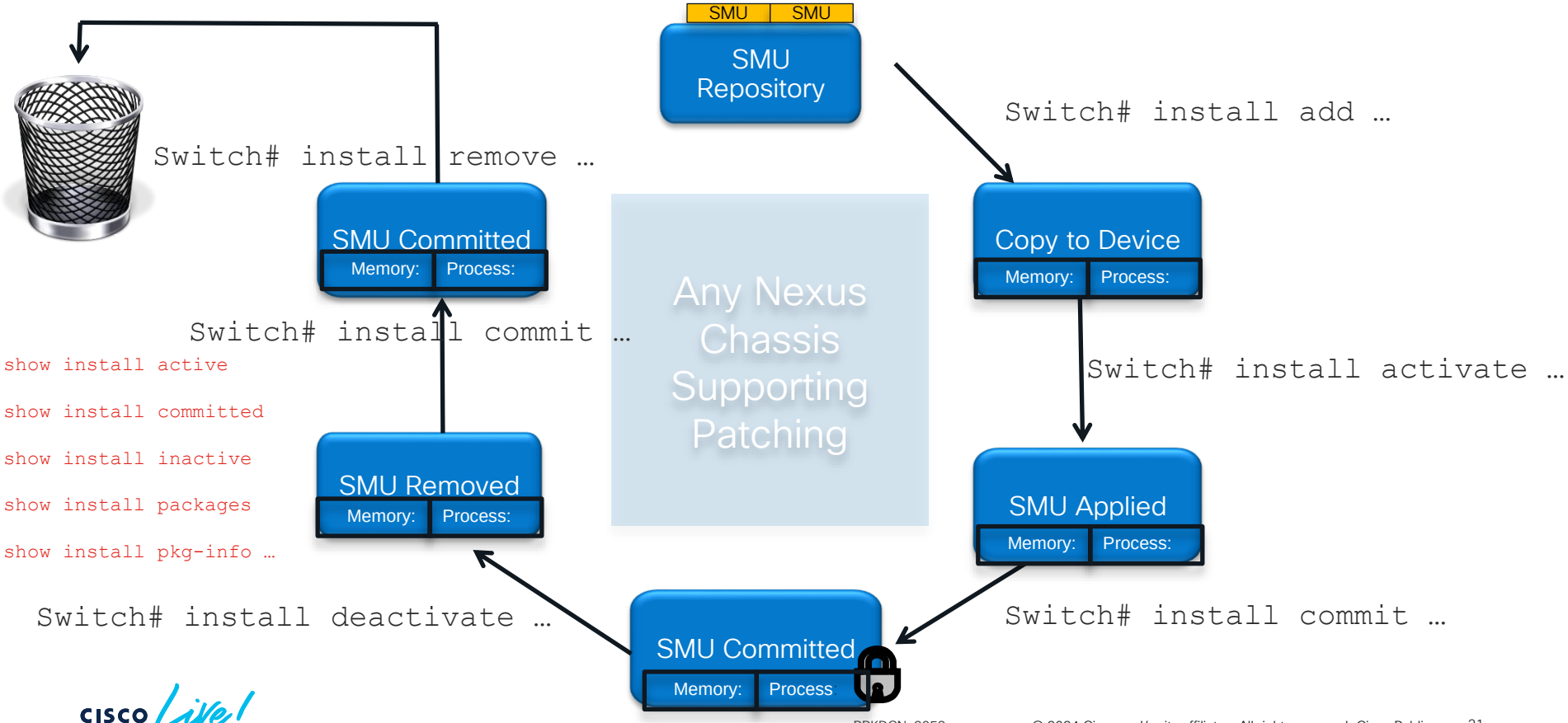
Overview

- Software Patching is Platform Independent
- Available on Nexus 9000 (6.1(2)I2)
- FCS NX-OS 7.2 (5/6/7k)
- Fully supported with ISSU

Benefits

- Reduce time to resolution in your network.
- SMUs in NX-OS build upon years of experience in IOS XR.
- Simplify customer operations for defect resolution and code qualification.
- Better utilize the software HA capabilities of NX-OS.
- Provide a common cross-platform experience (N9K/N7K/N6K/N5K).

SMU Lifecycle – CLI



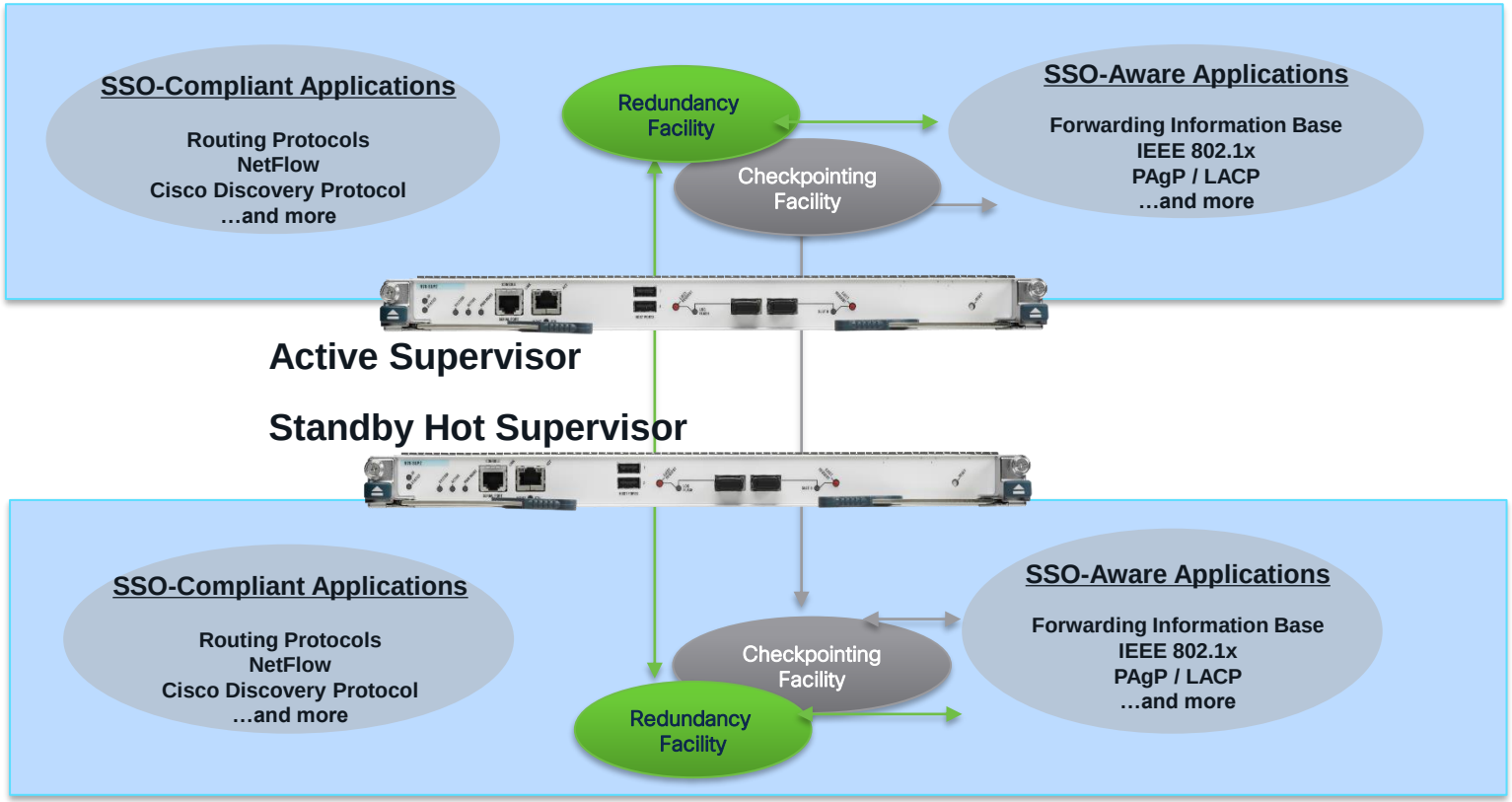
Patching Highlights

SMU Types

- Restart: Restarts affected process
  - Process restarted in all VDCs where running.
- ISSU SMU:
  - Dual Sup -> ISSU
  - Single Sup -> Reload

- Patching is for operationally impacting bugs without a ***workaround.***
  - ***Cannot patch to next release.***
- Patching is done in default/admin VDC and applies to all VDCs.
  - ***Patching is not available per-VDC.***
- ISSU will work with all, or a subset of patches applied.
  - ***You don't need to apply all patches.***
- Some SMUs may only have a single fix, others may have multiple packaged.

Stateful Switchover Mode
SSO-Aware and SSO-Compliant Applications



Routing Protocol Redundancy With NSF
(Graceful Restart)

Active Supervisor Engine Slot 1

EIGRP RIB	
Prefix	Next Hop
10.0.0.0	10.1.1.1
10.1.0.0	10.1.1.1
10.20.0.0	10.1.1.1

OSPF RIB	
Prefix	Next Hop
192.168.0	192.168.0.1
192.168.55.0	192.168.55.1
192.168.32.0	192.168.32.1

ARP Table	
IP	MAC
10.1.1.1	aabbcc:ddee32
10.1.1.2	adbb32:d34e43
10.20.1.1	aa25cc:ddeee8

FIB Table	
Prefix	Next HOP
10.1.1.1	aabbcc:ddee32
10.1.1.2	adbb32:d34e43
192.168.0.0	aa25cc:ddeee8

Standby Supervisor Engine Slot 2

EIGRP RIB	
Prefix	Next Hop
-	-
-	-
-	-

OSPF RIB	
Prefix	Next Hop
-	-
-	-
-	-

ARP Table	
IP	MAC
-	-
-	-
-	-

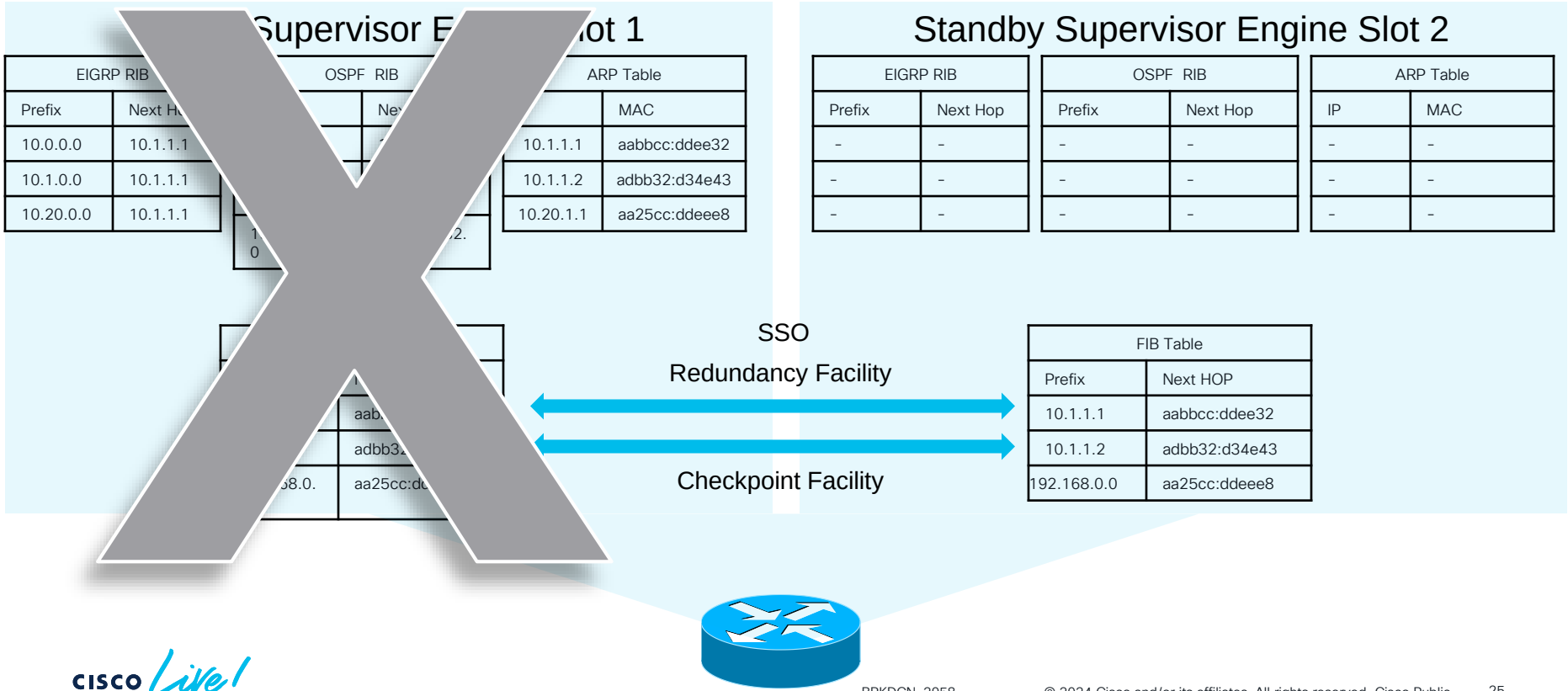
FIB Table	
Prefix	Next HOP
10.1.1.1	aabbcc:ddee32
10.1.1.2	adbb32:d34e43
192.168.0.0	aa25cc:ddeee8

SSO

Redundancy Facility

Checkpoint Facility

Routing Protocol Redundancy With NSF
(Graceful Restart)



Routing Protocol Redundancy With NSF
(Graceful Restart)

Standby Supervisor Engine Slot 2

EIGRP RIB	
Prefix	Next Hop
10.0.0.0	10.1.1.1
10.1.0.0	10.1.1.1
10.20.0.0	10.1.1.1

OSPF RIB	
Prefix	Next Hop
192.168.0	192.168.0.1
192.168.55.0	192.168.55.1
192.168.32.0	192.168.32.1

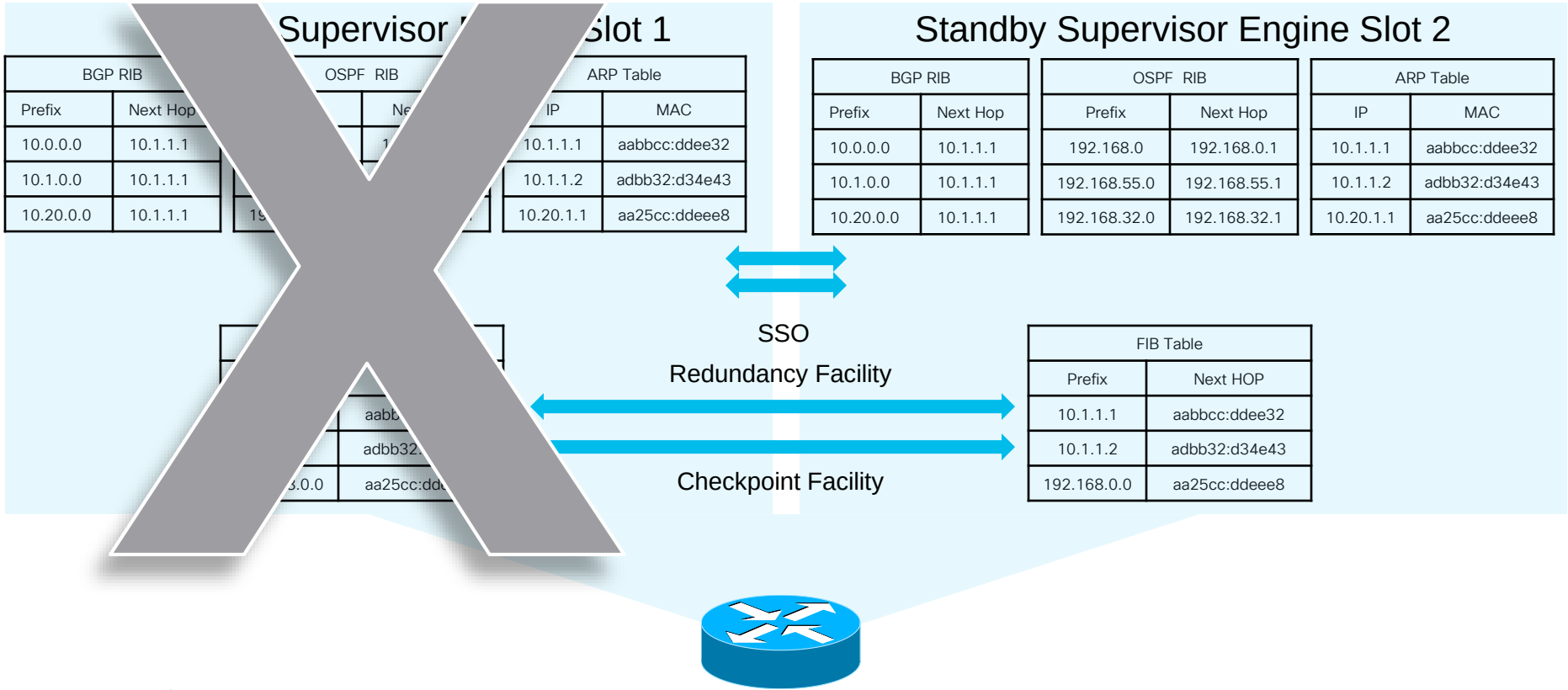
ARP Table	
IP	MAC
10.1.1.1	aabbcc:ddee32
10.1.1.2	adbb32:d34e43
10.20.1.1	aa25cc:ddeee8

FIB Table	
Prefix	Next HOP
10.1.1.1	aabbcc:ddee32
10.1.1.2	adbb32:d34e43
192.168.0.0	aa25cc:ddeee8

GR/NSF Signaling per protocol

Synchronization per protocol

Routing Protocol Redundancy With NSR
(Stateful Restart)



Routing Protocol Redundancy With NSR
(Stateful Restart)

Standby Supervisor Engine Slot 2

BGP RIB	
Prefix	Next Hop
10.0.0.0	10.1.1.1
10.1.0.0	10.1.1.1
10.20.0.0	10.1.1.1

OSPF RIB	
Prefix	Next Hop
192.168.0	192.168.0.1
192.168.55.0	192.168.55.1
192.168.32.0	192.168.32.1

ARP Table	
IP	MAC
10.1.1.1	aabbcc:ddee32
10.1.1.2	adbb32:d34e43
10.20.1.1	aa25cc:ddeee8

FIB Table	
Prefix	Next HOP
10.1.1.1	aabbcc:ddee32
10.1.1.2	adbb32:d34e43
192.168.0.0	aa25cc:ddeee8

No additional signaling required to maintain topology

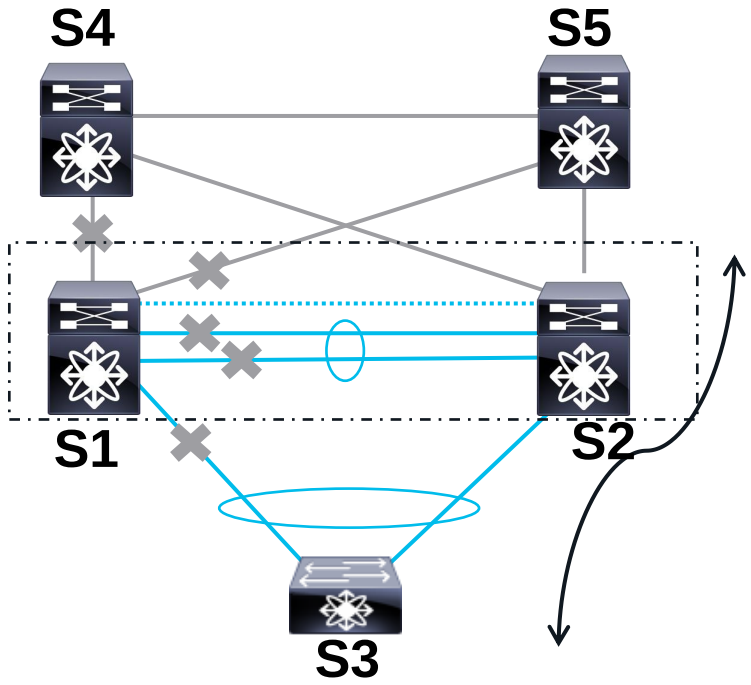
vPC Best Practice

- vPC Domain ID's
  - ✓ Use a unique vPC domain ID within a contiguous L2 domain to avoid MAC overlap.
- vPC Peer Link
  - ✓ Should be point-to-point connection & dedicated links.
- vPC Peer Keepalive Link
  - ✓ Dedicate a control plane in a dual-supervisor environment. Use a management switch.
- vPC peer-gateway
  - ✓ Acts as active gateway for frames addressed to peer switch. Avoid Peer Link forwarding.
- Use vPC peer-switch
  - ✓ Optimizes BPDU processing, single logical L2 entity
- Distribute port-channel member interfaces across line cards within the same chassis.
- Create a map for oversubscription aligned to current and future demand.
  - ✓ Deployment practice – 20:1 at access and 2:1 at Core.

vPC Configuration Best Practices

- vPC object tracking, tracks both peer-link and uplinks in a list of Boolean OR
- Object Tracking triggered when the track object goes down
- Suspends the vPCs on the impaired device.
- Traffic forwarded over the remaining vPC peer.

```
! Track the vpc peer link
track 1 interface port-channel11 line-protocol
! Track the uplinks
track 2 interface Ethernet1/1 line-protocol
track 3 interface Ethernet1/2 line-protocol

! Combine all tracked objects into one.
! "OR" means if ALL objects are down, this object will go down
track 10 list boolean OR
object 1
object 2
object 3

! If object 10 goes down on the primary vPC peer,
! system will switch over to other vPC peer and disable all local vPCs
vpc domain 1
track 10
```



Vxlan Considerations and Best Practices

- Use the Nexus Dashboard NDFC App for Vxlan configuration and management
- Vxlan EVPN preferred over Flood and learn
- Design Hierarchical Vxlan fabric to accommodate the scale out
- Ingress replication , Underlay multicast for BUM traffic handling
- Summarize external routes on border leaf or Advertise default routes on a per tenant basis
- Advertise only the LPM prefix routes of internal public layer 3 subnets out of border leaf switches
- Include all local loopbacks in underlay routing to make troubleshooting easy
- Same Vlan Per L2 VNI and consistent naming for vlan VNI pair

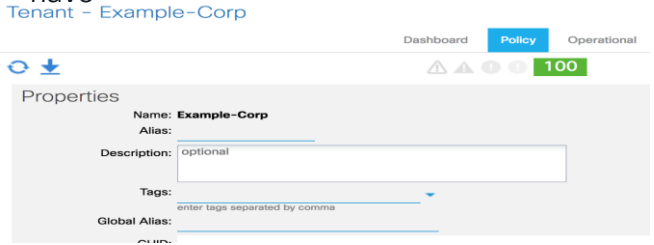
Operational Best Practices

MO Naming Convention

- Develop and plan the MO(Managed Objects) Naming Convention according to Organizations best Practice

Tags and Aliases

- Workaround to Rename Objects
- Objects can be grouped to make query easier
- Tags/Aliases have no functional impact- Where as Labels have

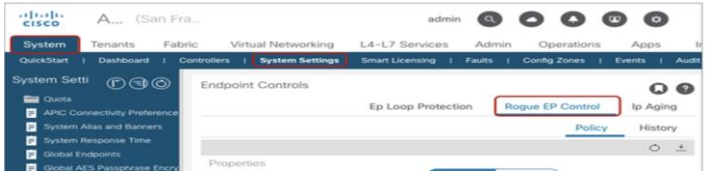


AAA Fallback to Local Auth

- Fallback domain should be set to local to avoid lockout

Loop Mitigation Settings

- Enable MCP (Miscabling Protocol) per vlan
  - To find out and disable loops caused by misbehaving external L2
- Rogue EP Control preferred over Endpoint loop protection



BD Level Configuration

- Do Not enable Unicast routing when gateway is not BD SVI
- Limit IP Learning to Subnet
- L2 Unknown unicast set to Flood
- ARP Flooding enabled

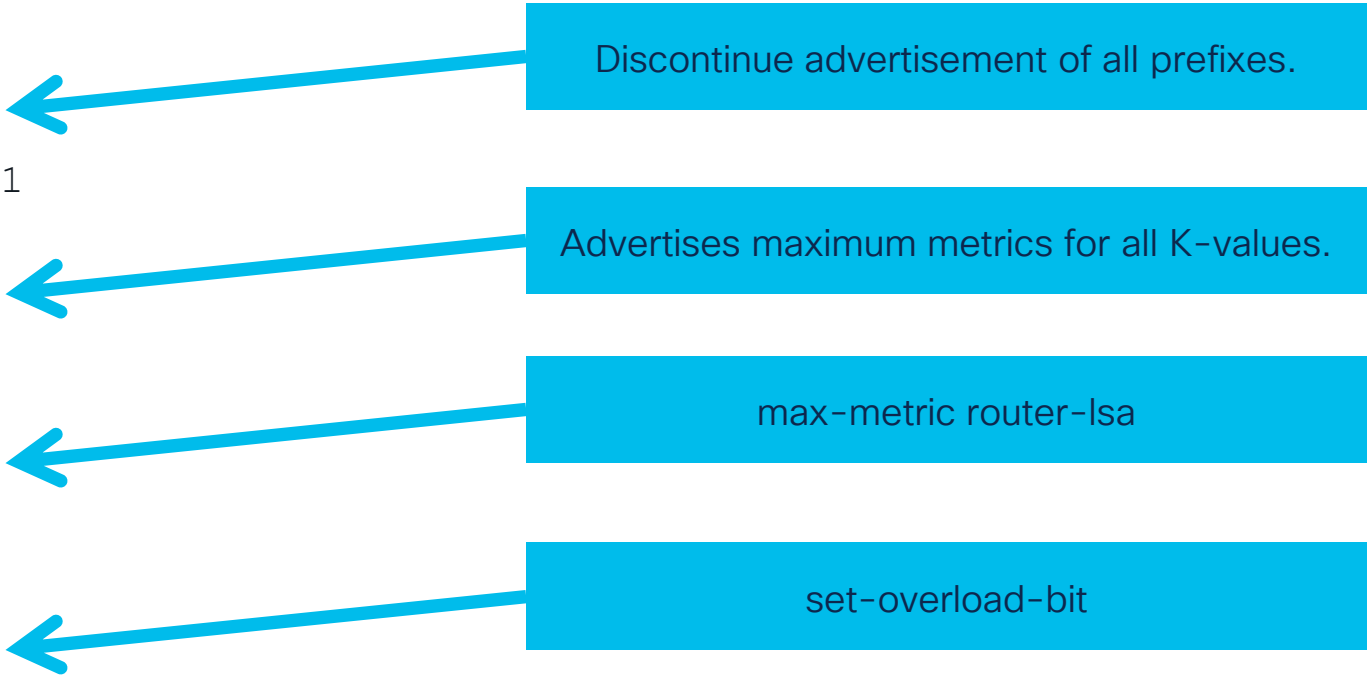
Fabric Wide Configuration

- IP Aging Policy
- Disable Remote EP Learning – On Border Leaf
- Enforce Subnet Check

NX-OS Graceful Insertion and Removal

Nexus Graceful Removal

```
router bgp 33
   isolate
 router eigrp 1
   isolate
 router ospf 1
   isolate
 router isis 1
   isolate
```



Nexus feature
Graceful Insertion

- Move the switch from Maintenance mode to Normal mode.
- Control plane maintained throughout isolation of the switch.
- Protocols advertise routes only after it is installed in hardware.

