
cisco Live!
Let's go

The bridge to possible

From Beginner to Champion:
Troubleshooting firepower clustering

Luis Daniel Restrepo Valencia, Technical Consulting Engineer, CX Centers EMEA

cisco Live!

BRKSEC-3691

Your Presenter

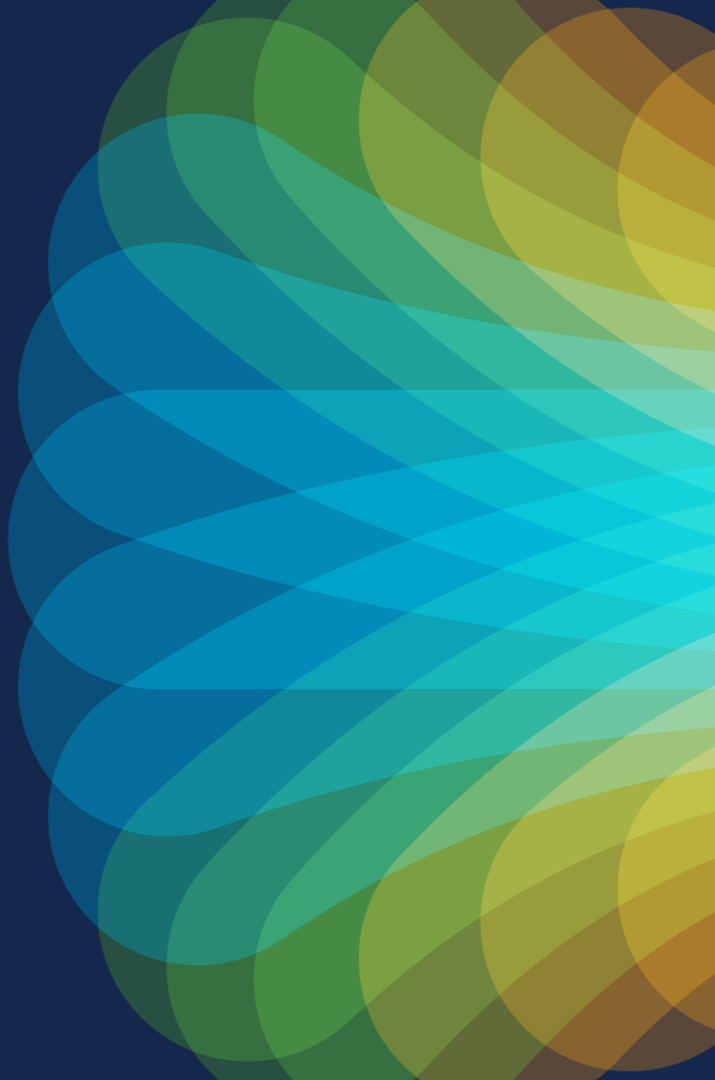
Luis Restrepo

- Electronics Engineer.
- 6 years as Technical Consulting Engineer in NGFW TAC.
  - AMER
  - EMEA
- Colombia.
- Passionate about Network/CyberSecurity.
- Hobbies:
  - Family Time, Running, Traveling.

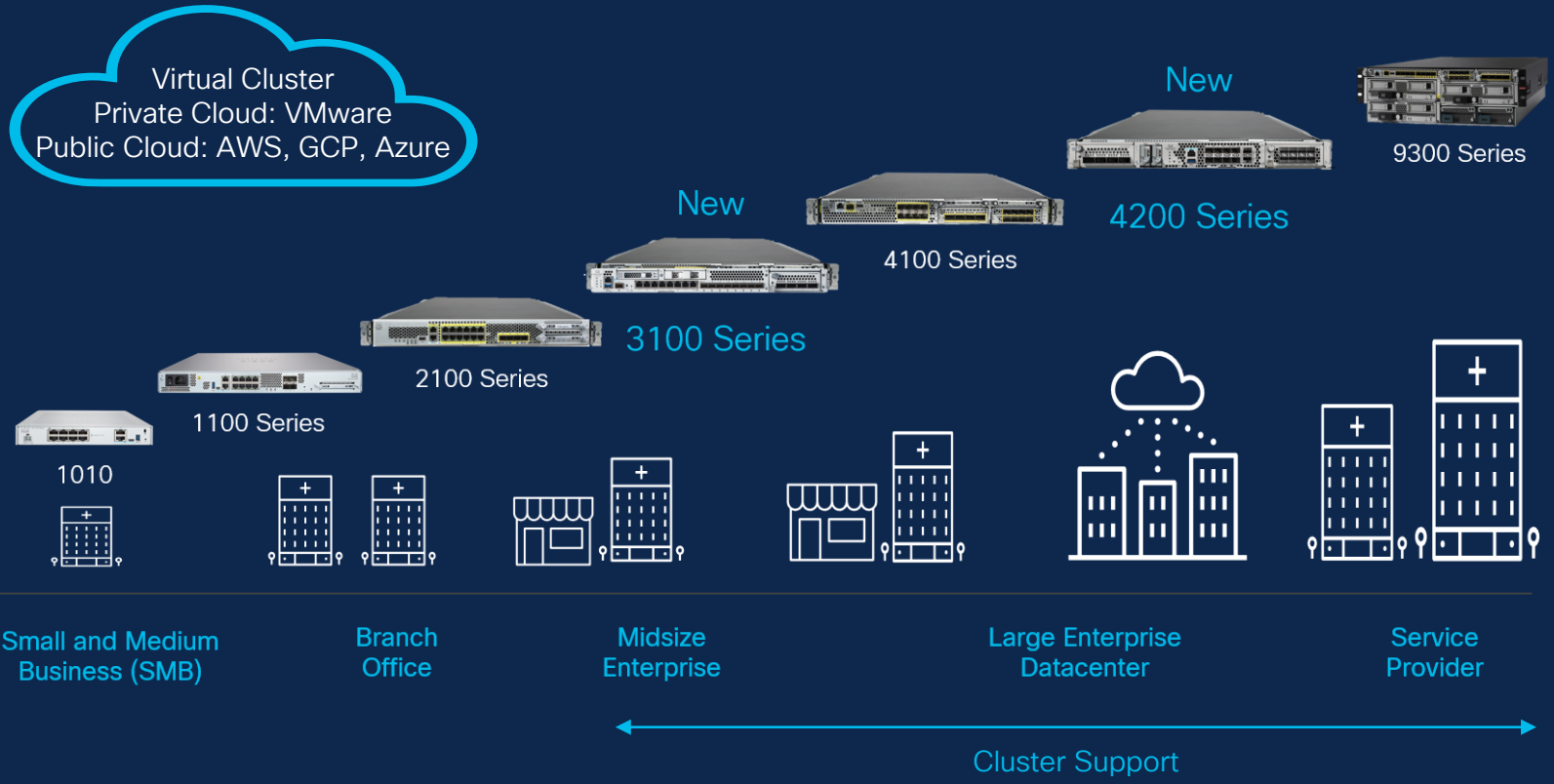
Agenda

- Introduction
- Troubleshooting
  - Know the Allies
  - Key Concepts
  - Ticket Reports
- Conclusion

Introduction



Cisco Secure Firewall Hardware Portfolio

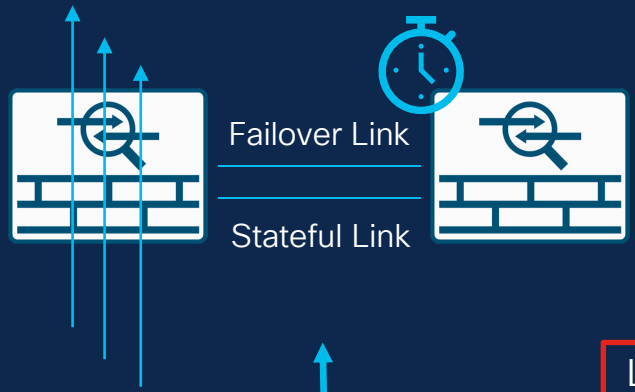


High-Availability (Failover)

Configuration replication

Two identical FTD's required

Primary/Secondary roles belong to each unit



States change between units based on health monitor

Limited to two units (not scalable), only one unit handle traffic at a time

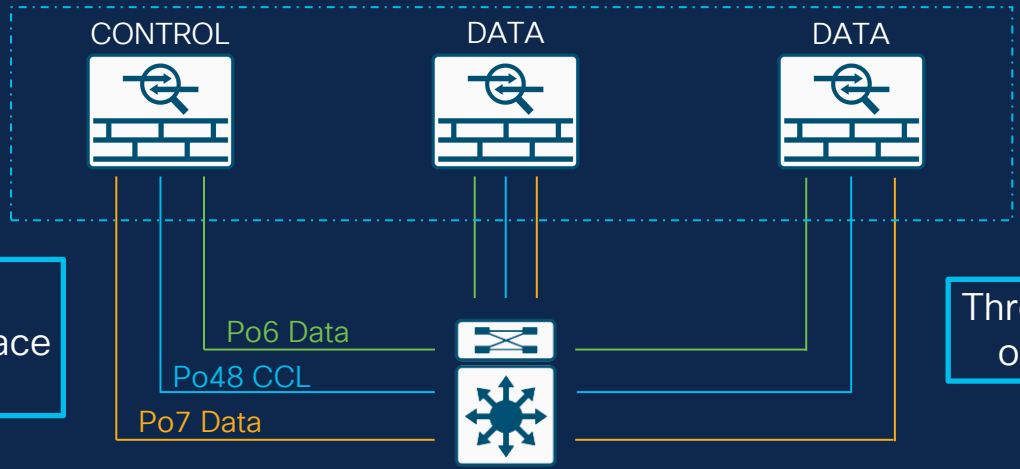
State replication

Clustering

Multiple devices grouped as one logical device

Connection states preserved on member failures

Virtual IP/MAC for first hop redundancy



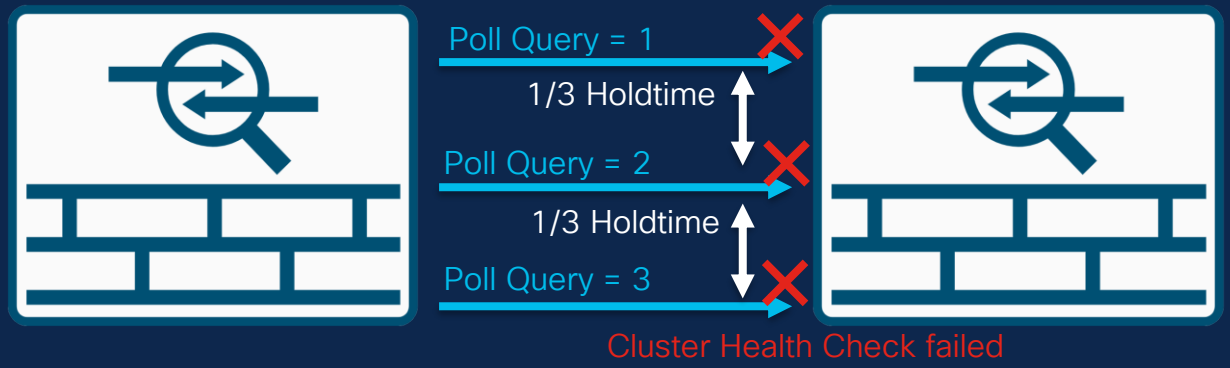
High-Availability by monitoring node, interface and service health

