

CISCO *Live!*

Let's go

#CiscoLive



The bridge to possible

ACI Troubleshooting

Optimize your APIC User Experience through API
Mastery

Gabriel Monroy, CX Principal Engineer
BRKDCN-2635

CISCO *Live!*

#CiscoLive



Cisco Webex App

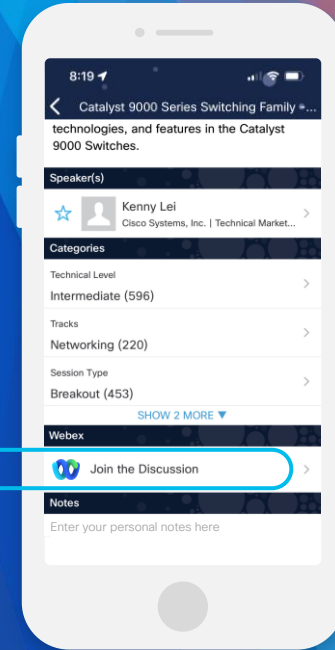
Questions?

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

How

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

Webex spaces will be moderated by the speaker until June 9, 2023.




<https://cislive.ciscoevents.com/cislivebot/#BRKDCN-2635>

Agenda

- You can't spell APIC without API
- Under-the-hood of an APIC Cluster
- Common API Usage Issues
- API Troubleshooting Tools
- Query Subscriptions as an ACI Troubleshooting Tool

Glossary of Acronyms

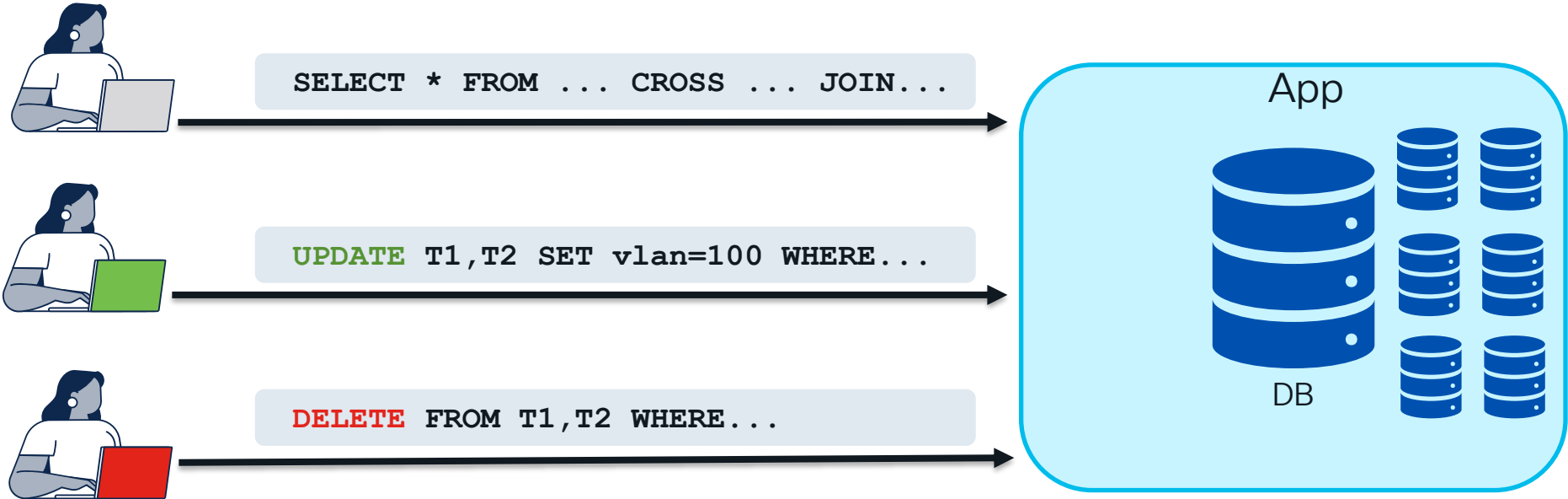
| Acronyms | Definitions |
|----------|---|
| ACI | Application Centric Infrastructure |
| APIC | Application Policy Infrastructure Controller |
| API | Application Programming Interface |
| DME | Data Management Engine (ACI Service) |
| FNV | Fabric Node Vector (ACI Switch registration info) |
| MIT | Management Information Tree |
| RV | Replica Vector (Shard/Replica State) |
| REST | Representational State Transfer – A specific architectural style for web services |



| Acronyms | Definitions |
|-----------|--|
| extXMLApi | DME that works with NGINX |
| PD | Policy Distributor – Performs Policy Validation |
| PE | Policy Element – Main Switch Policy DME |
| PM | Policy Manager – Main APIC Policy DME |
| MO | Managed Object (an ACI object saved in DME DBs) |
| DB | Database, can be split into shards and replicated across APICs |

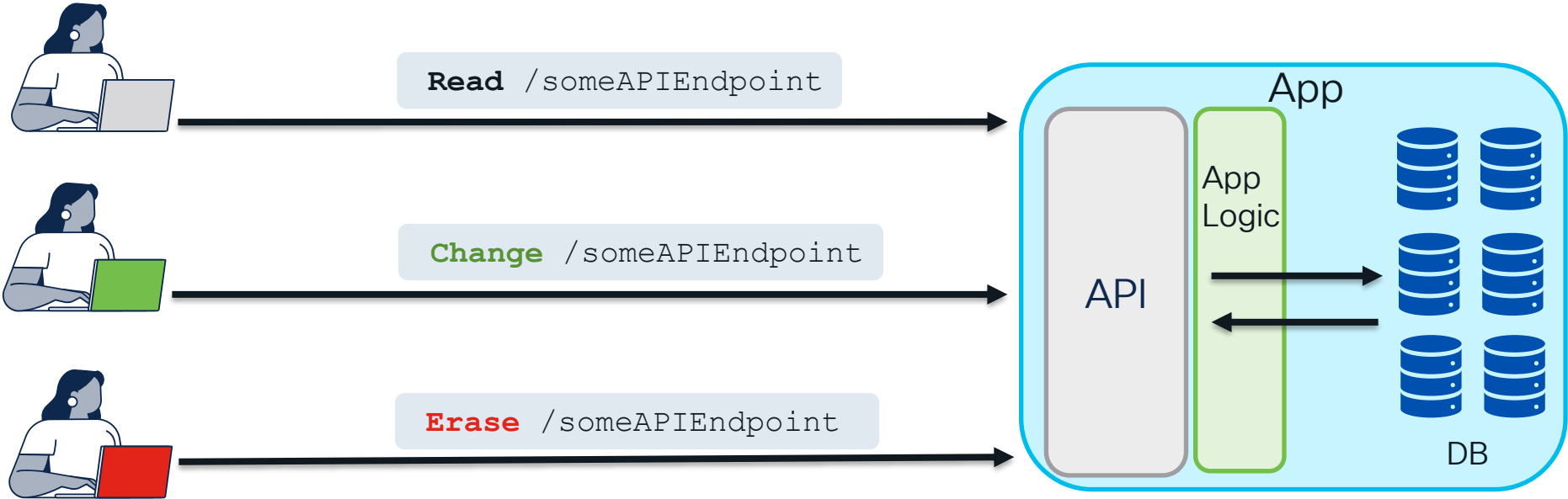
You can't spell
APIC without API

Before APIs



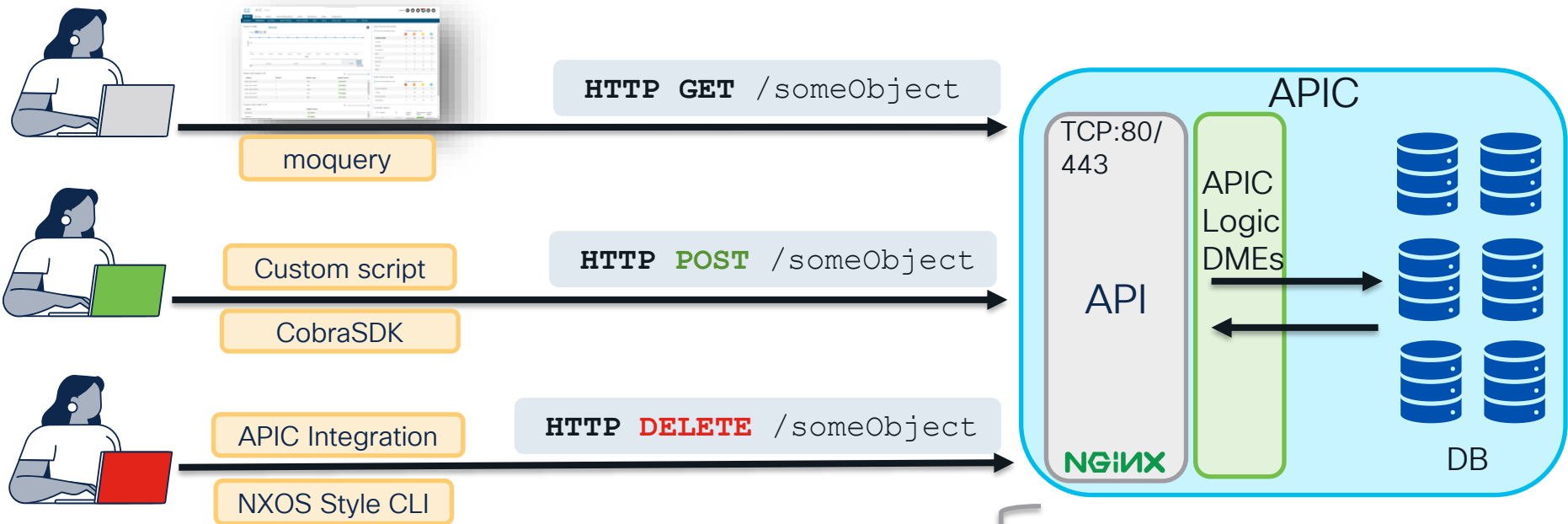
DB Manipulation is not user-friendly

Why have an API?



App Interface
Simplification

All ACI Interactions are via a REST API



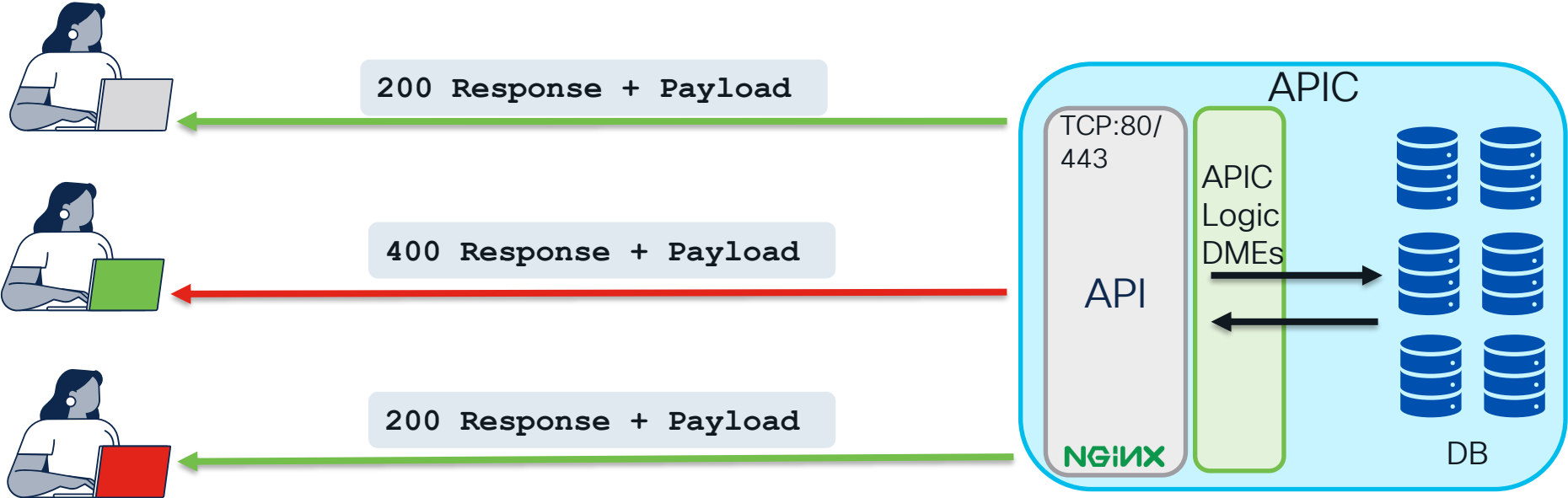
APIC supported REST Methods:

GET = R/O

POST = Create/Modify/Delete

DELETE = Delete

Read the Response code



Respond with HTTP/S Status Codes

2xx = OK

4xx = Client Error

5xx = Server Error

Anatomy of an APIC API Request

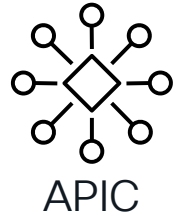


`/api/node/mo/uni/tn-CL/ap-CLApp/epg-DB.json`

DN Query

`/api/node/class/fvAEPg.json`

Class Query



APIC

`/node{-ID}`

Which Node?*

`/{mo|class}`

What type of Query?

