cisco
You make possible

Monitoring ACI

Providing a complete view of your fabric

Sadiq H. Memon
Lead Solutions Architect (Automotive) - Customer Delivery
@sadhussa

BRKACI-2271

cisco Live!
Barcelona | January 27-31, 2020

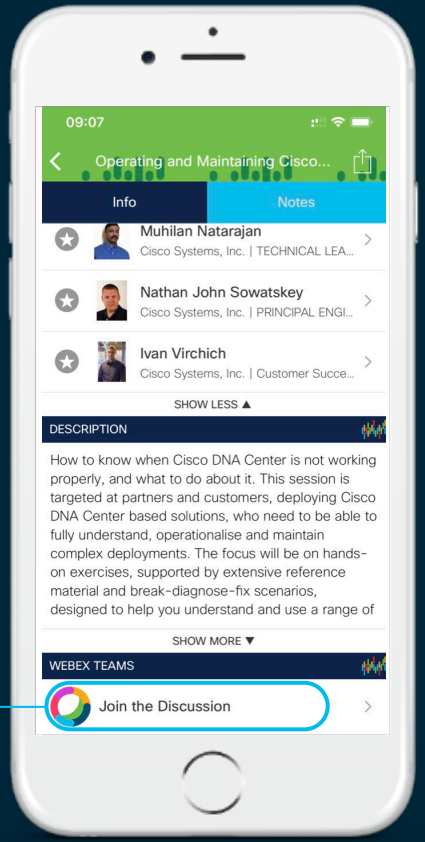
Cisco Webex Teams

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



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Agenda

- Importance of Monitoring
  - Proactive vs Reactive Approach
- Monitoring ACI
  - Faults & Health Score
- ACI Monitoring Built-in & Built-out Tools
  - Built-in Tools (SNMP, Syslog, SPAN, Netflow, REST)
  - Built-out Tools (TAP, NAE, Tetration, Splunk)
- How Proactive Monitoring Can Help During Troubleshooting?
- Conclusion

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Importance of Monitoring

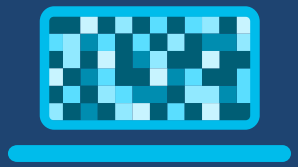
Top Consumer of IT Time: Troubleshooting (~43%)

4x

Network operators spend more time collecting data than analyzing while troubleshooting

Replication challenge

Troubleshooting an issue can be impossible if IT can't replicate the issue or see the issue as is it happening real time



Slow resolution

Downtime is expense; unplanned downtime cost Fortune 1000 $1.25-2.5B annually

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

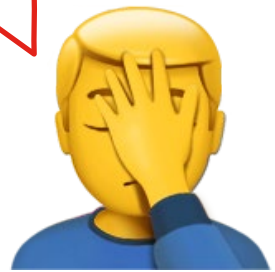
Problem: DC Paradigms Are Fundamentally Reactive

Intent Frequently Breaks …		We Always React …
Operational	→	Troubleshoot
Security	→	Scramble
Compliance	→	Fail audits
Change	→	Undo change

Leaving Us With …

An Inability to Assure Intent Proactively.

We are always in a reactive mode!



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Benefits of Monitoring

- Stay ahead of outages.
- Fix issues faster.
- Manage growing and changing networks.
- Identify security threats.
- Justify maintenance window.
- Achieve SLAs.
- Gain immediate ROI.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Monitoring ACI

Faults & Health Scores

Faults

- Faults in ACI are always in relationship to an object
- They are structured around the Management Information Tree
- Faults are visible only if they affect an object that is part of that objects tree.
- The lower the object in the tree, the more specific the faults are
- System Faults list all the faults in the ACI fabric

Fault Counts By Domain

☐ Hide Acked Faults ☐ Hide Delegated Faults

SYSTEM WIDE	**65**	**76**	**591**	**33**
Access	65	4	15	0
External	0	0	0	3
Framework	0	0	0	0
Infra	0	72	39	30
Management	0	0	8	0
Security	0	0	62	0
Tenant	0	0	467	0

Fault Counts By Type

☐ Hide Acked Faults ☐ Hide Delegated Faults

Communications	65	65	15	0
Config	0	2	482	23
Environmental	0	2	18	0
Operational	0	7	76	10

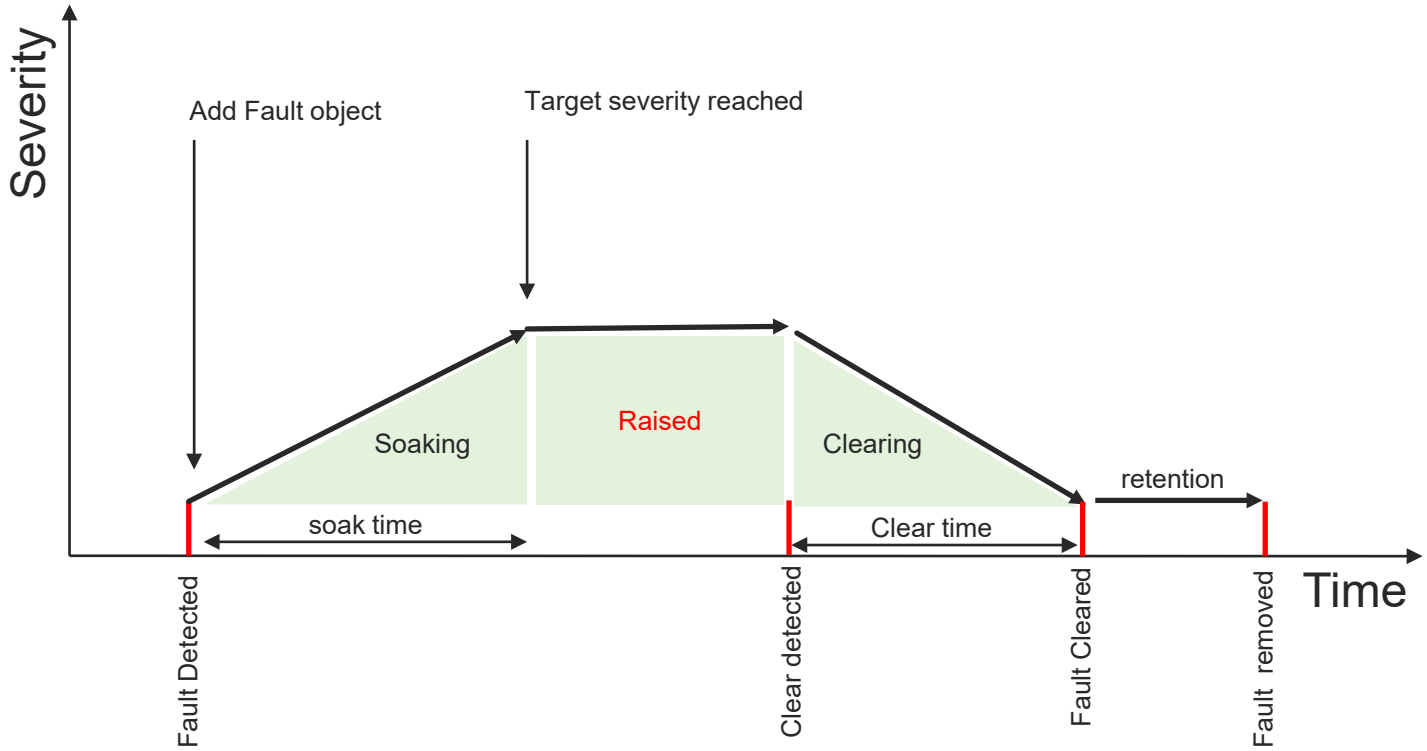
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Fault Triggers

- There are four type of fault triggers:
  - Fault Rules
  - Counters crossing thresholds
  - Task or state failures
  - Object resolution failures
- Faults are always raised on the node where the condition was detected (either a fabric node or controller)
- Users can’t define new faults

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

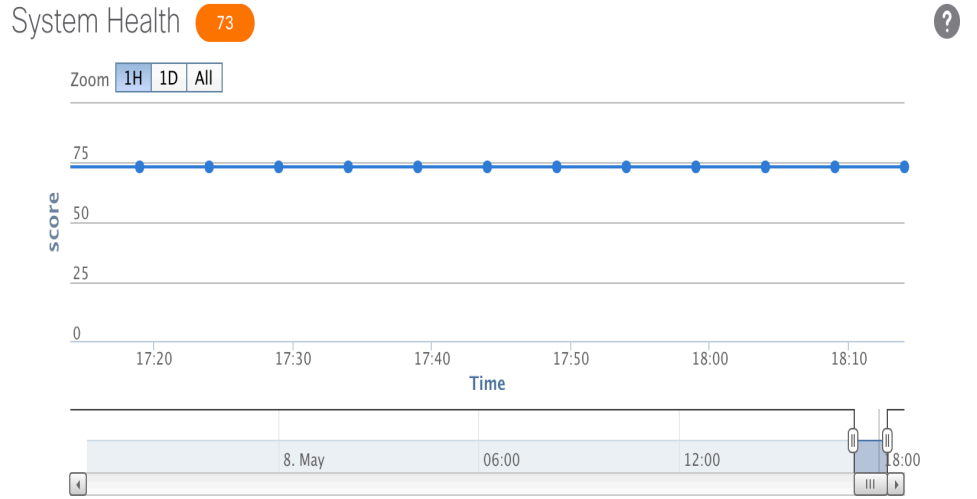
Fault Lifecycle



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Health Score

- Provides a quick overview of the health of the entire system/fabric
- A Fault will trigger a decrease in the health score of an object in the fabric & vice versa
- Computed based on the faults generated by objects in the fabric
- Range is from 0 to 100
- Policies can be used to tune how faults impact the overall health score



Nodes With Health ≤ 100 — 100

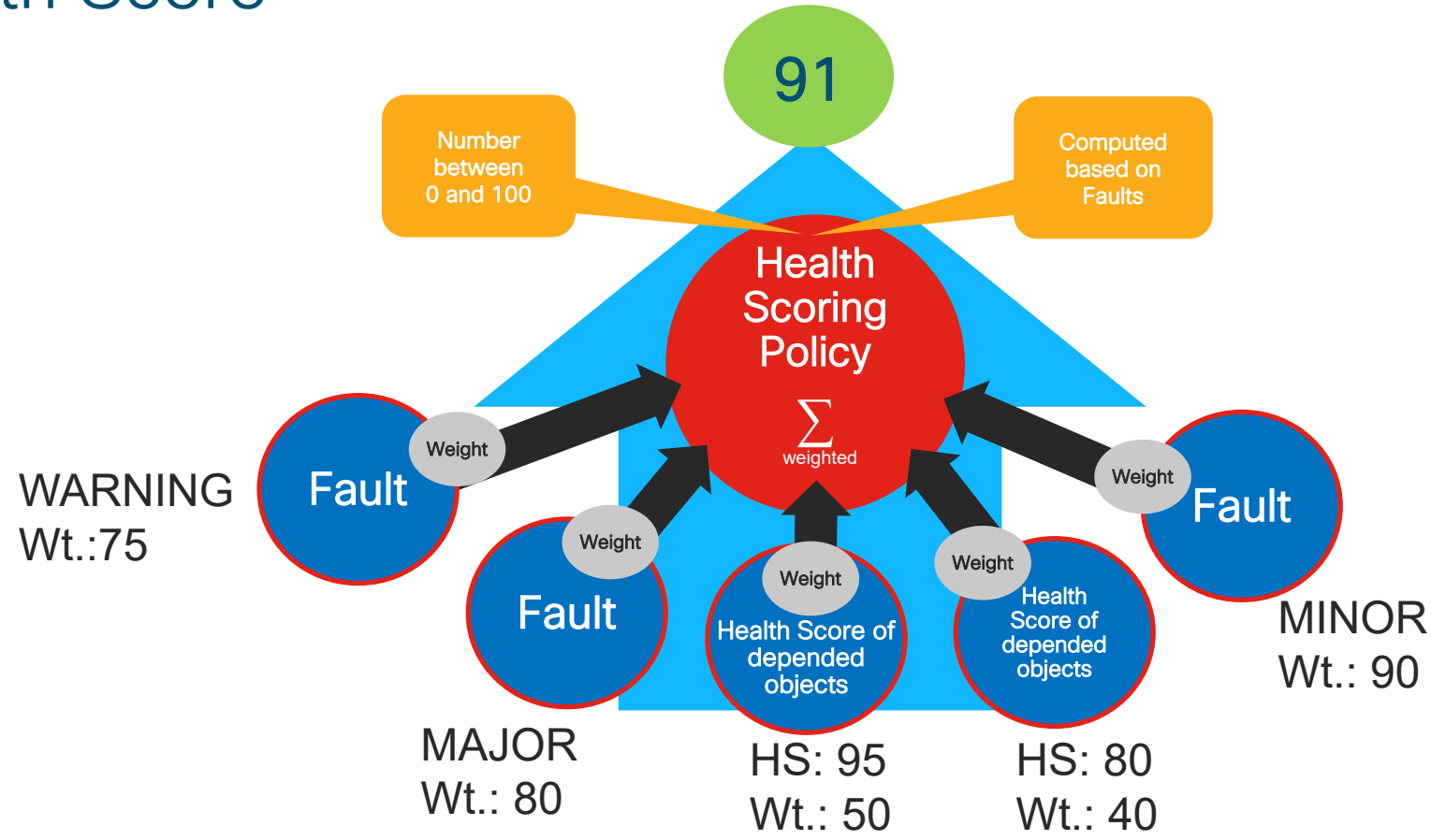
Name	Pod ID	Type	Health Score
tcsh1-f01-b0201	1	leaf	100
tcsh1-f01-b0202	1	leaf	100
tcsh1-f01-h1001	1	leaf	78
tcsh1-f01-h1002	1	leaf	78
tcsh1-f01-p3001	1	leaf	72

Tenants With Health ≤ 99 — 99

Name	Health Score
tO1	5

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Health Score



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ACI Monitoring

Built-in & Built-out Tools

solarwinds

AppDynamics

Cisco Tetration Analytics™

Gigamon

ScienceLogic

SevOne

What Tool to Pick ?

That gives you Piece of mind

cisco Live!

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ACI Built-in Tools

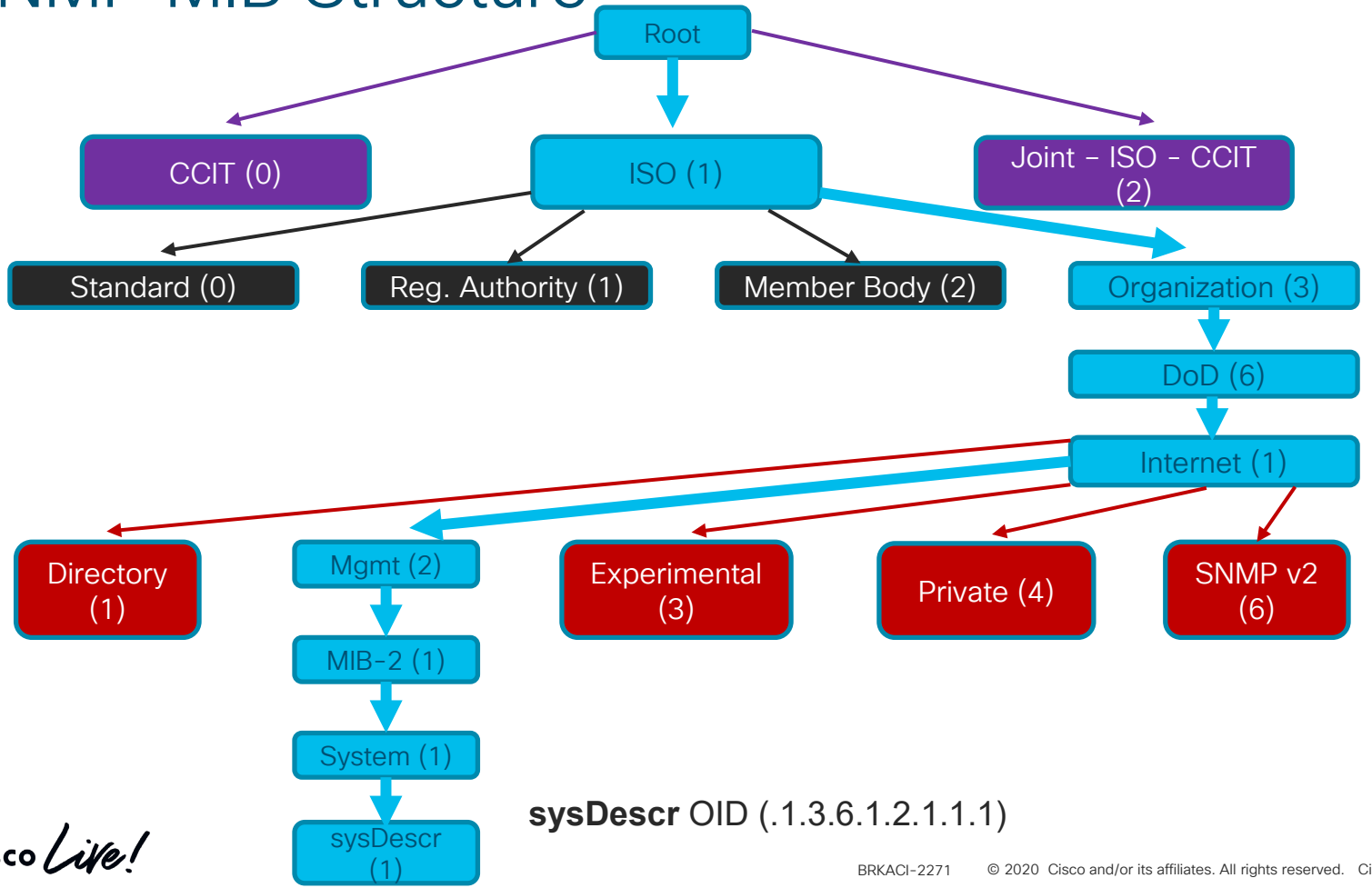
SNMP

SNMP Overview

- SNMP is Simple Network Management Protocol which is UDP based network protocol with port numbers 161 and 162
- It provides a mechanism for monitoring hardware devices
- Basic components are:
  - Managed Device: the hardware device to be monitored
  - Agent (SNMP software running on the Managed Device)
  - Network Management System: the monitoring system which has SNMP Client to communicate with the Agent running on the Managed Device
- SNMP is widely supported across several Cisco platforms
- The network parameter information shared between Managed Device and Management Station is called MIB

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

SNMP MIB Structure



sysDescr OID (.1.3.6.1.2.1.1.1)

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

SNMP Support in ACI

- SNMP is supported on both of the ACI hardware components:
  - Switches
  - APIC ← from release 1.2(1) and later
- The SNMP agents run independently on Switches and APIC and provide the monitoring information directly to the Management System.
- Following SNMP Features are supported:
  - SNMP Protocol Version 1, 2c and 3
  - SNMP Traps
- APIC supports a subset of MIBs in comparison to Switches
- Only SNMP Read Queries (Get, Next, Bulk, Walk) supported.
- SNMP Write commands are not supported.
- ACI supports a maximum of 10 Trap receivers.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

SNMP Support in ACI

- MIBs Supported
  - System
  - Cisco-IF-Extension-MIB
  - Entity-MIB
  - Cisco-Entity-FRU-Control-MIB
  - Cisco-Entity-Sensor-MIB
  - Cisco Process MIB
  - IF-MIB
  - OSPF v2, OSPFv3
  - BGP
  - Cisco-BGP
  - Cisco-IETF-ISIS
  - Cisco-BFD-MIB

- **Traps Supported**
  - coldstart
  - cefcFRUInserted, cefcFRURemoved
  - cefcFanTrayStatusChange, cefcModuleStatusChange
  - entSensorThresholdNotification
  - cefcPowerStatusChange
  - cpmCPURisingThreshold, cpmCPUFallingThreshold
  - ospfIfStateChange
    ospfNbrStateChange
  - cieLinkUp
    cieLinkDown

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/mib/list/mib-support.html

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

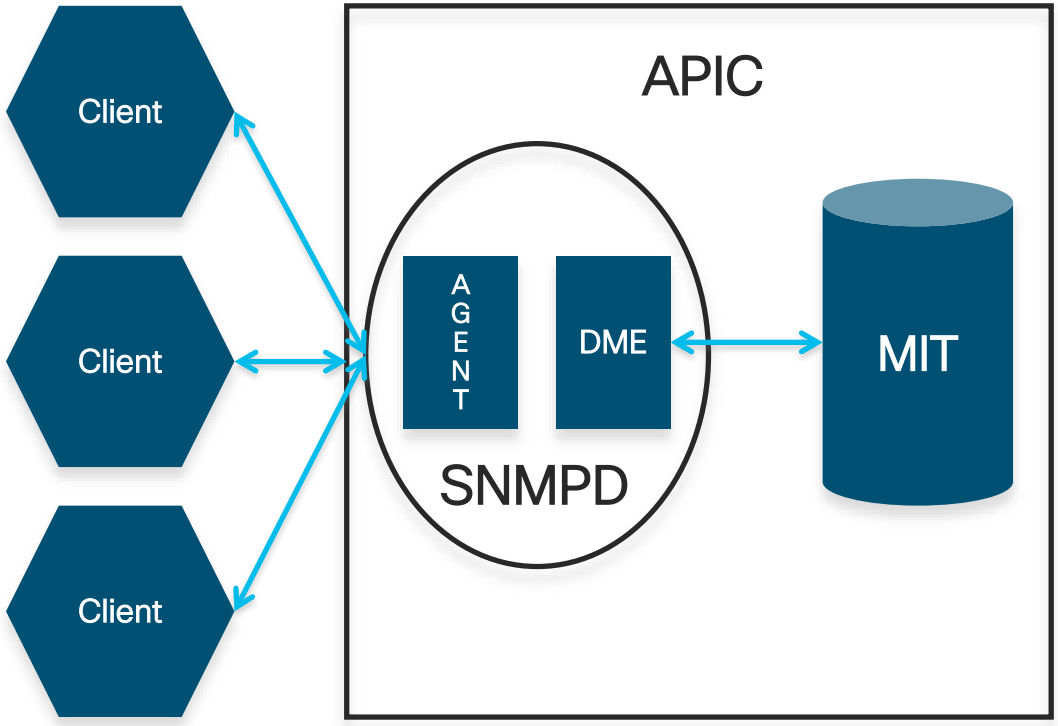
SNMP Support in ACI

- The APIC is build on the Policy Model. The policy framework defines Configuration Objects and Operational Objects (also known as Managed Object or MO).
- Each MO has a set of properties and the changes in properties of the MO can trigger “events” and “faults”.
- The SNMP on APIC defines the MIB Objects to ACI MOs and provides a translation of MO information to the SNMP Objects.
- Traps are generated based on the “events” or “faults” on the MOs.
- SNMP on APIC requires an explicit “Out-Of-Band Contract” on the APIC by permitting port (UDP:161).
- SNMP Traps are enabled based on policy scope under Access/Fabric/Tenant policies

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

SNMP Support in ACI

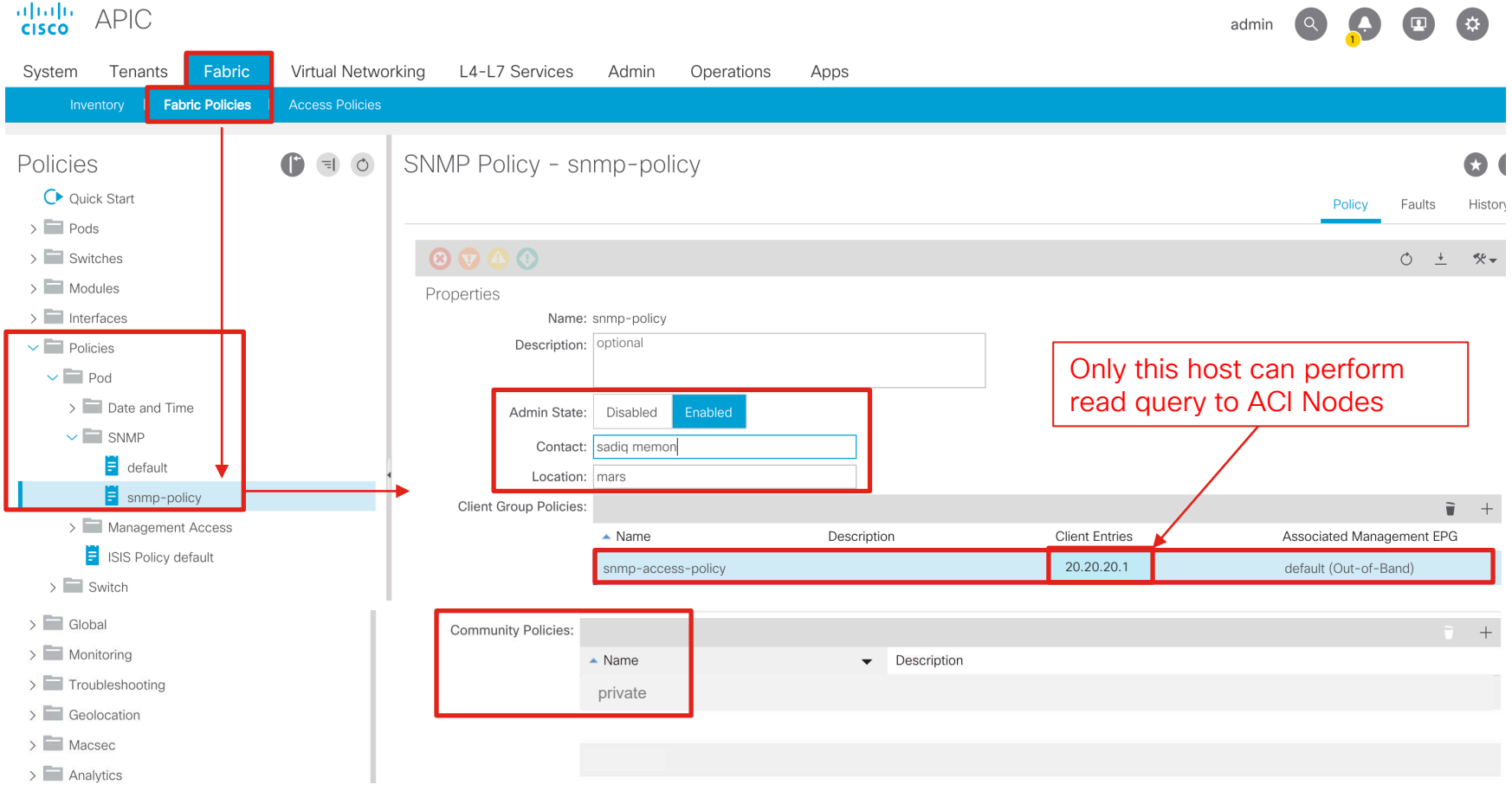
- The SNMPD process on APIC has two components:
  - **Agent:** The SNMP Agent is open-source net-snmp agent (version: 5.7.6). The SNMP agent handles SNMP sessions from the snmp clients. It handles the SNMP protocol processing.
  - **DME:** The SNMP DME handles the MIT interface to read the Managed Objects (MOs) and translate the information into SNMP Object Format.



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

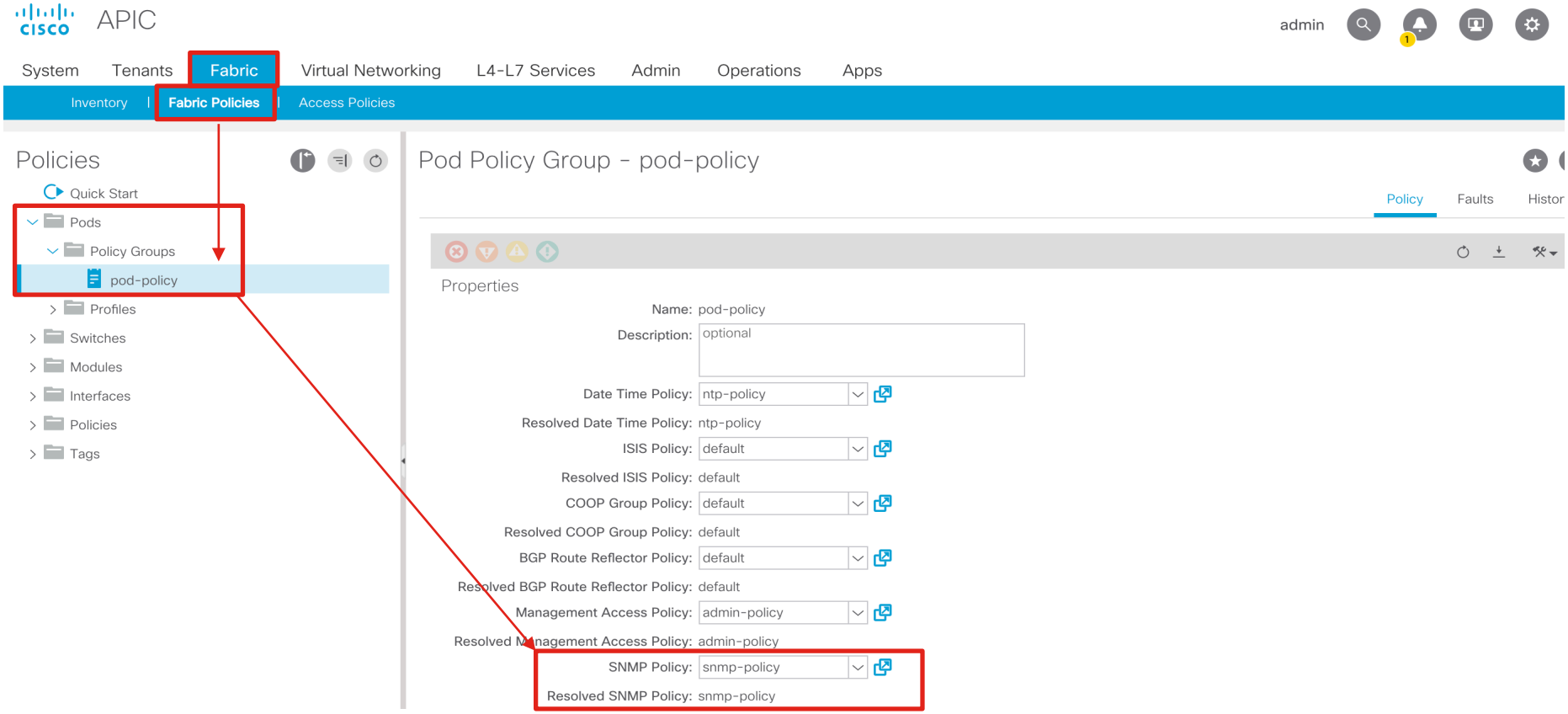
SNMP Configuration

Step 1: Define SNMP Policy



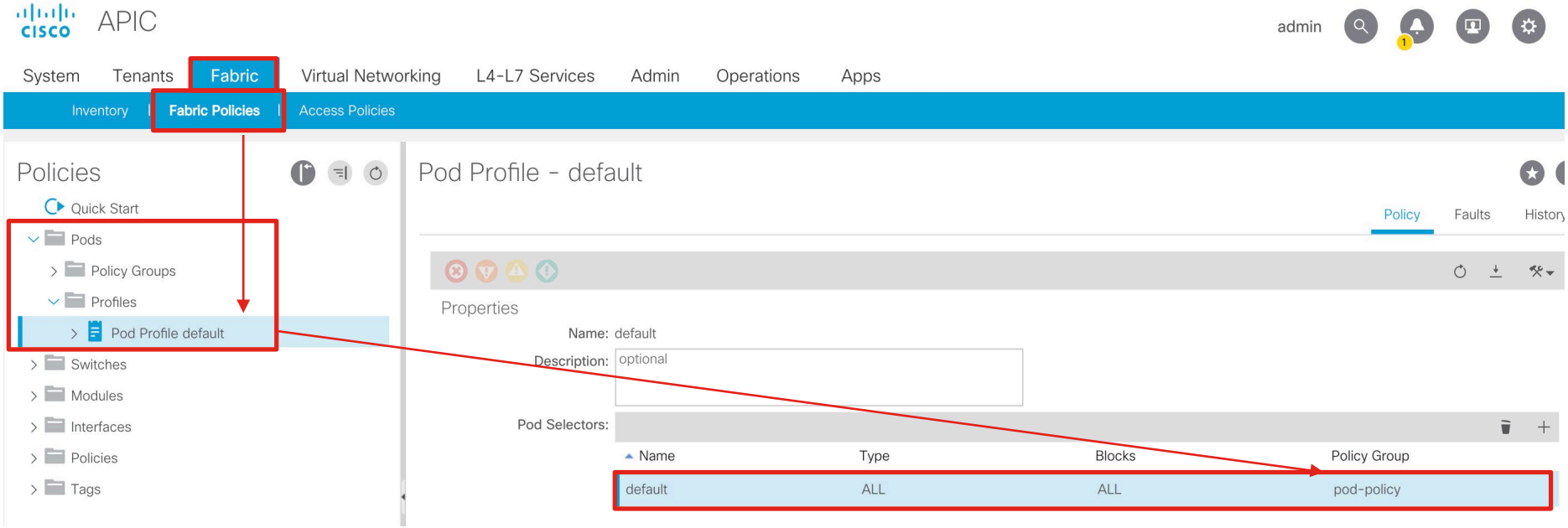
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Step 2: Add SNMP Policy to POD Policy Group



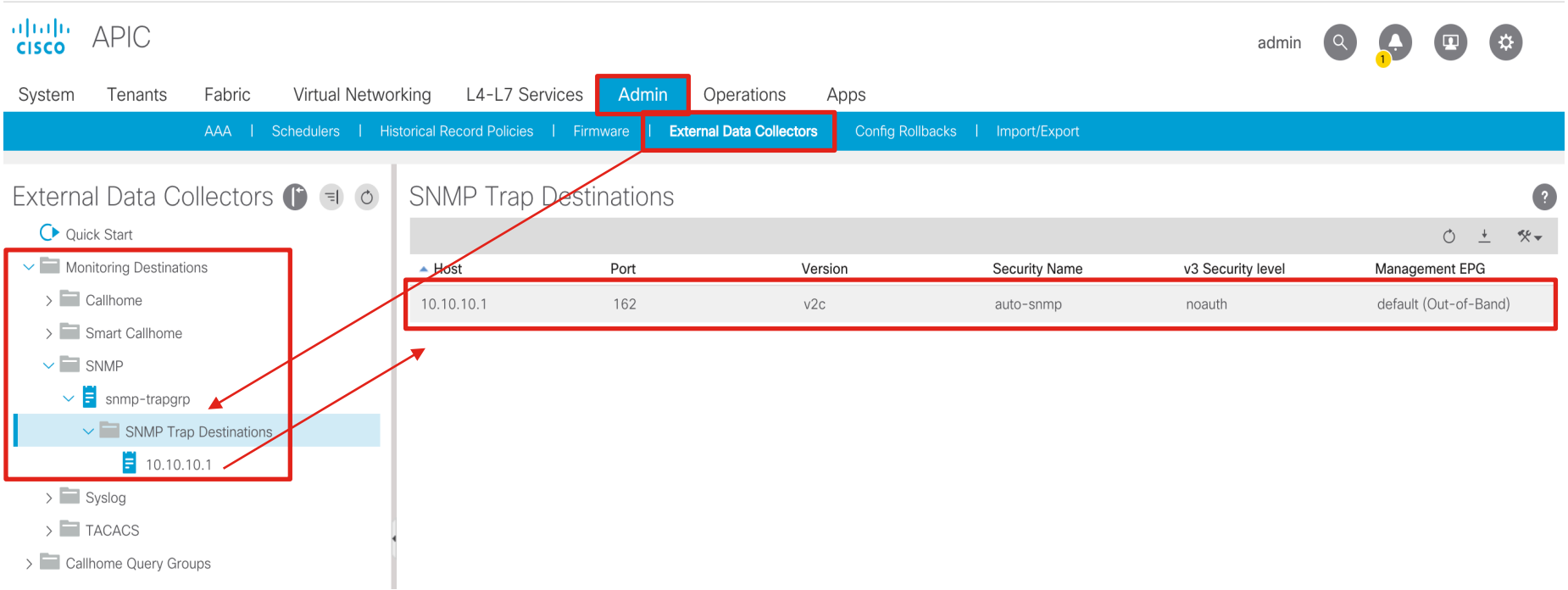
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Step 3: Add POD Policy Group to POD Profile



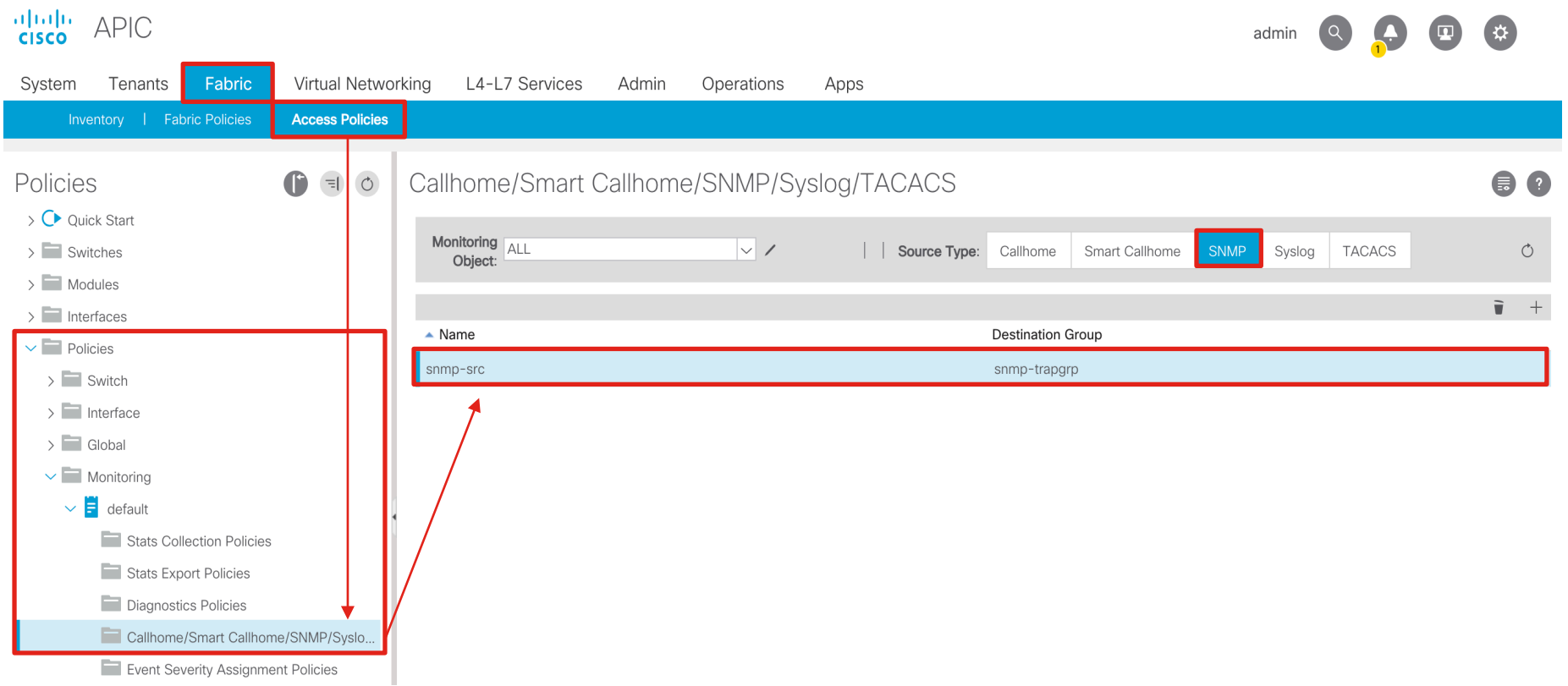
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Step 4: Define SNMP Trap Server(s)



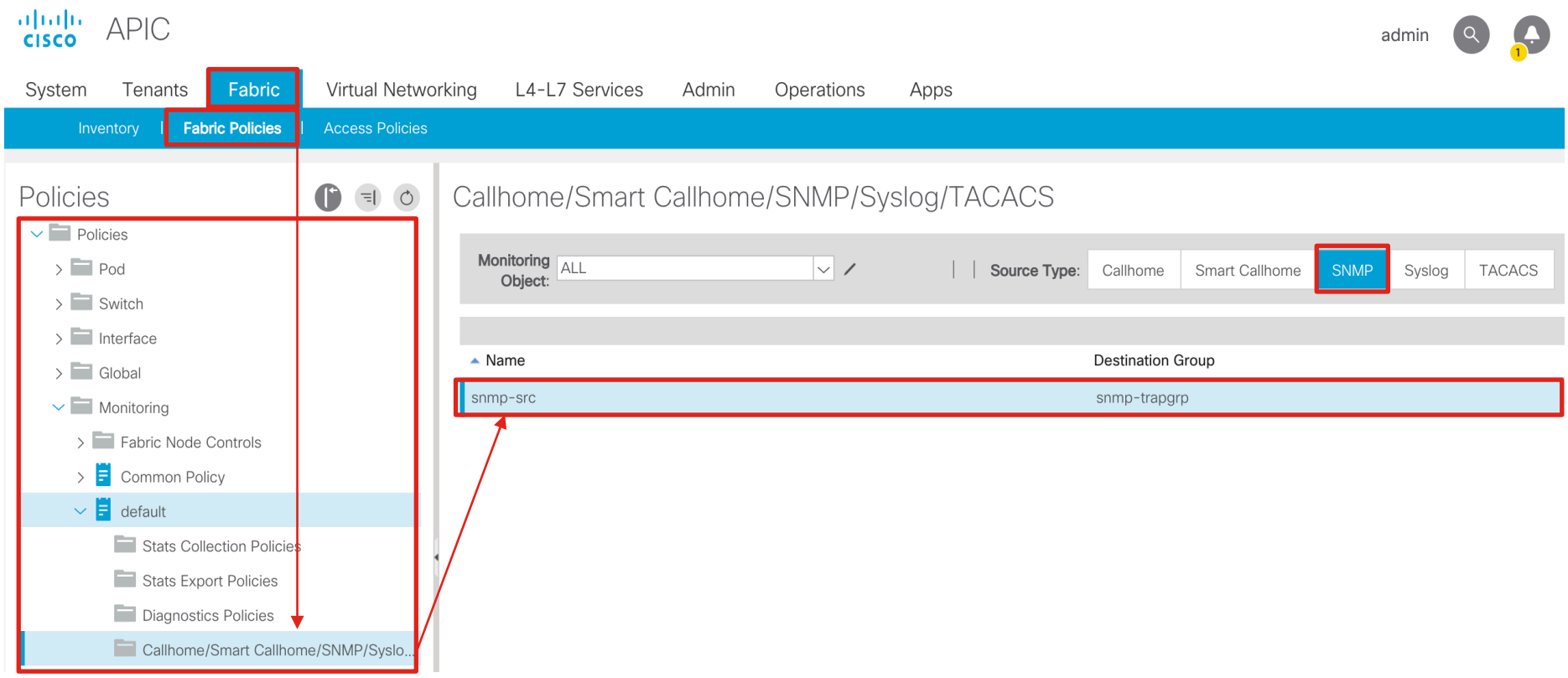
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Step 5: Define SNMP Source under Access Policies



