



You make **possible**



ACI Troubleshooting

VMware vDS VMM Integration

Joseph Ristaino – Technical Leader, DCBU Escalation

BRKACI-2645

CISCO *Live!*

Barcelona | January 27–31, 2020



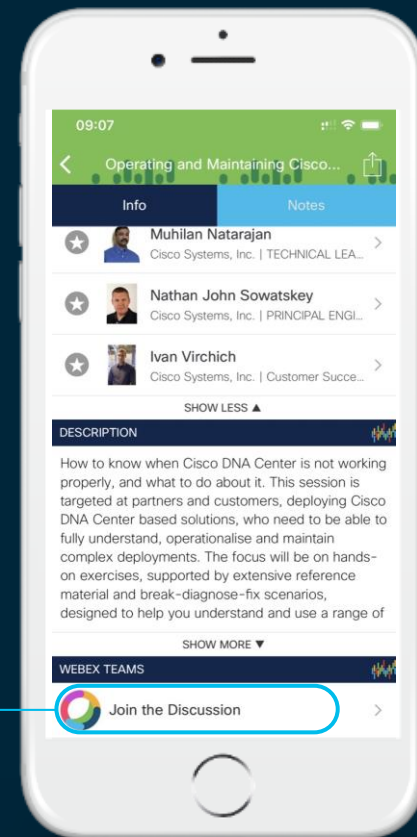
Cisco Webex Teams

Questions?

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

How

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



Agenda

- Introduction
- APIC to vCenter Connectivity
- Host Discovery
- Policy Download and Verification

Acronyms/Definitions

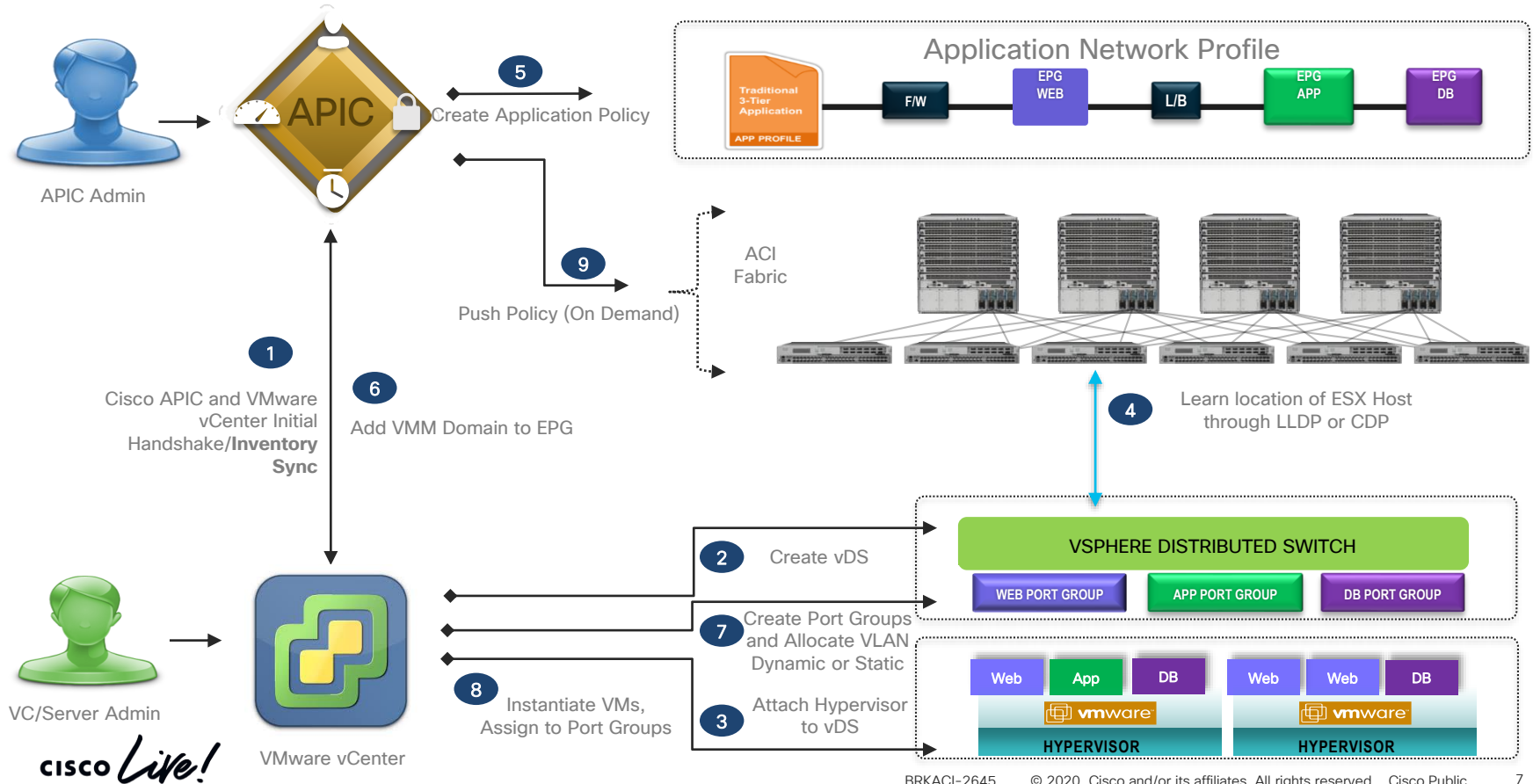
Reference Slide Icon →



Acronyms	Definitions	Acronyms	Definitions
ACI	Application Centric Infrastructure	fvIfConn	MO Object for VLAN Mapping to EPG and Port
AEP	Attachable Entity Profile	fvRsStPathAtt	MO Object for Static EPG Policy to Port
API	Application Programming Interface	LLDP	Link Layer Discovery Protocol
APIC	Application Policy Infrastructure Controller	UCS	Unified Computing System
CDP	Cisco Discovery Protocol	UFN	Unmanaged Fabric Node
DNS	Domain Name System	VC	Virtual Center
vDS	vSphere Distributed Switch	VM	Virtual Machine
EPG	Endpoint Group	VMM	Virtual Machine Manager
fabricLooseNode	MO Object for Blade Switch	VMNIC	Physical NIC on Host
FI	Fabric Interconnect (Blade Switch for UCS B Series Servers)	VNIC	Virtual NIC (for VM)
fvAttEntityPathAtt	MO Object for EPG Deployment to AEP		
fvDyPathAtt	MO Object for Dynamic EPG Policy to Port		

Introduction

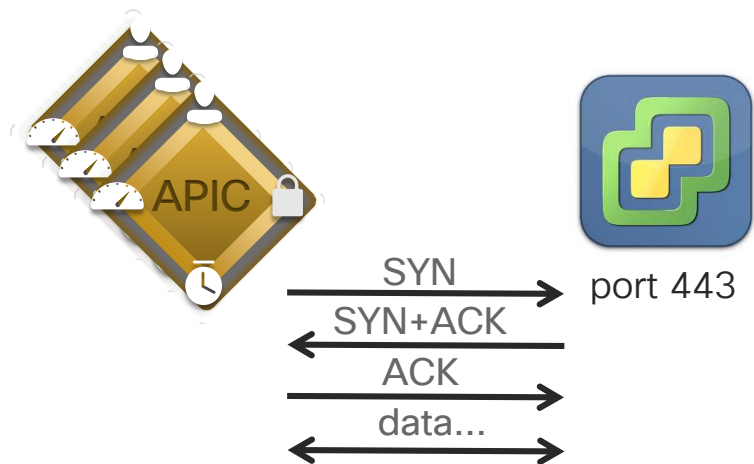
Cisco ACI Hypervisor Integration



APIC to vCenter Connectivity

APIC to vCenter Connection

Network Connection



Important Notes:

- APIC Initiates Handshake and Login with VC on **Port 443** via **OOB** or **In-Band** depending on preference.
- APIC connects to VC using a user account to pull the inventory, receive events, and push config
- Only 1 APIC Active Per VMM Domain
- Connection is handed to new APIC in case previous owner goes unavailable.

What If the connection is broken?

- vDS and/or Port Groups Will not be pushed
- Inventory Sync will Fail
- Events from VC will be missed on APIC

APIC to vCenter Connection

Troubleshooting - Faults

Virtual Networking > VMM Domains > VMWare > Policy > Faults

Affected Object: **comp/prov-VMware/ctrlr-[CiscoLive]-VC** 

Description: Fault delegate: Connection to VMM controller: 172.18.118.140 with name VC in datacenter jristain in domain: CiscoLive is failing repeatedly with error: []. Please verify network connectivity of VMM controller 172.18.118.140 and check VMM controller user credentials are valid.

Type: Communications



Hmmm, are my permissions correct?



Severity: major

Last Transition: 2019-02-19T17:28:33.205-05:00

Lifecycle: Soaking

Affected Object: **comp/prov-VMware/ctrlr-[CiscoLive]-VC** 

Description: Fault delegate: Connection to VMM controller: 172.18.118.140 with name VC in datacenter jristain in domain: CiscoLive is failing repeatedly with error: []. Please verify network connectivity of VMM controller 172.18.118.140 and check VMM controller user credentials are valid.