`/{DN|className}`

Distinguished name or Object Class

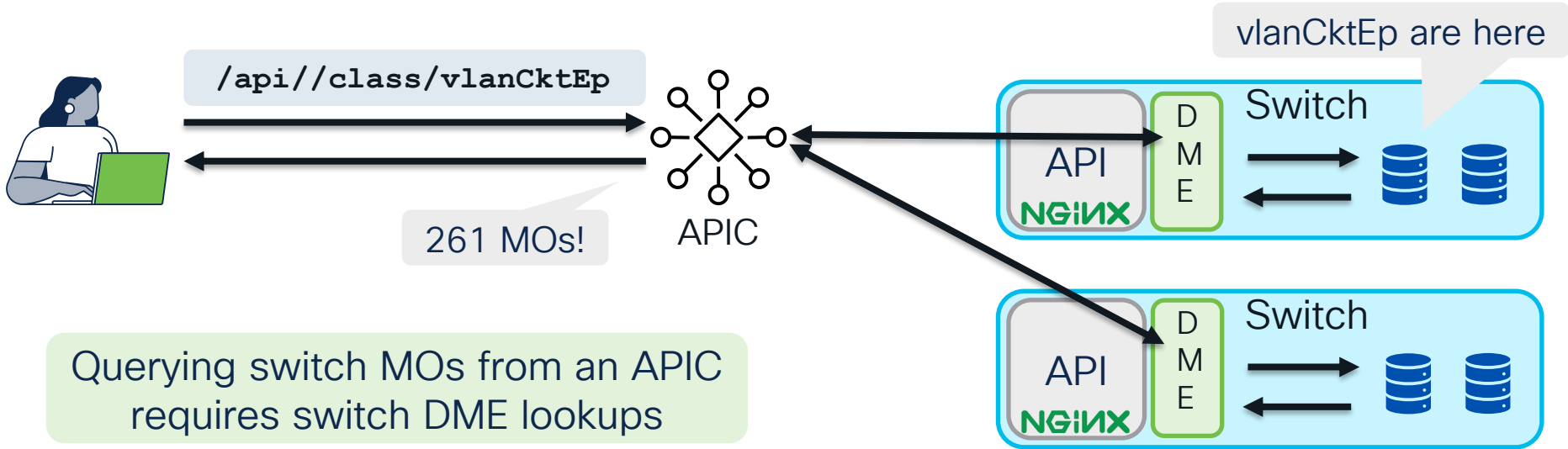
`.{xml|json}`

Response Encoding

`?[options]`

Filters, Selectors, query modifiers

What about Switches?



Querying switch MOs from an APIC requires switch DME lookups

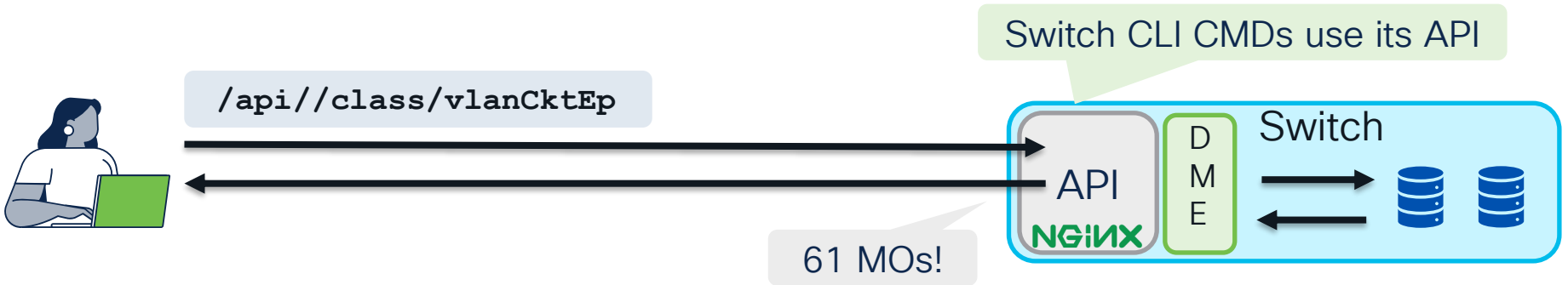
```
apic# moquery -c vlanCktEp
Total Objects shown: 261
```

```
# vlan.CktEp
```

```
dn : topology/pod-1/node-101/sys/ctx-[vxlan-x]/bd-[vxlan-y]/vlan-[vlan-777]
```

Contains pointer to source node

The Switches have an API too!



Query a Switch API to return just that Switch's Objects

```
Leaf-101# moquery -c vlanCktEp
Total Objects shown: 61

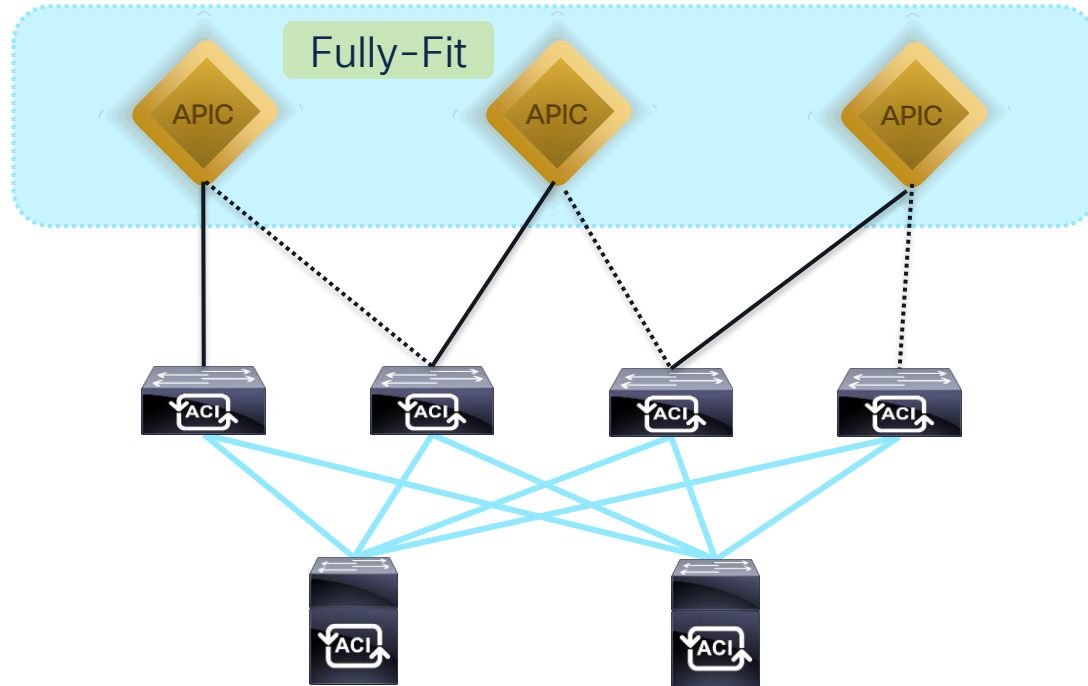
# vlan.CktEp
dn : sys/ctx-[vxlan-x]/bd-[vxlan-y]/vlan-[vlan-777]
```