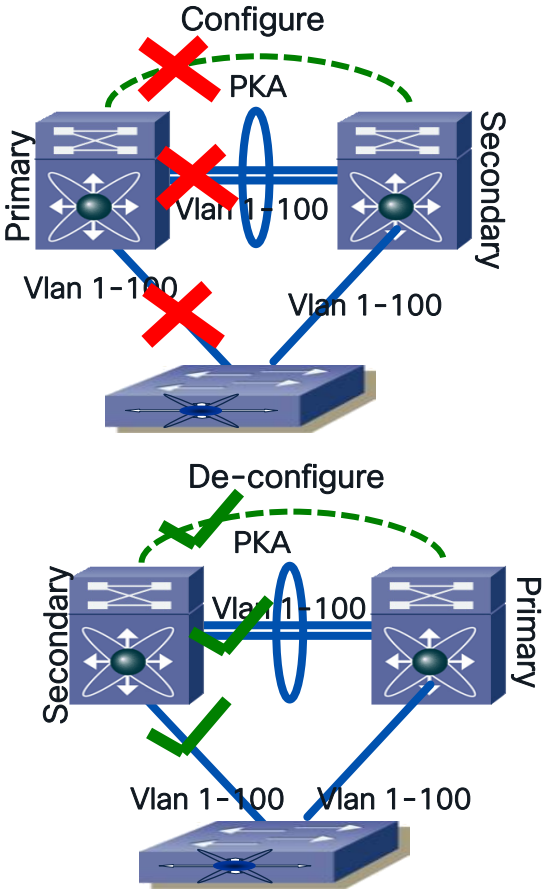
```
N9372(config)# no system
mode maintenance
Following configuration
will be applied:
  router bgp 33
    no isolate
  router eigrp 1
    no isolate
  router ospf 1
    no isolate
  router isis 1
    no isolate
```

VPC Shutdown Feature

This feature allows customer to manually “isolate” a switch from vPC domain. This is a vPC configuration option.

Pre-VPC Shutdown	VPC Shutdown Behavior

• No “shutdown” command.
• Manual Shutdown Required
  • Down vPCs
  • Down Peer Link
  • vPC Members
  • Etc.
	• Local switch isolated from remote.
	• Cannot exit shutdown without manual intervention.
	• When exiting, PKA, PL, and vPCs will be re-initialized; vPC domain brought to normal state.



Graceful Insertion and Removal

```
feature ospf

feature vpc
```

Isolate for
Change Window

OSPF:
max-metric router-lsa

VPC:
shutdown

Scripting takes time.

It'd be nice to
automate this...

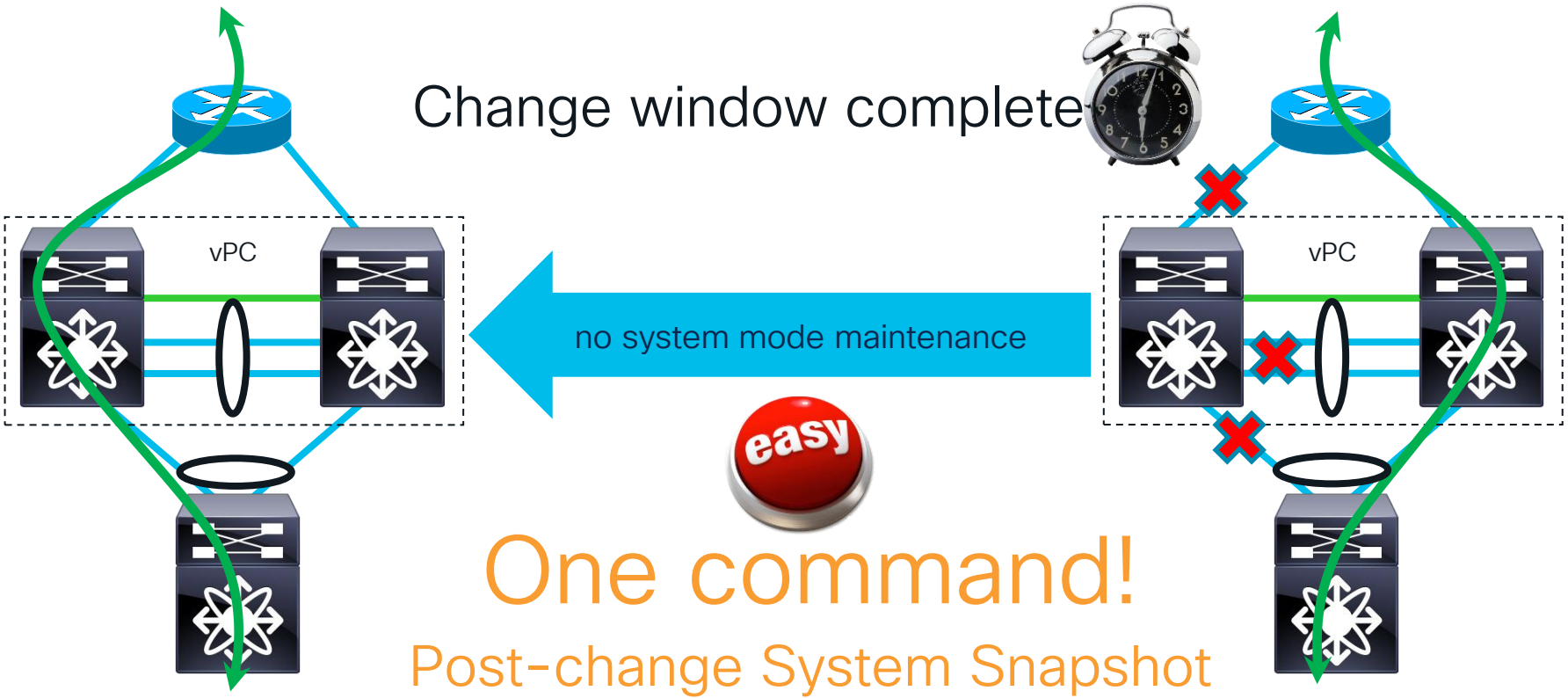
Graceful Insertion and Removal

Change window begins.

One command!

Pre-change System Snapshot

Graceful Insertion and Removal



Configuration Profiles

- Maintenance-mode profile is applied when entering GIR mode,
- Normal-mode profile is applied when GIR mode is exited.

Automatic Profiles	Manual Profiles
• Generated by default • Parses configuration to determine changes going into and out of GIR • Changes based on base protocol configuration settings. • Use: Maintenance Windows	• User created profile for maintenance-mode and normal-mode • Flexible selection of protocols for isolation • Use: maintenance windows and isolation during troubleshooting using preconfigured scripts.

Enabling Graceful Insertion and Removal
Automatic Profile Generation

```
N7K-1-Core# show system mode
System Mode : Normal
N7K-1-Core# config
Enter configuration commands, one per line.  End with
CNTL/Z.
N7K-1-Core(config)# system mode maintenance

BGP is not enabled, nothing to be done

EIGRP is not enabled, nothing to be done

OSPF is up..... will be shutdown
        OSPF TAG = 100, VRF = default
                config terminal
                router ospf 100
                shutdown
                end

OSPFv3 is not enabled, nothing to be done

ISIS is not enabled, nothing to be done

vPC is not enabled, nothing to be done

Interfaces will be shutdown
Do you want to continue (y/n)? [n] y
```

```
Generating maintenance-mode profile
Progressing.....................Done.

System mode operation completed successfully

N7K-1-Core# show system mode
System Mode : Maintenance
N7K-1-Core#
```

Enabling Graceful Insertion and Removal Custom Profile Generation

```
config-profile maintenance-mode type admin
router bgp 65001
 isolate
 sleep instance 1 10
router ospf 100
  isolate
  sleep instance 3 20
  vpc domain 20
   shutdown
  system interface shutdown exclude fex-fabric
```

```
config-profile normal-mode type admin
router bgp 65001
 no isolate
 sleep instance 1 10
router ospf 100
  no isolate
  sleep instance 3 20
  vpc domain 20
   no shutdown
  no system interface shutdown
```

- By default, GIR Mode will automatically generate profiles.
- CLI to disable automatic profile generation: dont-generate-profile
- If you enter GIR mode with automatic profile, it will overwrite your custom profile.

Graceful Insertion and Removal Mode for Unplanned Outages

system mode maintenance on-reload reset-reason *reason*

HW_ERROR-Hardware error,

SVC_FAILURE-Critical service failure,

KERN_FAILURE-Kernel panic,

WDOG_TIMEOUT-Watchdog timeout,

FATAL_ERROR-Fatal error,

MANUAL_RELOAD---Manual reload,

MATCH_ANY-Any of the above reasons,

ANY_OTHER-Any reload reason not specified above.

Nexus GIR Snapshots

- Used before and after a GIR mode to compare pre/post change operation.
- Snapshots are automatically generated when entering GIR mode.

```
switch# snapshot create snap1 For testing
Executing show interface... Done
Executing show bgp sessions vrf all... Done
Executing show ip eigrp topology summary... Done
Executing show vpc... Done
Executing show ip ospf vrf all... Done
Feature 'ospfv3' not enabled, skipping...
Snapshot 'snap1' created
Switch#
```

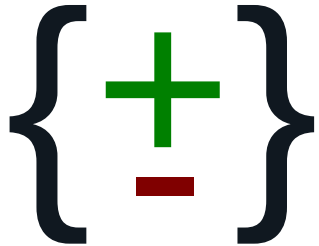
Nexus GIR Snapshots Comparison

```
Nexus# sh snapshots compare before_maintenance after_maintenance
================================================================================
Feature Tag           before_maintenance           after_maintenance
================================================================================

[bgp]
--------------------------------------------------------------------------------

[neighbor-id:100.120.1.221]
connectionsdropped 2                               **3**
lastflap              P1DT21H5M12S                 **P1DT21H25M47S**
lastread              P1DT21H25M12S                **PT0S**
lastwrite             P1DT21H25M14S                **PT0S**
state                 Established                  **Idle**
localport             52737                        **0**
remoteport            179                          **0**
notificationssent     2                            **3**
<...>
```

switch# **show snapshots compare snapshot1 snapshot2 ipv4routes**

metric	snapshot1	snapshot2	changed
# of routes	33	3	*
# of adjacencies	10	4	*

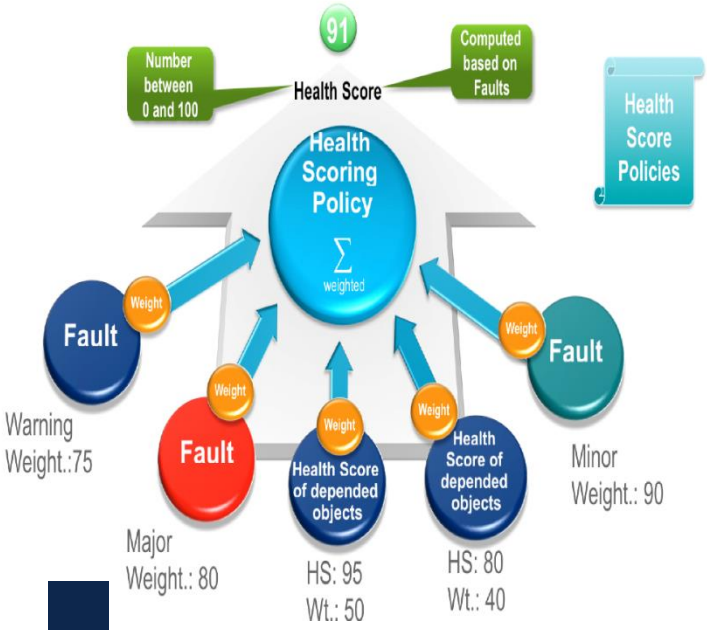
Prefix	Changed Attribute
23.0.0.0/8	not in snapshot2
10.10.10.1/32	not in snapshot2
21.1.2.3/8	adjacency index has changed from 29 (snapshot1) to 38 (snapshot2)



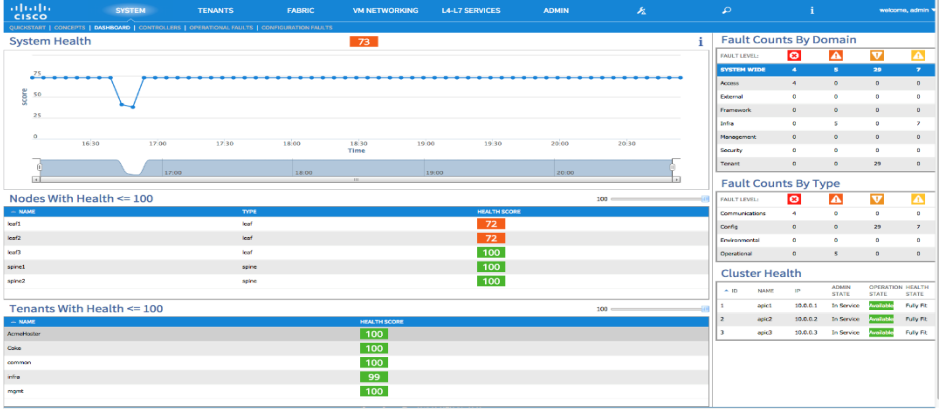
Tools to Manage DC

- Controller (APIC / NDFC)
- Nexus Insights

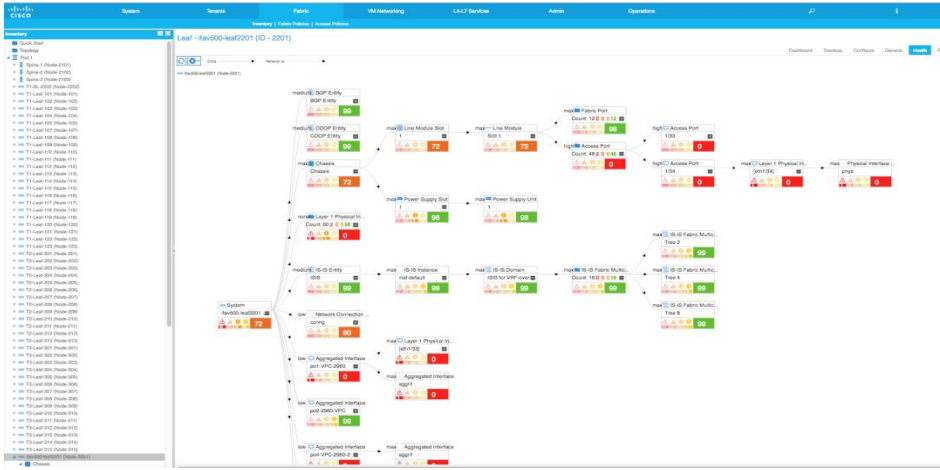
Health Score



Aggregated View



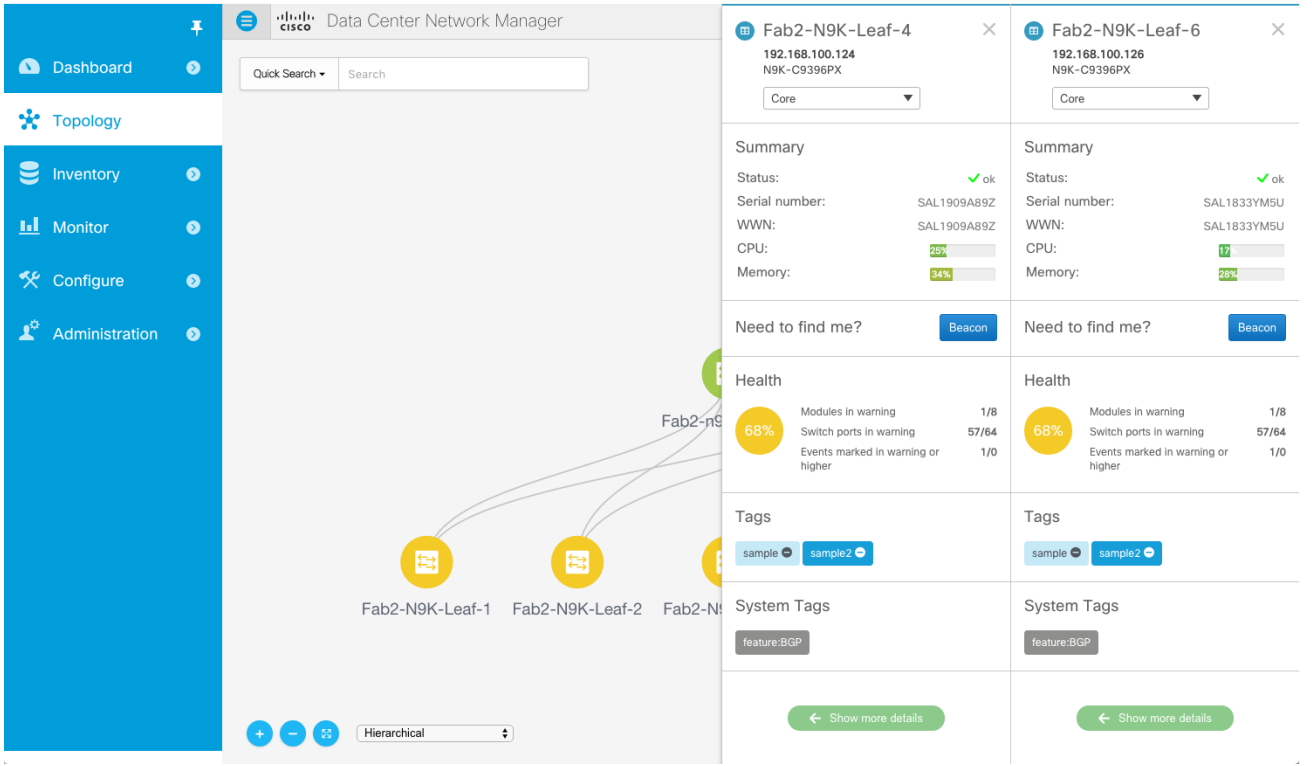
Fabric Topology View



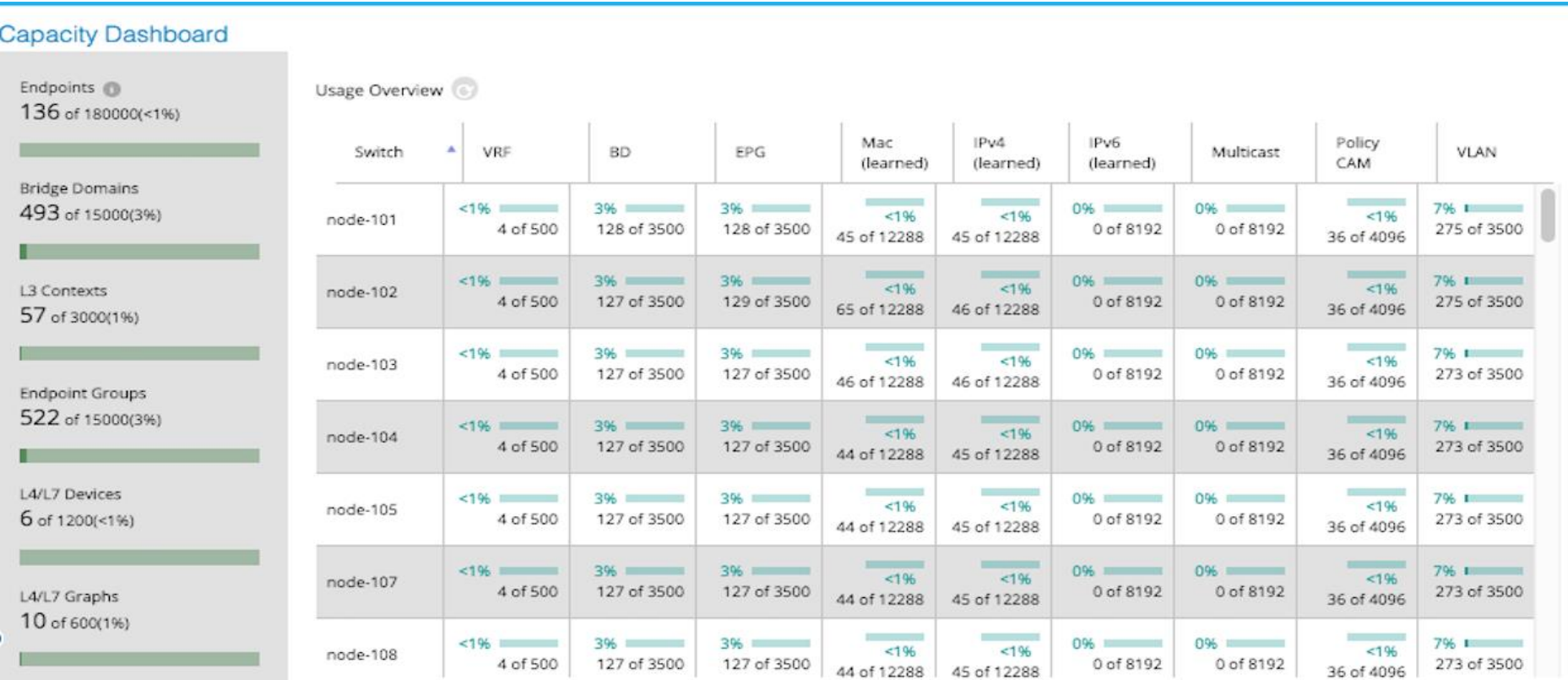
Aggregation of system-wide health, including pod health scores, tenant health scores, system fault counts domain and type and the APIC cluster health state.