Throughput scales 70-80% of aggregated capacity

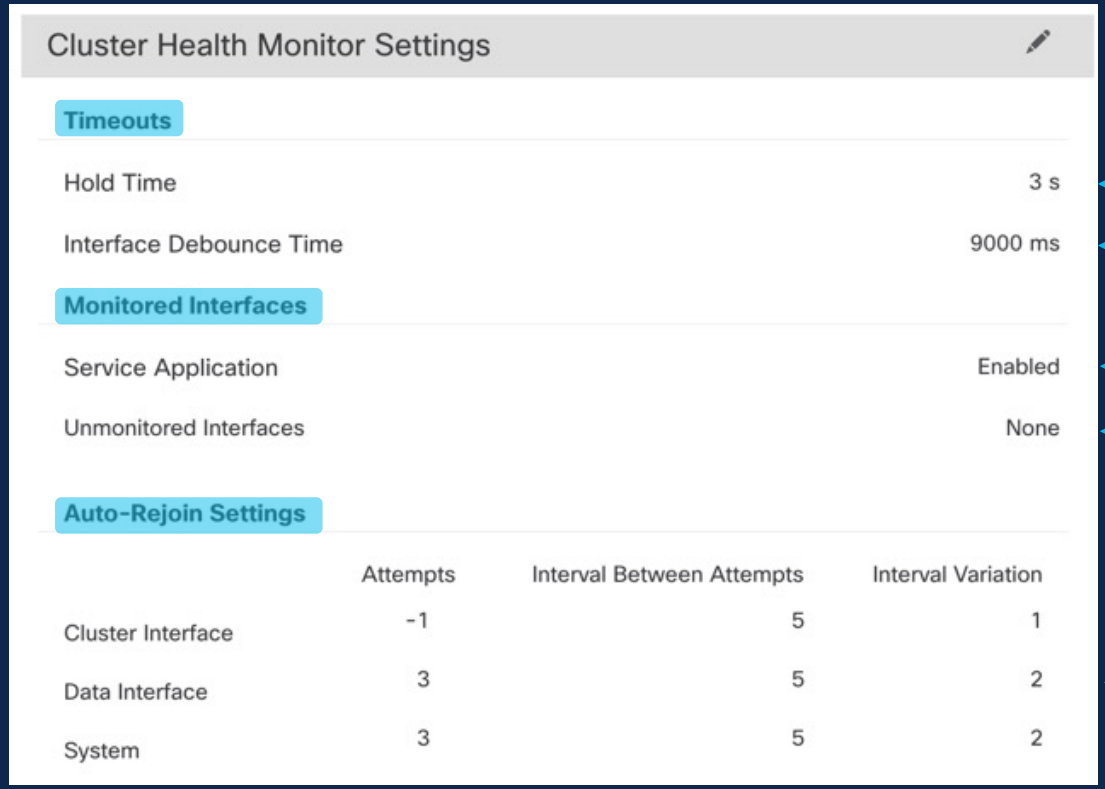
Connections scale 60% of aggregated capacity

Health Monitoring

- Members generates keepalive packets on CCL periodically.
- Control removes a unit from the cluster after 3 missed keepalives.
- Members are removed if they have Interface/Snort/Disk issues.
- Auto-rejoin can be configured for: CCL, Data interface or System.



Health Monitoring Settings FMC (7.3+)



Time unit waits to receive heartbeat messages, before marking it dead

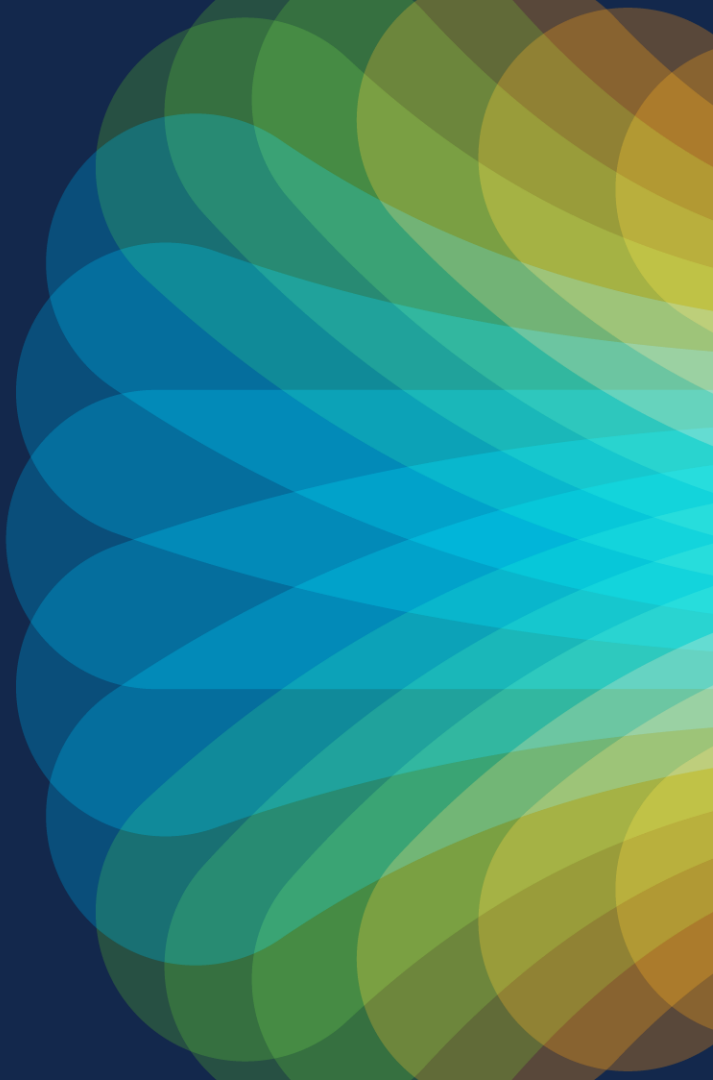
Time before the unit considers an interface to be failed

Snort + Disk monitoring

All interfaces are monitored by default

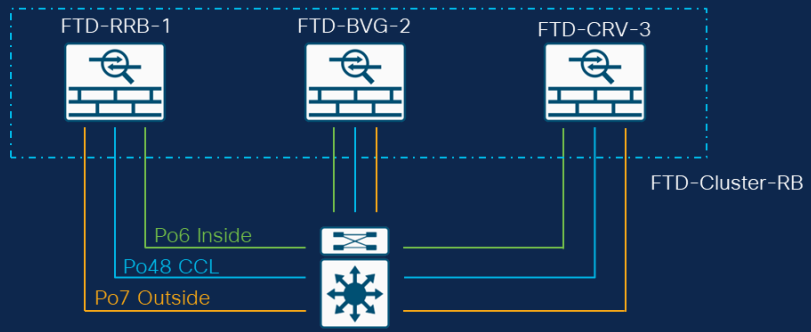
Auto-Rejoin Settings configuration

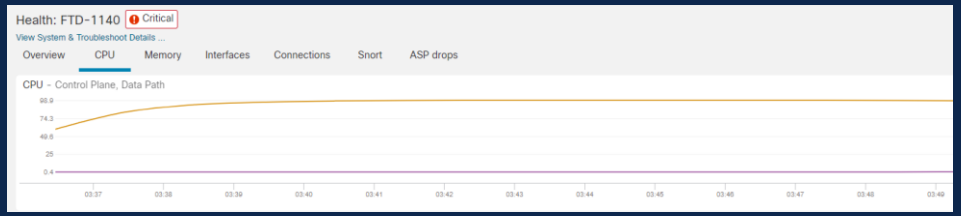
Troubleshooting



Champ Tip 1 – Understanding the problem is half the solution.

Collect as much information as possible from all cluster units.
This is key to save time in the overall troubleshooting process.





CPU Usage (per core)	CPU Usage (per core)	2023-09-14 03:47:09	CPU05 usage is 98.4%	98	n/a	!	FTD-1140
CPU Usage (per core)	CPU Usage (per core)	2023-09-14 03:47:09	CPU06 usage is 99.7%	100	n/a	!	FTD-1140
CPU Usage (per core)	CPU Usage (per core)	2023-09-14 03:47:09	CPU07 usage is 99.7%	100	n/a	!	FTD-1140
CPU Usage (per core)	CPU Usage (per core)	2023-09-14 03:47:09	CPU08 usage is 99.7%	100	n/a	!	FTD-1140
CPU Usage (per core)	CPU Usage (per core)	2023-09-14 03:47:09	CPU09 usage is 99.7%	100	n/a	!	FTD-1140
CPU Usage (per core)	CPU Usage (per core)	2023-09-14 03:47:09	CPU04 usage is 98.4%	98	n/a	!	FTD-1140
CPU Usage Data Plane	CPU Usage Data Plane	2023-09-14 03:47:09	Data Path average is 98.9%	99	n/a	!	FTD-1140

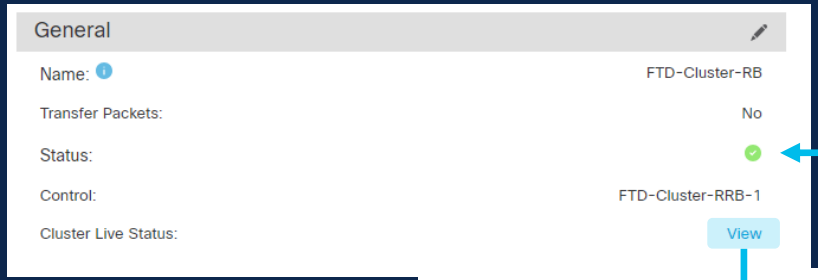
Champ Tip 2 – Ask the right questions

- When did the problem start?
- Were there any configuration changes recently?
- Were there any traffic profile changes?
- Is the problem happening all the time or is intermittent?
- When intermittent has it being correlated to specific times in the day or days in the week?
- Any recent device version upgrade or patch installation?