Source node pointer not in underlying object

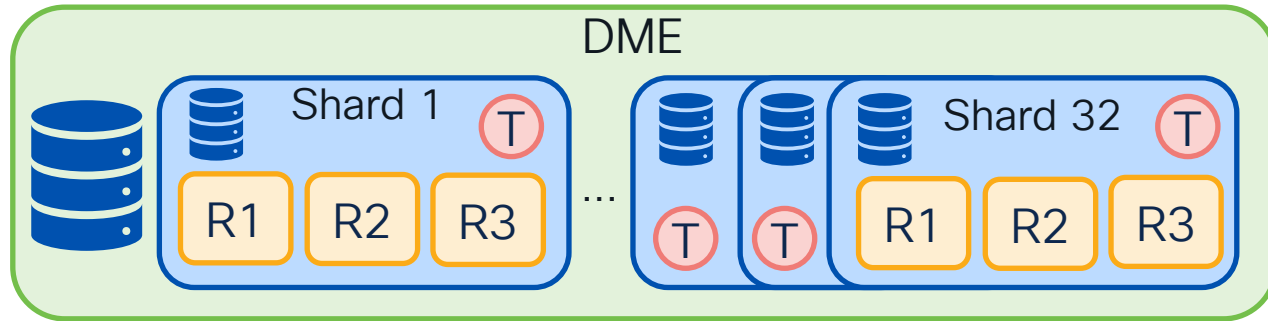
Under-the-hood of an APIC Cluster



An APIC Cluster



DMEs, Shards, Replicas and Tokens



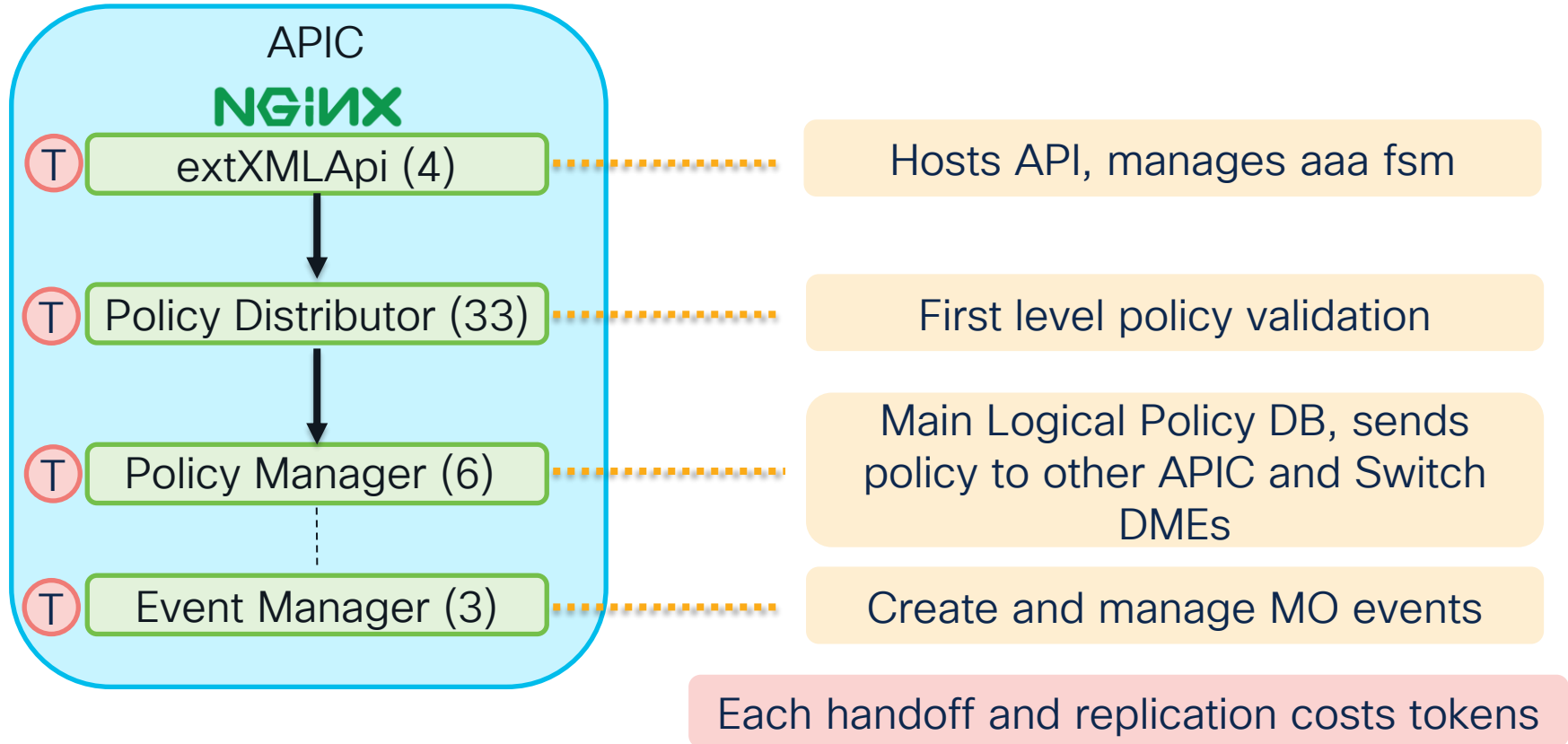
Not every DME is sharded

There are always 32 Shards*

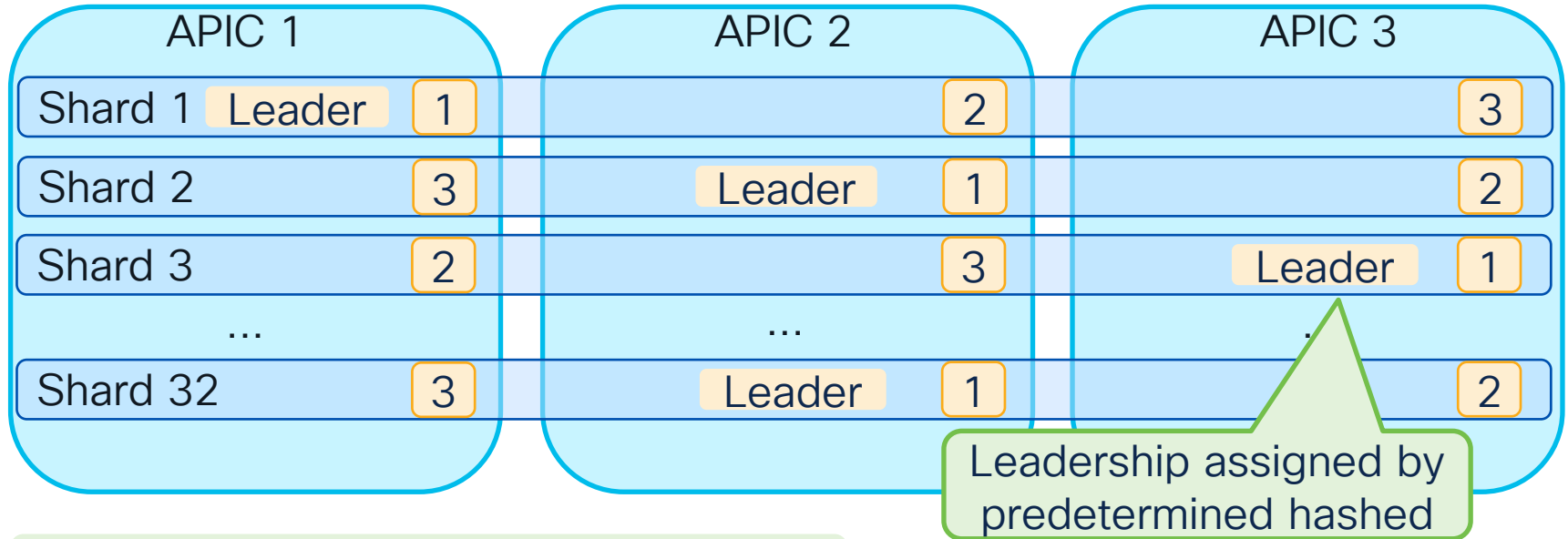
There are always 3 Replicas

Shards use a Token Queuing System

Main APIC DMEs for “general” configuration



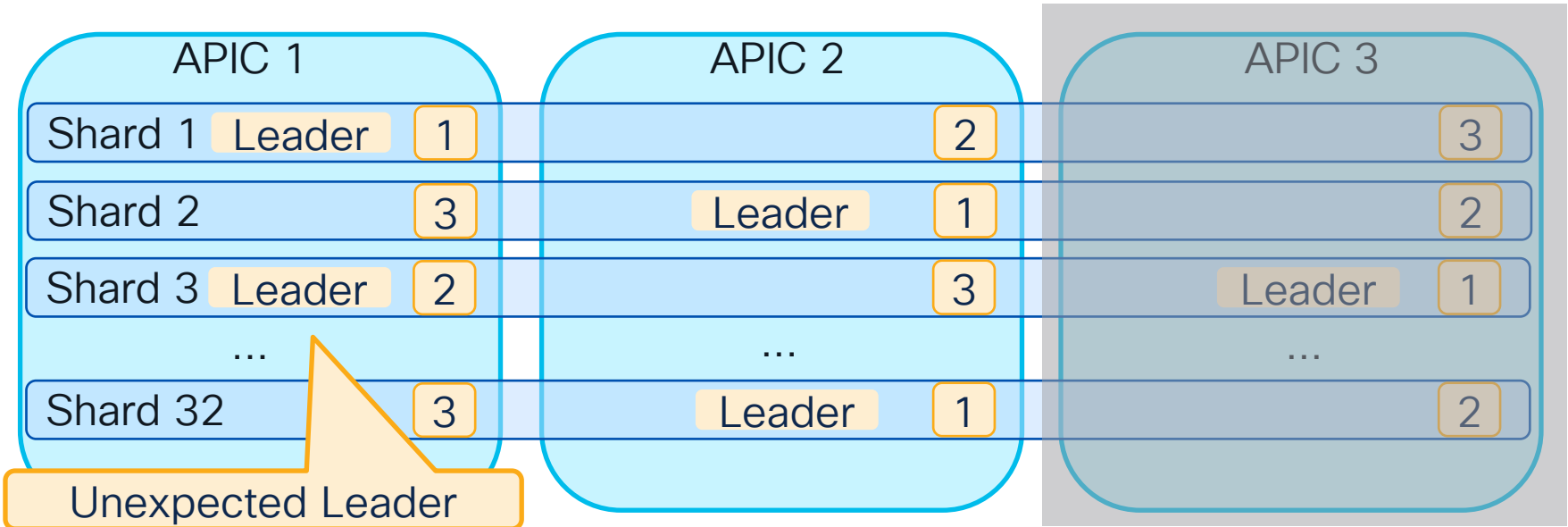
Fully-Fit 3 APIC Cluster – Shard Leadership



Shard Leader handles Write Operations

Multiple APICs = Distributed processing

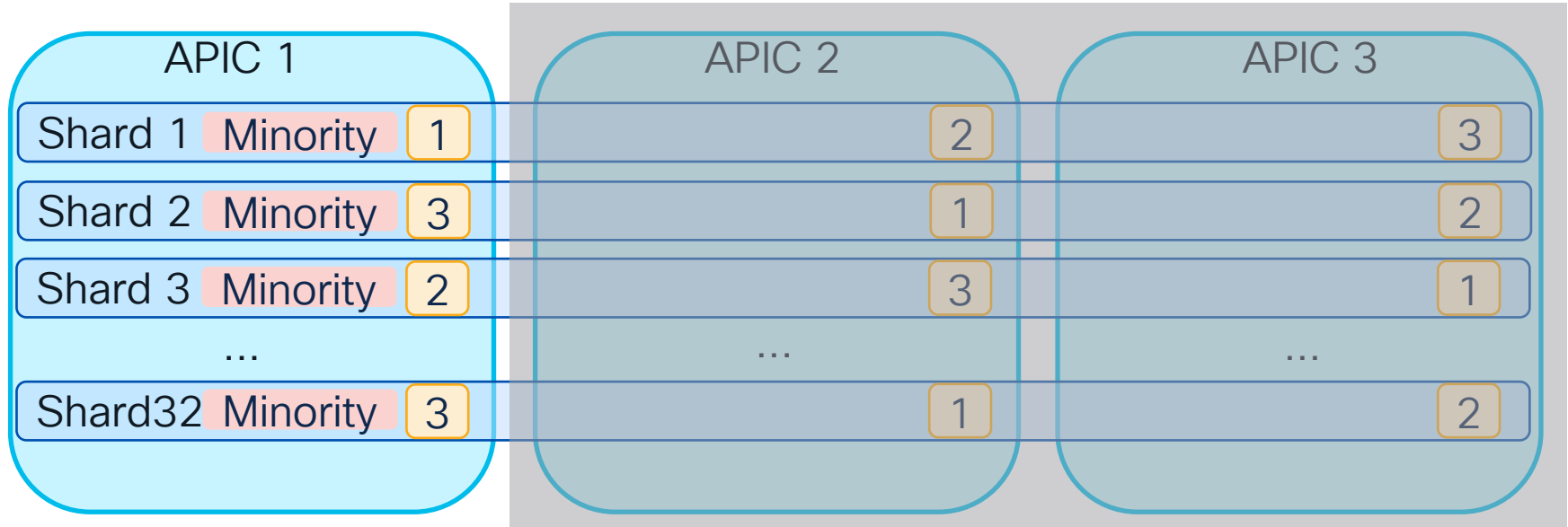
Degraded Leadership



Shards still have the Majority of Replicas; 2 out of 3

Write operations still available

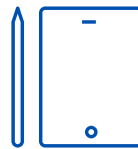
Diverged APIC Cluster - Minority State



Minority state = RO Operations

APIC 1 isolated from APIC 2 and 3

acidiag rvread svcID shardID



avread accepts <svc> <shard> <replica>

```
apic1# acidiag rvread -h
usage: acidiag rvread [-h] [subcommand [subcommand ...]]

positional arguments:
  subcommand optional svcID [shardID [replicID]]
```

Example: svcld 6 (PM) and shard 1

```
apic1# acidiag rvread 6 1
(6,1,1) st:6 lm(t):1(2022-03-09T03:56:31.224+00:00) le: reSt:LEADER ...
(6,1,2) st:6 lm(t):2(2022-03-09T03:48:04.444+00:00) le: reSt:FOLLOWER ...
(6,1,3) st:6 lm(t):3(2022-03-09T04:21:04.208+00:00) le: reSt:FOLLOWER ...
-----
clusterTime=<diff=-1099290 common=2022-04-15T21:33:22.809+00:00 local=2022-04-15T21:51:42.099+00:00
pF=<displForm=0 offsSt=0 offsVlu=0 lm(t):3(2020-01-08T20:53:53.081+00:00)>>
```

APIC 1 is leader of
Shard 1

Which APIC has that Replica; APIC 1 happens to have Replica 1

acidiag rvread <svcID> - Find Shard Leaders



```
apicl# acidiag rvread 6 | awk -F 'voGr' '{print $1}'
(6,1,1) st:6 lm(t):1(2022-03-09T03:56:31.224+00:00) le: reSt:LEADER
(6,1,2) st:6 lm(t):2(2022-03-09T03:48:04.444+00:00) le: reSt:FOLLOWER
(6,1,3) st:6 lm(t):3(2022-03-09T04:21:04.208+00:00) le: reSt:FOLLOWER
(6,2,1) st:6 lm(t):2(2022-03-09T03:56:32.244+00:00) le: reSt:LEADER
(6,2,2) st:6 lm(t):3(2022-03-09T04:21:02.145+00:00) le: reSt:FOLLOWER
(6,2,3) st:6 lm(t):1(2022-03-09T03:19:53.559+00:00) le: reSt:FOLLOWER
...
```

APIC 2 is Shard 2 Leader

APIC 2 has R1 of Shard 2

```
...
(6,31,1) st:6 lm(t):1(2022-03-09T03:56:30.094+00:00) le: reSt:LEADER
(6,31,2) st:6 lm(t):2(2022-03-09T03:48:28.880+00:00) le: reSt:FOLLOWER
(6,31,3) st:6 lm(t):3(2022-03-09T04:21:04.214+00:00) le: reSt:FOLLOWER
(6,32,1) st:6 lm(t):2(2022-03-09T03:56:36.575+00:00) le: reSt:LEADER
(6,32,2) st:6 lm(t):3(2022-03-09T04:21:05.076+00:00) le: reSt:FOLLOWER
(6,32,3) st:6 lm(t):1(2022-03-09T03:20:05.416+00:00) le: reSt:FOLLOWER
```

```
-----
clusterTime=<diff=-1099289 common=2022-04-15T21:50:54.647+00:00 local=2022-04-15T22:09:13.936+00:00
pF=<displForm=0 offsSt=0 offsVlu=0 lm(t):3(2020-01-08T20:53:53.081+00:00)>>
```

Summary of Cluster States

Fully Fit

R/W Operations Available

Expected Leaders

All shards/replicas reachable

Data Layer Degraded
Leadership

R/W Operations Available

Unexpected Leaders

Replica Majority reachable

Data Layer Diverged

R/O Operations

Minority State

Unreachable shards or replicas

Realm
of API
Issues

acidiag cluster - APICs

***Requires Admin Password**

APIC States

ChassisUUID

Shard/Replica Convergence

INFRA and OOB Ping tests

Version Verification

```
apic# acidiag cluster
```

```
Admin password:
```

```
Checking Wiring and UUID: OK
```

```
Checking AD Processes: Running
```

```
Checking All Apics in Commission State: OK
```

```
Checking All Apics in Active State: OK
```

```
Checking Leadership Degration: Optimal  
leaders
```

```
Ping OOB IPs:
```

```
APIC-1: 192.168.1.1 - OK
```

```
APIC-2: 192.168.1.2 - OK
```

```
APIC-3: 192.168.1.3 - OK
```

```
Ping Infra IPs:
```