New Topology

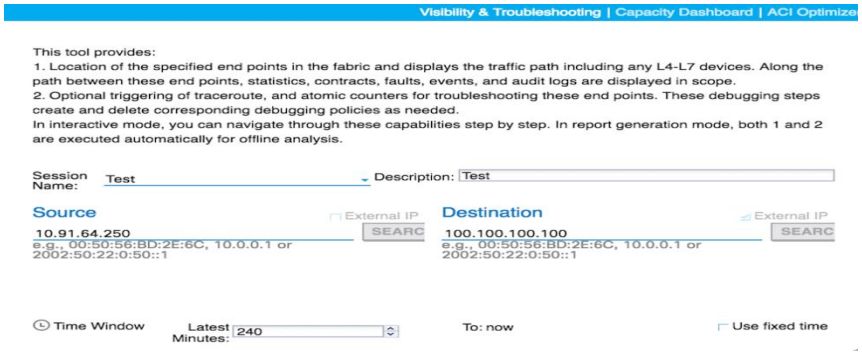
- Dynamic Arrangement
- Multi-Fabric/Overlay
- Arrange by Tier
  - Core, Ag, Access Leaf, Spine etc..
- Metadata Tags
- Show FEX links
- Device Pop-Over
- Side-By Side View

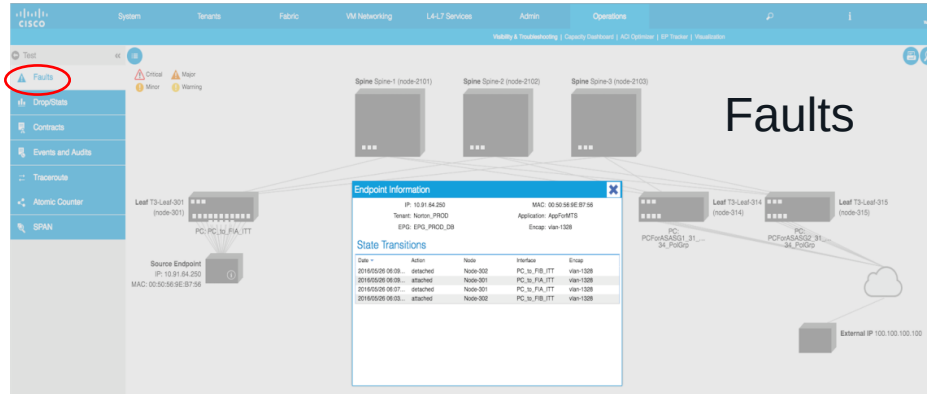


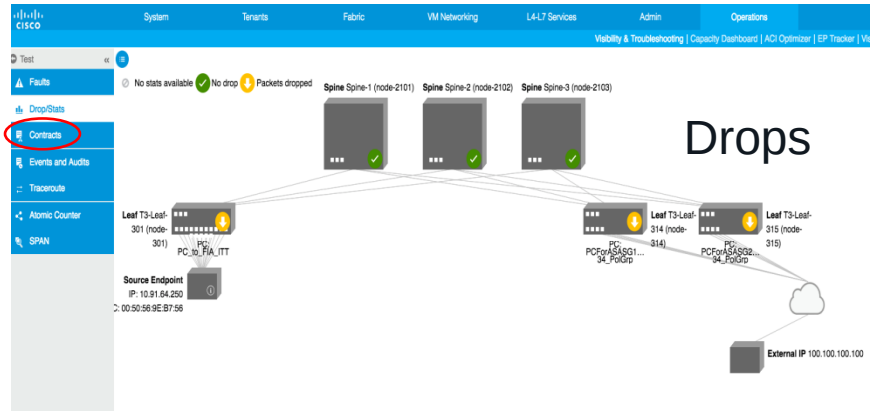
Capacity Dashboard
View the Capacity of Data Center Fabric –ACI

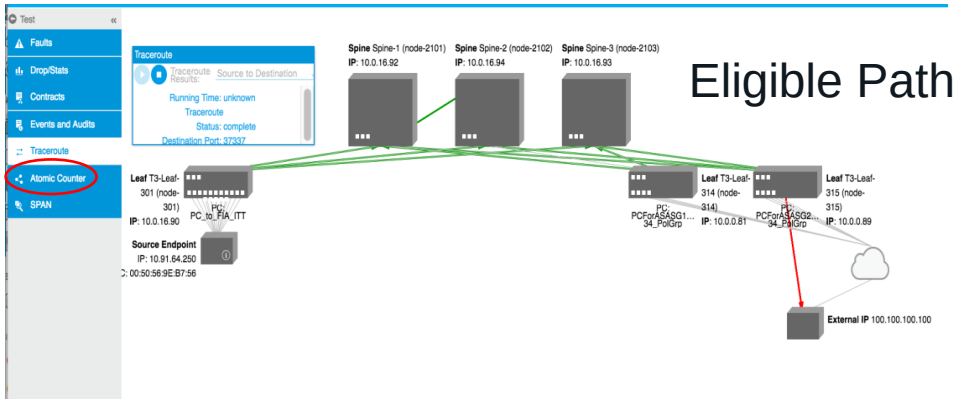


Troubleshoot a Flow
Use Inbuilt Visibility Engine



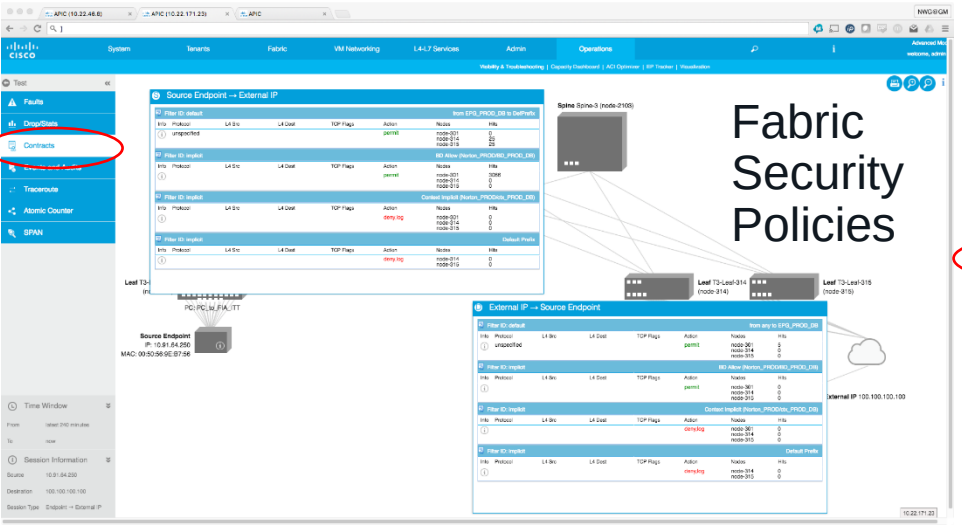


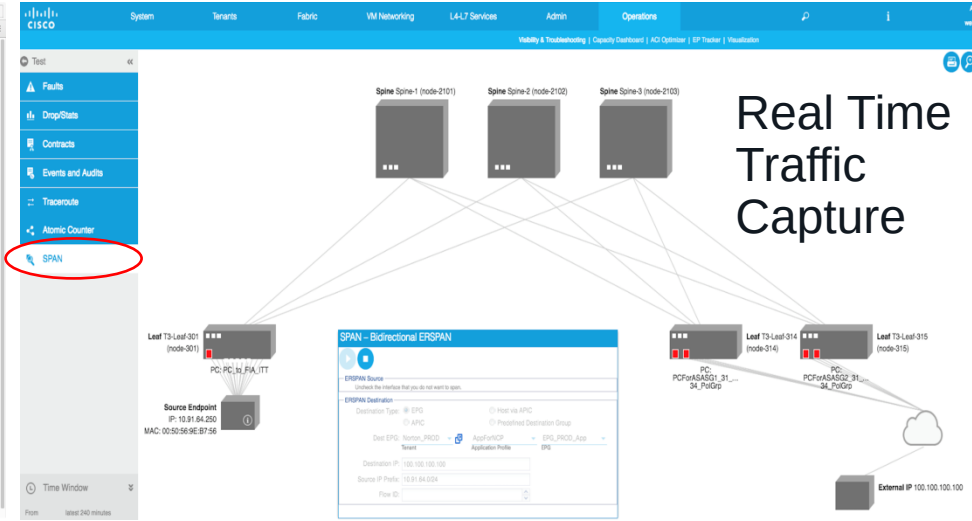




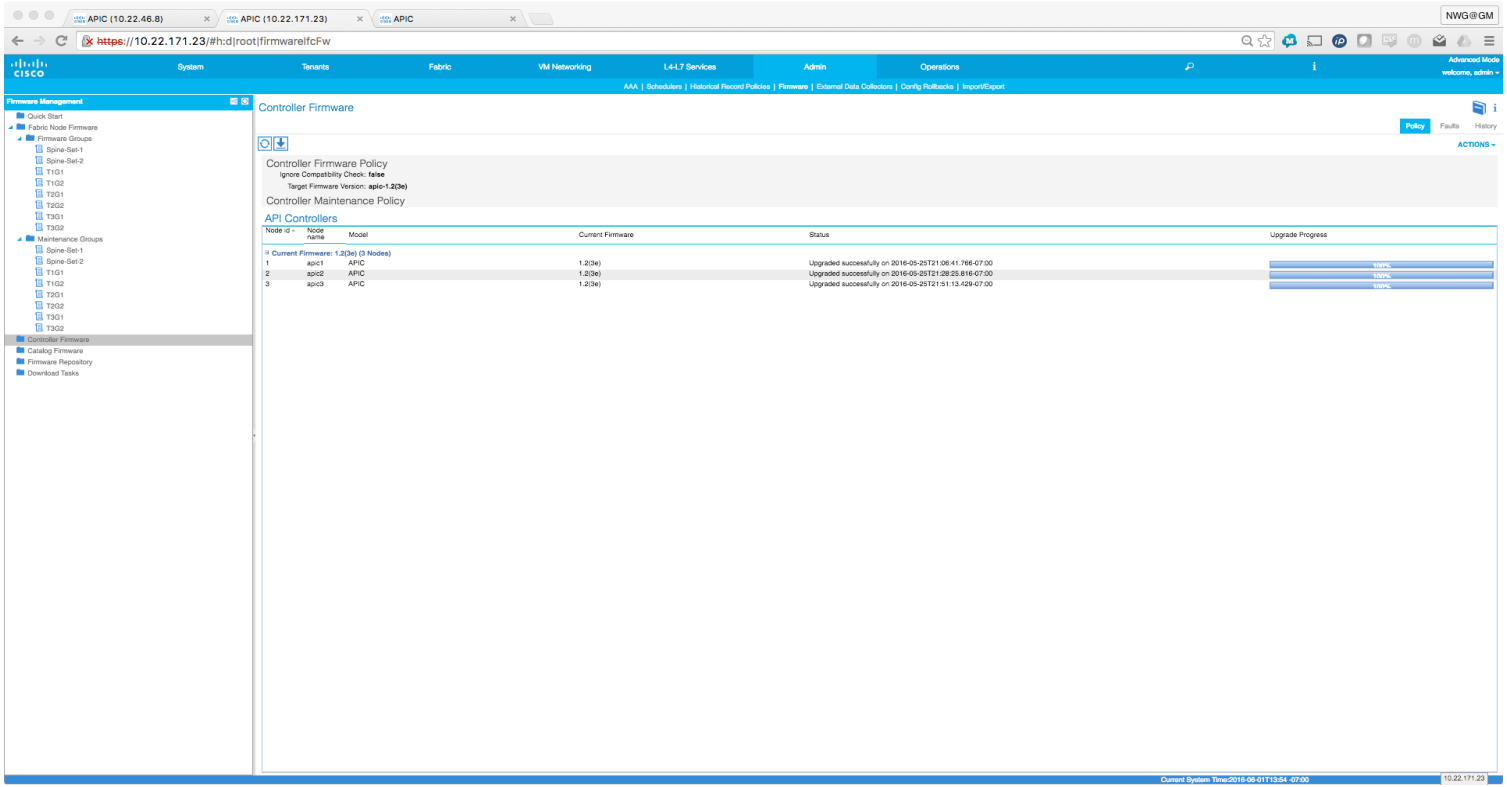
Troubleshoot a Flow

Use Inbuilt Visibility Engine



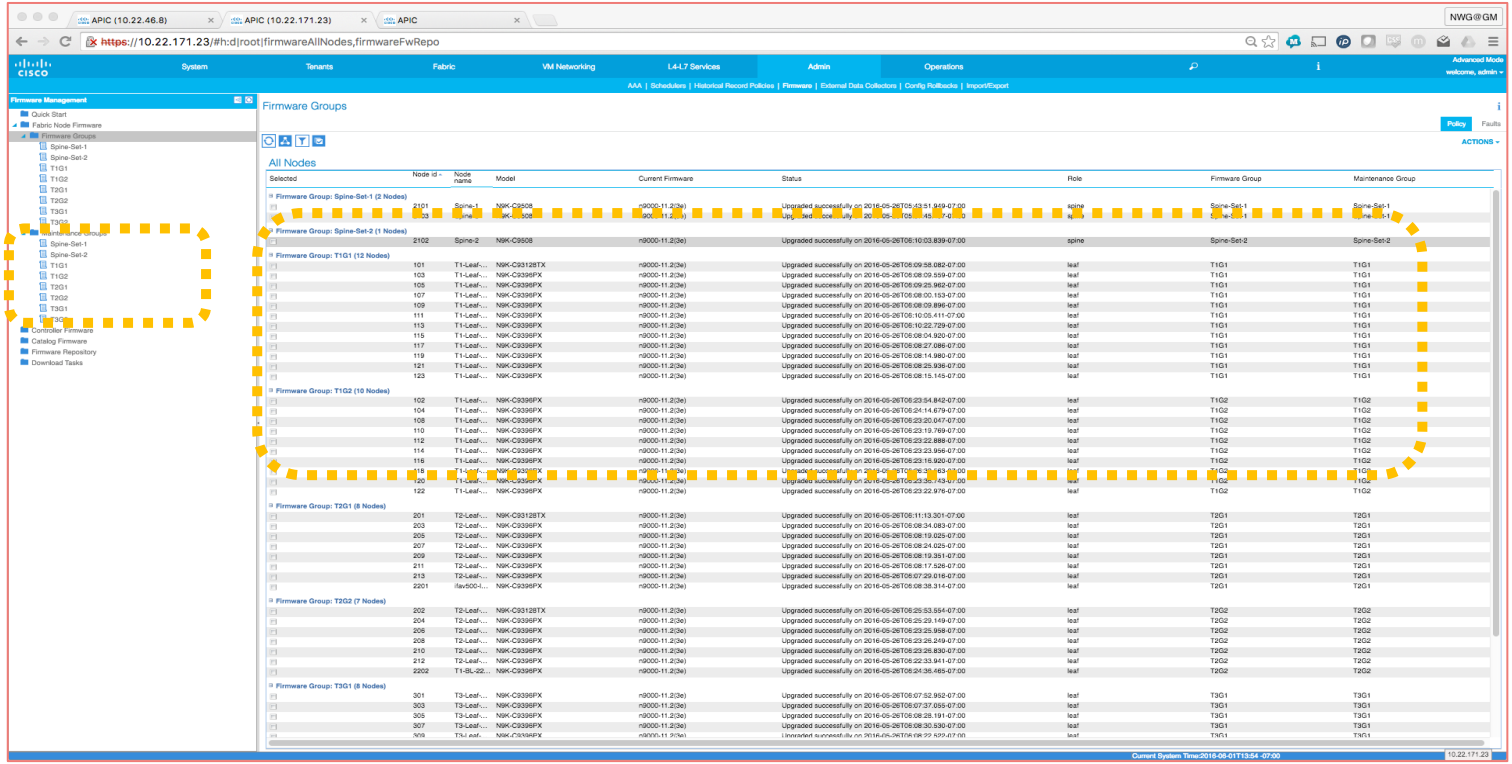


Maintenance Upgrade #1
Upgrade APIC

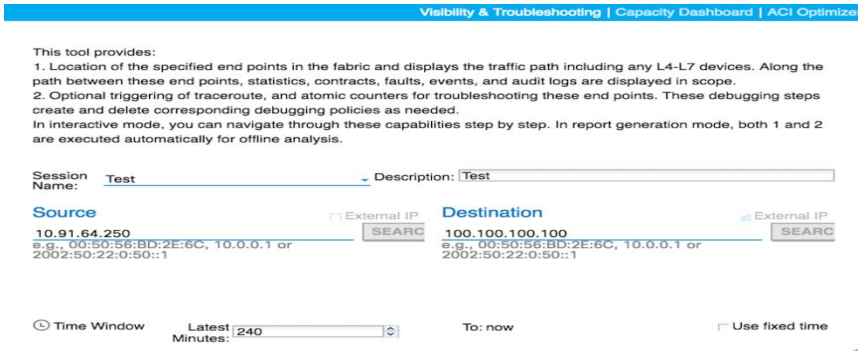


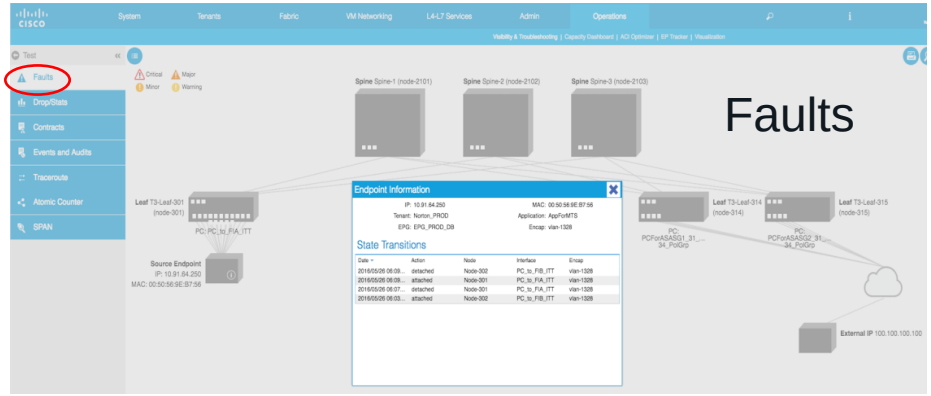
Maintenance Upgrade #2

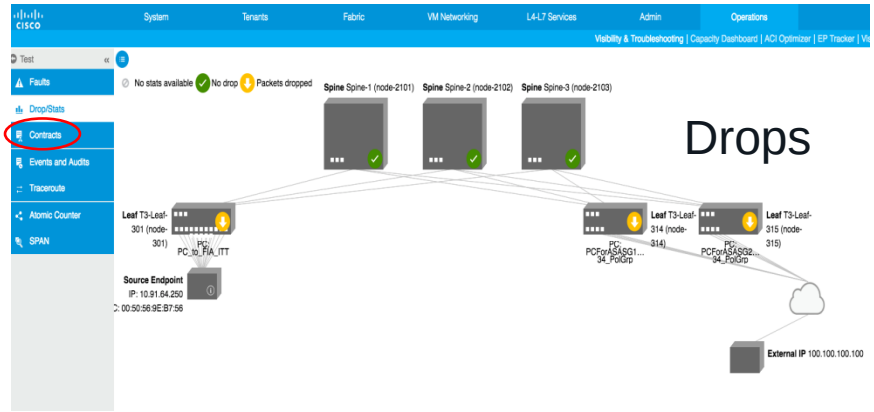
Create Groups

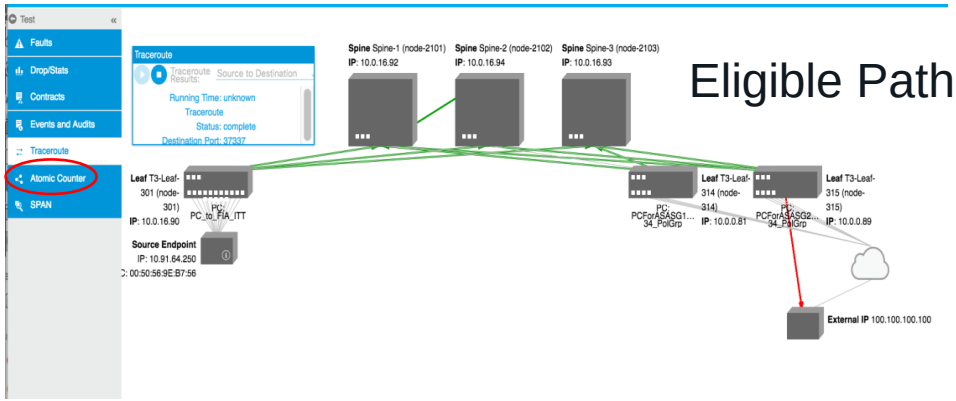


Troubleshoot a Flow
Use Inbuilt Visibility Engine





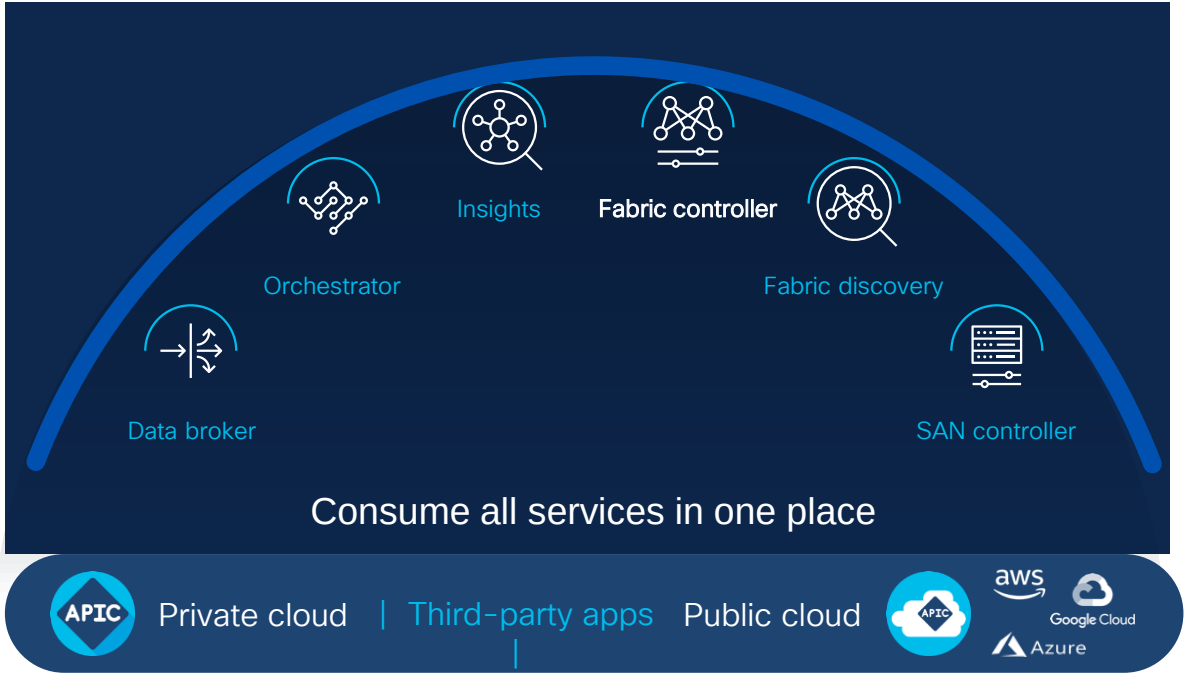




Cisco Nexus Dashboard Fabric Controller

Part of Nexus Dashboard
Simple to automate, simple to consume

With Nexus Dashboard Fabric Controller (NDFC)

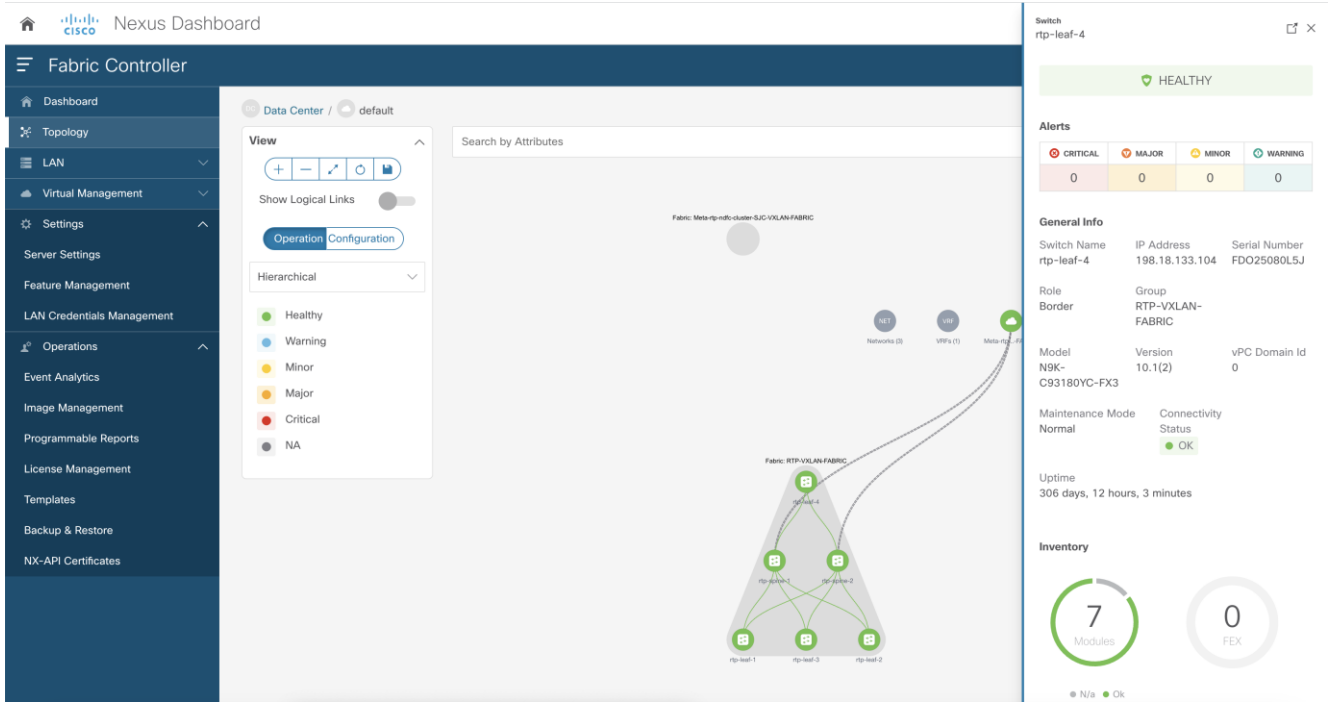


1. Single plane to build and manage multisite fabrics
2. NDFC is an application that you can invoke in single installation for SAN and for the fabric
3. IPAM integration for VXLAN EVPN fabrics
4. Micro Services Scaled mode – active/ active, increased scale for managed/monitored objects
5. Manages IOS-XE and IOS-XR platforms
6. Granular RBAC applicable to Multisite fabric management

New Topology

- Dynamic Arrangement
- Multi-Fabric/Overlay
- Arrange by Tier
  - Core, Ag, Access Leaf, Spine etc..
- Metadata Tags
- Show FEX links
- Device Pop-Over
- Side-By Side View