Type: Communications

Cause: connect-failed

Change Set: operSt (Old: online, New: offline), remoteOperIssues (Old: partial-inv, New:), usr (Old: aciladmin@vsphere.local, New: acilbroken@vsphere.local)

Created: 2019-02-19T17:28:33.205-05:00

Code: F0130

Number of

Occurrences: 1

Original Severity: r

Previous

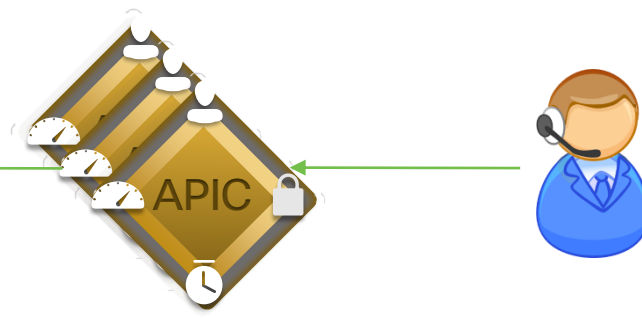
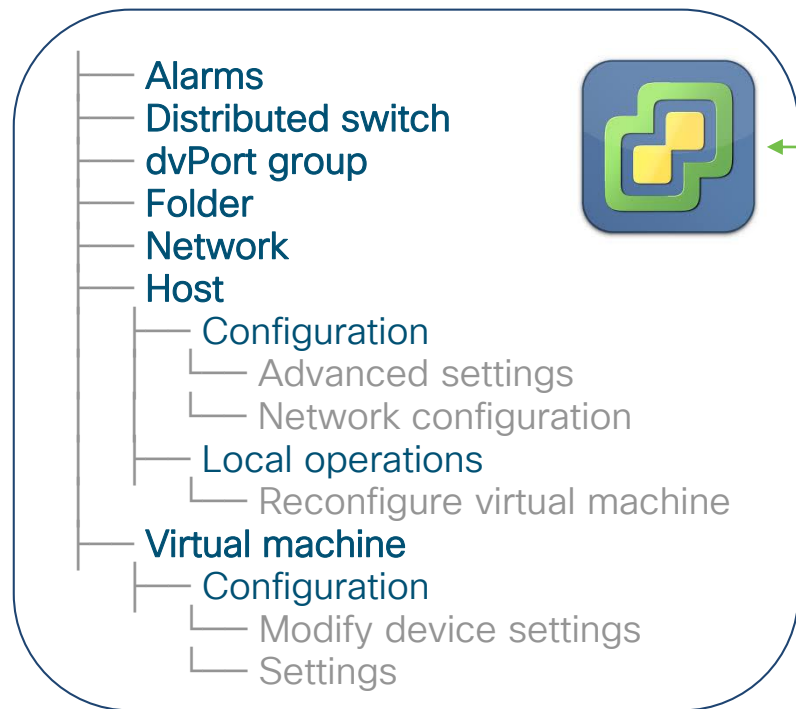
Severity:

Highest Severity: major

F0130

APIC to vCenter Connection

User Credentials



APIC needs access to the VMware API for the following:

- Inventory Sync
- vDS/Port Group Creation
- Event Subscriptions

APIC to vCenter Connection

Troubleshooting - Faults

Virtual Networking > VMM Domains > VMWare > Policy > Faults

Affected Object: **comp/prov-VMware/ctrlr-[CiscoLive]-VC** 

Description: Fault delegate: Connection to VMM controller: 172.18.118.140 with name VC in datacenter jristain in domain: CiscoLive is failing repeatedly with error: []. Please verify network connectivity of VMM controller 172.18.118.140 and check VMM controller user credentials are valid.

Type: Communications

Severity: major

Last Transition: 2019-02-19T17:28:33.205-05:00

Lifecycle: Soaking

Affected Object: **comp/prov-VMware/ctrlr-[CiscoLive]-VC** 

Description: Fault delegate: Connection to VMM controller: 172.18.118.140 with name VC in datacenter jristain in domain: CiscoLive is failing repeatedly with error: []. Please verify network connectivity of VMM controller 172.18.118.140 and check VMM controller user credentials are valid.

Type: Communications

Cause: connect-failed

Change Set: operSt (Old: online, New: offline), remoteOperIssues (Old: partial-inv, New:), usr (Old: aciadmin@vsphere.local, New: acibroken@vsphere.local)

Created: 2019-02-19T17:28:33.205-05:00

Code: F0130

Number of Occurrences: 1

Original Severity: major

Previous Severity: major

Severity: major

Highest Severity: major

F0130

Hmmm, but my permissions are all correct!

APIC to vCenter Connection

Troubleshooting – Find Shard Leader



1

Find Shard Leader

NXOS CLI on Any APIC

3.1(2)+

```
apic1# show vmware domain name CiscoLive
. . .
Domain Name           : CiscoLive
Virtual Switch Mode   : VMware Distributed Switch
. . .
vCenters:
Faults:(Critical, Major, Minor, Warning)
vCenter      Status   ESXs    VMs    Faults
-----
172.18.118.140 online    3       11    0,0,0,0
. . .
APIC Owner:
Controller    APIC      Ownership
-----
VC            apic1     Leader
VC            apic2     NonLeader
VC            apic3     NonLeader
. . .
```

OR

1

Find Shard Leader

Check MO file for each APIC

Any
Version

```
apic1# bash
admin@apic1:> cat /debug/apic1/vmmngr/comp/prov-VMware/
ctrlr-[CiscoLive]-VC/info/mo
CtrlrDn           : comp/prov-VMware/ctrlr-[CiscoLive]-VC
CurrentRole       : Leader
OperState         : 0
MainConnectionStatus : Connected
EventConnectionStatus : Connected
DropEventStatus   : False
TaskMapLoggingStatus : False
SharedEventLog     : False
MaxWorkerQueueSize : 300
CurrentWorkerQueueSize : 0
RcvdEventCount     : 4
EventCollectorId   : 0
                  : No more pending events
EventCollectorId   : 1
                  : No more pending events
UnprocessedEventCount : 0
PendingTasksCount   : 0
```

APIC to vCenter Connection

Shard Leader Verification



2 Check DNS

```
apic1# nslookup ciscolive-vcenter
Server:      10.11.12.13
Address:     10.11.12.13#53

Name:  ciscolive-vcenter.cisco.com
Address: 172.18.118.140
```

3 Check Route Table

```
apic1# bash
admin@apic1:~> route
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
default 192.168.4.1 0.0.0.0 UG 16 0 0 oobmgmt
10.0.0.0 10.0.0.30 255.255.0.0 UG 0 0 0 bond0.3091
10.0.0.30 0.0.0.0 255.255.255.255 UH 0 0 0 bond0.3091
```

4 Verify IP Connectivity

```
apic1# ping 172.18.118.140
PING 172.18.118.140 (172.18.118.140) 56(84) bytes of data.
64 bytes from 172.18.118.140: icmp_seq=1 ttl=61 time=0.512 ms
64 bytes from 172.18.118.140: icmp_seq=2 ttl=61 time=0.660 ms
64 bytes from 172.18.118.140: icmp_seq=3 ttl=61 time=0.624 ms

--- 172.18.118.140 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 0.512/0.598/0.660/0.069 ms
```

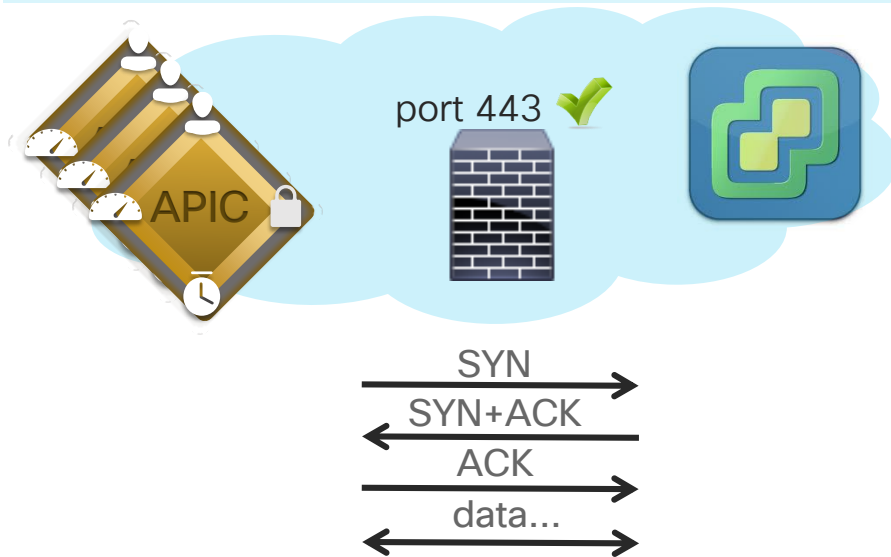
APIC to vCenter Connection

Troubleshooting - Connectivity

5

Check Firewall Rules

Port 443 must be **allowed** between all APICs and VC.
Including Windows Firewall!

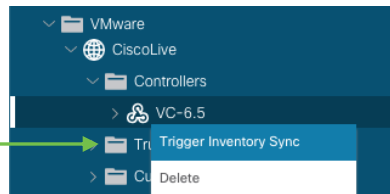


APIC Inventory Synchronization

- APIC **Synchronizes** with VC **every 24 hours**.

- Can also be triggered manually

Virtual Networking > VMM Domains > VMWare > Domain > Controller



- Purpose is to ensure we have full knowledge of VC state for correct programming
- Hosts and VM's** determine where policy can be pushed
- Port Groups and Network Settings** are checked for consistency between APIC and VC
- Attribute Tags and Folders** can be used as a MicroSegmentation Match Parameter



Hosts



VMs



Networking



Tags



Folders

APIC Inventory Synchronization

What If It Fails???