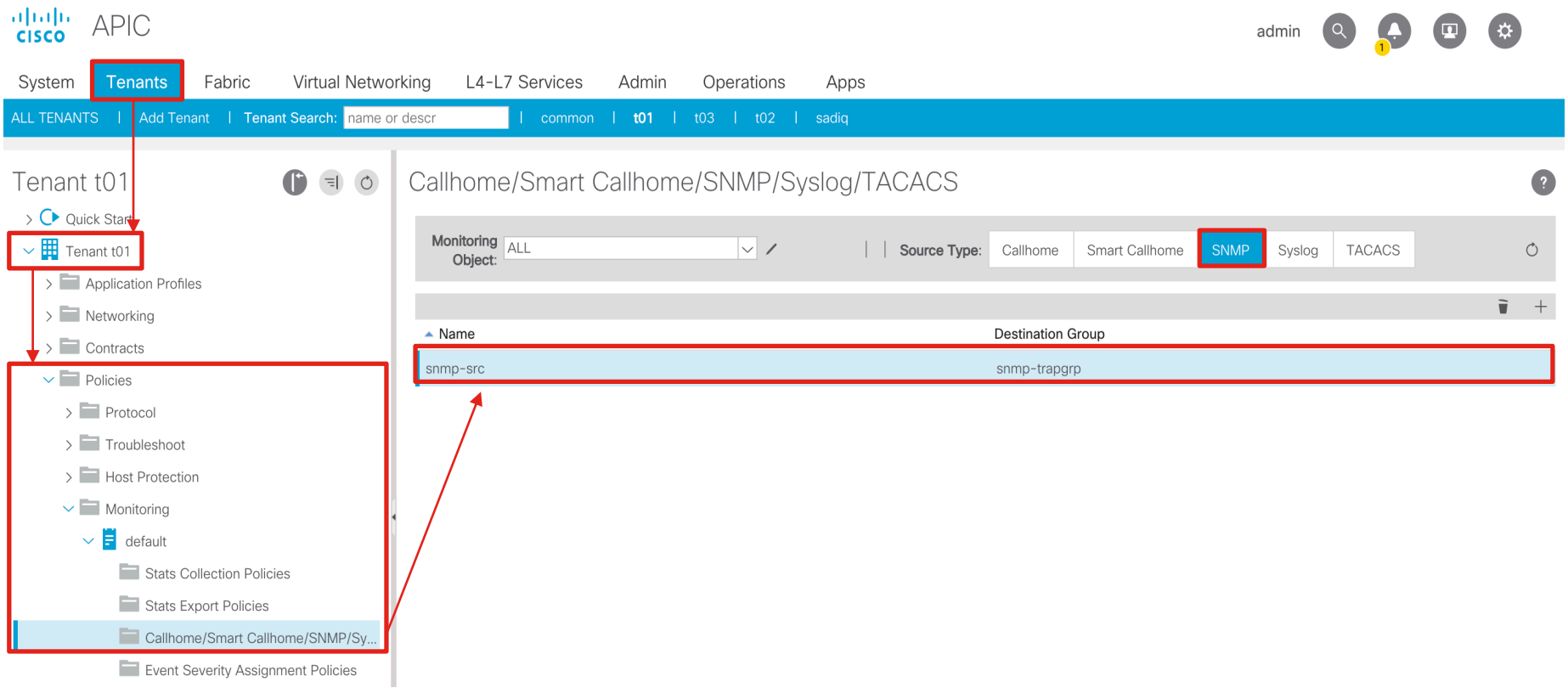
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Step 6: Define SNMP Source under Fabric Policies



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Step 7: Define SNMP Source under Tenant Policies

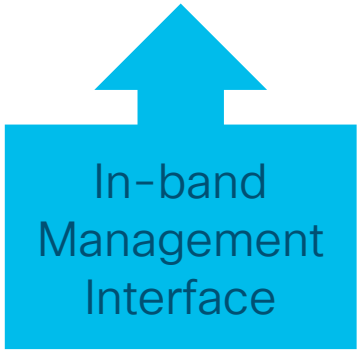


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Verify SNMP status

```
apic1# show snmp host
 IP-Address      Version   Security Level    Community
 --------------  -------   --------------    ---------
 10.10.10.1      v2c       noauth            auto-snmp
```

```
Leaf1# tcpdump -i kpm-inb -f port 162
```



For Out-of-Band Management, the interface is **eth0**

```
apic1# show snmp
Input Statistics:
   0 Read Only PDU
   0 Too big error status
   0 Illegal operation for community name supplied
   0 Get-response PDUs
   0 Unknown Community Name
   1 SNMP packets input
   0 Trap PDUs received
   15 Get-next PDUs
   0 General Errors
   0 Set-request PDUs
   11 Number of requested variables
   0 Encoding errors
   0 Bad SNMP Versions
   0 Number of altered variables
   0 Error status is Bad Value
   0 Get-request PDUs
   0 Unknown Context name
Output Statistics:
   0 Get-request PDUs generated
   25 Get-responses PDUs generated
   0 Set-requests PDUs generated
   0 No such name PDU
   0 General ouptput errors
   0 Get-next PDUs genereated
   1 SNMP packets output
   0 Too big error status generated
   0 Bad value PDU
   0 Trap PDUs generated
Other Statistics:
   0 Silent Drops
   0 Proxy Drops
   Disabled Authentication Traps Status

 Name          Admin State  Location    Contact  Description
 ------------- -----------  ----------  -------  -----------
 snmp-policy   enabled      mars        sadiq memon
```


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Syslog

Syslog Overview

- Syslog is a method to collect messages (Faults, Events, Audit, Session) from devices to a server running a syslog daemon.
- During operation, a *Fault* or *Event* in ACI system can trigger the sending of a system log (syslog) message to the console and/or to an external logging server.
- Fault-generated system messages are triggered by:
  - A fault rule.
  - A threshold crossing
  - A failure of a task or Finite State Machine (FSM) sequence.
- Event-generated system messages are triggered by:
  - An event rule.
  - An event in NX-OS of Leaf/Spine.
- Syslog like SNMP Traps are also enabled based on policy scope under Access/Fabric/Tenant policies

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

System Message Structure

timestamp host %LOG_LOCAL*(1-7)*-severity-SYSTEM_MSG [code][lifecycle state][rule][severity text] [DN of affected MO] Message-text

Example (Fault):

Apr 10 12:28:21 apic1 %LOG_LOCAL0-2-SYSTEM_MSG [F0321][soaking][unhealthy][critical] [topology/pod-1/ node-1/av/node-1/fault-F0321] Controller 1 is unhealthy because: Data Layer Partially Diverged

In this system message:

- Timestamp of the message is "Apr 10 12:28:21"
- "apic1" is the host and indicates that this message is generated by the controller.
- "2" (Major) is the severity level, indicating a "Critical" condition.
- "F0321" is the *Fault* code, which we can look up as "fltInfraWiNodeHealth" in the API documentation.
- "soaking" is the current lifecycle state of the fault.
- "unhealthy" is the cause of the fault.
- "topology/pod-1/node-1/av/node-1" is the DN of the affected object, which is node 1 in pod 1.
- "fault-F0321" is the DN of the fault object, which is a child of the affected object.
- "Controller 1 is unhealthy because: Data Layer Partially Diverged" is the message-text.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

System Message Structure

timestamp host %LOG_LOCAL*(1-7)*-severity-SYSTEM_MSG [code][lifecycle state][rule][severity text] [DN of affected MO] Message-text

Example (Event):

Apr 10 02:18:16 apic1 %LOG_LOCAL3-6-SYSTEM_MSG [E4208219][Link-state-change][info] [topology/pod-1/lnkcnt-216/lnk-2101-1-9-to-216-1-49] Link State of Fabric Link is set to ok

In this system message:

- Timestamp of the message is "Apr 10 12:28:21"
- "apic1" is the host and indicates that this message is generated by the controller.
- "6" (Info) is the severity level, indicating an "informational" message.
- "E4208219" is the *Event* code, which we can look up as "fabric_Link_linkStateChange" in the API documentation.
- "link-state-change" is the cause of the fault.
- "topology/pod-1/lnkcnt-216/lnk-2101-1-9-to-216-1-49" is the DN of the affected object, which is a link.
- "Link State of Fabric Link is set to ok" is the message-text.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

System Message Severity Level

	Severity Level (NXOS)	ITU Level (ACI)	Description
0	emergency		System is un-usable
1	alert	critical	Immediate action required
2	critical	major	Critical condition
3	error	minor	Error condition
4	warning	warning	Warning condition
5	notification	cleared	Normal but significant condition
6	informational	(info)	Informational message only
7	debugging	(not used)	Message that appears during debugging only

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Some Important log Messages to parse for trouble ticket

Fault No.	Fault Object Name	Description
F1543	fltFabricNodeInactive	Fabric Node Un-reachable
F0532	fltEthpmIfPortDownInfraEpg	Host interface is DOWN and is in use by EPG
F1385	fltOspfAdjEpFailed	OSPF Adjacency is DOWN
F0299	fltBgpPeerEntryFailed	BGP Peer is not ESTABLISHED
F1296	fltVpcIfIfDown	VPC interface is DOWN while Peer interface is DOWN as well
F2705	fltVpcIfIfImpaired	VPC interface is DOWN while Peer interface is UP
F1262	fltInfraServiceOptimalLeadership	APIC reports some services do not have ideal replica leaders of shards
F0321	fltInfraWiNodeHealth	APIC reports the distributed internal database (data layer) of the controller cluster is not fully functional
F1394	fltEthpmIfPortDownFabric	Fabric Port is DOWN
F0475	fltTunnelIfDestUnreach	Tunnel Destination Un-reachable
F0360	fltIsisFmcastTreeTreeInactive	Operational state of a Mcast tree changes to inactive in the fabric
F1360	fltCoopAdjEpCoopAdjEpDown	Coop Adjacency is DOWN

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Some Important log Messages to parse for trouble ticket

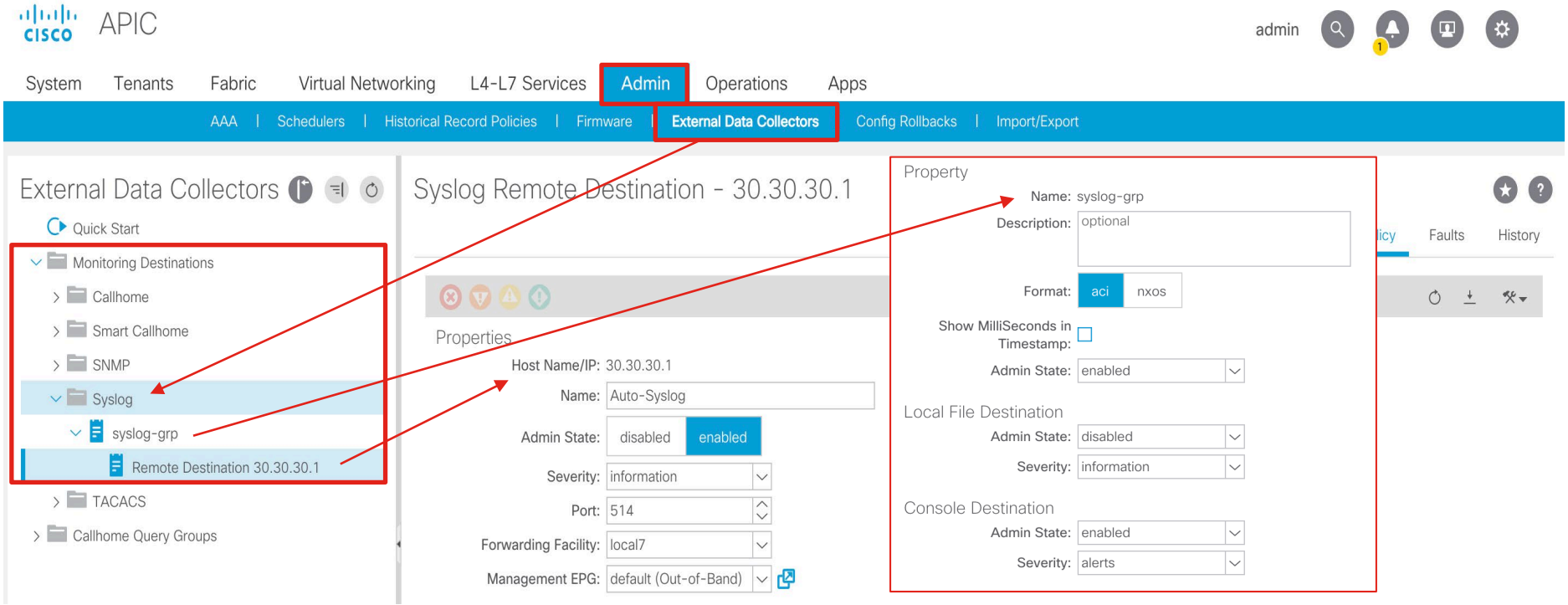
Fault No.	Fault Object Name	Description
F0411	fltEqptPsuFailed	Power Supply Unit is Failed in Fabric Node
F0412	fltEqptPsuFanFailed	Power Supply Unit FAN is Failed in Fabric Node
F0413	fltEqptPsuSlotPsuMissing	Power Supply Unit is Missing/Removed from Fabric Node
F1317	fltEqptPsgPNonRedun	Power Supply Unit is Non-Redundant in Fabric Node
F1318	fltEqptPsgPZeroPwr	Power Supply Unit is not detected correctly in Fabric Node
F1321	fltEqptFtFanTrayFailed	FAN Tray failed in Spine (Nexus 9500)
F1322	fltEqptFanFanFailed	FAN failed in Spine (Nexus 9500)
F1323	fltEqptFtSlotFanTrayMissing	FAN Tray Missing/Removed from Spine (Nexus 9500)
F1451	fltEqptPsuShut	No Power in Power Supply Unit
F1526	fltEqptSlotFailed	Fabric Module or Line Card Failed in Spine (Nexus 9500)
F0101	fltEqptStorageFailed	Storage device on APIC Failed
F2992	fltSvcredirRsDestAttOperSt Failed	PBR service destination goes to failed state

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/2-x/syslog/guide/b_ACI_System_Messages_Guide.html

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

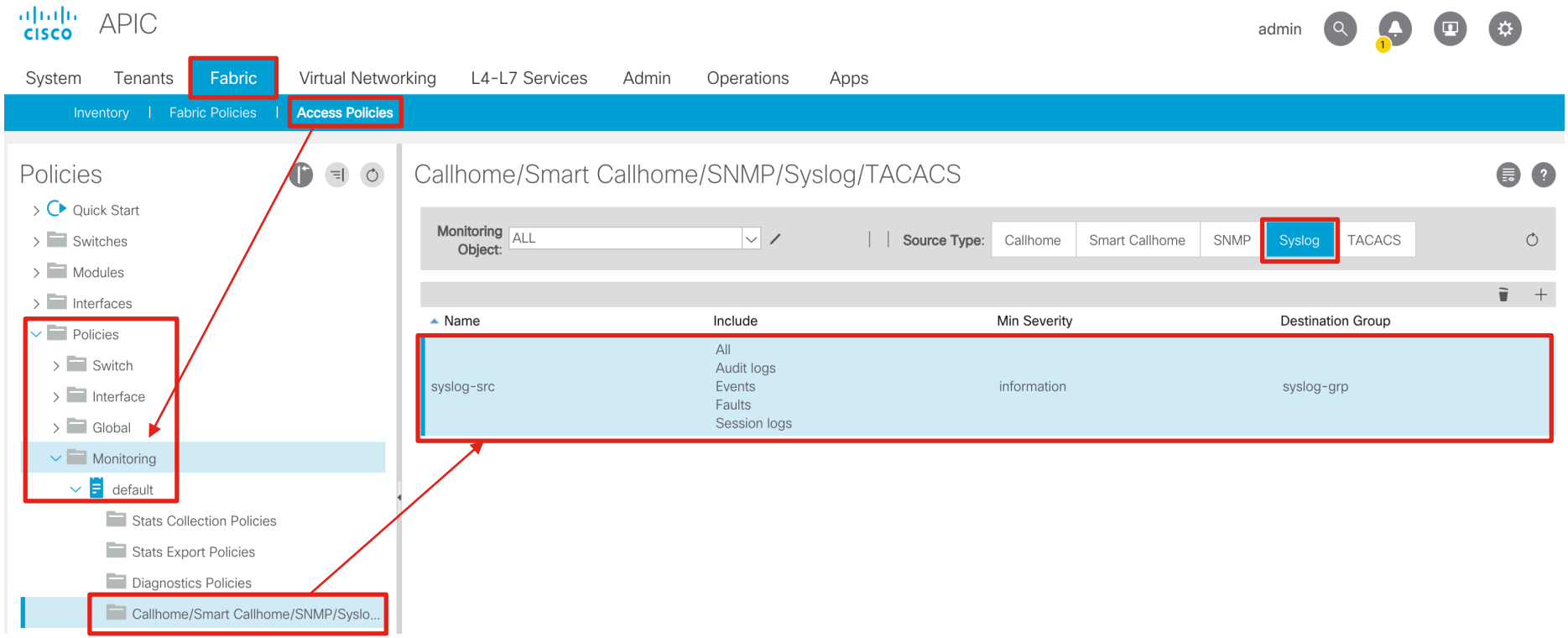
Syslog Configuration

Step 1: Define External Syslog Server(s)



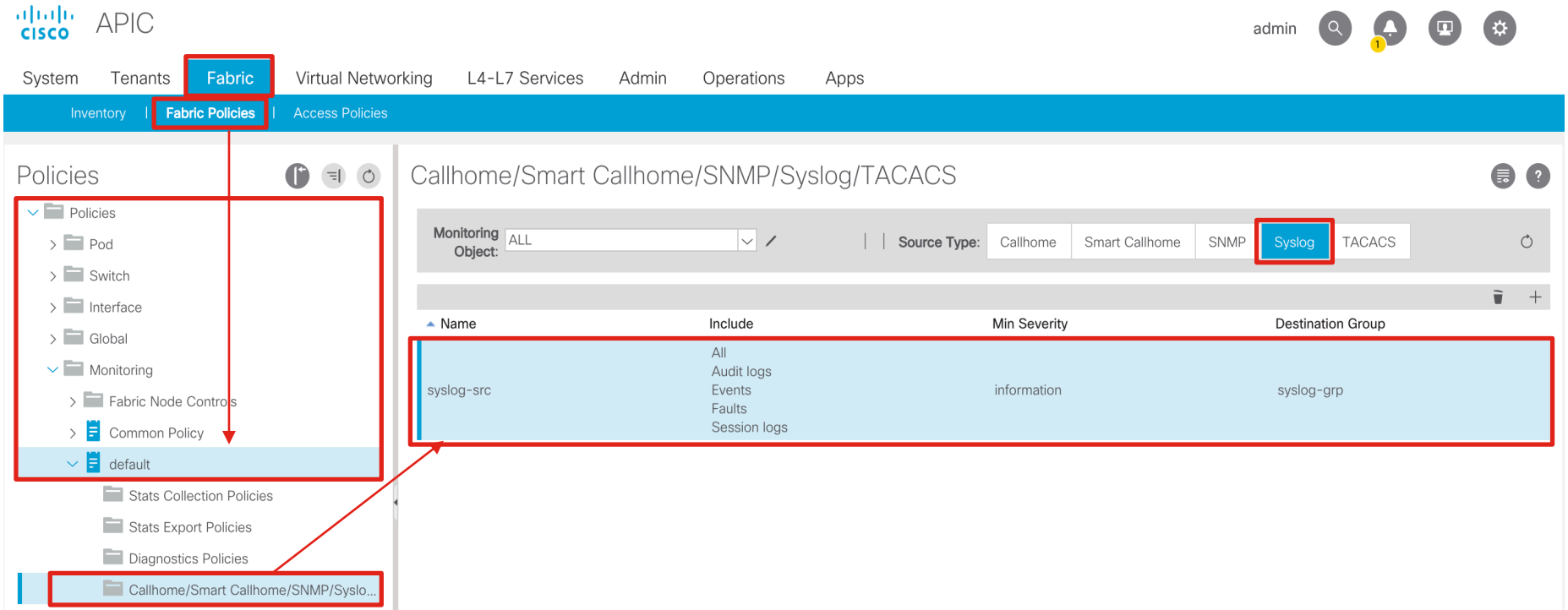
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Step 2: Define Syslog Source under Access Policies



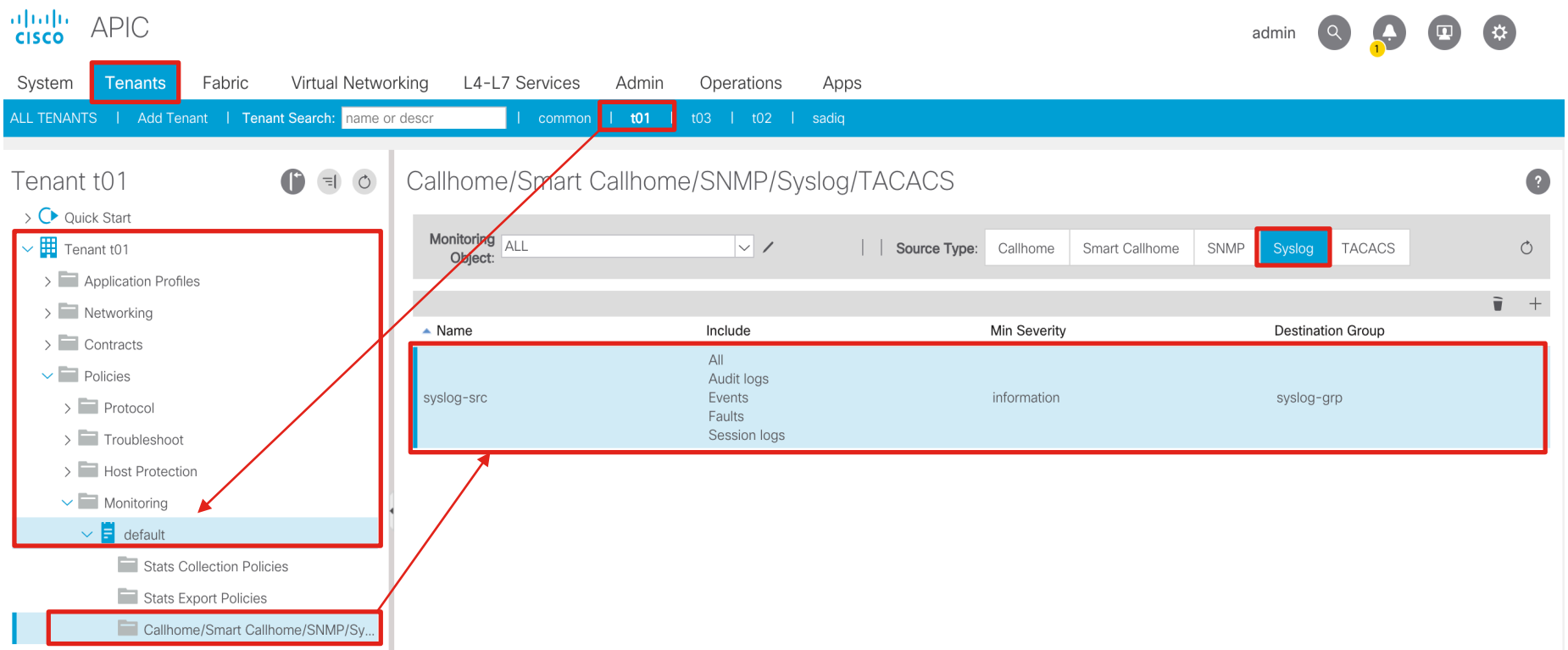
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Step 3: Define Syslog Source under Fabric Policies



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Step 4: Define Syslog Source under Tenant Policies



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Verify Syslog status

In-band Management Interface.
For Out-of-Band Management Interface, use eth0

```
Leaf1# tcpdump -i kpm_inb -f port 514
```

```
apic1# show running-config logging
# Command: show running-config logging
# Time: Sun May 12 20:15:03 2019
  logging server-group syslog-grp
    console
    server 30.30.30.1 severity information facility local7 mgmtepg oob port 514
    exit
```

Shutdown any port such as eth1/5 on Leaf.
You should see syslog on your server.
****

May 12 17:43:17 192.88.196.132 Sep 23 12:43:05 leaf1005 %LOG_LOCAL7-6-SYSTEM_MSG [E4205126][port-down][info][sys/phys-[eth1/5]/phys] Port is down. Reason: adminCfgChng

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

SPAN

Switch Port Analyzer (SPAN) support in ACI

- SPAN in ACI can be configured in 4 different categories:
  - **Access** – for monitoring traffic originating from access ports in leaf nodes
  - **Fabric** – for monitoring traffic from fabric ports in leaf or spine nodes
  - **Tenant** – for monitoring traffic from endpoint groups (EPGs) within a tenant
  - **Visibility & Troubleshooting** – Initiate SPAN based on defined endpoint to endpoint
- SPAN traffic competes with user traffic for switch resources. To minimize the load, filter SPAN to copy only the specific traffic for analysis during troubleshooting.
- Layer 3 sub-interface cannot be configured as a SPAN source.
- Tenant and access SPAN use the encapsulated remote extension of SPAN (ERSPAN) type I, while fabric SPAN uses ERSPAN type II
- SPAN destination *cannot* be external L2 or L3

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ACI SPAN Feature

	Tenant SPAN	Fabric SPAN	Access SPAN	Troubleshooting SPAN
Source	EPG	Fabric Links (leaf or spine)	Leaf downlink port	Endpoint
Destination	ERSPAN	ERSPAN	ERSPAN, Leaf downlink port	ERSPAN, APIC
Filter	None	Bridge Domain, VRF	None, EPG, Routed Outside (L3out)	None

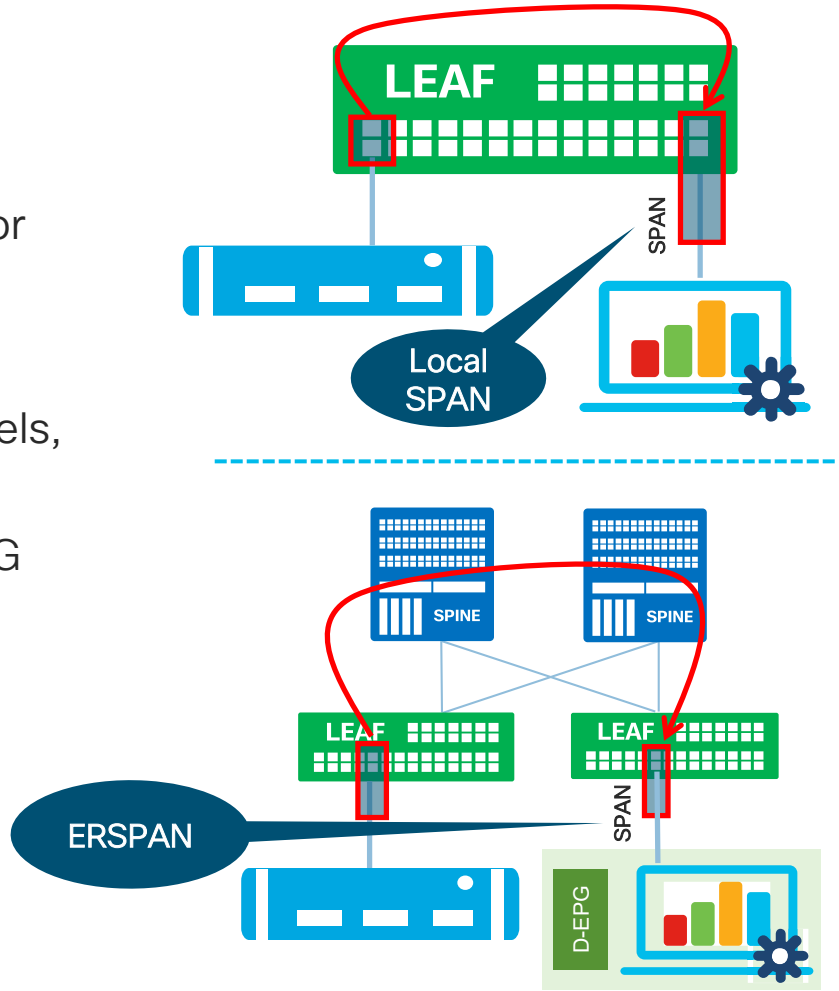
SPAN Filter with DROP/5 Tuple
4.1 & later

ACI Code 3.2 & later

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Access SPAN

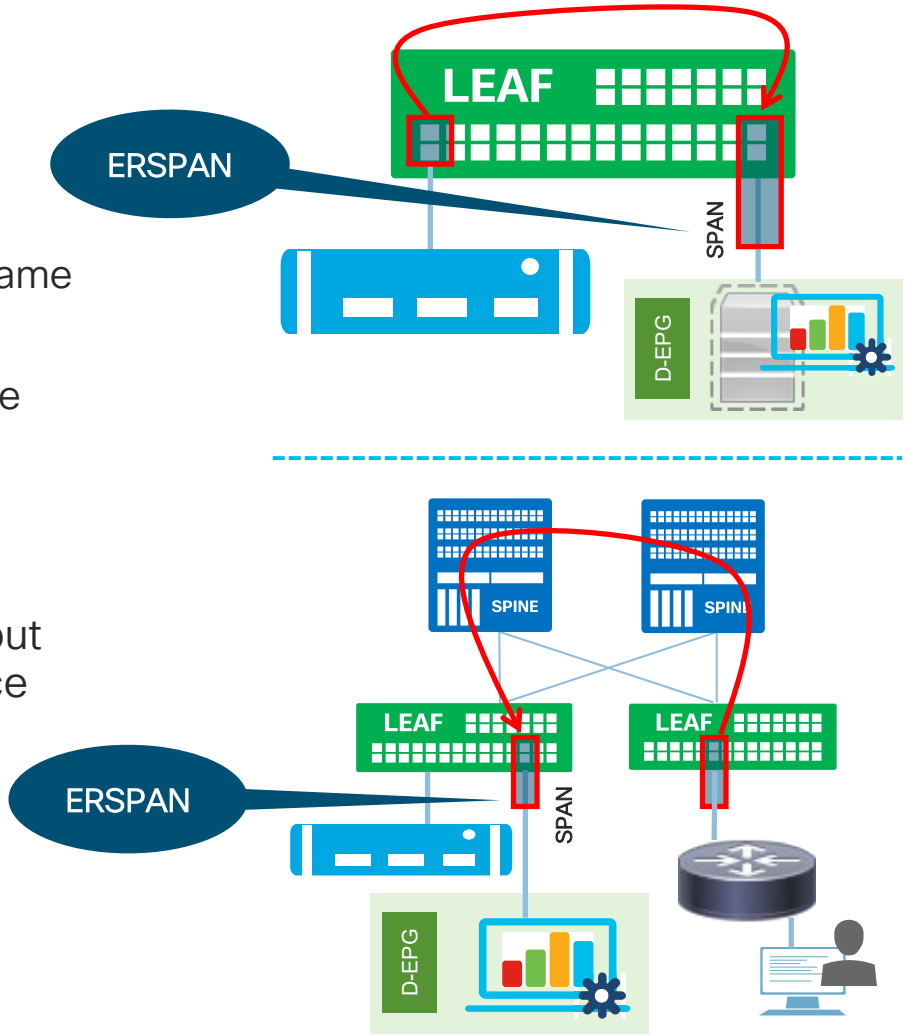
- Access SPAN is used to configure Local SPAN or ERSPAN on leaf switches
- SPAN can be ingress, egress, or both directions
- SPAN sources can be physical port, port-channels, VPC port-channels, or VPC component ports
- Access SPAN supports filters such as None, EPG and Routed Outside
- Access SPAN EPG filter is translated to a VLAN filter when the SPAN session is programmed on the leaf.



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Access SPAN

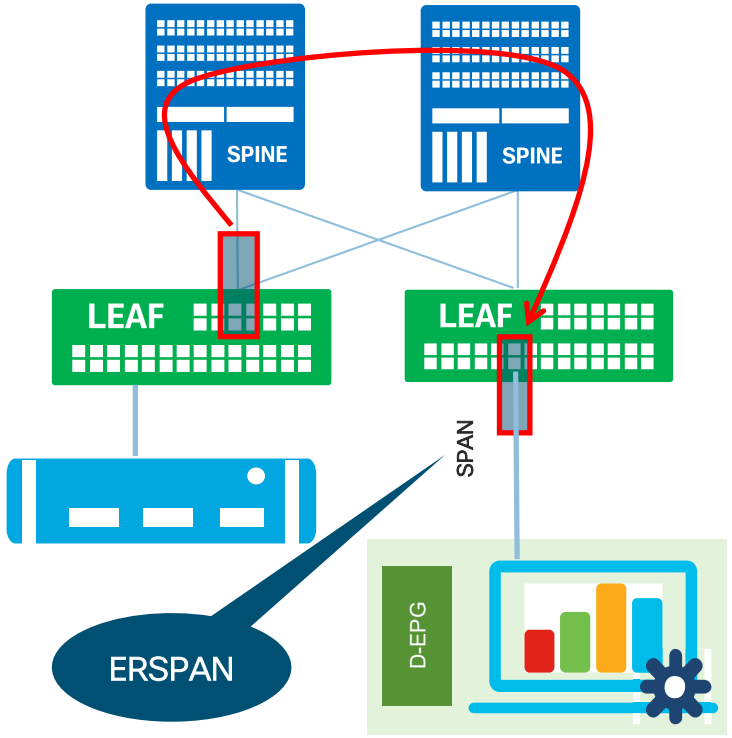
- Destination of Access SPAN *must* be ERSPAN if running on Virtual Machine even connected to same leaf as Source.
- Routed Outside SPAN filter represents one of the following
  - L3out routed sub-interface
  - L3out SVI
- Routed Outside SPAN will filter based on L3out VLAN for routed sub-interface or SVI interface
- Encap value in Routed Outside SPAN is:
  - Mandatory for routed sub-interface and SVI
  - Not applicable for routed interface



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Fabric SPAN

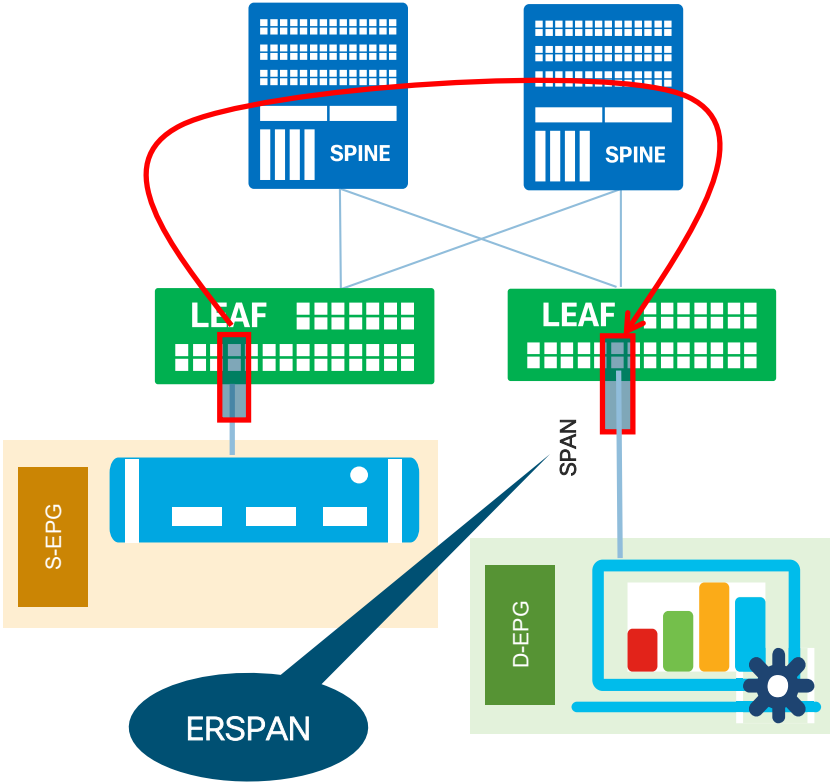
- Fabric SPAN captures packets from the Fabric ports (Leaf/Spine)
- Fabric SPAN can be filer by VRF or Bridge Domain
- SPAN Destination can only be ERSPAN
- ERSPAN Type II Encapsulation



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Tenant SPAN

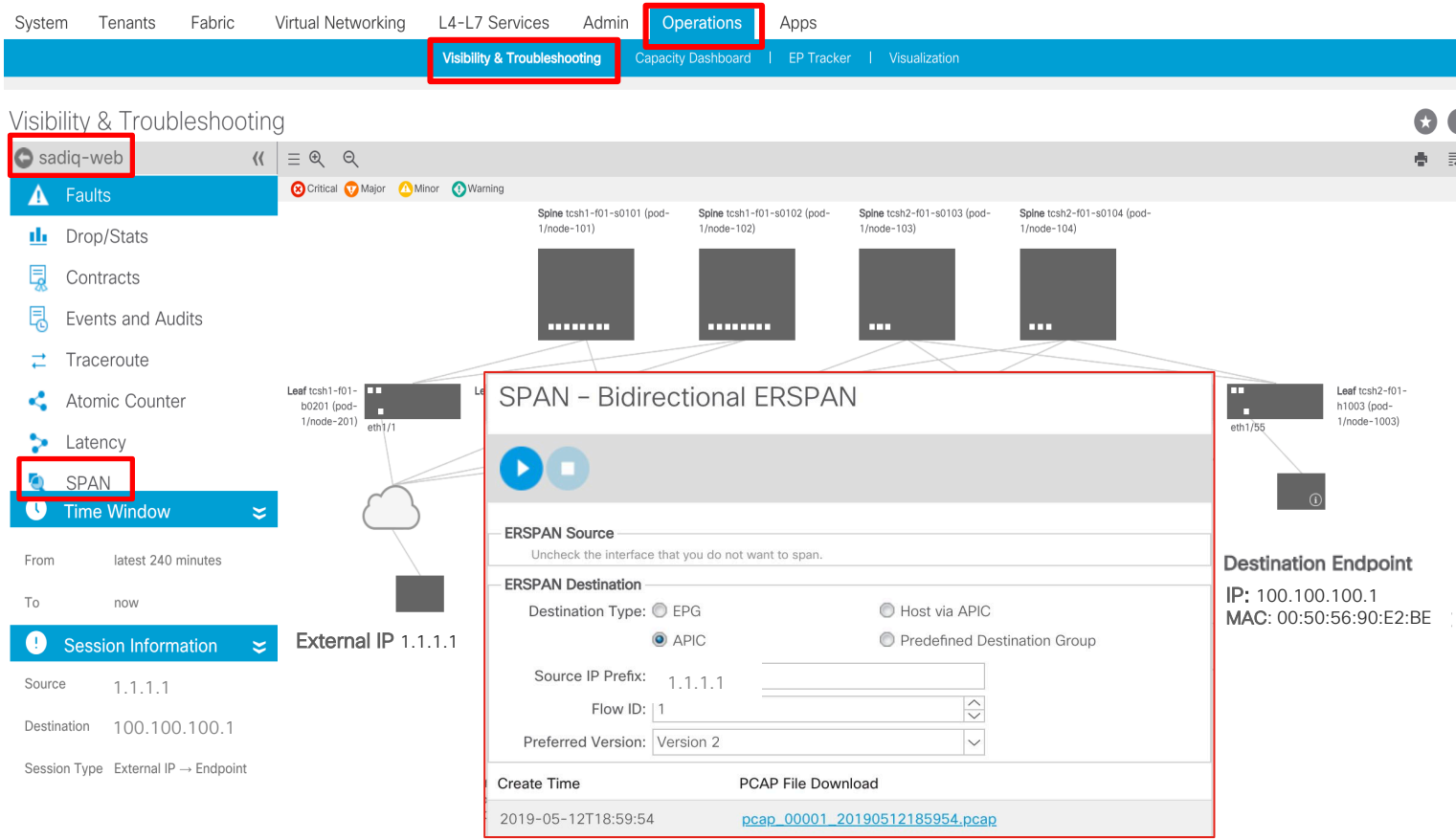
- A tenant operator can configure a Tenant SPAN around it's own application profile policies.
- The source of the SPAN can be any Application Profile EPG
- The destination can be another EPG from the Tenant Application Profile
- Best practice to define a special EPG (management) and associate station to receive ERSPAN



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Visibility & Troubleshooting SPAN

- Useful to take a quick look of your EP connectivity issue remotely.
- No need to have packet capture host.
- In-band management is mandatory.