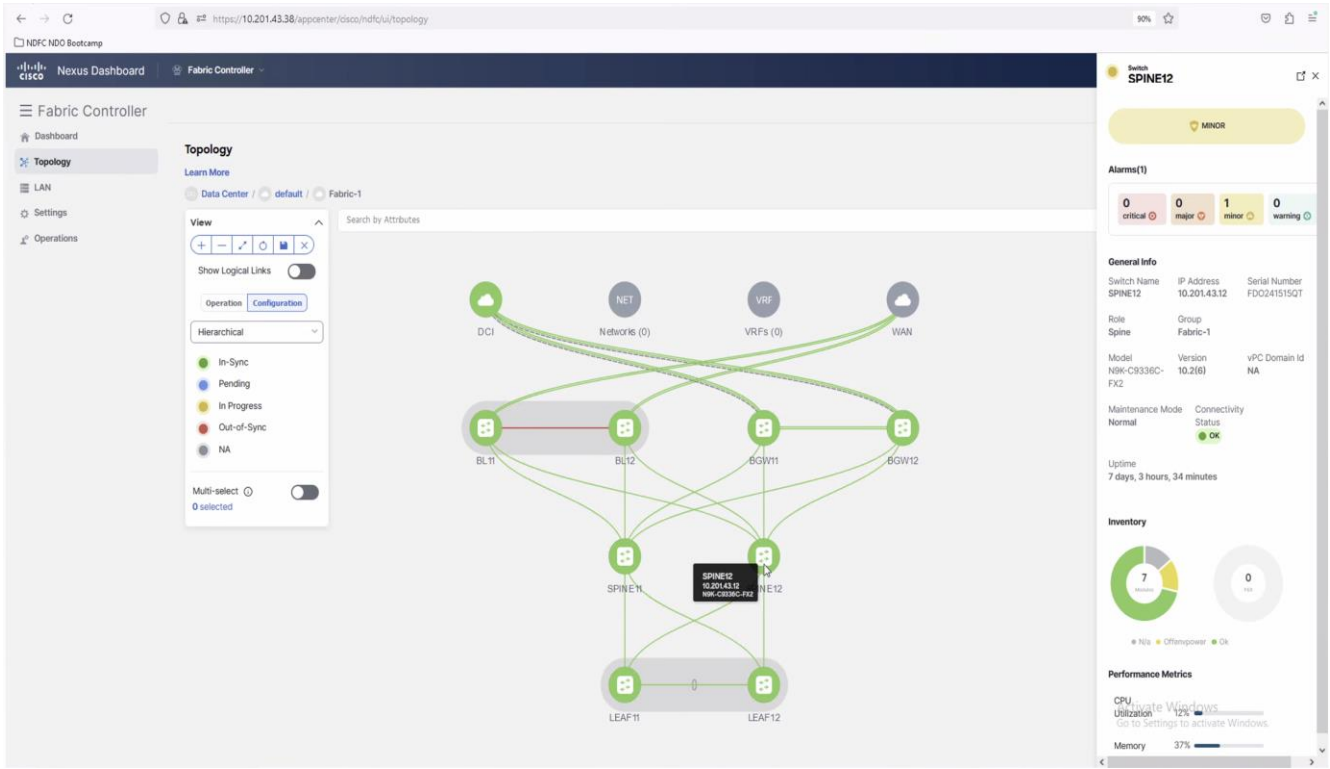
Side-By-Side Views



New Topology

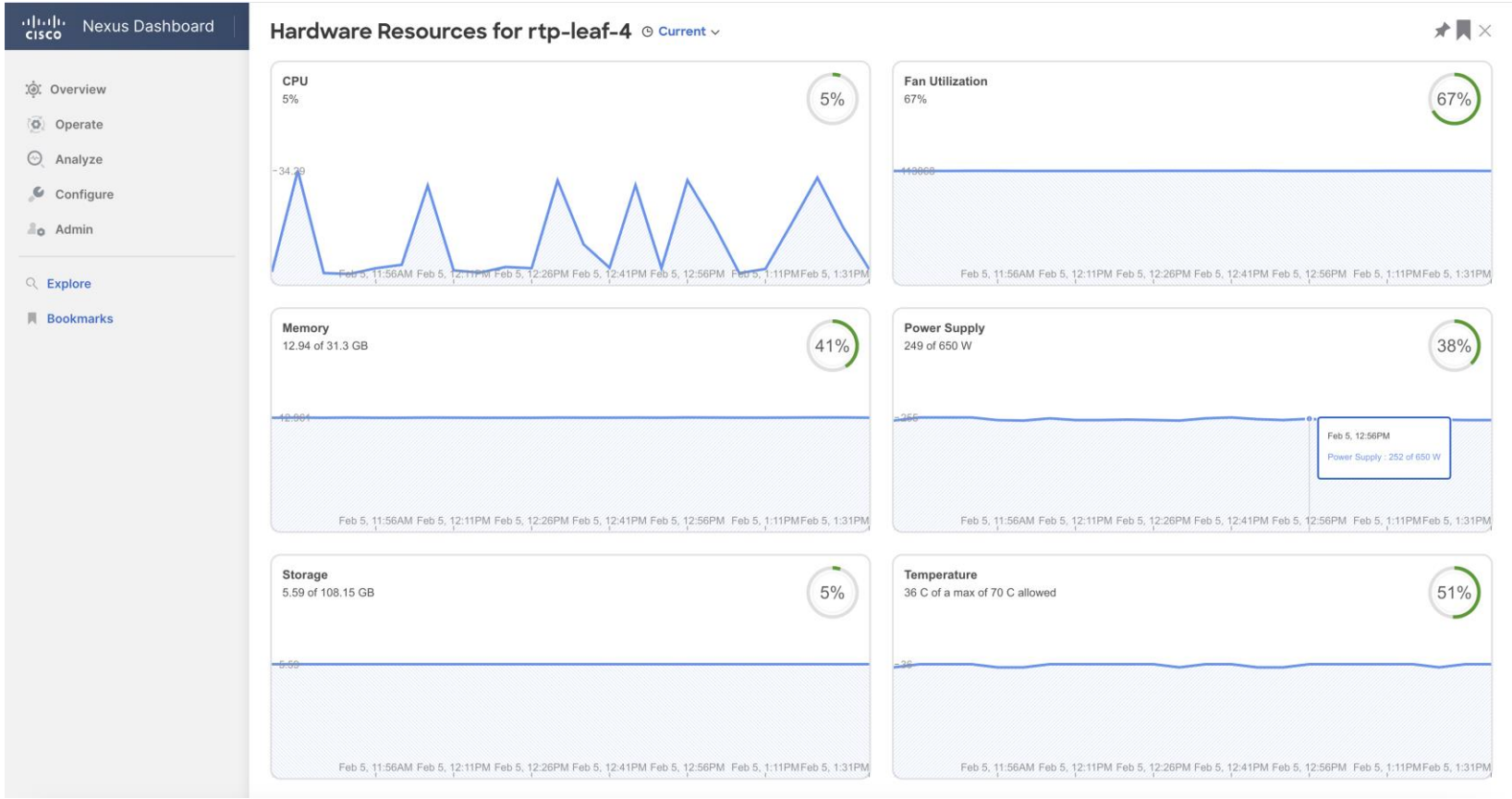
Side-By-Side Views

- Dynamic Arrangement
- Multi-Fabric/Overlay
- Arrange by Tier
  - Core, Ag, Access Leaf, Spine etc..
- Metadata Tags
- Show FEX links
- Device Pop-Over
- Side-By Side View



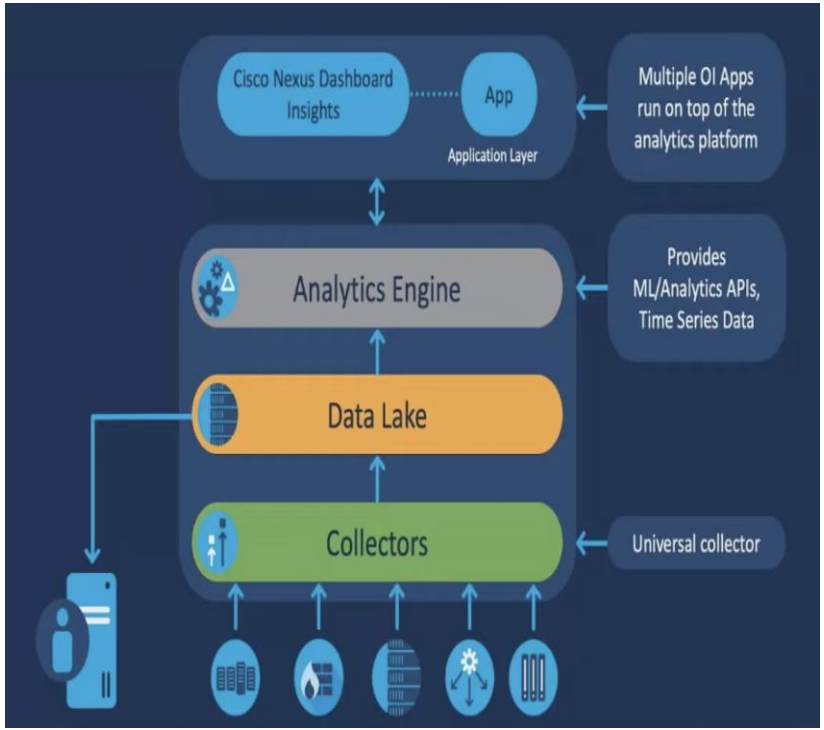
Capacity Dashboard

View the Capacity of non ACI Fabric



Nexus Dashboard

Efficient Operations at the DC (AIOPs)- Nexus Dashboard



Ingest Anything

A common data model for applications and infrastructure that unifies data across domains

Query Anything

Search using a Unified Query Layer across our AIOps data platform

Visualize Anything

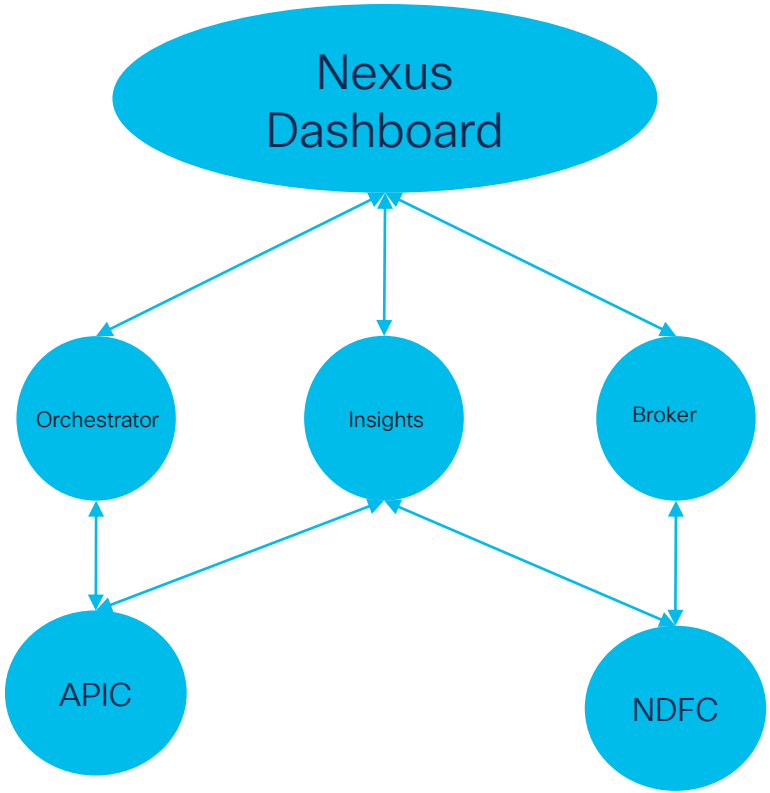
See your apps and infra through
a new set of lenses with Hypergraph and Dash Studio

Alert Anything

Harnessing the power of the new AIOps data platform for more sophisticated health rules

Note: Application insights using AppD integration with nexus insight upgrade is not covered in this session

Unified Datacenter Controller views



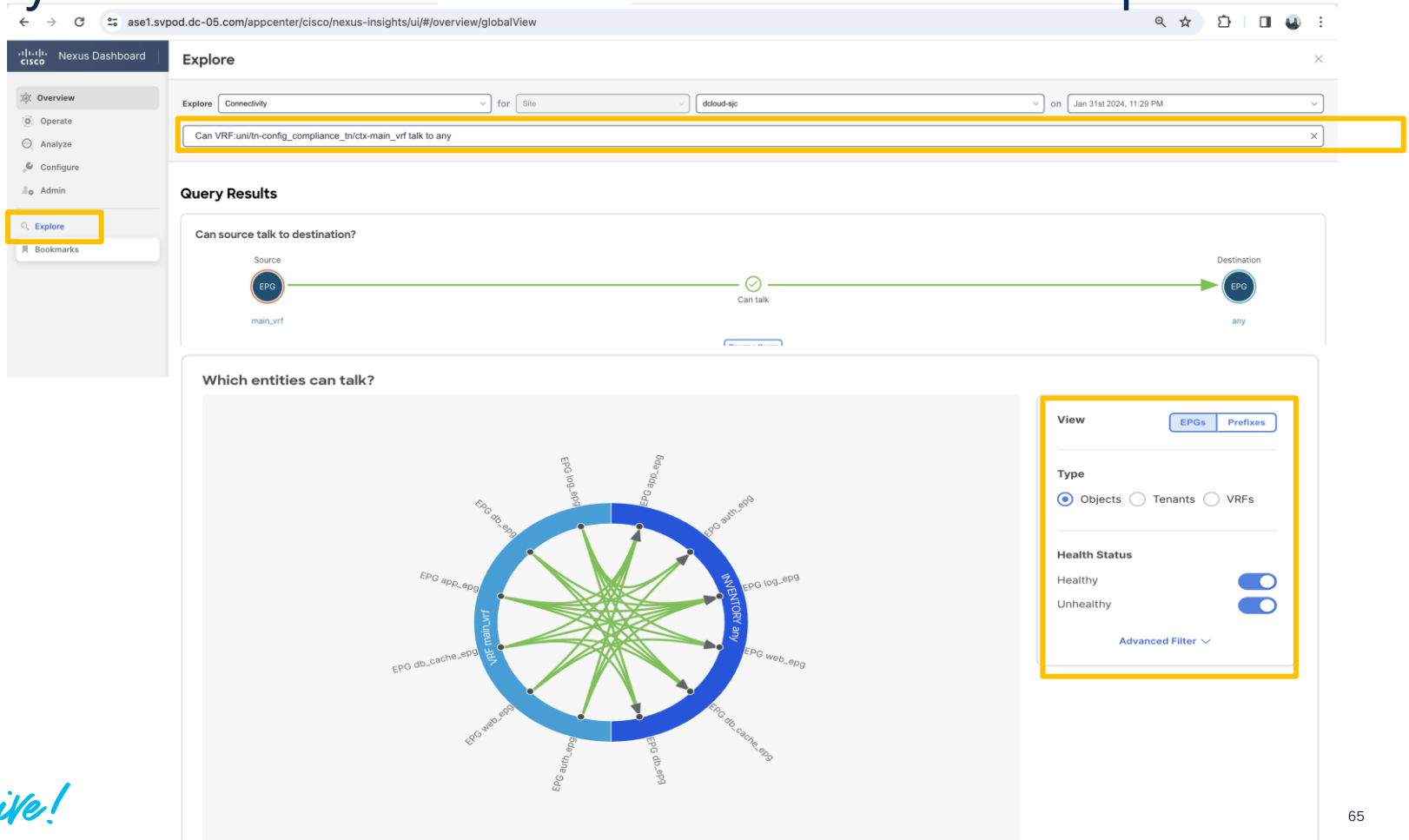
#1 Benchmarking

#2 Upgrade planning

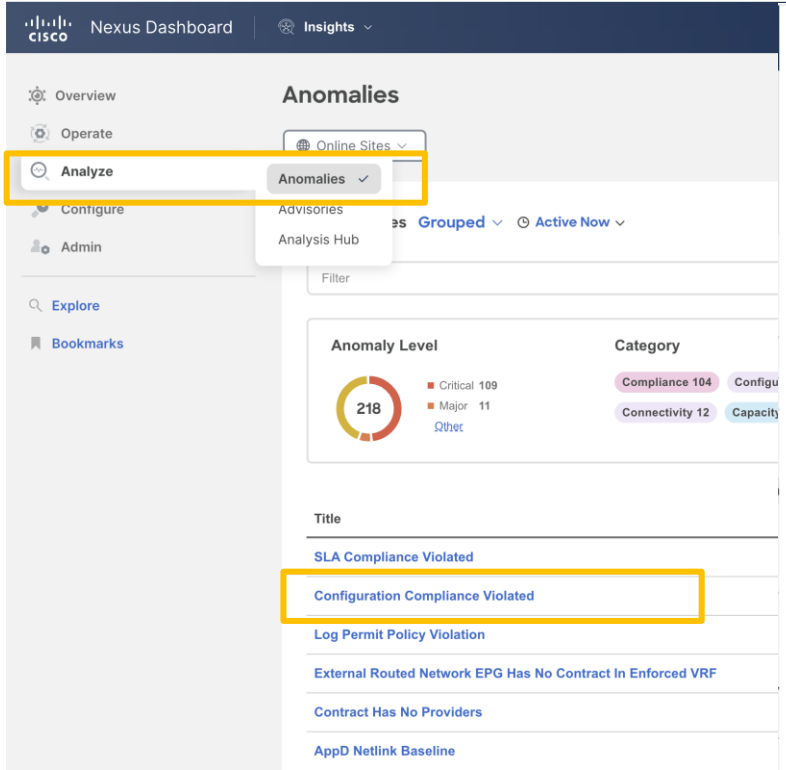
- Day 0 , Day 1 and Day 2
- Software Image management
- Migrations

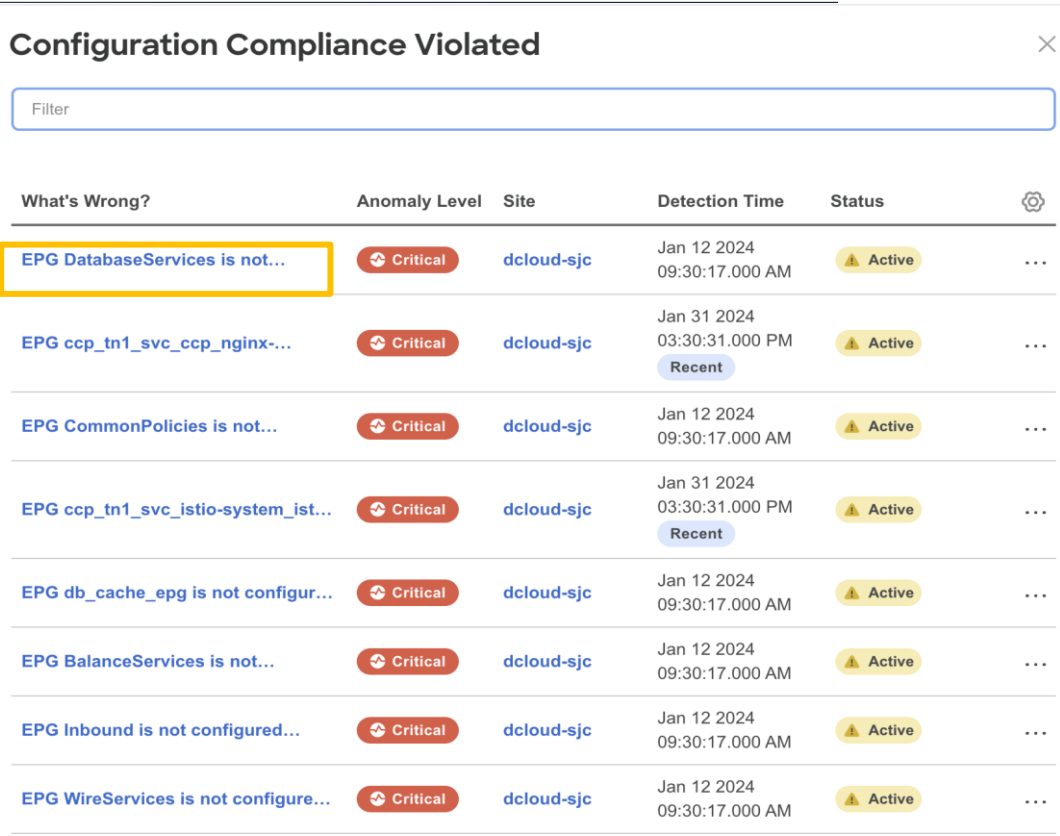
#3 Pre and Post Change window baselining

Verify Fabric Communication & relationship



Analyse the Anomalies





Analyse the Anomalies

What's the impact?

The attributes of the specified object do not match those in the configuration compliance requirement.

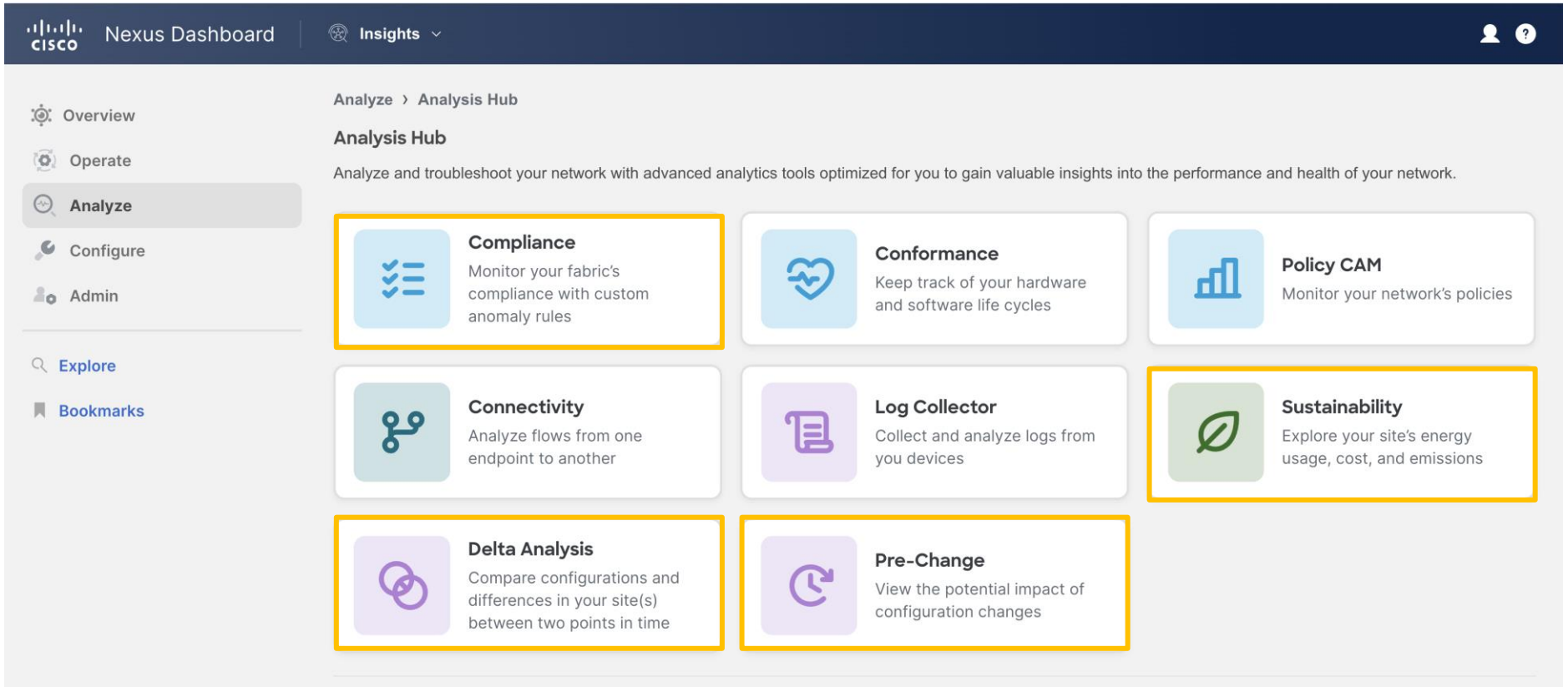
Requirement	Object Type	Object Name	Scope
test sj	EPG	**DatabaseServices**	common

How do I fix it?