- New Config may be missing in vCenter
- Dynamic Policy Download to Leafs may stop working!
- Fault is Raised

Fault Properties

Affected Object: `comp/prov-VMware/ctrl-[CiscoLive]-VC`

Description: Fault delegate: Operational issues detected for VMM controller: 172.18.118.140 with name VC in datacenter jristain in domain: CiscoLive due to error: Received partial inventory in the last inventory sync. Please look for Faults under VM and Host and fix them via VCenter, then manually re-trigger inventory sync on APIC

Last Transition: 2019-02-19T17:28:33.208-05:00

Lifecycle: Raised

Affected Object: `comp/prov-VMware/ctrl-[CiscoLive]-VC`

Description: Fault delegate: Operational issues detected for VMM controller: 172.18.118.140 with name VC in datacenter jristain in domain: CiscoLive due to error: Received partial inventory in the last inventory sync. Please look for Faults under VM and Host and fix them via VCenter, then manually re-trigger inventory sync on APIC

Type: Operational

Cause: operational-issues

Change Set: operSt (Old: online, New: offline), remoteOperIssues (Old: partial-inv, New:), usr (Old: aciadmin@vsphere.local, New: acibroken@vsphere.local)

Created: 2019-02-19T16:42:05.760-05:00

Code: F0132

F0132



Hosts



VMs



Networking



Tags



Folders

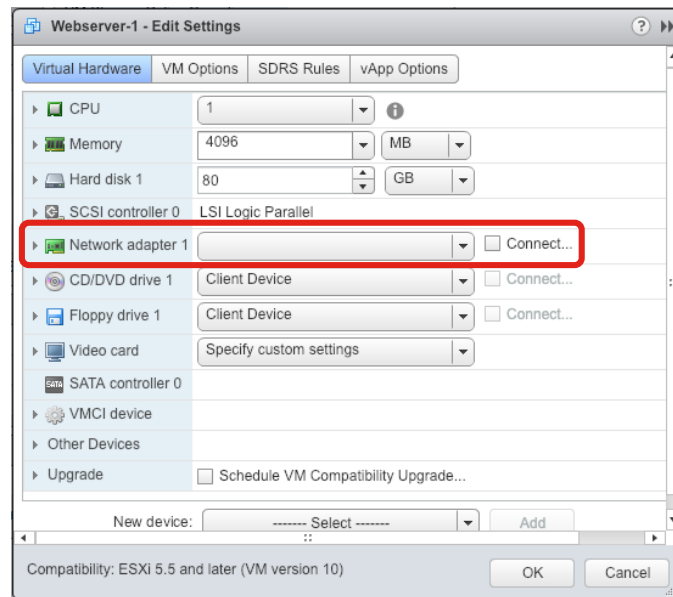
APIC Inventory Synchronization

Common Failure Scenarios

VMs with Invalid Backings

Problem:

- If a VM is moved from one VC to another, and the old port group is not present on the new VC, the VM will have an **“Invalid Backing”**
- This causes **Inventory Sync to Fail** because the network information cannot be retrieved!



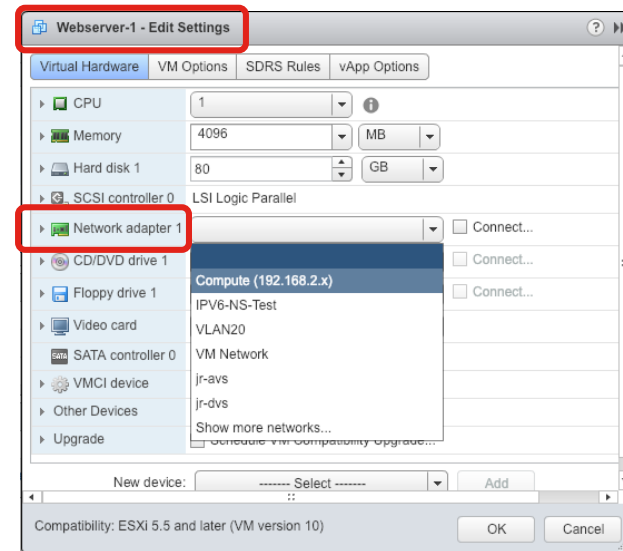
APIC Inventory Synchronization

Common Failure Scenarios

VMs with Invalid Backings

Fix – Prior to 3.2(4) Release

- 1 Tail VMM Log on Shard Leader
- 2 Manually Trigger Inventory Sync
- 3 Find VM(s) and assign valid network



```
apic1# bash
admin@apic1:~> cd /var/log/dme/log
admin@apic1:log> tail -f svc_ifc_vmmmgr.bin.log | egrep -i "Inventory pull|failed to update"
6348||19-02-19 16:39:55.782-05:00||ifc_vmmmgr||WARN|||CiscoLive: VC: 0x563e3b4e4a10: Failed to update VnicCfg Webserver-1:Network adapter 1
6348||19-02-19 16:39:55.899-05:00||ifc_vmmmgr||INFO|||CiscoLive: VC: 0x563e3b4e4a10: getHvHealthProvider | starting inventory pull...
6348||19-02-19 16:39:55.904-05:00||ifc_vmmmgr||DBG4||fn=[startInventoryPull]||CiscoLive: VC: 0x563e3b4e4a10: Inventory pull is Partial.
```

APIC Inventory Synchronization

Common Failure Scenarios

VMs with Invalid Backings

Fix – 3.2(4) Release and Above

- 1 Inventory Sync will still complete
- 2 Fault is raised to alert which VM has the issue!

Fault Properties

General Troubleshooting History

Fault Code: F2842
Severity: major
Last Transition: 2019-02-19T15:30:12.742-05:00
Lifecycle: Soaking
Affected Object: [comp/prov-VMware/ctrlr-\[CiscoLive\]-VC/vm-vm-165/vnic-00:50:56:82:51:74](#)
Description: Fault delegate: Operational issues detected for VNIC Network adapter 1 on VM Webserver-1 in VMM controller: 172.18.118.140 with name VC in datacenter jristain in domain: CiscoLive due to error: VNIC is attached to an invalid DVS Port Group or unable to communicate with vCenter.
Type: Operational
Cause: operational-issues
Change Set: issues (Old: , New: vnic-miss-epg-fault)
Created: 2019-02-19T15:30:12.742-05:00
Code: F2842

Affected Object: [comp/prov-VMware/ctrlr-\[CiscoLive\]-VC/vm-vm-165/vnic-00:50:56:82:51:74](#)

Description: Fault delegate: Operational issues detected for VNIC Network adapter 1 on VM Webserver-1 in VMM controller: 172.18.118.140 with name VC in datacenter jristain in domain: CiscoLive due to error: VNIC is attached to an invalid DVS Port Group or unable to communicate with vCenter.

APIC Inventory Synchronization

Common Failure Scenarios

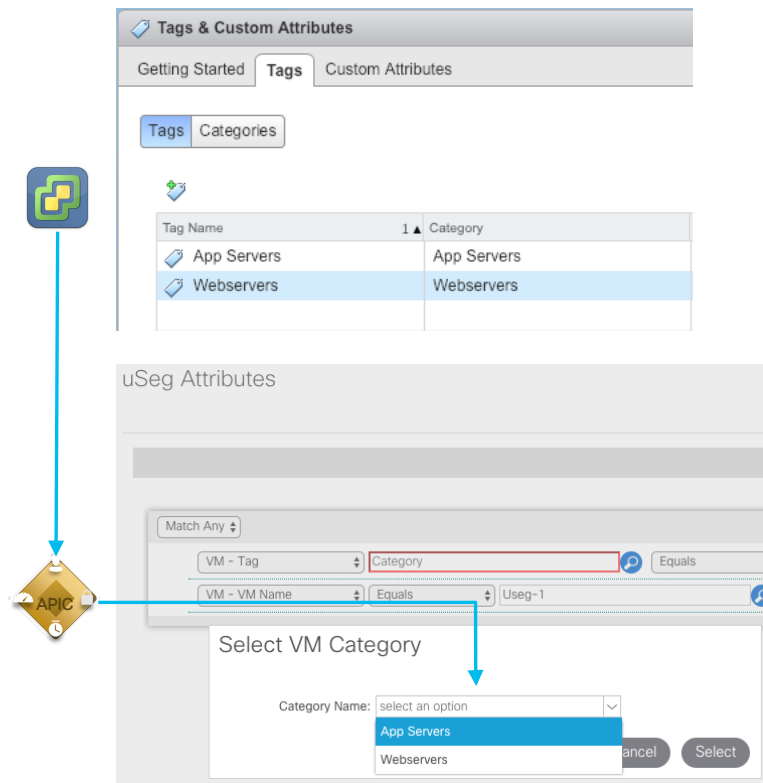
Unable to Retrieve Tag or Folder Inventory

Problem:

- Starting in VC 6.0, VMware introduced attribute tags. Starting in Version 2.3, APIC can use Tags as a match parameter for USEG. Starting in Version 3.2, APIC can use Folders as a match parameter for USEG.
- Inventory can fail if **there is a large number of tags or folders**.

Supported Numbers:

VC Version	# of Tags
6.0	500
6.5	1000



APIC Inventory Synchronization

Common Failure Scenarios

Unable to Retrieve Tag or Folder Inventory

Fix – 3.2(7)+



1

Tagging can be toggled on VMM Domain



2

Folder Collection can be toggled on VMM Domain



3

Folder Collection Optimizations available in 4.2

Properties

Name: CiscoLive

Virtual Switch: Distributed Switch

Associated Attachable Entity

Profiles: **Name**

jr-aep

Encapsulation: vlan

Delimiter:

Enable Tag Collection: ☐

Enable VM Folder Data Retrieval: ☐

Access Mode: **Read Only Mode** **Read Write Mode**

Endpoint Retention Time (seconds): 0

VLAN Pool: jr-dynamic-pool(dynan)

*Virtual Networking > VMM Domains >
VMWare > Policy*

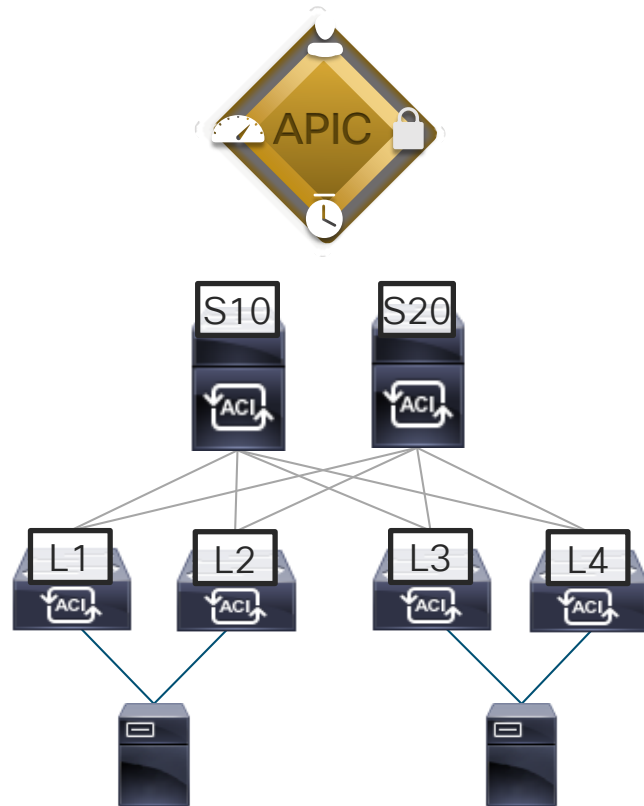
```
admin@apic1:~> moquery -c compCtrlr -f "comp.Ctrlr.domName=="CiscoLive\" | egrep "Tag|Folder"
enableTag          : no
enableVmFolder     : no
vsphereTag         : yes
```

Host Discovery

Host Discovery

Why is it needed?