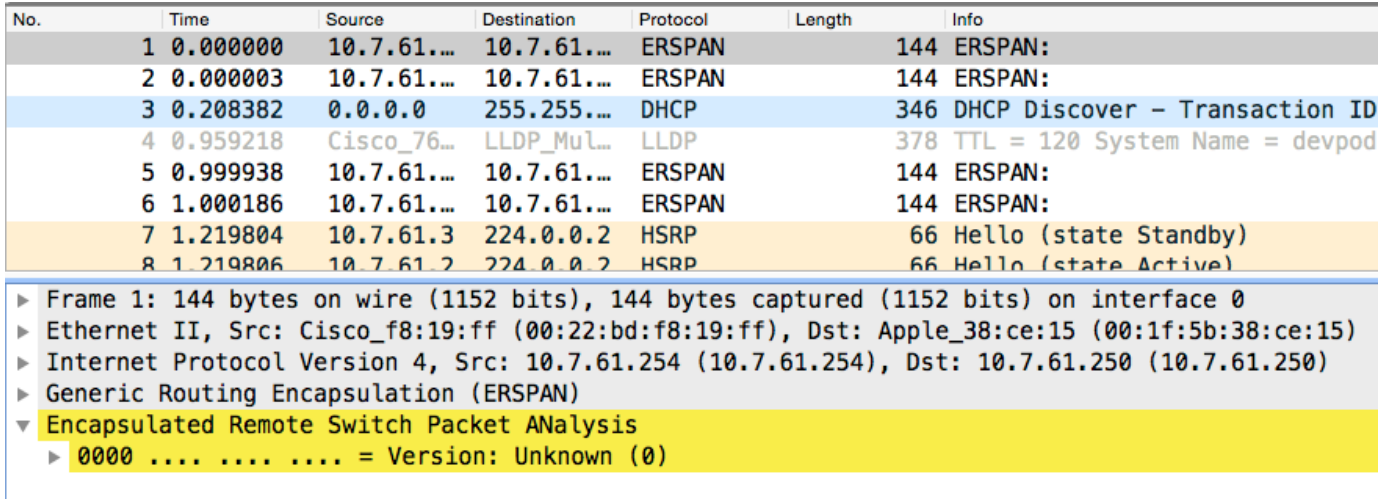


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Wireshark Decode

- For Tenant SPAN you force decode of ERSPAN traffic due to invalid version packet header
  - This is due to limitation in hardware ASIC at leaf level for this SPAN session type

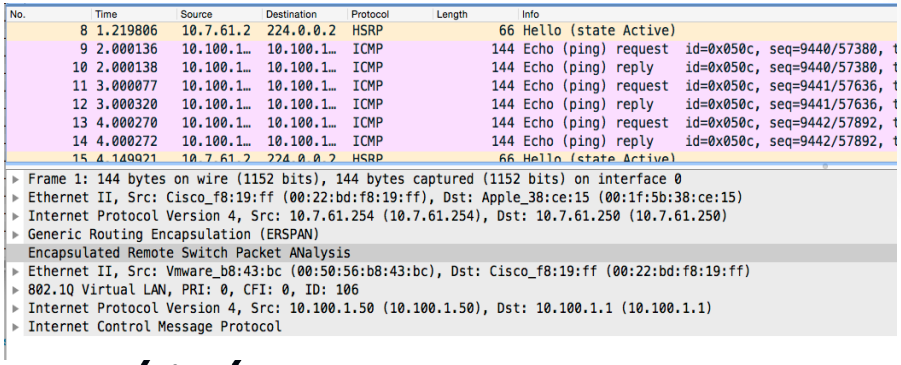
For Gen1 hardware only

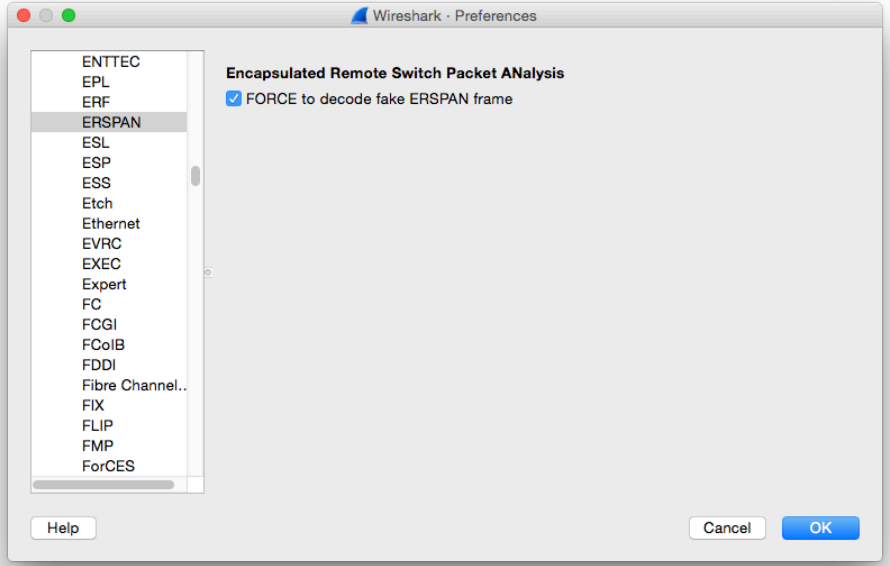


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Wireshark Decode

- For all non-local SPAN you have to force decode of ERSPAN traffic due to invalid version classifier in packet
- In Wireshark program, under *Preferences* > *Protocols*
  - Click **Force to decode fake ERSPAN**

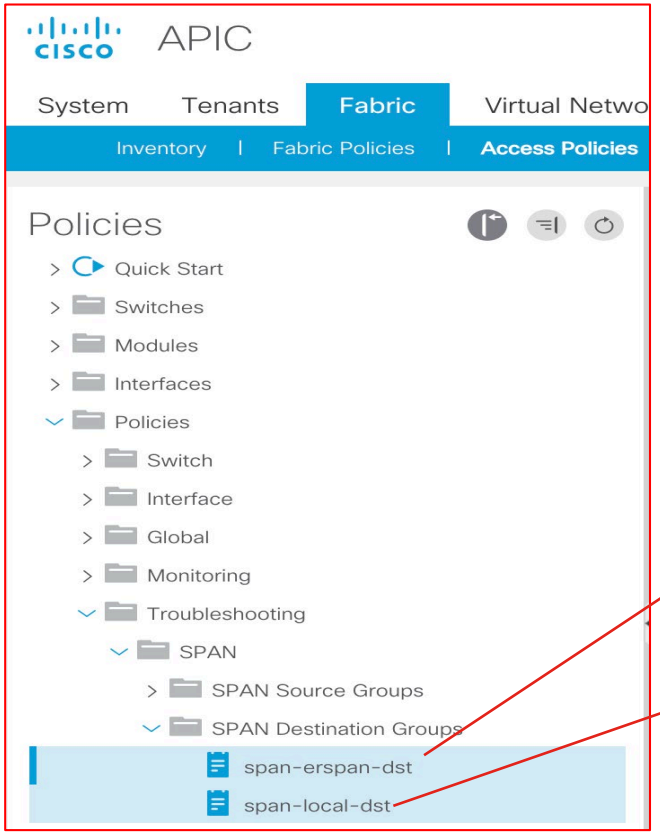


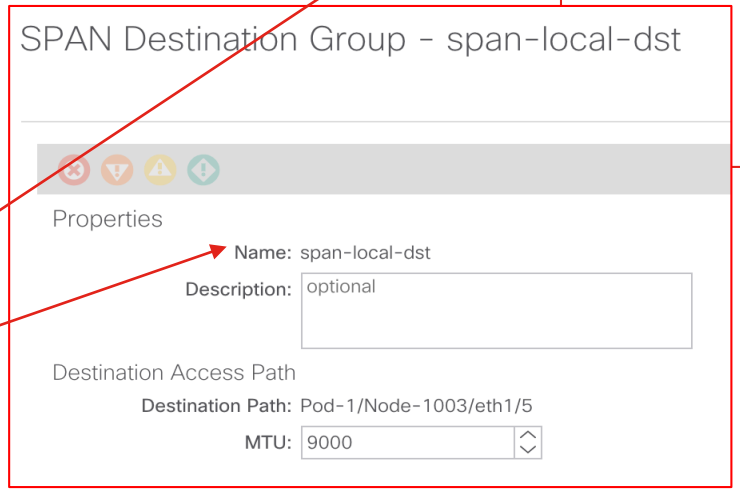


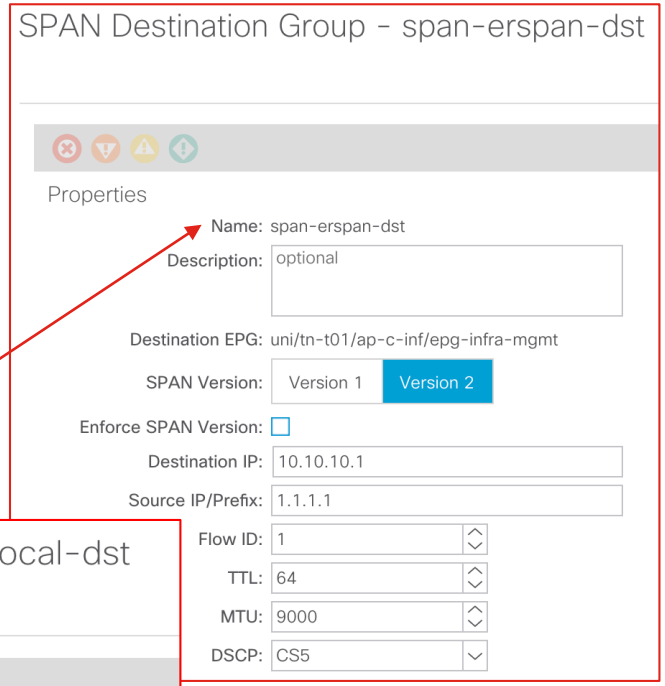
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

SPAN Configuration

Access SPAN (Destination)

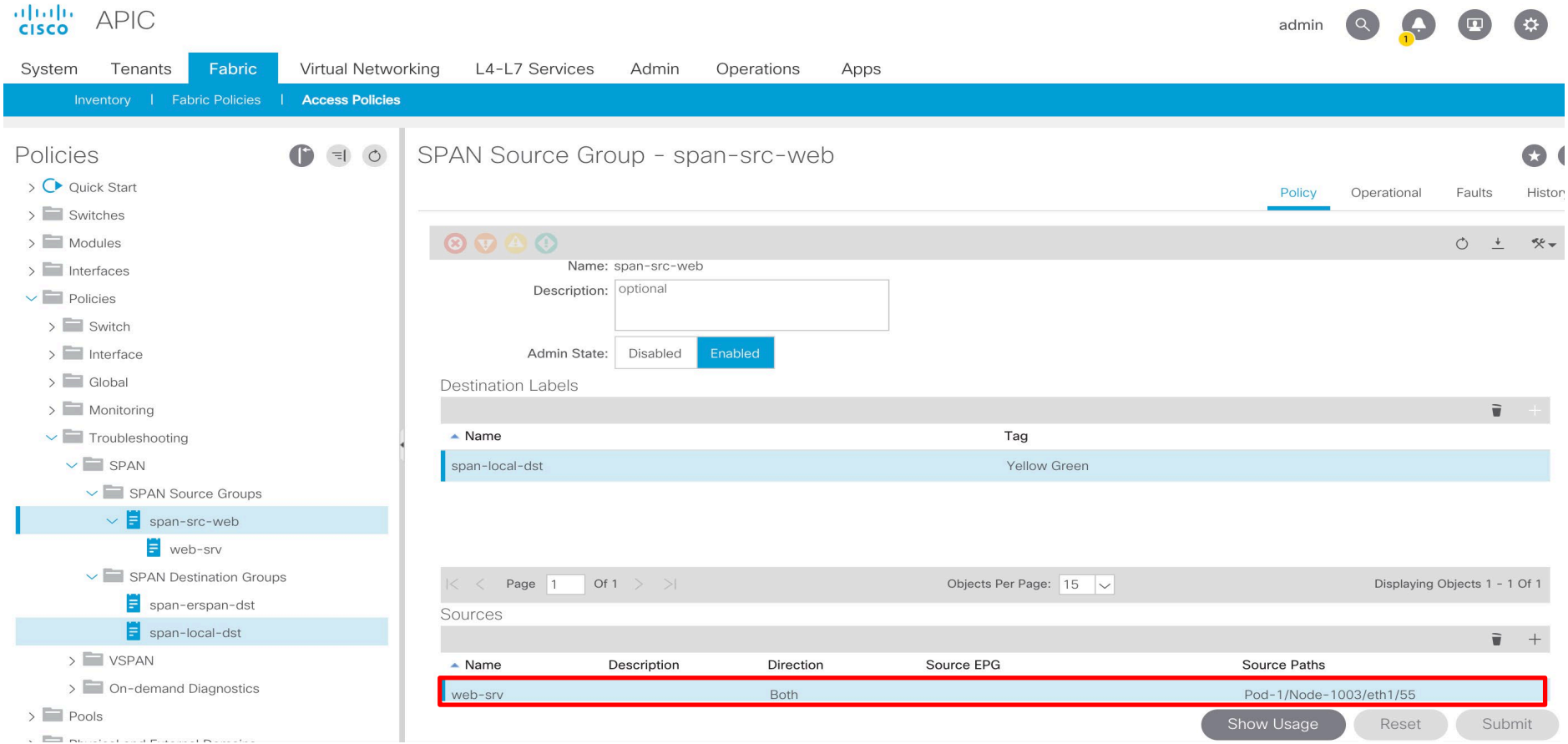






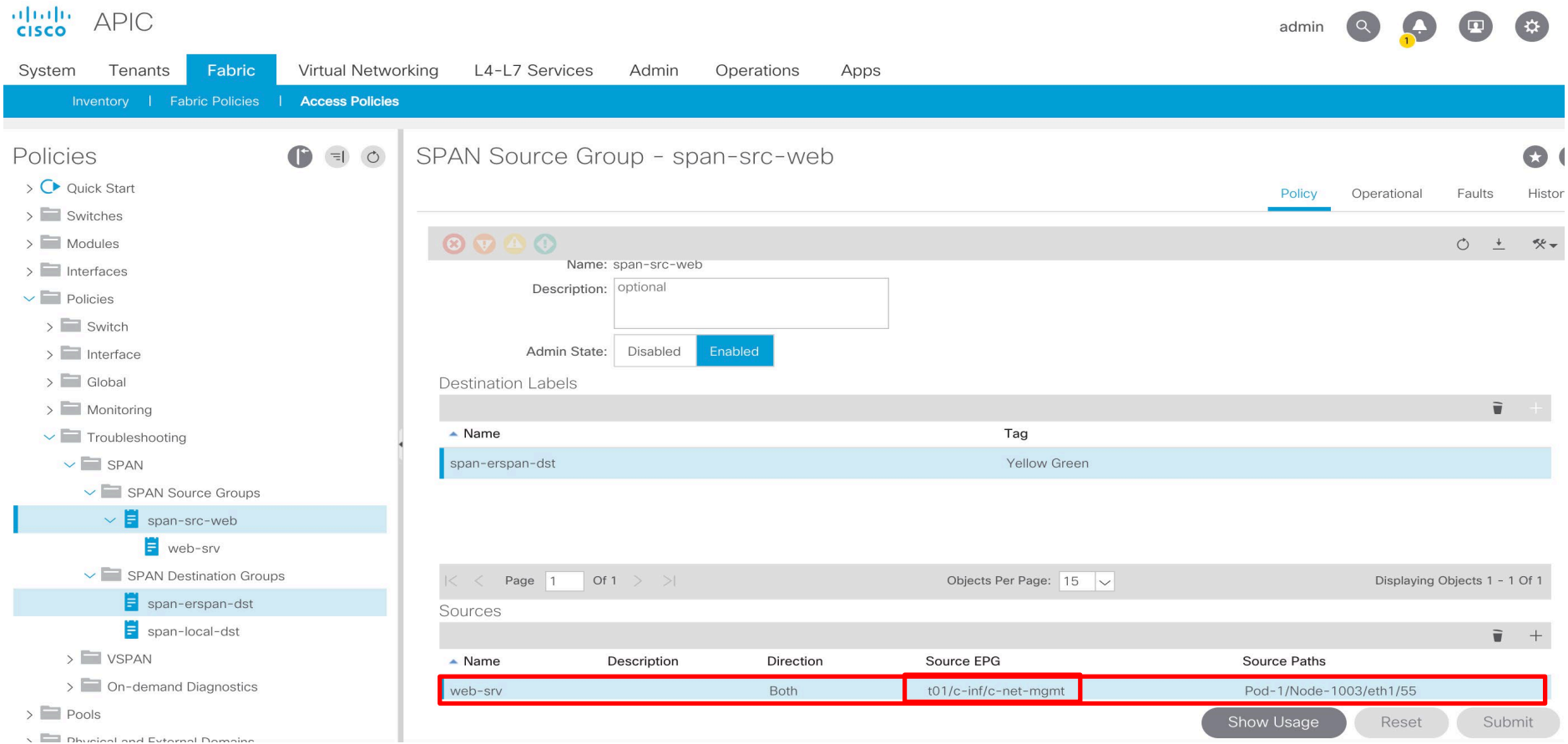
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Access SPAN (Source – w/Filter None)



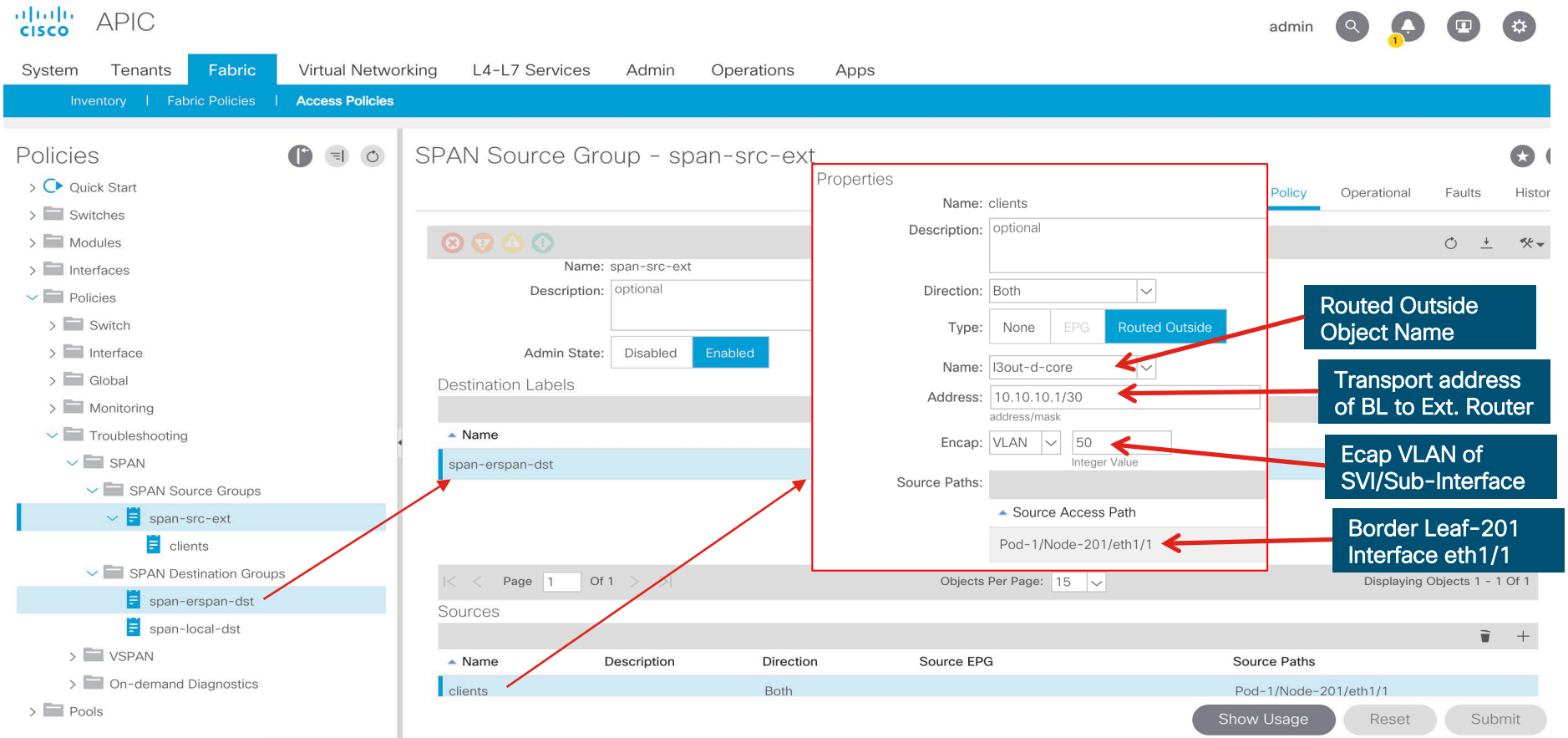
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Access SPAN (Source – w/Filter EPG)



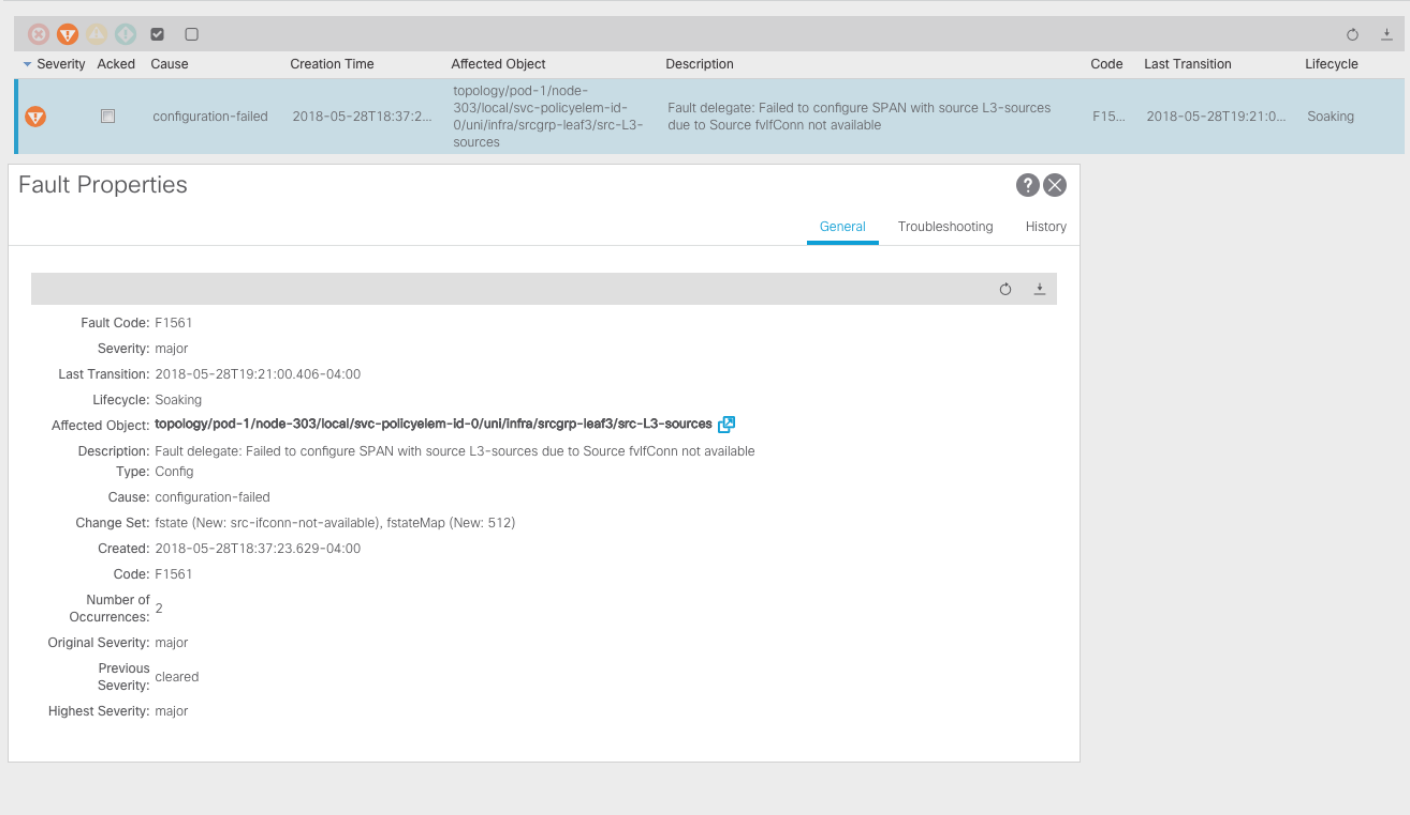
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Access SPAN (Source – w/Filter Routed Outside)



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Access SPAN (Source – w/Filter Routed Outside)

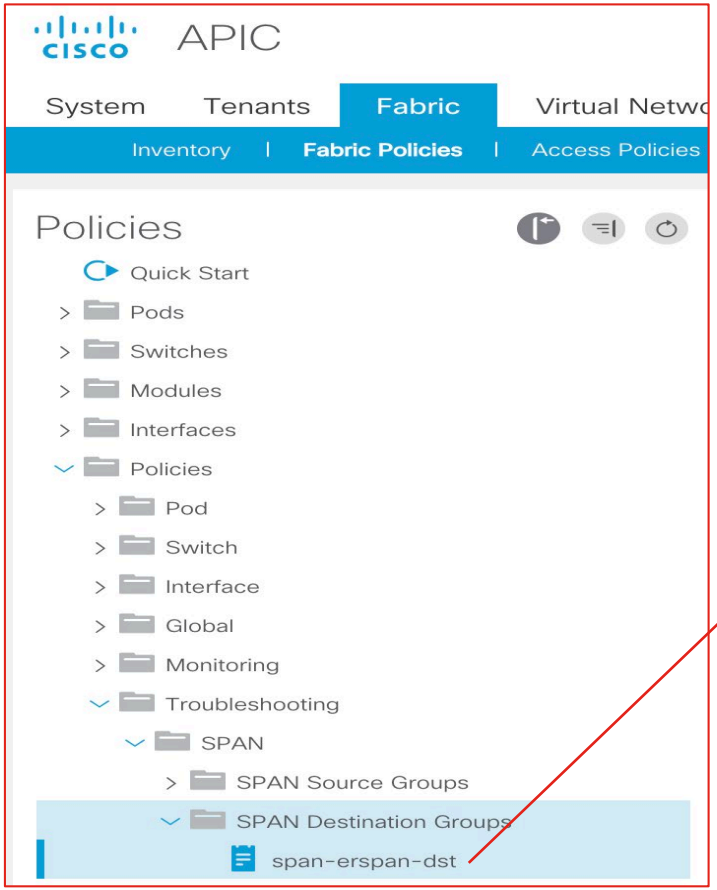


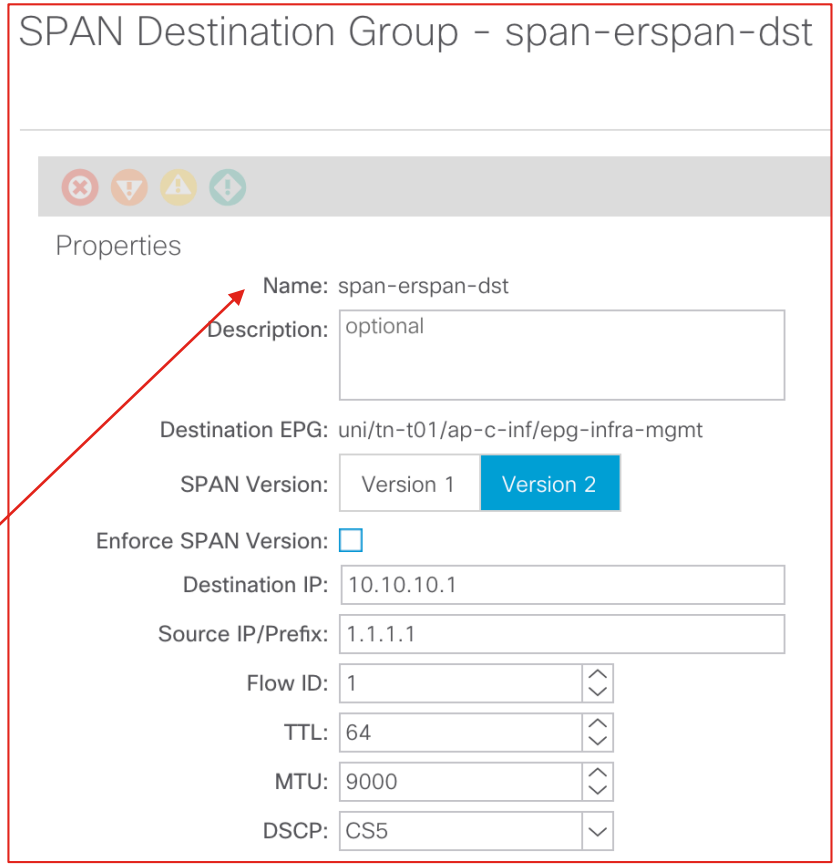
Fault

Fault F1561 raised if IP address does not match Border Leaf transport address connecting to external router.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

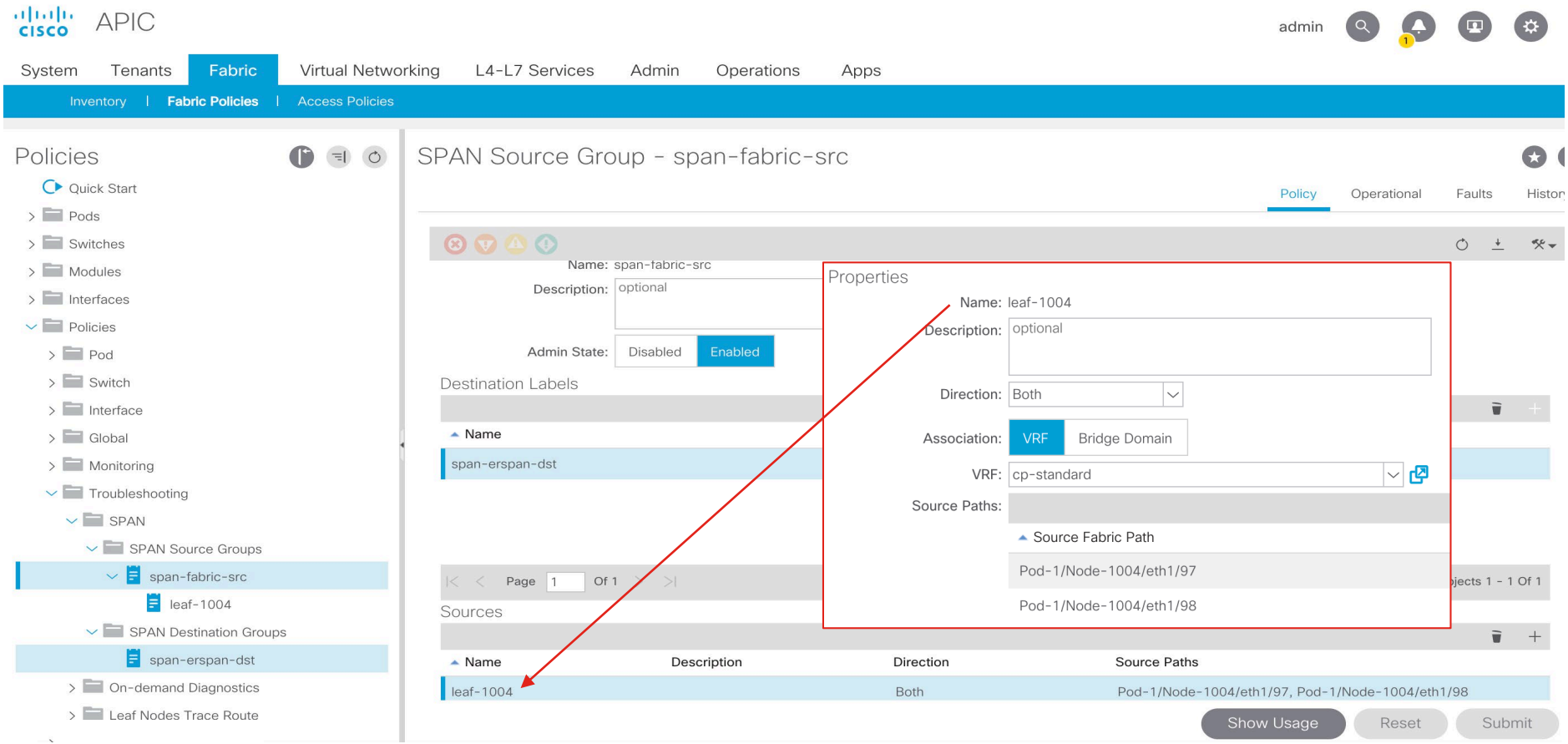
Fabric SPAN (Destination)





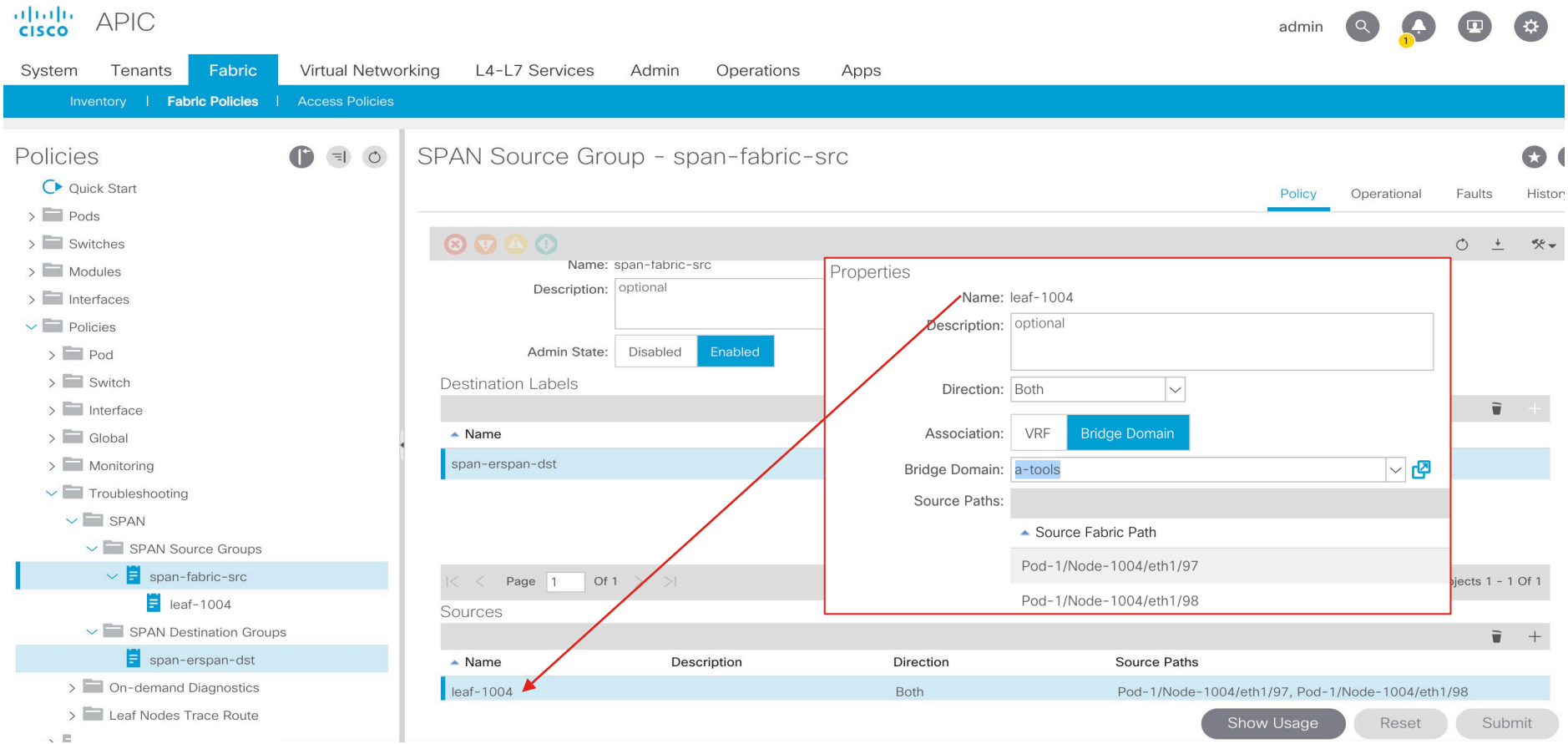
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Fabric SPAN (Source – w/Filter VRF)



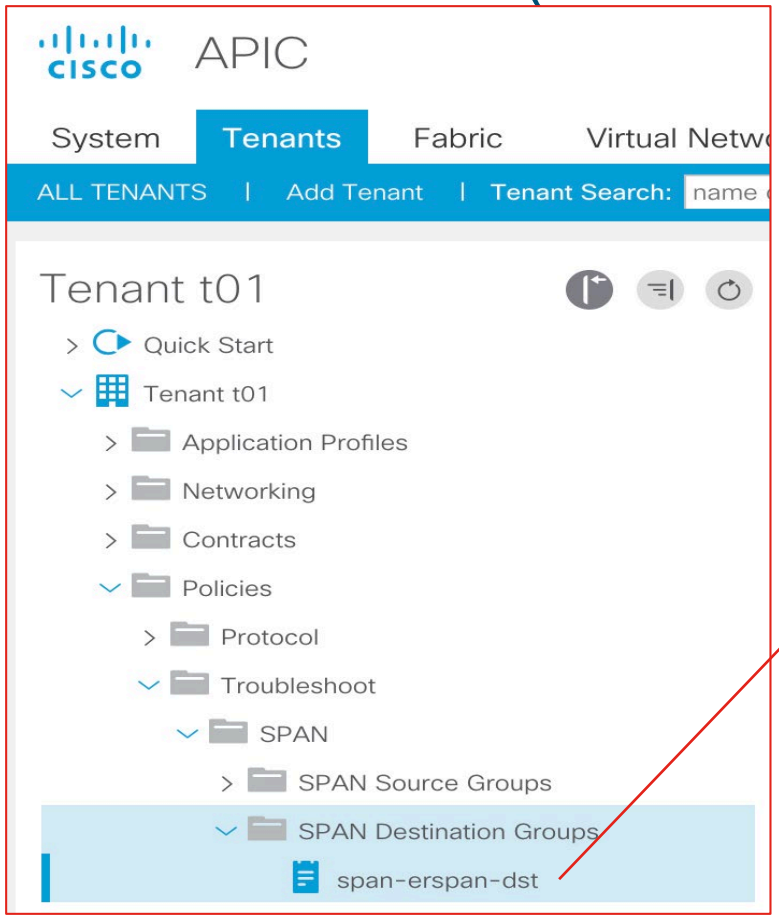
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

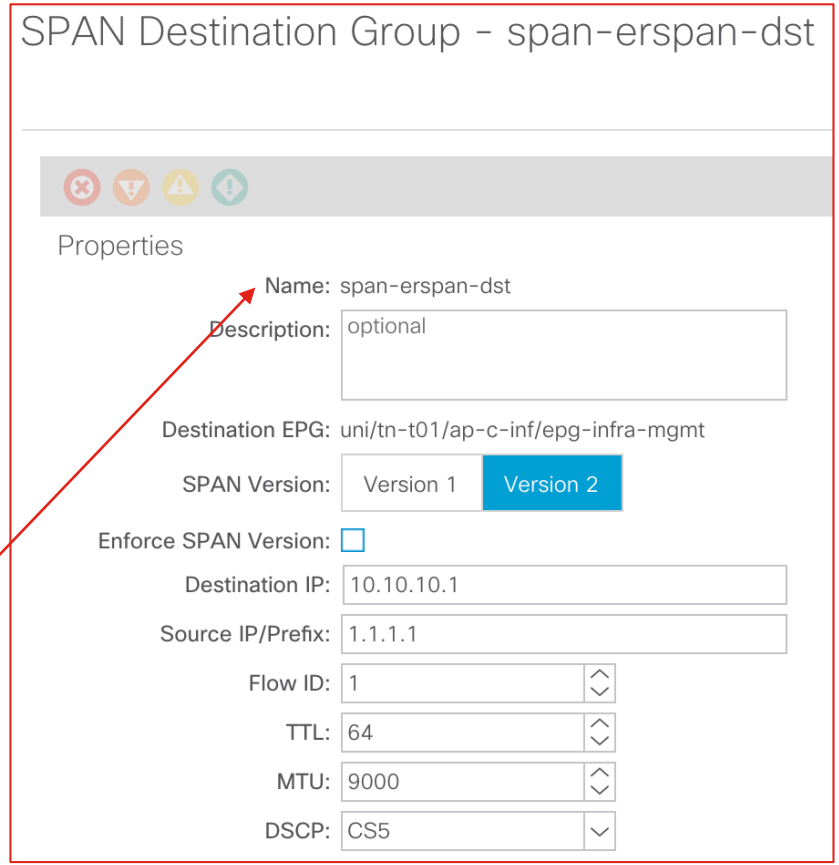
Fabric SPAN (Source – w/Filter Bridge Domain)



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

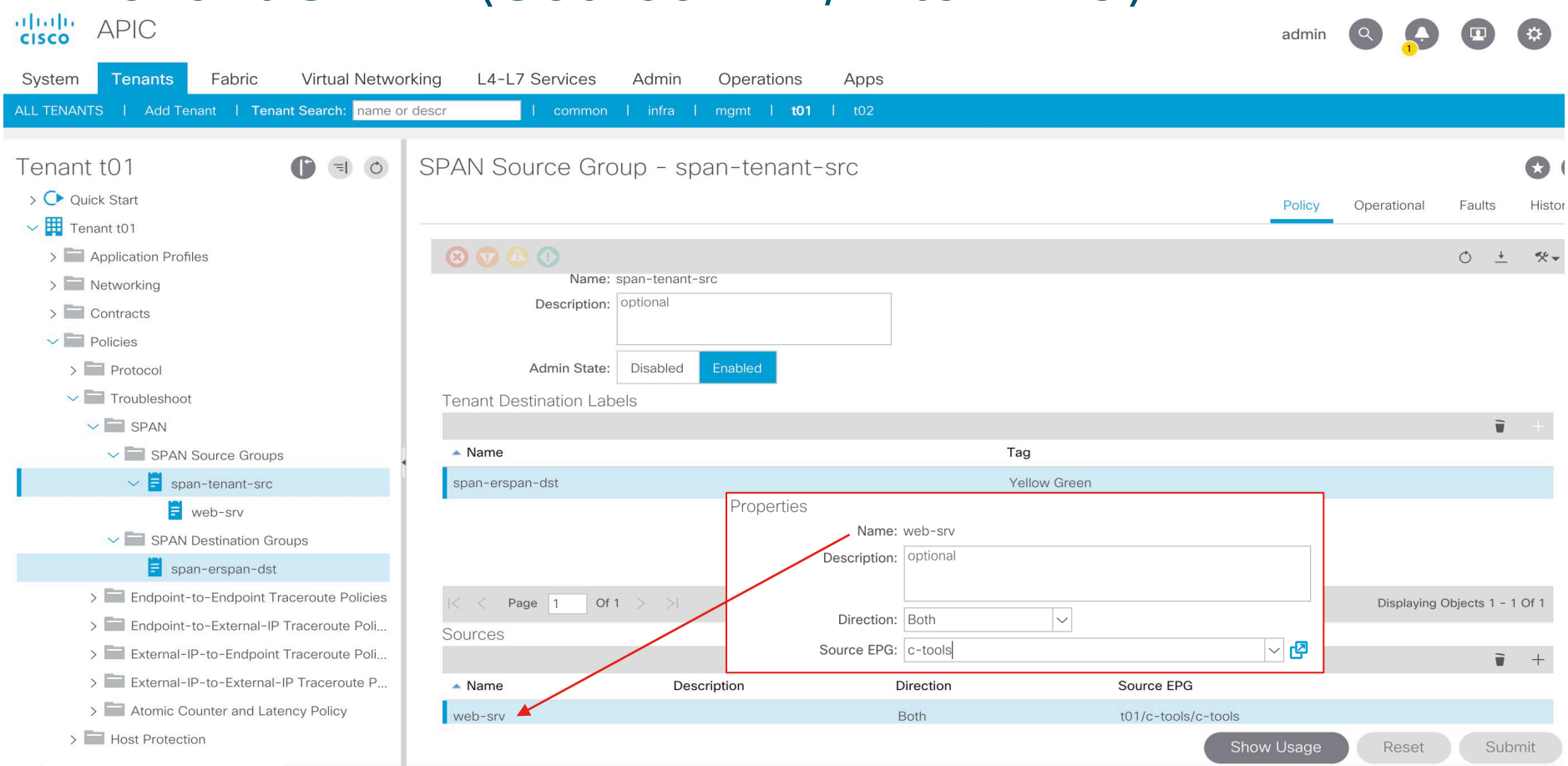
Tenant SPAN (Destination)





© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Tenant SPAN (Source – w/Filter EPG)



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

APIC Show commands

```
APIC2# show monitor access session leaf3
Type           : access
Session        : leaf3  *** Session not created by CLI ***
Node           : 303
Type           : local
Admin state    : enabled
Oper state     : up (active)
Dest Interface : eth1/21

 Interface/Vlan/Vxlan    State   State Qualifier   Dir     Encap/BdEncap
FabEncap/CtxEncap
 ----------------------  ------  ----------------  ------  --------------------  ---
-----------------
po2                     up      active            both    vlan-811
vxlan-15564700
```


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Leaf Show commands

```
Leaf3# show monitor session all
   session 3
---------------
description       : Span session 3
type              : local
state             : up (active)
mode              : access
source intf       :
    rx            : Po2
    tx            : Po2
    both          : Po2
source VLANs      :
    rx            :
    tx            :
    both          :
filter VLANs      : 76
filter L3Outs     : vlan74
destination ports : Eth1/21
```


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Netflow

Netflow Overview

- Netflow is a method of caching flows passing through a router or a switch.
- These flows can then be exported out to a Netflow Collector.
- Netflow data is used for:
  - Bandwidth Monitoring
  - Isolating application slowness
  - Cyber threat forensics
  - Network usage billing
- Netflow components are:
  - Monitor
  - Exporter
  - Collector

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Netflow Support in ACI

- Netflow is supported starting from ACI code 2.2(1) release on Gen-2 cloud-scale platform.
  - EX Leaf 2.2(1) release
  - FX Leaf 2.3(1) release
  - Remote Leaf 4.0(1) release
- Nexus 9300 cloud-scale leaf platform can be configured in either:
  - Analytics Mode (Default) ⟹ Cisco Tetration Analytics
  - Netflow Mode ⟹ Netflow Collector
- Netflow Policies can be configured under:
  - Access Policies (Leaf downlink ports - access, vpc, port-channel).
  - Tenant Policies (Bridge Domain, L3Out)
- Netflow is *NOT* supported on spine switches

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Netflow Support in ACI

- Netflow can be enable on VMWare DVS if integrated with ACI (in-band management is required)
- Netflow *ONLY* supports Exporter version 9
- Netflow in ACI does *NOT* support active/inactive timers. Flow records are exported to collectors every 1 minute.
- The filter TCAM has no labels for bridge domain or interfaces. If a NetFlow monitor is added to 2 bridge domains, the NetFlow monitor uses 2 rules for IPv4, or 8 rules for IPv6. As such, the scale is very limited with the 1K filter TCAM.