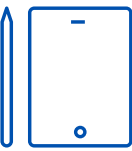
```
APIC-1: 10.0.0.1 - OK
```

```
APIC-2: 10.0.0.2 - OK
```

```
APIC-3: 10.0.0.3 - OK
```

```
Checking APIC Versions: Same (5.2(4d))
```

acidiag cluster - APICs



```
apic# acidiag cluster
Admin password:

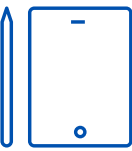
Checking Wiring and UUID: OK
Checking AD Processes: Running
Checking All Apics in Commission State: OK
Checking All Apics in Active State: OK
Checking Fabric Nodes: OK
Checking Apic Fully-Fit: OK
Checking Shard Convergence: OK
Checking Leadership Degradation: Optimal leader for all shards
Ping OOB IPs:
APIC-1: 172.21.208.154 - OK
APIC-2: 172.21.208.155 - OK
APIC-3: 172.21.208.156 - OK
Ping Infra IPs:
APIC-1: 10.0.0.1 - OK
APIC-2: 10.0.0.2 - OK
APIC-3: 10.0.0.3 - OK
Checking APIC Versions: Same (5.2(4d))
Checking SSL: OK
Full file system(s): None
```

Check acidiag manual for DME names



```
apic# man acidiag
Service IDs:
  ...
  3 - eventmgr
  4 - extXMLApi
  5 - policyelem
  6 - polycmgr
  7 - reader
  8 - ae
  9 - topomgr
  ...
 31 - opflexp
 32 - analytics
 33 - policydist
 34 - plgnhandler
 35 - domainmgr
 36 - licensmgr
```

Checking Tokens of DMEs



```
cat /debug/<apic-hostname>/<dme-name>/ifm/debug/mo
```

```
apic1# cat /debug/apic1/policymgr/ifm/debug/mo | egrep "id |tokens.available"
    id                : 0
tokens.available    : 1000

    id                : 1
tokens.available    : 902

    id                : 2
tokens.available    : 1000

    id                : 3
tokens.available    : 727

    id                : 4
tokens.available    : 852
...
```

PM Shard 1 has 902/1000
tokens available

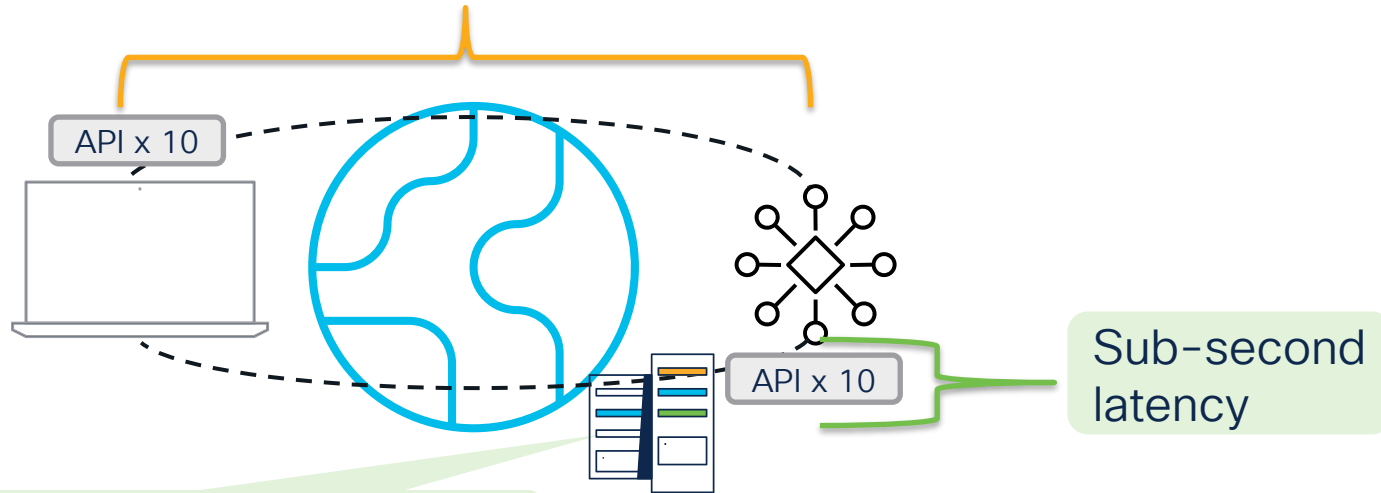
Common API Usage Issues



UI Usage Issue – Can I go the distance?

Issue: UI across a complex topology compounds symptoms of High API Usage

VPNs, Inspection, proxy, etc for .5s latency



Login Usage Issue – Login per Request

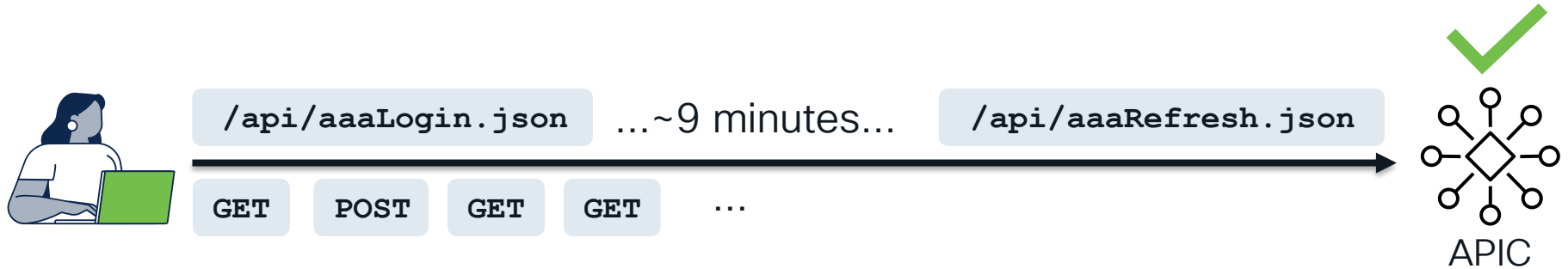


Doubles rate of query

Each login spawns a new session

Login Rate of 2 Requests/second is the default non-configurable throttle

Proper Login Usage – Session Refresh



A successful Login returns cookie:
`imdata.aaaLogin.attributes.token`

GET `aaaRefresh` with cookie:
Extends session by configured timeout

Proper Login Usage – User Certificate Signature



Generating the Signature



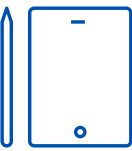
APIC-Request-Signature=**signature**;
APIC-Certificate-Algorithm=v1.0;
APIC-Certificate-Fingerprint=fingerprint;
APIC-Certificate-DN=user_cert_dn;

1. Build Payload from API Request:
“GET/api/class/fvTenant.json”

2. Calculate Signature with `.key`
against Payload

3. Convert Signature to base64 format
and add to cookies of request

Signed Request – CURL Example



```
# PREREQS: CRT/KEY generated. CRT added to APIC Local User.
# REQUEST: GET

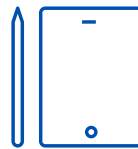
# Prep Request Payload
echo -n 'GET/api/class/fvTenant.json' > payload.txt

# Use private key to generate signature
openssl dgst -sha256 -sign automation.key payload.txt > payload_sig.bin

# Convert signature to base64
openssl base64 -A -in payload_sig.bin -out payload_sig.base64

# Send the CURL with specific cookies including base64 signature and DN of APIC Local User CRT.
curl -k --cookie \
"APIC-Request-Signature=...base64_signature...\
APIC-Certificate-Algorithm=v1.0; \
APIC-Certificate-Fingerprint=fingerprint; \
APIC-Certificate-DN=uni/userext/user-automation/usercert-autocert" \
"https://a.p.i.c/api/class/fvTenant.json"
```

Signed Request – Python Example

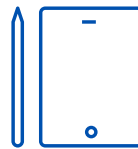


```
openssl req -new -newkey rsa:1024 -days 36500 -nodes -x509 -keyout automation.key -out automation.crt  
-subj '/CN=Auto User/O=Cisco Live/C=US'
```

```
from OpenSSL.crypto import FILETYPE_PEM, load_privatekey,  
sign  
import requests  
import base64  
  
APIC_ADDR = "https://a.p.i.c"  
USERNAME = "automation"  
CERT_MO = "autocert"  
  
key_file_path = f"{USERNAME}.key"  
cert_dn = f"uni/userext/user-{{USERNAME}}/usercert-  
{CERT_MO}"  
  
method = "GET"  
api = "/api/class/fvTenant.json"  
url = APIC_ADDR + api
```

```
with open(key_file_path, "r") as f:  
    key = f.read()  
  
x509Key = load_privatekey(FILETYPE_PEM, key)  
payload = method.encode("utf-8") + api.encode("utf-8")  
  
signedDigest = sign(x509Key, payload, "sha256")  
signature = base64.b64encode(signedDigest).decode("utf-  
8")  
  
cookies = {  
    "APIC-Request-Signature": signature,  
    "APIC-Certificate-Algorithm": "v1.0",  
    "APIC-Certificate-Fingerprint": "fingerprint",  
    "APIC-Certificate-DN": cert_dn,  
}  
r = requests.get(url, cookies=cookies, verify=False)
```

Track a Signed Request – nginx logs



```
apic1# egrep Signature /var/log/dme/log/nginx.bin.log

...snip...

5649||
2023-04-25T10:18:30.451349393-04:00||
nginx||
DBG4||
co=doer:255:127:0xff0000000a1c8c18:1||
Requested UserCert uni/userext/user-automation/usercert-autocert Fingerprint fingerprint
Signature VMtWcs3MU...Algorithm Version 1.0...
```

Signature from cookies
of sent Request

Username for cert
lookup + audit logging

Certificate Object to
verify signature against

Request Usage Issues – Optimize per Use-Case

Use Case: I want to monitor Node 101 Interface Stats

```
topology/pod-1/node-101/sys/phys-[eth1/1]/dbgEtherStats
```

DN root is
topology, not uni

Pod ID and Node ID are
both Parent Objects

Interface ID is a
Parent Parameter

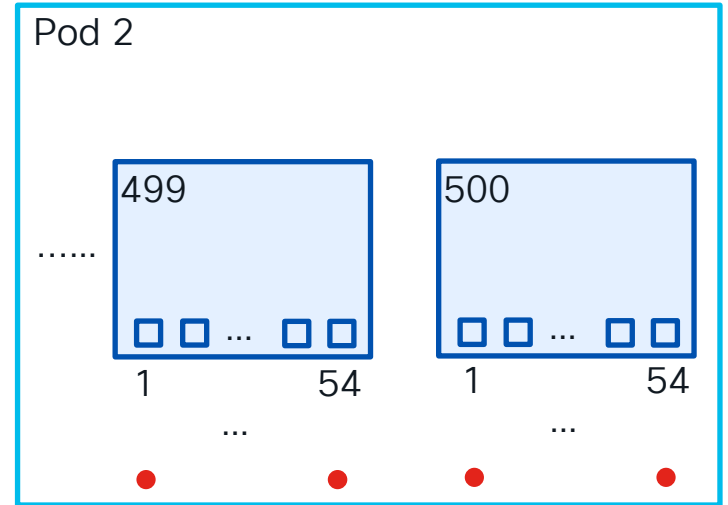
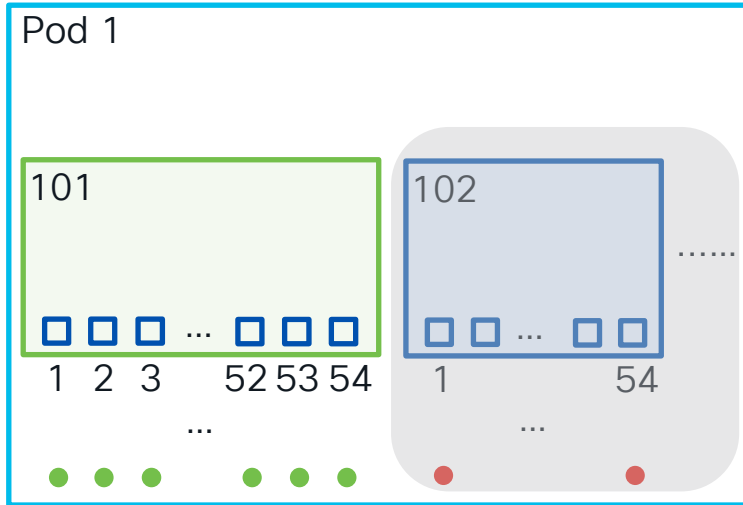
rmonEtherStats is the
className of the MO in
question

Request Usage – The Flexibility of the API

5.2(6e)+
*300K

Use Case: I want to monitor Node 101 Interface Stats

- Pod
 - Heavy Volume
- Switch
 - Just Right
- Interface
 - High Count
- rmonEtherStats
 - Heavy Volume



Goal: Use Query Options to Filter based on use case

100K* Response Object limit

Interface Stats Object



```
apic# moquery -d 'topology/pod-1/node-101/sys/phys-[eth1/1]/dbgEtherStats'
{
  "totalCount": "1",
  "imdata": [
    {
      "rmonEtherStats": {
        "attributes": {
          "broadcastPkts": "15964",
          "cRCAAlignErrors": "0",
          "dn": "topology/pod-1/node-101/sys/phys-[eth1/1]/dbgEtherStats",
          ...
          "rXNoErrors": "46046",
          "tXNoErrors": "73140",
          ...
        }
      }
    }
  ]
}
```