- APIC Will learn the location of the hosts via LLDP or CDP Adjacency
- This information is used to **push policy dynamically** to the leafs as resources attach
- **Saves TCAM and VLAN port count** when resources are not needed.
- If Adjacency is missing, Dynamic Policy will not be pushed



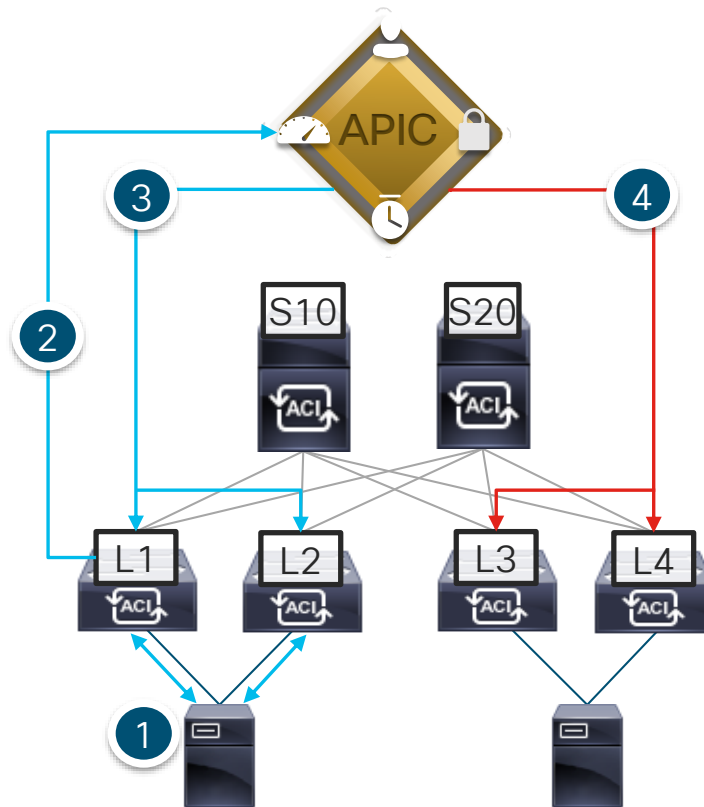
Host Discovery

How Do We Think it Works?

Maybe??



1. LLDP or CDP is exchanged between Hosts and Leaf switches?
2. Leafs tell APIC the ports in which hosts are connected as long as traffic is received?
3. APIC pushes Policy to Leaf/Port?
4. If LLDP or CDP stops, APIC can remove policy?

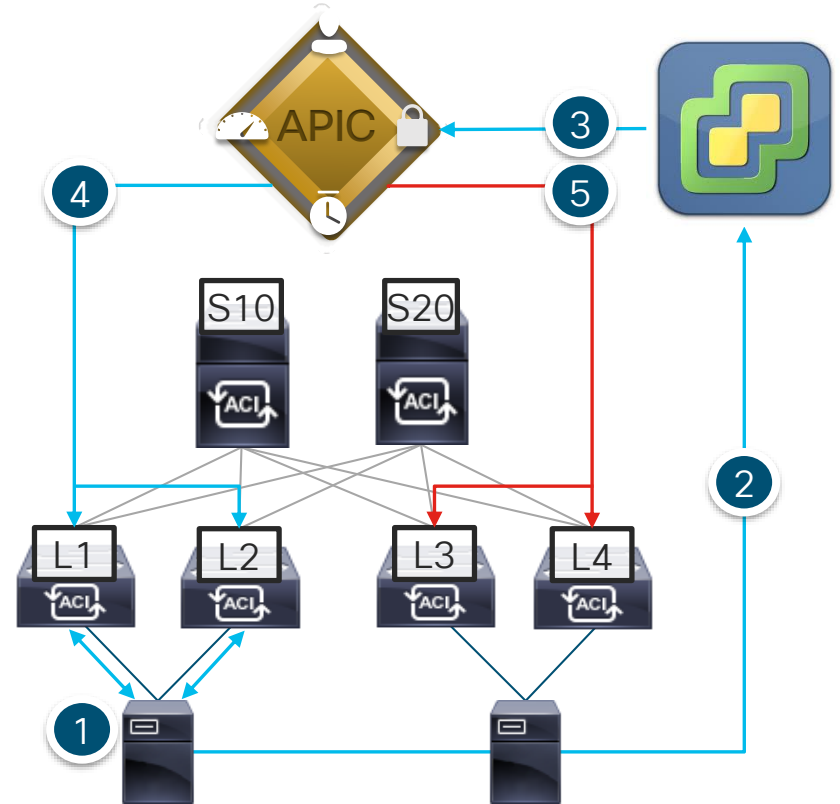


Host Discovery

How it Actually Works!



1. LLDP or CDP is exchanged between Hosts and Leaf switches
2. Hosts Report Adjacency Info to VC
3. vCenter Notifies APIC of Adjacency Info
4. APIC pushed Policy to Leaf/Port
5. If vCenter Adjacency info is lost, APIC can remove policy



Host Discovery

Troubleshooting - Faults

- APIC knows about Host via Inventory Sync
- If Adjacency is missing, a **Fault will be raised**

Virtual Networking > VMM Domains > VMWare > Policy > Faults

Fault Properties

General Troubleshooting History

Fault Code: F606391
Severity: major
Last Transition: 2019-02-23T12:03:37.685-05:00

Lifecycle: Raised

Affected Object: **comp/prov-VMware/ctrlr-[CiscoLive]-VC-6.5/hv-host-36**

Description: Fault delegate: [FSM:FAILED]: Get LLDP/CDP adjacency information for the physical adapters on the host: 192.168.2.22(TASK:ifc:vmmmgr:CompHvGetHpNicAdj)

Type: Config
Cause: fsm-failed
Change Set:

Lifecycle: Raised

Affected Object: **comp/prov-VMware/ctrlr-[CiscoLive]-VC-6.5/hv-host-36**

Description: Fault delegate: [FSM:FAILED]: Get LLDP/CDP adjacency information for the physical adapters on the host: 192.168.2.22(TASK:ifc:vmmmgr:CompHvGetHpNicAdj)

Host Discovery

Troubleshooting – VC Config

Discovery Protocol Mismatch

- vCenter Can only operate in **one** discovery mode: **LLDP or CDP**
- vCenter Setting **Needs to Match** what is being sent by Leaf



Networking > vDS > Configure



The screenshot shows the 'Configure' page for a vDS in the Cisco vCenter. The left sidebar has a 'Settings' section with 'Properties' selected. The main area shows the 'Properties' section with a 'Discovery protocol' tab selected. The 'Discovery protocol' section shows 'Type: Cisco Discovery Protocol' and 'Operation: Both'. A red box highlights this section, and a blue arrow points to it from the right.

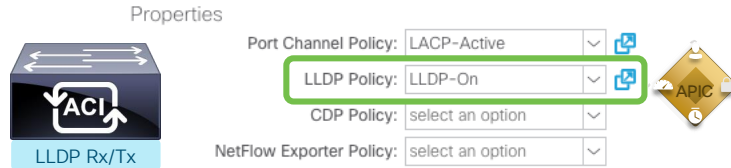
Properties	
General	
Name:	CiscoLive
Manufacturer:	VMware, Inc.
Version:	6.5.0
Number of uplinks:	8
Number of ports:	8
Network I/O Control:	Disabled
Description:	
APIC Virtual Switch	
Advanced	
MTU:	9000 Bytes
Multicast filtering mode:	Basic
Discovery protocol	
Type:	Cisco Discovery Protocol
Operation:	Both
Administrator contact	
Name:	
Other details:	

Host Discovery

Troubleshooting – VC Config

Fix Discovery Protocol Mismatch!

- APIC can push vDS Global config to VC to **ensure consistency**
- This includes Discovery Protocol, Port-Channel Config, Netflow, etc
- Done via “Vswitch Policy”
LLDP Takes Precedence over CDP



Networking > vDS > Configure



The screenshot shows the 'Configure' tab of the vDS configuration page. The left sidebar lists various settings, with 'Properties' selected. The main panel displays the 'Properties' section, which includes 'General', 'Description', 'Advanced', and 'Discovery protocol' sections. The 'Discovery protocol' section is highlighted with a green box and contains the following information:

Discovery protocol	
Type:	Link Layer Discovery Protocol
Operation:	Both

A blue arrow points from the 'APIC' icon in the diagram to this 'Discovery protocol' section.

Virtual Networking > VMM Domains > VMWare > Policy > Vswitch Policy

cisco Live!