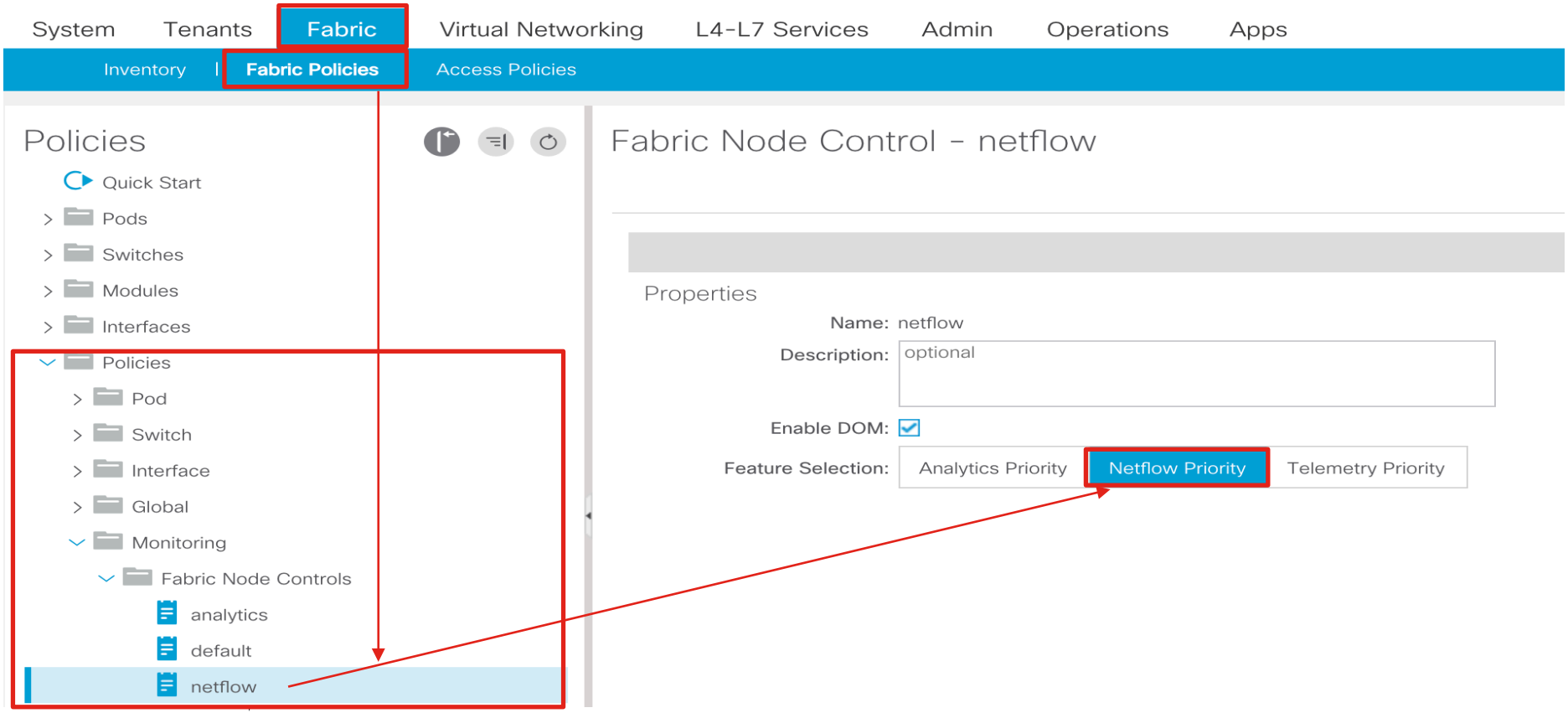
For more details ….

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/kb/b_KB_Cisco_APIC_and_NetFlow.html

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

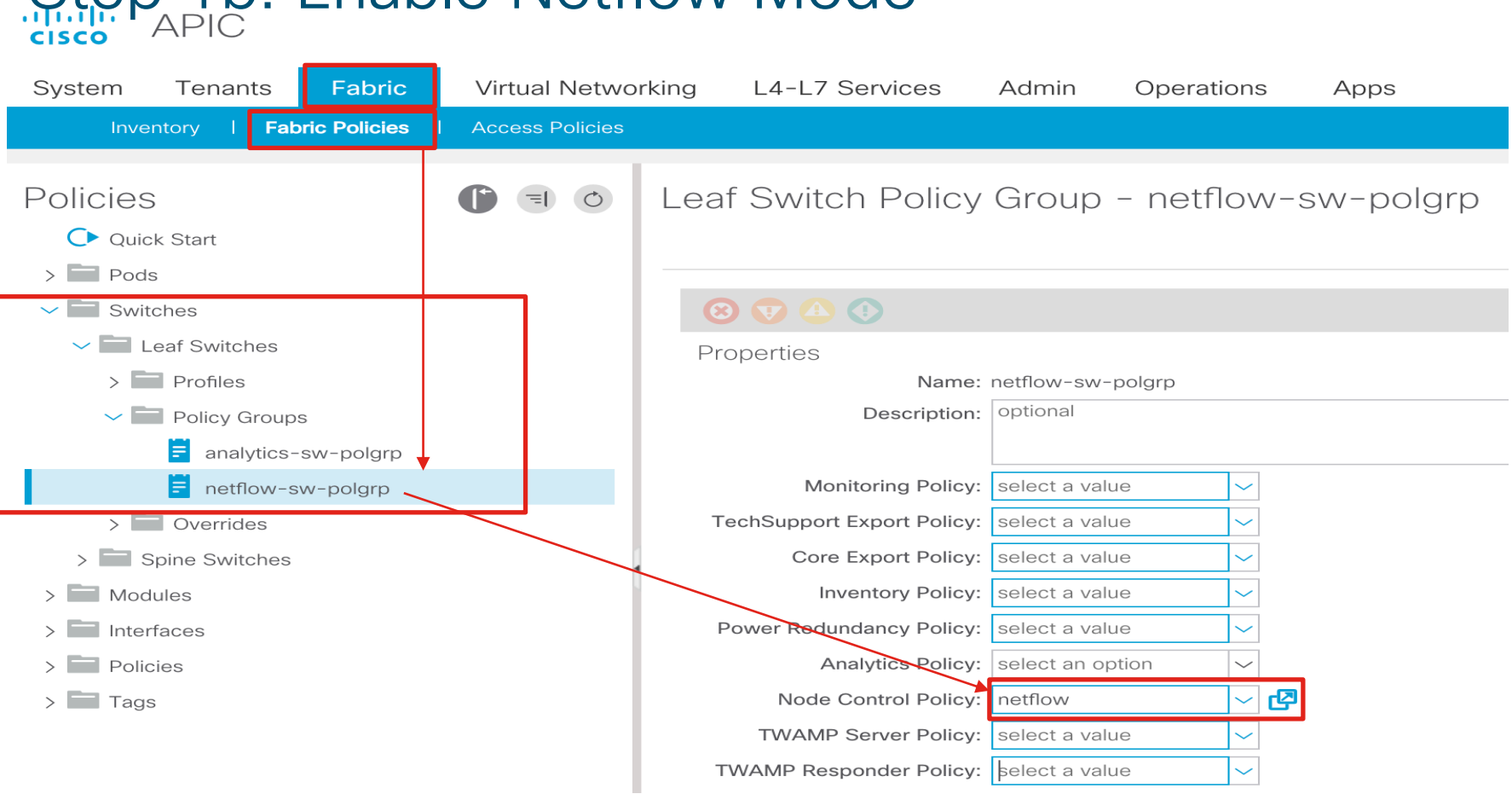
Netflow Configuration

Step 1a: Enable Netflow Mode



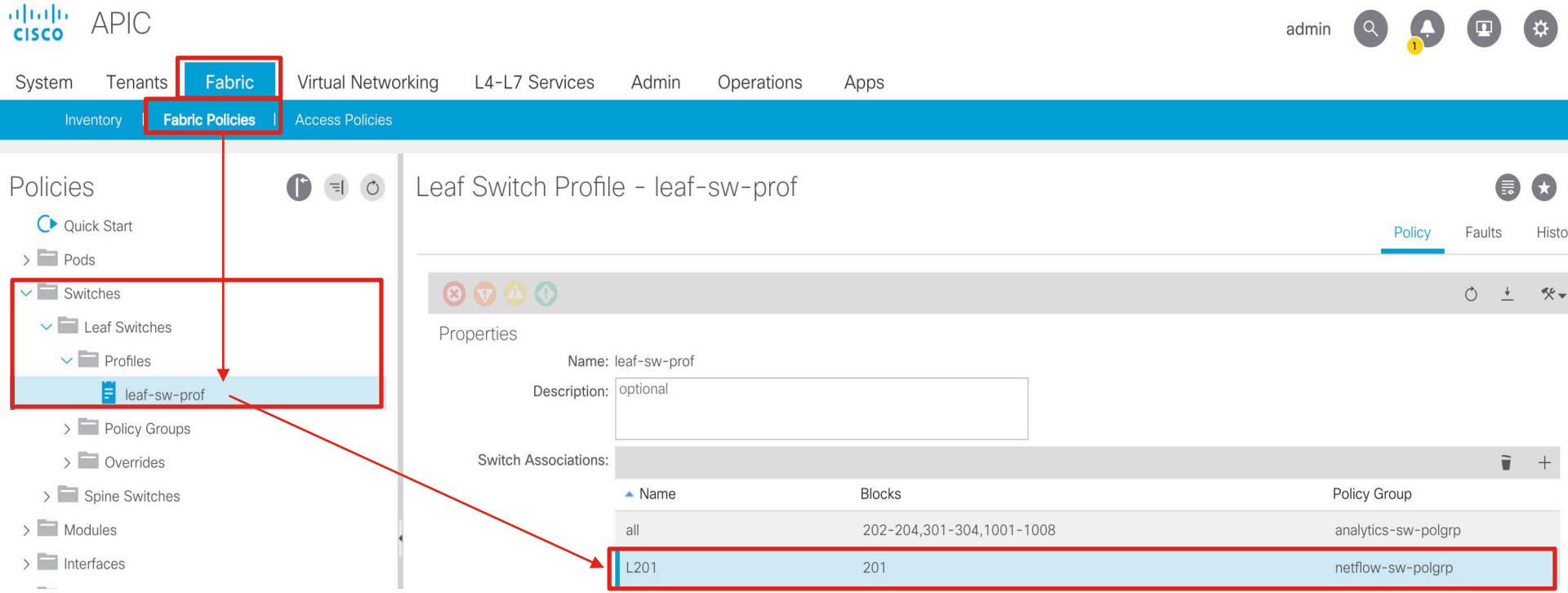
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Step 1b: Enable Netflow Mode



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Step 1c: Enable Netflow Mode



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Step 2a: Define Netflow under Access Policies

APIC

System | Tenants | **Fabric** | Virtual Networking | L4-L7 Services | Admin | Operations | Apps

Inventory | Fabric Policies | **Access Policies**

Policies

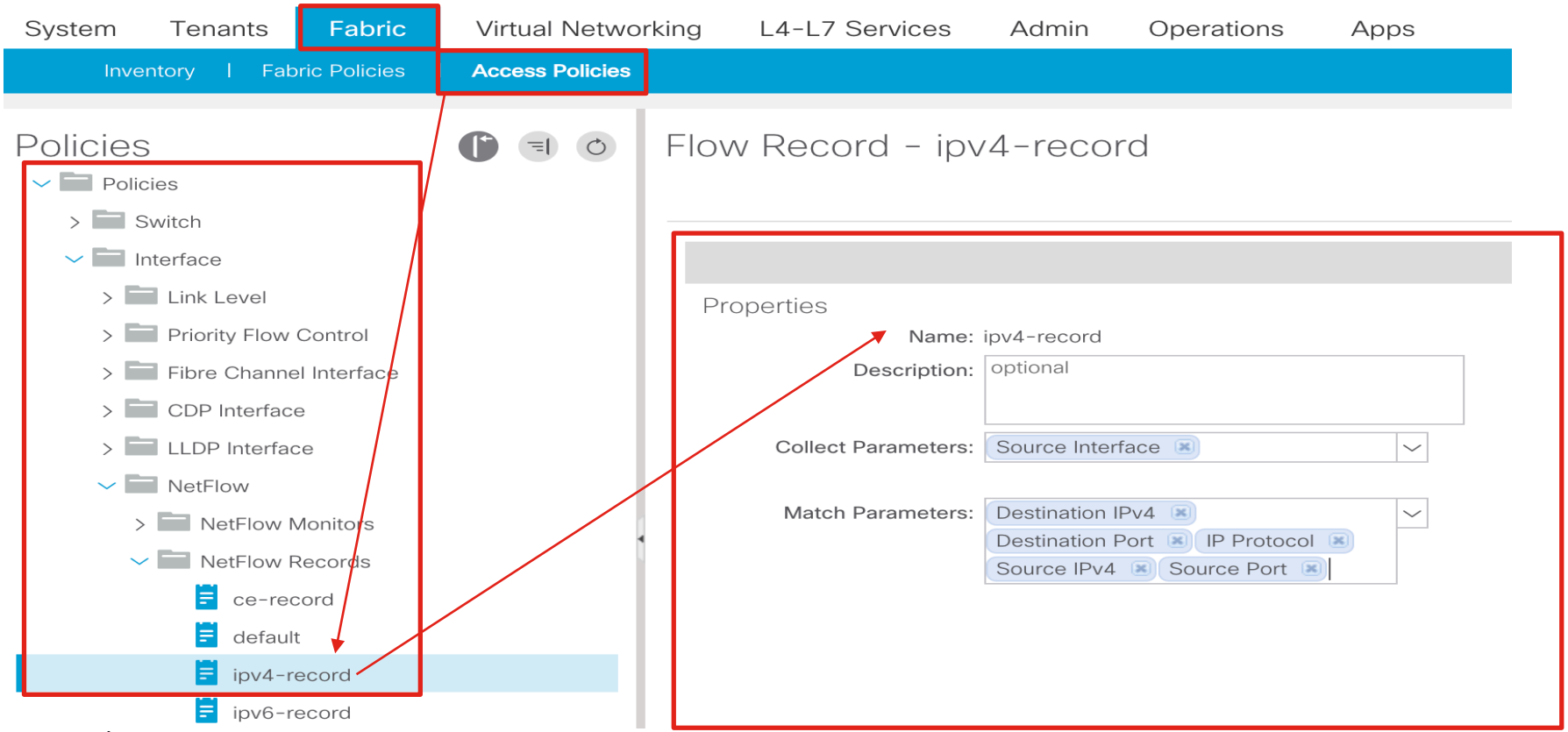
- Quick Start
- Switches
- Modules
- Interfaces
- Policies
  - Switch
    - Spanning Tree
    - Fibre Channel Node
    - Fibre Channel SAN
    - CoPP Spine
    - CoPP Leaf
    - Virtual Port Channel default
    - VPC Domain
    - BFD
    - NetFlow Node
      - default

NetFlow Node Policies

Name	Stats Collect Interval (s)	Stats Template Interval (s)
default	60	300

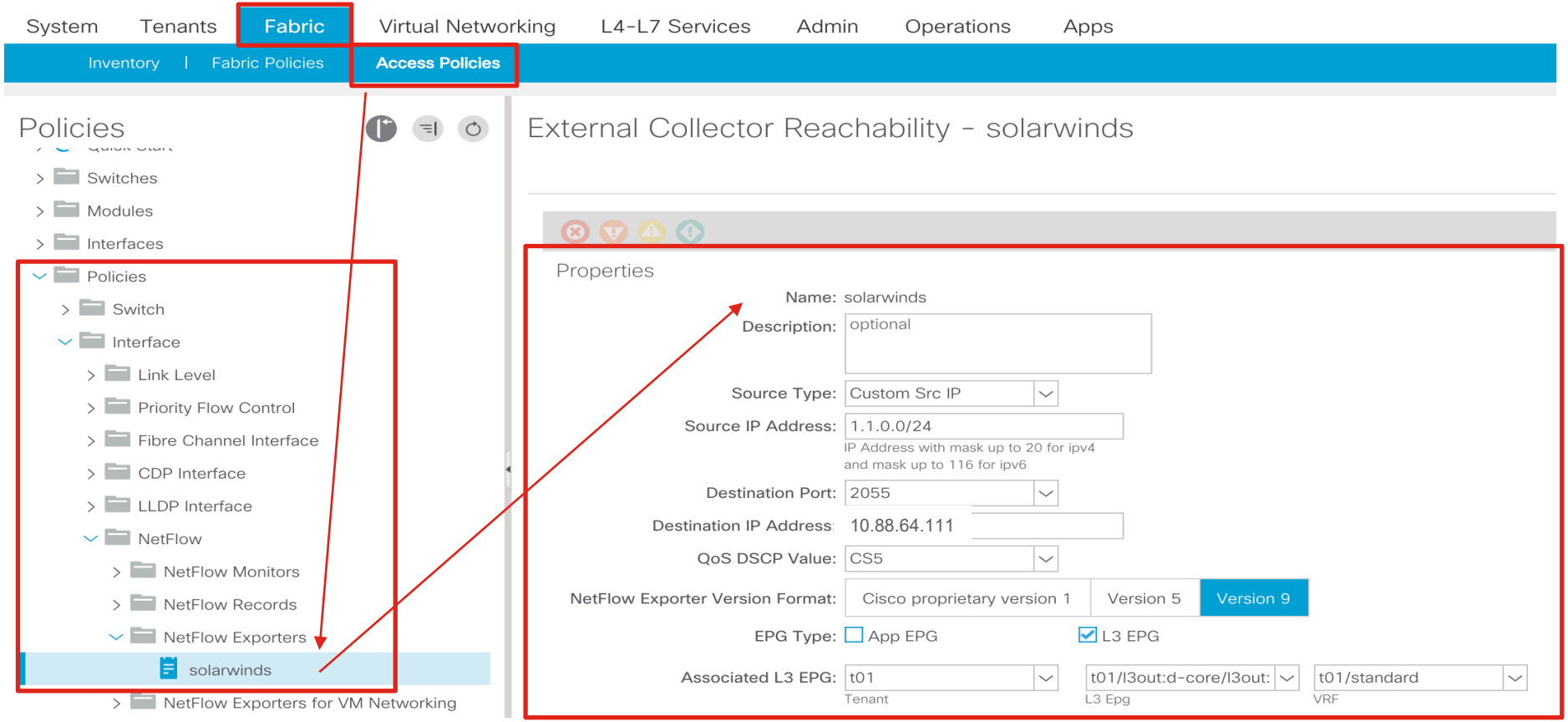
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Step 2b: Define Netflow under Access Policies



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

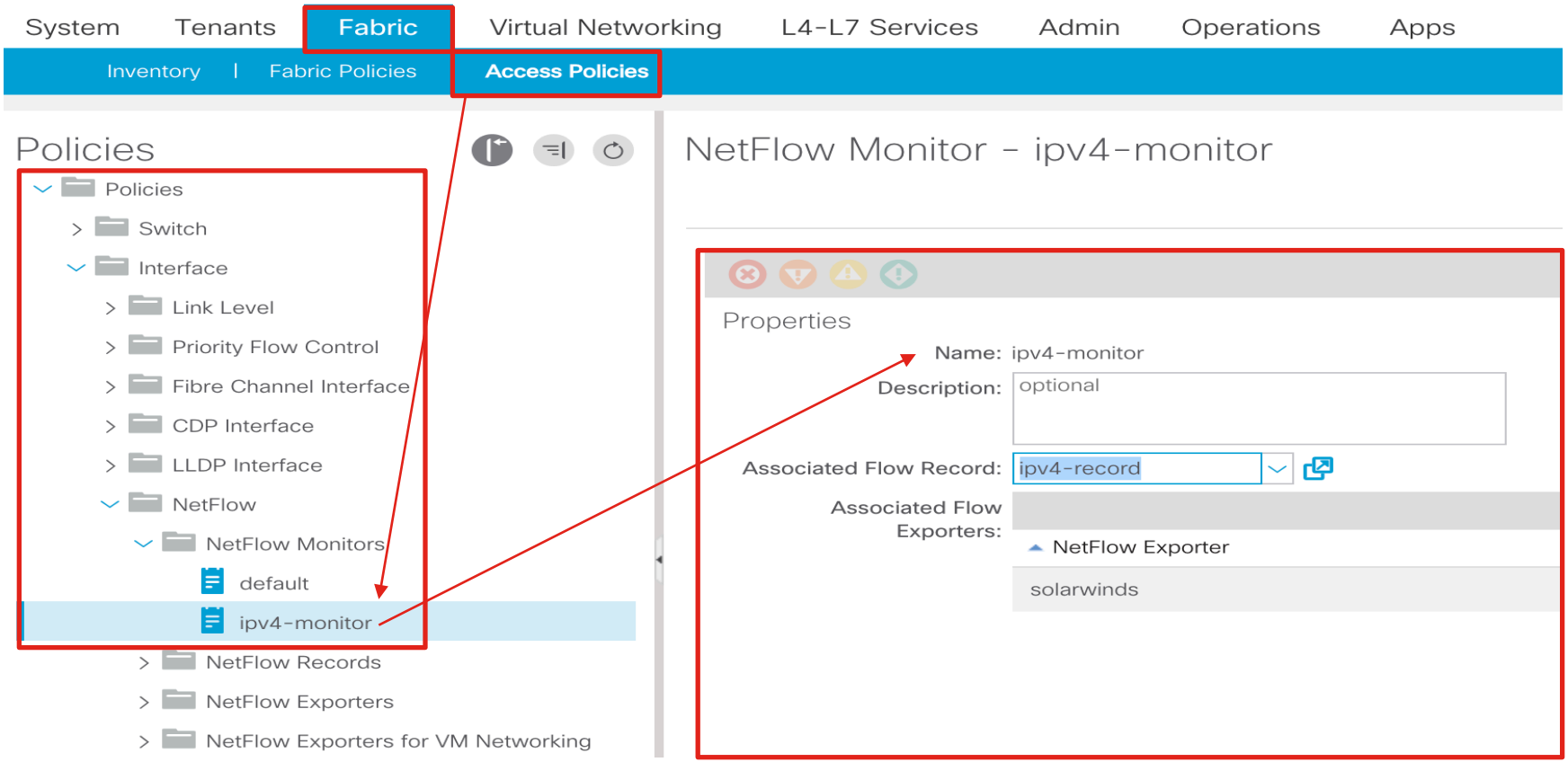
Step 2c: Define Netflow under Access Policies



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

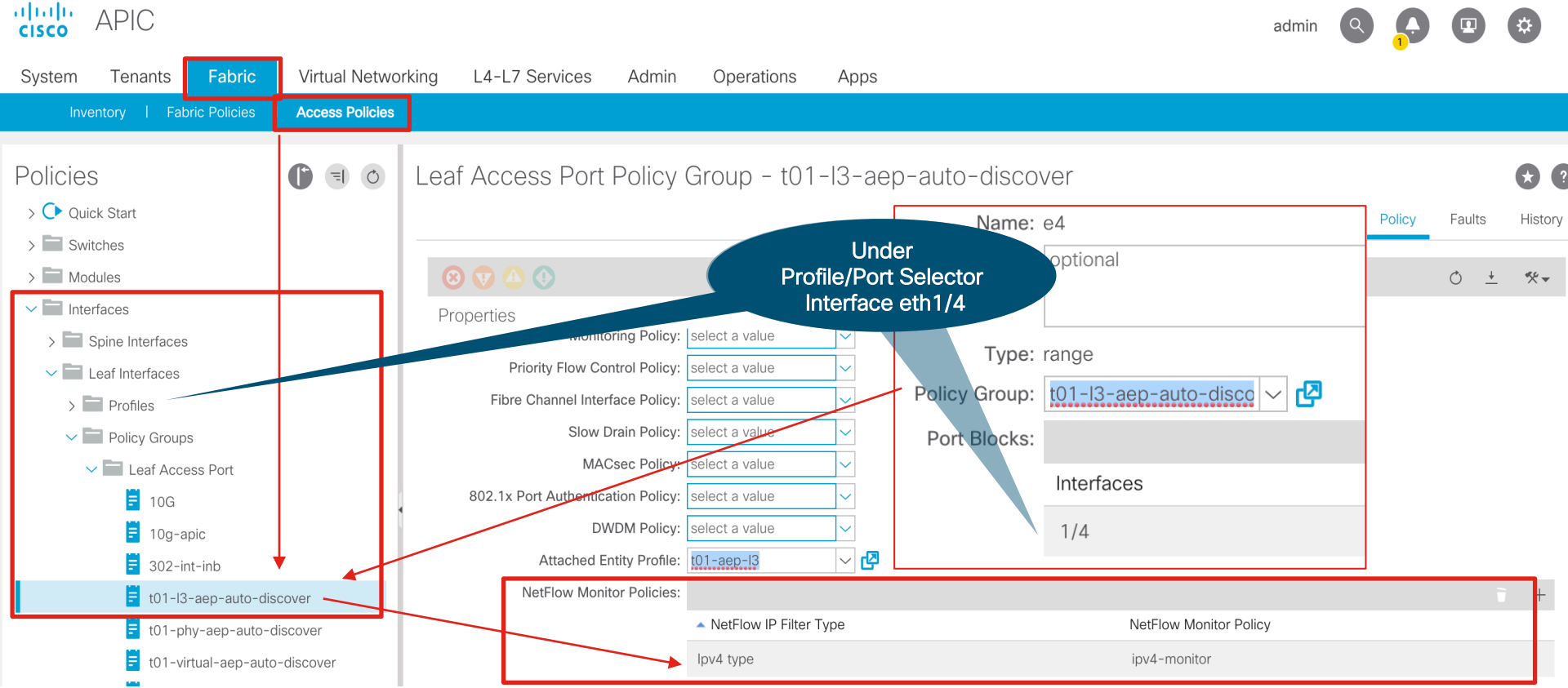
Step 2d: Define Netflow under Access Policies

APIC



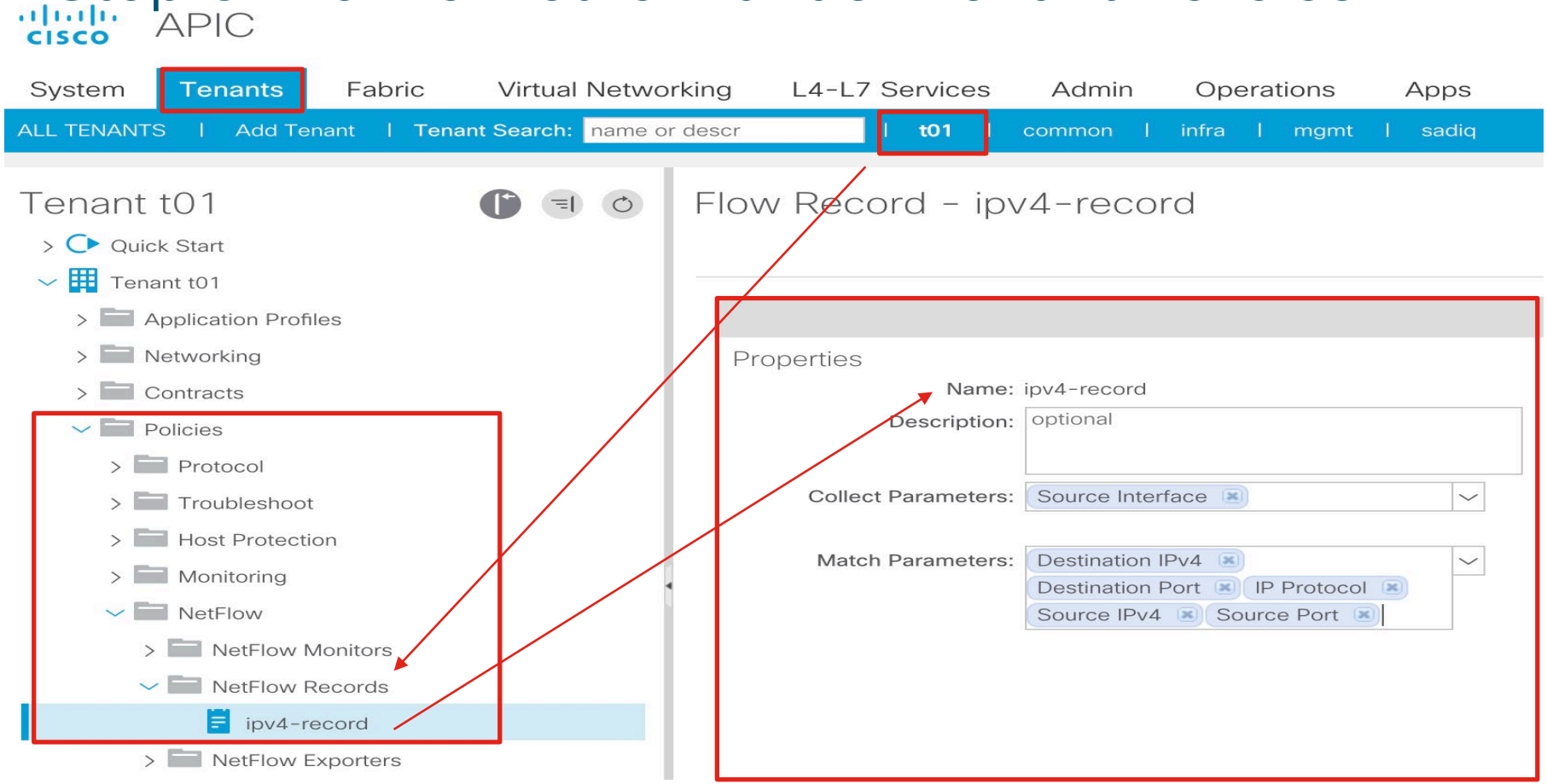
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Step 2e: Define Netflow under Access Policies



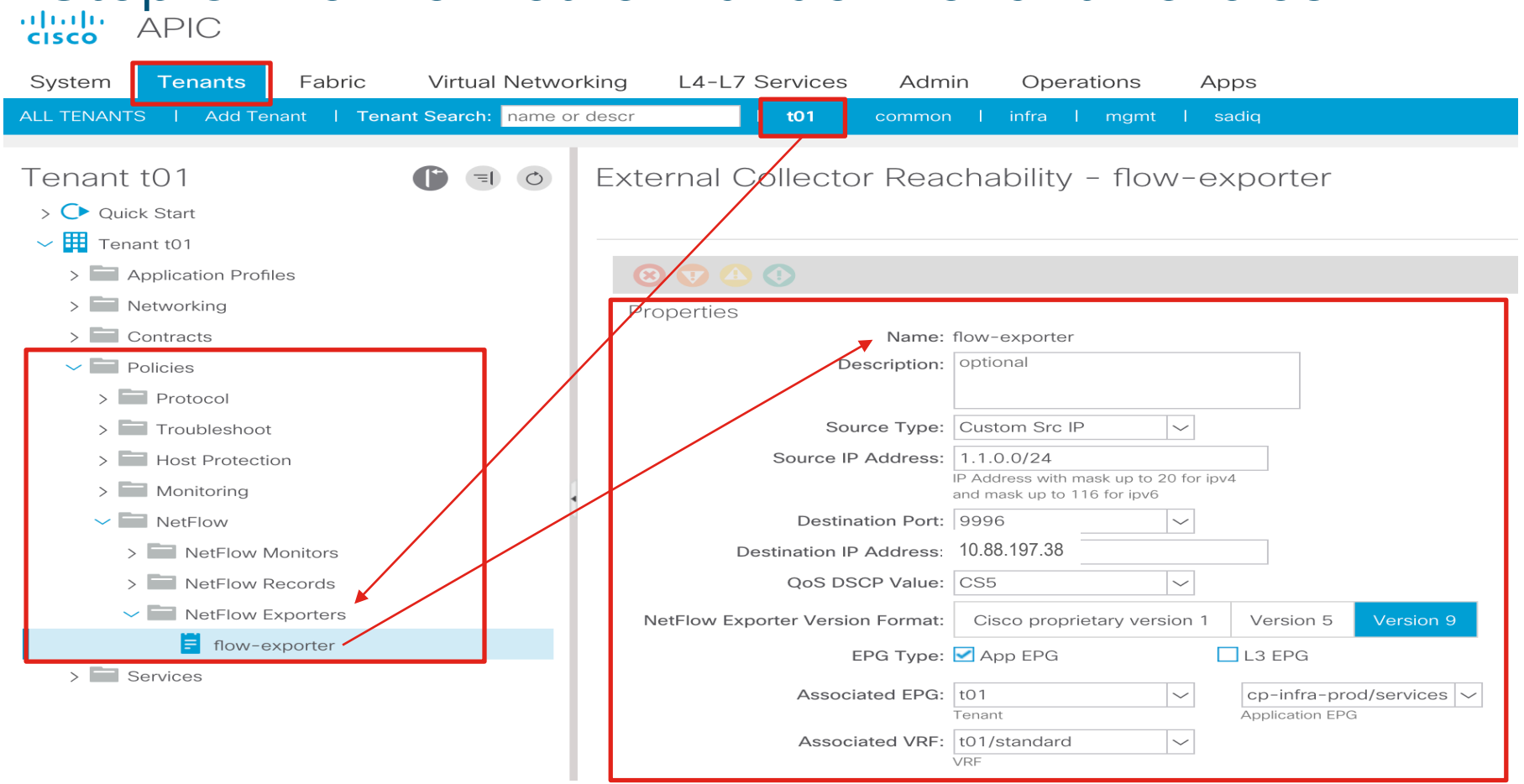
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Step 3: Define Netflow under Tenant Policies



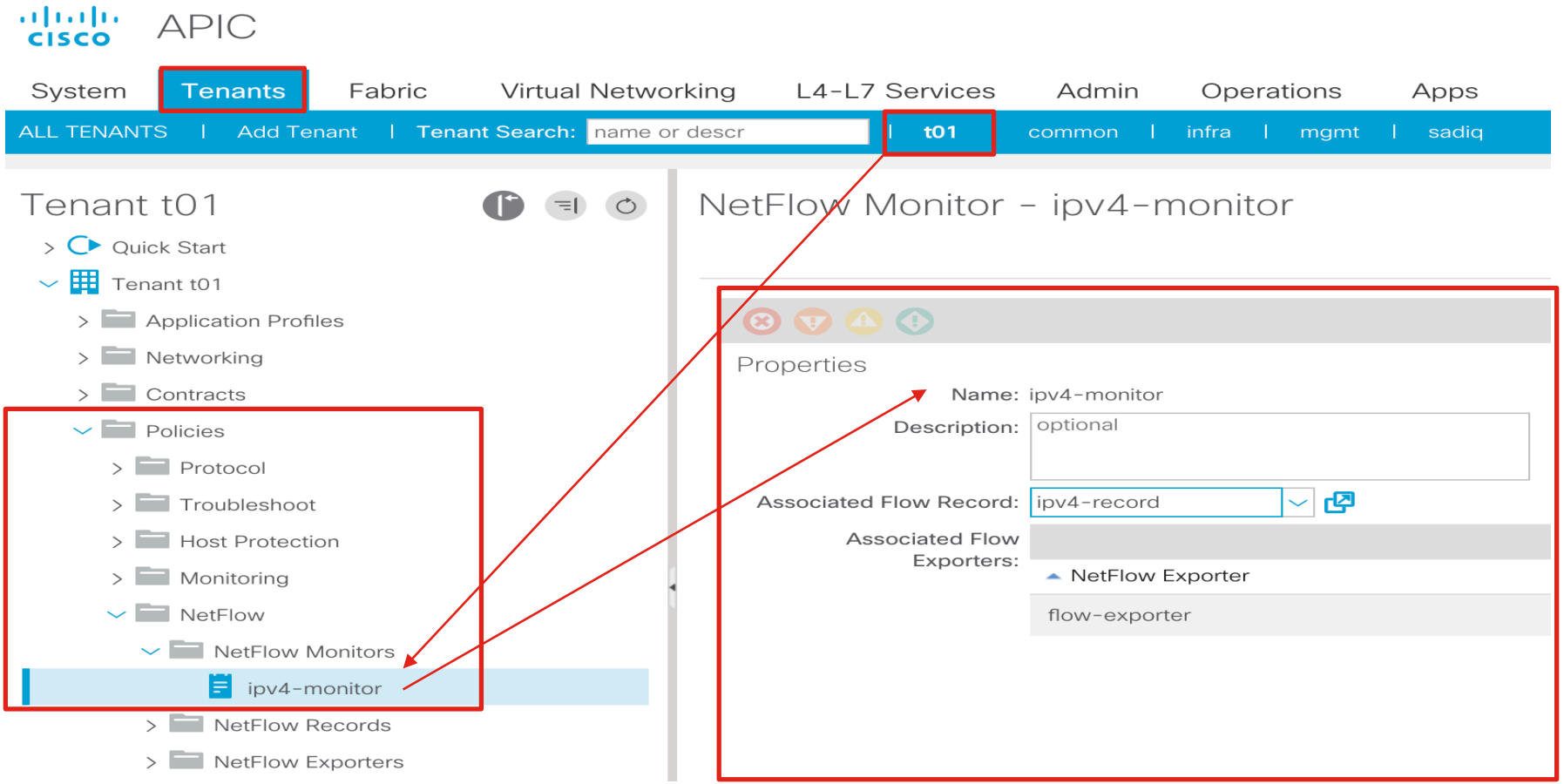
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Step 3: Define Netflow under Tenant Policies