Know The Allies

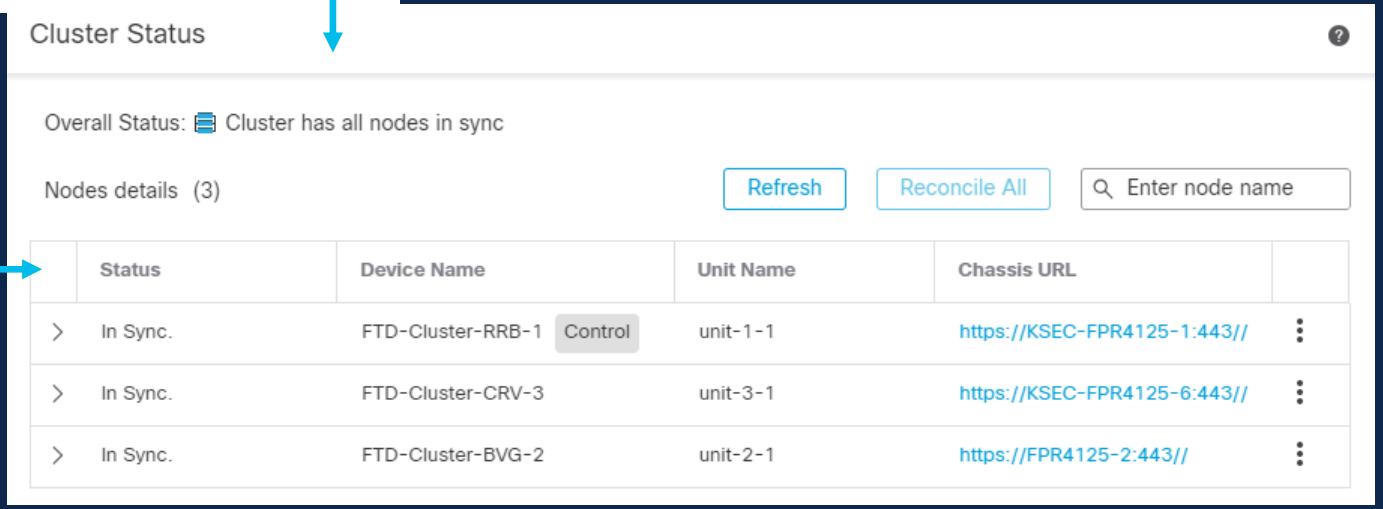
FMC Allies – Cluster Status

Under **Devices > Device Management > Cluster > General**

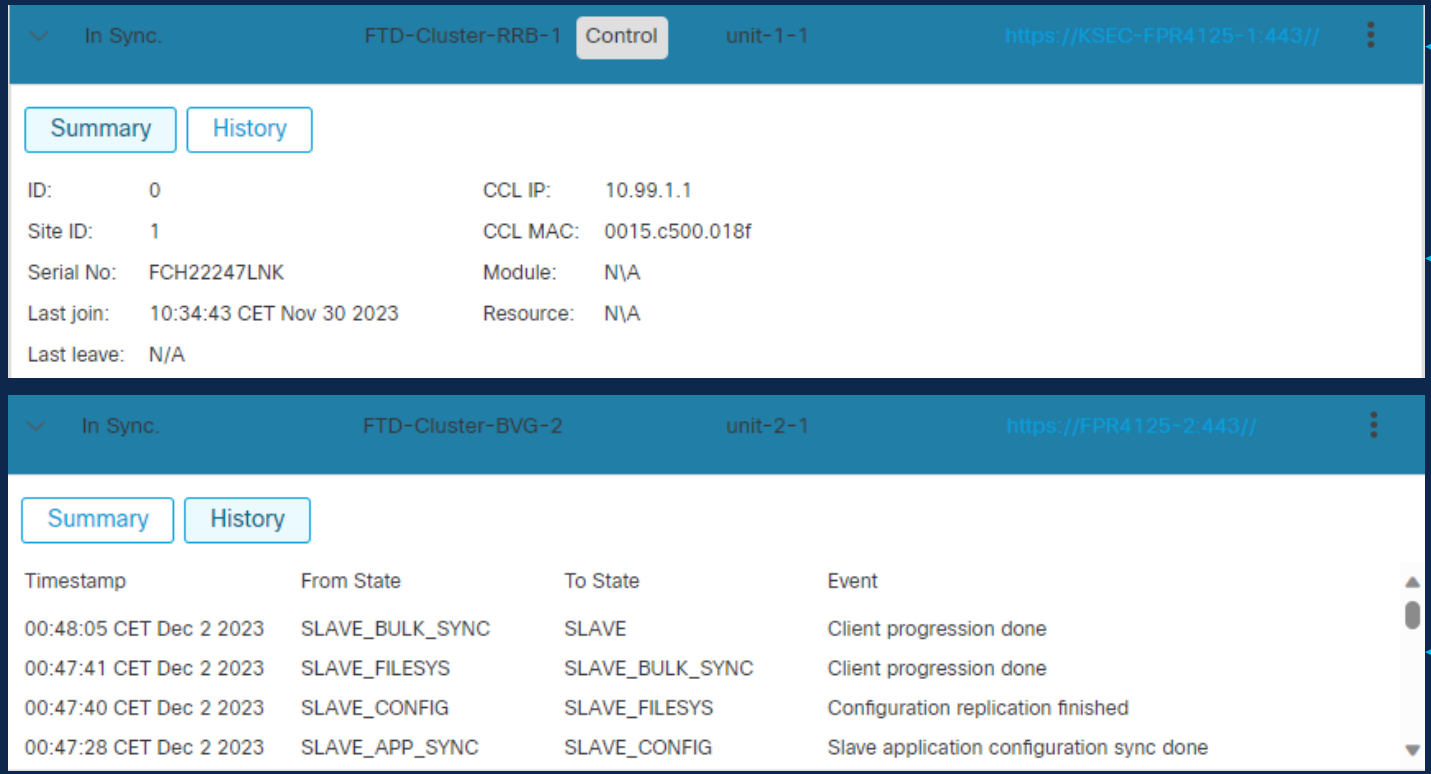


General cluster status and information

Additional cluster details



FMC Allies – Cluster Status



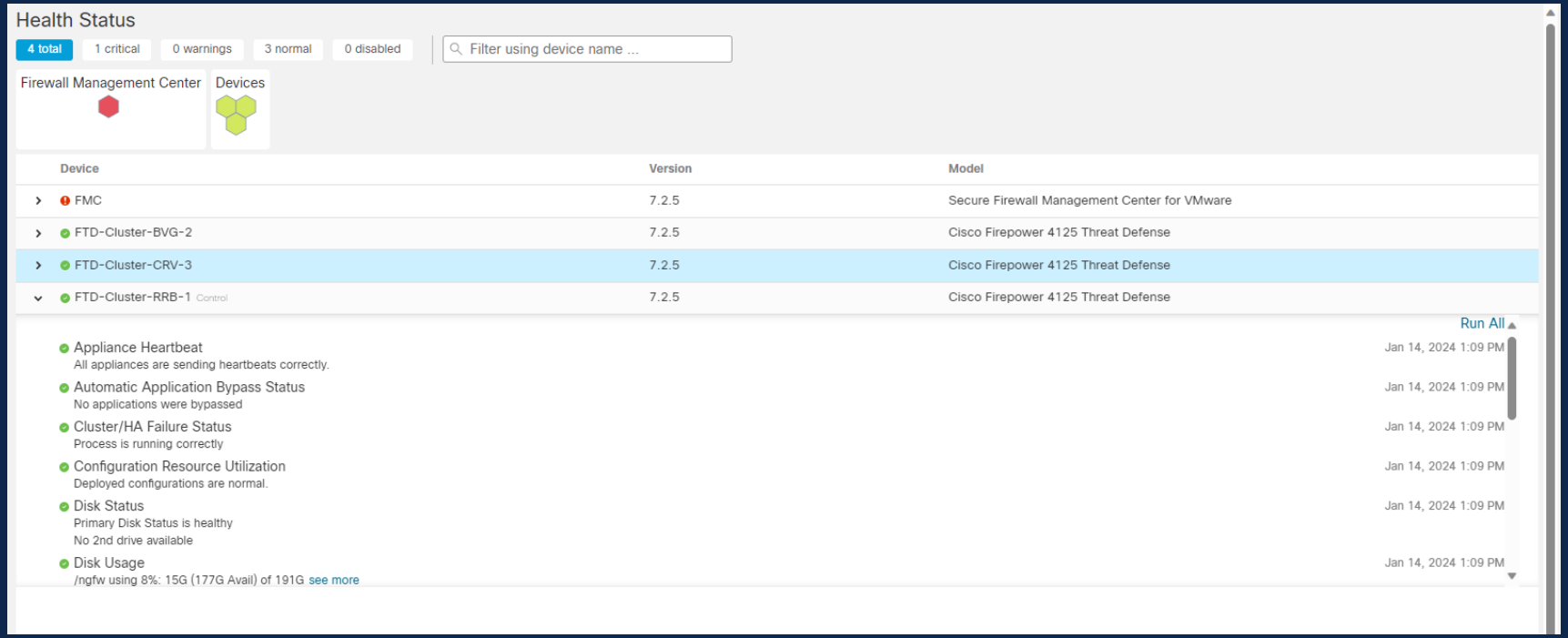
Unit state

Last join/leave and CCL IP/MAC

Unit event history and state information

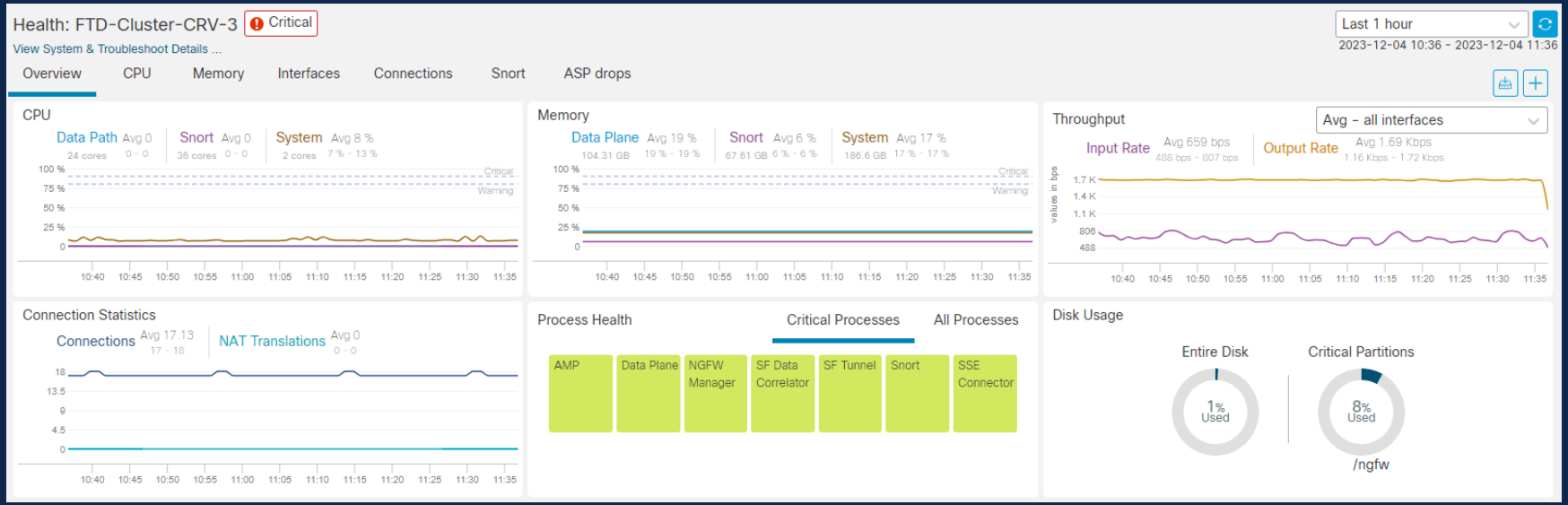
FMC Allies – Health Monitoring

On **Health > Monitor**, performance and alert information is available.



FMC Allies - Health Monitoring

Selecting the device, shows graphs on CPU, memory, throughput, connections, etc.



CLI Allies – Cheat Sheet

Reference

CLI Commands	Description
show cluster info	Cluster general info
show cluster info health	Summarized cluster health info
show cluster history	Cluster history/state details
cluster exec <cmd>	To exec commands on multiple units
capture <name> . . .	To capture traffic on units
show cluster info trace	Debug level cluster messages
show logging	Check clustering related syslog's

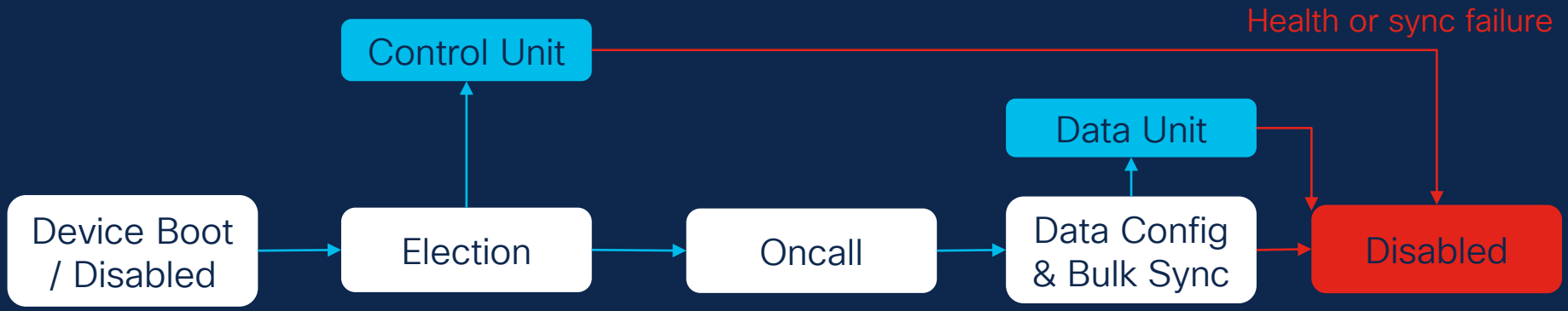
Key Concepts

Unit Roles/Functions

- Control Unit – (Previously Master)
  - One per cluster, elected based on configured priority or first to join.
  - In charge of centralized functions and management.
  - Has ownership of virtual IP address for connections to the cluster.
  - Process regular transit connections.
- Data Unit – (Previously Slave)
  - Process regular transit connections.
  - Can transition to Control role in case of failures.

Champ Tip 3. Documentation have updated terminology, however CLI still uses previous one in older versions.