Host Discovery

General Troubleshooting

1

Check ACI Access Policies

*Fabric > Access Policies >
Interface Policies*

Associate Policy to Interface
Policy Group



Properties

Name: LLDP-On

Description: optional

Alias:

Receive State: Disabled

Enabled

Transmit State: Disabled

Enabled

2

Check Host Adjacency Info

Host > Configure > Physical Adapters



Device	Actual Speed	Configured Speed
Intel Corporation I350 Gigabit Network Connection		
vmnic0	1000 Mb	1000 Mb
vmnic1	Down	Auto negotiate
Cisco Systems Inc Cisco VIC Ethernet NIC		
vmnic2	10000 Mb	10000 Mb
vmnic3	10000 Mb	10000 Mb

Physical network adapter: vmnic2

Link Layer Discovery Protocol

Property	Value
Chassis ID	00:2a:10:0e:20:75
Port ID	Eth1/33
Time to live	113
TimeOut	30
Samples	10231
Management Address	192.168.4.12
Port Description	topology/pod-1/protpaths-101-102/pathep-[jr-ucsc1-vpc]
System Description	topology/pod-1/node-101
System Name	fab3-leaf101

Peer device capability

Capability	Value
Router	Enabled
Transparent bridge	Enabled
Source route bridge	Disabled
Network switch	Disabled
Host	Disabled
IGMP	Disabled
Repeater	Disabled

00:2a:10:0e:20:75

Eth1/33

113

30

10231

192.168.4.12

topology/pod-1/protpaths-101-102/pathep-[jr-ucsc1-vpc]

topology/pod-1/node-101

fab3-leaf101

Host Discovery

General Troubleshooting

3

Verify Adjacency in APIC
*Virtual Networking > VMM Domains
> VMWare > Policy > Controller >
Hypervisor > General*



Hypervisor - 192.168.2.22

Topology **General** Stats Faults History

Properties

Name: 192.168.2.22
Type: Hypervisor Host
Status: Powered On

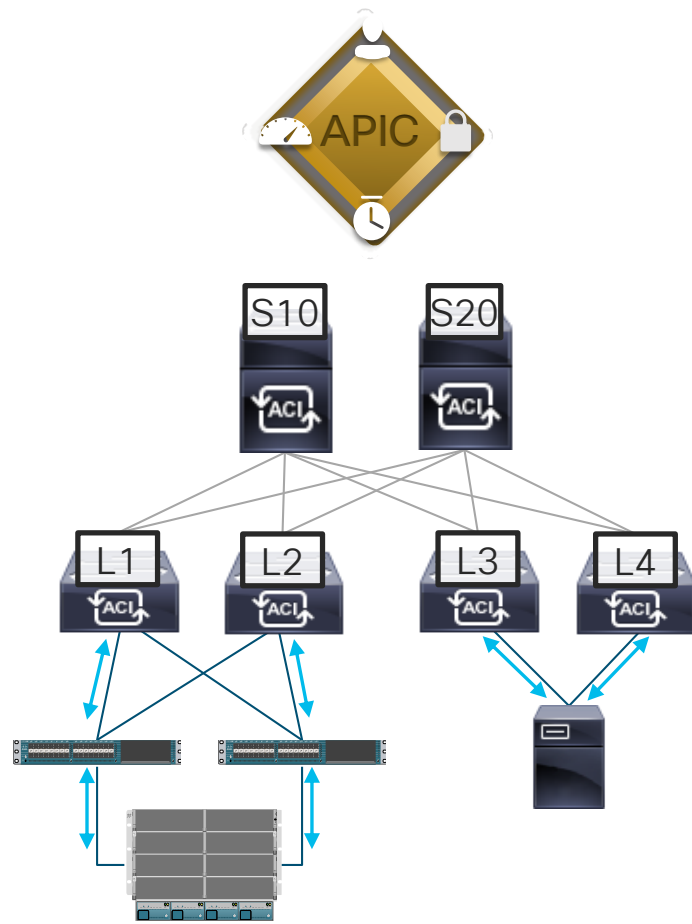
Hypervisor NICs

Name	MAC	State	Faults	Link Speed	Duplex Mode	Neighbor
vmnic0	E8:65:49:9E...	Up	0 0 0 0	1000 Mb	True	
vmnic1	E8:65:49:9E...	Down	0 0 0 0	unknown	Unknown	
vmnic2	78:BA:F9:E...	Up	0 0 0 0	10000 Mb	True	Eth1/33
vmnic3	78:BA:F9:E...	Up	0 0 0 0	10000 Mb	True	Eth1/33

Host Discovery

What About Blade Switches?

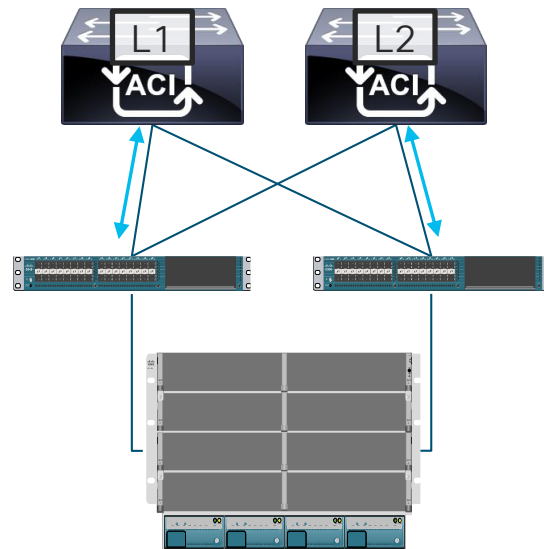
- Blade Switches may be an LLDP or CDP termination point
- Leaf switches may see LLDP or CDP from Blade Switch and not actual host
- APIC will get Host LLDP or CDP Info from VC but it will show **Blade Switch Adjacency**
- APIC needs a way to “**stitch**” the connection between **Blade Switch** and **End Host** so it can deploy Config to Blade Switch Ports



Host Discovery

Blade Switch = Unmanaged Fabric Node

- **Unmanaged Fabric Nodes(UFN)** are Discovered and Created Dynamically via LLDP or CDP
- Classname is called **"fabricLooseNode"**
- If UFN is not seen in APIC, Dynamic Policy cannot be pushed!



Fabric > Inventory > Fabric Membership > Unmanaged Fabric Nodes



Registered Nodes Nodes Pending Registration Unreachable Nodes **Unmanaged Fabric Nodes**

! These nodes, known as loose nodes, are externally connected. For example, a blade switch connected to a leaf node.

ID	System Name	System Description
192.168.2.46	UCS-A	Cisco Nexus Operating System (NX-...)
192.168.2.47	UCS-B	Cisco Nexus Operating System (NX-...)

```
admin@apic1:~> moquery -c fabricLooseNode | egrep "id|dn|sysName"
id      : 192.168.2.46
dn      : topology/lnode-192.168.2.46
sysName : UCS-A
id      : 192.168.2.47
dn      : topology/lnode-192.168.2.47
sysName : UCS-B
```

Host Discovery

Blade Switch Troubleshooting

1

Check Host Adjacency Info

Host > Configure > Physical Adapters



192.168.2.170

Getting Started Summary Monitor

Configure Permissions VMs Datastores

Physical adapters

Device	Actual Speed	Configured Speed
Cisco Systems Inc Cisco VIC Ethernet NIC		
vmnic0	20000 Mb	20000 Mb
vmnic1	20000 Mb	20000 Mb
vmnic2	20000 Mb	20000 Mb
vmnic3	20000 Mb	20000 Mb

Physical network adapter: vmnic2

All Properties CDP LLDP

Link Layer Discovery Protocol

Chassis ID	8c:60:4f:6d:f6:7c
Port ID	Veth1348
Time to live	117
TimeOut	30
Samples	75
Management Address	192.168.2.46
Port Description	Vethernet1348
System Description	unknown
System Name	UCS-A
Vlan ID	1

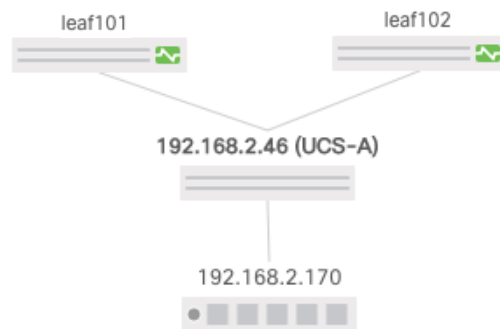
Peer device capability

Router	Disabled
Transparent bridge	Enabled
Source route bridge	Disabled
Network switch	Disabled
Host	Disabled
IGMP	Disabled
Repeater	Disabled

2

Double Click Unmanaged Fabric Node

Ensure Topology is Built to Host!



cisco *Live!*

Fabric > Inventory > Fabric Membership > Unmanaged Fabric Nodes

Host Discovery

Blade Switch Common Issues

1

CDP/LLDP Not Enabled

CDP/LLDP Must be sent from Blade Switch to Leafs and Downlink Hosts

For UCS, this is done via network Control Policy on vNIC

2

Changing MGMT IP Breaks Connectivity

VC will see new MGMT IP in Adjacency, but will not update APIC

Trigger Manual Inventory Sync to Fix

3

VMM VLANS Not Added to Blade Switch

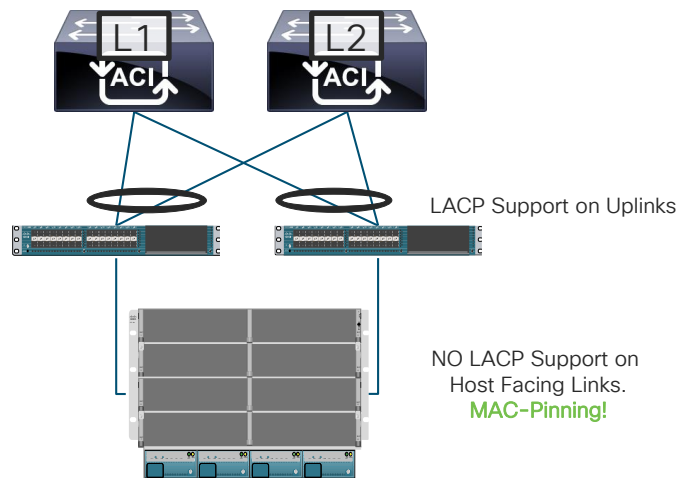
APIC Cannot Program Third Party Blade Switch. UCSM Integration available in 4.1(1) release.