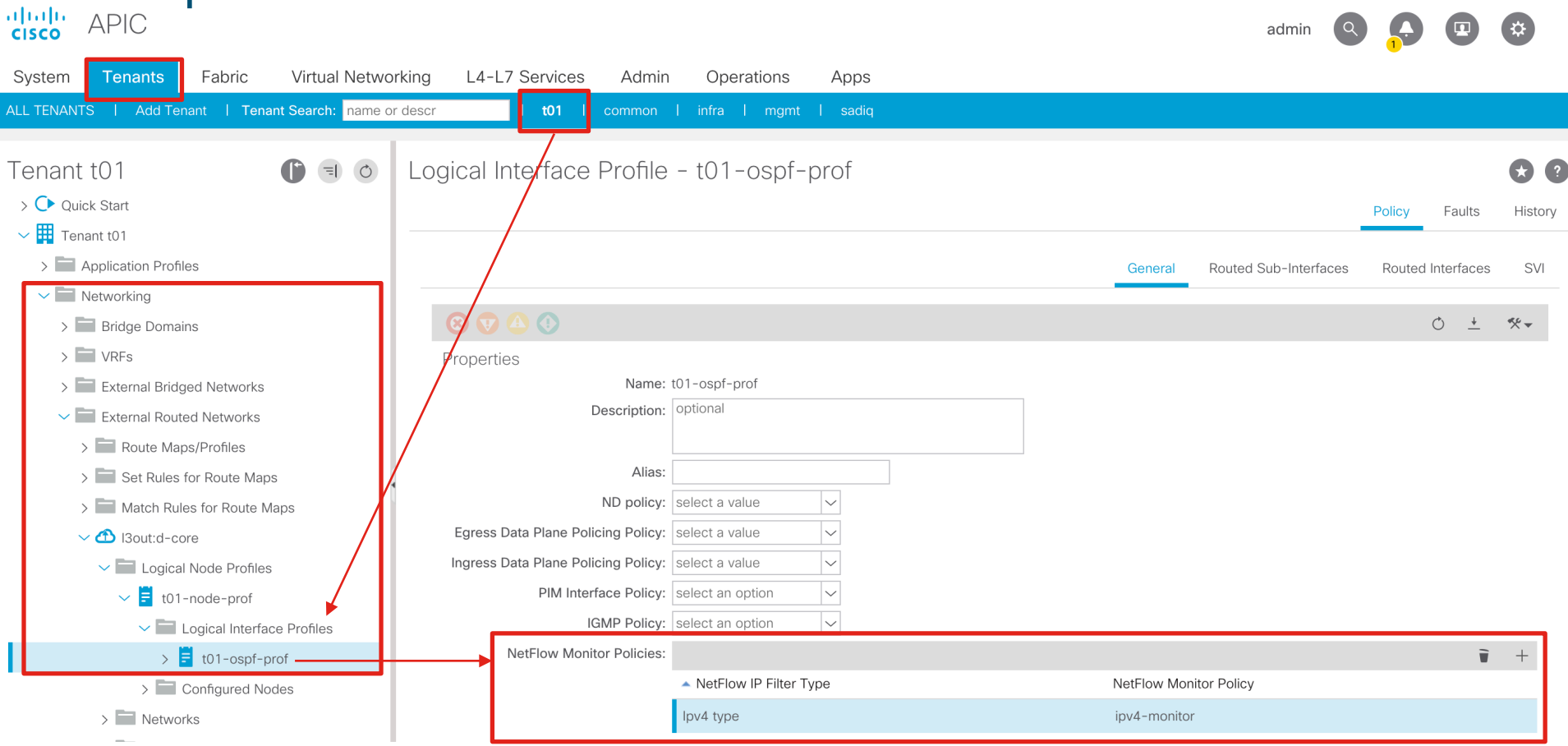
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Step 3: Define Netflow under Tenant Policies



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Step 3: Define Netflow under Tenant Policies



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Verify Netflow status

```
tcsh1-f02-b0201# show flow cache ipv4
IPV4 Entries
SIP             DIP             BD ID   S-Port   D-Port   Protocol  Byte Count       Packet Count     TCP FLAGS  if_id       flowStart
10.88.146.51    10.88.197.48    4611    53       37779    17        144              1                0x0        0x1a003000  28365088  283650
10.88.150.154   2.2.2.2         4611    28570    1967     17        98               1                0x0        0x1a003000  28367890  283678
10.88.144.73    10.88.197.53    4611    5640     59228    6         70               1                0x10       0x1a003000  28365680  283656
10.88.194.7     10.88.193.14    4611    58282    4353     6         10456            98               0x18       0x1a003000  28365917  283675
```

tcsh1-f02-b0201# **show flow exporter**
Flow exporter **solarwinds**:
- Destination: 10.86.84.111
- VRF: t01:standard (1)
- Destination UDP Port 2055
- Source: 1.1.0.201
- DSCP 40
- Export Version 9
  - Sequence number 2656
  - Data template timeout 0 seconds
- Exporter Statistics
  - Number of Flow Records Exported **8582**
  - Number of Templates Exported **9**
  - Number of Export Packets Sent **255**
  - Number of Export Bytes Sent **349040**
  - Number of Destination Unreachable Events 0
  - Number of No Buffer Events 0
  - Number of Packets Dropped (No Route to Host) 0
  - Number of Packets Dropped (other) 0
  - Number of Packets Dropped (Output Drops) 0
  - Time statistics were last cleared: Never

Feature Prio: Netflow

tcsh1-f02-b0201# **show flow exporter**
Flow exporter t01:**flow-exporter**:
- Destination: 10.88.197.38
- VRF: t01:standard (1)
- Destination UDP Port 9996
- Source: 1.1.0.201
- DSCP 44
- Export Version 9
  - Sequence number 895
  - Data template timeout 0 seconds
- Exporter Statistics
  - Number of Flow Records Exported **30240**
  - Number of Templates Exported **30**
  - Number of Export Packets Sent **895**
  - Number of Export Bytes Sent **1229700**
  - Number of Destination Unreachable Events 0
  - Number of No Buffer Events 0
  - Number of Packets Dropped (No Route to Host) 0
  - Number of Packets Dropped (other) 0
  - Number of Packets Dropped (Output Drops) 0
  - Time statistics were last cleared: Never

Feature Prio: Netflow

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Verify Netflow status

```
tcsh1-f02-b0201# show interface snmp-ifindex
-----------------------------------------------
Port          IFMIB Ifindex (hex)
-----------------------------------------------
mgmt0          83886080  (0x05000000)
Eth1/1         436207616 (0x1a000000)
Eth1/2         436211712 (0x1a001000)
Eth1/3         436215808 (0x1a002000)
Eth1/4         436219904 (0x1a003000)
```

NetFlow Analyzer

License will expire in 29 days | Get Quote | Purchase

Dashboard | Inventory | WLC | Attacks | DPI | NCM | IPSLA | Alarms | Maps

Overview | Apps | Qos | WAN Monitors | WLC

Top N Interfaces by Speed

Hourly Report

Device IP	Interface Name	Speed IN	Speed Out
1.1.0.201	IfIndex436219904	100.634 Kbps	0.00 bps

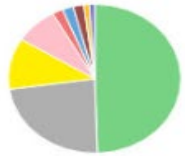
Top N Interfaces by Utilization

Hourly Report

Device IP	Interface Name	Utilization IN	Utilization Out
1.1.0.201	IfIndex436219904	10 %	0 %

Top N Application

Hourly Report



- https -- 19.346 MB
- f5-iquery -- 4.419 MB
- domain -- 961.762 KB
- http -- 747.512 KB
- icmp -- 334.546 KB
- mit-ml-dev -- 9.063 MB
- gsmtap -- 3.111 MB
- Unknown_App -- 790.354 KB
- glrpc -- 346.568 KB
- ssh -- 42.205 KB

Top N Devices by Speed

Hourly Report

Device Name	Speed	Avg Speed
1.1.0.201(1.1.0.201)	310.032 Kbps	112.585 Kbps

Top N IP Groups by Utilization

Hourly Report

IPGroup Name	Utilization IN	Utilization Out
Mail Sites	0 %	0 %
Social Network Sites	0 %	0 %

Activate Windows
Go to Settings to activate Windows.

REST API

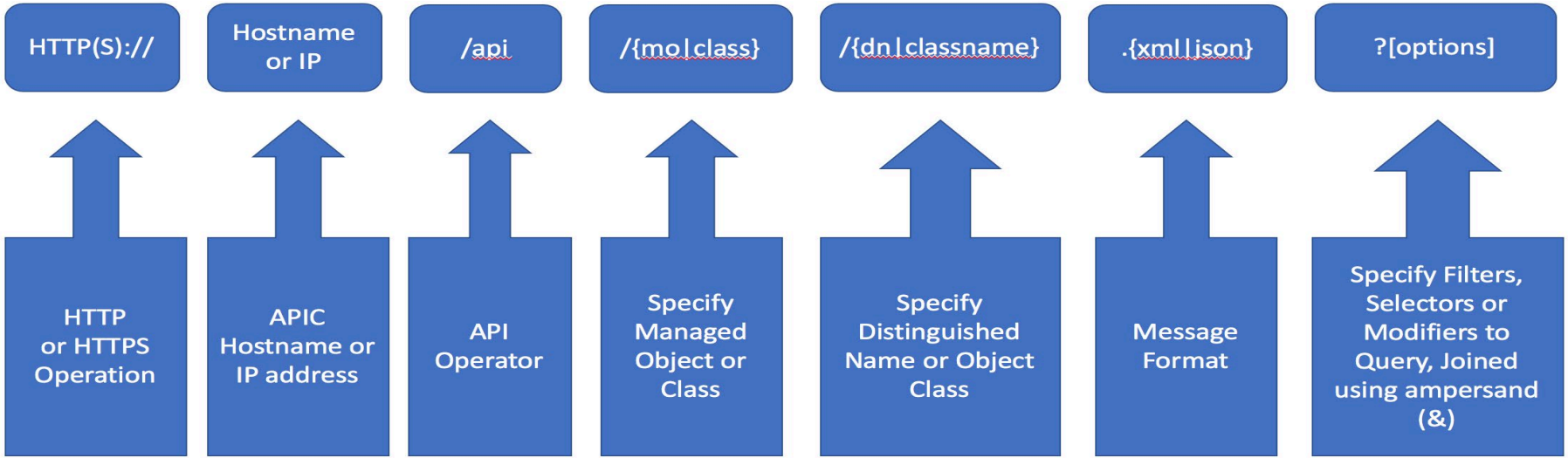
Monitoring Using REST API

- REpresentational State Transfer or **REST** is client server communication method based on HTTP or HTTPS protocol
- Client makes a resource request to Server and in response Server transfer the representation state of the requested resource
- The messages that gets transferred between client and server contains JavaScript Object Notation (JSON) or Extensible Markup Language (XML) format documents
- Lightweight on managed devices as compared to other monitoring protocols
- APIC also stores fabric wide statistical data that makes REST an ideal interface for monitoring as well.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Monitoring Using REST API

- Monitoring ACI using REST is a pull method where data is retrieved from APIC
- Requires read-only GET operation
- URL Format for a typical REST call



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Monitoring Using REST API

- Resource Path changes with the type of MO or Object Class query
  - For Policy Based Managed Object MO such as Tenant, App Prof, EPG etc. query

    /api/mo/uni/tn-*tenant_name*/.....

  - For Node Based Managed Object MO such as Node Chassis, LC, FM, Interface etc. query

    /api/mo/topology/pod-*number*/node-*number*/sys/.....

  - Retrieving an Object Class information

    /api/class/....

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Monitoring Using REST API

- REST offers wide range of filtering options to narrow down the query

Filter Type	Syntax	Cobra Query Property	Description
query-target	{self | children | subtree}	AbstractQuery.queryTarget	Define the scope of a query
target-subtree-class	*class name*	AbstractQuery.classFilter	Respond-only elements including the specified class
query-target-filter	*filter expressions*	AbstractQuery.propFilter	Respond-only elements matching conditions
rsp-subtree	{no | children | full}	AbstractQuery.subtree	Specifies child object level included in the response
rsp-subtree-class	*class name*	AbstractQuery.subtreeClassFilter	Respond only specified classes
rsp-subtree-filter	*filter expressions*	AbstractQuery.subtreePropFilter	Respond only classes matching conditions
rsp-subtree-include	{faults | health :stats : ...}	AbstractQuery.subtreeInclude	Request additional objects
order-by	*classname.property* | {asc | desc}	Not Implemented	Sort the response based on the property values

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Monitoring Using REST API

- REST Filters can be applied in URI with a (?) symbol.
- Multiple Filters can be joined with (&) symbol

Example:

GET → https://{{apic-host-or-ip}}/api/mo/*topology/pod-1/node-1001/sys*.json?query-target=children&target-subtree-class=*eqptCh*

For more information :

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/rest-api-config/Cisco-APIC-REST-API-Configuration-Guide-401/Cisco-APIC-REST-API-Configuration-Guide-401_chapter_0110.pdf

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Important REST Queries (APIC)

- Monitoring CPU and Memory

  GET → https://{{apic-host-or-ip}}/api/class/procEntity.json

- Monitoring Disk Utilization

  GET → https://{{apic-host-or-ip}}/api/class/eqptStorage.json

- Monitoring Interfaces

  GET → https://{{apic-host-or-ip}}/api/mo/topology/pod-1/node-1/sys.json?query-target=subtree&target-subtree-class=l3EncRtdIf

- Monitoring APIC Cluster State

  GET → https://{{apic-host-or-ip}}/api/mo/topology/pod-1/node-1/sys.json

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Important REST Queries (Leafs/Spines)

- Monitoring CPU Utilization

  GET → https://{{apic-host-or-ip}}/api/class/procSysCPU1h.json

procSysCPU5min	procSysCPU15min	procSysCPU1h	procSysCPU1d
procSysCPU1w	procSysCPU1mo	procSysCPU1qtr	procSysCPU1year

- Monitoring Memory Utilization

  GET → https://{{apic-host-or-ip}}/api/class/procSysMem1h.json

procSysMem5min	procSysMem15min	procSysMem1h	procSysMem1d
procSysMem1w	procSysMem1mo	procSysMem1qtr	procSysMem1year

- Monitoring Power Supply Units (PSU)

  GET → https://{{apic-host-or-ip}}/api/mo/topology/pod-1/node-201/sys/ch/psuslot-1.json

- Monitoring FAN

  GET → https://{{apic-host-or-ip}}/api/mo/topology/pod-1/node-201/sys ch/ftslot-1.json

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Important REST Queries (Leafs/Spines)

- Monitoring SUP

  GET → https://{{apic-host-or-ip}}/api/mo/topology/pod-1/node-101/sys/ch/supslot-1/sup.json

- Monitoring Line Card

  GET → https://{{apic-host-or-ip}}/api/mo/topology/pod-1/node-101/sys/ch/lcslot-1/lc.json

- Monitoring Fabric Module

  GET → https://{{apic-host-or-ip}}/api/mo/topology/pod-1/node-101/sys/ch/fcslot-1/fc.json

- Monitoring Node Membership

  GET → https://{{apic-host-or-ip}}/api/mo/topology/pod-1/node-202/sys.json

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Important REST Queries (Leafs/Spines)

- Monitoring SUP

  GET → https://{{apic-host-or-ip}}/api/mo/topology/pod-1/node-101/sys/ch/supslot-1/sup.json

- Monitoring Line Card

  GET → https://{{apic-host-or-ip}}/api/mo/topology/pod-1/node-101/sys/ch/lcslot-1/lc.json

- Monitoring Fabric Module

  GET → https://{{apic-host-or-ip}}/api/mo/topology/pod-1/node-101/sys/ch/fcslot-1/fc.json

- Monitoring Single Node Membership

  GET → https://{{apic-host-or-ip}}/api/mo/topology/pod-1/node-202/sys.json

- Monitoring All Node Membership

  GET → https://{{apic-host-or-ip}}/api/mo/topology/pod-1.json?query-target=children&target-subtree-class=fabricNode

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Important REST Queries (Leafs/Spines)

- Monitoring Interface Status

  GET → https://{{apic-host-or-ip}}/api/mo/topology/pod-1/node-202/sys/phys-[eth1/1]/dbgEtherStats.json

- Monitoring Application Traffic (t01 is Tenant, 3-tier is AP, db is EPG)

  GET → https://{{apic-host-or-ip}}/api/mo/uni/tn-t01/ap-3-tier/epg-db.json?query-target=self&rsp-subtree-include=stats

- Monitoring OSPF Peer Adjacency (t01:standard is VRF, Eth1/4 is the port, 20.88.193.130 is peer router ID)

  GET → https://{{apic-host-or-ip}}/api/mo/topology/pod-1/node-202/sys/ospf/inst-default/dom-t01:standard/if-[eth1/4]/adj-20.88.193.130.json?query-target=subtree&target-subtree-class=ospfAdjStats,ospfAdjEp

- Monitoring PBR Service Graph (10.15.250.26 is FW interface IP, 2555904 is VRF VNID)

  GET → https://{{apic-host-or-ip}}/api/mo/topology/pod-1/node-201/sys/svcredir/inst/destgrp-1/rsdestAtt-[topology/pod-1/node-201/sys/svcredir/inst/dest-[10.15.250.26]-[vxlan-2555904]].json

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ACI Built-out Tools

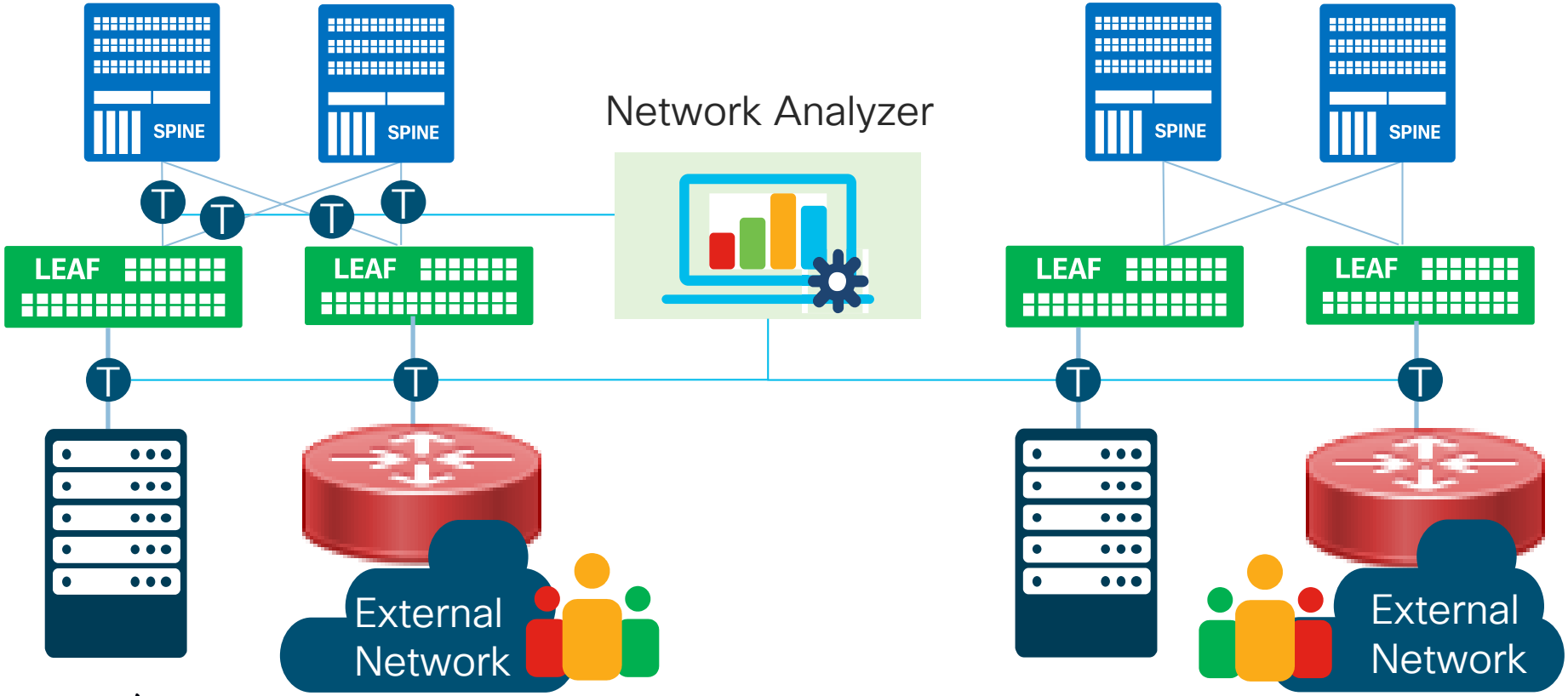
TAP

Test Access Point (TAP)

- TAP is a device in between two network devices connected links
- All traffic flowing between network devices are captured without a potential of loosing data as in the case of SPAN
- No configuration is needed as it is installed inline between network devices on the wire
- TAP is a costly solution than SPAN
- TAP sends the capture data to monitoring tool for further analysis
- TAPs are mainly used for security purposes and also in certain cases for network visibility
- Many network monitor vendors offers the solution with TAPs via 40G BiDi, 40G MM, 40G SM, 100GMM, 100G SM etc

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Test Access Point (TAP) Connection Options



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

TAP Configuration

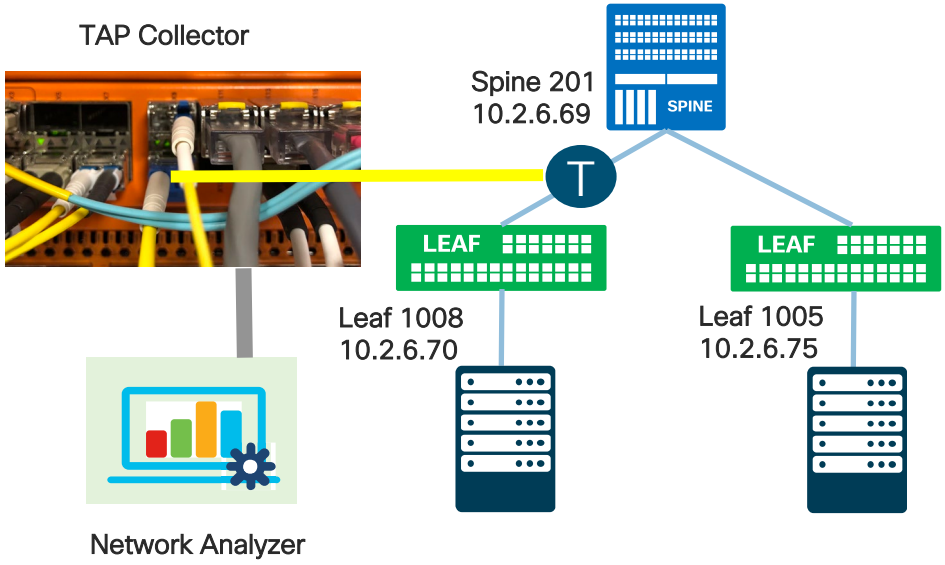
Test Access Point (TAP) Configuration

```
port 1/1/x9 type network
port 1/1/x9 alias lab-f01-h1008_TAP
port 1/1/x9 params admin enable

port 1/1/x10 type network
port 1/1/x10 alias lab-f01-s201_TAP
port 1/1/x10 params admin enable

port 1/1/x11 type tool
port 1/1/x11 alias analyzer
port 1/1/x11 params admin enable

map-passall alias leaf_tap_sadiq
roles replace Default,admin to owner_roles
from 1/1/x9,1/1/x10
to 1/1/x11
```



All Ports | Ports Discovery | Statistics

Ports

Filter | Quick Port Editor | Export

Filtered By : **Alias** | Total Filtered Ports : **3** | Clear Filter

Columns

Port Id	Alias	Type	Speed	Admin	Link Status	Transceiver Type	SFP Power	Avg Util Tx/Rx (last hr)	Port Filter	Discovery Protocol
1/1/x9	Lab-f01-h1008_TAP	N	10G	Enabled	up	sfp+ lr	-6.60	0 / 0.01	—	Off
1/1/x10	Lab-f01-s201_TAP	N	10G	Enabled	up	sfp+ lr	-5.75	0 / 0.16	—	Off
1/1/x11	analyzer	T	1G	Enabled	up	sfp cu		1.74 / 0	—	Off

Test Access Point (TAP) Physical Connectivity

TAP

TAP Collector

LEAF

Leaf 1008
10.2.6.70

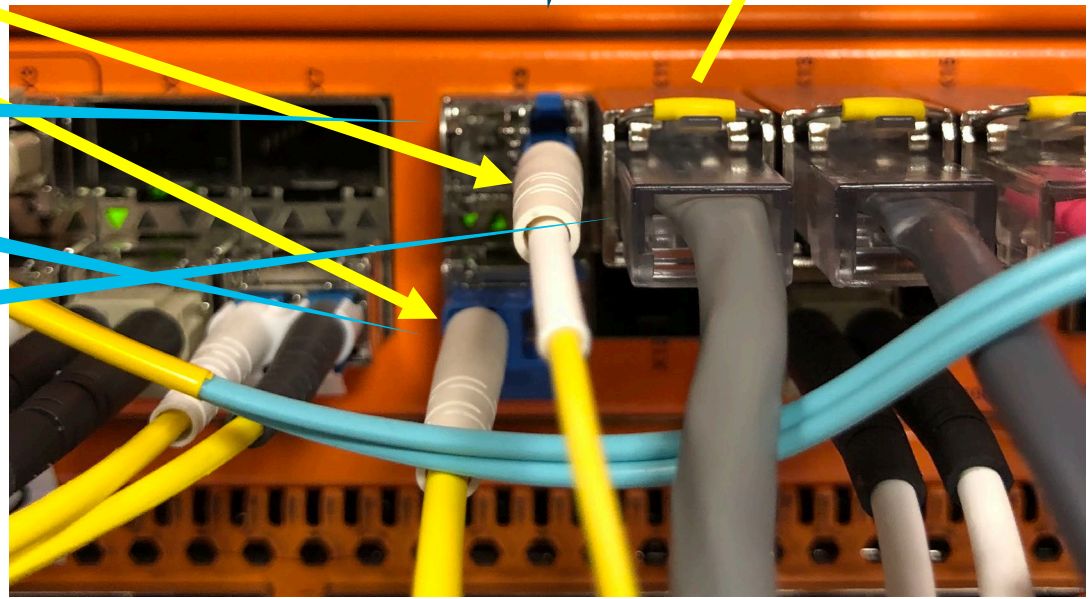
Network Analyzer

Port 1/1/x9

Port 1/1/x10

Port 1/1/x11

Spine 201
10.2.6.69



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Test Access Point (TAP) Verification

TAP Collector Output

```
tcsgm001 [tcsgm: master] # show port utilization
=============================================================================================================
Port        Type      Speed    Utilization   Threshold      Last time      threshold      triggered
                      (Mb/s)                 Tx     Rx      High    Low    Tx     Rx
-------------------------------------------------------------------------------------------------------------
1/1/x9      network   10000                   0.00   0.26    0   0          -      -
1/1/x10     network   10000                   0.00   0.01    0   0          -      -
1/1/x11     tool      1000                    2.78   0.00    0   0          -      -
```

FDO22091HJ0	1	1008	0	tcsh1-f02-h1008	N9K-C93180LC-EX	leaf	10.2.6.70/32	True	yes	Active
FDO21462Q...	1	1005	0	tcsh2-f02-h1005	N9K-C93180LC-EX	leaf	10.2.6.75/32	True	yes	Active

a-cp-internal-prod-web	regular	16482194	225.0.184.112	00:22:B...	Hardwar...	lse	True	.88.197.193/27
a-cp-infra-services	regular	16285612	225.1.4.32	00:22:B...	Hardwar...		True	.88.197.33/27

Leaf 1008 & Leaf 1005 TEP Address

BD Multicast Address

```
No.   Time      Source        Destination     Protocol  Length  Info
   46 0.2370…   10.2.6.70     225.0.184.112   UDP          114  44917 → 48879 Len=68
   47 0.2403…   10.2.6.75     239.255.255.240 UDP          110  13041 → 48879 Len=64
   48 0.2403…   10.2.6.75     239.255.255.224 UDP          190  19074 → 48879 Len=144
   49 0.2407…   10.2.6.70     225.1.4.32      UDP          114  44917 → 48879 Len=68

▶ Frame 46: 114 bytes on wire (912 bits), 114 bytes captured (912 bits)
▶ Ethernet II, Src: AppleTec_0c:0c:0c (00:0c:0c:0c:0c:0c), Dst: IPv4mcast_b8:70 (01:00:5e:00:b8:70)
▶ 802.1Q Virtual LAN, PRI: 6, DEI: 0, ID: 2
▶ Internet Protocol Version 4, Src: 10.2.6.70, Dst: 225.0.184.112
▶ User Datagram Protocol, Src Port: 44917, Dst Port: 48879
▼ Data (68 bytes)
    Data: c8580001fb7f9200ffffffffffff0022bdf819ff08060001...
    [Length: 68]

0000  01 00 5e 00 b8 70 00 0c  0c 0c 0c 0c 81 00 c0 02   ..^..p.. ........
0010  08 00 45 d8 00 60 00 00  00 00 20 11 ef fc 0a 02   ..E..`.. .. .....
0020  06 46 e1 00 b8 70 af 75  be ef 00 4c 00 00 c8 58   .F...p.u ...L...X
0030  00 01 fb 7f 92 00 ff ff  ff ff ff ff 00 22 bd f8   ........ .....".
0040  19 ff 08 06 00 01 08 00  06 04 00 01 00 22 bd f8   ........ .....".
0050  19 ff 13 58 c5 c1 ff ff  ff ff ff ff 13 58 c5 c3   ...X.... .....X..
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0070  00 00                                             ..
```


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Network Assurance Engine (NAE)

Cisco Network Assurance Engine

Enables Operations Teams to

- Predict change impact
- Verify network-wide behavior
- Assure network security compliance
- Quickly root-cause and fix issues

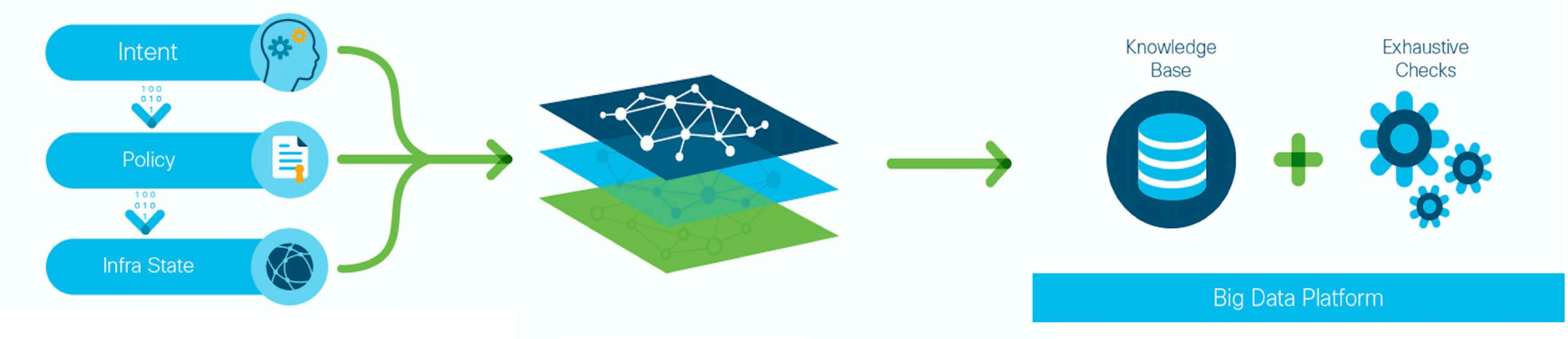
A new software solution for Operations Teams that

- Mathematically models the intent based data center network
- Does **precise reasoning** on policy, config, dynamic state to proactively identify problems.
- Generates Smart Events - What, who, where, why, how to fix
- Provides continuous verification, pro-active insights, deep visibility, and corrective actions

Transforms Network Operations from Reactive To Proactive

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Network Assurance Engine: How it Works



Data Collection

Capture DC Wide Intent, Policy, Control/State across Forwarding & Security

Formal Modeling of Network

Precise Mathematical Models that codify Cisco's 30+ Years of Networking and Cross Customer Domain Knowledge

Continuous Analysis

Models verify that **Network operates per Intent** and accurately tell what is wrong, where, why, impact and how to fix

ACI Expert in the NOC watching the state of fabric 24 hours a day x 365 days a year!

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Verification Results Delivered via Smart Events

What ?

Severity	Event Category	Event Name
	Filter	Filter
⚠	TENANT_FORWARDING	OVERLAPPING_SUBNETS_ACROSS_BDS_IN_VRF
⚠	CHANGE_ANALYSIS	PERMIT_POLICY_SHADOWED_BY_DENY_POLICY

Who and Where ?

Impacted Bd Subnet	Subnet's Owner BD
[5.1.32.101/24]	testbddup3

Why ?

Failing Condition

Subnets defined under the BDs/EPGs are not unique.

How to fix ?

Suggested Next Steps

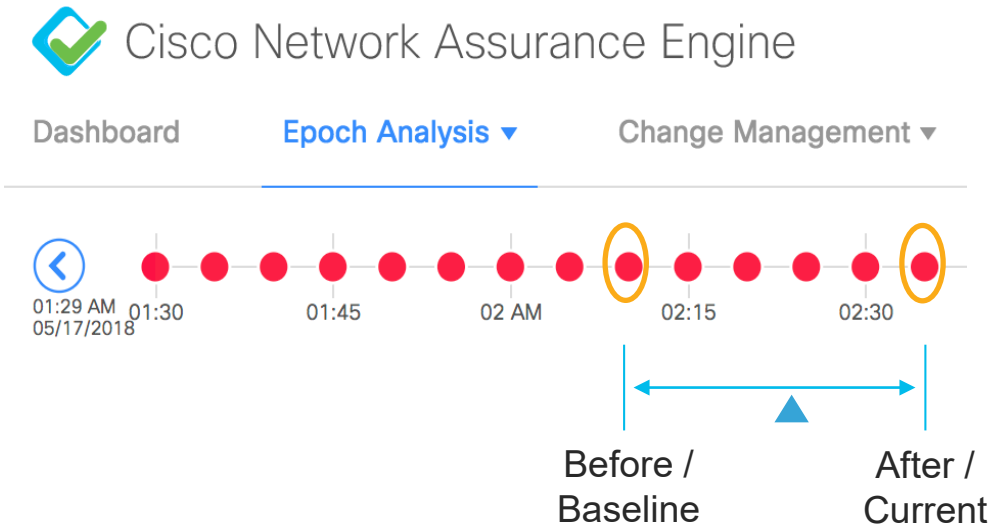
- For all the BDs/EPGs listed, determine the correct BD/EPG subnet.
- Configure unique subnets across BDs/EPGs in a VRF.

Reduce Mean Time to Repair with Precise Analysis and Remediation

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Epoch Delta Analysis

Correlated Ad hoc Analysis Workflow



4 Qs, correlated answers…

- What changed?
- Who was impacted?
- Was it due to config changes?
- What happened as a result?

Use Cases

- Change Management
- Root-cause analysis
- Migration
- Maintenance Upgrades
- Capacity Management

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Tetration Analytics

Why Cisco Tetration ?

Know your applications: what's running and what's critical

Understand what can or should be deployed in public cloud versus on premises

Reduce attack surface with fine-grained segmentation, zero-trust policy and behavior based baselining

Automate policy as workloads scale or move across infrastructure

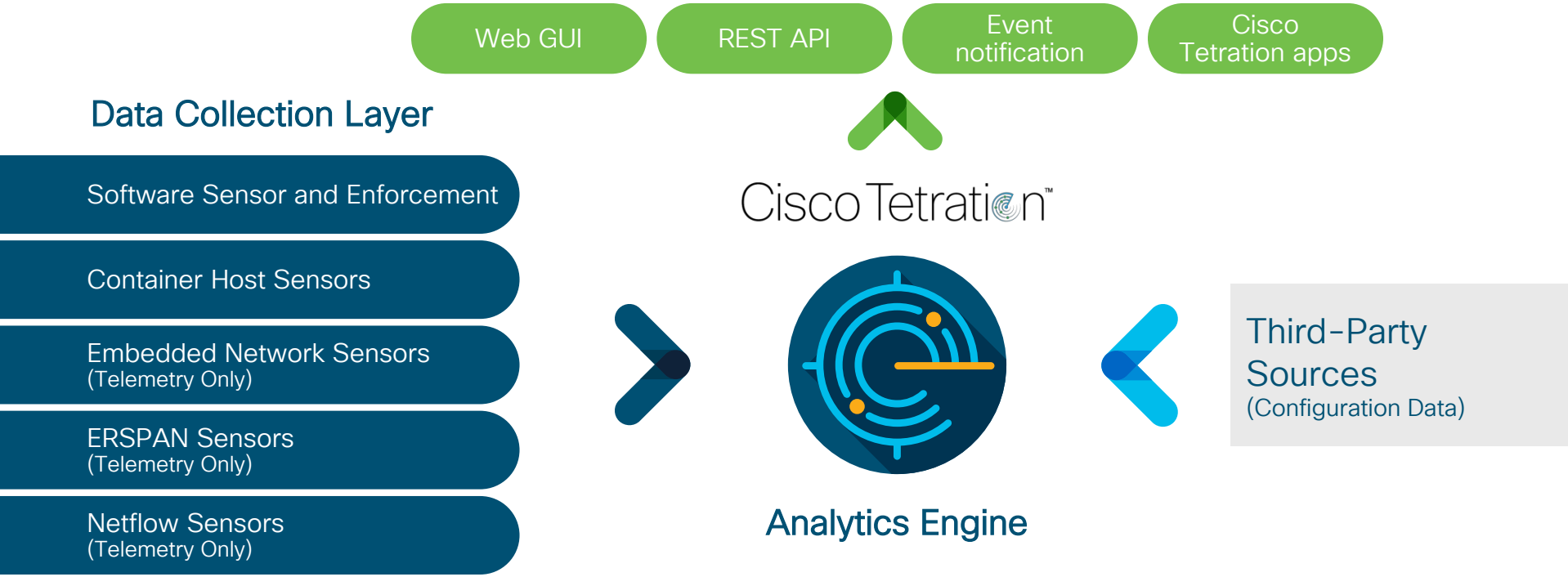
Define a compliance model to track changes and policy violations

Challenges in building a Secure Hybrid IT environment without compromising agility

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

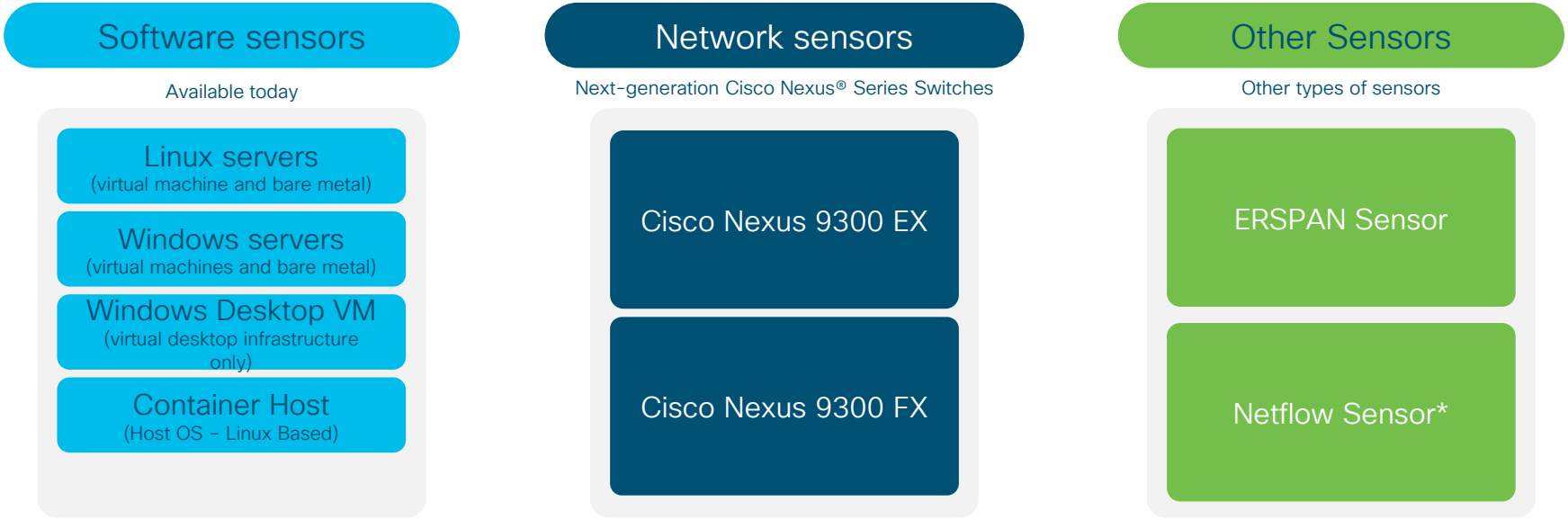
Cisco Tetration Platform

Architecture Overview



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Tetration analytics data sources



*Note: Available for POC/Trail purposes only

Main features

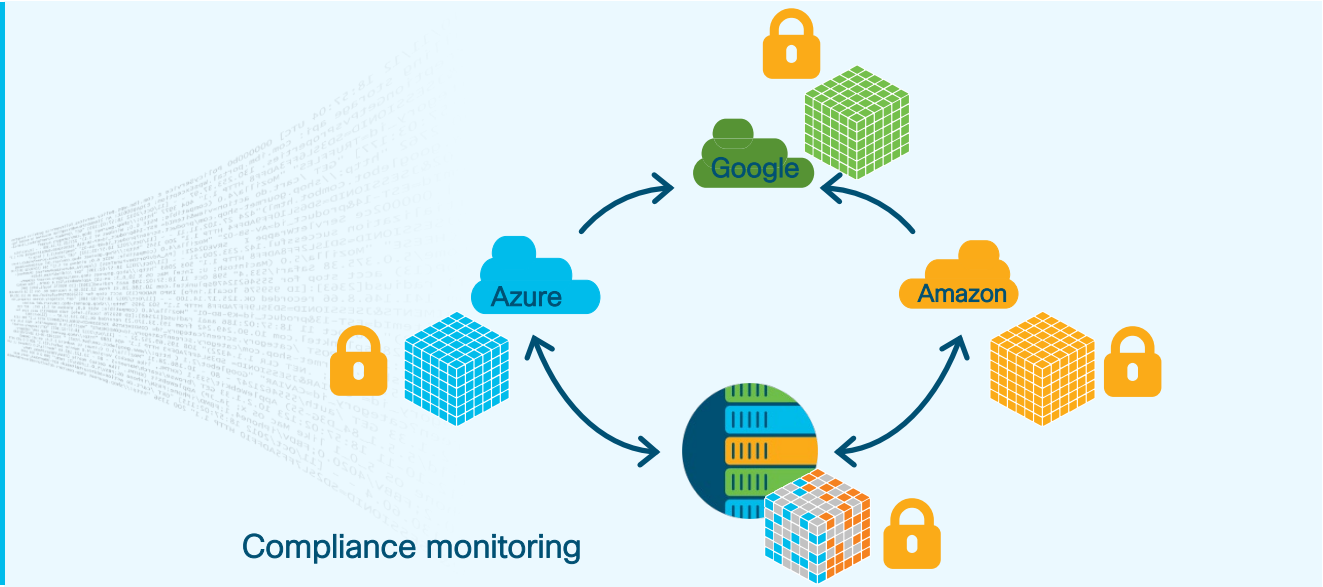
- ✓ Low CPU overhead (SLA enforced)
- ✓ Low network overhead
- ✓ **New** Enforcement point (software agents)
- ✓ Highly secure (code signed and authenticated)
- ✓ Every flow (no sampling) and no payload

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Enforcement of policy across any floor tile

Cisco Tetration Analytics™

1. Generates unique policy per workload
2. Pushes policy to all workloads
3. Workload securely enforces policy
4. Continuously recomputes policy from identity and classification changes

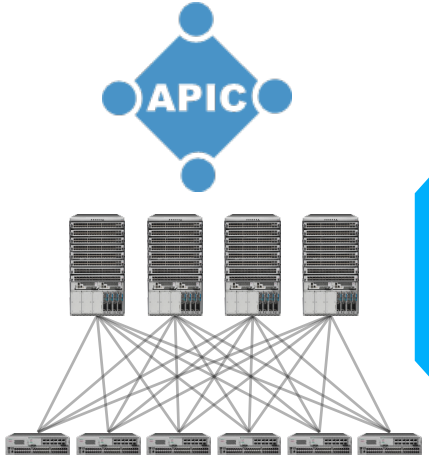


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Splunk

ACI-Splunk: What is Supported?