Clustering Election Process

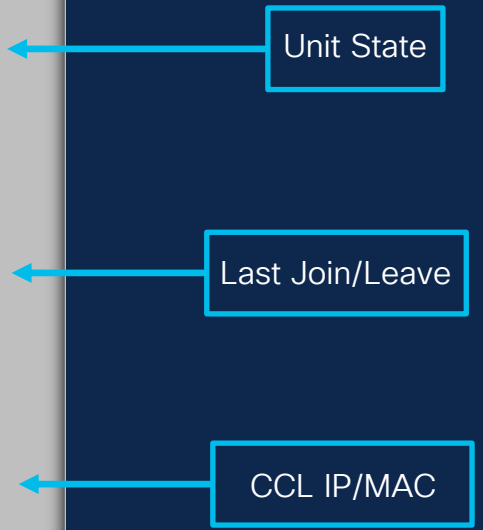



```
FTD-Cluster-BVG-2# show cluster history
================================================================================
From State              To State                Reason
================================================================================
00:46:31 CET Dec 2 2023
DISABLED                ELECTION                Enabled from CLI
00:46:31 CET Dec 2 2023
ELECTION                ONCALL                  Event: Cluster unit unit-1-1 state is MASTER
00:46:31 CET Dec 2 2023
ONCALL                  SLAVE_COLD              Slave proceeds with configuration sync
.
00:47:41 CET Dec 2 2023
SLAVE_FILESYS           SLAVE_BULK_SYNC         Client progression done
00:48:05 CET Dec 2 2023
SLAVE_BULK_SYNC         SLAVE                   Client progression done
```

Cluster Info Command

Champ Tip 4 - Always use the **show cluster info** command as first reference point for troubleshooting

```
FTD-Cluster-BVG-2# show cluster info
Cluster FTD-Cluster-RB: On
    Interface mode: spanned
Cluster Member Limit : 16
    This is "unit-2-1" in state SLAVE
        ID          : 1
        Site ID     : 1
        Version     : 9.18(3)53
        Serial No.: FCH22247MKJ
        CCL IP      : 10.99.2.1
        CCL MAC     : 0015.c500.028f
        Last join : 00:46:31 CET Dec 2 2023
        Last leave: 00:41:28 CET Dec 2 2023
Other members in the cluster:
    Unit "unit-1-1" in state MASTER
        ID          : 0
        Site ID     : 1
        Version     : 9.18(3)53
        Serial No.: FCH22247LNK
        CCL IP      : 10.99.1.1
        CCL MAC     : 0015.c500.018f
        Last join : 10:34:43 CET Nov 30 2023
        Last leave: N/A
```



Cluster Control Link (CCL)

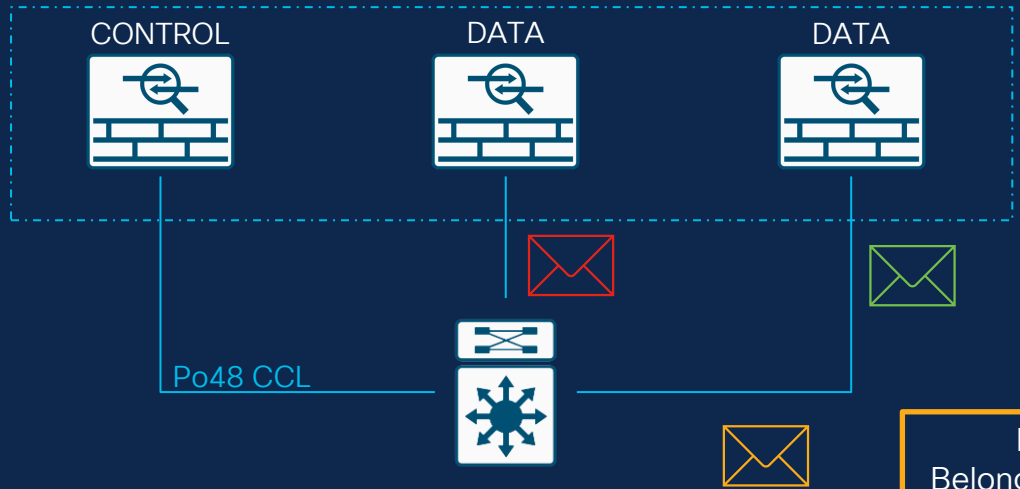
Carries all data and communications between cluster members

Requires dedicated interfaces

CCL MTU must be 100+ bytes higher that data interfaces

CCL Interface flaps force unit out of cluster

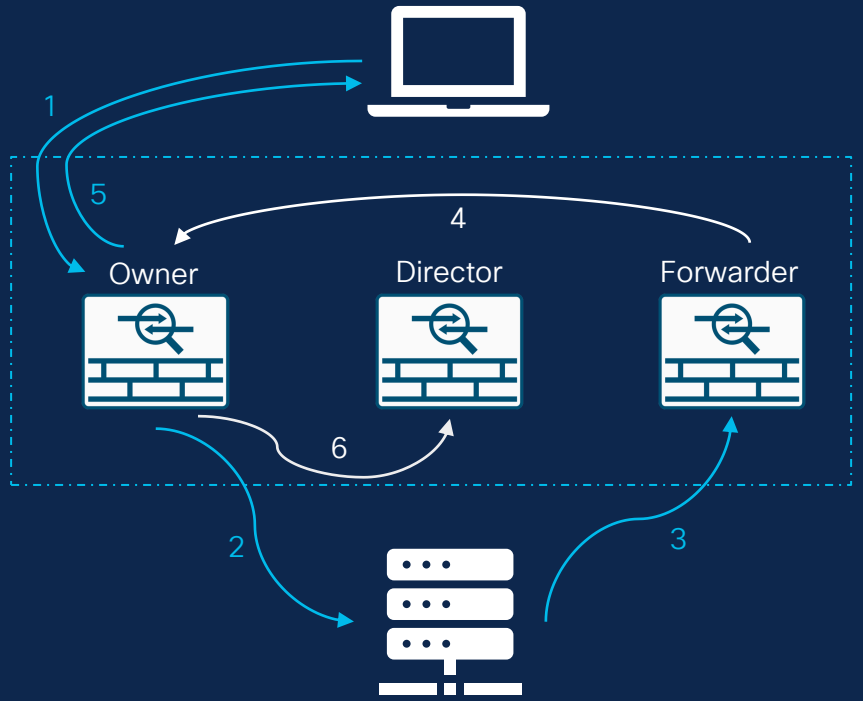
Cluster control protocol data path messages
Info about flow Owner/Director/Forwarder
Unicast
UDP 4193



Heartbeats packets
Used for health monitor
L3 Broadcast
UDP 49495

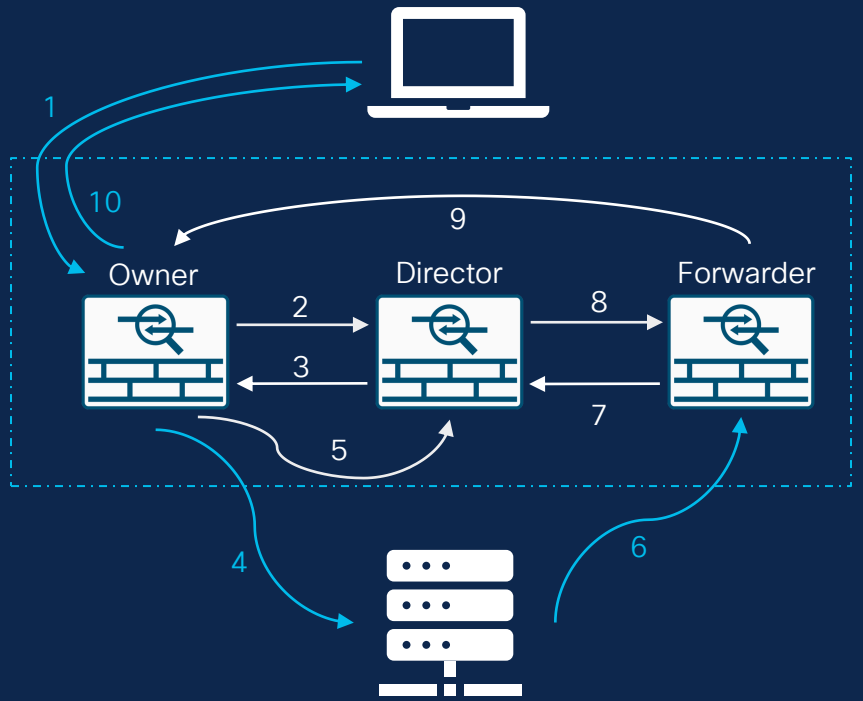
Data Packets
Belonging to traffic flows
forwarded by/to other units

New TCP Connection



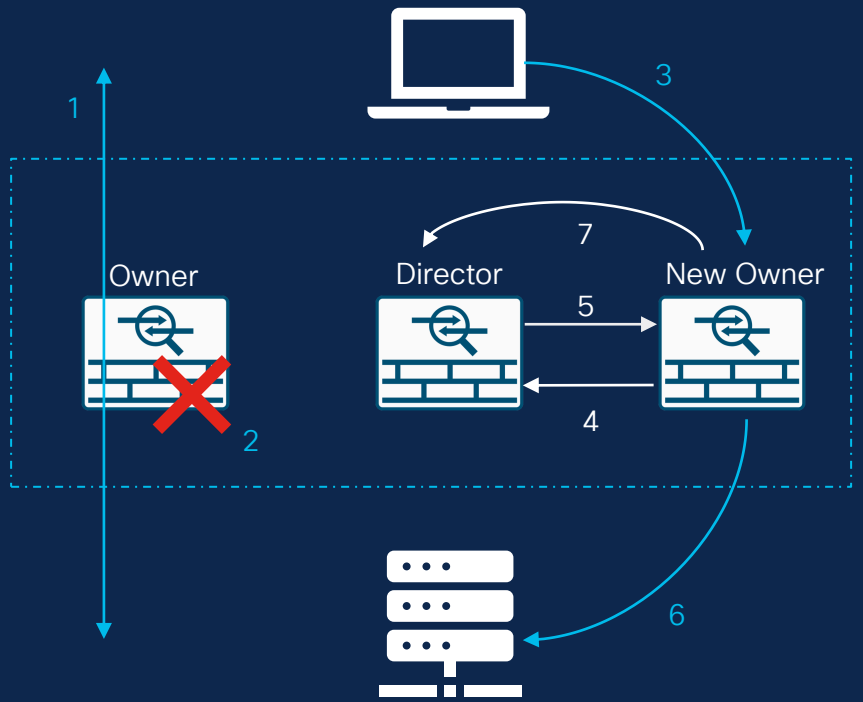
1. TCP SYN – New Connection.
2. Owner, add TCP SYN Cookie, deliver to server.
3. TCP SYN-ACK, received by different unit.
4. Redirection to Owner based on TCP SYN Cookie, unit becomes Forwarder.
5. SYN-ACK sent to client.
6. Update Director.

New UDP Connection



1. UDP – New Connection.
2. Query to Director.
3. Unit becomes Owner if not found.
4. Deliver to server.
5. Update Director.
6. Response arrives on another unit.
7. Query Director.
8. Owner is returned.
9. Packet redirected to Owner. Unit becomes Forwarder.
10. Response is sent to client.

Member Failures



1. Existing connection established.
2. Owner fails and leaves cluster.
3. Next packet load balanced to another member.
4. Query Director.
5. New Owner assigned.
6. Packet delivered to destination.
7. Update Director.