Query Options Usage

Defaults

Target Modifiers

query-target

target-subtree-class

query-target-filter

Response Filters

rsp-subtree

rsp-subtree-class

rsp-subtree-filter

rsp-subtree-include

Sort and Sizing

order-by

page

page-size

time-range

Defaults

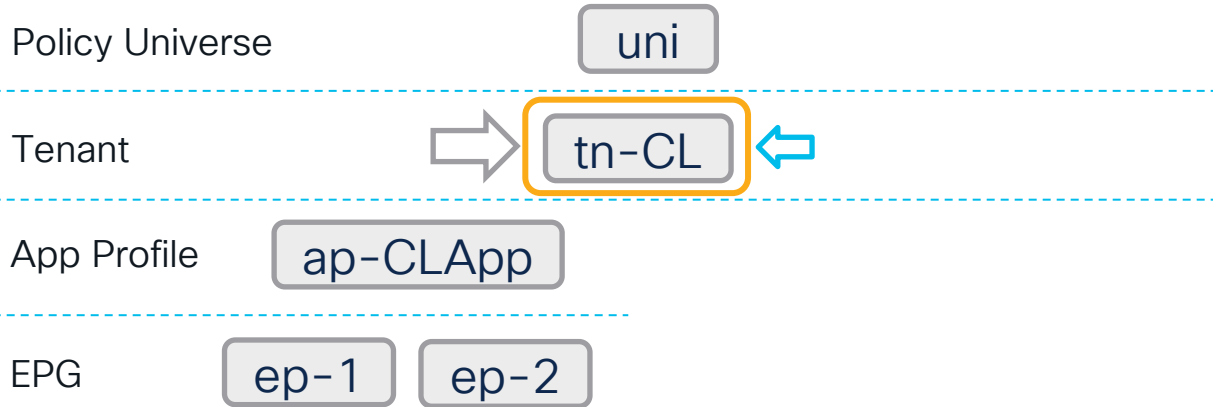
```
/api/mo/uni/tn-CL.xml
```

```
/api/class/fvTenant.xml
```

```
?query-target=self &rsp-subtree=no
```

Options – Defaults

`uni/tn-CL.xml` ?query-target=**self** &rsp-subtree=**no**



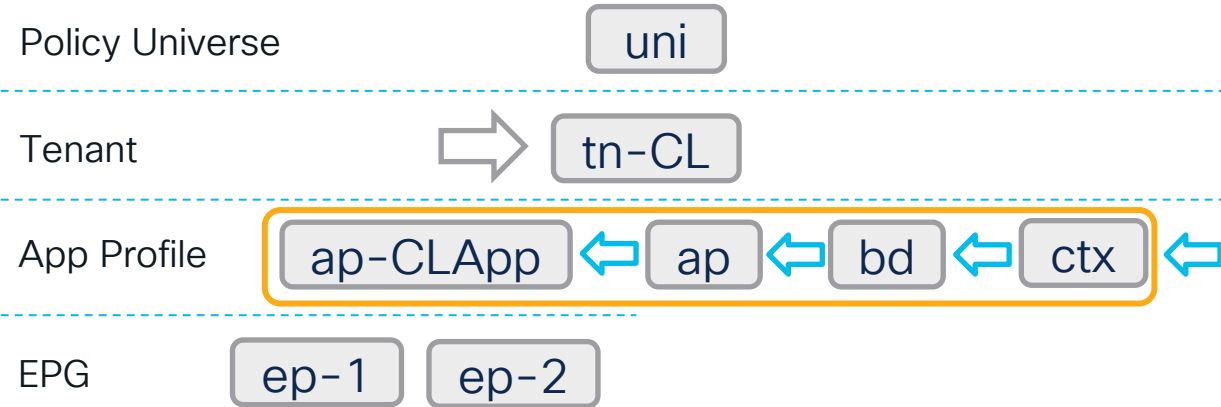
Response

- fvTenant

MOs returned: 1

Options – Query Target Children

`uni/tn-CL.xml ?query-target=children`



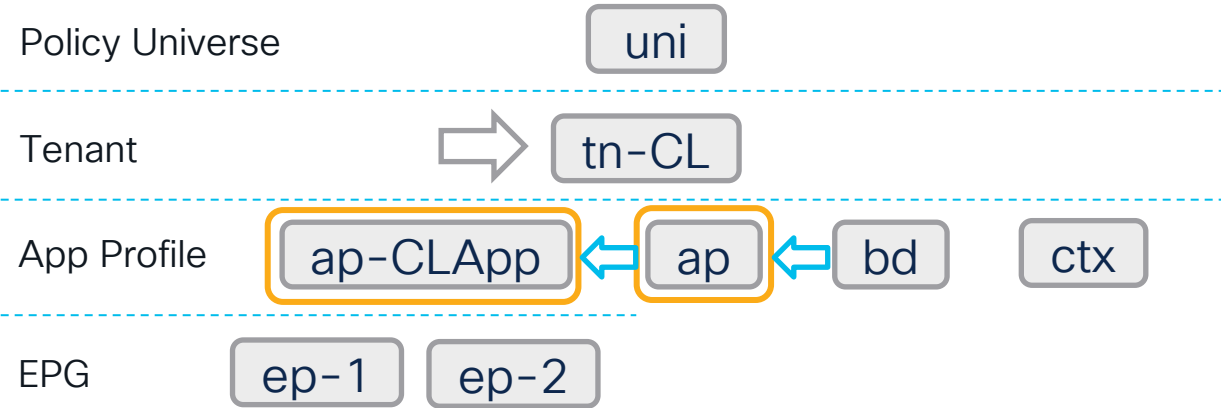
Response

- fvAp
- fvAp
- ...every other child
- fvBd
- fvCtx
- ...and so on

MOs returned: 2+

Options – Target Subtree Class

`uni/tn-CL.xml ?query-target=children &target-subtree-class=fvAp`



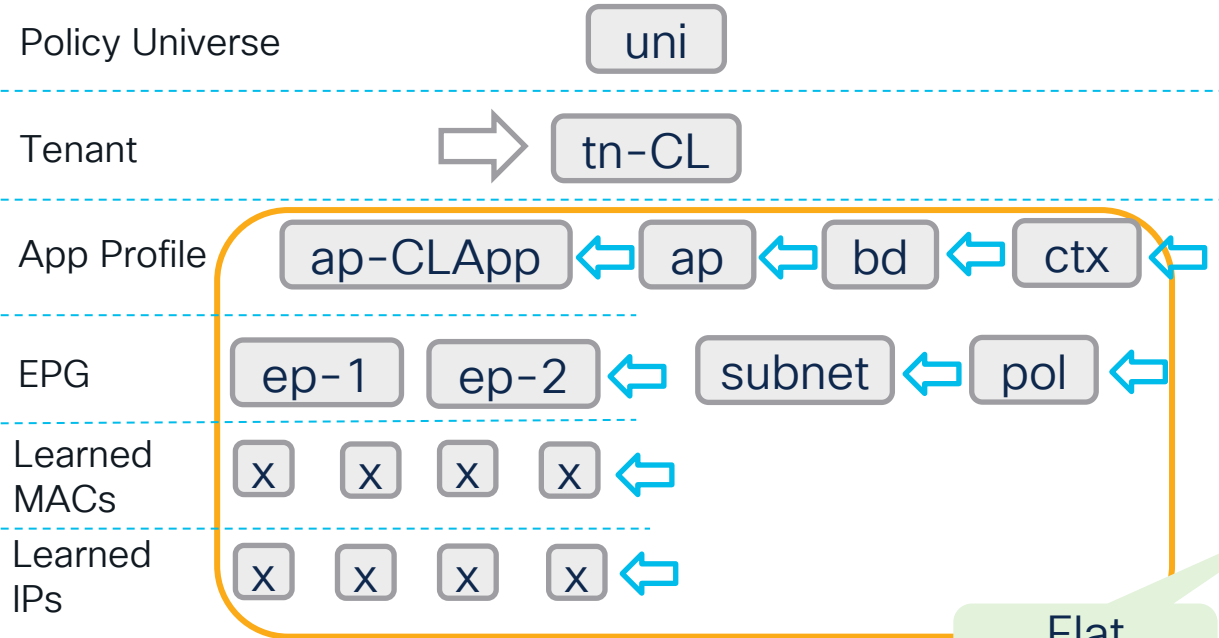
Response

- fvAp
- fvAp

MOs returned:
only child fvAp

Options – Query Target Subtree

`uni/tn-CL.xml ?query-target=subtree`



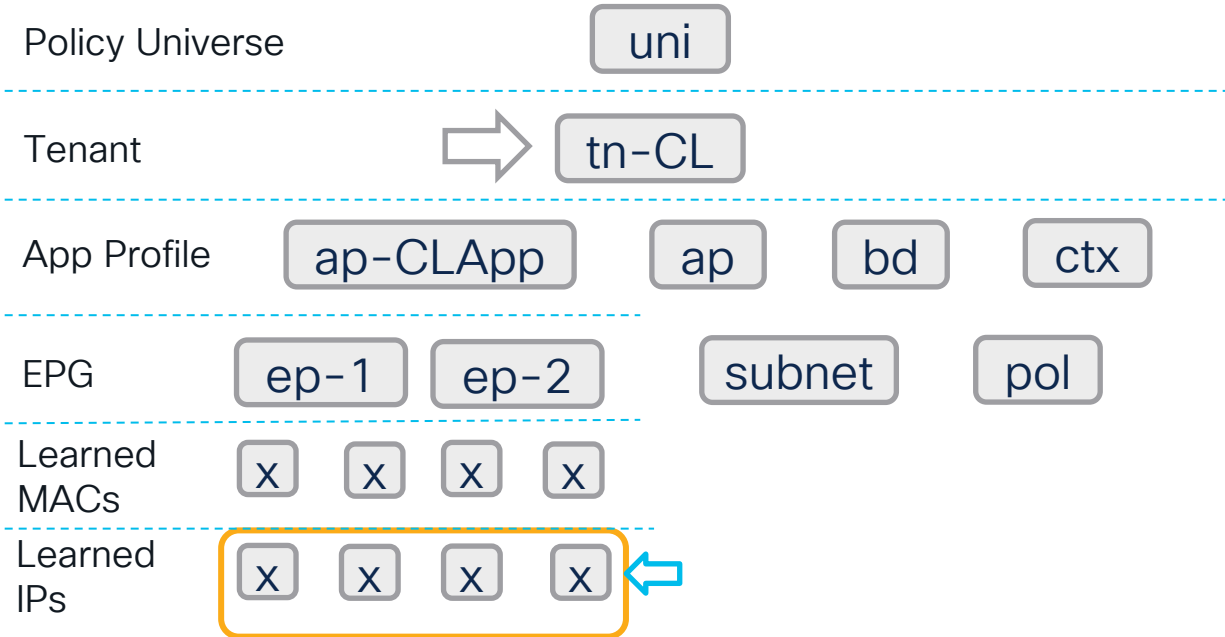
Response

- fvAp
- fvAp
- fvAEPg
- fvStPathAtt
- fvCEp
- fvlp
- ...and so on

MOs returned: x00+

Options – Query Target Subtree

`uni/tn-CL.xml ?query-target=subtree &target-subtree-class=fvIp`



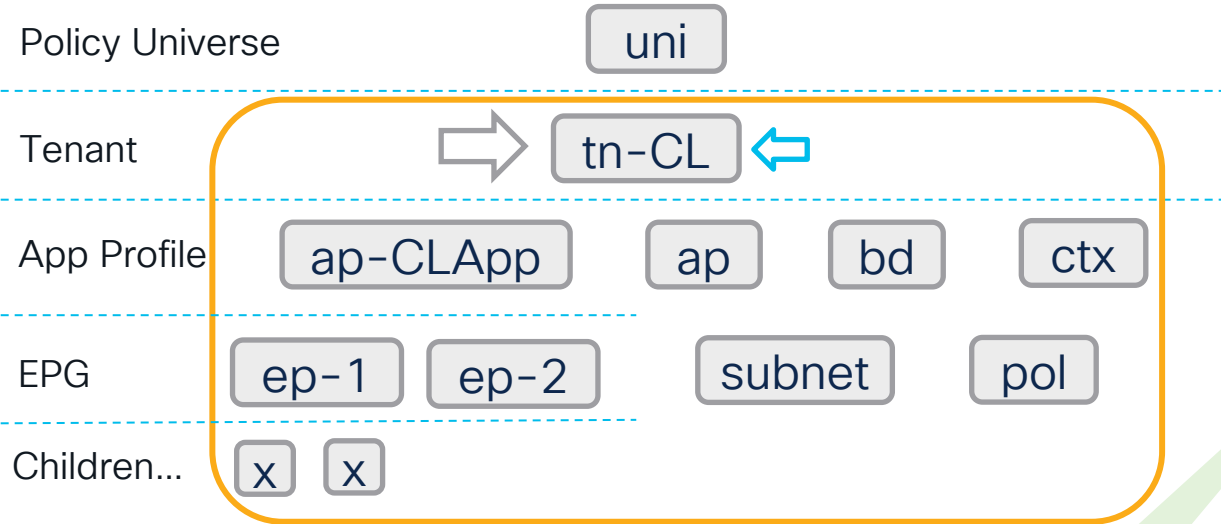
Response

- fvlp
- fvlp
- fvlp
- fvlp

MOs returned: 4

Options – Response Subtree

`uni/tn-CL.xml` ?query-target=**self** &rsp-subtree=**full**



Powerful when combined with a class query

Nested structure!