Cisco ACI App & Add-on for Splunk Enterprise version 4.1.3 – Splunk Certified



Available on **splunkbase**
1800+ downloads, 160+ installs

- Central proactive monitoring
- Operational Analytics
- Audit, Risk and Compliance
- Cross-tier visibility
- Syslog integration

Supported on APIC 1.3 and higher

Compatible with Splunk Enterprise 6.4 & above

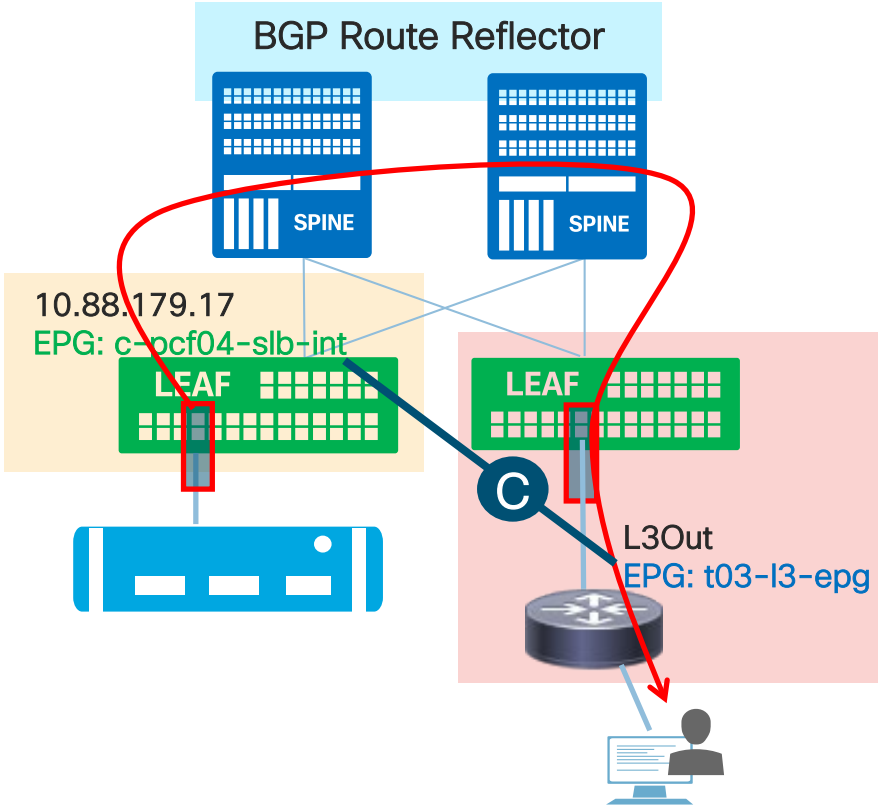
Monitor Multiple ACI Fabrics	Multi-Pod visibility	Micro-Segmentation support	Enhanced user interface with drill down capabilities

How Proactive Monitoring helps in Troubleshooting?

Use Case - 1

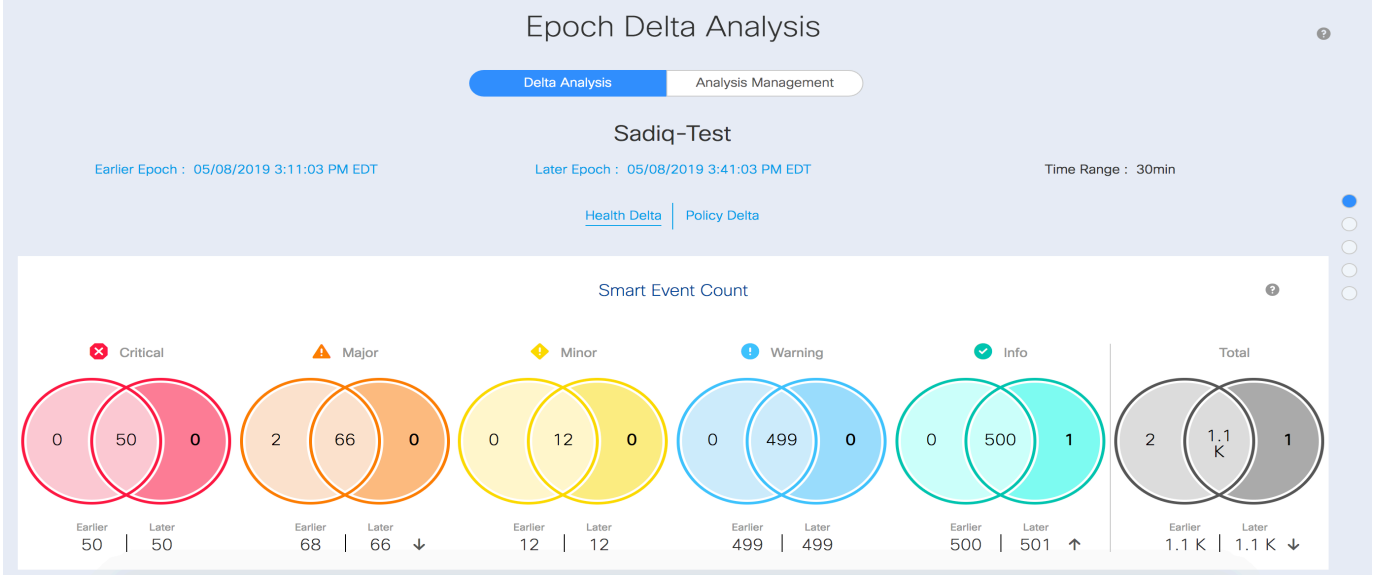
Subnet in ACI NOT reachable- NAE

- BD with Subnet is advertised outside with association to L3Out
- An EPG is associated to BD and statically bind to interface using encap VLAN.
- The VLAN must be part of VLAN pool that is part of Physical Domain.
- Physical Domain is associated to AAEP which is part of interface Policy Group that is part of Interface Profile with port connected to end-host.
- Ensure Route Reflector is configured and functioning on Spines.
- Contract is created between internal EGP and External EPG
- L3Out is functioning properly with external network.



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Subnet in ACI *NOT* reachable– NAE



All Smart Events (1,130)

Aggregated (55) | Individual

55 rows

Severity	Event Category	Event Subcategory	Event Name	Epoch	Count
⚠	TENANT_FORWARDING	SUBNET_ROUTE	BD_WITH_SUBNET_MARKED_EXTERNAL_HAS_L3OUT_BUT_NO_CONTRACT_WITH_EXTERNAL_EPG		1

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Subnet in ACI *NOT* reachable– NAE

```
SADHUSSA-M-W0JK:~ sadiqmemon$ ping 10.88.179.17
PING 10.88.179.17 (10.88.179.17): 56 data bytes
Request timeout for icmp_seq 0
Request timeout for icmp_seq 1
Request timeout for icmp_seq 2
^C
--- 10.88.179.17 ping statistics ---
4 packets transmitted, 0 packets received, 100.0% packet loss
```

Event Found In	Earlier Epoch : 05/08/2019 3:11 PM
Description	VRF is in enforced mode and BD subnet is advertised externally via an L3Out but the EPG(s) belonging to the BD do not have any contract with the External EPG belonging to the L3Out.
Impact	BD subnets will not be advertised.

Affected Objects Details

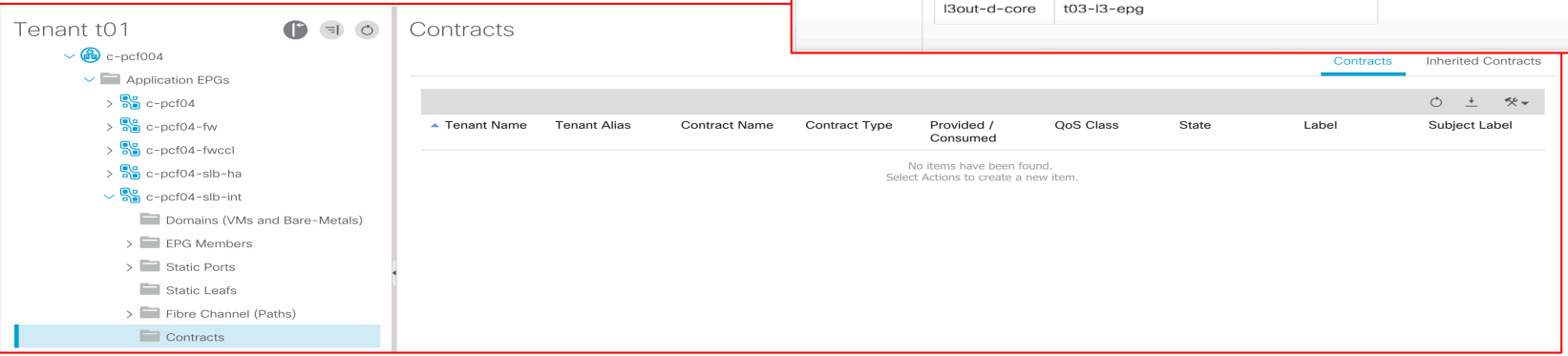
VRF's Tenant	VRF	BD Subnet
t01 *	cp-standard *	[10.88.179.17/29] *

Checks

Check Code	Failing Condition	Suggested Next Steps
26	BD has a subnet marked external and associated with L3Out but none of the EPGs that belong to this BD has contract with the External EPG.	1. Determine if the BD subnet needs to be advertised to the L3Out in question. 2. If not, remove the L3Out <> BD association from this BD. 3. If yes, determine the right EPG(s) that should be communicating with the corresponding external EPG(s) and use an existing contract or create a new contract as appropriate to enable this communication.

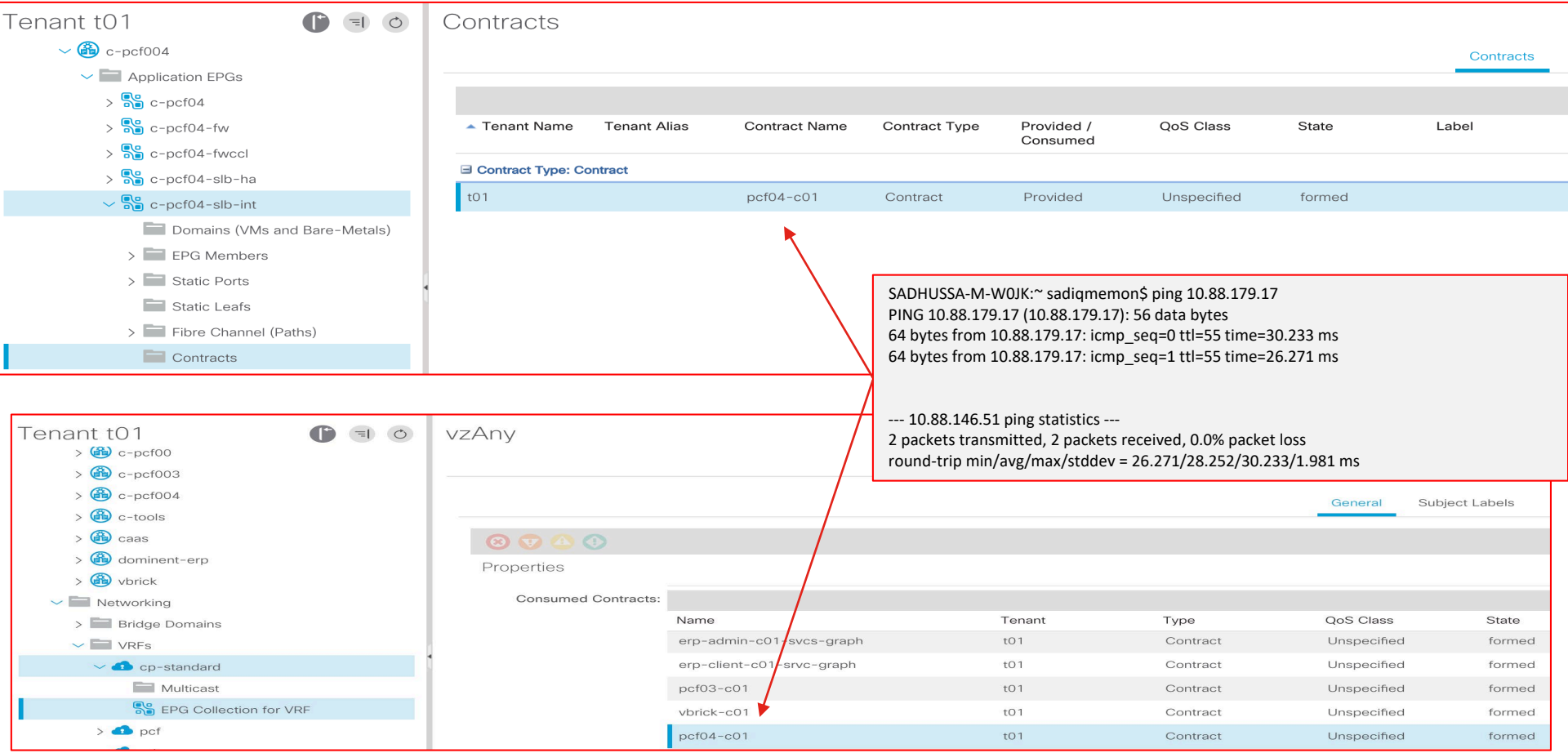
BD's Tenant	BD	App Profile	EPGs that belong to the BD
t01 *	a-pcf04-slb-int *	c-pcf004	c-pcf04-slb-int

L3Out	External EPGs that belong to the L3Out
l3out-d-core	t03-l3-epg



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Subnet in ACI *NOT* reachable– NAE

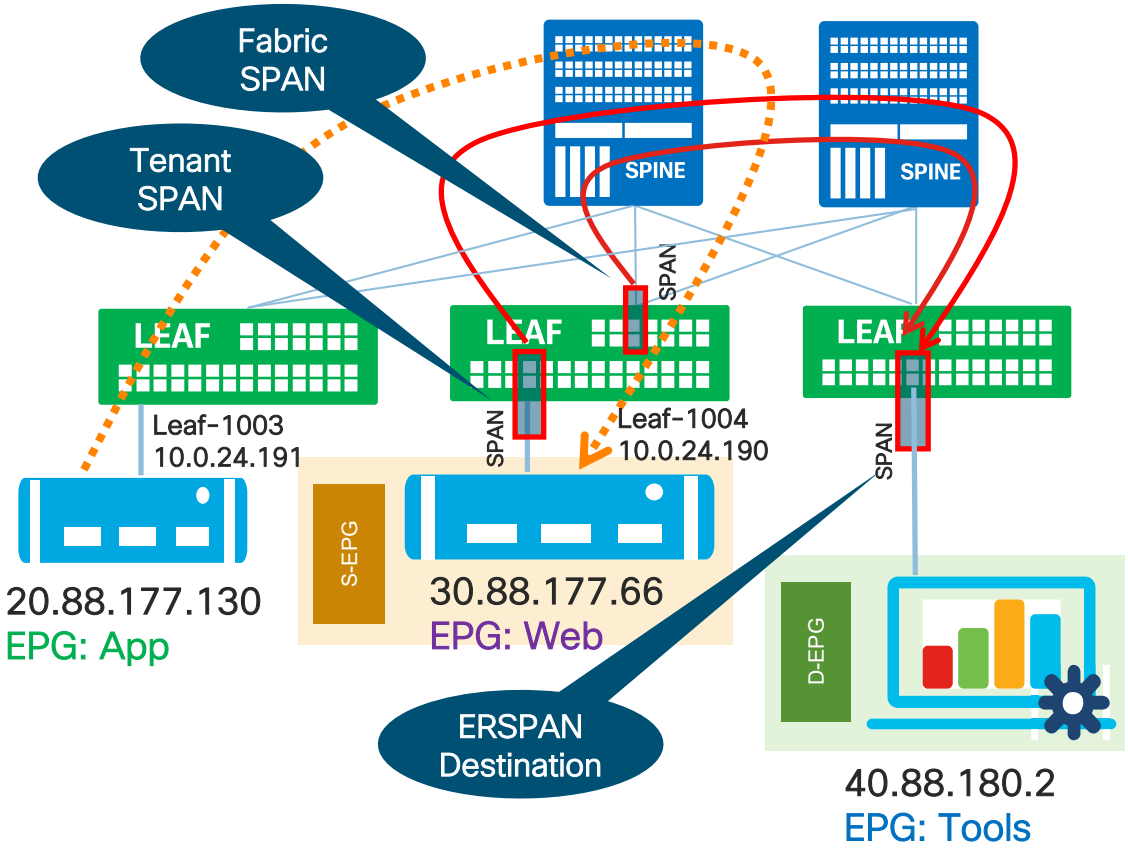


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Use Case - 2

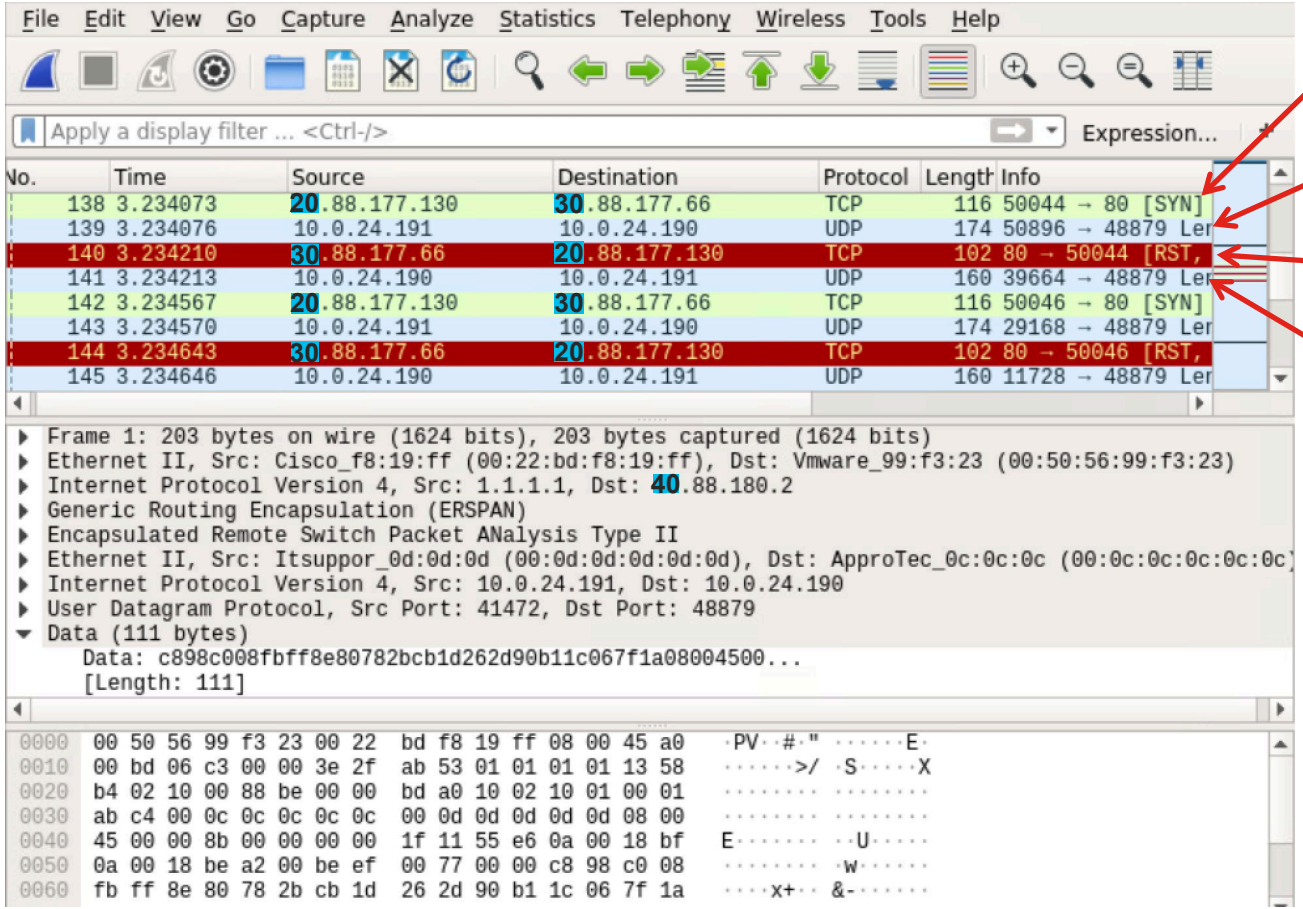
Web Server Unreachable – SPAN (Tenant/Fabric)

- Application team complained that their Application can no longer reach a web server.
- A Server with IP address **20.88.177.130** part of "EGP: App' is no longer able to reach web server **30.88.177.66** part of "EPG: Web".
- Due to sensitivity of application, Network team was capturing data as part of application visibility.
  - Tenant SPAN with source EPG: Web
  - Fabric SPAN with source fabric ports eth1/97-98 connected to Spines
  - SPAN Destination is a data storage **40.88.180.2** part of "EPG: Tools"



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Web Server Unreachable – SPAN (Tenant/Fabric)



(SYN) sent from server (20.88.177.130) to Web Server (30.88.177.66)

Leef-1003 forwarding that (SYN) encapsulated in VXLAN to Leaf-1004

Web Server Resetting (RST) the TCP connection

(RST) is carried over from Leaf-1004 to Leaf-1003

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Web Server Unreachable – SPAN (Tenant/Fabric)

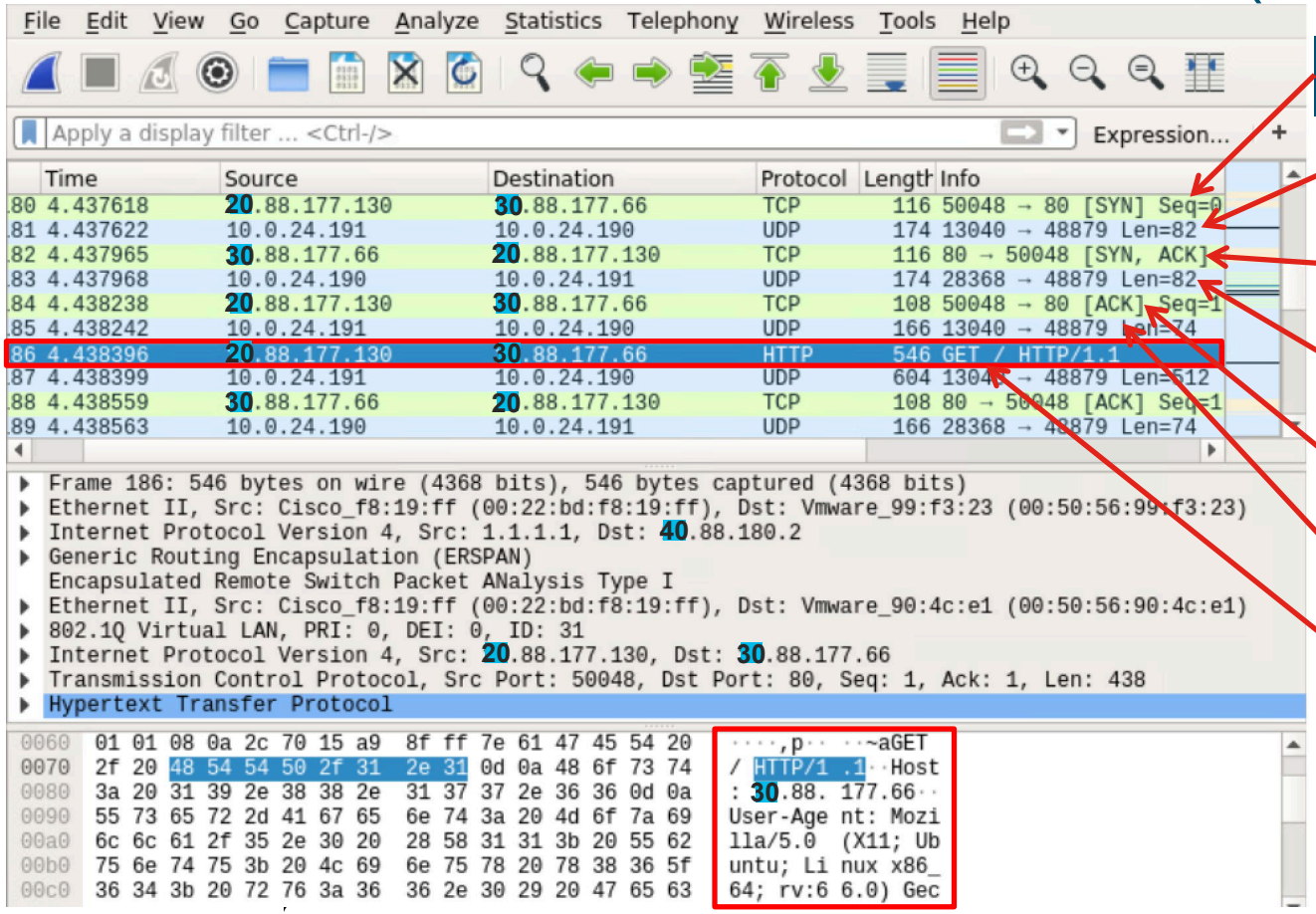
Apache web service is down on server 30.88.177.66

```
shussa36@k8s:~$ ps -ef | grep apache
shussa36 13869  3423  0 15:56 pts/1    00:00:00 grep --color=auto apache
shussa36@k8s:~$
shussa36@k8s:~$
shussa36@k8s:~$ sudo systemctl start apache2.service
shussa36@k8s:~$
shussa36@k8s:~$
shussa36@k8s:~$ ps -ef | grep apache
root     13892     1  0 15:56 ?        00:00:00 /usr/sbin/apache2 -k start
www-data 13895 13892  0 15:56 ?        00:00:00 /usr/sbin/apache2 -k start
www-data 13896 13892  0 15:56 ?        00:00:00 /usr/sbin/apache2 -k start
shussa36 13954  3423  0 15:56 pts/1    00:00:00 grep --color=auto apache
shussa36@k8s:~$
```

Apache web service started on server 30.88.177.66

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Web Server Unreachable – SPAN (Tenant/Fabric)



(SYN) sent from server (20.88.177.130) to Web Server (30.88.177.66)

Leef-1003 forwarding that (SYN) encapsulated in VXLAN to Leaf-1004

Web Server (30.88.177.66) connected to Leaf-1004 sending (SYN-ACK)

(SYN-ACK) is carried over from Leaf-1004 to Leaf-1003

(ACK) sent from server (20.88.177.130) to Web Server (30.88.177.66)

Leef-1003 forwarding that (ACK) encapsulated in VXLAN to Leaf-1004

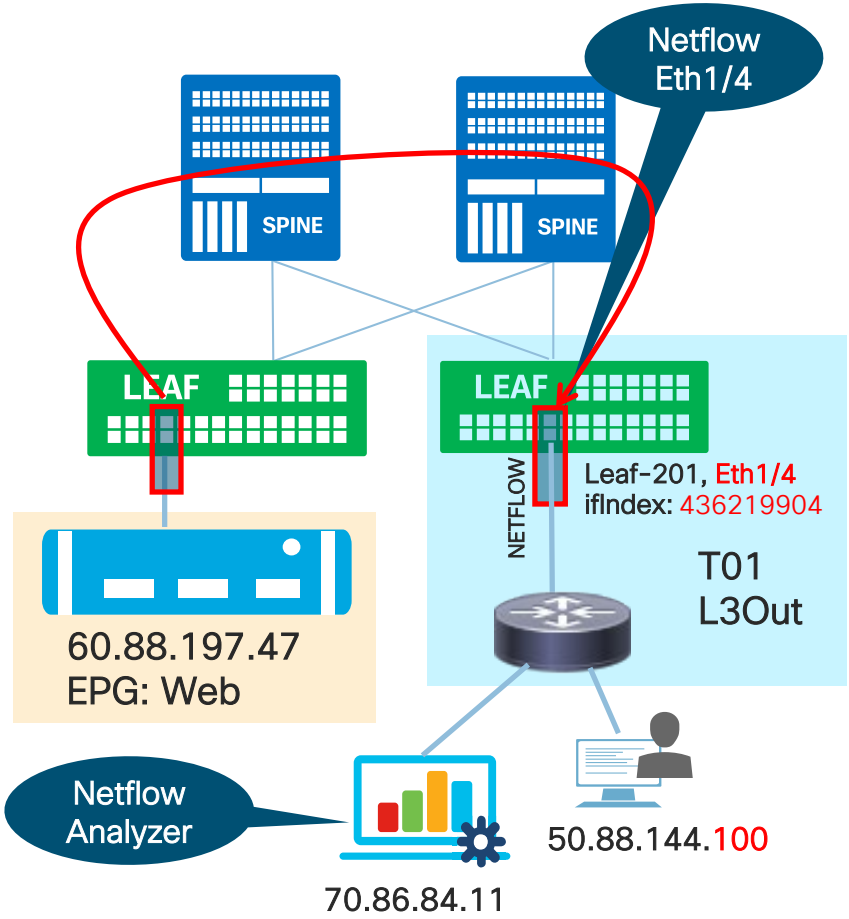
Leef-1003 requesting a GET via HTTP to Web Server (30.88.177.66)

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Use Case - 3

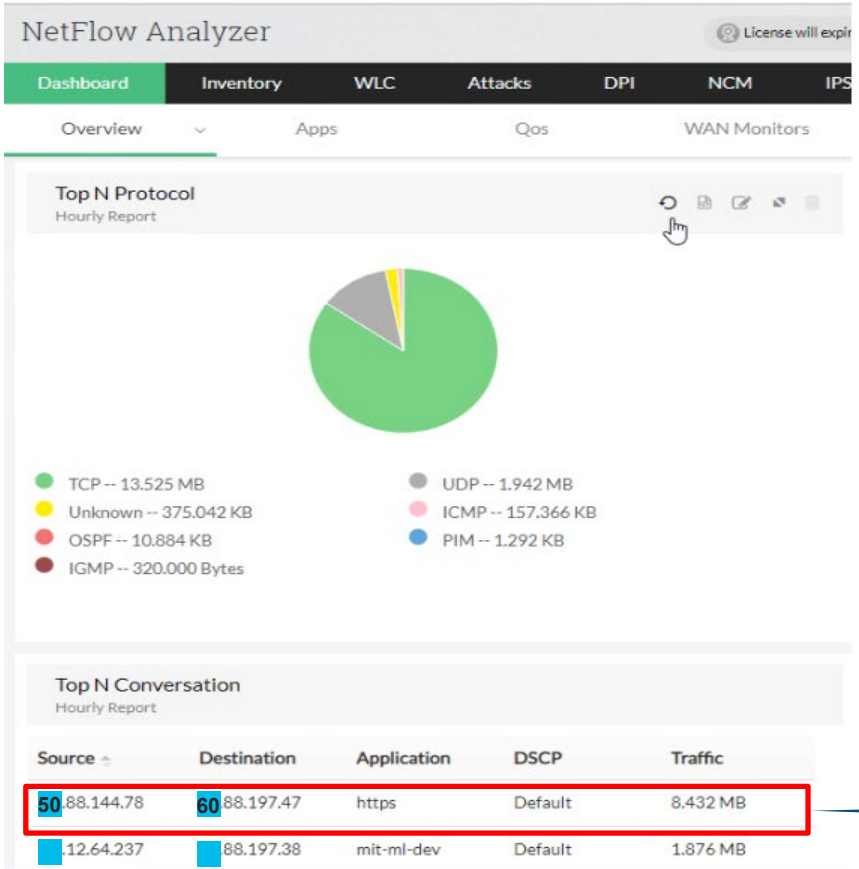
Web Application Malfunctioning– Netflow (Tenant)

- Application team complained that their web application is not functioning properly.
- An external client with IP address **50.88.144.78** consuming web services from server **60.88.197.47** part of "**EPG: Web**".
- Due to sensitivity of application, Network team was collecting flow data as part of application visibility.
  - Create Flow Record (IPv4-Record)
  - Create Flow Exporter (**70.86.84.11**)
  - Create Flow Monitor
  - Enable Netflow under External Routed Network on Border Leaf 201 interface eth1/4



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

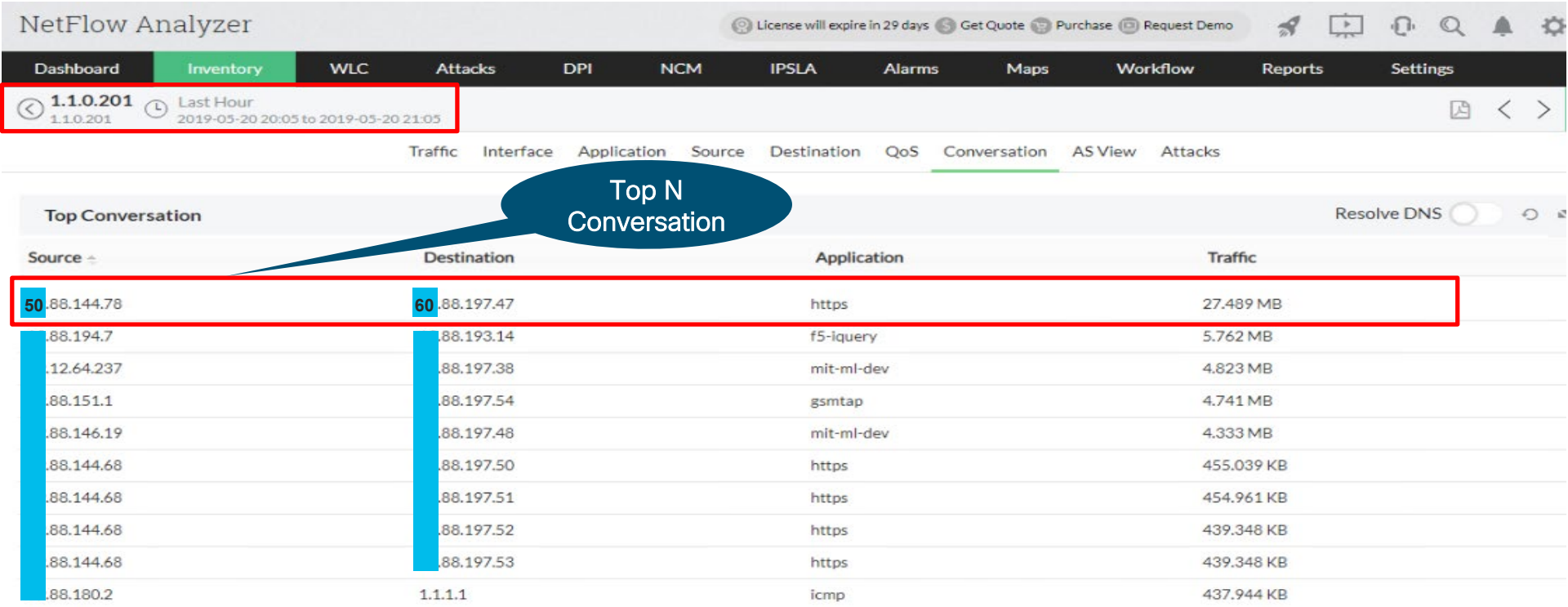
Web Application Malfunctioning – Netflow (Tenant)



Top N Conversation

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Web Application Malfunctioning – Netflow (Tenant)



After proofing Web Server functioning normal through NetFlow, culprit identified to be the Client Machine

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Use Case - 4

Server Interface Down – SNMP Trap

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	.88.196.130	.88.146.197	SNMP	280	snmpV2-trap 1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.1.4.1.0 1.3.6.1.2.1.2.2.1.1.436215808 1.3.6.1.2.1.2.…
2	0.100376	.88.196.130	.88.146.197	SNMP	208	snmpV2-trap 1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.1.4.1.0 1.3.6.1.2.1.2.2.1.7.436215808 1.3.6.1.2.1.2.…
3	47.356648	.88.196.130	.88.146.197	SNMP	280	snmpV2-trap 1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.1.4.1.0 1.3.6.1.2.1.2.2.1.1.436215808 1.3.6.1.2.1.2.…
4	47.456989	.88.196.130	.88.146.197	SNMP	208	snmpV2-trap 1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.1.4.1.0 1.3.6.1.2.1.2.2.1.7.436215808 1.3.6.1.2.1.2.…

```
[Stream index: 0]
▼ Simple Network Management Protocol
    version: v2c (1)
    community: auto-snmp
  ▼ data: snmpV2-trap (7)
    ▼ snmpV2-trap
        request-id: 704
        error-status: noError (0)
        error-index: 0
      ▼ variable-bindings: 9 items
        ▶ 1.3.6.1.2.1.1.3.0: 541933
        ▼ 1.3.6.1.6.3.1.1.4.1.0: 1.3.6.1.4.1.9.9.276.0.1 (iso.3.6.1.4.1.9.9.276.0.1)
            Object Name: 1.3.6.1.6.3.1.1.4.1.0 (i…
            Value (OID): 1.3.6.1.4.1.9.9.276.0.1 (iso.3.6.1.4.1.9.9.276.0.1)
        ▶ 1.3.6.1.2.1.2.2.1.1.436215808: 436215808
        ▶ 1.3.6.1.2.1.2.2.1.7.436215808: 2
        ▶ 1.3.6.1.2.1.2.2.1.8.436215808: 2
        ▶ 1.3.6.1.2.1.31.1.1.1.1.436215808: 657468312f33
        ▶ 1.3.6.1.2.1.2.2.1.3.436215808: 6
```

```
0030  04 09 61 75 74 6f 2d 73  6e 6d 70 a7 81 da 02 02   ..auto-s nmp.....
0040  02 c0 02 01 00 02 01 00  30 81 cd 30 0f 06 08 2b   ........ 0..0...+
0050  06 01 02 01 01 03 00 43  03 08 44 ed 30 19 06 0a   .......C ..D.0...
0060  2b 06 01 06 03 01 01 04  01 00 06 0b 2b 06 01 04   +....... ....+...
0070  01 09 09 82 14 00 01 30  16 06 0e 2b 06 01 02 01   .......0 ...+....
0080  02 02 01 01 81 d0 80 c0  00 02 04 1a 00 20 00 30   ........ ..... .0
0090  13 06 0e 2b 06 01 02 01  02 02 01 07 81 d0 80 c0   ...+.... ........
00a0  00 02 01 02 30 13 06 0e  2b 06 01 02 01 02 02 01   ....0... +.......
00b0  08 81 d0 80 c0 00 02 01  02 30 19 06 0f 2b 06 01   ........ .0...+..
00c0  02 01 1f 01 01 01 01 81  d0 80 c0 00 04 06 65 74   ........ ......et
00d0  68 31 2f 33 30 13 06 0e  2b 06 01 02 01 02 02 01   h1/3  .. +.......
00e0  03 81 d0 80 c0 00 02 01  06 30 18 06 0e 2b 06 01   ........ .0...+..
00f0  02 01 02 02 01 02 81 d0  80 c0 00 04 06 65 74 68   ........ .....eth
0100  31 2f 33 30 13 06 0f 2b  06 01 02 01 1f 01 01 01   1/3  ..+ ........
0110  12 81 d0 80 c0 00 04 00                           ........
```

SNMP Community

Port Eth 1/3

https://snmp.cloudapps.cisco.com/Support/SNMP/do/BrowseOID.do?local=en

Object Information

Specific Object Information

Object	cieLinkDown
OID	1.3.6.1.4.1.9.9.276.0.1
Status	current
MIB	CISCO-IF-EXTENSION-MIB ; - View Supporting Images
Trap Components	ifIndex ifAdminStatus ifOperStatus ifName ifType
Description	"A cisco specific linkDown notification signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state (but not from the notPresent state). The varbinds for this notification indicate the interface information of the communication link."