Connection Roles Information

Reference

Roles	Description	Flags
Owner	Unit receiving connection.	UIO
Forwarder	Unit that forwards packets to Owner.	z
Director	Unit that handles Owner lookup request from Forwarders.	Y
Backup Owner	If the Director is not the same as the Owner, then the Director is the Backup Owner. If the Owner is also the Director, then a separate backup Owner is chosen.	Y (Director also backup Owner) y (Director not backup Owner)
Fragment Owner	Unit that handles fragmented traffic.	-

Flags Reference Examples

```
FTD-Cluster-RRB-1# cluster exec show conn
unit-1-1(LOCAL):*******************************************************
18 in use, 40 most used
Cluster:
fwd connections: 0 in use, 12 most used
dir connections: 0 in use, 22 most used
centralized connections: 0 in use, 10 most used

TCP OUTSIDE 172.18.202.150:443 INSIDE 172.18.201.100:44394, idle 0:00:00, bytes 487413076, flags UIO N1

unit-2-1:*******************************************************
18 in use, 46 most used
Cluster:
fwd connections: 0 in use, 16 most used
dir connections: 0 in use, 8 most used
centralized connections: 0 in use, 0 most used

unit-3-1:*******************************************************
15 in use, 42 most used
Cluster:
fwd connections: 1 in use, 7 most used
dir connections: 1 in use, 32 most used
centralized connections: 0 in use, 0 most used

TCP OUTSIDE 172.18.202.150:443 INSIDE 172.18.201.100:44394, idle 0:00:06, bytes 0, flags y
```

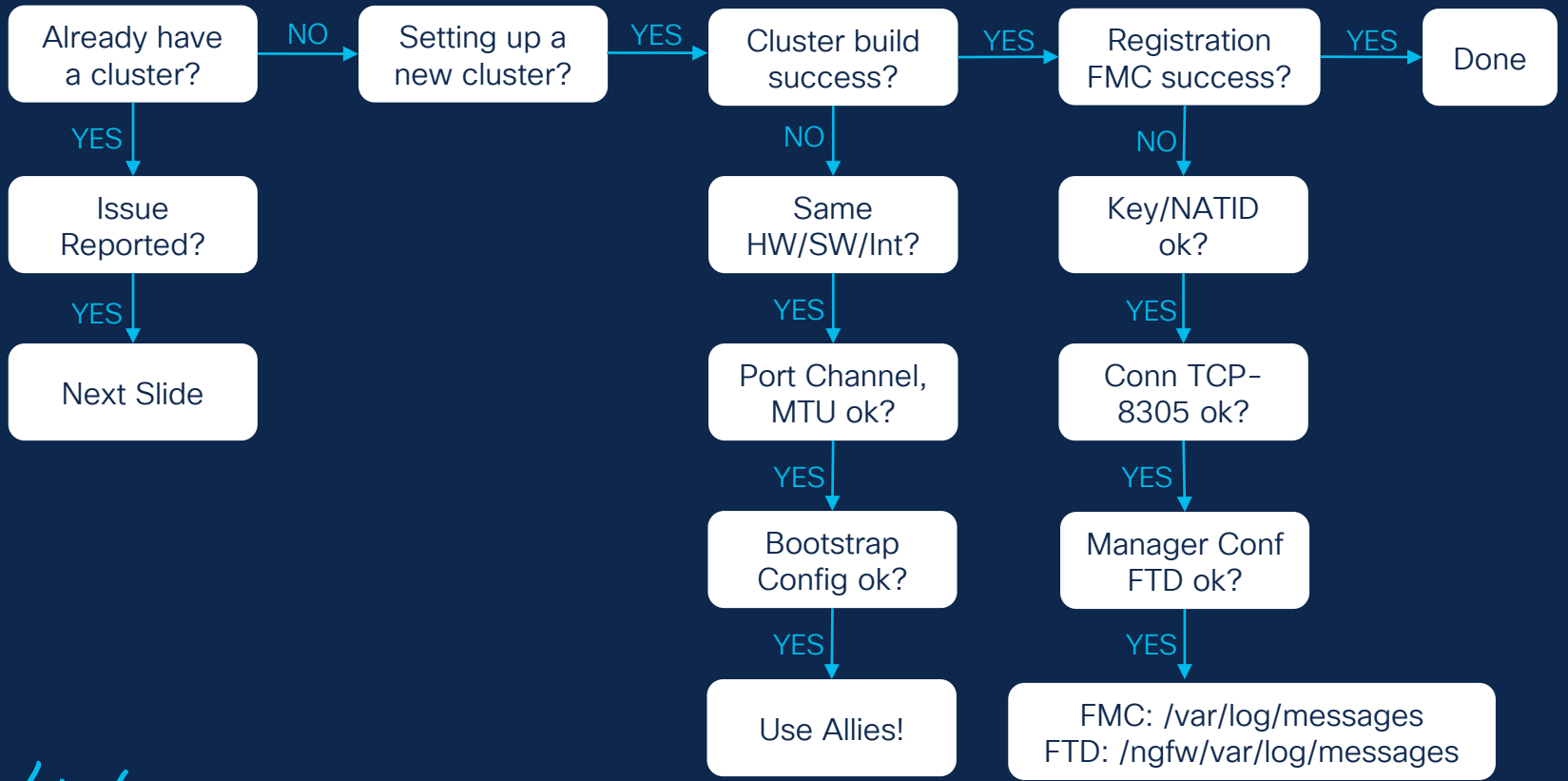
Connection Count

Owner + Director

Backup Owner

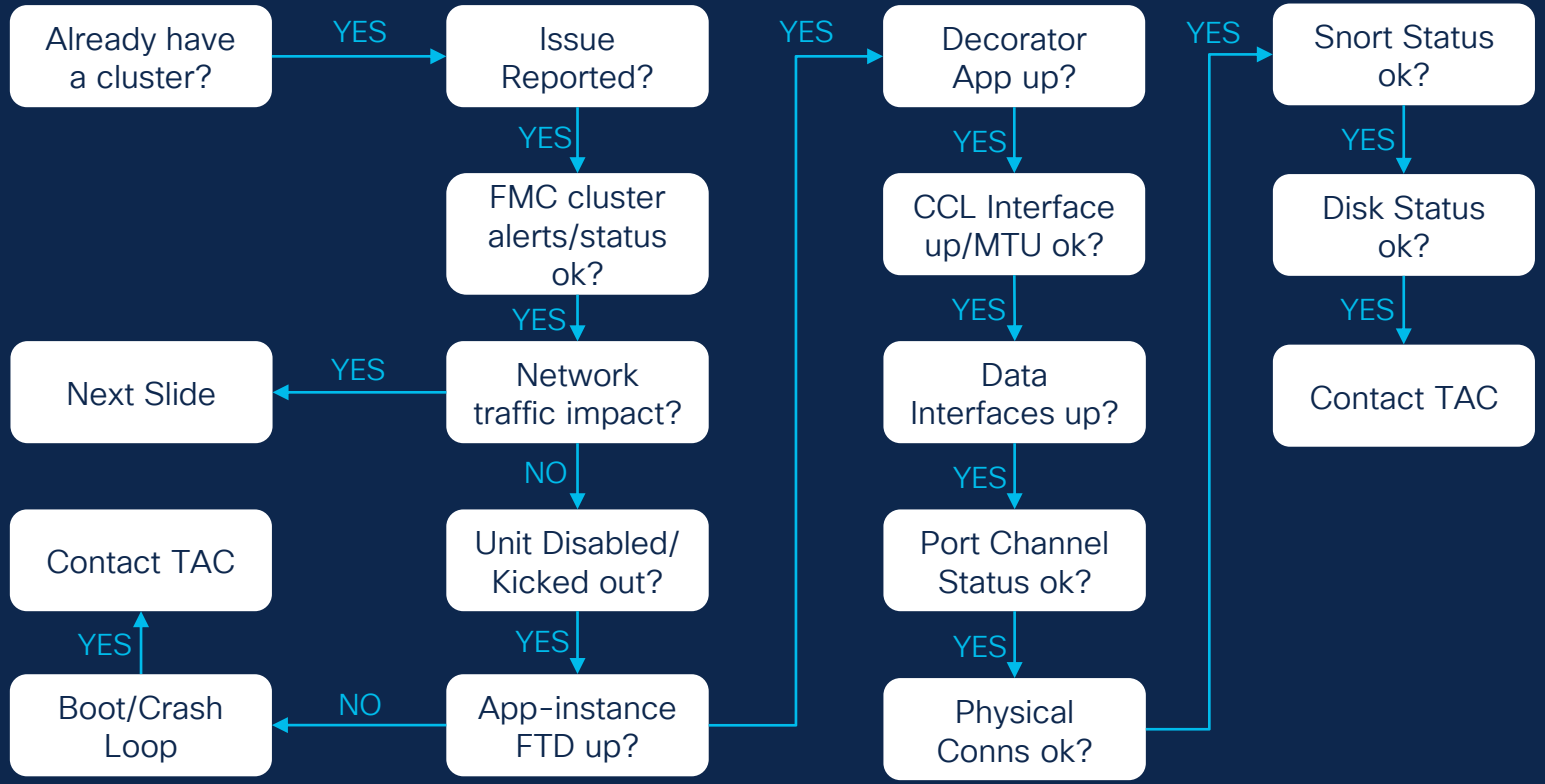
Setup Cluster Troubleshooting Methodology

Reference



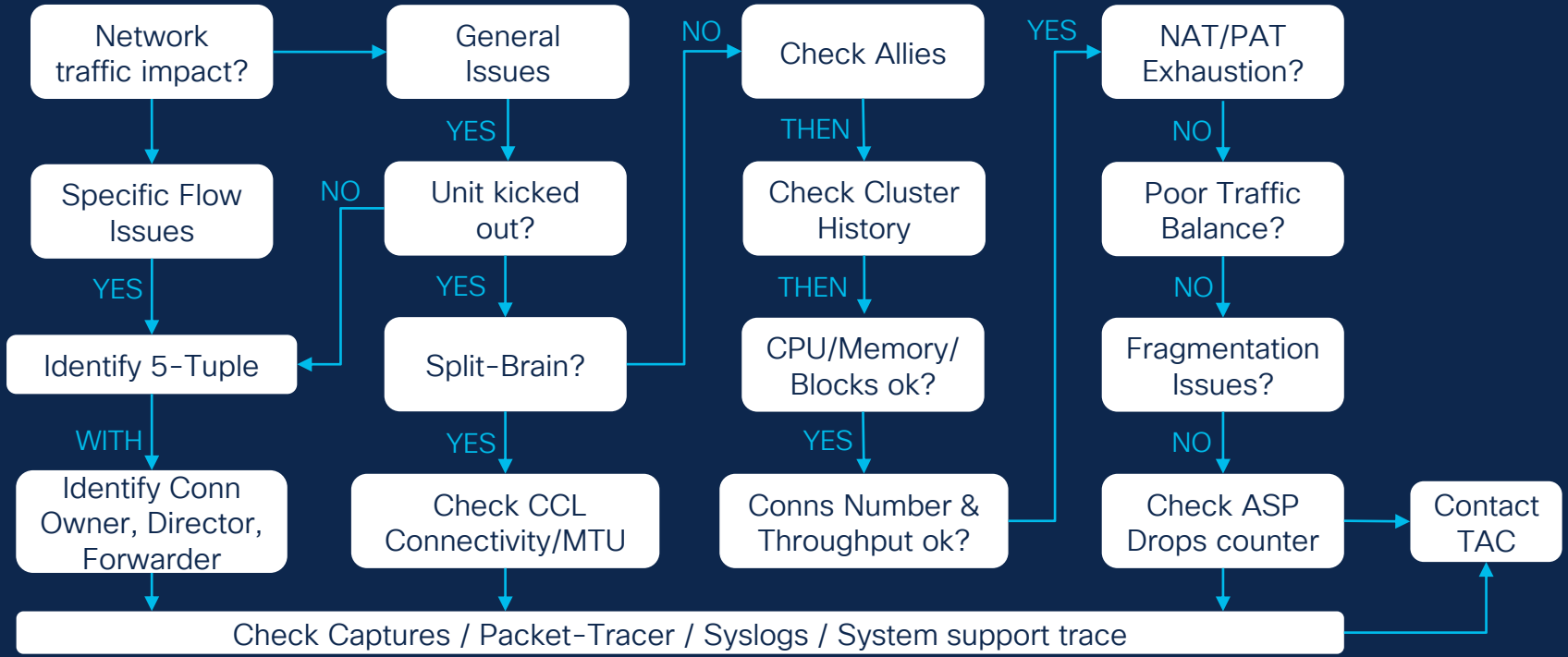
Cluster Health Troubleshooting Methodology

Reference



Data Plane Troubleshooting Methodology

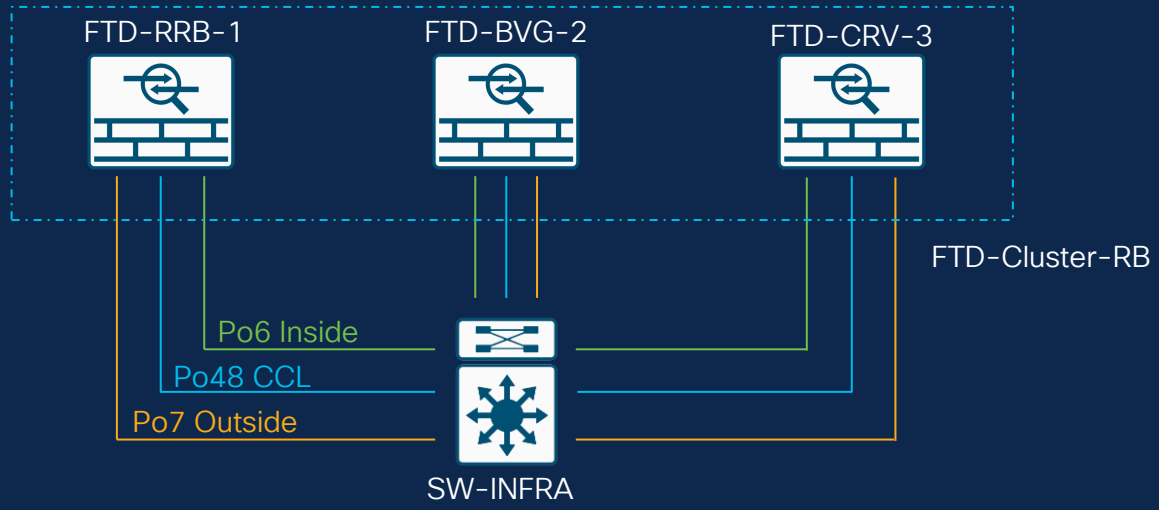
Reference



Ticket Reports

Giant Snorty (Imaginary-Scenario Company)

- Has a 3-unit cluster of 4125's.
- This cluster acts as perimeter firewall for their network.
- 7 Tickets were opened for the security engineer to handle.