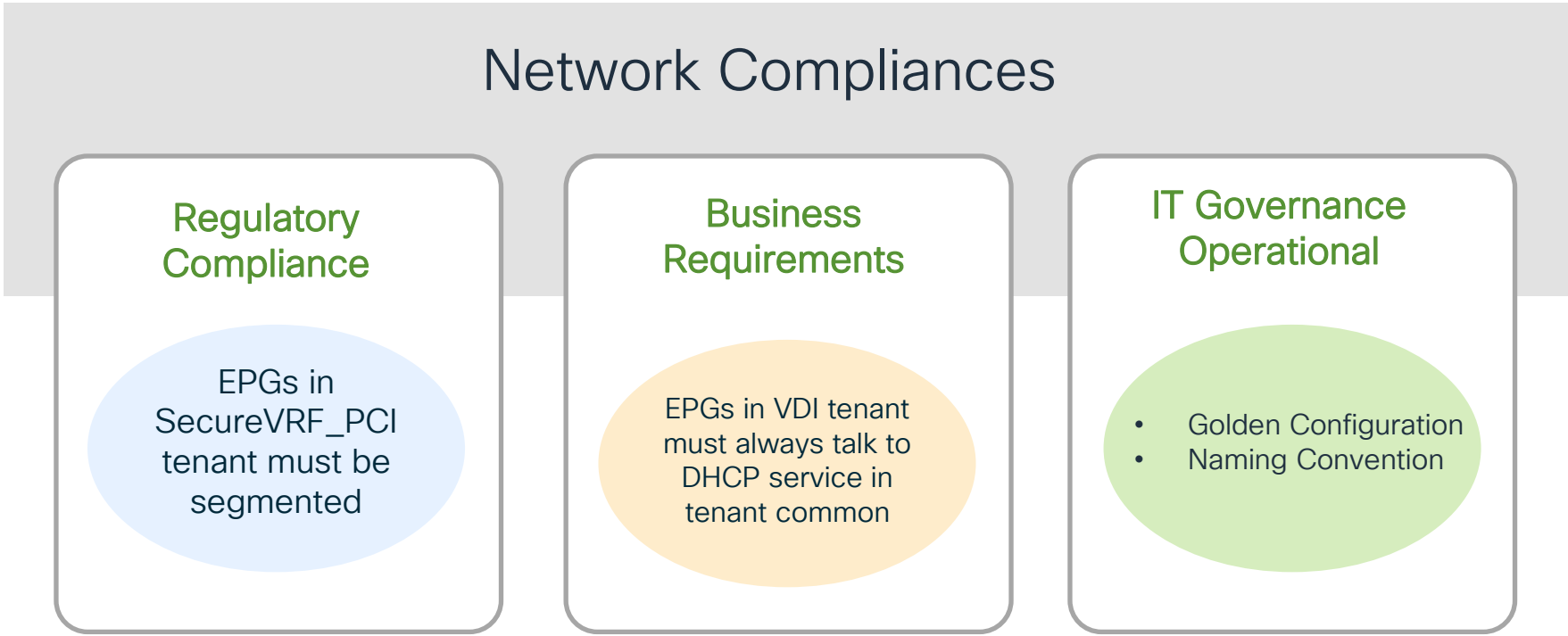
Recommended Solution Failing Condition (1/1)

To fix this anomaly, ensure the expected and the configured values match for all attributes. When making configuration changes, always adhere to best practices around maintenance windows as some changes might be disruptive.

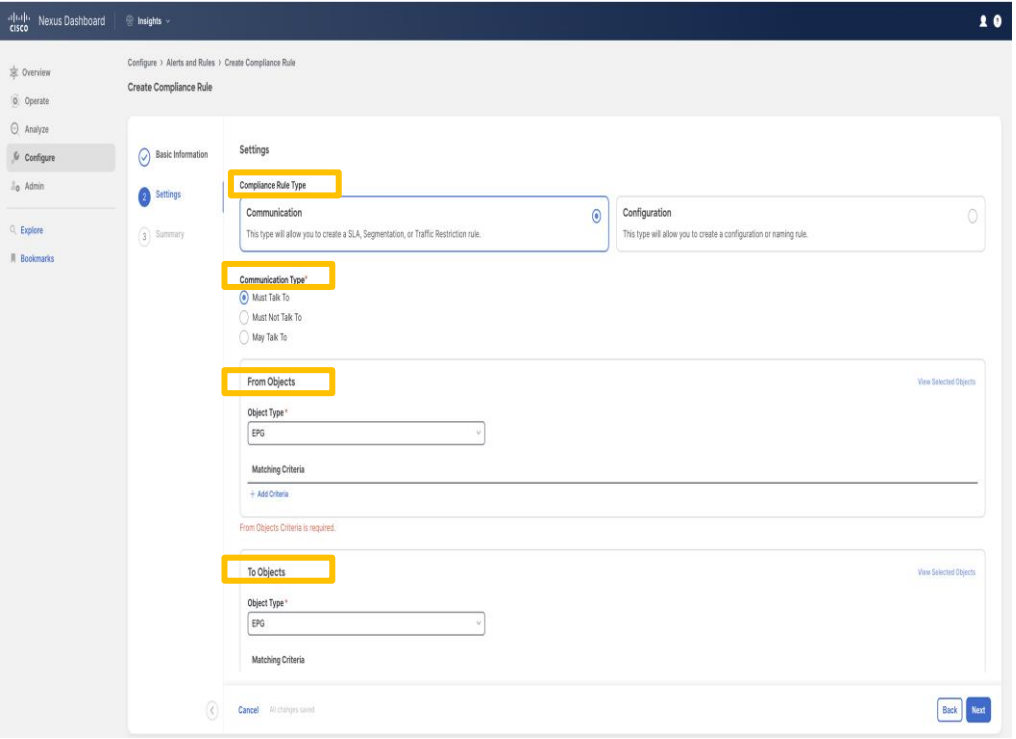
Analysis Hub – The one stop shop for operations

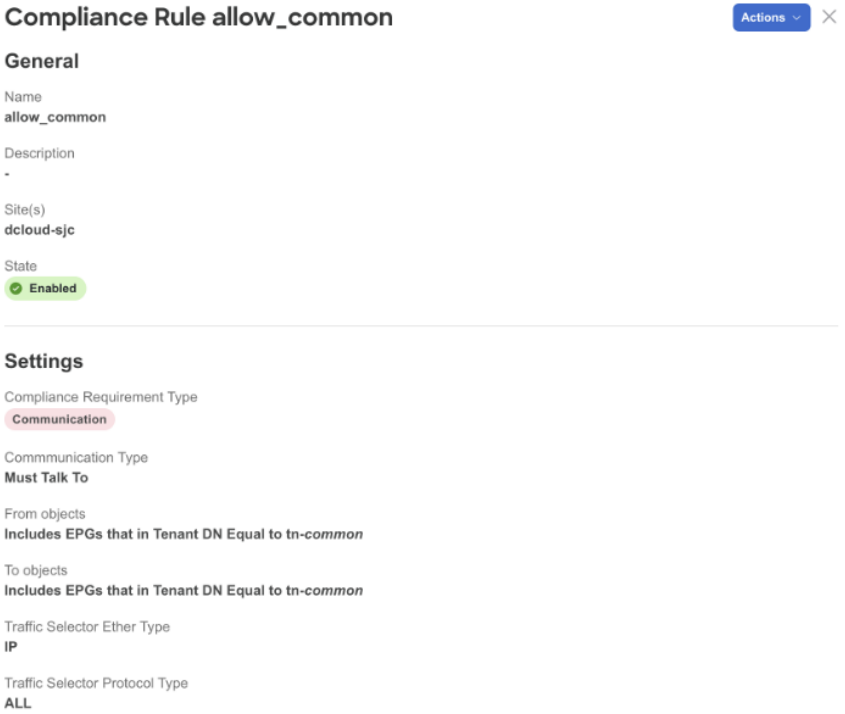


Network Compliances Use Cases



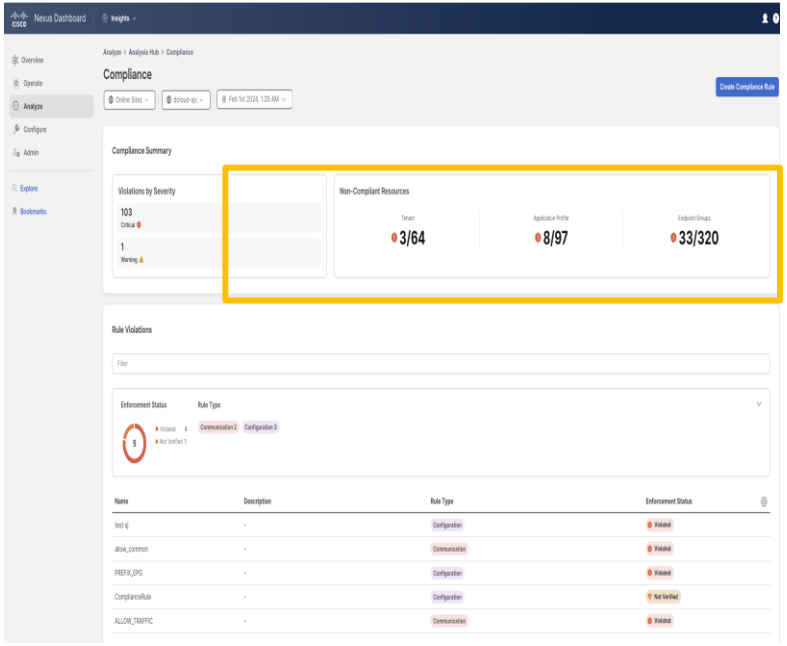
Creating Network Compliances Use Cases

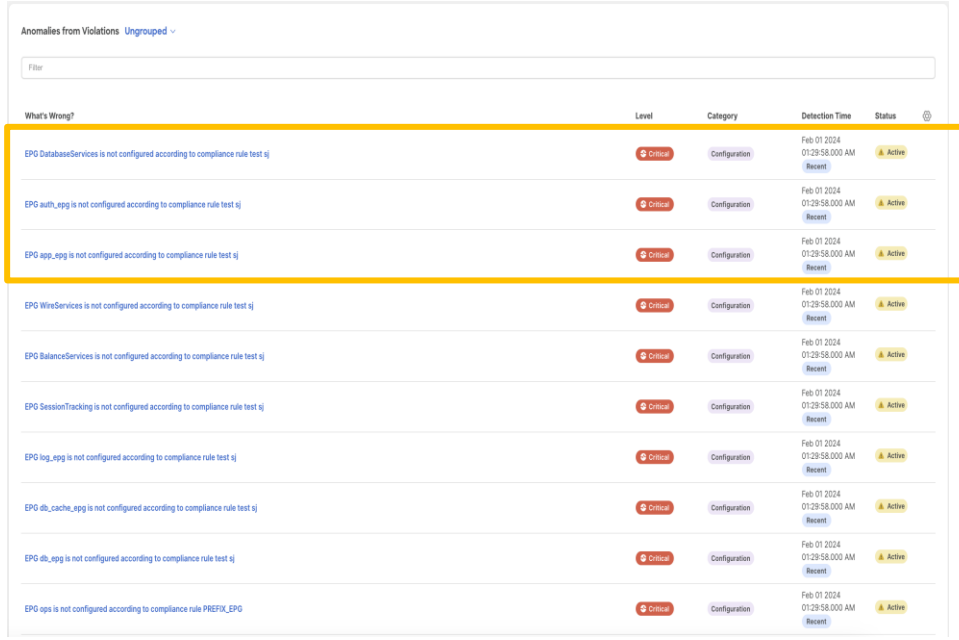




View Compliance Analysis Status – Analysis hub

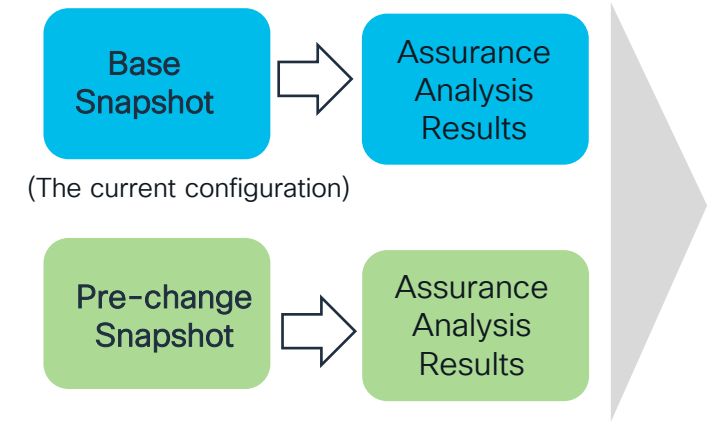
Compliance is a top-level option in the Analysis Hub.
On the Compliance page, the summary of the compliance analysis of the site is shown for the selected time window.





Pre-Change Analysis using Nexus Dashboard

Analyzes and Reveals the impacts of intended configuration changes.

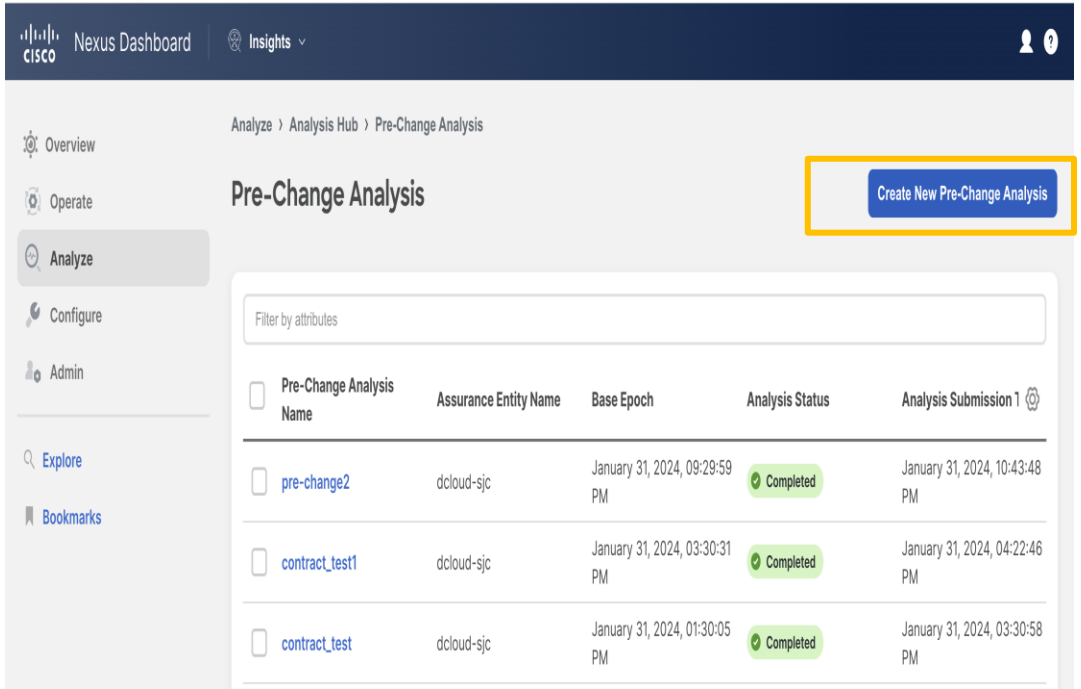


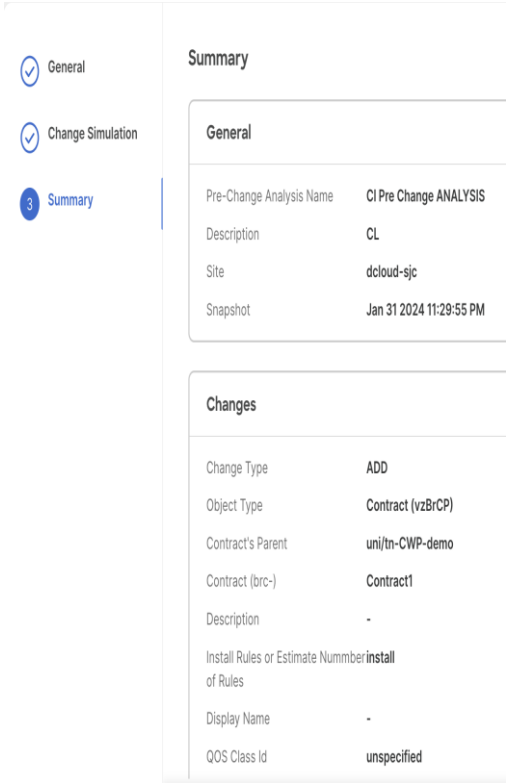
- ✓ Pre Change Analysis – Reveals the impact of the changes.
- ✓ Operations can also have custom snapshots

Other features: Anomaly detection and correlation (software, config or hardware), Upgrade pre-check and post-check across multiple fabrics, data plane dependency mapping and micro burst detection

Create and Run a Pre-Change Analysis

Pre-Change Analysis is within the “Analysis Hub” Option in the Analyze panel. Users can create, edit, clone or delete a pre-change analysis.





Upgrade Assist

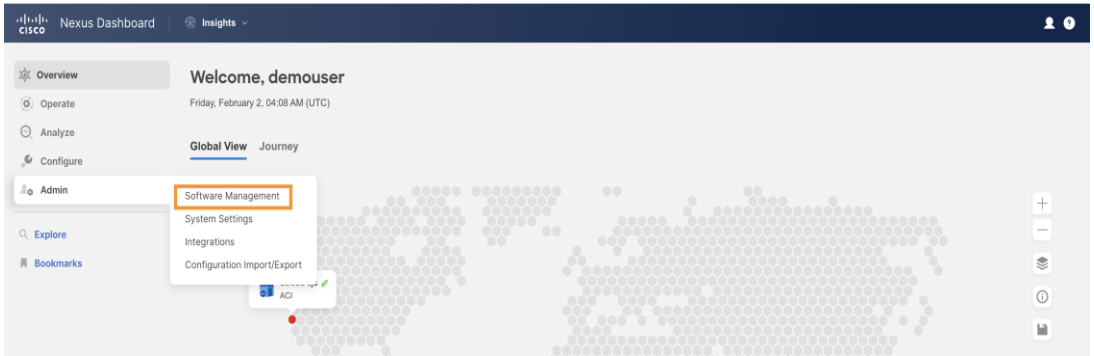
Overview Upgrade Assist

- The upgrade assist feature helps to identify
  - What issues are affecting nodes with the current software versions running on them
  - What issues will no longer be seen post software upgrade
- This is done based off of metadata and affects both ACI and NDFC

How to do an upgrade analysis

Reference

- To start an upgrade analysis, select Admin -> Software management

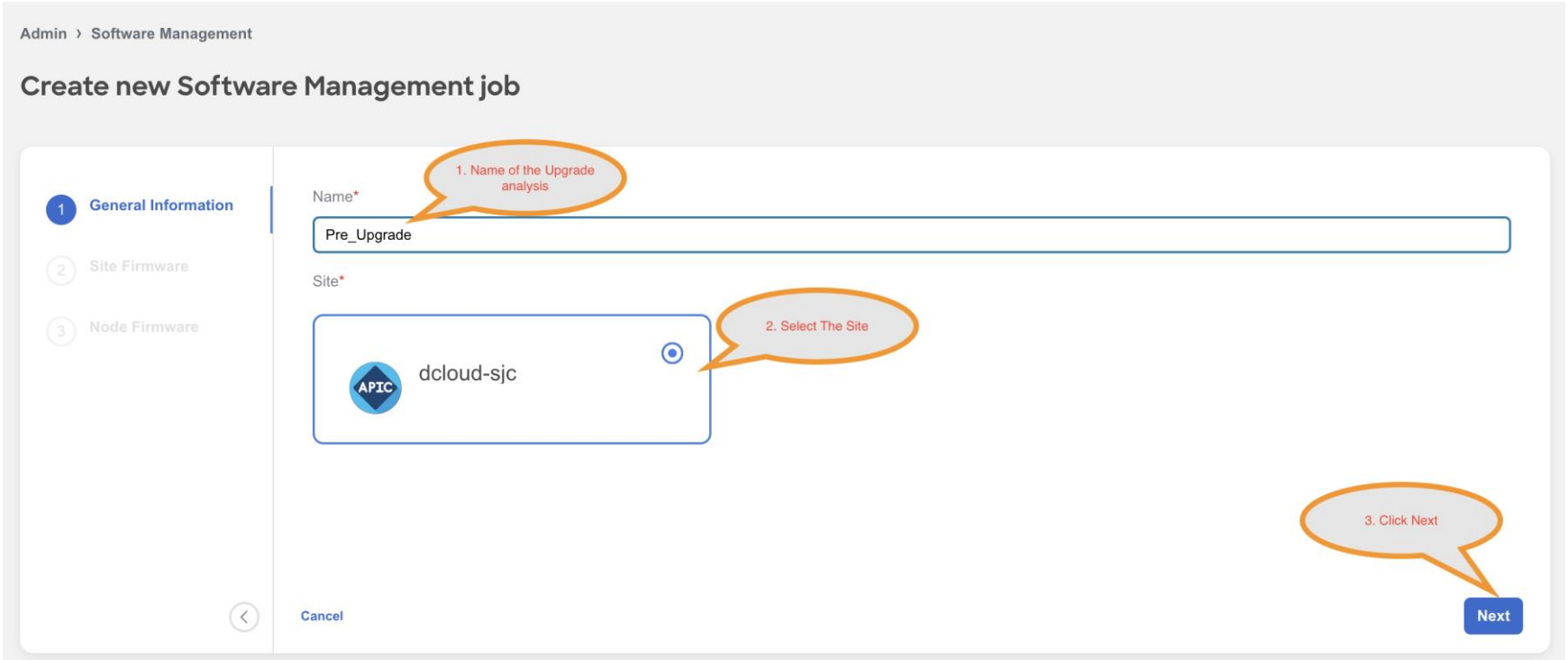


- Start a New Analysis

How to do an upgrade analysis

Reference

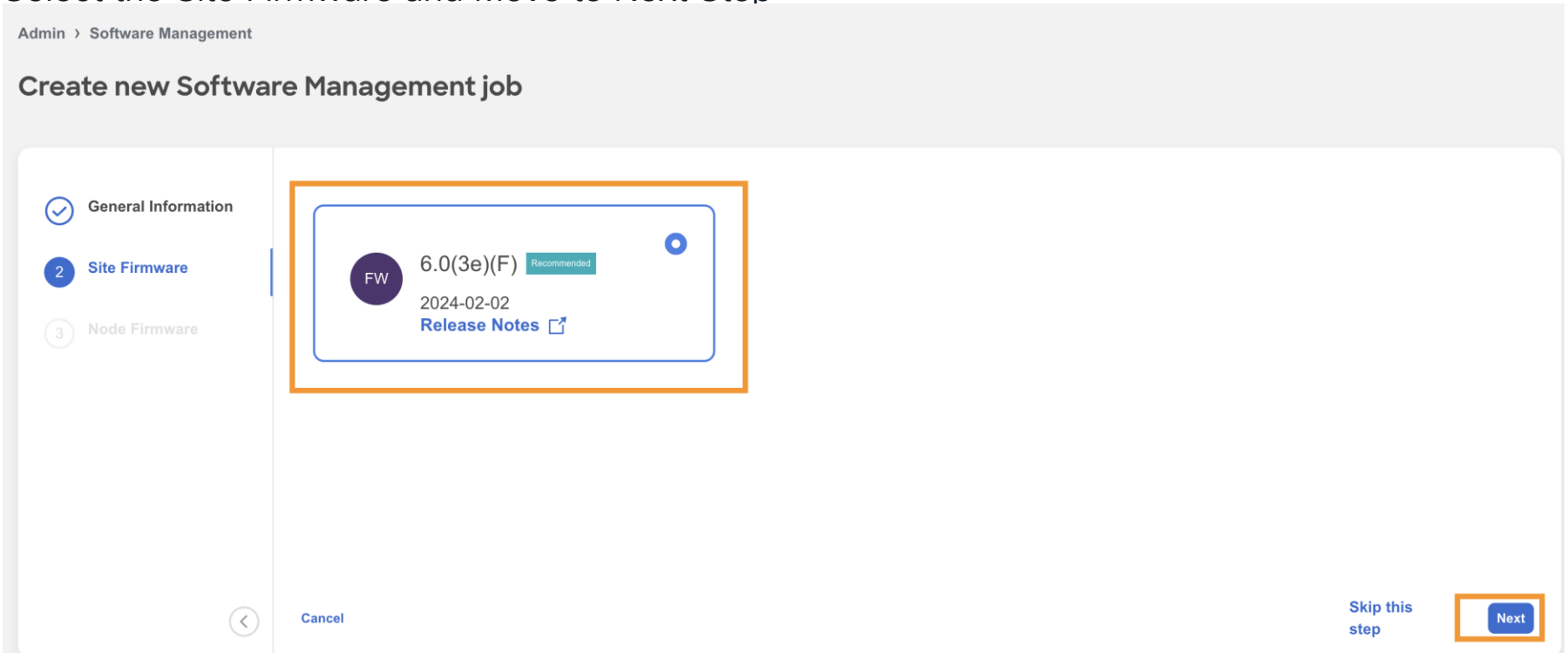
Create a New software management Job



How to do an upgrade analysis

Reference

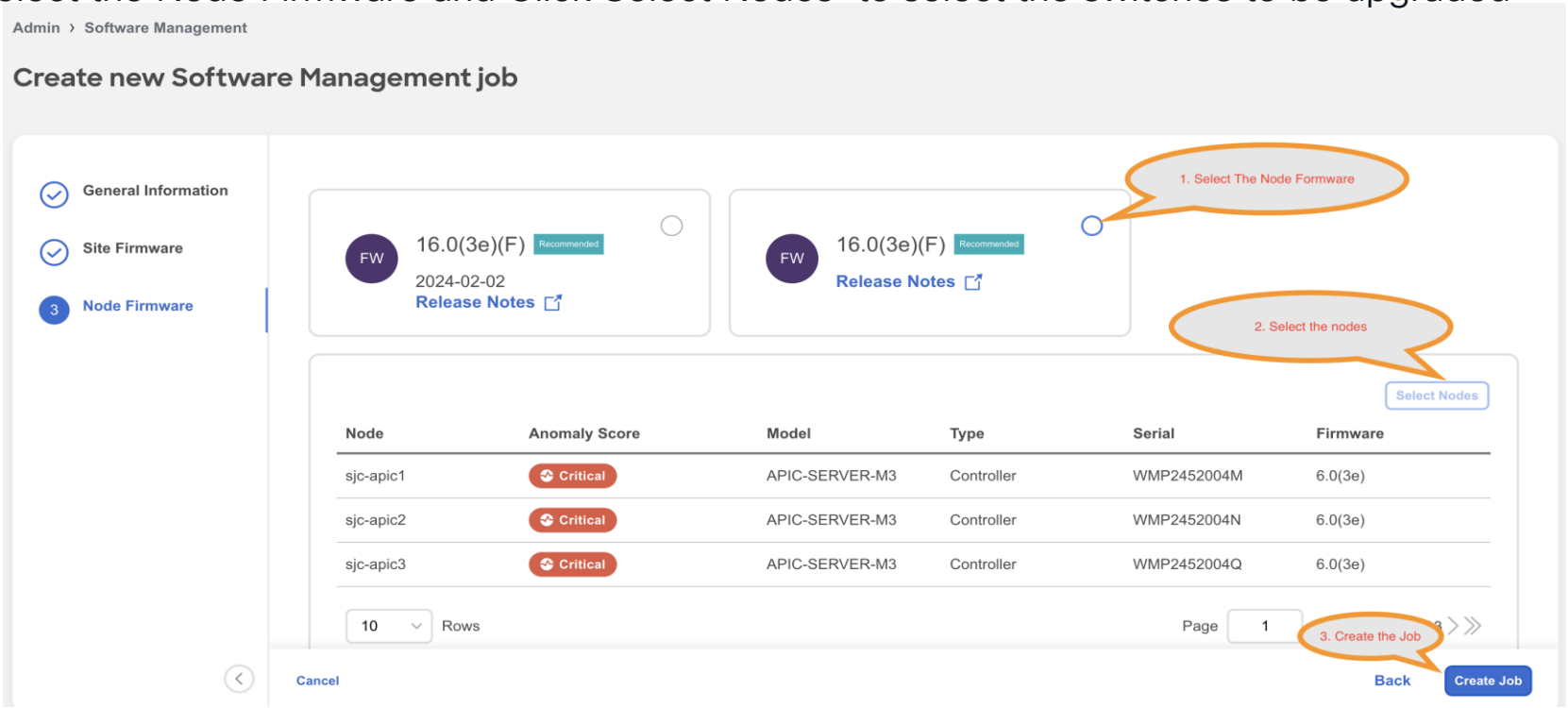
Select the Site Firmware and Move to Next Step