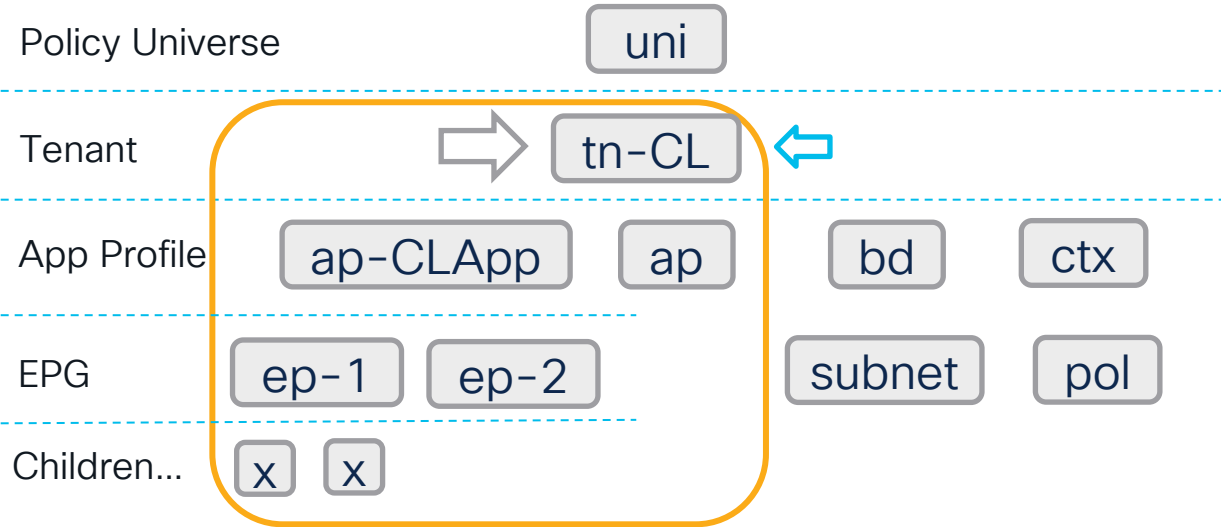
Response

- fvTenant
 - fvBD
 - fvSubnet
 - fvCtx
 - fvAp
 - fvAEPg
 - fvCEp
 - ...

MOs returned:
1 parent, all branches

Options – Response Subtree Class

`uni/tn-CL.xml` ?rsp-subtree=**full** &rsp-subtree-class=**fvAp**



Focus on branches of the class(es) specified

Response

- fvTenant
 - fvAp
 - fvAp
 - fvAEPg
 - fvAEPg
 - fvCEp
 - ...and so on

MOs returned:
1 parent, fvAp branch

Advanced Options – The Filters

Target Modifiers

query-target

target-subtree-class

query-target-filter

Uses same syntax

Response Filters

rsp-subtree

rsp-subtree-class

rsp-subtree-filter

rsp-subtree-include

Filter Syntax

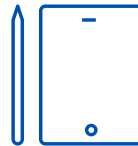
L.O.(class.param, "value")

eq(fvAp.name, "CLapp")

`class/fvTenant.xml` ?query-target-filter=eq(fvTenant.name, "CL")

`class/fvTenant.xml` ?rsp-subtree-filter=eq(fvTenant.name, "CL")

Advanced Options – All Logical Operators



| Logical Operator | Description |
|------------------|---------------------------------|
| eq | Equal to |
| ne | Not equal to |
| lt | Less than |
| gt | Greater than |
| le | Less than or equal to |
| ge | Greater than or equal to |
| bw | Between |
| not | Logical inverse |
| and | Logical AND |
| or | Logical OR |
| xor | Logical exclusive OR |
| true | Boolean TRUE |
| false | Boolean FALSE |
| anybit | TRUE if at least one bit is set |
| allbits | TRUE if all bits are set |
| wcard | Wildcard |
| pholder | Property holder |
| passive | Passive holder |

Multiple Filter Syntax

```
L.O.(class.param, "value")
```

```
and(  
  ne(fvAp.name, "CLapp"),  
  ne(fvAP.name, "TRapp")  
)
```

Advanced Options – Response Subtree Include

Target Modifiers

query-target

target-subtree-class

query-target-filter

Unique Behaviors

Response Filters

rsp-subtree

rsp-subtree-class

rsp-subtree-filter

rsp-subtree-include

Response

- moCount
count: 528430
dn: cnt

MOs returned: 1

```
class/eventRecord.xml ?rsp-subtree-include=count
```

Advanced Options – Response Subtree Include

Related MOs

| Operator | Class |
|----------------|----------------------|
| audit-logs | aaaModLR |
| event-logs | eventRecord |
| fault-records | faultRecord |
| health-records | healthRecord |
| count | moCount of top level |

Child MOs

| Operator | Class |
|-----------|--------------------------|
| faults | faultInst, faultDelegate |
| health | healthInst |
| relations | **many |
| stats | **many |
| tasks | **very low level |

Response Options

| Operator | Returns |
|-----------|---|
| subtree | Must be used with no-scope, pulls subtree into logic |
| no-scoped | Only return above 'included' objects, not the parents. Flattens the result. |
| required | Only return parent MO if 'included' child object exists. |

Example Response Subtree Include Queries

Get Count of all Mos under all Tenants

`class/fvTenant.xml`

`?query-target=subtree &rsp-subtree-include=count`

Get audits for subtree of tn-CL

`uni/tn-CL.xml ?rsp-subtree-include=audit-logs, subtree, no-scoped`

Get live faults for subtree of tn-CL

`uni/tn-CL.xml`

`?query-target=subtree &rsp-subtree-include=faults, no-scoped`

Advanced Options – Sort and Paginate

Sort and Sizing

order-by

page

page-size

time-range

Sort – ascending or descending

```
class/aaaModLR.xml
```

```
?order-by=aaaUser.firstName|desc
```

Paginate through chunks of response

```
class/aaaModLR.xml
```

```
?page=0 &page-size=1000
```

High Churn Record objects
may result in duplicates

Advanced Options – time-range Record Freeze*

Sort and Sizing

order-by

page

page-size

time-range 5.2(3)+

Freeze Rolling Records

`class/eventRecord.xml`

`?page=0 &page-size=2000 &time-range=24h`

time-range units

hours

weeks

months

Range

syntax

xxh

xxweek

xxmonth

yyyy-mm-dd|yyyy-mm-dd

Must start with page=0, then leaf through page+=1 to maintain freeze

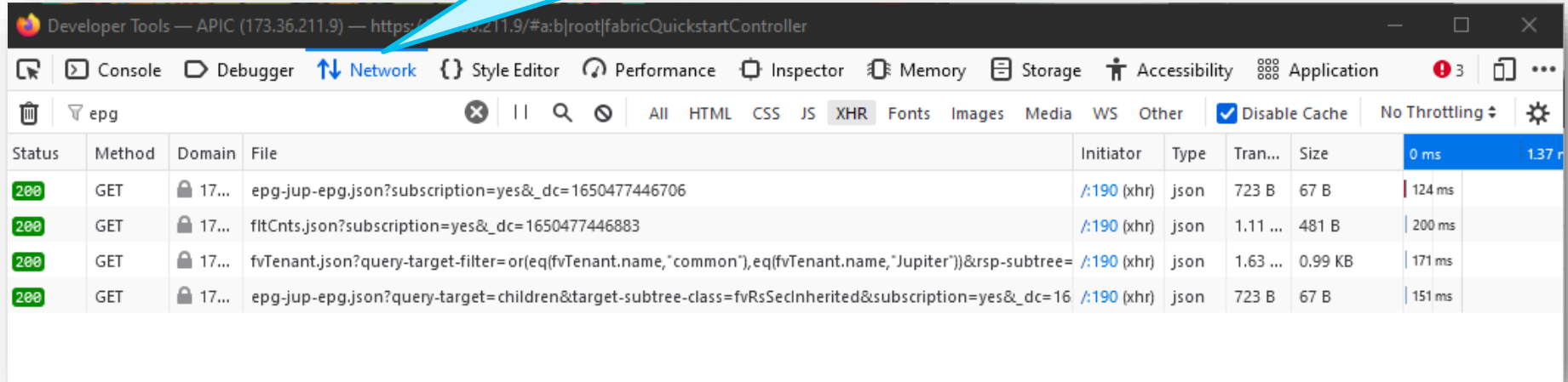
page-size limit of 2000

Auto-sorts on time

API Troubleshooting Tools

When using the UI - Browser Dev Tools

“Network” Tab



The screenshot shows the Network tab of browser developer tools. The top navigation bar includes Console, Debugger, Network (selected), Style Editor, Performance, Inspector, Memory, Storage, Accessibility, and Application. The Network tab is filtered for 'egg' and shows a list of requests. The 'XHR' filter is active. The table below lists the requests with their status, method, domain, file, initiator, type, transfer size, and response size.

| Status | Method | Domain | File | Initiator | Type | Tran... | Size | 0 ms | 1.37 r |
|--------|--------|--------|---|-------------|------|----------|---------|--------|--------|
| 200 | GET | 17... | epg-jup-epg.json?subscription=yes&_dc=1650477446706 | /:190 (xhr) | json | 723 B | 67 B | 124 ms | |
| 200 | GET | 17... | fltCnts.json?subscription=yes&_dc=1650477446883 | /:190 (xhr) | json | 1.11 ... | 481 B | 200 ms | |
| 200 | GET | 17... | fvTenant.json?query-target-filter=or(eq(fvTenant.name,"common"),eq(fvTenant.name,"Jupiter"))&rsp-subtree= | /:190 (xhr) | json | 1.63 ... | 0.99 KB | 171 ms | |
| 200 | GET | 17... | epg-jup-epg.json?query-target=children&target-subtree-class=fvRsSecInherited&subscription=yes&_dc=16 | /:190 (xhr) | json | 723 B | 67 B | 151 ms | |

Browser Dev Tools – The Request

The screenshot shows the Chrome DevTools Network tab. The 'Headers' sub-tab is active, displaying the details of a selected GET request. A blue callout box points to the request entry in the list.

| Sta... | Me... | D... | File | Initi... | T... | Tr... | Size |
|--------|-------|------|---|----------|-------|-------|-------|
| 200 | GET | ... | epg-jup-epg.json?subscription=yes&_dc=1650477446706 | :/19... | js... | 7... | 67 B |
| 200 | GET | ... | fltCnts.json?subscription=yes&_dc=1650477446883 | :/19... | js... | 1... | 481 B |
| 200 | GET | ... | fvTenant.json?query-target-filter=or(eq(fvTenant.name,"common"),eq(fv /:19... js... 1.... 0.99 KB | :/19... | js... | 7... | 67 B |
| 200 | GET | ... | epg-jup-epg.json?query-target=children&target-subtree-class=fvRsSe | :/19... | js... | 7... | 67 B |

Request Details:

- Method: GET
- URL: https://173.36.211.9/api/node/class/fvTenant.json?query-target-filter=or(eq(fvTenant.name,"common"),eq(fvTenant.name,"Jupiter"))&rsp-subtree=children&rsp-subtree-class=monEPGPoI&subscription=yes&_dc=1650477447012
- Status: 200 OK
- Version: HTTP/1.1
- Transferred: 1.63 KB (0.99 KB size)
- Referrer Policy: strict-origin-when-cross-origin

Response Headers (658 B):

- Access-Control-Allow-Credentials: false
- Access-Control-Allow-Headers: Origin, X-Requested-With, Content-Type, Accept, DevCookie, APIC-challenge, Request-Tag
- Access-Control-Allow-Methods: POST,GET,OPTIONS,DELETE
- Access-Control-Allow-Origin: http://127.0.0.1:8000
- Cache-Control: no-cache="Set-Cookie, Set-Cookie2"
- Client-Cert-Enabled: false
- Connection: keep-alive
- Content-Length: 1015

Summary: 4 requests, 1.59 KB / 4.16 KB transferred, Finish: 11.13 min

The full request sent by the browser

Browser Dev Tools – Timing

The screenshot shows the Chrome DevTools Network tab with the 'Timings' sub-tab selected. A table of network requests is visible, with the third request highlighted. To the right of the table, a 'Request Timing' section displays a horizontal bar chart showing the duration of various phases: Blocked (0 ms), DNS Resolution (0 ms), Connecting (0 ms), TLS Setup (0 ms), Sending (0 ms), Waiting (171 ms), and Receiving (0 ms). A blue callout box points to the 'Waiting' phase, and a green callout box points to the 'Waiting' bar.