VLANs must be configured and trunked to uplinks/hosts

4

Intermittent Traffic Loss

*Traffic loss seen with IP Hash Load Balancing
UCSB FI's cannot run LACP and form a vPC down to the blades. Route based on originating virtual port/Physical NIC load must be used (MAC-Pinning ACI vSwitch Policy).*



Host Discovery

Troubleshooting – LLDP/CDP Traffic on Leaf

1

Check LLDP on Interface



```
leaf101# show lldp interface ethernet 1/33
Interface Information:
Enable (tx/rx/dcbx): Y/Y/N Port Mac address: 00:2a:10:0e:20:75
```

2

Check Counters on Interface

```
leaf101# show lldp traffic interface ethernet 1/33
LLDP interface traffic statistics:
```

```
Total frames transmitted: 2887
Total entries aged: 0
Total frames received: 2887
Total frames received in error: 0
Total frames discarded: 0
Total unrecognized TLVs: 0
```

1

Check CDP on Interface



```
leaf101# show cdp interface ethernet 1/33
Ethernet1/33 is
  CDP enabled on interface
  Refresh time is 60 seconds
  Hold time is 180 seconds
```

2

Check Counters on Interface

```
leaf101# show cdp traffic interface ethernet 1/33
```

```
-----
Traffic statistics for Ethernet1/33
```

```
Input Statistics:
```

```
Total Packets: 100
```

```
...
```

```
Output Statistics:
```

```
Total Packets: 100
```

```
...
```

Host Discovery

Troubleshooting – LLDP/CDP Traffic on Host

1 Check LLDP Receive on Interface



LLDP Rx/Tx

```
[root@esx1:~] pktcap-uw --uplink vmnic2 --ethtype 0x88cc
16:02:08.816915[1] Captured at EtherswitchDispath point, TSO not
enabled, Checksum not offloaded and not verified, length 352.
Segment[0] ---- 9018 bytes:
0x0000: 0180 c200 000e 002a 100e 2075 88cc 0207
0x0010: 0400 2a10 0e20 7504 0807 4574 6831 2f33
...
```

2 Check LLDP Transmit on Interface

```
[root@esx1:~] pktcap-uw --uplink vmnic2 --ethtype 0x88cc --dir 1
16:02:08.816915[1] Captured at EtherswitchDispath point, TSO not
enabled, Checksum not offloaded and not verified, length 352.
Segment[0] ---- 140 bytes:
0x0000: 0180 c200 000e 0050 5657 a0c3 88cc 0207
0x0010: 0676 6d6e 6963 3204 0703 0050 5657 a0c3
...
```

1 Check CDP Receive on Interface



CDP Rx/Tx

```
[root@esx1:~] pktcap-uw --uplink vmnic2 --ethtype 0x2000
16:02:08.816915[1] Captured at EtherswitchDispath point, TSO not
enabled, Checksum not offloaded and not verified, length 352.
Segment[0] ---- 9018 bytes:
0x0000: 0100 0ccc cccc 002a 100e 2075 0123 aaaa
0x0010: 0300 000c 2000 02b4 a86d 0001 001d 6661
...
```

2 Check CDP Transmit on Interface

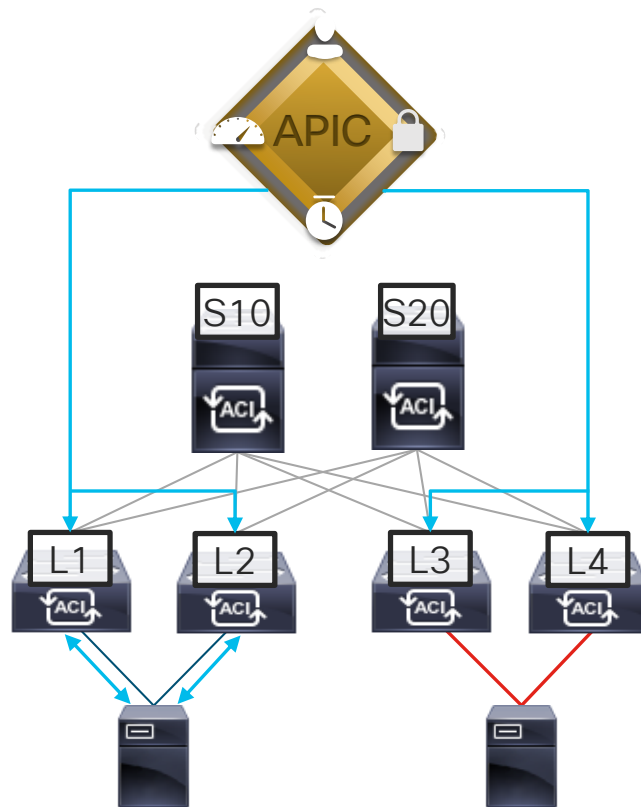
```
[root@esx1:~] pktcap-uw --uplink vmnic2 --ethtype 0x2000 --dir 1
16:02:08.816915[1] Captured at EtherswitchDispath point, TSO not
enabled, Checksum not offloaded and not verified, length 352.
Segment[0] ---- 169 bytes:
0x0000: 0100 0ccc cccc 0050 5657 a0c3 009b aaaa
0x0010: 0300 000c 2000 02b4 3047 0001 0015 6a72
...
```

Policy Download and Verification

Policy Download and Verification

When is Policy Pushed?

- APIC Provides Flexibility in deciding where/when to push/pull VLANs and Contracts to the Leafs
- Behavior is defined when the VMM Domain is mapped to the EPG via the **Resolution and Deployment Immediacy**
- Behavior is per EPG and not Global to VMM Domain



Policy Download and Verification

When is Policy Pushed?

Resolution Immediacy

- Determines when Contracts/VLANs should be Downloaded to the Leafs

On-Demand

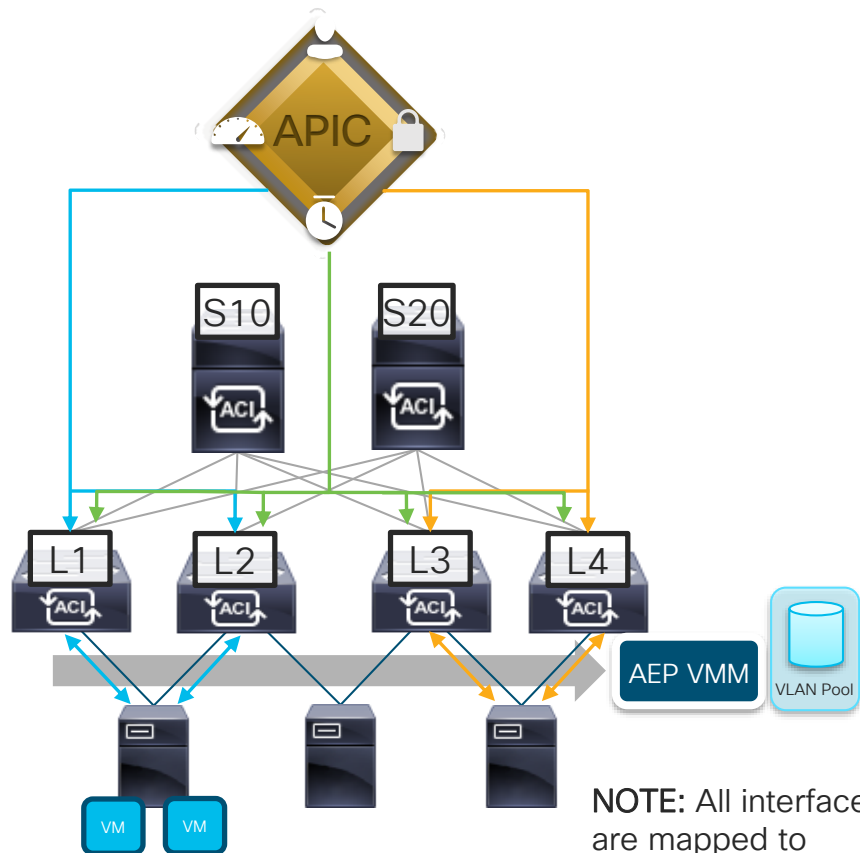
- Policy is pushed when a **VM is added to the Port-Group**, and the VM is on a host with a **valid LLDP/CDP Adjacency**

Immediate

- Policy is pushed when LLDP/CDP adjacency is detected from Host

Pre-Provision

- Policy is pushed to all ports/leafs tied to the AEP independent of Adjacency



NOTE: All interfaces are mapped to correct AEP!

Policy Download and Verification

When is Policy Pushed?

Deployment Immediacy

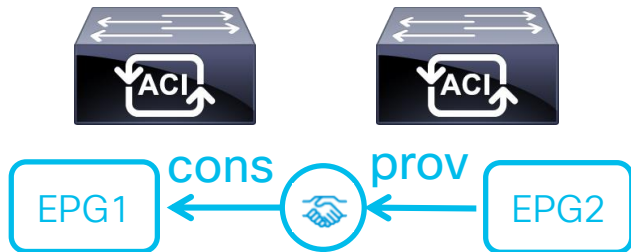
- Determines when Contracts Are Installed in Leaf TCAM

On-Demand

- Contract is installed when first packet is received by VM.

Immediate

- Contract is installed when policy is first downloaded to leaf.