How to do an upgrade analysis

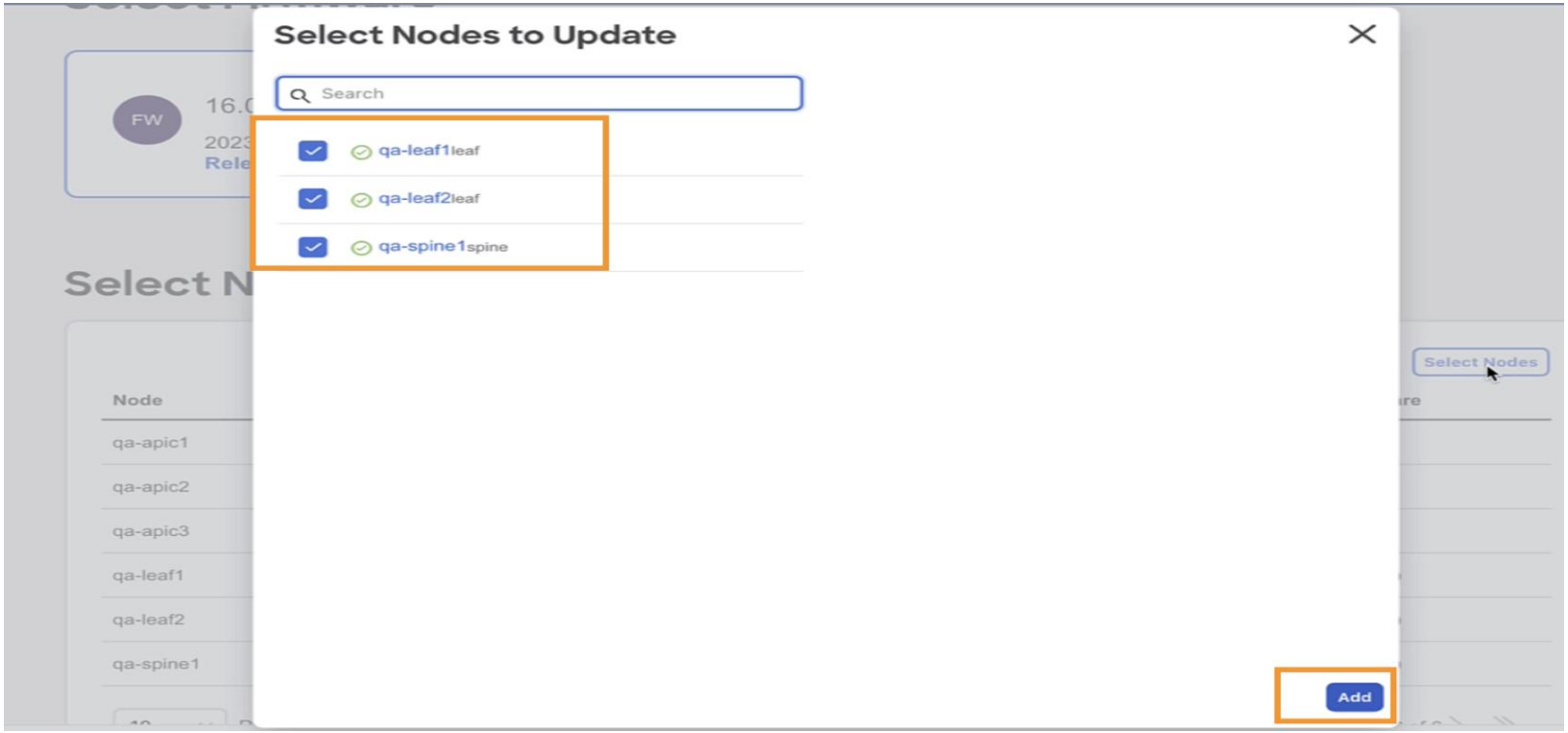
Reference

Select the Node Firmware and Click Select Nodes to select the switches to be upgraded



How to do an upgrade analysis

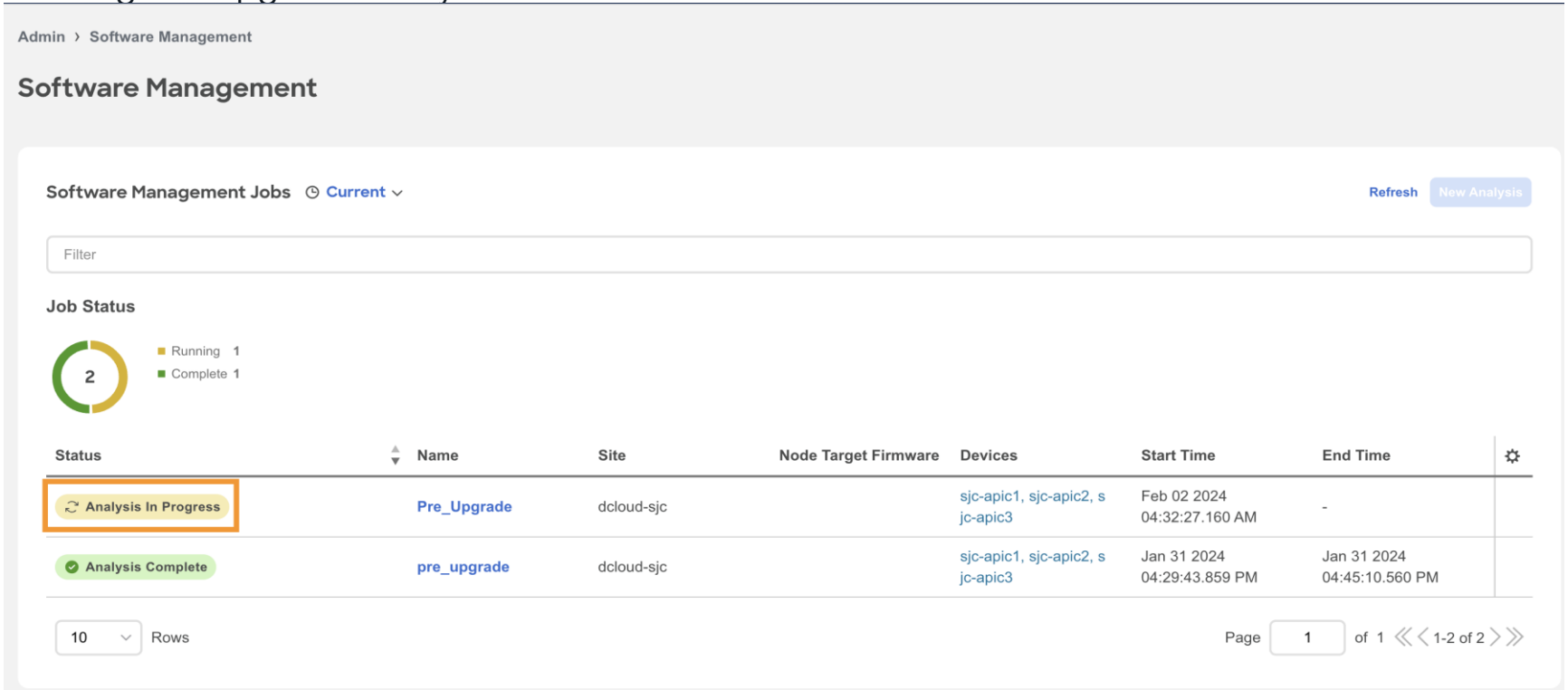
Node Selection



Reference

How to do an upgrade analysis

Viewing the Upgrade Analysis Results

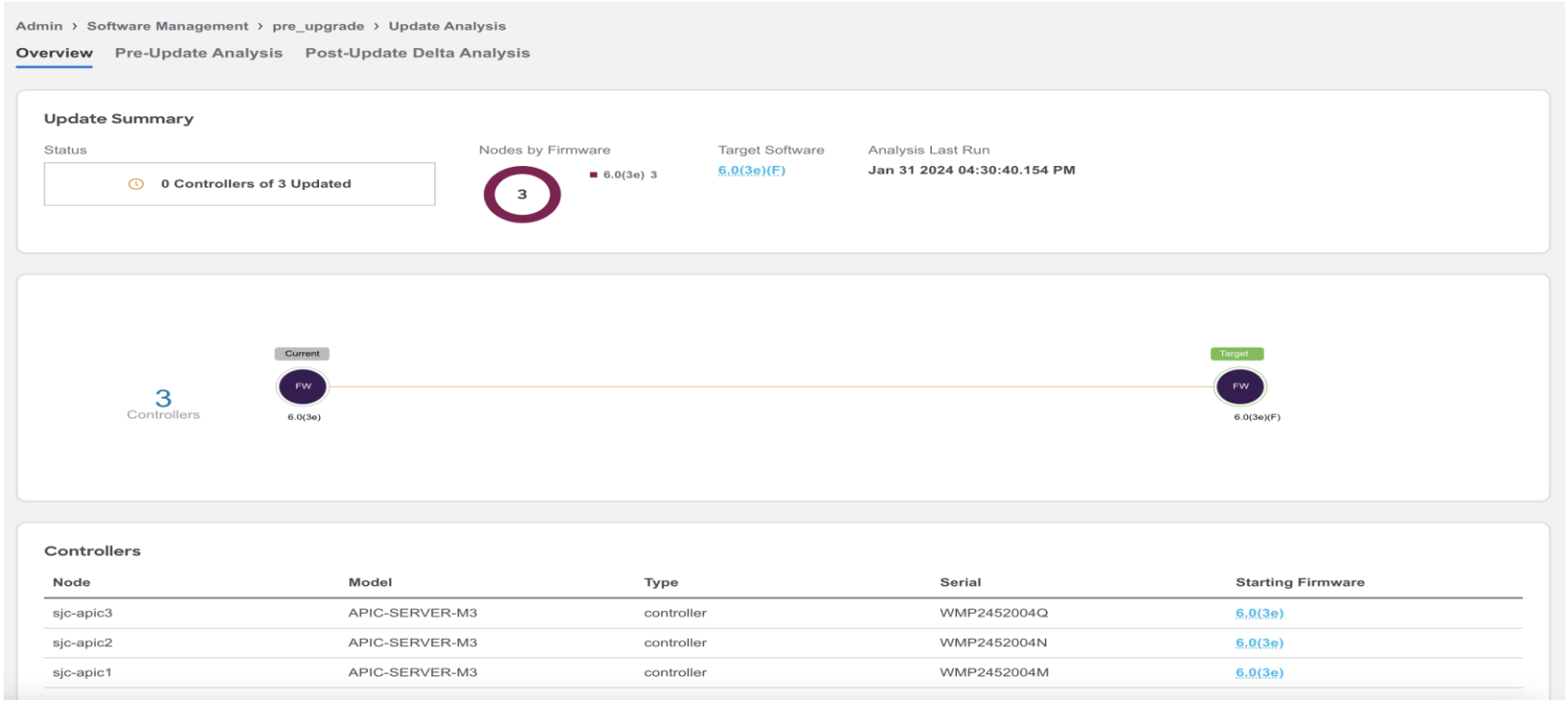


Reference

How to do an upgrade analysis

Viewing the Upgrade Analysis Details

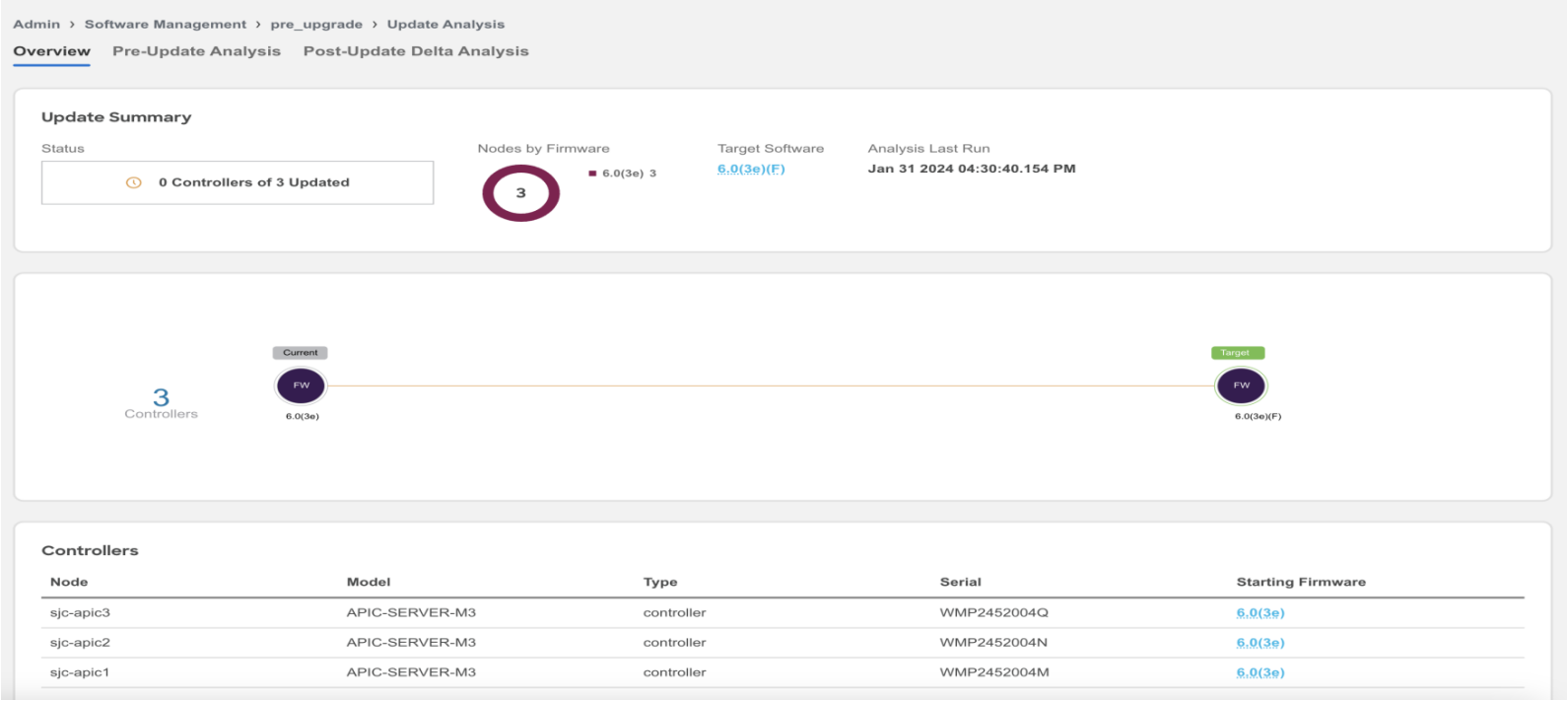
Reference



How to do an upgrade analysis

Reference

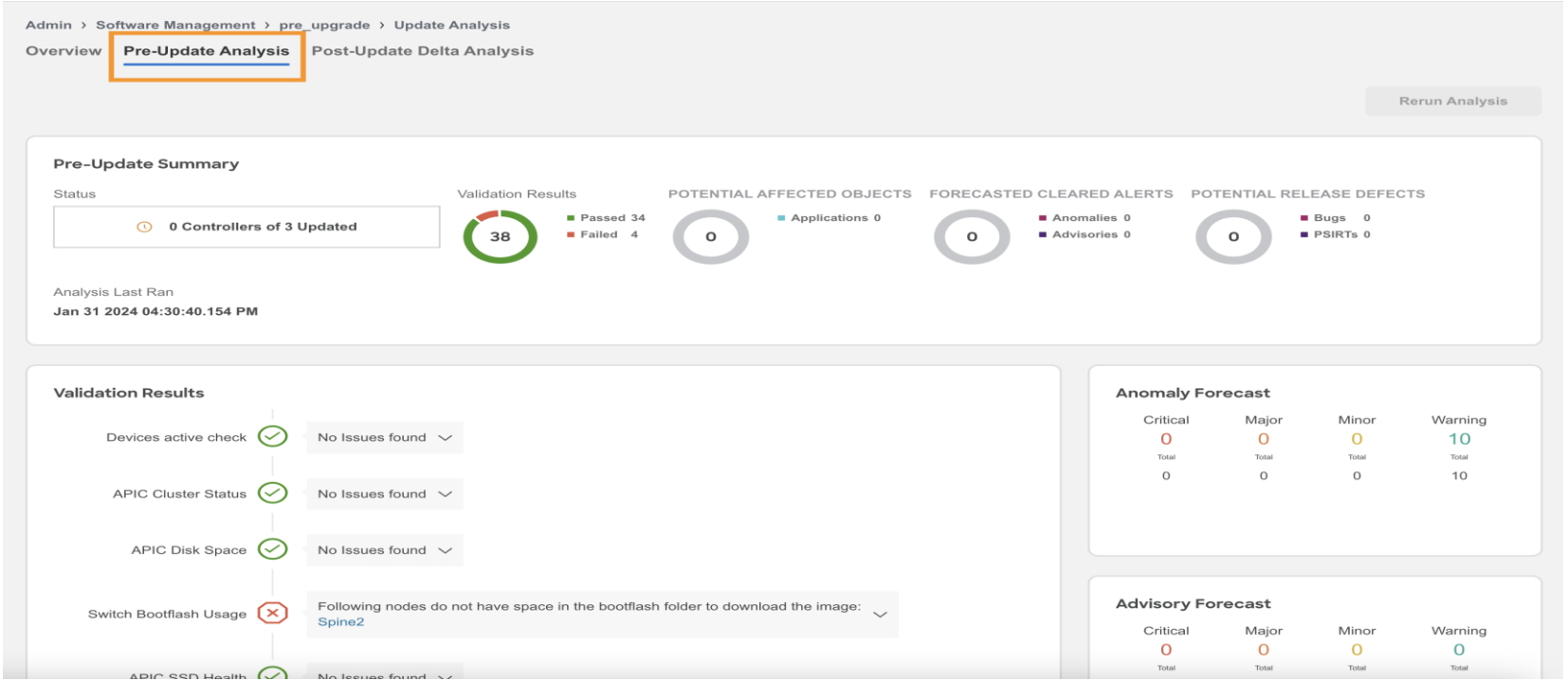
Viewing the Upgrade Analysis Details



How to do an upgrade analysis

Reference

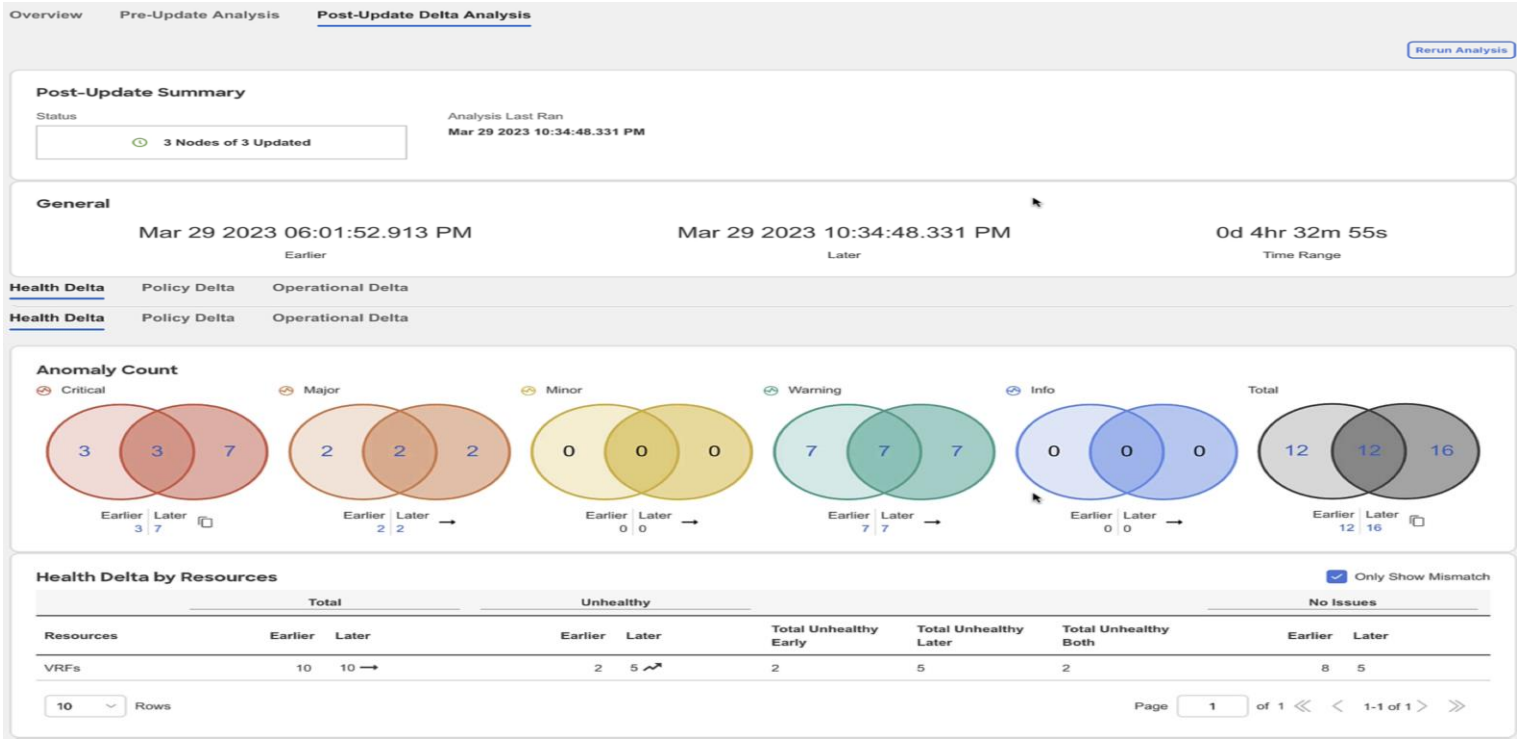
Pre Update Analysis



How to do an upgrade analysis

Reference

Run delta analysis After the actual upgrade is completed



How to do an upgrade analysis

Reference

The areas checked for during pre-upgrade analysis for ‘ACI are listed’ below

1	Critical faults	No Critical Faults from System -> Faults
2	OOB management IP	Ensure static OOB Management IP is configured
3	vPC nodes	Configure vPC for the listed leaf nodes to avoid traffic loss during the reboot of leaf nodes.
4	Route reflectors	Configure vPC for the listed leaf nodes to avoid traffic loss during the reboot of leaf nodes.
5	NTP status	Configure NTP to avoid any issues in DB sync between nodes, SSL certificate check, etc.
6	Infra VLAN id	Check if configured infra VLAN ID are same across nodes
7	Fabric Recovery Enabled	Check if Fabric Recovery is in progress
8	CIMC compatibility	Check if running recommended CIMC version
9	Version compatibility	Check version is compatible or multi-hop upgrade is needed
10	Target firmware check	Check if image is copied and available in device
11	SNMPv3 auth compatibility	Check SNMPv3 authorization and/or privacy
12	Remote leaf compatibility	Check if remote leaf is not supported in the target version.
13	Multi-Tier compatibility	Check if Remote leaf is not supported in the target version
14	Bootflash storage	Check for space in bootflash folder to download image
15	Spine redundancy	Check if each pod upgrades spine nodes with at least two separate groups to avoid traffic loss. Spines should not be in maintenance group.
16	Hardware compatibility	Check if hardware is compatible with version
17	Maintenance groups	Check if maintenance groups were created in pre 4.0 release
18	APIC Cluster Status	Check if APIC Cluster status is fully fit for all APIC nodes