| Sta... | Me... | D... | File | Initi... | T... | Tr... | Size | Headers | Cookies | Request | Response | Timings | Stack Trac... |
|--------|-------|------|---|----------|-------|-------|---------|----------------|-----------------|--------------------|----------|---------|---------------|
| 200 | GET | ... | epg-jup-epg.json?subscription=yes&_dc=1650477446706 | :/19... | js... | 7... | 67 B | Queued: 292 ms | Started: 292 ms | Downloaded: 463 ms | | | |
| 200 | GET | ... | fltCnts.json?subscription=yes&_dc=1650477446883 | :/19... | js... | 1... | 481 B | | | | | | |
| 200 | GET | ... | fvTenant.json?query-target-filter=or(eq(fvTenant.name,"common"),eq(fvTenant.name,"common")) | :/19... | js... | 1... | 0.99 KB | | | | | | |
| 200 | GET | ... | epg-jup-epg.json?query-target=children&target-subtree-class=fvRsSei | :/19... | js... | 7... | 67 B | | | | | | |

Request Timing

- Blocked: 0 ms
- DNS Resolution: 0 ms
- Connecting: 0 ms
- TLS Setup: 0 ms
- Sending: 0 ms
- Waiting: 171 ms
- Receiving: 0 ms

Timing of different phases

171 ms between sending then receiving response

4 requests | 1.59 KB / 4.16 KB transferred | Finish: 14.17 min

Browser Dev Tools – Slow APIC Response

The screenshot shows the Chrome DevTools Network tab with the 'Timings' panel selected. The network log shows a list of requests, with the 11th request highlighted in blue. The 'Timings' panel for this request shows a 'Waiting' phase of 1.10 min, which is significantly longer than the other phases (Blocked, DNS Resolution, Connecting, TLS Setup, Sending, Receiving), all of which are 0 ms.

| Sta... | M... | D... | File | Init... | T... | T... | Size | Blocked | DNS Resolution | Connecting | TLS Setup | Sending | Waiting | Receiving |
|--------|------|------|---|---------|------|------|------|---------|----------------|------------|-----------|---------|----------|-----------|
| 200 | GET | ... | egg-jup-egg.json?query-target=children&target-subtree-class=fvF | /:19... | j... | 7... | 67 B | 0 ms | 0 ms | 0 ms | 0 ms | 0 ms | 1.10 min | 0 ms |

~66000ms between sending then receiving response

System Response Time – Enable Calculation

APIC (site2) admin

System Tenants Fabric Virtual Networking Admin Operations Apps Integrations

QuickStart | Dashboard | Controllers | **System Settings** | Smart Licensing | Faults | History | Config Zones | Active Sessions | Security

System Settings

- APIC Connectivity Preferences
- APIC Passphrase
- BD Enforced Exception List
- BGP Route Reflector
- Control Plane MTU
- COOP Group
- Date and Time
- Endpoint Controls
- Fabric Security
- Fabric-Wide Settings
- Global AES Passphrase Encryption Sett...
- Global Endpoints (Beta)
- Intersight
- ISIS Policy
- Load Balancer
- Port Tracking
- Proxy Policy
- PTP and Latency Measurement
- Quota
- Remote Leaf POD Redundancy Policy
- System Alias and Banners
- System Global GIPo
- System Performance**

System Performance

System Response Time Faults History

Properties

Calculation: Disabled Enabled

Response Threshold (ms): 85000

Frequency (sec): 300

Top Slowest Requests: 5

Response Threshold = “Slow” threshold to flag a request

Frequency = how often to check

Top Slowest Requests = # of Requests to track within each interval, per APIC

Server Response Time – View Slowest Requests

APIC (site2) admin

System | Tenants | Fabric | Virtual Networking | Admin | Operations | Apps | Integrations

QuickStart | Dashboard | **Controllers** | System Settings | Smart Licensing | Faults | History | Config Zones | Active Sessions | Security

Controllers

- Quick Start
- Topology
- Controllers
 - apic1 (Node-1)**
 - Cluster as Seen by Node
 - Containers
 - Equipment Fans
 - Equipment Sensors
 - Interfaces
 - Memory Slots
 - NTP Details
 - Power Supply Units
 - Processes
 - Server Response Time**
 - SMU patch version
 - Storage
 - apic2 (Node-2)
 - apic3 (Node-3)
- Controller Policies
- Retention Policies

Server Response Time

Properties

Average Response Time (ms): 489
Requests Served: 77
Exceeded Requests: 0

Slowest requests in the last 300 seconds:

| Host Name | Method | Order | Code | Response Size (Bytes) | Response Time | Start Time | URL |
|-----------------------|--------|-------|------|-----------------------|---------------|----------------|--------------------------------------|
| ::ffff:172.21.208.205 | GET | 1 | 503 | 257 | 90811 | 2023-01-03T... | /api/node/class/faultInfo.json |
| ::ffff:172.21.208.205 | GET | 2 | 503 | 170 | 90688 | 2023-01-03T... | /api/node/class/eventRecord.json |
| ::ffff:10.1.0.1 | GET | 3 | 503 | 169 | 90494 | 2023-01-03T... | /api/node/mo/topology/pod-2.json |
| ::ffff:127.0.0.1 | GET | 4 | 503 | 172 | 90473 | 2023-01-03T... | /api/node/class/topSystem.json |
| ::ffff:172.21.208.162 | GET | 5 | 503 | 189 | 90331 | 2023-01-03T... | /api/class/firmwareCtrlrRunning.json |

90000ms+ for a faultInfo query

Source IP | Response Code | Timestamp | HTTP Request Method | Response Time | API Endpoint

Server Response Time – Threshold Events

Event - 4295863187

Properties

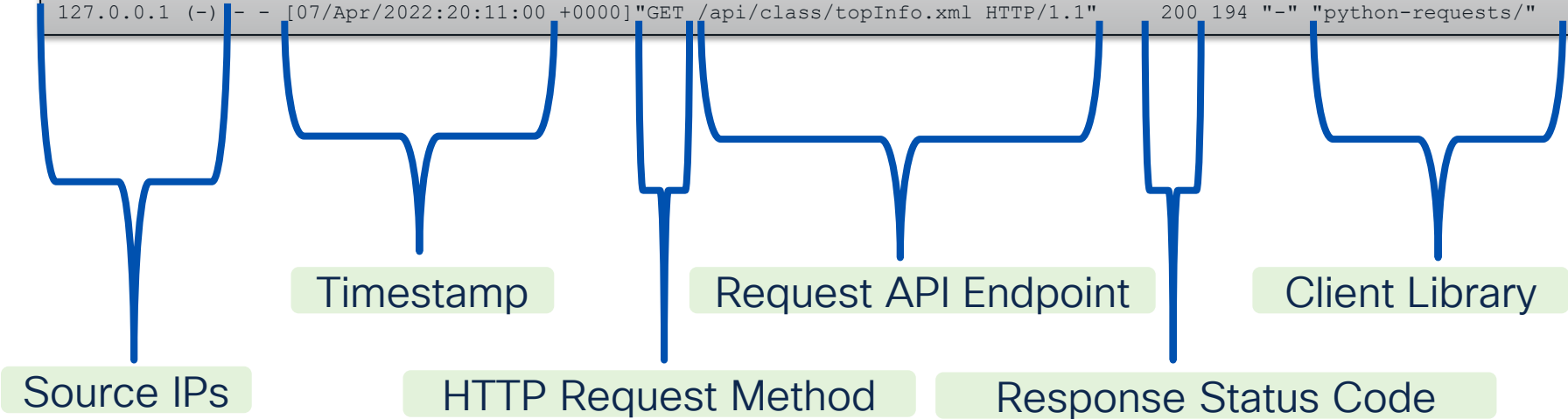
- ID: 4295863187
- Description: At least one request exceeded the requested response time. Requests Exceeded = [18]
- Severity: minor
- Affected Object: **topology/pod-1/node-1/web/apiAvgResp**
- Created: 2023-05-30T20:13:45.032+00:00
- Code: E4216978
- Cause: ResponseTimeOfAtLeastOneRequestHigherThanRequested
- Change Set: apiState (Old: No change, New: Requests Slow), avgRespTime (Old: 18, New: 1354), reqExceed (Old: 0, New: 18), reqServed (Old: 18, New: 718)
- Action: state-transition
- Action Trigger: oper
- Transaction ID: 18374686480873112000
- User: internal

18 Requests exceeded defined threshold

NGINX Includes access.log

Every Request to [this] APIC is logged

```
apicl# tail /var/log/dme/log/access.log
127.0.0.1 (-) - - [07/Apr/2022:20:10:59 +0000] "GET /api/class/topInfo.xml HTTP/1.1" 200 194 "-" "python-requests"
127.0.0.1 (-) - - [07/Apr/2022:20:10:59 +0000] "GET /api/class/topInfo.xml HTTP/1.1" 200 194 "-" "python-requests"
127.0.0.1 (-) - - [07/Apr/2022:20:10:59 +0000] "GET /api/class/topSystem.xml HTTP/1.1" 403 243 "-" "Python-urllib"
127.0.0.1 (-) - - [07/Apr/2022:20:10:59 +0000] "GET /api/class/fvTenant.xml HTTP/1.1" 200 15863 "-" "Python-urllib"
127.0.0.1 (-) - - [07/Apr/2022:20:11:00 +0000] "GET /api/class/topInfo.xml HTTP/1.1" 200 194 "-" "python-requests/"
```



Access Log Analyzer

http://cs.co/Access_Log_Analyzer

```
apicl# python /tmp/accLogAnalyzer.py
apicl# cat acclogAnalysis_2022-06-07T17:50:27.output
```

Access Log Time Analysis Summary:

Total # of Requests: 46669

Time Coverage: 109.416666667 Minutes (6565.0 s)

Avg # of Reqs: 7.11 Queries per second

Burst Summary: 602 15+ requests-per-second bursts found.

Remote Address Summary:

Remote addr '127.0.0.1' request count: 10811 (%23.17 of total reqs)

Remote addr '192.168.2.32' request count: 28431 (%60.92 of total reqs)

...

User-Agent Summary:

User-agent 'Mozilla/5.0 (Wi...' request count: 3398 (%7.28 of total reqs)

User-agent 'python-requests...' request count: 29052 (%62.25 of total reqs)

...

Response Status Summary:

Response code '200' count: 20008 (%42.87 of total reqs)

Response code '403' count: 17036 (%36.5 of total reqs)

...

50k queries over ~2 hours

Who?

What?

Why?

NGINX Request Throttle

The screenshot shows the Cisco Fabric Manager interface. The 'Fabric' tab is selected, and the 'Management Access' policy is highlighted in the left sidebar. The main panel displays the configuration for 'Management Access - default'. The 'Request Throttle' settings are highlighted with a green box, showing 'Request Throttle' set to 'Enabled' and 'Throttle Rate' set to '20 Requests/Minute'. Other settings include 'Admin State: Disabled', 'Port: 80', 'Redirect: Disabled', 'Allow Origins: http://127.0.0.1:8000', and 'Allow Credentials: Disabled'. The 'HTTPS' section shows 'Admin State: Enabled', 'Port: 443', 'Allow Origins: http://127.0.0.1:8000', 'Allow Credentials: Disabled', and 'SSL Protocols' checked for 'TLSv1.1' and 'TLSv1.2'. The 'DH Param' section shows '1024', '2048', '4096', and 'None' options.