Policy Download and Verification

Pre-Provision Use Cases

1 Management VMK Ports

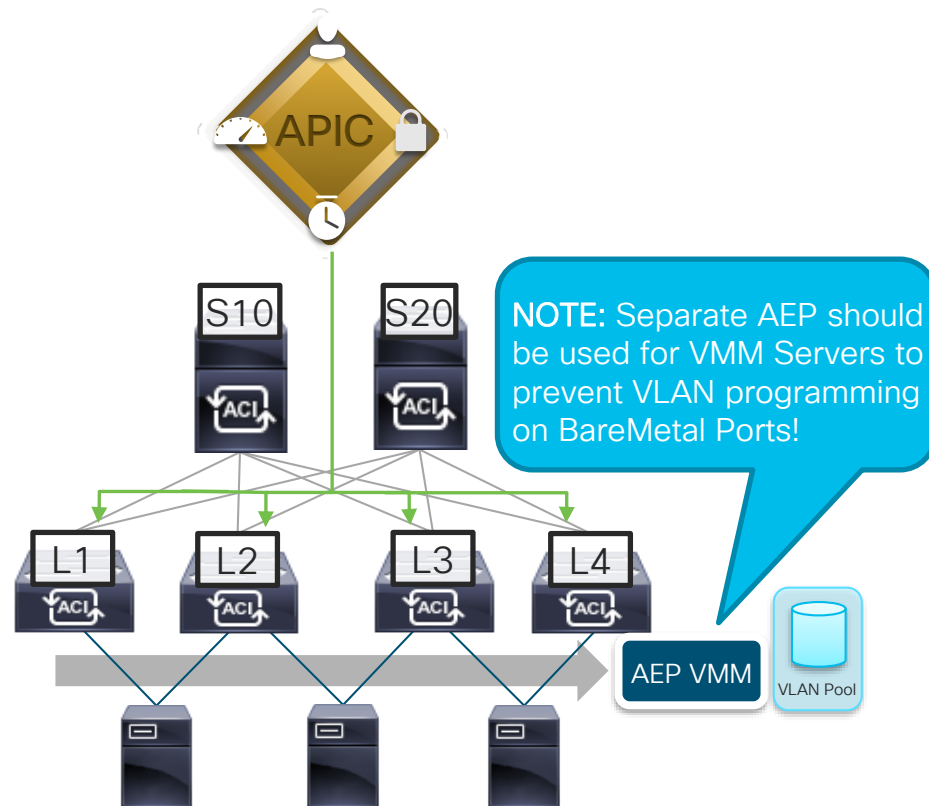
If Host management is on APIC vDS, networking needs to be in place statically so host can talk to VC. Otherwise APIC can't learn about adjacency to push the management policy. (Chicken and the Egg)

2 Maintenance

During maintenance, where links or adjacencies may flap, pre-provision can improve convergence since policy is always present on port

3 Troubleshooting

If Dynamic Policy is not working, you can enable pre-provision to see if policy is pushed. From there you can troubleshoot Dynamic Policy Download.



Policy Download and Verification

On Demand Troubleshooting

- Learning Source flagged as “**learned**” means VM has sent data to leaf.
- **Deployment Immediacy** On Demand is pushed when VM is marked as “learned”.

Tenants > Tenant > App Profile > EPG > Operational > Client End-Points

What if Endpoint doesn't have “learned” flag?

- 1 Check Faults on VMM Domain
- 2 Check Faults on EPG
- 3 Ensure VM is sending Traffic
- 4 VLAN are configured on Blade Switch (if applicable)

cisco *Live!*

EPG - Webserver

EPG - Webserver									
Summary Policy Operational Stats Health Faults History									
Client End-Points Configured Access Policies Contracts Controller End-Points Learned End-Points									
100 [Icons] [Refresh] [Download]									
End Point	MAC	IP	Learning Source	Hosting Server	Reporting Controller Name	Interface	Multi-cast Address	Encap	
Webserver-1	00:50:56:82:51:74	---	learned vmm	192.168.2.22	VC-6.5	Pod-1/Node-101-102/...	---	vlan-2038	
Pod-1/Node-101-102/jr-ucsc1-vpc (learned,vmm)									

Policy Download and Verification

On Demand Troubleshooting

- Learning Source flagged as “vmm” means VC notified APIC that VM has been placed in Port Group and Host where VM lives has a valid LLDP/CDP Adjacency
- Resolution Immediacy is pushed to leafs when VM is marked as “vmm” learned.

What if Endpoint doesn't have “vmm” flag?

- 1 Check Faults on VMM Domain
- 2 Check Faults on EPG
- 3 Check VNIC on VM for correct Port Group Mapping

cisco *Live!*

Tenants > Tenant > App Profile > EPG > Operational > Client End-Points

EPG - Webserver

Summary Policy **Operational** Stats Health Faults History

Client End-Points Configured Access Policies Contracts Controller End-Points Learned End-Points

End Point	MAC	IP	Learning Source	Hosting Server	Reporting Controller Name	Interface	Multi-Encap Address
Webserver-1	00:50:56:82:51:74	---	vmm	192.168.2.22	VC-6.5	Pod-1/Node-101-102/...	---

Pod-1/Node-101-102/jr-ucsc1-vpc (vmm)

Policy Download and Verification

On Demand Path Deployment

- VMM Learn in **EPG** triggers “Dynamic Path”: **fvDyPathAtt** Object pushed to **leaf** where Host attaches.
- **VLAN** is mapped to **interfaces** using connection object: **fvIfConn**
- **If Object is Missing**: Ensure EP is learnt as “vmm” in **EPG** and Adjacency is seen in APIC!

```
admin@apic1:~> moquery -c fvDyPathAtt | grep Webserver
```

```
dn : uni/epg/fv-[uni/tn-CiscoLive/ap-CiscoLive/epg-Webserver]/node-101/dyatt-[topology/pod-1/protpaths-101-102/pathep-[jr-ucsc1-vpc]]
```

```
dn : uni/epg/fv-[uni/tn-CiscoLive/ap-CiscoLive/epg-Webserver]/node-102/dyatt-[topology/pod-1/protpaths-101-102/pathep-[jr-ucsc1-vpc]]
```



```
admin@apic1:~> moquery -c fvIfConn | grep Webserver
```

```
dn: uni/epg/fv-[uni/tn-CiscoLive/ap-CiscoLive/epg-Webserver]/node-101/dyatt-[topology/pod-1/protpaths-101-102/pathep-[jr-ucsc1-vpc]]/conndef/conn-[vlan-2038]
```

```
dn: uni/epg/fv-[uni/tn-CiscoLive/ap-CiscoLive/epg-Webserver]/node-102/dyatt-[topology/pod-1/protpaths-101-102/pathep-[jr-ucsc1-vpc]]/conndef/conn-[vlan-2038]
```



Policy Download and Verification

Path Deployment – UI Verification

The screenshot displays the Cisco APIC (Application Policy Infrastructure Controller) web interface. The top navigation bar includes the Cisco logo, the text 'APIC', and a user profile 'admin' with search, notifications, and settings icons. Below this is a secondary navigation bar with tabs: System, Tenants (selected), Fabric, Virtual Networking, L4-L7 Services, Admin, Operations, Apps, and Integrations. The 'Tenants' tab is active, showing a search bar and filters for 'ALL TENANTS', 'Add Tenant', and 'Tenant Search: name or descr'. The left sidebar shows a tree view under 'CiscoLive' with categories like 'Quick Start', 'CiscoLive', 'Application Profiles', 'CiscoLive', 'Application EPGs', 'Appserver', 'Webserver', 'Domains (VMs and Bare-Metals)', 'EPG Members', 'Static EPG Members', 'Dynamic EPG Members' (highlighted), 'Static Ports', 'Static Leafs', 'Fibre Channel (Paths)', 'Contracts', 'Static Endpoint', 'Subnets', 'L4-L7 Virtual IPs', and 'L4-L7 IP Address Pool'. The main content area shows the 'Dynamic EPG Members' page with a table listing members: 'node-101-[jr-ucsc1-vpc]-[vlan-2038]' and 'node-102-[jr-ucsc1-vpc]-[vlan-2038]'. A blue callout box highlights the 'Dynamic EPG Members' section, showing a zoomed-in view of the table content.

Dynamic EPG Members

Dynamic Epg Members
node-101-[jr-ucsc1-vpc]-[vlan-2038]
node-102-[jr-ucsc1-vpc]-[vlan-2038]

Policy Download and Verification

Immediate Path Deployment

- Same Validation as On Demand, But **fvDyPathAtt** is pushed to all leafs/ports with Valid Adjacency.
- For Blade Switch, fvDyPathAtt is associated to fabricLooseNode
- **If Object is Missing:** Ensure Adjacency is seen in APIC!

```
admin@apic1:~> moquery -c fvDyPathAtt | grep Webserver
```

```
dn : uni/epp/fv-[uni/tn-CiscoLive/ap-CiscoLive/epg-Webserver]/node-101/dyatt-[topology/pod-1/node-101/sys/lsnode-192.168.2.46]
dn : uni/epp/fv-[uni/tn-CiscoLive/ap-CiscoLive/epg-Webserver]/node-102/dyatt-[topology/pod-1/node-102/sys/lsnode-192.168.2.46]
dn : uni/epp/fv-[uni/tn-CiscoLive/ap-CiscoLive/epg-Webserver]/node-101/dyatt-[topology/pod-1/node-101/sys/lsnode-192.168.2.47]
dn : uni/epp/fv-[uni/tn-CiscoLive/ap-CiscoLive/epg-Webserver]/node-102/dyatt-[topology/pod-1/node-102/sys/lsnode-192.168.2.47]
dn : uni/epp/fv-[uni/tn-CiscoLive/ap-CiscoLive/epg-Webserver]/node-101/dyatt-[topology/pod-1/protpaths-101-102/pathep-[jr-ucsc1-vpc]]
dn : uni/epp/fv-[uni/tn-CiscoLive/ap-CiscoLive/epg-Webserver]/node-102/dyatt-[topology/pod-1/protpaths-101-102/pathep-[jr-ucsc1-vpc]]
```



```
admin@apic1:~> moquery -c fvIfConn | grep Webserver
```

```
dn: uni/epp/fv-[uni/tn-CiscoLive/ap-CiscoLive/epg-Webserver]/node-101/dyatt-[topology/pod-1/node-101/sys/lsnode-192.168.2.46]/conndef/conn-[vlan-2038]
dn: uni/epp/fv-[uni/tn-CiscoLive/ap-CiscoLive/epg-Webserver]/node-102/dyatt-[topology/pod-1/node-102/sys/lsnode-192.168.2.46]/conndef/conn-[vlan-2038]
dn: uni/epp/fv-[uni/tn-CiscoLive/ap-CiscoLive/epg-Webserver]/node-101/dyatt-[topology/pod-1/node-101/sys/lsnode-192.168.2.47]/conndef/conn-[vlan-2038]
dn: uni/epp/fv-[uni/tn-CiscoLive/ap-CiscoLive/epg-Webserver]/node-102/dyatt-[topology/pod-1/node-102/sys/lsnode-192.168.2.47]/conndef/conn-[vlan-2038]
dn: uni/epp/fv-[uni/tn-CiscoLive/ap-CiscoLive/epg-Webserver]/node-101/dyatt-[topology/pod-1/protpaths-101-102/pathep-[jr-ucsc1-vpc]]/conndef/conn-[vlan-2038]
dn: uni/epp/fv-[uni/tn-CiscoLive/ap-CiscoLive/epg-Webserver]/node-102/dyatt-[topology/pod-1/protpaths-101-102/pathep-[jr-ucsc1-vpc]]/conndef/conn-[vlan-2038]
```