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Server Interface UP – SNMP Trap

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	.88.196.130	.88.146.197	SNMP	280	snmpV2-trap 1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.1.4.1.0 1.3.6.1.2.1.2.2.1.1.436215808 1.3.6.1.2.1.2.…
2	0.100376	.88.196.130	.88.146.197	SNMP	208	snmpV2-trap 1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.1.4.1.0 1.3.6.1.2.1.2.2.1.7.436215808 1.3.6.1.2.1.2.…
3	47.356648	.88.196.130	.88.146.197	SNMP	280	snmpV2-trap 1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.1.4.1.0 1.3.6.1.2.1.2.2.1.1.436215808 1.3.6.1.2.1.2.…
4	47.456989	.88.196.130	.88.146.197	SNMP	208	snmpV2-trap 1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.1.4.1.0 1.3.6.1.2.1.2.2.1.7.436215808 1.3.6.1.2.1.2.…

```
▶ Frame 3: 280 bytes on wire (2240 bits), 280 bytes captured (2240 bits) on interface 0
▶ Ethernet II, Src: Cisco_0d:4c:43 (e4:c7:22:0d:4c:43), Dst: Vmware_a1:bd:a2 (00:50:56:a1:bd:a2)
▶ Internet Protocol Version 4, Src: .88.196.130, Dst: .88.146.197
▶ User Datagram Protocol, Src Port: 56004, Dst Port: 162
▼ Simple Network Management Protocol
    version: v2c (1)
    community: auto-snmp
  ▼ data: snmpV2-trap (7)
    ▼ snmpV2-trap
        request-id: 706
        error-status: noError (0)
        error-index: 0
      ▼ variable-bindings: 9 items
        ▶ 1.3.6.1.2.1.1.3.0: 546670
        ▼ 1.3.6.1.6.3.1.1.4.1.0: 1.3.6.1.4.1.9.9.276.0.2 (iso.3.6.1.4.1.9.9.276.0.2)
            Object Name: 1.3.6.1.6.3.1.1.4.1.0 (iso.3.6.1.6.3.1.1.4.1.0)
            Value (OID): 1.3.6.1.4.1.9.9.276.0.2 (iso.3.6.1.4.1.9.9.276.0.2)
        ▶ 1.3.6.1.2.1.2.2.1.1.436215808: 436215808
        ▶ 1.3.6.1.2.1.2.2.1.7.436215808: 1
```

```
0030  04 09 61 75 74 6f 2d 73  6e 6d 70 a7 81 da 02 02   ..auto-s nmp.....
0040  02 c2 02 01 00 02 01 00  30 81 cd 30 0f 06 08 2b   ........ 0..0...+
0050  06 01 02 01 01 03 00 43  03 08 57 6e 30 19 06 0a   .......C ..Wn0...
0060  2b 06 01 06 03 01 01 04  01 00 06 0b 2b 06 01 04   +....... ....+...
0070  01 09 09 82 14 00 02 30  16 06 0e 2b 06 01 02 01   .......0 ...+....
0080  02 02 01 01 81 d0 80 c0  00 02 04 1a 00 20 00 30   ........ ..... .0
0090  13 06 0e 2b 06 01 02 01  02 02 01 07 81 d0 80 c0   ...+.... ........
00a0  00 02 01 01 30 13 06 0e  2b 06 01 02 01 02 02 01   ....0... +.......
00b0  08 81 d0 80 c0 00 02 01  01 30 19 06 0f 2b 06 01   ........ .0...+..
00c0  02 01 1f 01 01 01 01 81  d0 80 c0 00 04 06 65 74   ........ ......et
00d0  68 31 2f 33 30 13 06 0e  2b 06 01 02 01 02 02 01   h1/3 .. +.......
00e0  03 81 d0 80 c0 00 02 01  06 30 18 06 0e 2b 06 01   ........ .0...+..
00f0  02 01 02 02 01 02 81 d0  80 c0 00 04 06 65 74 68   ........ .....eth
0100  31 2f 33 30 13 06 0f 2b  06 01 02 01 1f 01 01 01   1/3 ..+ ........
0110  12 81 d0 80 c0 00 04 00                           ........
```

SNMP Community

Port Eth 1/3

https://snmp.cloudapps.cisco.com/Support/SNMP/do/BrowseOID.do?local=en

Object Information

Specific Object Information

Object	cieLinkUp
OID	1.3.6.1.4.1.9.9.276.0.2
Status	current
MIB	CISCO-IF-EXTENSION-MIB ; - View Supporting Images
Trap Components	ifIndex ifAdminStatus ifOperStatus ifName ifType
Description	"A cisco specific linkUp trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links left the down state and transitioned into some other state (but not into the notPresent state). The varbinds for this notification indicate the interface information of the communication link."

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Server Interface Down – Syslog

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	[redacted].88.196.130	[redacted].88.146.198	Syslog	173	LOCAL7.INFO: Dec 06 16:26:46.727 tcsh1-f02-h1001 %LOG_-6-SYSTEM_MSG [E4208843][transition][i
2	0.009195	[redacted].88.196.130	[redacted].88.146.198	Syslog	189	LOCAL7.INFO: Dec 06 16:26:46.736 tcsh1-f02-h1001 %LOG_-6-SYSTEM_MSG [E4205126][port-down][in
3	0.011327	[redacted].88.196.130	[redacted].88.146.198	Syslog	189	LOCAL7.INFO: Dec 06 16:26:46.739 tcsh1-f02-h1001 %LOG_-6-SYSTEM_MSG [E4215671][port-down][in
4	39.826806	[redacted].88.196.130	[redacted].88.146.198	Syslog	173	LOCAL7.INFO: Dec 06 16:27:26.556 tcsh1-f02-h1001 %LOG_-6-SYSTEM_MSG [E4208843][transition][i
5	39.831104	[redacted].88.196.130	[redacted].88.146.198	Syslog	244	LOCAL7.CRIT: Dec 06 16:27:26.560 tcsh1-f02-h1001 %LOG_-2-SYSTEM_MSG [F0532][soaking][interfa
6	47.323634	[redacted].88.196.130	[redacted].88.146.198	Syslog	255	LOCAL7.CRIT: Dec 06 16:27:34.053 tcsh1-f02-h1001 %LOG_-2-SYSTEM_MSG [F0532][soaking_clearing

```
▶ Frame 2: 189 bytes on wire (1512 bits), 189 bytes captured (1512 bits) on interface 0
▶ Ethernet II, Src: Cisco_0d:4c:43 (e4:c7:22:0d:4c:43), Dst: Vmware_a1:ca:32 (00:50:56:a1:ca:32)
▶ Internet Protocol Version 4, Src: [redacted].88.196.130, Dst: [redacted].88.146.198
▶ User Datagram Protocol, Src Port: 50995, Dst Port: 514
▼ Syslog message: LOCAL7.INFO: Dec 06 16:26:46.736 tcsh1-f02-h1001 %LOG_-6-SYSTEM_MSG [E4205126][port-down][info][sys/phys-[eth1/3]/phys] Port is down. Reason: adminCfgChng\n
    1011 1... = Facility: LOCAL7 - reserved for local use (23)
    .... .110 = Level: INFO - informational (6)
    Message: Dec 06 16:26:46.736 tcsh1-f02-h1001 %LOG_-6-SYSTEM_MSG [E4205126][port-down][info][sys/phys-[eth1/3]/phys] Port is down. Reason: adminCfgChng\n
```

Also parse on
Port Down Fault
F0532

```
0000  00 50 56 a1 ca 32 e4 c7  22 0d 4c 43 08 00 45 00   .PV..2.. ".LC..E.
0010  00 af cc 23 00 00 3c 11  34 22 13 58 c4 82 13 58   ...#..<. 4".X...X
0020  92 c6 c7 33 02 02 00 9b  11 e8 3c 31 39 30 3e 44   ...3.... ..<190>D
0030  65 63 20 30 36 20 31 36  3a 32 36 3a 34 36 2e 37   ec 06 16 :26:46.7
0040  33 36 20 74 63 73 68 31  2d 66 30 32 2d 68 31 30   36 tcsh1 -f02-h10
0050  30 31 20 25 4c 4f 47 5f  2d 36 2d 53 59 53 54 45   01 %LOG_ -6-SYSTE
0060  4d 5f 4d 53 47 20 5b 45  34 32 30 35 31 32 36 5d   M_MSG [E 4205126]
0070  5b 70 6f 72 74 2d 64 6f  77 6e 5d 5b 69 6e 66 6f   [port-do wn][info
0080  5d 5b 73 79 73 2f 70 68  79 73 2d 5b 65 74 68 31   ][sys/ph ys-[eth1
0090  2f 33 5d 2f 70 68 79 73  5d 20 50 6f 72 74 20 69   /3]/phys ] Port i
00a0  73 20 64 6f 77 6e 2e 20  52 65 61 73 6f 6e 3a 20   s down.  Reason:
00b0  61 64 6d 69 6e 43 66 67  43 68 6e 67 0a            adminCfg Chng.
```


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Server Interface UP – Syslog

No.	Time	Source	Destination	Protocol	Length	Info
4	39.826806	.88.196.130	.88.146.198	Syslog	173	LOCAL7.INFO: Dec 06 16:27:26.556 tcsh1-f02-h1001 %LOG_-6-SYSTEM_MSG [E4208843][transit
5	39.831104	.88.196.130	.88.146.198	Syslog	244	LOCAL7.CRIT: Dec 06 16:27:26.560 tcsh1-f02-h1001 %LOG_-2-SYSTEM_MSG [F0532][soaking][i
6	47.323634	.88.196.130	.88.146.198	Syslog	255	LOCAL7.CRIT: Dec 06 16:27:34.053 tcsh1-f02-h1001 %LOG_-2-SYSTEM_MSG [F0532][soaking_cl
7	47.328166	.88.196.130	.88.146.198	Syslog	163	LOCAL7.INFO: Dec 06 16:27:34.058 tcsh1-f02-h1001 %LOG_-6-SYSTEM_MSG [E4205125][port-up
8	47.329992	.88.196.130	.88.146.198	Syslog	163	LOCAL7.INFO: Dec 06 16:27:34.060 tcsh1-f02-h1001 %LOG_-6-SYSTEM_MSG [E4215670][port-up

```
▶ Frame 7: 163 bytes on wire (1304 bits), 163 bytes captured (1304 bits) on interface 0
▶ Ethernet II, Src: Cisco_0d:4c:43 (e4:c7:22:0d:4c:43), Dst: Vmware_a1:ca:32 (00:50:56:a1:ca:32)
▶ Internet Protocol Version 4, Src: .88.196.130, Dst: .88.146.198
▶ User Datagram Protocol, Src Port: 50995, Dst Port: 514
▼ Syslog message: LOCAL7.INFO: Dec 06 16:27:34.058 tcsh1-f02-h1001 %LOG_-6-SYSTEM_MSG [E4205125][port-up][info][sys/phys-[eth1/3]/phys] Port is up\n
    1011 1... = Facility: LOCAL7 - reserved for local use (23)
    .... .110 = Level: INFO - informational (6)
    Message: Dec 06 16:27:34.058 tcsh1-f02-h1001 %LOG_-6-SYSTEM_MSG [E4205125][port-up][info][sys/phys-[eth1/3]/phys] Port is up\n
```

```
0000  00 50 56 a1 ca 32 e4 c7  22 0d 4c 43 08 00 45 00   .PV..2.. ".LC..E.
0010  00 95 dd 7b 00 00 3c 11  22 e4 13 58 c4 82 13 58   ...{..<. "..X...X
0020  92 c6 c7 33 02 02 00 81  be cd 3c 31 39 30 3e 44   ...3.... ..<190>D
0030  65 63 20 30 36 20 31 36  3a 32 37 3a 33 34 2e 30   ec 06 16 :27:34.0
0040  35 38 20 74 63 73 68 31  2d 66 30 32 2d 68 31 30   58 tcsh1 -f02-h10
0050  30 31 20 25 4c 4f 47 5f  2d 36 2d 53 59 53 54 45   01 %LOG_ -6-SYSTE
0060  4d 5f 4d 53 47 20 5b 45  34 32 30 35 31 32 35 5d   M_MSG [E 4205125]
0070  5b 70 6f 72 74 2d 75 70  5d 5b 69 6e 66 6f 5d 5b   [port-up ][info][
0080  73 79 73 2f 70 68 79 73  2d 5b 65 74 68 31 2f 33   sys/phys -[eth1/3
0090  5d 2f 70 68 79 73 5d 20  50 6f 72 74 20 69 73 20   ]/phys]  Port is
00a0  75 70 0a                                          up.
```


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Use Case - 5

External Network Connectivity Down– SNMP Trap

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	[redacted].88.196.40	[redacted].88.146.197	SNMP	279	snmpV2-trap 1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.1.4.1.0 1.3.6.1.2.1.2.2.1.1.436219904 1.3.6.1.2.1.2.2.1.7.436219904 1.3.6.1.2.1.2.2.1.8.436219904 1.3.6.1.2.1.31.1.1.1.
2	0.100329	[redacted].88.196.40	[redacted].88.146.197	SNMP	207	snmpV2-trap 1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.1.4.1.0 1.3.6.1.2.1.2.2.1.7.436219904 1.3.6.1.2.1.2.2.1.1.436219904 1.3.6.1.2.1.2.2.1.8.436219904 1.3.6.1.6.3.1.1.4.3.0
3	0.200781	[redacted].88.196.40	[redacted].88.146.197	SNMP	204	snmpV2-trap 1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.1.4.1.0 1.3.6.1.2.1.14.1.1.0 1.3.6.1.2.1.14.7.1.1.[redacted]88.192.27.0 1.3.6.1.2.1.14.7.1.2.[redacted]88.192.27.0 1.3.6.1.2.1.14.7.1
4	203.029540	[redacted].88.196.40	[redacted].88.146.197	SNMP	279	snmpV2-trap 1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.1.4.1.0 1.3.6.1.2.1.2.2.1.1.436219904 1.3.6.1.2.1.2.2.1.7.436219904 1.3.6.1.2.1.2.2.1.8.436219904 1.3.6.1.2.1.31.1.1.1.
5	203.129882	[redacted].88.196.40	[redacted].88.146.197	SNMP	207	snmpV2-trap 1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.1.4.1.0 1.3.6.1.2.1.2.2.1.7.436219904 1.3.6.1.2.1.2.2.1.1.436219904 1.3.6.1.2.1.2.2.1.8.436219904 1.3.6.1.6.3.1.1.4.3.0

```
community: auto-snmp
data: snmpV2-trap (7)
  snmpV2-trap
    request-id: 31
    error-status: noError (0)
    error-index: 0
    variable-bindings: 6 items
      1.3.6.1.2.1.1.3.0: 7321432
        Object Name: 1.3.6.1.2.1.1.3.0 (iso.3.6.1.2.1.1.3.0)
        Value (Timeticks): 7321432
      1.3.6.1.6.3.1.1.4.1.0: 1.3.6.1.2.1.14.16.2.16 (iso.3.6.1.2.1.14.16.2.16)
        Object Name: 1.3.6.1.6.3.1.1.4.1.0 (iso.3.6.1.6.3.1.1.4.1.0)
        Value (OID): 1.3.6.1.2.1.14.16.2.16 (iso.3.6.1.2.1.14.16.2.16)
      1.3.6.1.2.1.14.1.1.0: [redacted].88.193.131
        Object Name: 1.3.6.1.2.1.14.1.1.0 (iso.3.6.1.2.1.14.1.1.0)
        Value (IpAddress): [redacted].88.193.131
      1.3.6.1.2.1.14.7.1.1.[redacted] 88.192.27.0: [redacted] 88.192.27
        Object Name: 1.3.6.1.2.1.14.7.1.1[redacted].88.192.27.0 (iso.3.6.1.2.1.14.7.1.1[redacted].192.27.0)
        Value (IpAddress): [redacted].88.192.27
      1.3.6.1.2.1.14.7.1.2.[redacted] 88.192.27.0: 0
        Object Name: 1.3.6.1.2.1.14.7.1.2.[redacted]192.27.0 (iso.3.6.1.2.1.14.7.1.2.[redacted] 88.192.27.0)
        Value (Integer32): 0
      1.3.6.1.2.1.14.7.1.12.[redacted]8.192.27.0: 1
        Object Name: 1.3.6.1.2.1.14.7.1.12.[redacted] 88.192.27.0 (iso.3.6.1.2.1.14.7.1.12.[redacted]88.192.27.0)
        Value (Integer32): 1
```

```
0000  00 50 56 a1 bd a2 e4 c7  22 0d 4c 43 08 00 45 00   .PV..... ".LC..E.
0010  00 be 2f 12 00 00 3c 11  d1 7f 13 58 c4 28 13 58   ../...<. ...X.(.X
0020  92 c5 8a cb 00 a2 00 aa  f8 1d 30 81 9f 02 01 01   ........ ..0.....
0030  04 09 61 75 74 6f 2d 73  6e 6d 70 a7 81 8e 02 01   ..auto-s nmp.....
0040  1f 02 01 00 02 01 00 30  81 82 30 0f 06 08 2b 06   .......0 ..0...+.
0050  01 02 01 01 03 00 43 03  6f b7 58 30 17 06 0a 2b   ......C. o.X0...+
0060  06 01 06 03 01 01 04 01  00 06 09 2b 06 01 02 01   ........ ...+....
0070  0e 10 02 10 30 11 06 09  2b 06 01 02 01 0e 01 01   ....0... +.......
0080  00 40 04 13 58 c1 83 30  17 06 0f 2b 06 01 02 01   .@..X..0 ...+....
0090  0e 07 01 01 13 58 81 40  1b 00 40 04 13 58 c0 1b   .....X.@ ..@..X..
00a0  30 14 06 0f 2b 06 01 02  01 0e 07 01 02 13 58 81   0...+... ......X.
00b0  40 1b 00 02 01 00 30 14  06 0f 2b 06 01 02 01 0e   @.....0. ..+.....
00c0  07 01 0c 13 58 81 40 1b  00 02 01 01               ....X.@. ....
```

SNMP Community

https://snmp.cloudapps.cisco.com/Support/SNMP/do/BrowseOID.do?local=en

Specific Object Information

Object	ospfIfState
OID	1.3.6.1.2.1.14.7.1.12
Type	INTEGER
Permission	read-only
Status	current
Values	1 : down 2 : loopback 3 : waiting 4 : pointToPoint 5 : designatedRouter 6 : backupDesignatedRouter 7 : otherDesignatedRouter
MIB	OSPF-MIB ; - View Supporting Images
Description	The OSPF Interface State.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

External Network Connectivity UP– SNMP Trap

No.	Time	Source	Destination	Protocol	Length	Info
5	203.129882	[redacted].88.196.40	[redacted].88.146.197	SNMP	207	snmpV2-trap 1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.1.4.1.0 1.3.6.1.2.1.2.2.1.7.436219904 1.3.6.1.2.1.2.2.1.1.436219904 1.3.6.1.2.1.2.2.1.8.436219904 1.3.6.1.6.3.1.1.4.3.0
6	203.230214	[redacted].88.196.40	[redacted].88.146.197	SNMP	204	snmpV2-trap 1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.1.4.1.0 1.3.6.1.2.1.14.1.1.0 1.3.6.1.2.1.14.7.1.1.[redacted]88.192.27.0 1.3.6.1.2.1.14.7.1.2.[redacted].192.27.0 1.3.6.1.2.1.14.7.1
7	206.734440	[redacted].88.196.40	[redacted].88.146.197	SNMP	229	snmpV2-trap 1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.1.4.1.0 1.3.6.1.2.1.14.1.1.0 1.3.6.1.2.1.14.10.1.1[redacted].88.192.26.0 1.3.6.1.2.1.14.10.1.2[redacted]88.192.26.0 1.3.6.1.2.1.14.1
8	207.836111	[redacted].88.196.40	[redacted].88.146.197	SNMP	229	snmpV2-trap 1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.1.4.1.0 1.3.6.1.2.1.14.1.1.0 1.3.6.1.2.1.14.10.1.1[redacted].88.192.26.0 1.3.6.1.2.1.14.10.1.2[redacted]88.192.26.0 1.3.6.1.2.1.14.1
9	207.936577	[redacted].88.196.40	[redacted].88.146.197	SNMP	229	snmpV2-trap 1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.1.4.1.0 1.3.6.1.2.1.14.1.1.0 1.3.6.1.2.1.14.10.1.1[redacted].88.192.26.0 1.3.6.1.2.1.14.10.1.2[redacted]88.192.26.0 1.3.6.1.2.1.14.1

```
community: auto-snmp
▼ data: snmpV2-trap (7)
  ▼ snmpV2-trap
      request-id: 34
      error-status: noError (0)
      error-index: 0
    ▼ variable-bindings: 6 items
      ▼ 1.3.6.1.2.1.1.3.0: 7341736
          Object Name: 1.3.6.1.2.1.1.3.0 (iso.3.6.1.2.1.1.3.0)
          Value (Timeticks): 7341736
      ▼ 1.3.6.1.6.3.1.1.4.1.0: 1.3.6.1.2.1.14.16.2.16 (iso.3.6.1.2.1.14.16.2.16)
          Object Name: 1.3.6.1.6.3.1.1.4.1.0 (iso.3.6.1.6.3.1.1.4.1.0)
          Value (OID): 1.3.6.1.2.1.14.16.2.16 (iso.3.6.1.2.1.14.16.2.16)
      ▼ 1.3.6.1.2.1.14.1.1.0: [redacted].88.193.131
          Object Name: 1.3.6.1.2.1.14.1.1.0 (iso.3.6.1.2.1.14.1.1.0)
          Value (IpAddress): [redacted]88.193.131
      ▼ 1.3.6.1.2.1.14.7.1.1.[redacted]88.192.27.0: [redacted]88.192.27
          Object Name: 1.3.6.1.2.1.14.7.1.1.[redacted].88.192.27.0 (iso.3.6.1.2.1.14.7.1.[redacted].88.192.27.0)
          Value (IpAddress): [redacted].88.192.27
      ▼ 1.3.6.1.2.1.14.7.1.2.[redacted]88.192.27.0: 0
          Object Name: 1.3.6.1.2.1.14.7.1.2.19[redacted].27.0 (iso.3.6.1.2.1.14.7.1.2.[redacted]88.192.27.0)
          Value (Integer32): 0
      ▼ 1.3.6.1.2.1.14.7.1.12.[redacted].192.27.0: 4
          Object Name: 1.3.6.1.2.1.14.7.1.12.[redacted].88.192.27.0 (iso.3.6.1.2.1.14.7.1.12.[redacted].88.192.27.0)
          Value (Integer32): 4
```

```
0000  00 50 56 a1 bd a2 e4 c7  22 0d 4c 43 08 00 45 00   .PV..... ".LC..E.
0010  00 be b1 e5 00 00 3c 11  4e ac 13 58 c4 28 13 58   ......<. N..X.(.X
0020  92 c5 8a cb 00 a2 00 aa  a4 cb 30 81 9f 02 01 01   ........ ..0.....
0030  04 09 61 75 74 6f 2d 73  6e 6d 70 a7 81 8e 02 01   ..auto-s nmp.....
0040  22 02 01 00 02 01 00 30  81 82 30 0f 06 08 2b 06   "......0 ..0...+.
0050  01 02 01 01 03 00 43 03  70 06 a8 30 17 06 0a 2b   ......C. p..0...+
0060  06 01 06 03 01 01 04 01  00 06 09 2b 06 01 02 01   ........ ...+....
0070  0e 10 02 10 30 11 06 09  2b 06 01 02 01 0e 01 01   ....0... +.......
0080  00 40 04 13 58 c1 83 30  17 06 0f 2b 06 01 02 01   .@..X..0 ...+....
0090  0e 07 01 01 13 58 81 40  1b 00 40 04 13 58 c0 1b   .....X.@ ..@..X..
00a0  30 14 06 0f 2b 06 01 02  01 0e 07 01 02 13 58 81   0...+... ......X.
00b0  40 1b 00 02 01 00 30 14  06 0f 2b 06 01 02 01 0e   @.....0. ..+.....
00c0  07 01 0c 13 58 81 40 1b  00 02 01 04               ....X.@. ....
```

SNMP Community

https://snmp.cloudapps.cisco.com/Support/SNMP/do/BrowseOID.do?local=en

Specific Object Information

Object	ospfIfState
OID	1.3.6.1.2.1.14.7.1.12
Type	INTEGER
Permission	read-only
Status	current
Values	1 : down 2 : loopback 3 : waiting 4 : pointToPoint 5 : designatedRouter 6 : backupDesignatedRouter 7 : otherDesignatedRouter
MIB	OSPF-MIB ; - View Supporting Images
Description	The OSPF Interface State.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

External Network Connectivity UP– SNMP Trap

No.	Time	Source	Destination	Protocol	Length	Info
5	203.129882	[redacted].88.196.40	[redacted].88.146.197	SNMP	207	snmpV2-trap 1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.1.4.1.0 1.3.6.1.2.1.2.2.1.7.436219904 1.3.6.1.2.1.2.2.1.1.436219904 1.3.6.1.2.1.2.2.1.8.436219904 1.3.6.1.6.3.1.1.4.3.0
6	203.230214	[redacted].88.196.40	[redacted].88.146.197	SNMP	204	snmpV2-trap 1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.1.4.1.0 1.3.6.1.2.1.14.1.1.0 1.3.6.1.2.1.14.7.1.1.[redacted].88.192.27.0 1.3.6.1.2.1.14.7.1.2.[redacted].88.192.27.0 1.3.6.1.2.1.14.7.1
7	206.734440	[redacted].88.196.40	[redacted].88.146.197	SNMP	229	snmpV2-trap 1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.1.4.1.0 1.3.6.1.2.1.14.1.1.0 1.3.6.1.2.1.14.10.1.1.[redacted].88.192.26.0 1.3.6.1.2.1.14.10.1.2.[redacted].88.192.26.0 1.3.6.1.2.1.14.1
8	207.836111	[redacted].88.196.40	[redacted].88.146.197	SNMP	229	snmpV2-trap 1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.1.4.1.0 1.3.6.1.2.1.14.1.1.0 1.3.6.1.2.1.14.10.1.1.[redacted].88.192.26.0 1.3.6.1.2.1.14.10.1.2.[redacted].88.192.26.0 1.3.6.1.2.1.14.1
9	207.936577	[redacted].88.196.40	[redacted].88.146.197	SNMP	229	snmpV2-trap 1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.1.4.1.0 1.3.6.1.2.1.14.1.1.0 1.3.6.1.2.1.14.10.1.1.[redacted].88.192.26.0 1.3.6.1.2.1.14.10.1.2.[redacted].88.192.26.0 1.3.6.1.2.1.14.1

```
▼ data: snmpV2-trap (7)
  ▼ snmpV2-trap
      request-id: 37
      error-status: noError (0)
      error-index: 0
    ▼ variable-bindings: 7 items
      ▼ 1.3.6.1.2.1.1.3.0: 7342205
          Object Name: 1.3.6.1.2.1.1.3.0 (iso.3.6.1.2.1.1.3.0)
          Value (Timeticks): 7342205
      ▼ 1.3.6.1.6.3.1.1.4.1.0: 1.3.6.1.2.1.14.16.2.2 (iso.3.6.1.2.1.14.16.2.2)
          Object Name: 1.3.6.1.6.3.1.1.4.1.0 (iso.3.6.1.6.3.1.1.4.1.0)
          Value (OID): 1.3.6.1.2.1.14.16.2.2 (iso.3.6.1.2.1.14.16.2.2)
      ▼ 1.3.6.1.2.1.14.1.1.0: [redacted].88.193.131
          Object Name: 1.3.6.1.2.1.14.1.1.0 (iso.3.6.1.2.1.14.1.1.0)
          Value (IpAddress): [redacted].88.193.131
      ▼ 1.3.6.1.2.1.14.10.1.1.[redacted].88.192.26.0: [redacted]88.192.26
          Object Name: 1.3.6.1.2.1.14.10.1.1.[redacted].88.192.26.0 (iso.3.6.1.2.1.14.10.1.1.[redacted].88.192.26.0)
          Value (IpAddress): [redacted].88.192.26
      ▼ 1.3.6.1.2.1.14.10.1.2.[redacted].88.192.26.0: 0
          Object Name: 1.3.6.1.2.1.14.10.1.2.[redacted].88.192.26.0 (iso.3.6.1.2.1.14.10.1.2.[redacted].88.192.26.0)
          Value (Integer32): 0
      ▼ 1.3.6.1.2.1.14.10.1.3.[redacted].88.192.26.0: [redacted]88.193.129
          Object Name: 1.3.6.1.2.1.14.10.1.3.[redacted].88.192.26.0 (iso.3.6.1.2.1.14.10.1.3.[redacted].88.192.26.0)
          Value (IpAddress): [redacted].88.193.129
      ▼ 1.3.6.1.2.1.14.10.1.6.[redacted].88.192.26.0: 8
          Object Name: 1.3.6.1.2.1.14.10.1.6.[redacted].88.192.26.0 (iso
          Value (Integer32): 8
```

https://snmp.cloudapps.cisco.com/Support/SNMP/do/BrowseOID.do?local=en

Specific Object Information

Object	ospfNbrState
OID	1.3.6.1.2.1.14.10.1.6
Type	INTEGER
Permission	read-only
Status	current
Values	1 : down 2 : attempt 3 : init 4 : twoWay 5 : exchangeStart 6 : exchange 7 : loading 8 : full
MIB	OSPF-MIB ; - View Supporting Images
Description	The state of the relationship with this neighbor.

OSPF Adjacency Log State
exchangeStart : 5
Exchange : 6
Full : 8

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

External Network Connectivity Down– Syslog

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	.88.196.40	.88.146.198	Syslog	173	LOCAL7.INFO: Dec 07 11:16:05.675 tcsh1-f02-b0201 %LOG_-6-SYSTEM_MSG [E4208843][transition][info][sys/phys-[eth1/4]] PhysIf eth1/4 modified\n
2	0.208658	.88.196.40	.88.146.198	Syslog	189	LOCAL7.INFO: Dec 07 11:16:05.884 tcsh1-f02-b0201 %LOG_-6-SYSTEM_MSG [E4205126][port-down][info][sys/phys-[eth1/4]/phys] Port is down. Reason: adminCfgChng\n
3	0.211054	.88.196.40	.88.146.198	Syslog	189	LOCAL7.INFO: Dec 07 11:16:05.886 tcsh1-f02-b0201 %LOG_-6-SYSTEM_MSG [E4215671][port-down][info][sys/phys-[eth1/4]/phys] Port is down. Reason: adminCfgChng\n
4	0.220849	.88.196.40	.88.146.198	Syslog	231	LOCAL7.INFO: Dec 07 11:16:05.896 tcsh1-f02-b0201 %LOG_-6-SYSTEM_MSG [E4205066][oper-state-change][info][sys/ospf/inst-default/dom-t01:standard/if-[eth1/4]] OSPF in
5	0.225741	.88.196.40	.88.146.198	Syslog	186	LOCAL7.INFO: Dec 07 11:16:05.901 tcsh1-f02-b0201 %LOG_-6-SYSTEM_MSG [E4208059][oper-state-change][info][sys/cdp/inst/if-[eth1/4]] CDP interface is Down\n

```
▶ Frame 4: 231 bytes on wire (1848 bits), 231 bytes captured (1848 bits) on interface 0
▶ Ethernet II, Src: Cisco_0d:4c:43 (e4:c7:22:0d:4c:43), Dst: Vmware_a1:ca:32 (00:50:56:a1:ca:32)
▶ Internet Protocol Version 4, Src: .88.196.40, Dst: .88.146.198
▶ User Datagram Protocol, Src Port: 46602, Dst Port: 514
▼ Syslog message: LOCAL7.INFO: Dec 07 11:16:05.896 tcsh1-f02-b0201 %LOG_-6-SYSTEM_MSG [E4205066][oper-state-change][info][sys/ospf/inst-default/dom-t01:standard/if-[eth1/4]] OSPF interface eth1/4 is changed to Down\n
    101. .... = Facility: LOCAL7 - reserved for local use (23)
    .... .110 = Level: INFO - informational (6)
    Message: Dec 07 11:16:05.896 tcsh1-f02-b0201 %LOG_-6-SYSTEM_MSG [E4205066][oper-state-change][info][sys/ospf/inst-default/dom-t01:standard/if-[eth1/4]] OSPF interface eth1/4 is changed to Down\n
```

```
0000  00 50 56 a1 ca 32 e4 c7  22 0d 4c 43 08 00 45 00   .PV..2.. ".LC..E.
0010  00 d9 eb c0 00 00 3c 11  14 b5 13 58 c4 28 13 58   ......<. ...X.(.X
0020  92 c6 b6 0a 02 02 00 c5  09 c2 3c 31 39 30 3e 44   ........ ..<190>D
0030  65 63 20 30 37 20 31 31  3a 31 36 3a 30 35 2e 38   ec 07 11 :16:05.8
0040  39 36 20 74 63 73 68 31  2d 66 30 32 2d 62 30 32   96 tcsh1 -f02-b02
0050  30 31 20 25 4c 4f 47 5f  2d 36 2d 53 59 53 54 45   01 %LOG_ -6-SYSTE
0060  4d 5f 4d 53 47 20 5b 45  34 32 30 35 30 36 36 5d   M_MSG [E 4205066]
0070  5b 6f 70 65 72 2d 73 74  61 74 65 2d 63 68 61 6e   [oper-st ate-chan
0080  67 65 5d 5b 69 6e 66 6f  5d 5b 73 79 73 2f 6f 73   ge][info ][sys/os
0090  70 66 2f 69 6e 73 74 2d  64 65 66 61 75 6c 74 2f   pf/inst- default/
00a0  64 6f 6d 2d 74 30 31 3a  73 74 61 6e 64 61 72 64   dom-t01: standard
00b0  2f 69 66 2d 5b 65 74 68  31 2f 34 5d 5d 20 4f 53   /if-[eth 1/4]] OS
00c0  50 46 20 69 6e 74 65 72  66 61 63 65 20 65 74 68   PF inter face eth
00d0  31 2f 34 20 69 73 20 63  68 61 6e 67 65 64 20 74   1/4 is c hanged t
00e0  6f 20 44 6f 77 6e 0a                              o Down.
```

Also parse OSPF Peer Down Fault F1385

BGP Peer Down F0299

```
Dec 13 23:03:30.361 dc1h1-f91-h1003 %LOG_-4-SYSTEM_MSG [F0299][soaking][protocol-bgp-adjacency-down][warning][sys/bgp/inst/dom-t01:standard/peer-[.34.174.20/32]/ent-[.34.174.20]/fault-F0299]
```


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

External Network Connectivity UP– Syslog

```
No.   Time        Source          Destination     Protocol  Length  Info
   17 206.860275  [redacted].88.196.40  [redacted].88.146.198  Syslog    290  LOCAL7.WARNING: Dec 07 11:19:32.545 tcsh1-f02-b0201 %LOG_-4-SYSTEM_MSG [F1385][soaking][protocol-ospf-adjacency-down][warning][sys/ospf/inst-default/dom-t01:standa
   18 206.862844  [redacted].88.196.40  [redacted].88.146.198  Syslog    251  LOCAL7.INFO: Dec 07 11:19:32.547 tcsh1-f02-b0201 %LOG_-6-SYSTEM_MSG [E4205067][oper-state-change][info][sys/ospf/inst-default/dom-t01:standard/if-[eth1/4]/adj-[redacted].8
   19 207.976144  [redacted].88.196.40  [redacted].88.146.198  Syslog    252  LOCAL7.INFO: Dec 07 11:19:33.661 tcsh1-f02-b0201 %LOG_-6-SYSTEM_MSG [E4205067][oper-state-change][info][sys/ospf/inst-default/dom-t01:standard/if-[eth1/4]/adj-[redacted].8
   20 207.998981  [redacted].88.196.40  [redacted].88.146.198  Syslog    300  LOCAL7.WARNING: Dec 07 11:19:33.684 tcsh1-f02-b0201 %LOG_-4-SYSTEM_MSG [F1385][soaking_clearing][protocol-ospf-adjacency-down][warning][sys/ospf/inst-default/dom-t
L  21 207.999951  [redacted].88.196.40  [redacted].88.146.198  Syslog    248  LOCAL7.INFO: Dec 07 11:19:33.685 tcsh1-f02-b0201 %LOG_-6-SYSTEM_MSG [E4205067][oper-state-change][info][sys/ospf/inst-default/dom-t01:standard/if-[eth1/4]/adj-[redacted].8

▶ Frame 21: 248 bytes on wire (1984 bits), 248 bytes captured (1984 bits) on interface 0
▶ Ethernet II, Src: Cisco_0d:4c:43 (e4:c7:22:0d:4c:43), Dst: Vmware_a1:ca:32 (00:50:56:a1:ca:32)
▶ Internet Protocol Version 4, Src: [redacted].88.196.40, Dst: [redacted].88.146.198
▶ User Datagram Protocol, Src Port: 46602, Dst Port: 514
▼ Syslog message: LOCAL7.INFO: Dec 07 11:19:33.685 tcsh1-f02-b0201 %LOG_-6-SYSTEM_MSG [E4205067][oper-state-change][info][sys/ospf/inst-default/dom-t01:standard/if-[eth1/4]/adj-[redacted].88.193.129] OSPF adjacency state is changed to Full\n
    1011 1... = Facility: LOCAL7 - reserved for local use (23)
    .... .110 = Level: INFO - informational (6)
    Message: Dec 07 11:19:33.685 tcsh1-f02-b0201 %LOG_-6-SYSTEM_MSG [E4205067][oper-state-change][info][sys/ospf/inst-default/dom-t01:standard/if-[eth1/4]/adj-[redacted].88.193.129] OSPF adjacency state is changed to Full\n

0000  00 50 56 a1 ca 32 e4 c7  22 0d 4c 43 08 00 45 00   .PV..2.. ".LC..E.
0010  00 ea ae e1 00 00 3c 11  51 83 13 58 c4 28 13 58   ......<. Q..X.(.X
0020  92 c6 b6 0a 02 02 00 d6  8a b9 3c 31 39 30 3e 44   ........ ..<190>D
0030  65 63 20 30 37 20 31 31  3a 31 39 3a 33 33 2e 36   ec 07 11 :19:33.6
0040  38 35 20 74 63 73 68 31  2d 66 30 32 2d 62 30 32   85 tcsh1 -f02-b02
0050  30 31 20 25 4c 4f 47 5f  2d 36 2d 53 59 53 54 45   01 %LOG_ -6-SYSTE
0060  4d 5f 4d 53 47 20 5b 45  34 32 30 35 30 36 37 5d   M_MSG [E 4205067]
0070  5b 6f 70 65 72 2d 73 74  61 74 65 2d 63 68 61 6e   [oper-st ate-chan
0080  67 65 5d 5b 69 6e 66 6f  5d 5b 73 79 73 2f 6f 73   ge][info ][sys/os
0090  70 66 2f 69 6e 73 74 2d  64 65 66 61 75 6c 74 2f   pf/inst- default/
00a0  64 6f 6d 2d 74 30 31 3a  73 74 61 6e 64 61 72 64   dom-t01: standard
00b0  2f 69 66 2d 5b 65 74 68  31 2f 34 5d 2f 61 64 6a   /if-[eth 1/4]/adj
00c0  2d 31 39 2e 38 38 2e 31  39 33 2e 31 32 39 5d 20   -[redacted].88.1 93.129]
00d0  4f 53 50 46 20 61 64 6a  61 63 65 6e 63 79 20 73   OSPF adj acency s
00e0  74 61 74 65 20 69 73 20  63 68 61 6e 67 65 64 20   tate is  changed
00f0  74 6f 20 46 75 6c 6c 0a                            to Full.
```

ACI Log State	OSPF Adjacency Log State
Soaking	Not Full – INIT
Soaking_Clearing	Exstart
	Exchange
	Full

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Use Case - 6

Leaf/Spine Reload– SNMP Trap

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	[redacted].88.196.194	[redacted].88.146.197	SNMP	137	snmpV2-trap 1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.1.4.1.0 1.3.6.1.6.3.1.1.4.3.0
2	0.100450	[redacted].88.196.194	[redacted].88.146.197	SNMP	199	snmpV2-trap 1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.1.4.1.0 1.3.6.1.2.1.14.1.1.0 1.3.6.1.2.1.14.7.1.1.0.0.0.0.0 1.3.6.1.2.1.14.7.1.2.0.0.0.0.0 1.3.6.1.2.1.14.7.1.12.0.0.0.0
3	0.200681	[redacted].88.196.194	[redacted].88.146.197	SNMP	199	snmpV2-trap 1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.1.4.1.0 1.3.6.1.2.1.47.1.1.1.1.4.48 1.3.6.1.2.1.47.1.1.1.1.2.48 1.3.6.1.2.1.47.1.1.1.1.7.48
4	0.302278	[redacted].88.196.194	[redacted].88.146.197	SNMP	156	snmpV2-trap 1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.1.4.1.0 1.3.6.1.4.1.9.9.117.1.2.1.1.2.48 1.3.6.1.4.1.9.9.117.1.2.1.1.4.48
5	0.401342	[redacted].88.196.194	[redacted].88.146.197	SNMP	156	snmpV2-trap 1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.1.4.1.0 1.3.6.1.4.1.9.9.117.1.1.2.1.2.48 1.3.6.1.4.1.9.9.117.1.1.2.1.1.48

```
▶ Frame 1: 137 bytes on wire (1096 bits), 137 bytes captured (1096 bits) on interface 0
▶ Ethernet II, Src: Cisco_0d:4c:43 (e4:c7:22:0d:4c:43), Dst: Vmware_a1:bd:a2 (00:50:56:a1:bd:a2)
▶ Internet Protocol Version 4, Src: [redacted].88.196.194, Dst: [redacted].88.146.197
▶ User Datagram Protocol, Src Port: 56529, Dst Port: 162
▼ Simple Network Management Protocol
    version: v2c (1)
    community: auto-snmp
  ▼ data: snmpV2-trap (7)
    ▼ snmpV2-trap
        request-id: 1
        error-status: noError (0)
        error-index: 0
      ▼ variable-bindings: 3 items
        ▶ 1.3.6.1.2.1.1.3.0: 20392
        ▼ 1.3.6.1.6.3.1.1.4.1.0: 1.3.6.1.6.3.1.1.5.1 (iso.3.6.1.6.3.1.1.5.1)
            Object Name: 1.3.6.1.6.3.1.1.4.1.0 (iso.3.6.1.6.3.1.1.4.1.0)
            Value (OID): 1.3.6.1.6.3.1.1.5.1 (iso.3.6.1.6.3.1.1.5.1)
```

https://snmp.cloudapps.cisco.com/Support/SNMP/do/BrowseOID.do?local=en

Specific Object Information

Object	coldStart
OID	1.3.6.1.6.3.1.1.5.1
Status	current
MIB	SNMPv2-MIB ; - View Supporting Images
Description	"A coldStart trap signifies that the SNMP entity, supporting a notification originator application, is reinitializing itself and that its configuration may have been altered."