Ticket Report #1

Ticket #1 – General Questions

Customer Symptom:

- Are DHCP Server and client supported with clustering setups?
- Are dynamic routing protocols supported with clustering setups?

Resolution:

- Based on Cisco documentation DHCP Server/Client are unsupported features on clustering.
- Dynamic routing protocols are supported and it’s a centralized feature.

Unsupported Features

- Remote Access VPN (SSL/IPsec).
- DHCP client, server, and proxy.
- Virtual tunnel interfaces (VTI).
- Management Center UCAPL/CC mode.
- Integrated routing and bridging.
- Failover configuration.

Centralized Features

The following features are only supported in the Control node.

- Application inspections (DCERPC, ESMTP, NetBIOS, PPTP, RSH, SQLNET, SUNRPC, TFTP, XDMCP).
- Static route monitoring.
- Site-to-Site VPN.
- IGMP/PIM multicast control plane protocol processing.
- Dynamic Routing.

Ticket Report #2

Ticket #2 – Throughput Testing Issues

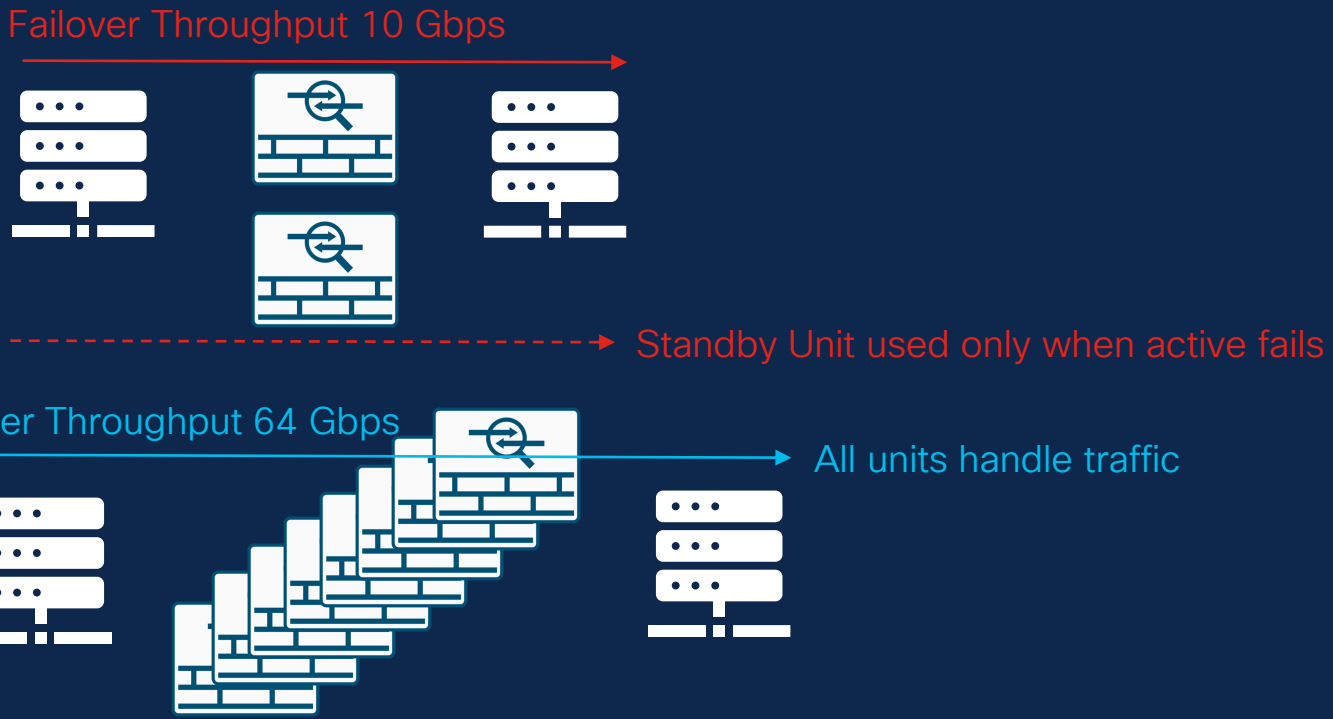
Customer Symptom:

- On our FPR4125 cluster we are expecting 135 Gbps of throughput (datasheet information), when doing performance test we cannot reach those values, why?

Resolution:

- When combining multiple units into a cluster, the total expected performance is ~80% of the maximum combined throughput.
- In this case if each unit has 45 Gbps as standalone, on 3-unit cluster the approximate combined throughput would be (80% of 135 Gbps = 108 Gbps).
- Calculations are based on 1024B packet size.

Performance Scaling Factor

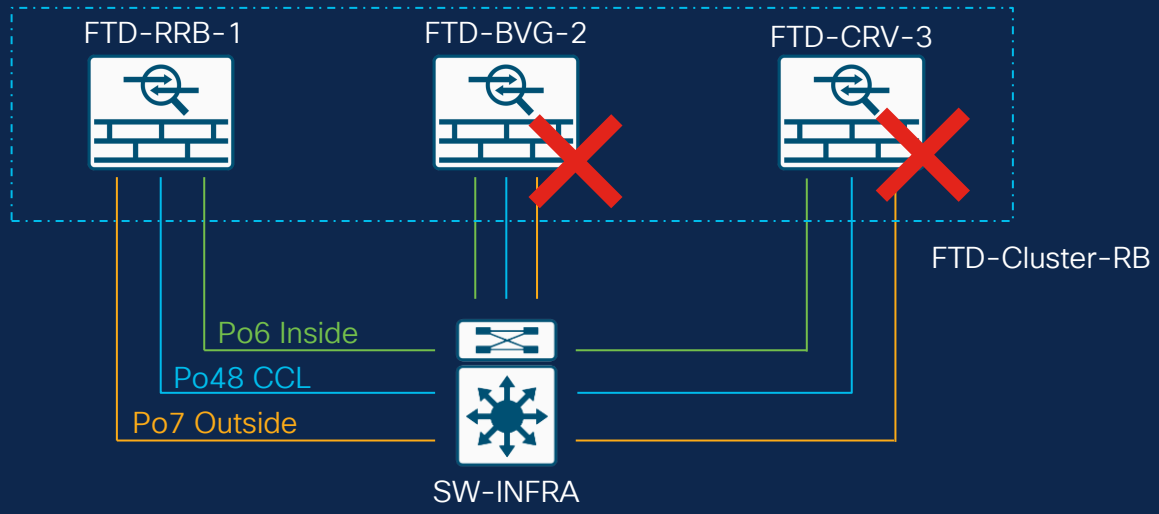


Ticket Report #3

Ticket #3 – Datacenter Activity Report

Customer Symptom:

- Yesterday there was a planned activity in the datacenter.
- Clustering on two units was reported as disabled afterwards.



Champ Tip 5 - Use FMC as starting troubleshooting point

FTD-Cluster-BVG-2

⚠ Cluster/Failover St... STANDALONE (FCH22247MKJ) CLUSTER_STATE_DISABLED (Received control message DISABLE (interface health check failure))

FTD-Cluster-CRV-3

⚠ Cluster/Failover St... STANDALONE (FLM251700E8) CLUSTER_STATE_DISABLED (Cluster interface down)

FMC Alerts

Nodes details (3) Refresh Reconcile All Enter node name

	Status	Device Name	Unit Name	Chassis URL
>	In Sync.	FTD-Cluster-RRB-1 Control	unit-1-1	https://KSEC-FPR4125-1:443//
v	Clustering is disabled	FTD-Cluster-CRV-3	unit-3-1	https://KSEC-FPR4125-6:443//

Unit 3-1

Summary History

Timestamp	From State	To State	Event
18:46:53 UTC Dec 6 2023	SLAVE	DISABLED	Cluster interface down
23:48:05 UTC Dec 1 2023	SLAVE	SLAVE	Event: Cluster unit unit-2-1 state is SLAVE
23:47:41 UTC Dec 1 2023	SLAVE	SLAVE	Event: Cluster unit unit-2-1 state is SLAVE_BULK_SYNC
23:47:40 UTC Dec 1 2023	SLAVE	SLAVE	Event: Cluster unit unit-2-1 state is SLAVE_FILESYS

Unit went from Data to Disabled

Champ Tip 6 – Check Allies, First Control Unit

```
FTD-Cluster-RRB-1# Asking slave unit unit-3-1 to quit because it failed unit health-check.
FTD-Cluster-RRB-1# Asking slave unit unit-2-1 to quit because it failed interface health check 1 times (last failure
on Port-channel6), rejoin will be attempted after 5 min.

FTD-Cluster-RRB-1# show cluster info
Cluster FTD-Cluster-RB: On
    Interface mode: spanned
Cluster Member Limit : 16
    This is "unit-1-1" in state MASTER
        ID          : 0
        Site ID     : 1
        Version     : 9.18(3)53
        Serial No.: FCH22247LNK
        CCL IP      : 10.99.1.1
        CCL MAC     : 0015.c500.018f
        Last join : 10:34:43 CET Nov 30 2023
        Last leave: N/A
```

Units 2-1 & 3-1 kicked out

```
FTD-Cluster-RRB-1# show cluster history

19:46:53 CET Dec 6 2023
MASTER                  MASTER              Event: Cluster unit unit-3-1 state
                                            is DISABLED

20:12:13 CET Dec 6 2023
MASTER                  MASTER              Event: Asking slave unit unit-2-1
                                            to quit because it failed
                                            interface health check 1
                                            times (last failure on Port-channel6),
                                            rejoin will be attempted
                                            after 5 min.

20:12:13 CET Dec 6 2023
MASTER                  MASTER              Event: Cluster unit unit-2-1 state
                                            is DISABLED
```

Champ Tip 7 – Restore failed units ASAP to avoid oversubscription of a single unit!