Relies on NGINX Rate Limiting

Set Throttle Rate in R/M or R/S

Track per client IP address

Does not affect Self (UI + CLI)

Burst of Rate x 2 + NoDelay

Threshold cross = 503 response

Throttled Requests Receive 503 Response

```
apicl# tail /var/log/dme/log/access.log
192.168.1.1 (-) - - [03/Jan/2023:19:22:06 +0000]"GET /api/class/eventRecord.xml... HTTP/1.1" 200 494 "-" "python..."
192.168.1.1 (-) - - [03/Jan/2023:19:22:06 +0000]"GET /api/class/eventRecord.xml... HTTP/1.1" 503 494 "-" "python..."
192.168.1.1 (-) - - [03/Jan/2023:19:22:06 +0000]"GET /api/class/eventRecord.xml... HTTP/1.1" 503 494 "-" "python..."
```

503s follow successful responses

```
apicl# tail /var/log/dme/log/error.log
...limiting requests, excess: 40.292 by zone "httpsClientTagZone", client: h.o.s.t, request: "GET /api/class/..."

2023/04/17 20:19:14 [error] ... limiting requests, excess: 40.292 by zone "httpsClientTagZone", client: h.o.s.t, ...
request: "GET /api/node/...", host: "a.p.i.c"
```

Focus on addressing the source of the high rate of requests

Common Response Code Reasons

200

All good

4xx

Response Code

Possible Reasons

| | |
|-----|---|
| 400 | PD rule hit; Duplicate object, new requirement, etc |
| 401 | Authentication Issue; session expired, incorrect login Domain |
| 403 | API signing issue; incorrect signature calculation. Auth issue; Token timeout and new session required |

503

Response Code

Possible Reasons

| | |
|--|--|
| Unable to deliver the message ...temporary overload | Check that all APICs are fully-fit, check for DME token exhaustion NGINX throttle enabled, Request Throttled; check nginx error.log |
|--|--|

Query Subscriptions as an ACI Troubleshooting Tool

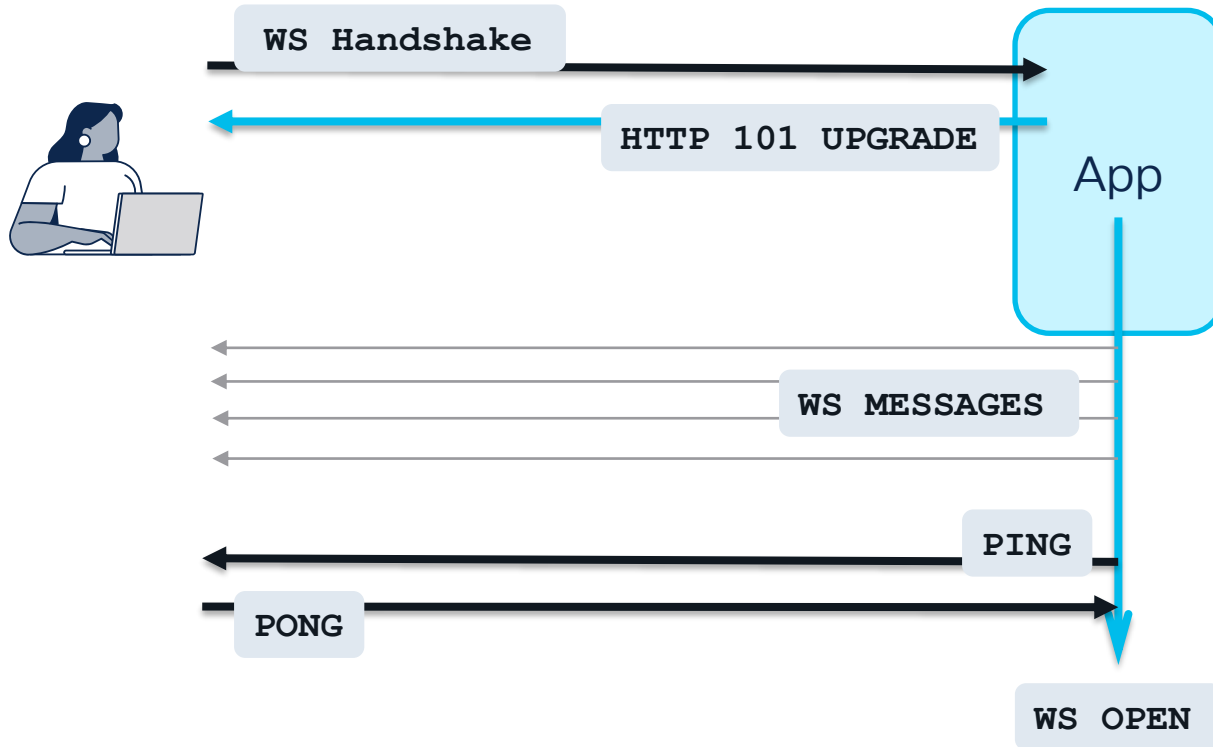
We are now the champions of Polling



Single transactional request, with single response

How do I track live MO changes without a timer?

Let's talk WebSockets

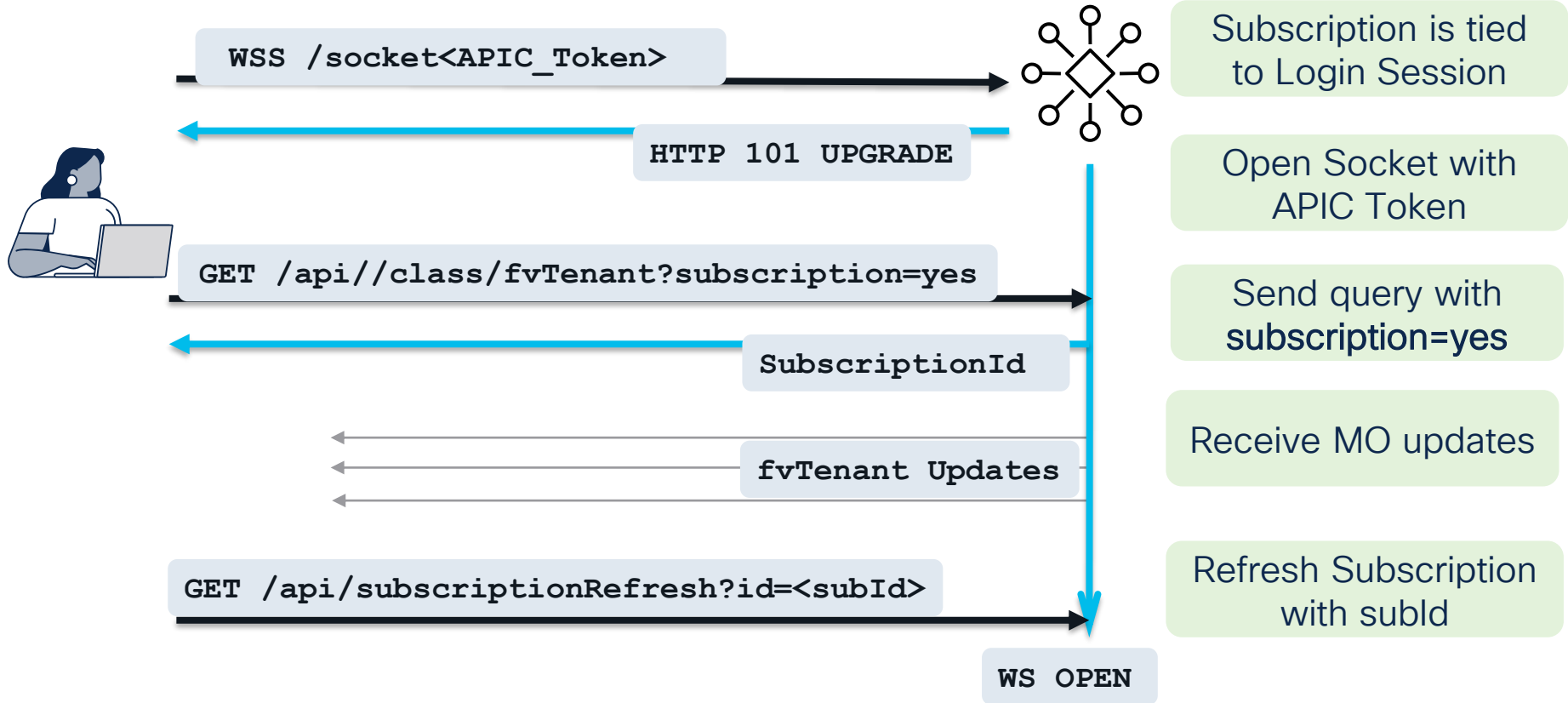


Handshake to OPEN channel

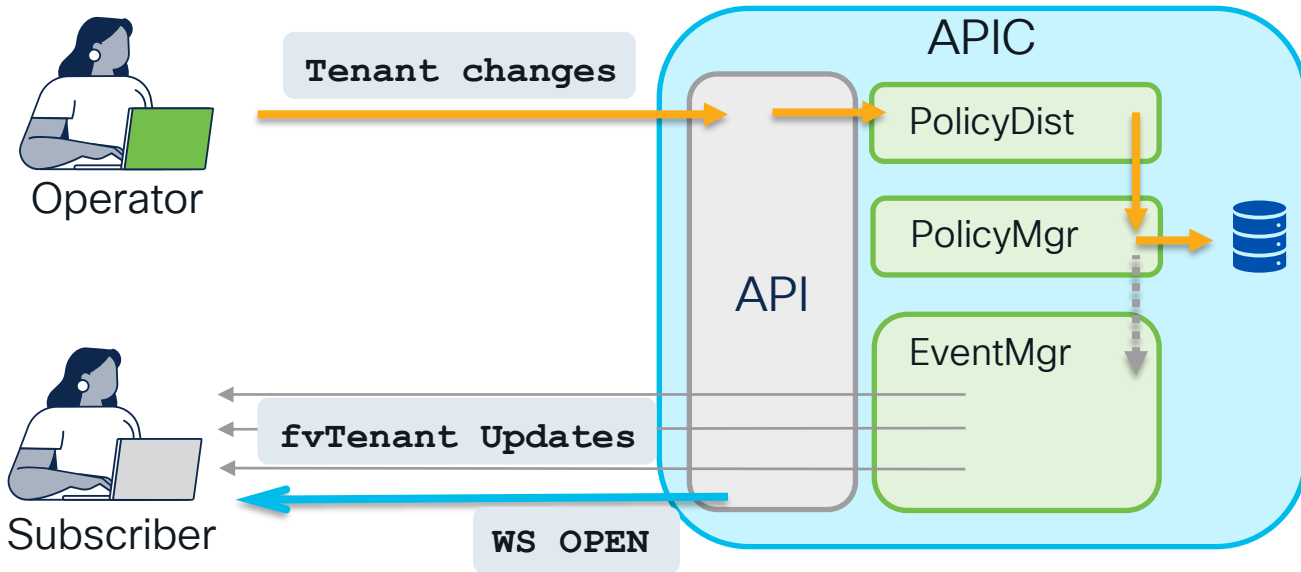
As App State changes, User receives Messages

Keepalives used to maintain OPEN

Subscribing to Query Results via WebSockets



Subscription - Under the hood



Receive MO events that go through eventMgr

Logical MO changes - explicit config changes

Record MO changes - audits, faults, events

No Stats MO changes - frequency intensive

Subscribable MOs subject to change: epRecord

Query Subscription Notification Message

http://cs.co/APIC_Websocket_Starter

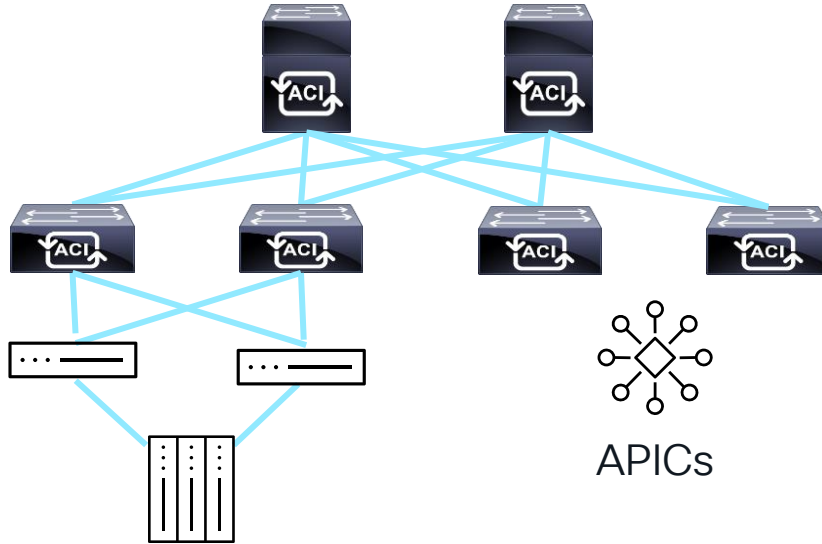
```
mypc$ python apic_query_subscription.py -a a.p.i.c -u gmonroy -x
gmonroy password:
***** WebSocket Subscription Status & Messages *****

https://a.p.i.c/api/class/fvTenant.xml
    ?subscription=yes&query-target=subtree&target-subtree-class=fvAEPg,fvBD
- Subscription ID: 72339464170766337

***** WebSocket Subscription Messages *****
...
<imdata subscriptionId="72339464170766337">
<fvAEPg ... dn="uni/tn-CiscoLive/ap-cl-ap/epg-CL_EPG" status="created" .../>
...
<imdata subscriptionId="72339464170766337">
<fvBD ... dn="uni/tn-CiscoLive/BD-cl-bd"... status="modified"/>
```

SubId in each message

Go Beyond Configuration, Go full DevOps



Consider MOs of importance going into a Maintenance Window

Ex: Monitor fabricLooseNodes during VMM Maintenance

Use Query Subscriptions to track those MOs during maintenance

Fill out your session surveys!



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



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



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

Continue your education

CISCO *Live!*

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



The bridge to possible

Thank you

CISCO *Live!*

#CiscoLive

CISCO *Live!*

Let's go

#CiscoLive