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Leaf/Spine Reload– Syslog

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	[redacted].88.196.194	[redacted].88.146.198	Syslog	179	LOCAL7.INFO: Dec 06 16:46:22.750 tcsh2-f02-h1003 %LOG_-6-SYSTEM_MSG [E4205231][transition][info][sys/action/lsubj-[sys/ch]] LSubj sys/ch created\n
2	1.314162	[redacted].88.196.194	[redacted].88.146.198	Syslog	182	LOCAL7.CRIT: Dec 06 16:46:24.065 tcsh2-f02-h1003 %LOG_-2-SYSTEM_MSG [E4204936][transition][critical][sys] %PLATFORM-1-PFM_ALERT: Rebooting Chassis\n
3	1.345841	[redacted].88.196.195	[redacted].88.146.198	Syslog	220	LOCAL7.ERR: Dec 06 16:46:24.096 tcsh2-f02-h1004 %LOG_-3-SYSTEM_MSG [F0508][soaking][vpc-domain-down][major][sys/vpc/inst/dom-2/fault-F0508] vPC domain bringup faile
4	1.360640	[redacted].88.196.195	[redacted].88.146.198	Syslog	191	LOCAL7.INFO: Dec 06 16:46:24.111 tcsh2-f02-h1004 %LOG_-6-SYSTEM_MSG [E4205118][role-change][info][sys/vpc/inst/dom-2] vPC role status has changed to Master.\n
5	1.366964	[redacted].88.196.195	[redacted].88.146.198	Syslog	194	LOCAL7.INFO: Dec 06 16:46:24.117 tcsh2-f02-h1004 %LOG_-6-SYSTEM_MSG [E4205116][peer-if-down][info][sys/vpc/inst/dom-2/if-1] Peer vPC 1003-1004-vpc-e17 is down.\n
6	1.374925	[redacted].88.196.195	[redacted].88.146.198	Syslog	193	LOCAL7.INFO: Dec 06 16:46:24.125 tcsh2-f02-h1004 %LOG_-6-SYSTEM_MSG [E4205116][peer-if-down][info][sys/vpc/inst/dom-2/if-2] Peer vPC 1003-1004-vpc-e2 is down.\n
7	1.389570	[redacted].88.196.195	[redacted].88.146.198	Syslog	221	LOCAL7.ERR: Dec 06 16:46:24.140 tcsh2-f02-h1004 %LOG_-3-SYSTEM_MSG [F0475][soaking][interface-tunnel-down][major][sys/tunnel-[tunnel18]/fault-F0475] Tunnel destinat
8	1.397702	[redacted].88.196.195	[redacted].88.146.198	Syslog	219	LOCAL7.INFO: Dec 06 16:46:24.148 tcsh2-f02-h1004 %LOG_-6-SYSTEM_MSG [E4208070][oper-state-change][info][sys/tunnel-[tunnel18]] Interface tunnel18 is down reason Des
9	1.461967	[redacted].88.196.131	[redacted].88.146.198	Syslog	220	LOCAL7.ERR: Dec 06 16:46:24.212 tcsh1-f02-h1002 %LOG_-3-SYSTEM_MSG [F0475][soaking][interface-tunnel-down][major][sys/tunnel-[tunnel1]/fault-F0475] Tunnel destinati

```
▶ Frame 2: 182 bytes on wire (1456 bits), 182 bytes captured (1456 bits) on interface 0
▶ Ethernet II, Src: Cisco_0d:4c:43 (e4:c7:22:0d:4c:43), Dst: Vmware_a1:ca:32 (00:50:56:a1:ca:32)
▶ Internet Protocol Version 4, Src: [redacted].88.196.194, Dst: [redacted].88.146.198
▶ User Datagram Protocol, Src Port: 37460, Dst Port: 514
▼ Syslog message: LOCAL7.CRIT: Dec 06 16:46:24.065 tcsh2-f02-h1003 %LOG_-2-SYSTEM_MSG [E4204936][transition][critical][sys]  %PLATFORM-1-PFM_ALERT: Rebooting Chassis\n
    1011 1... = Facility: LOCAL7 - reserved for local use (23)
    .... .010 = Level: CRIT - critical conditions (2)
    Message: Dec 06 16:46:24.065 tcsh2-f02-h1003 %LOG_-2-SYSTEM_MSG [E4204936][transition][critical][sys]  %PLATFORM-1-PFM_ALERT: Rebooting Chassis\n
```

▼ Syslog message: LOCAL7.CRIT: Dec 06 16:46:24.065 tcsh2-f02-h1003 %LOG_-2-SYSTEM_MSG [E4204936][transition][critical][sys] %PLATFORM-1-PFM_ALERT: Rebooting Chassis\n

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Use Case - 7

VPC Down/UP – SNMP Trap

No.	Time	Source	Destination	Protocol	Length	Info
224	134.625374	.88.196.194	.88.146.197	SNMP	171	snmpV2-trap 1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.1.4.1.0 1.3.6.1.4.1.9.9.187.1.2.5.1.17.1.4.10.2.20.65 1.3.6.1.4.1.9.9.187.1.2.5.1.3.1.4.10.2.20.65
225	183.683380	.88.196.194	.88.146.197	SNMP	286	snmpV2-trap 1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.1.4.1.0 1.3.6.1.2.1.2.2.1.1.436211712 1.3.6.1.2.1.2.2.1.7.436211712 1.3.6.1.2.1.2.2.1.8.436211712 1.3.6.1.2.1.31.1.1.1.1
226	183.783782	.88.196.194	.88.146.197	SNMP	208	snmpV2-trap 1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.1.4.1.0 1.3.6.1.2.1.2.2.1.7.436211712 1.3.6.1.2.1.2.2.1.1.436211712 1.3.6.1.2.1.2.2.1.8.436211712 1.3.6.1.6.3.1.1.4.3.0
227	183.884023	.88.196.194	.88.146.197	SNMP	274	snmpV2-trap 1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.1.4.1.0 1.3.6.1.2.1.2.2.1.1.369098752 1.3.6.1.2.1.2.2.1.7.369098752 1.3.6.1.2.1.2.2.1.8.369098752 1.3.6.1.2.1.31.1.1.1.1
228	183.984369	.88.196.194	.88.146.197	SNMP	208	snmpV2-trap 1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.1.4.1.0 1.3.6.1.2.1.2.2.1.7.369098752 1.3.6.1.2.1.2.2.1.1.369098752 1.3.6.1.2.1.2.2.1.8.369098752 1.3.6.1.6.3.1.1.4.3.0
229	184.685690	.88.196.194	.88.146.197	SNMP	282	snmpV2-trap 1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.1.4.1.0 1.3.6.1.2.1.2.2.1.1.436273152 1.3.6.1.2.1.2.2.1.7.436273152 1.3.6.1.2.1.2.2.1.8.436273152 1.3.6.1.2.1.31.1.1.1.1
230	184.785925	.88.196.194	.88.146.197	SNMP	208	snmpV2-trap 1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.1.4.1.0 1.3.6.1.2.1.2.2.1.7.436273152 1.3.6.1.2.1.2.2.1.1.436273152 1.3.6.1.2.1.2.2.1.8.436273152 1.3.6.1.6.3.1.1.4.3.0
231	184.886229	.88.196.194	.88.146.197	SNMP	274	snmpV2-trap 1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.1.4.1.0 1.3.6.1.2.1.2.2.1.1.369098753 1.3.6.1.2.1.2.2.1.7.369098753 1.3.6.1.2.1.2.2.1.8.369098753 1.3.6.1.2.1.31.1.1.1.1
232	184.986564	.88.196.194	.88.146.197	SNMP	208	snmpV2-trap 1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.1.4.1.0 1.3.6.1.2.1.2.2.1.7.369098753 1.3.6.1.2.1.2.2.1.1.369098753 1.3.6.1.2.1.2.2.1.8.369098753 1.3.6.1.6.3.1.1.4.3.0

```
Frame 231: 274 bytes on wire (2192 bits), 274 bytes captured (2192 bits) on interface 0
Ethernet II, Src: Cisco_0d:4c:43 (e4:c7:22:0d:4c:43), Dst: Vmware_a1:bd:a2 (00:50:56:a1:bd:a2)
Internet Protocol Version 4, Src: 88.196.194, Dst: .88.146.197
User Datagram Protocol, Src Port: 56529, Dst Port: 162
Simple Network Management Protocol
    version: v2c (1)
    community: auto-snmp
    data: snmpV2-trap (7)
        snmpV2-trap
            request-id: 231
            error-status: noError (0)
            error-index: 0
```

```
1.3.6.1.2.1.2.2.1.7.369098753: 1
    Object Name: 1.3.6.1.2.1.2.2.1.7.369098753 (iso.3.6.1.2.1.2.2.1.7.369098753)
    Value (Integer32): 1
1.3.6.1.2.1.2.2.1.8.369098753: 2
    Object Name: 1.3.6.1.2.1.2.2.1.8.369098753 (iso.3.6.1.2.1.2.2.1.8.369098753)
    Value (Integer32): 2
1.3.6.1.2.1.31.1.1.1.1.369098753: 706f32
    Object Name: 1.3.6.1.2.1.31.1.1.1.1.369098753 (iso.3.6.1.2.1.31.1.1.1.1.369098753)
    Value (OctetString): 706f32
1.3.6.1.2.1.2.2.1.3.369098753: 53
```

https://snmp.cloudapps.cisco.com/Support/SNMP/do/BrowseOID.do?local=en

Specific Object Information

Object	ifOperStatus
OID	1.3.6.1.2.1.2.2.1.8
Type	INTEGER
Permission	read-only
Status	current
Values	1 : up 2 : down 3 : testing 4 : unknown 5 : dormant 6 : notPresent 7 : lowerLayerDown
MIB	IF-MIB ; - View Supporting Images

Po2 – Hex Value to be converted to ASCII

```
1.3.6.1.2.1.2.2.1.7.369098753: 1
    Object Name: 1.3.6.1.2.1.2.2.1.7.369098753 (iso.3.6.1.2.1.2.2.1.7.369098753)
    Value (Integer32): 1
1.3.6.1.2.1.2.2.1.8.369098753: 1
    Object Name: 1.3.6.1.2.1.2.2.1.8.369098753 (iso.3.6.1.2.1.2.2.1.8.369098753)
    Value (Integer32): 1
1.3.6.1.2.1.31.1.1.1.1.369098753: 706f32
    Object Name: 1.3.6.1.2.1.31.1.1.1.1.369098753 (iso.3.6.1.2.1.31.1.1.1.1.369098753)
    Value (OctetString): 706f32
1.3.6.1.2.1.2.2.1.3.369098753: 53
    Object Name: 1.3.6.1.2.1.2.2.1.3.369098753 (iso.3.6.1.2.1.2.2.1.3.369098753)
    Value (Integer32): 53
```

Po2 – Hex Value to be converted to ASCII

Specific Object Information

Object	ifType
OID	1.3.6.1.2.1.2.2.1.3
Type	IANAifType

53:propVirtual

VPC Down/UP – Syslog

Also parse on System Message F1296, F2705

No.	Time	Source	Destination	Protocol	Length	Info
6	1.374925	.88.196.195	.88.146.198	Syslog	193	LOCAL7.INFO: Dec 06 16:46:24.125 tcsh2-f02-h1004 %LOG_-6-SYSTEM_MSG [E4205116][peer-if-down][info][sys/vpc/inst/dom-2/if-2] Peer vPC 1003-1004-vpc-e2 is down.\n
7	1.389570	.88.196.195	.88.146.198	Syslog	221	LOCAL7.ERR: Dec 06 16:46:24.140 tcsh2-f02-h1004 %LOG_-3-SYSTEM_MSG [F0475][soaking][interface-tunnel-down][major][sys/tunnel-[tunnel18]/fault-F0475] Tunnel destinat
8	1.397702	.88.196.195	.88.146.198	Syslog	219	LOCAL7.INFO: Dec 06 16:46:24.148 tcsh2-f02-h1004 %LOG_-6-SYSTEM_MSG [E4208070][oper-state-change][info][sys/tunnel-[tunnel18]] Interface tunnel18 is down reason Des
9	1.461967	.88.196.131	.88.146.198	Syslog	220	LOCAL7.ERR: Dec 06 16:46:24.212 tcsh1-f02-h1002 %LOG_-3-SYSTEM_MSG [F0475][soaking][interface-tunnel-down][major][sys/tunnel-[tunnel1]/fault-F0475] Tunnel destinati
10	1.462123	.88.196.130	.88.146.198	Syslog	221	LOCAL7.ERR: Dec 06 16:46:24.211 tcsh1-f02-h1001 %LOG_-3-SYSTEM_MSG [F0475][soaking][interface-tunnel-down][major][sys/tunnel-[tunnel18]/fault-F0475] Tunnel destinat

```
Frame 6: 193 bytes on wire (1544 bits), 193 bytes captured (1544 bits) on interface 0
Ethernet II, Src: Cisco_0d:4c:43 (e4:c7:22:0d:4c:43), Dst: Vmware_a1:ca:32 (00:50:56:a1:ca:32)
Internet Protocol Version 4, Src: 88.196.195, Dst: 88.146.198
User Datagram Protocol, Src Port: 58273, Dst Port: 514
Syslog message: LOCAL7.INFO: Dec 06 16:46:24.125 tcsh2-f02-h1004 %LOG_-6-SYSTEM_MSG [E4205116][peer-if-down][info][sys/vpc/inst/dom-2/if-2] Peer vPC 1003-1004-vpc-e2 is down.\n
    1011 1... = Facility: LOCAL7 - reserved for local use (23)
    .... .110 = Level: INFO - informational (6)
    Message: Dec 06 16:46:24.125 tcsh2-f02-h1004 %LOG_-6-SYSTEM_MSG [E4205116][peer-if-down][info][sys/vpc/inst/dom-2/if-2] Peer vPC 1003-1004-vpc-e2 is down.\n
```

```
▼ Syslog message: LOCAL7.INFO: Dec 06 16:46:24.125 tcsh2-f02-h1004 %LOG_-6-SYSTEM_MSG [E4205116][peer-if-down][info][sys/vpc/inst/dom-2/if-2] Peer vPC 1003-1004-vpc-e2 is down.\n
```

No.	Time	Source	Destination	Protocol	Length	Info
805	598.564075	.88.196.194	.88.146.198	Syslog	190	LOCAL7.INFO: Dec 06 16:56:21.341 tcsh2-f02-h1003 %LOG_-6-SYSTEM_MSG [E4205113][interface-vpc-up][info][sys/vpc/inst/dom-2/if-2] vPC 1003-1004-vpc-e2 is up.\n
806	598.860094	.88.196.194	.88.146.198	Syslog	189	LOCAL7.INFO: Dec 06 16:56:21.637 tcsh2-f02-h1003 %LOG_-6-SYSTEM_MSG [E4205129][fop-change][info][sys/aggr-[po1]] first operational port changed to eth1/2.\n
807	598.864072	.88.196.194	.88.146.198	Syslog	169	LOCAL7.INFO: Dec 06 16:56:21.641 tcsh2-f02-h1003 %LOG_-6-SYSTEM_MSG [E4205127][port-up][info][sys/phys-[eth1/2]/aggrmbrif] Port is up.\n
808	598.869885	.88.196.194	.88.146.198	Syslog	254	LOCAL7.CRIT: Dec 06 16:56:21.647 tcsh2-f02-h1003 %LOG_-2-SYSTEM_MSG [F0532][raised_clearing][interface-physical-down][critical][sys/phys-[eth1/2]/phys/fault-F0532]
809	598.873630	.88.196.194	.88.146.198	Syslog	163	LOCAL7.INFO: Dec 06 16:56:21.651 tcsh2-f02-h1003 %LOG_-6-SYSTEM_MSG [E4205125][port-up][info][sys/phys-[eth1/2]/phys] Port is up\n

```
Frame 805: 190 bytes on wire (1520 bits), 190 bytes captured (1520 bits) on interface 0
Ethernet II, Src: Cisco_0d:4c:43 (e4:c7:22:0d:4c:43), Dst: Vmware_a1:ca:32 (00:50:56:a1:ca:32)
Internet Protocol Version 4, Src: 88.196.194, Dst: 88.146.198
User Datagram Protocol, Src Port: 40485, Dst Port: 514
Syslog message: LOCAL7.INFO: Dec 06 16:56:21.341 tcsh2-f02-h1003 %LOG_-6-SYSTEM_MSG [E4205113][interface-vpc-up][info][sys/vpc/inst/dom-2/if-2] vPC 1003-1004-vpc-e2 is up.\n
    1011 1... = Facility: LOCAL7 - reserved for local use (23)
    .... .110 = Level: INFO - informational (6)
    Message: Dec 06 16:56:21.341 tcsh2-f02-h1003 %LOG_-6-SYSTEM_MSG [E4205113][interface-vpc-up][info][sys/vpc/inst/dom-2/if-2] vPC 1003-1004-vpc-e2 is up.\n
```

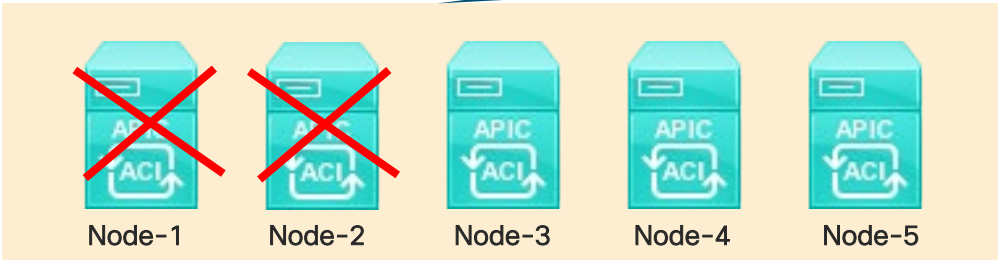
```
▼ Syslog message: LOCAL7.INFO: Dec 06 16:56:21.341 tcsh2-f02-h1003 %LOG_-6-SYSTEM_MSG [E4205113][interface-vpc-up][info][sys/vpc/inst/dom-2/if-2] vPC 1003-1004-vpc-e2 is up.\n
```


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Use Case - 8

APIC Cluster Issues- Syslog

APIC Cluster Degraded



Parse Faults F1262 and F0321

```
[truncated]Syslog message: LOCAL7.CRIT: Dec 11 15:05:55.486 tcsh1-f02-a0004 %LOG_-2-SYSTEM_MSG [F0321][soaking][unhealthy][critical][topology/pod-1/node-4/av/node-5/fault-F0321] Controller 5 is unhealthy because: Data Layer Partially Degr
[truncated]Syslog message: LOCAL7.CRIT: Dec 11 15:05:55.488 tcsh1-f02-a0004 %LOG_-2-SYSTEM_MSG [F0321][soaking][unhealthy][critical][topology/pod-1/node-4/av/node-3/fault-F0321] Controller 3 is unhealthy because: Data Layer Partially Degr
[truncated]Syslog message: LOCAL7.CRIT: Dec 11 15:05:55.490 tcsh1-f02-a0004 %LOG_-2-SYSTEM_MSG [F0321][soaking][unhealthy][critical][topology/pod-1/node-4/av/node-4/fault-F0321] Controller 4 is unhealthy because: Data Layer Partially Degr
Syslog message: LOCAL7.CRIT: Dec 11 15:05:55.492 tcsh1-f02-a0004 %LOG_-2-SYSTEM_MSG [F0321][soaking][unhealthy][critical][topology/pod-1/node-4/av/node-1/fault-F0321] Controller 1 is unhealthy because: Unknown\n
[truncated]Syslog message: LOCAL7.ERR: Dec 11 15:05:56.012 tcsh1-f02-a0004 %LOG_-3-SYSTEM_MSG [F1262][soaking][unhealthy][minor][topology/pod-1/node-4/lon/svc-ifc_bootmgr/fault-F1262] Non optimal leader for some database partitions of Acc
Syslog message: LOCAL7.CRIT: Dec 11 15:05:57.969 tcsh1-f02-a0004 %LOG_-2-SYSTEM_MSG [F0321][soaking][unhealthy][critical][topology/pod-1/node-4/av/node-2/fault-F0321] Controller 2 is unhealthy because: Unknown\n
```


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Use Case - 9

Fabric Issues- Syslog

Node Fabric port down F1394

5/20/19 6:02:22.000 PM
May 20 18:02:22 [redacted].88.196.40 Oct 01 13:02:24 tcsh1-f02-b0201 %LOG_LOCAL7-3-SYSTEM_MSG [F1394][soaking][interface-physical-down][minor][sys/phys-[eth1/30]/phys/fault-F1394] Port is down, reason:notconnect(connected), used by:Fabric
host = [redacted].88.196.40 | source = udp:514 | sourcetype = cisco_syslog

5/20/19 6:02:20.000 PM
May 20 18:02:20 [redacted].88.196.40 Oct 01 13:02:22 tcsh1-f02-b0201 %LOG_LOCAL7-3-SYSTEM_MSG [F1394][soaking][interface-physical-down][minor][sys/phys-[eth1/29]/phys/fault-F1394] Port is down, reason:sfpAbsent(connected), used by:Fabric
host = [redacted].88.196.40 | source = udp:514 | sourcetype = cisco_syslog

Node Fabric Tunnel Interface down F0475

5/20/19 6:02:22.000 PM
May 20 18:02:22 [redacted].88.196.40 Oct 01 13:02:24 tcsh1-f02-b0201 %LOG_LOCAL7-3-SYSTEM_MSG [F0475][soaking][interface-tunnel-down][major][sys/tunnel-[tunnel23]/fault-F0475] Tunnel destination is not reachable.
host = [redacted].88.196.40 | source = udp:514 | sourcetype = cisco_syslog

Node Fabric ISIS Adj down F0360

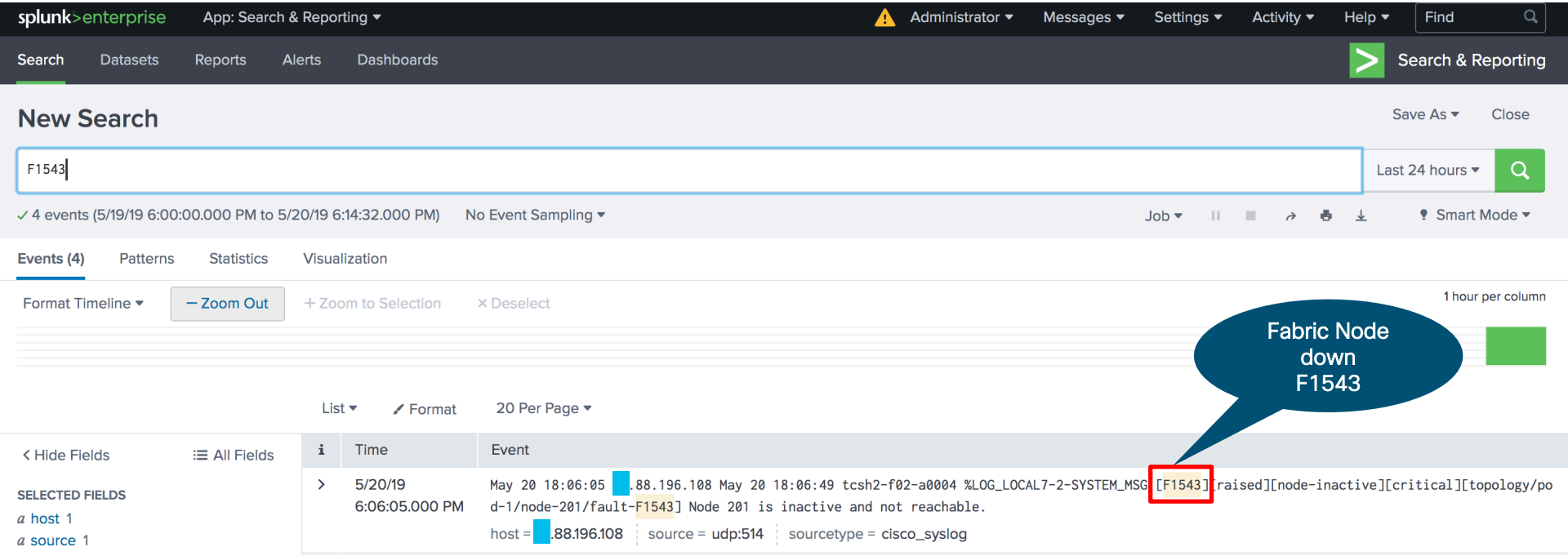
5/20/19 6:02:22.000 PM
May 20 18:02:22 [redacted].88.196.40 Oct 01 13:02:24 tcsh1-f02-b0201 %LOG_LOCAL7-4-SYSTEM_MSG [F0360][soaking][protocol-isis-down][warning][sys/isis/inst-default/dom-overlay-1/fmtree-12/fault-F0360] Tree id 12 with root 10.2.6.66 became inactive
host = [redacted].88.196.40 | source = udp:514 | sourcetype = cisco_syslog

Node Fabric CooP Adj down F1360

5/20/19 6:02:22.000 PM
May 20 18:02:22 [redacted].88.196.40 Oct 01 13:02:24 tcsh1-f02-b0201 %LOG_LOCAL7-4-SYSTEM_MSG [F1360][soaking][protocol-coop-adjacency-down][warning][sys/coop/inst/dom-overlay-1/oracle-[10.2.6.65/32]/fault-F1360] Operational state is down, reason:Route not reachable
host = [redacted].88.196.40 | source = udp:514 | sourcetype = cisco_syslog

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Fabric Issues- Syslog



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Use Case - 10

Hardware Issues- Syslog

Power Supply/FAN Failure
System Messages
F0411-F0413, F1317, F1318,
F1321-F1323, F1451

Apr 16 20:54:55 Lef101 %LOG_LOCAL7-3-SYSTEM_MSG [F0412][soaking_clearing][equipment-psufan-failed][minor][sys/ch/psuslot-2/psu/fault-F0412] Fan in power supply failed

Apr 16 21:30:13 Leaf101 %LOG_LOCAL7-6-SYSTEM_MSG [F0411][retaining][equipment-psu-failed][cleared][sys/ch/psuslot-2/psu/fault-F0411] Power supply failed. (serial number DBA21365760)

LC/FM Failure
System Messages
F1526

Feb 15 00:28:13 spine201 %LOG_LOCAL0-2-SYSTEM_MSG [F1526][raised][equipment-card-failed][critical][sys/ch/lcslot-1/fault-F1526] Module 1 failed

APIC HDD Failure
System Messages
F0101

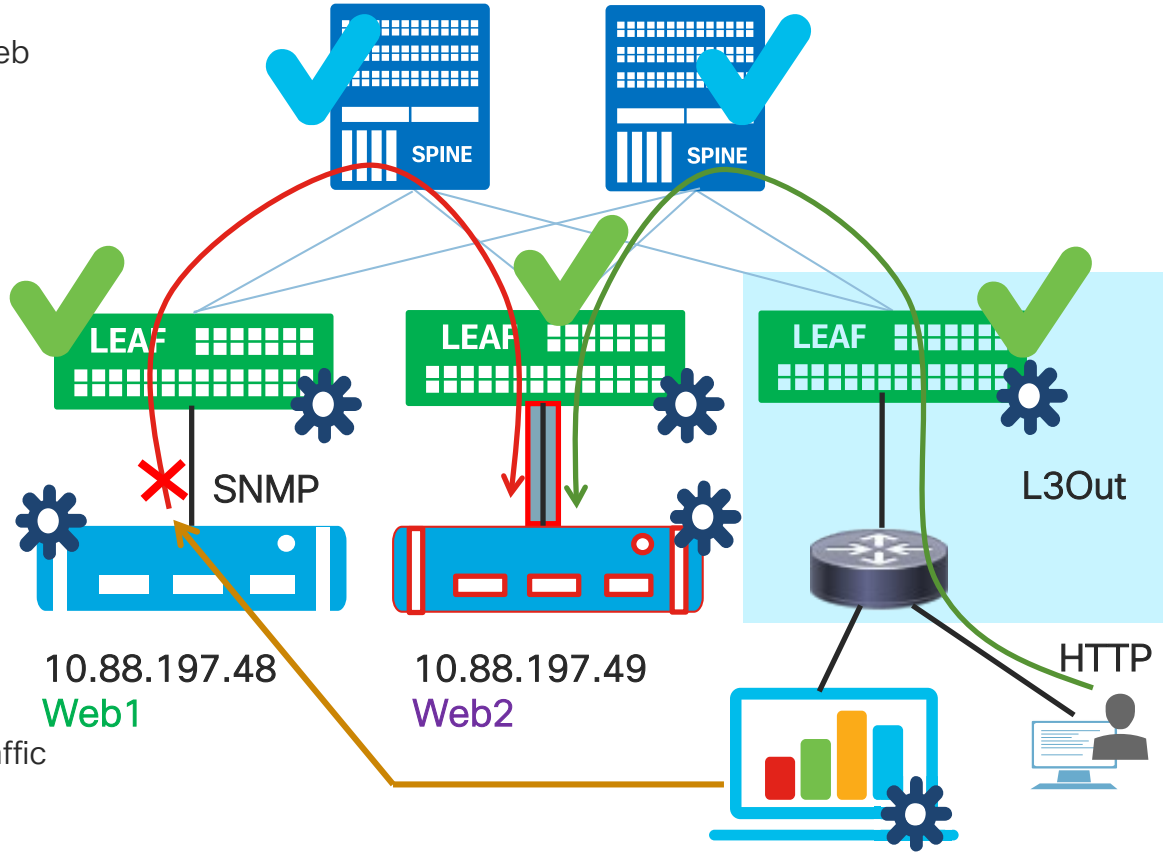
Mar 14 12:38:58 apic1 %LOG_LOCAL7-3-SYSTEM_MSG [F0101][raised][equipment-failed][major][topology/pod-1/node-1/sys/ch/p-[/dev/sdf]-f-[/dev/sdf]/fault-F0101] Storage unit /dev/sdf on Node 1 has failed.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Use Case - 11

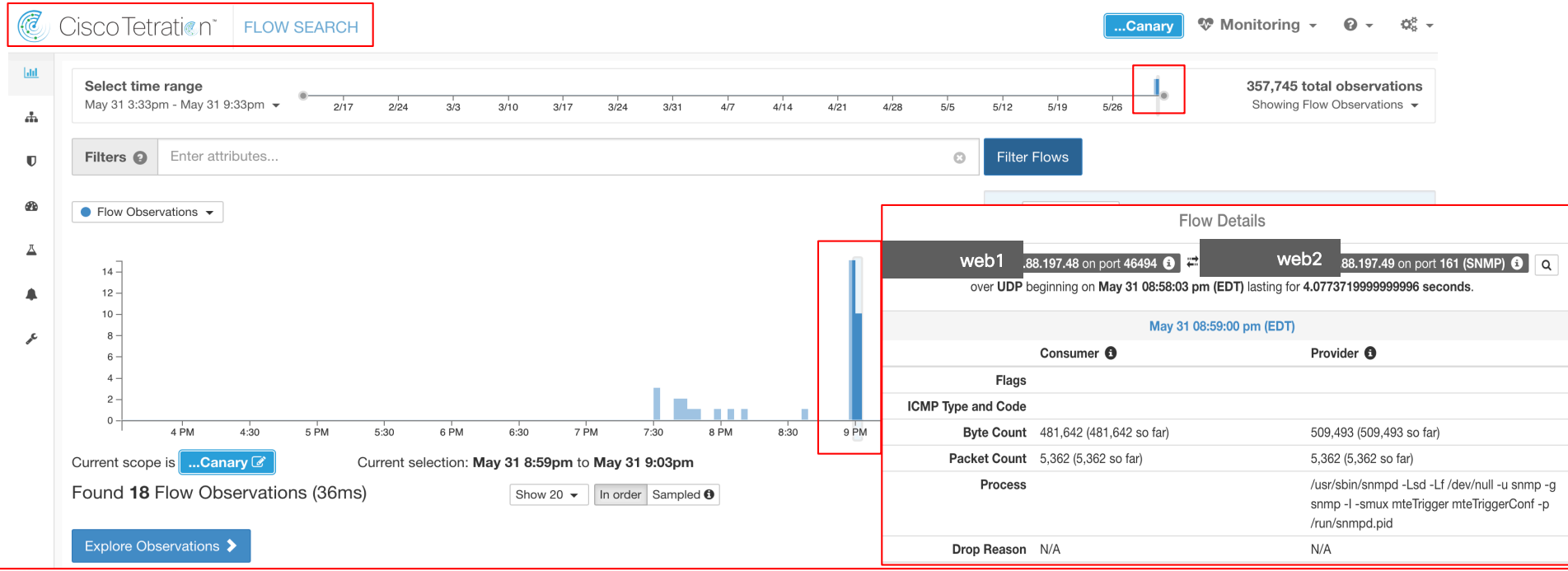
Application Performance Issues – Tetration

- Application team complained that their web application is poorly performing.
- ACI infrastructure found to be functioning properly
- Web2 server interface on Leaf showing congestion.
- On investigation via Tetration, web2 got hacked. As a result, SNMP daemon is installed and running on web2.
- web1 is constantly pulling snmp mib information from web2, that ultimately is saturating the link.
- Tetration Deep Visibility and Enforcement Agents are installed on web2.
- Enforcement policy is applied on web2 to only allow the desired HTTP and ICMP traffic



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

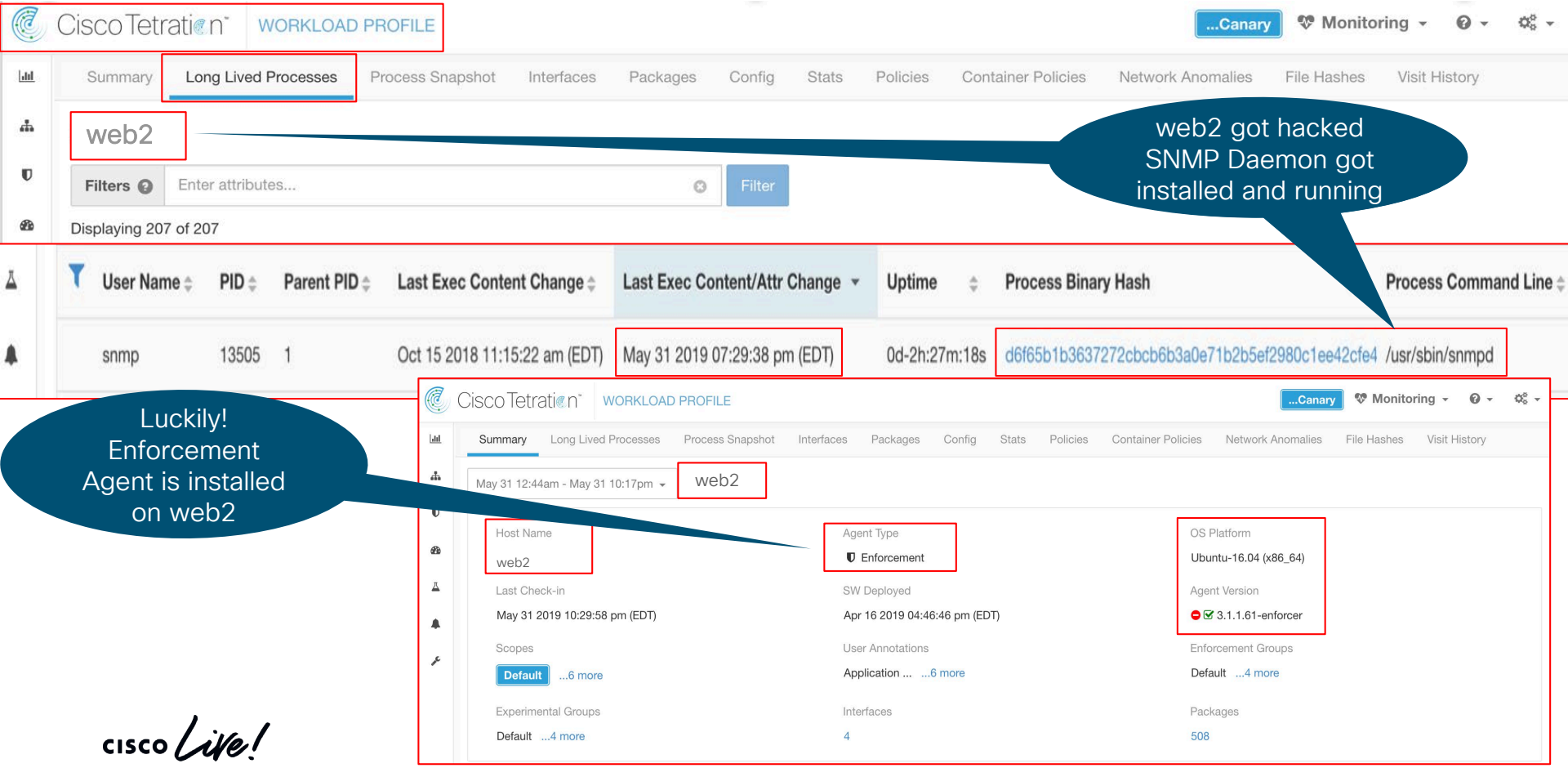
Application Performance Issues – Tetration



Timestamp	Consumer Hostname	Provider Hostname	Consumer Address	Provider Address	Consumer Port	Provider Port	Protocol	Service Name	Address Type
May 31 8:59:00pm	web1	web2	10.88.197.48	10.88.197.49	46494	161	UDP	SNMP	IPv4
May 31 8:59:00pm	web1	web2	10.88.197.48	10.88.197.49	58348	161	UDP	SNMP	IPv4

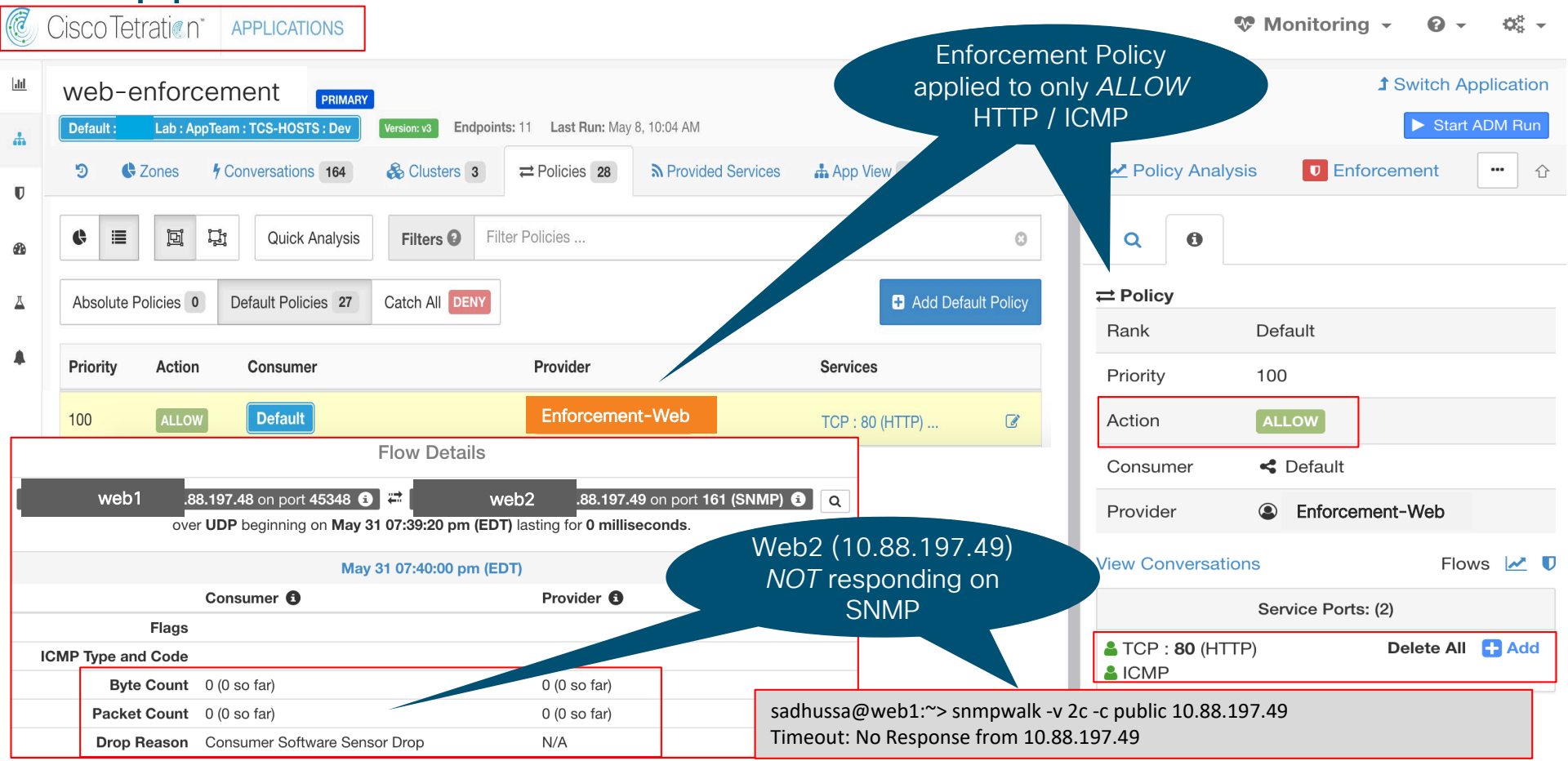
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Application Performance Issues – Tetration



cisco Live!

Application Performance Issues – Tetration



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

"Growing a datacenter infrastructure that relies more heavily on virtualization, security and efficiency requires a comprehensive and strategic approach to monitoring."

Richard Rauch – President & CEO

APCON

https://conversational.cioreview.com/cxoinsight/is-network-monitoring-keeping-pace-with-data-center-growth-and-virtualization-nid-23118-cid-202.html

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

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.

cisco Live!

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Continue your education

Demos in the Cisco campus

Walk-in labs

Meet the engineer 1:1 meetings

Related sessions

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Thank you

cisco Live!

You make **possible**