Champ Tip 8 – Divide & Conquer, one issue/unit at a time

Control Unit:

```
FTD-Cluster-RRB-1# show cluster info trace | inc unit-2-1
Dec 06 20:12:13.832 [INFO]Peer unit-2-1(1) reported its Port-channel6 is down
Dec 06 20:12:13.832 [INFO]Slave unit unit-2-1 reports inconsistent cluster interface state for interface Port-channel6
(up on master unit, down on slave unit).
Dec 06 20:12:13.832 [DBUG]Send CCP message to unit-2-1(1): CCP_MSG_IFC_REJOIN_FAIL_COUNTER
Dec 06 20:12:13.832 [DBUG]Send CCP message to unit-2-1(1): CCP_MSG_QUIT from unit-1-1 to unit-2-1 for reason
CLUSTER_QUIT_REASON_IFC_HC
Dec 06 20:12:13.832 [ALERT]Asking slave unit unit-2-1 to quit because it failed interface health check 1 times (last
failure on Port-channel6), rejoin will be attempted after 5 min
Dec 06 20:12:13.832 [INFO]State machine notify event CLUSTER_EVENT_MEMBER_STATE (unit-2-1,DISABLED,0)
.
Dec 06 20:17:17.674 [DBUG]Receive CCP message: CCP_MSG_ELEC_REQ from unit-2-1
Dec 06 20:17:17.784 [INFO]State machine notify event CLUSTER_EVENT_MEMBER_STATE (unit-2-1,SLAVE_COLD,0)
Dec 06 20:17:17.784 [INFO]FTD - CD proxy received state notification (SLAVE_COLD) from unit unit-2-1
Dec 06 20:17:17.794 [INFO]CCL MTU test to unit unit-2-1 passed
Dec 06 20:17:17.814 [INFO]State machine notify event CLUSTER_EVENT_MEMBER_STATE (unit-2-1,SLAVE_APP_SYNC,0)
Dec 06 20:19:37.793 [INFO]Peer unit-2-1(1) reported its Port-channel6 is down
Dec 06 20:32:03.176 [INFO]Peer unit-2-1(1) reported its Port-channel6 is down
```

Data interface reported as down (Port-Channel6)

Data unit was kicked out due to interface health check

Champ Tip 9 – Check Data Unit

Cluster is disabled

LINA

```
FTD-Cluster-BVG-2# Unit is kicked out from cluster because of interface health check failure.
FTD-Cluster-BVG-2# Cluster disable is performing cleanup..done.
FTD-Cluster-BVG-2# All data interfaces have been shutdown due to clustering being disabled. To recover either enable
clustering or remove cluster group configuration.
```

FXOS

```
FTD-Cluster-BVG-2# scope eth-uplink; scope fabric a; show port-channel
Port Channel:
Port Channel  Id Name  Port Type  Admin State Oper State  Port Channel Mode Allowed Vlan State Reason
    --------------- ---------------- ------------------ ----------- ---------------- ------------------ ------------
  6        Port-channel6  Data       Enabled     Failed       Active           All       No operational members
  7        Port-channel7  Data       Enabled     Failed       Active           All       No operational members
 48        Port-channel48 Cluster    Enabled     Up           Active           All       Port is enabled and up

FTD-Cluster-BVG-2# connect fxos
FTD-Cluster-BVG-2(fxos)# show port-channel summary
Flags:  D - Down         P - Up in port-channel (members)
        I - Individual   H - Hot-standby (LACP only)
        s - Suspended    r - Module-removed
        S - Switched     R - Routed
        U - Up (port-channel)
        M - Not in use. Min-links not met
--------------------------------------------------------------------------------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------------------------
6     Po6(SD)     Eth      LACP      Eth1/2(D)
7     Po7(SD)     Eth      LACP      Eth1/3(s)
48    Po48(SU)    Eth      LACP      Eth1/4(P)    Eth1/5(P)
```

Port-Channel6 Down

FXOS

```
FTD-Cluster-BVG-2# connect fxos
FTD-Cluster-BVG-2(fxos)# show lacp internal event-history interface ethernet 1/2
64) FSM:<Ethernet1/2> Transition at 297515 usecs after Wed Dec  6 19:12:13 2023    Previous state:
[LACP_ST_PORT_MEMBER_COLLECTING_AND_DISTRIBUTING_ENABLED]    Triggered event: [LACP_EV_UNGRACEFUL_DOWN]    Next state:
[LACP_ST_PORT_IS_DOWN_OR_LACP_IS_DISABLED]
65) FSM:<Ethernet1/2> Transition at 376781 usecs after Wed Dec  6 19:12:13 2023    Previous state:
[LACP_ST_PORT_IS_DOWN_OR_LACP_IS_DISABLED]    Triggered event: [LACP_EV_UNGRACEFUL_DOWN]    Next state:
[FSM_ST_NO_CHANGE]
```

SWITCH

```
GIANT-SNORTY-CORE1#show int status | inc 4/15
Gi4/15        FTD-BVG-2-P2 - E disabled     201            full   auto 10/100/1000BaseT
GIANT-SNORTY-CORE1#show int status | inc 4/17
Gi4/17        FTD-BVG-2-P4-CCL - E connected    209        a-full a-1000 10/100/1000BaseT
GIANT-SNORTY-CORE1#show int status | inc 4/18
Gi4/18        FTD-BVG-2-P5-CCL - E connected    209        a-full a-1000 10/100/1000BaseT

interface GigabitEthernet4/15
 description KSEC-FPR4125-2 - E1/2
 switchport
 switchport access vlan 201
 switchport mode access
 shutdown
 channel-group 40 mode active
 spanning-tree portfast edge
end
```

Ungraceful down from LACP events

Interface was shutdown as part of activity

Ticket #3 – Troubleshoot

```
FTD-Cluster-CRV-3# show cluster info
Cluster FTD-Cluster-RB: On
    Interface mode: spanned
Cluster Member Limit : 16
    This is "unit-3-1" in state MASTER
        ID          : 0
        Site ID     : 1
        Version     : 9.18(3)53
        Serial No.: FLM251700E8
        CCL IP      : 10.99.3.1
        CCL MAC     : 0015.c500.038f
        Last join : 18:52:39 UTC Dec 6 2023
        Last leave: 18:46:50 UTC Dec 6 2023
Other members in the cluster:
    There is no other unit in the cluster
```

```
FTD-Cluster-CRV-3# show cluster history
18:46:53 UTC Dec 6 2023
SLAVE                DISABLED              Cluster interface down

18:51:54 UTC Dec 6 2023
DISABLED             ELECTION              Enabled from CLI

18:52:39 UTC Dec 6 2023
ELECTION             MASTER_CONFIG         Enabled from CLI

18:52:39 UTC Dec 6 2023
MASTER_CONFIG        MASTER_POST_CONFIG    Client progression done

18:52:40 UTC Dec 6 2023
MASTER_POST_CONFIG   MASTER                Master post config done
and waiting for ntfy
```

Units 1-1 & 3-1 are Control at the same time (Split-Brain)

Unit 3-1 doesn't see other units on CCL

Unit 3-1 transitions from Data > Disabled > Control

Champ Tip 10 – Split-brain scenarios happen when two units consider themselves as the control unit at the same time. This is impactful, as there will be duplicated IP addresses.

Ticket #3 - Troubleshoot

LINA

```
FTD-Cluster-CRV-3# show int ip br
Interface                  IP-Address      OK?           Method Status      Protocol
Port-channel6              172.18.201.1    YES           manual up          up
Port-channel7              172.18.202.1    YES           manual up          up
Port-channel48             10.99.3.1       YES           unset  up          up
Ethernet1/1                unassigned      YES           unset  up          up
FTD-Cluster-RRB-1#

FTD-Cluster-RRB-1# show int po48
Interface Port-channel48 "cluster", is up, line protocol is up
  Hardware is EtherSVI, BW 2000 Mbps, DLY 1000 usec
        Description: Clustering Interface
        MAC address 0015.c500.038f, MTU 1600
        IP address 10.99.3.1, subnet mask 255.255.0.0
```

Interface is up and right MTU is set

```
FTD-Cluster-CRV-3# ping cluster 10.99.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.99.1.1, timeout is 2 seconds:
?????
Success rate is 0 percent (0/5)
```

No connectivity over CCL

Ticket #3 - Troubleshoot

FXOS

```
FTD-Cluster-CRV-3# connect fxos
FTD-Cluster-CRV-3(fxos)# show port-channel database
port-channel48
    Last membership update is successful
    2 ports in total, 2 ports up
    First operational port is Ethernet1/5
    Age of the port-channel is 7d:01h:11m:52s
    Time since last bundle is 7d:01h:11m:38s
    Last bundled member is Ethernet1/5
    Ports:   Ethernet1/4     [active ] [up]
             Ethernet1/5     [active ] [up] *
```

Port-Channel status ok, member ports active/up

SWITCH

```
GIANT-SNORTY-CORE1# show run int Po45
interface Port-channel45
 switchport
 switchport access vlan 206
 switchport mode access
 mtu 1600
 spanning-tree portfast edge
end
```

Champ Tip 11 – Always have in hand working configuration from adjacent devices for comparison.

Wrong VLAN was configured on Port-Channel45 as part of activity

Ticket #3 – Summary

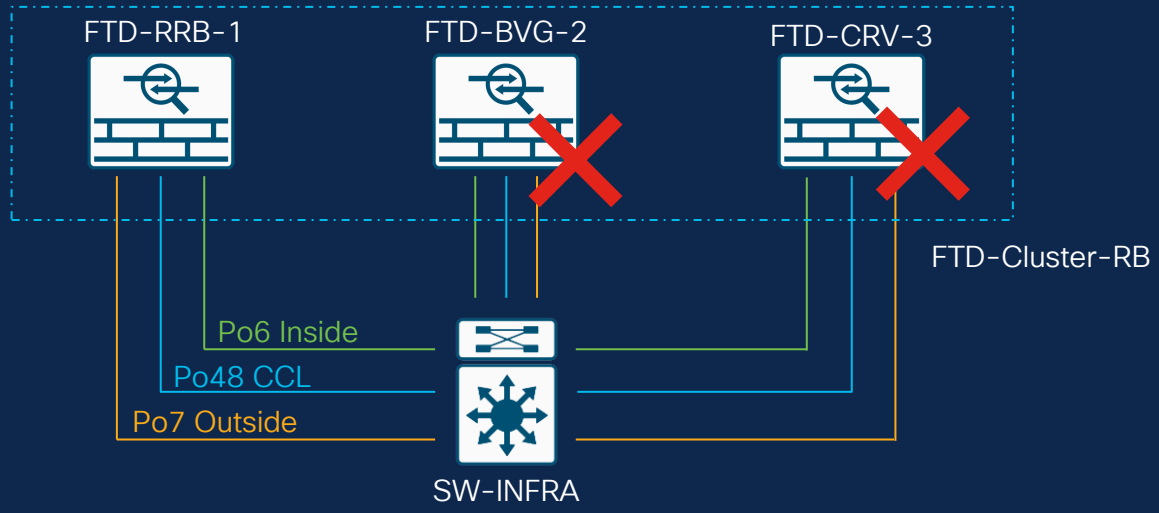
- Two data units were kicked out from cluster (unit 2 & 3).
- Only recent change was an activity performed on the datacenter switches.
- After investigating configuration was OK on cluster units, however Control unit reported:
  - Unit-2-1: Interface health check.
  - Unit-3-1: Unit health check.
- Issue was identified as misconfiguration on adjacent devices, causing data interface and CCL failures.

Ticket Report #4

Ticket #4 – Service Health Report

Customer Symptom:

- Today two of our units were reported as kicked out from the cluster at different times.
- There was no impact, but customer is afraid it can happen again.