How to do an upgrade analysis

Reference

The areas checked for during pre-upgrade analysis for NXOS are listed below

#	Validation Step	Description
1	validate po summary	Check if all port-channel members are in (P) state
2	validate vpcs	Check if vpc status is “up”
3	validate vpc role	Check if local vPC role is secondary
4	validate sticky bit	Check if local switch vPC sticky bit is False
5	validate hsrp state	Check if "hsrp mgo state" is Active/Standby
6	validate mods	Check if module in ok/active/standby state and diag pass
7	validate ospf	Check if OSPF is in FULL FULL/DR state
8	validate bgp	Check if BGP session is in Up State
9	validate free space	Check if bootflash on active/standby supervisor is greater than threshold
10	validate logging nvram	Check for Severity 1, 2 or 3 messages
11	validate logging log	Check for Severity 1, 2 or 3 messages
12	validate mod exceptions	Check for non-user initiated resets
13	validate redundancy	Check if redundancy status is "Active with HA standby" for EOR
14	validate reset reason	Check if module was reset due to reasons other than those initiated by user
15	validate system reset reason	Check if module was reset due to reasons other than those initiated by user
16	validate diag module	Checks if previously initiated diag had shown failure
17	validate flash ramdisk	Check if all filesystems are equal to or below integer percentage
18	validate console mgmt	Check if console register bits are RTS|DTR|DSR
19	validate environment	Check if all modules are in ok state and backup power present
20	validate arp table	Check if certain number of ARP'S are in INCOMPLETE
21	validate cores	Check if core files are present
22	validate device connectivity	Check if we are able to reach the device with PolicyGateway/NDFC/SIM

Migration Best Practices

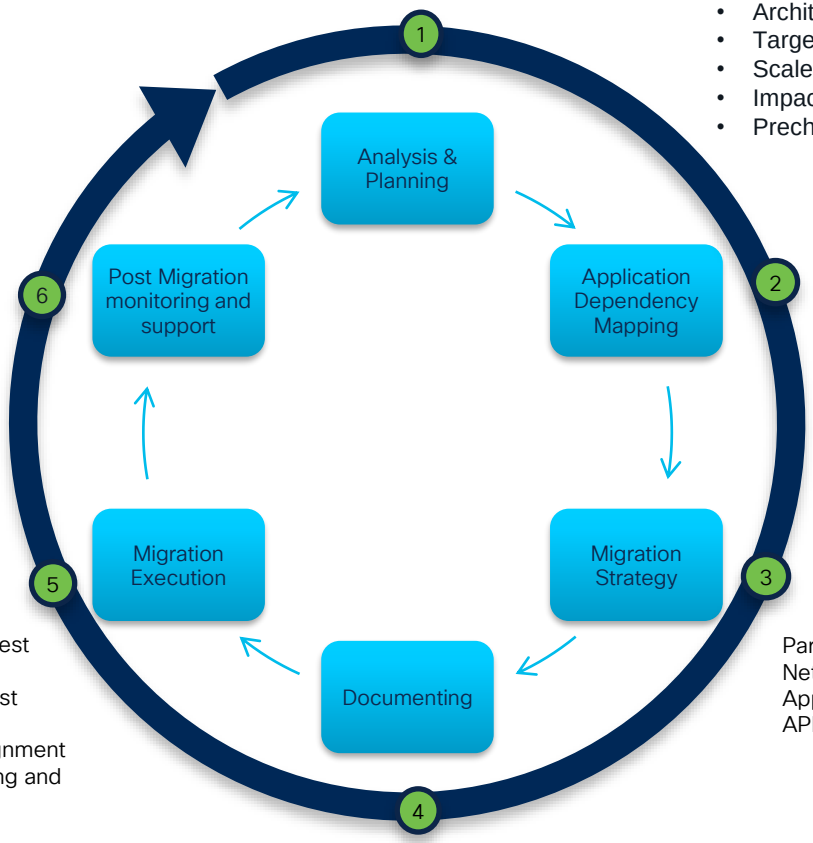
Datacenter Migration – Strategy and Approach

Source Architecture

Spanning Tree	Fabric Path
Vxlan	ACI

Destination Architecture

Vxlan
ACI



- Architecture Governance
- Target Architecture definition
- Scale Considerations
- Impact Analysis
- Prechecks and Validations

- Nexus Dashboard or Cisco Secure Workload (flow metrics or ADM)
- Open-Source automation
- Business Process
- Server to port Mapping
- Automated policy generation

Parallel Vs Hybrid
Network Centric migration
Application based migration
APM during Migration

Runbook, Validation , Rollback

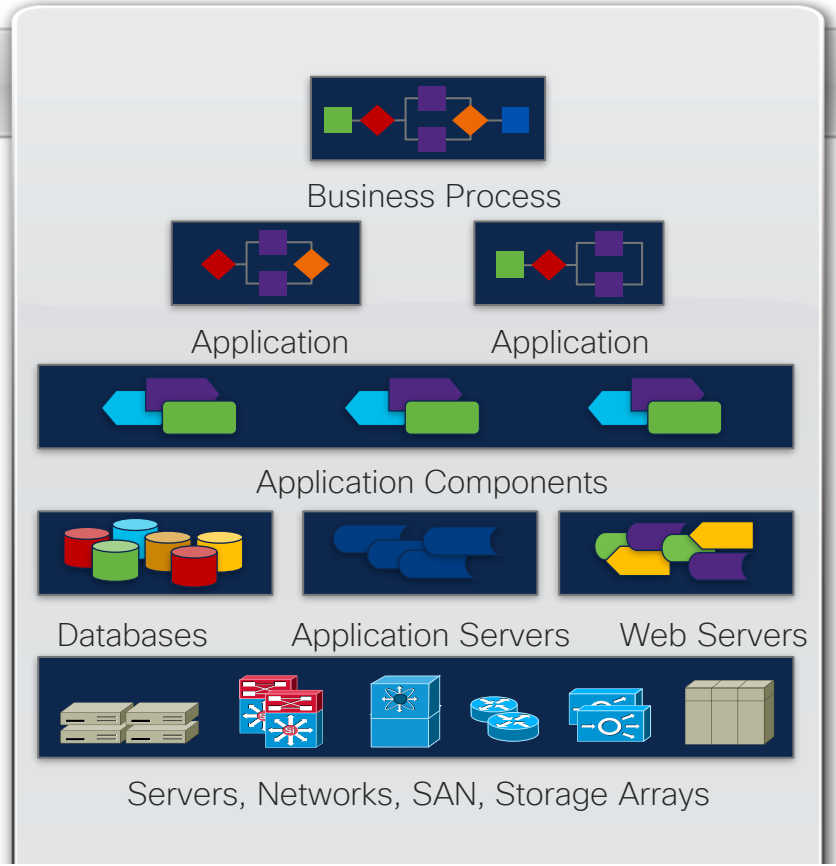
- Change Management Best practices
- SW and HW Platform best practices
- Go – No Go strategy alignment
- Validations before , during and after migration
- Reporting

- APM monitoring
- Issue resolution and SLA
- Detailed Health analysis

Discover Hidden Interdependencies

Discovery

- What do I need to migrate?
  - Understand installed asset base (applications, server, storage, network)
  - Understand interdependencies
- Understand business and operational constraints
  - Core business processes
  - Operational processes
  - Application criticality (prioritize)
  - Current DR capability
  - Available downtime window for migration
- Understand facilities requirements and constraints
  - Power, cooling and rack space
  - Regulatory compliance constraints

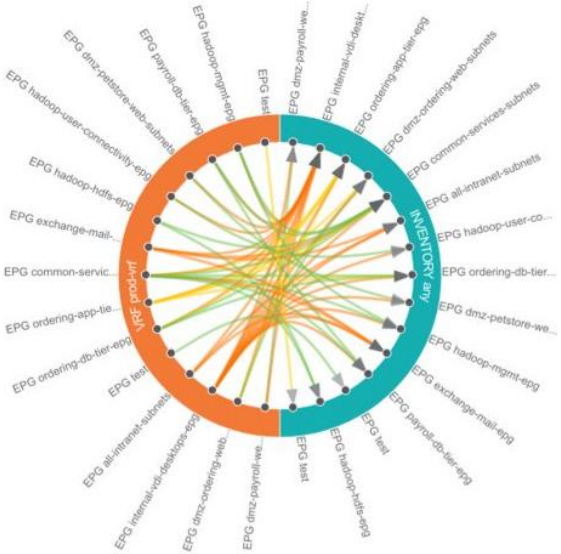


Datacenter Migration Scenarios and Considerations

- Application workload visibility options
- Baseline connectivity Considerations
- Gateway Considerations
- Site Based considerations – for scalability
- Constructs based considerations

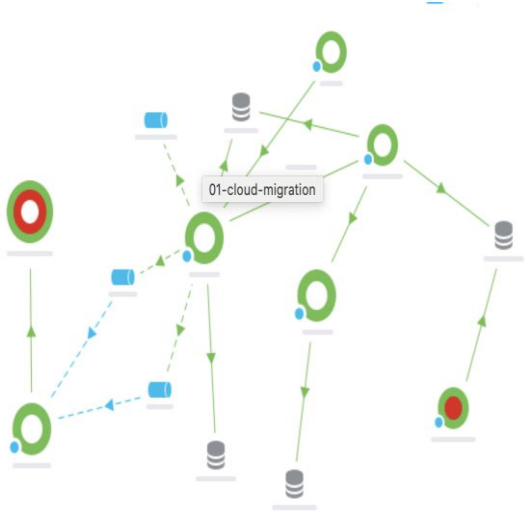
Visibility Considerations and Best Practices for Migration

Application dependency Mapping



Application Dependency Mapping

Application flow Map



Application Flow Mapping

1. Selecting Application for Migration

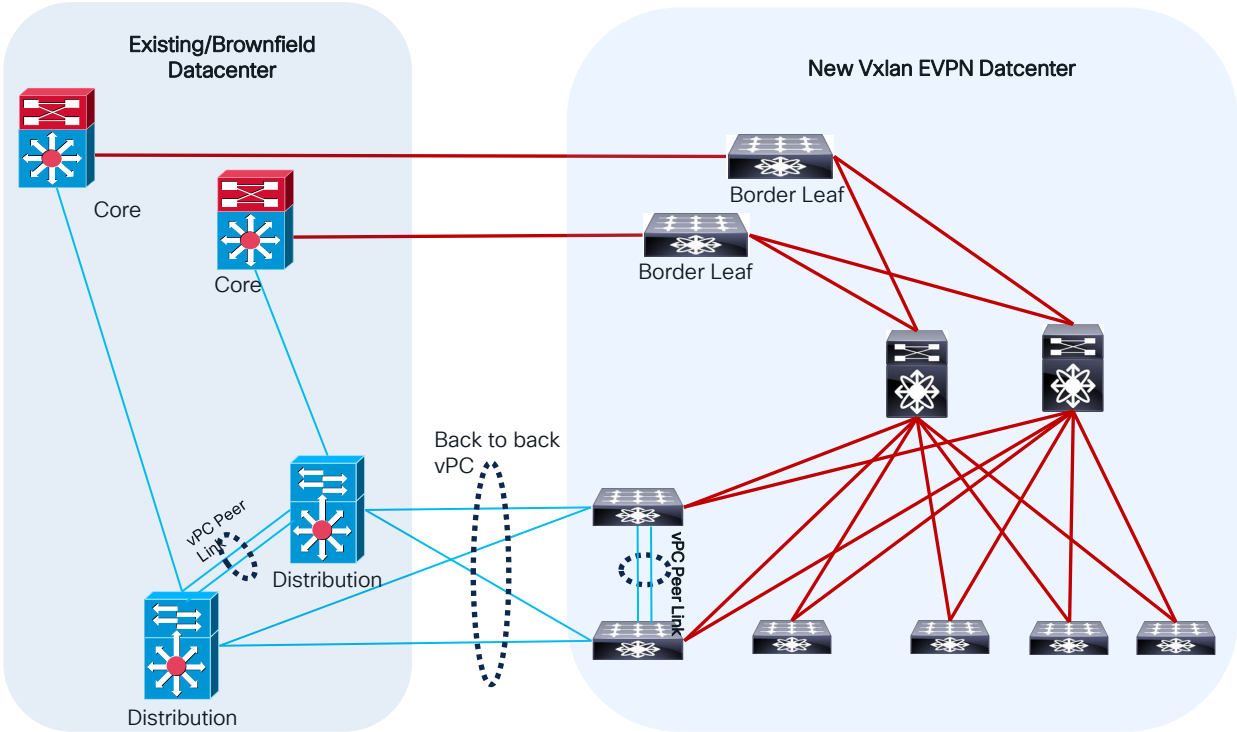
2. benchmark digital experience

3. review the following during Migrations
   a) Application performance monitoring
   b) Latency considerations
   c) Avoiding Suboptimal routing conditions

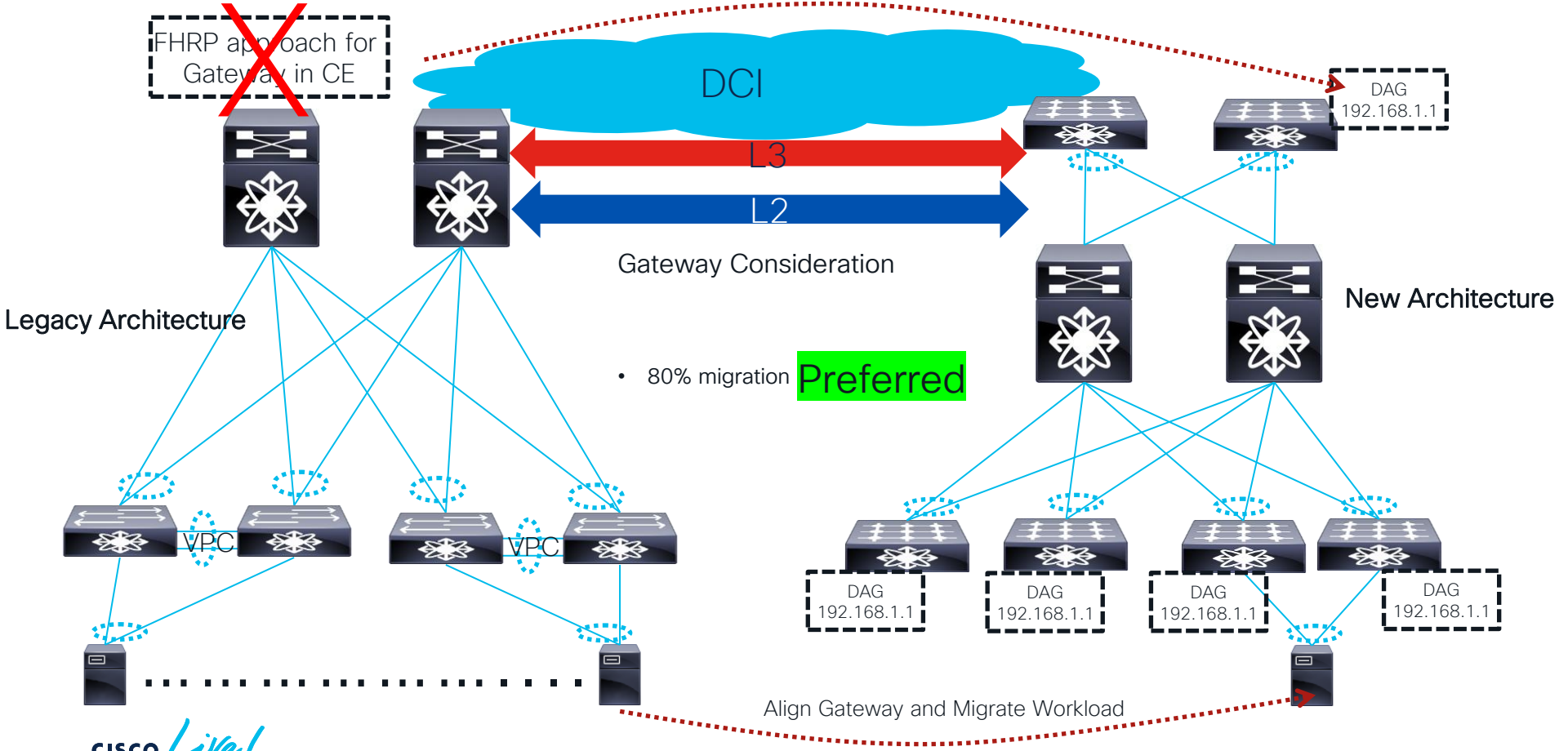
4. Application Performance Monitoring After the migration

Network Considerations for Datacenter Migration

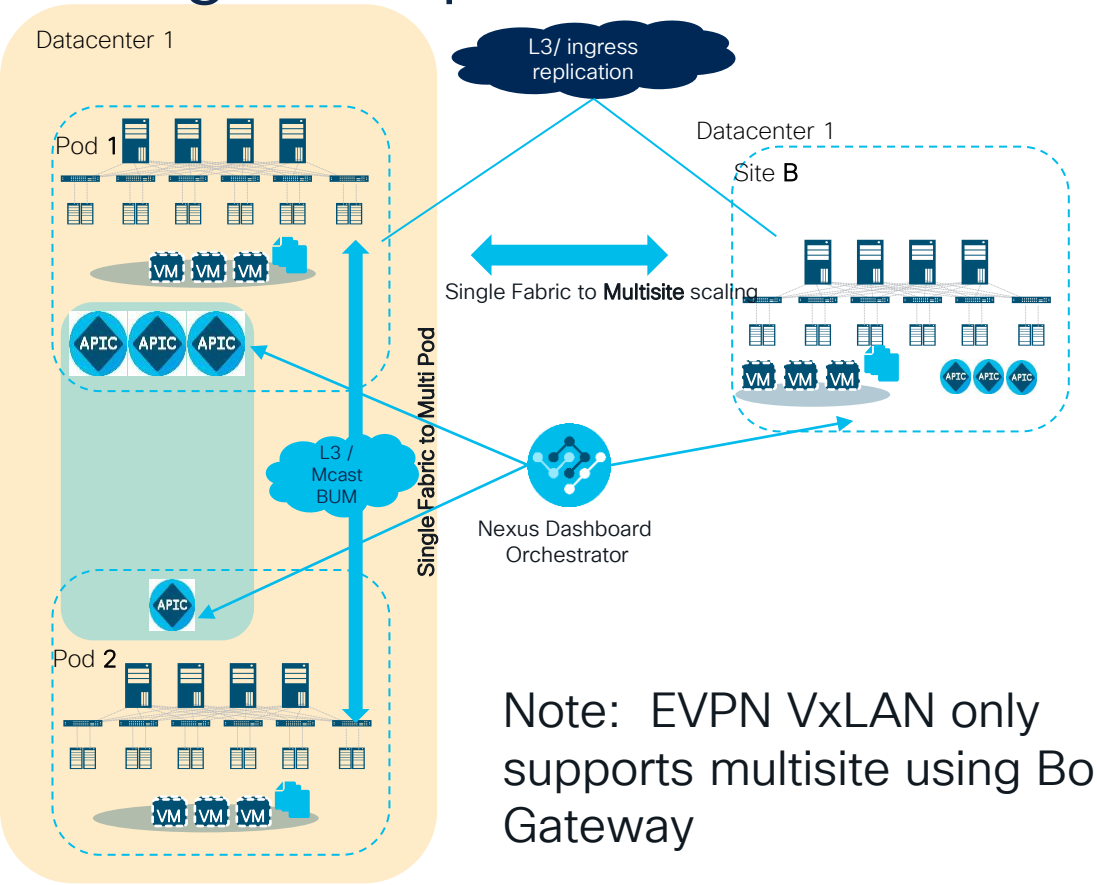
1	Migration Planning	Build a parallel vxlan fabric Establish L2 connection between legacy and new vxlan fabric Establish Dedicated L3 interconnect Between 2 fabrics
2	Layer 2 Considerati on	Dedicated Leaf for L2 Connection using double sided VPC STP Root bridge placement in the fabric
3	Layer 3 Considerati on	Non VPC Border Leaf switches for existing Connections to the core No summarization on border routers during Migration
4	Overlapping Vlans	Vlan translation on the Migration Leaf



Gateway Migrations from Legacy to EVPN environment



Migration practices for Scaling out – use case with ACI



1. Scale Consideration in Data Center 1; options –
   - Multi Pod – same mgmt domain
   - Multi site – separate mgmt. domain

2. Multi-Pod Consideration
   - Extension of APIC cluster- no new policy consideration
   - Special emphasis on the underlay BUM (Mcast support)

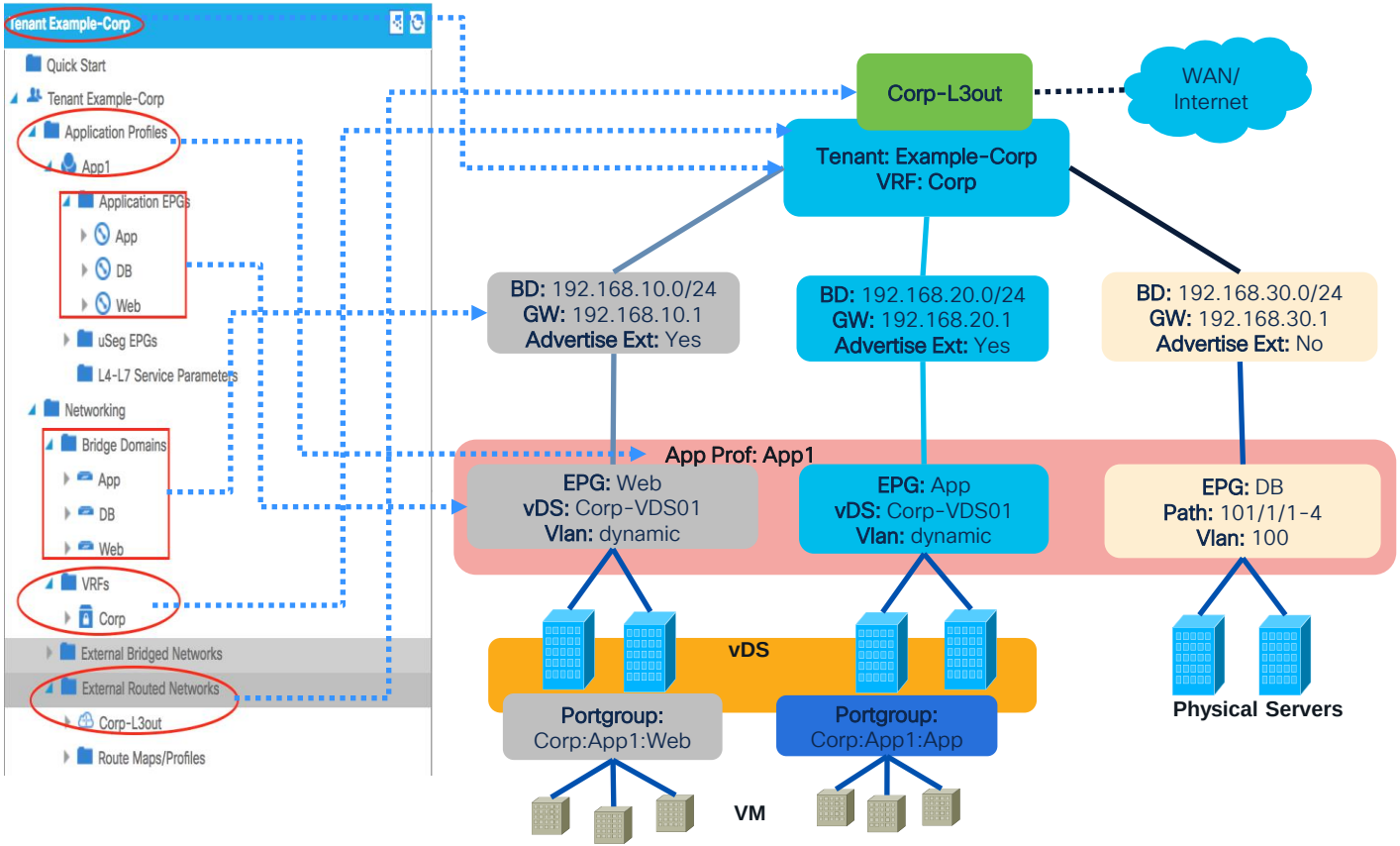
3. Multi-site consideration for policy –
   - Creating new policies Vs importing existing policies
   - Hardware consideration and service block localization for multisite
   - Controller based redundancy for multisite