Policy Download and Verification

Pre-Provision Path Deployment

- Pre-Provision is the same as pushing static path, but to every leaf/interface tied to AEP
- Path and VLAN Deployment get pushed using fvAttEntityPathAtt Object
- If Object is Missing: Ensure Interface is tied to AEP for VMM Domain

```
admin@apic1:~> moquery -c fvAttEntityPathAtt | grep Webserver
dn: uni/epp/fv-[uni/tn-CiscoLive/ap-CiscoLive/epg-Webserver]/node-101/attEntitypathatt-[CiscoLive]
dn: uni/epp/fv-[uni/tn-CiscoLive/ap-CiscoLive/epg-Webserver]/node-102/attEntitypathatt-[CiscoLive]
```

```
admin@apic1:~> moquery -c fvRsStPathAtt | grep Webserver
dn: uni/epp/fv-[uni/tn-CiscoLive/ap-CiscoLive/epg-Webserver]/node-101/attEntitypathatt-[CiscoLive]/rsstPathAtt-[sys/conng/path-[po1]]
dn: uni/epp/fv-[uni/tn-CiscoLive/ap-CiscoLive/epg-Webserver]/node-101/attEntitypathatt-[CiscoLive]/rsstPathAtt-[sys/conng/path-[po2]]
dn: uni/epp/fv-[uni/tn-CiscoLive/ap-CiscoLive/epg-Webserver]/node-101/attEntitypathatt-[CiscoLive]/rsstPathAtt-[sys/conng/path-[po3]]
dn: uni/epp/fv-[uni/tn-CiscoLive/ap-CiscoLive/epg-Webserver]/node-102/attEntitypathatt-[CiscoLive]/rsstPathAtt-[sys/conng/path-[po1]]
dn: uni/epp/fv-[uni/tn-CiscoLive/ap-CiscoLive/epg-Webserver]/node-102/attEntitypathatt-[CiscoLive]/rsstPathAtt-[sys/conng/path-[po2]]
dn: uni/epp/fv-[uni/tn-CiscoLive/ap-CiscoLive/epg-Webserver]/node-102/attEntitypathatt-[CiscoLive]/rsstPathAtt-[sys/conng/path-[po3]]
```

```
admin@apic1:~> moquery -c fvIfConn | grep Webserver
dn: uni/epp/fv-[uni/tn-CiscoLive/ap-CiscoLive/epg-Webserver]/node-101/attEntitypathatt-[CiscoLive]/conndef/conn-[vlan-2038]
dn: uni/epp/fv-[uni/tn-CiscoLive/ap-CiscoLive/epg-Webserver]/node-102/attEntitypathatt-[CiscoLive]/conndef/conn-[vlan-2038]
```


Policy Download and Verification

When is Policy Removed?

Prior to Version 3.0

On-Demand

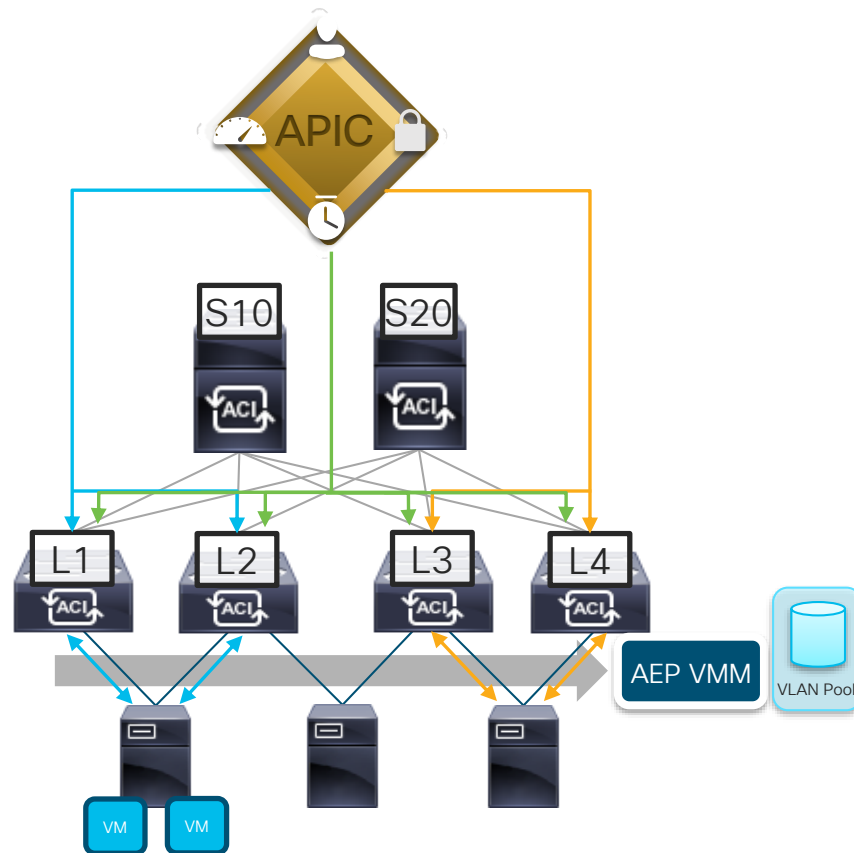
1. If No VM's exist in EPG
- OR
2. If interface is removed from AEP

Immediate

1. If LLDP/CDP is removed From Host
2. If interface is removed from AEP

Pre-Provision

1. If VMM Domain is Removed From EPG
2. If interface is removed from AEP



Policy Download and Verification

When is Policy Removed from Interface?

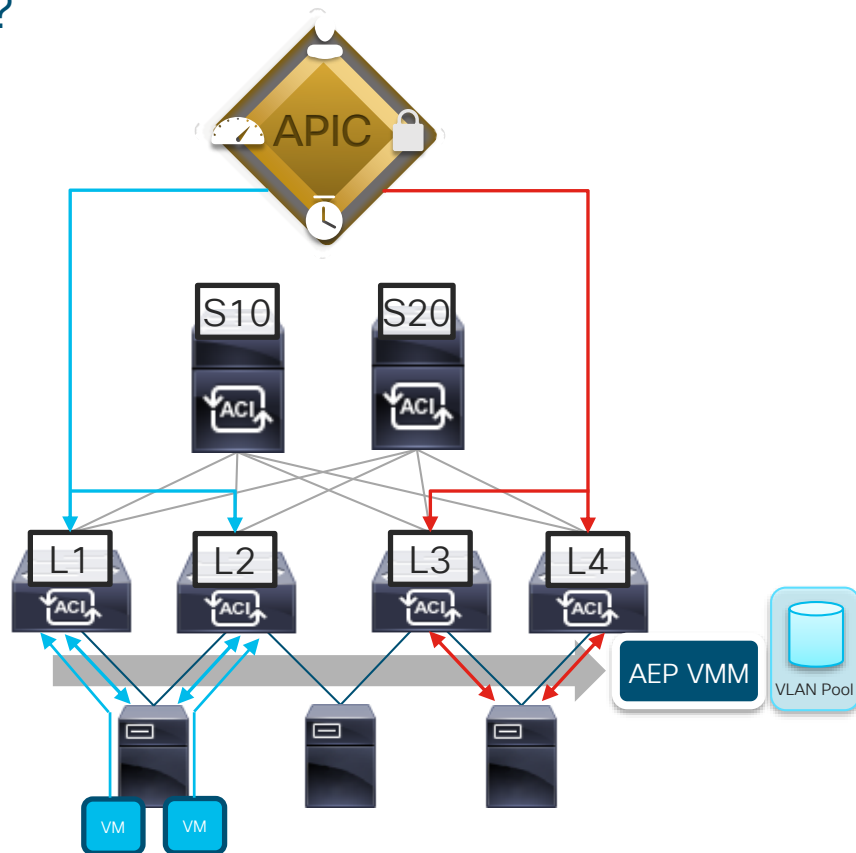
Version 3.0 and Higher

- On-Demand and Immediate
1. If No VM's exist in VMWare PortGroup
AND
LLDP/CDP goes away from host
AND
VM Traffic Stops and Ages Out

2. If Interface is Removed From AEP

Pre-Provision

1. Behavior is the same



Complete your online session survey



- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (starting on Thursday) to receive your Cisco Live t-shirt.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Content Catalog on ciscolive.com/emea.

Cisco Live sessions will be available for viewing on demand after the event at ciscolive.com.

Continue your education



Demos in the
Cisco campus



Walk-in labs



Meet the engineer
1:1 meetings



Related sessions



Thank you





You make **possible**