Note: EVPN VxLAN only supports multisite using Border Gateway

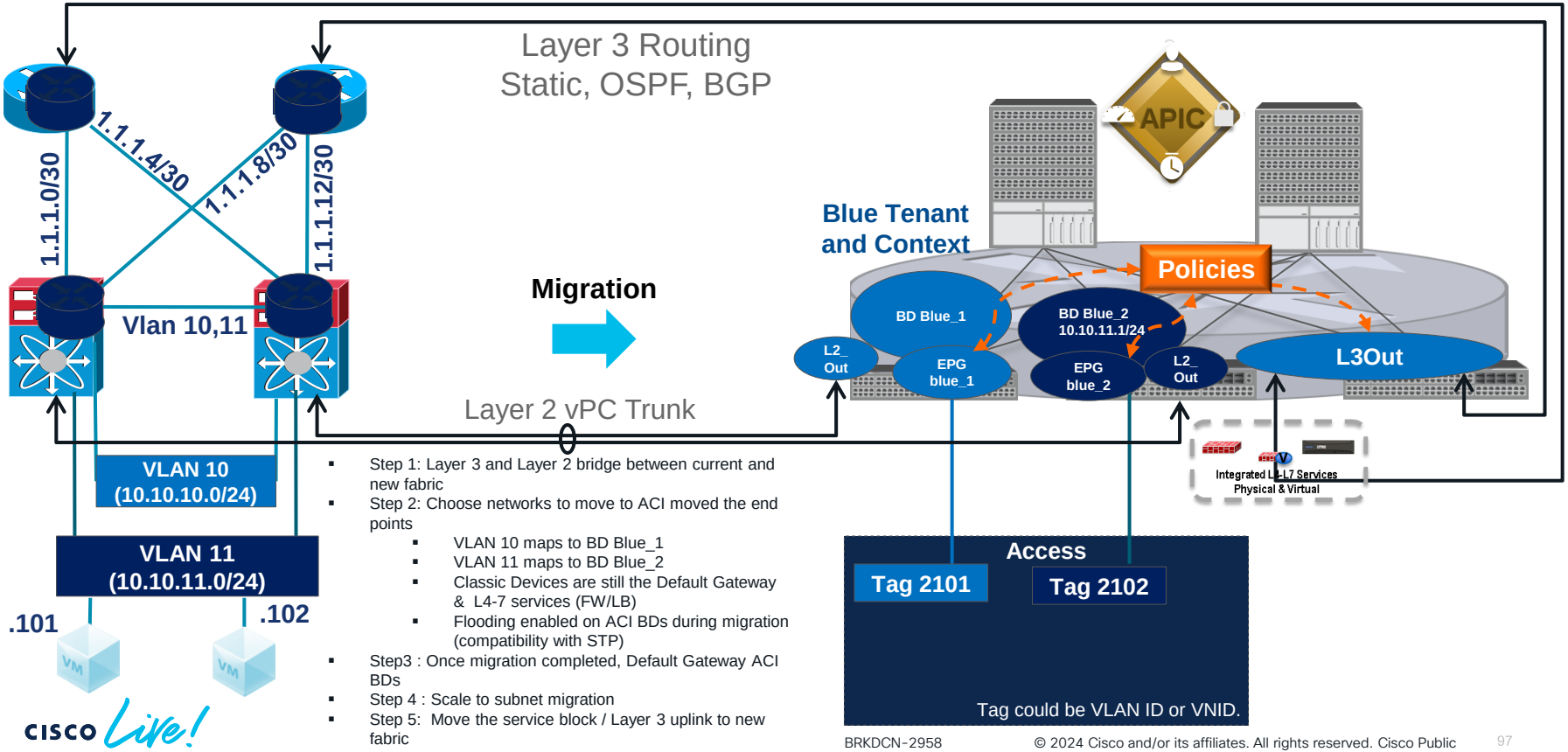
ACI Network Centric Deployment

Network configuration

- VRF CORP …. vrf configuration
- Interface VLAN 100 192.168.10.0/24), VIP 192.168.10.1, VRF corp
- Trunk the switch ports with respective vlans
- VMware port Group Assignment
- Routing Configuration for subnets



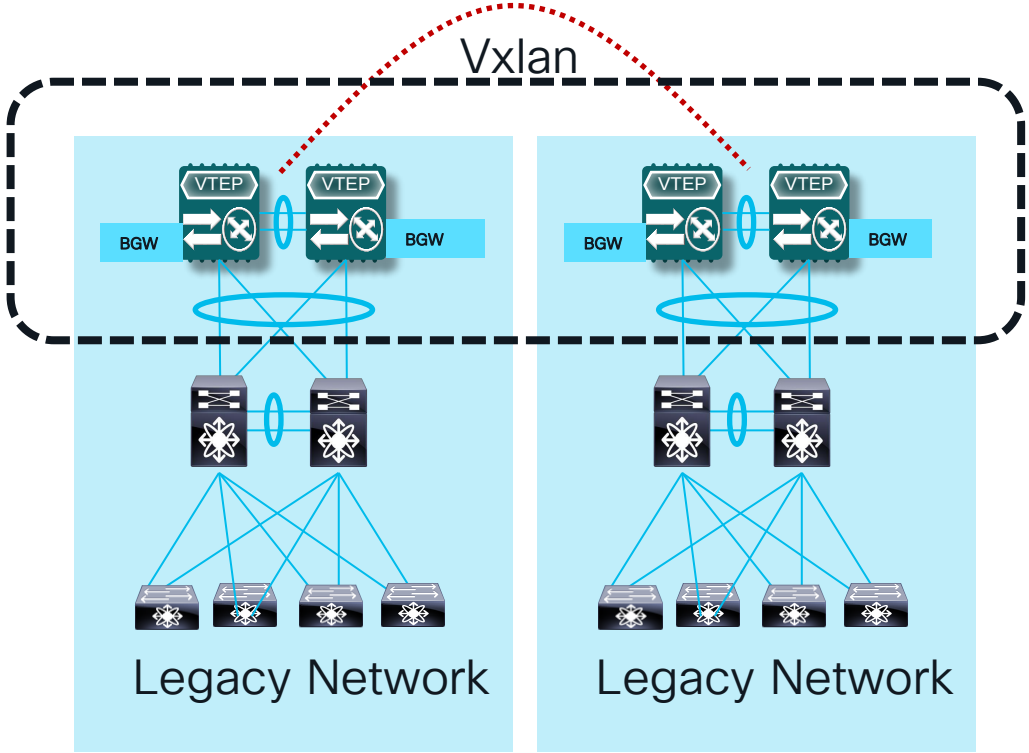
ACI Migration Example



- Step 1: Layer 3 and Layer 2 bridge between current and new fabric
- Step 2: Choose networks to move to ACI moved the end points
  - VLAN 10 maps to BD Blue_1
  - VLAN 11 maps to BD Blue_2
  - Classic Devices are still the Default Gateway & L4-7 services (FW/LB)
  - Flooding enabled on ACI BDs during migration (compatibility with STP)
- Step3 : Once migration completed, Default Gateway ACI BDs
- Step 4 : Scale to subnet migration
- Step 5: Move the service block / Layer 3 uplink to new fabric

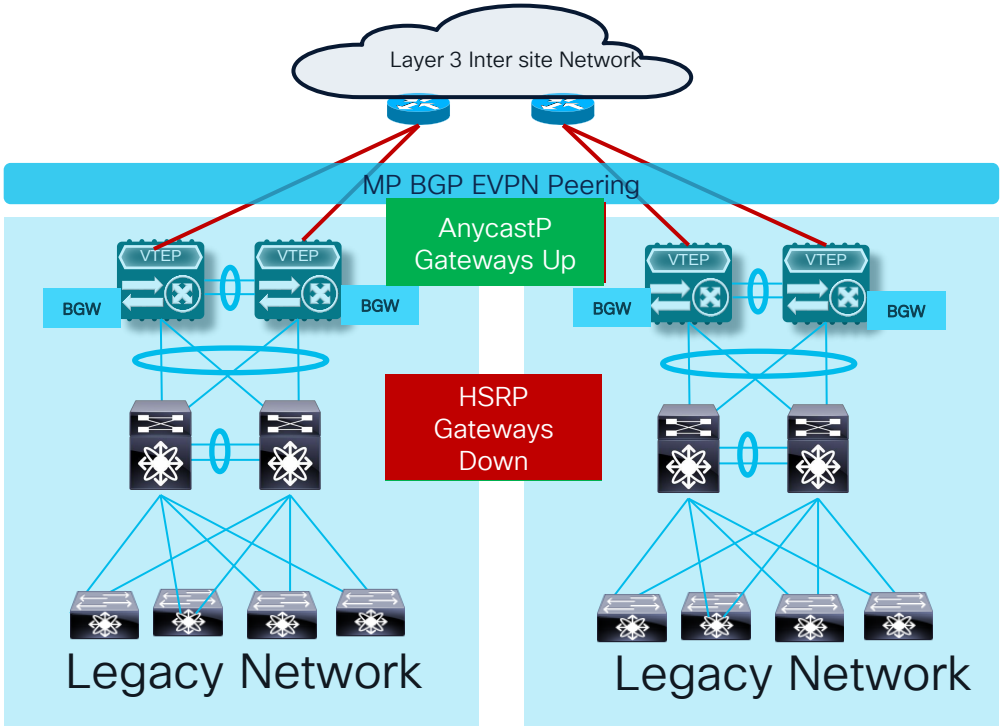
Network Interconnectivity using VXLAN EVPN Border Gateway

- Border Gateway (BGW) provides interconnectivity and translation between multiple Vxlan Sites
- vPC Border Gateway is positioned as replacement for traditional DCI
- Benefits:
  - ✓ Connects to layer 2 domains or 2 domains to EVPN fabric with fault isolation
  - ✓ Simple to deploy compare to old DCI technology and uses EVPN concept
  - ✓ Supports endpoints connected to BGW – cost effective for smaller fabrics Vx Dedicated anycast BGW
- Architectural Benefits
  - Control Plane and Data plane
  - Integrated L2/L3 Extension
  - Fault Containment: BGW provides EVPN Multicast Storm Control
  - Transport Agnostic - Vxlan tunnel built over any IP connectivity
  - Multihoming and Multipath Load sharing



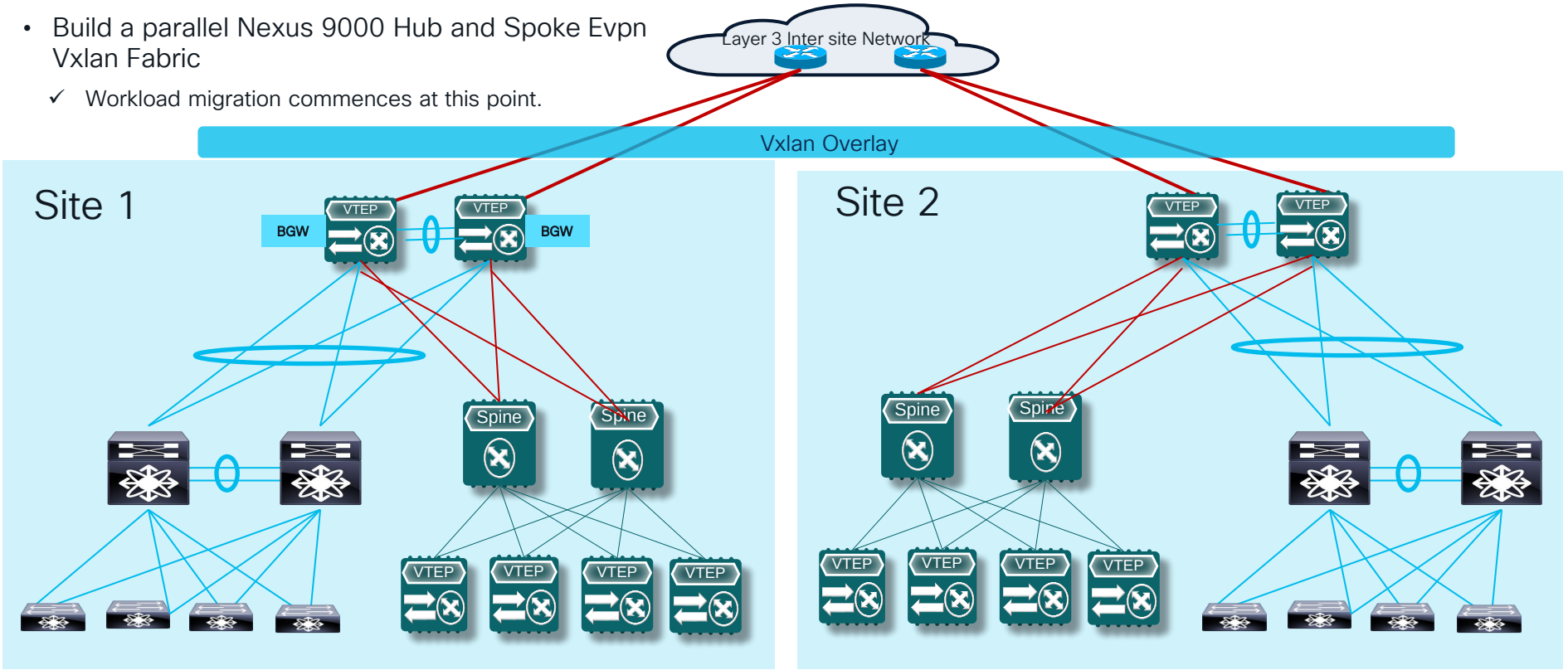
Legacy Network to VXLAN EVPN Migration using Border Gateway

- Introduce a pair of BGW to Legacy sites
  - ✓ Back to back vPC provide multipath connectivity
  - ✓ No STP loops as Double sided vpc provides a single link
- Bringh up vPC BGW Underlay network
  - ✓ Route peering between BGW and first Hop layer 3 devices in the intersite network.
  - ✓ eBGP is recommended as the Underlay protocol
- Configure vPC BGW overlay network
  - ✓ MP-BGP as the overlay Control Plane between BGW nides in two sites.
  - ✓ Full mesh eBGP or route servers in external network depending on size of network
- Configure L2 extension across sites
  - ✓ Should be point-to-point connection & dedicated links.
- Migrate HSRP Gateway on Distribution to Anycast Gateway on BGW
  - ✓ Should be point-to-point connection & dedicated links.

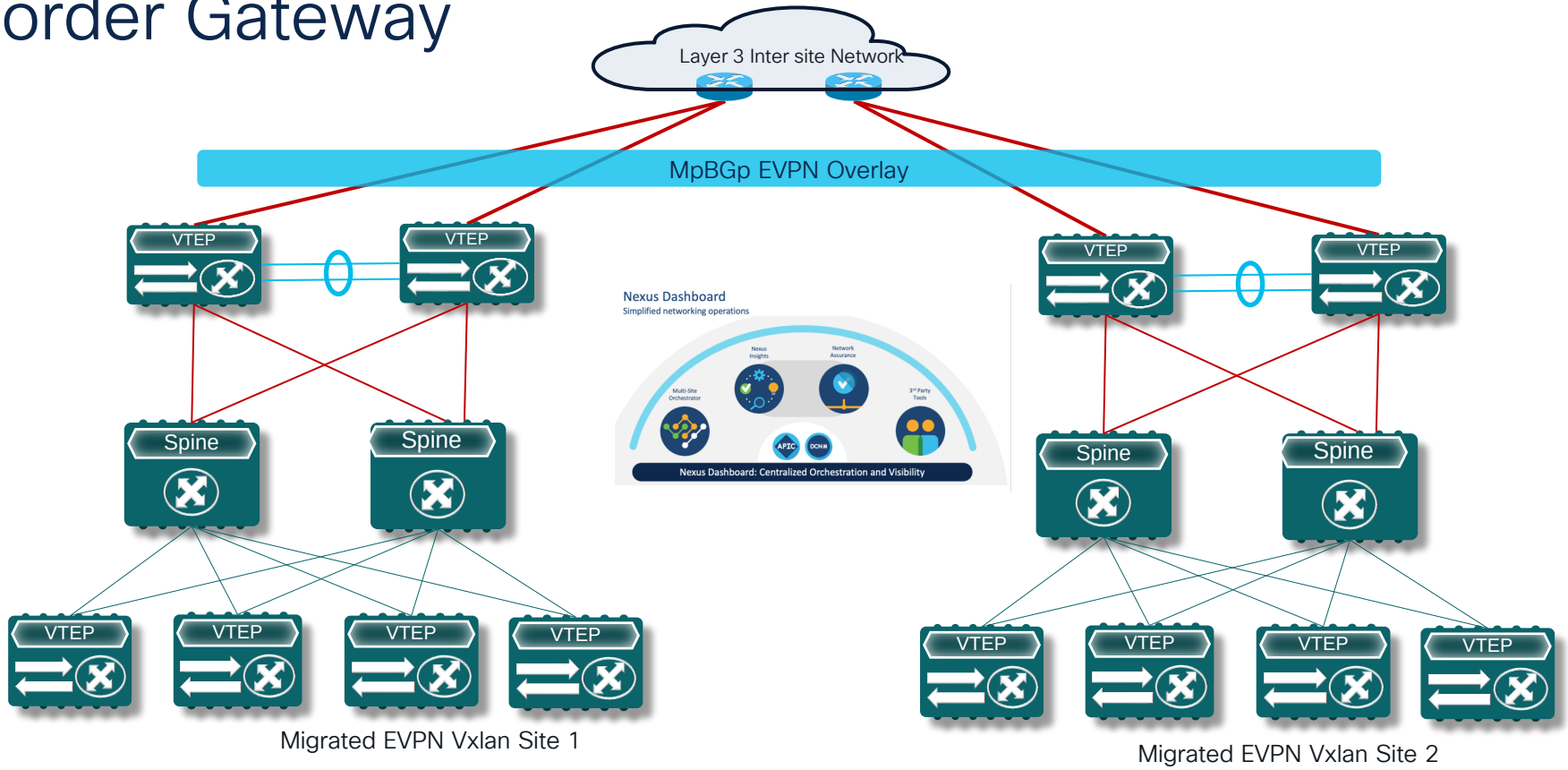


Transition Legacy Network to VXLAN EVPN using Border Gateway – Final Step

- Build a parallel Nexus 9000 Hub and Spoke Evpn Vxlan Fabric
  - ✓ Workload migration commences at this point.



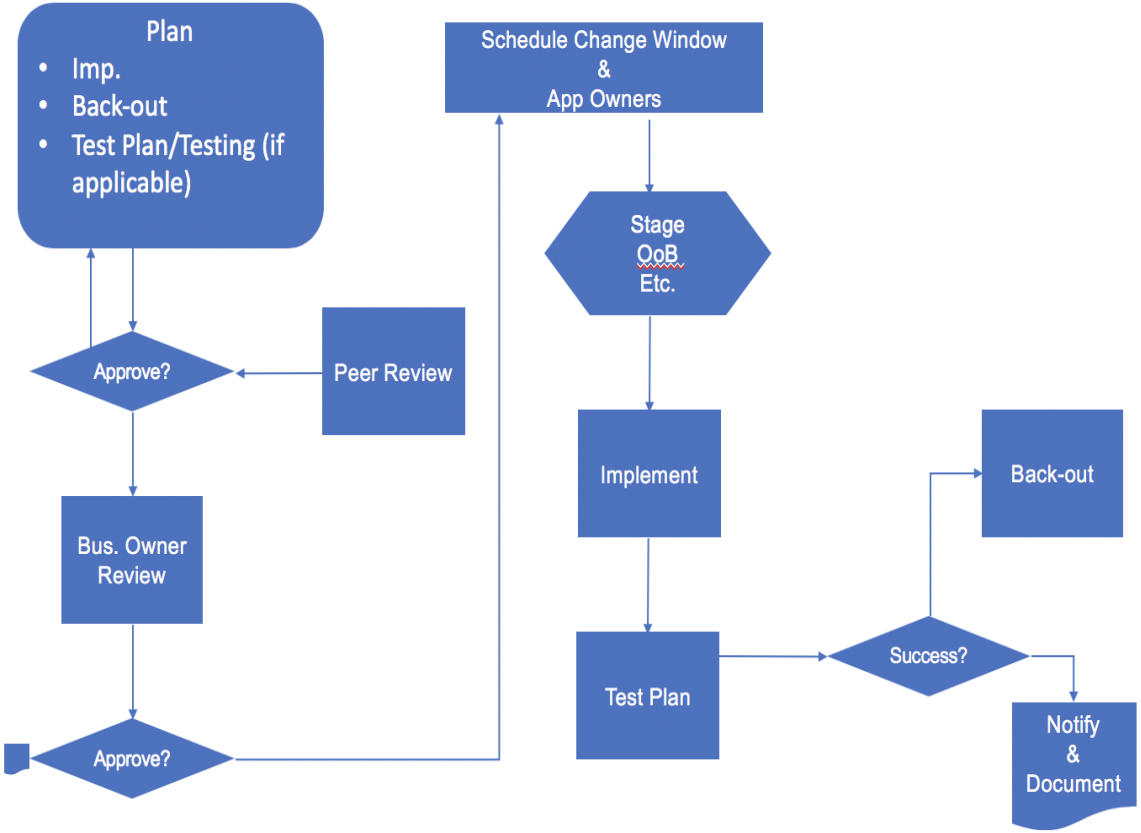
Legacy Network to VXLAN EVPN Migration using Border Gateway



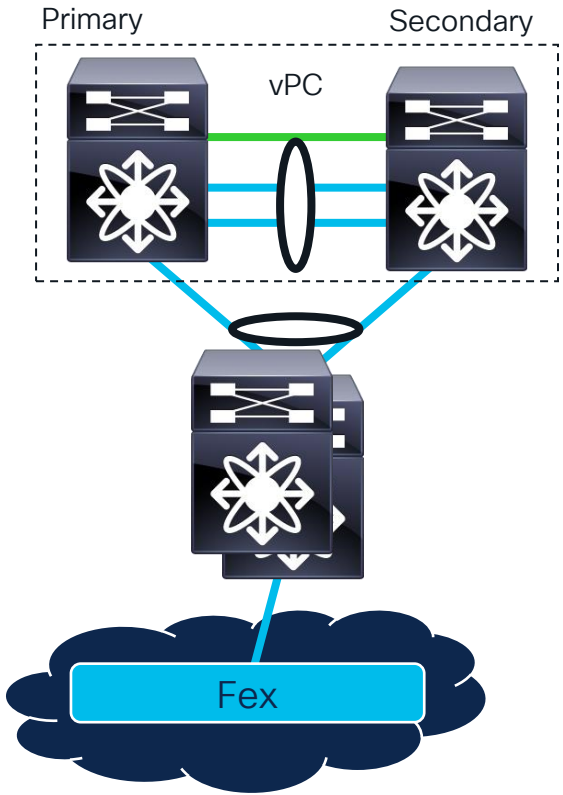
Change Management

Maintenance Windows – Golden Rules

- Change Review Board
- Schedule when environment will be least impacted.
- Software Staging
- Verify out of band.
- Test! After *and* before.



Traditional vPC Environment Change
Change Best Practice and Window



Core Isolation

1. Graceful L3 Protocol Isolation
2. Layer 2 Isolation
   - VPC
3. Interface Isolation

Using GIR Mode Steps 1-3 could be achieved prescriptively.

Access Isolation

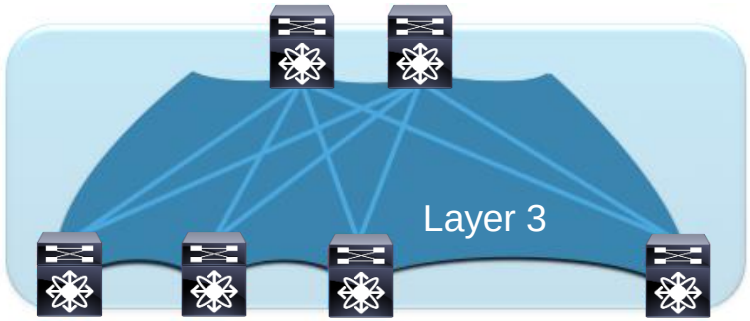
1. Layer 2 Isolation
   - VPC
2. Interface Isolation
   1. Fex-fabric (include/exclude)
   2. Dual-attached FEX Procedure * Recommended

Using GIR Mode Steps 1-2 could be achieved prescriptively.

NOTE: Maintenance mode consideration should be based on Fex-fabric connectivity.

If change window is for software upgrade or spot fix, consider ISSU or SMU feasibility.

L3 Environment
Change Best Practice and Window



Core Isolation

1. Graceful L3 Protocol Isolation
2. Interface Isolation

Using GIR Mode Steps 1-2 could be achieved prescriptively.

Access Isolation

1. L3 Protocol isolation
2. Layer 2 Isolation
    - vPC
3. Interface Isolation
    1. Fex-fabric (include/exclude)
    2. Dual-attached FEX Procedure * Recommended

Using GIR Mode, prescriptive isolation is possible.

If change window is for software upgrade or spot fix, consider ISSU or SMU feasibility.

Summary

Putting it all Together

- What to use? GIR Mode? Patching? ISSU? All of them?

Option \ Situation	Critical Bug Fix & PSIRT	Hardware Upgrade	New Features
ISSU	✓	X	✓
GIR + Cold Boot	✓	X	✓
GIR + Disruptive Installer	✓	X	✓
SMU Restart	✓	X	X
GIR + SMU ISSU	✓	X	X
GIR	X	✓	X

Datacenter Operations –key take ways

- Understand the features and relations to best practices
- Utilize Software hardware best practice in deployment of the Data center
- Change Management features
  - Isolation (GIR)
- Tools used to manage DC environment
  - Day 0,1,2 use controllers based on automation
  - Assurance to manage DC use Nexus Insights

Datacenter Migrations –key take ways

1. Verify environment conforms to data center networking best practices, and leverage DC controllers
2. Isolate Node to minimize the disruption - leverage features like GIR for change window planning
3. Leverage the Migration methodology and use cases to customize your transformation

Technical session surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!
- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.
- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.

Cisco learning and certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.

Learn

Cisco U.
IT learning hub that guides teams and learners toward their goals

Cisco Digital Learning
Subscription-based product, technology, and certification training

Cisco Modeling Labs
Network simulation platform for design, testing, and troubleshooting

Cisco Learning Network
Resource community portal for certifications and learning

Train

Cisco Training Bootcamps
Intensive team & individual automation and technology training programs

Cisco Learning Partner Program
Authorized training partners supporting Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training
Accelerated curriculum of product, technology, and certification courses

Certify

Cisco Certifications and Specialist Certifications
Award-winning certification program empowers students and IT Professionals to advance their technical careers

Cisco Guided Study Groups
180-day certification prep program with learning and support

Cisco Continuing Education Program
Recertification training options for Cisco certified individuals

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**


cisco
The bridge to possible
Thank you
cisco Live!


cisco Live!
Let's go