Ticket #4 – General Troubleshooting

```
FTD-Cluster-RRB-1# show cluster info
Cluster FTD-Cluster-RB: On
    Interface mode: spanned
Cluster Member Limit : 16
    This is "unit-1-1" in state MASTER
        ID          : 0
        Site ID     : 1
        Version     : 9.18(3)53
        Serial No.: FCH22247LNK
        CCL IP      : 10.99.1.1
        CCL MAC     : 0015.c500.018f
        Last join : 10:34:43 CET Nov 30 2023
        Last leave: N/A
```

Units 2-1 & 3-1 kicked out from cluster

```
FTD-Cluster-RRB-1# show cluster history

20:40:09 CET Dec 8 2023
MASTER                MASTER              Event: Asking slave unit unit-3-1
                                          to quit due to snort Application
                                          health check failure, and
                                          slave's application state
                                          is down.

20:40:09 CET Dec 8 2023
MASTER                MASTER              Event: Cluster unit unit-3-1
                                          state is DISABLED
```

Unit 3-1 was kicked out due to snort check failure

Ticket #4 – General Troubleshooting

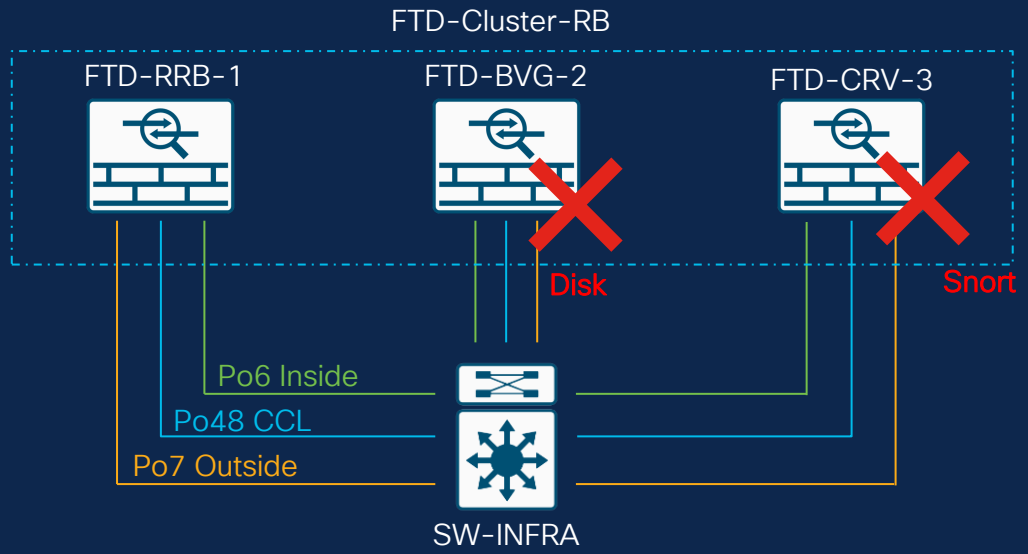
```
FTD-Cluster-RRB-1# show cluster info health
Member ID to name mapping:
  0 - unit-1-1(myself)    1 - unit-2-1    2 - unit-3-1

                          0         1         2
Ethernet1/1               up        up        up
Port-channel48            up        up        up
Port-channel6             up        up        up
Port-channel7             up        up        up

Unit overall              healthy   healthy   healthy
Service health status:
                          0         1         2
diskstatus   (monitor on) up        down        up
snort        (monitor on) up        up        down
Cluster overall           healthy
```

Data interfaces and CCL healthy

Issues reported on disk unit-2 and snort unit-3



Ticket #4 – Snort Troubleshooting

Snort3 crash detected

```
root@FTD-Cluster-CRV-3:/home/admin# less /ngfw/var/log/messages
Dec  8 19:40:09 FTD-Cluster-CRV-3 SF-IMS[14435]: [14435] pm:process [INFO] Calling crash command
'/ngfw/usr/local/sf/bin/snort3-save-crashinfo.py' for process 'b5aa1e6e-9083-11ee-8acd-b047ae363bfc'.
Dec  8 19:40:09 FTD-Cluster-CRV-3 SF-IMS[14572]: [14687] ndclientd:ndclientd [WARN] [snort]: NDCSnortFailedPM: Received Invalid
Snort PID:0
Dec  8 19:40:09 FTD-Cluster-CRV-3 SF-IMS[14572]: [14687] ndclientd:ndclientd [WARN] [snort] Received a signal of snort failure
from PM
Dec  8 19:40:09 FTD-Cluster-CRV-3 SF-IMS[14572]: [14687] ndclientd:ndclientd [WARN] [snort] Critical process failures have
exceeded the threshold!
Dec  8 19:40:09 FTD-Cluster-CRV-3 SF-IMS[14572]: [14668] ndclientd:ndclientd [WARN] [snort] Service has failed, stopping
Notification Daemon heartbeats.
Dec  8 19:40:09 FTD-Cluster-CRV-3 SF-IMS[14572]: [14668] ndclientd:ndclientd [WARN] [snort] sending version [2] HB stop message
Dec  8 19:40:09 FTD-Cluster-CRV-3 Notification Daemon[14571]: Notification Daemon: NGFW-1.0-snort-1.0--->OFFLINE
Dec  8 19:40:09 FTD-Cluster-CRV-3 Notification Daemon[14571]: Notification Daemon: Sending a Status Down for NGFW-1.0-snort-1.0
with failure reason More than 50 percent of snort instances are down

Dec  8 19:48:34 FTD-Cluster-CRV-3 Notification Daemon[14571]: Notification Daemon: Sending UP Status Update NGFW-1.0-snort-1.0
Dec  8 19:48:34 FTD-Cluster-CRV-3 Notification Daemon[14571]: Service Up: Last Heartbeat received at Fri Dec  8 19:48:34 2023

root@FTD-Cluster-CRV-3:/home/admin# pmtool status | grep " - " | grep -i "snort"
b5aa1e6e-9083-11ee-8acd-b047ae363bfc (de,snort) - Running 105788
```

After ~8 mins the process is reported up

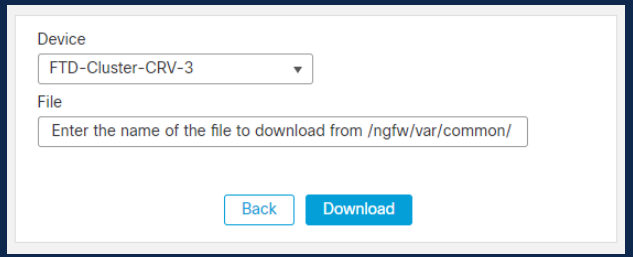
Ticket #4 – Snort Troubleshooting

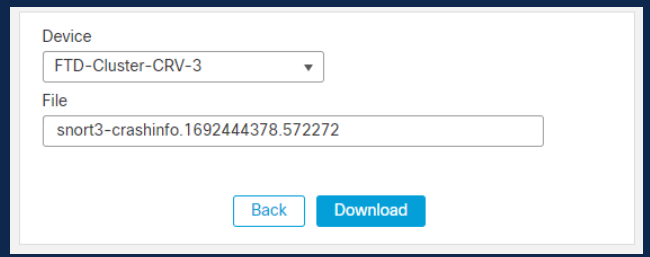
```
root@FTD-Cluster-CRV-3:/home/admin# ls -l /ngfw/var/log/crashinfo/
-rw-r--r-- 1 root root 1037 Dec 08 19:40 snort3-crashinfo.1692444378.572272
```

Provide TAC for analysis

Champ Tip 12 – Snort cores/crash files can be found in the following locations:
Snort 2 – /ngfw/var/data/cores/ or /ngfw/var/common/
Snort 3 – /ngfw/var/log/crashinfo/ – /ngfw/var/data/cores/ – /ngfw/var/common/

Champ Tip 13 –
1. Copy crash/core files to /ngfw/var/common/ folder on expert mode.
2. Access FMC via HTTPS and go under **System > Health > Monitor**.
3. Select FTD where the Core Files were generated **Advanced Troubleshooting > View System & Troubleshooting details > File Download**:





Ticket #4 – Disk Troubleshooting

LINA

```
FTD-Cluster-RRB-1# show cluster history

16:24:09 CET Dec 8 2023
MASTER                MASTER              Event: Asking slave unit unit-2-1
                                          to quit due to diskstatus
                                          Application health check
                                          failure, and slave's application
                                          state is down
```

Unit was kicked due to disk check failure. This happens when /ngfw disk usage is over 94%

EXPERT

```
admin@FTD-Cluster-BVG-2:~$ df -ha
Filesystem      Size  Used Avail Use% Mounted on
rootfs           81G   76G  4.6G  95% /
proc              0     0     0    - /proc
sysfs             0     0     0    - /sys
devtmpfs         81G  1.9G   79G   3% /dev
tmpfs            94G  1.9M   94G   1% /run
tmpfs            94G  2.1M   94G   1% /var/volatile
devpts            0     0     0    - /dev/pts
/dev/sda1       1.5G  156M  1.4G  11% /mnt/boot
/dev/sda2       977M  1.1M  925M   1% /opt/cisco/config
/dev/sda3       4.6G  115M  4.3G   3% /opt/cisco/platform/logs
/dev/sda5        49G  284K   47G   1% /var/data/cores
/dev/sda6       688G  189G  500G  28% /opt/cisco/csp
/dev/sda6       191G  184G  7.1G  97% /ngfw
```

/ngfw showing 97% disk utilization

Ticket #4 – Disk Troubleshooting

```
root@FTD-Cluster-BVG-2:/ngfw# find /ngfw -type f -exec du -Sh {} + | sort -rh | head -n 15
find: File system loop detected; '/ngfw/Volume/root1/ngfw' is part of the same file system loop as '/ngfw'.
171G    /ngfw/badfile
8.8G    /ngfw/Volume/.swaptwo
531M    /ngfw/var/sf/cloud_download/cisco_uridb_large_1705310873
531M    /ngfw/usr/local/sf/cloud_download/cisco_uridb_large_1705310873
```

Champ Tip 14 – Disk Utilization have three commons issues:

1. Large files.
2. Addition of many small files.
3. Issues with log rotation or space not being freed due to a process keeping files open.

Champ Tip 15 – Increase available disk space by deleting the following: old backup files, troubleshoot files under /ngfw/var/common/. Don't delete files/folders if not completely sure.

Useful commands:
df -ha > expert
find /ngfw -type f -exec du -Sh {} + | sort -rh | head -n 15 > expert
lsof | grep deleted > expert

Ticket #4 – Summary

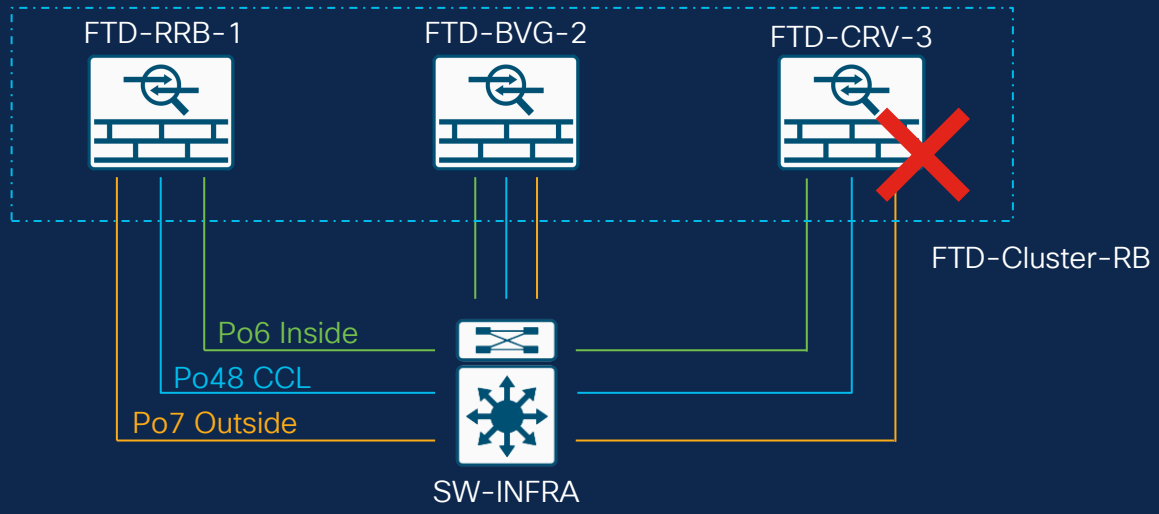
- Two Data units were kicked out from cluster (unit 2 & 3).
- No recent changes were performed.
- After investigating configuration was OK on cluster units, however Control unit reported:
  - Unit-2-1: Application Health Check Failure due to disk.
  - Unit-3-1: Application Health Check Failure due to snort.
- Big file filling disk was removed for unit 2.
- Snort Crash was identified and provided to TAC for review.

Ticket Report #5

Ticket #5 – Unit Replacement Report

Customer Symptom:

- One of the cluster units had a hardware failure and was replaced.
- Replacement unit is not able to join the cluster.



Ticket #5 – FMC Checks

Unit 3-1 replacement unable to join cluster

Ticket #5 – Troubleshooting MTU

```
Cluster disable is performing cleanup..done.
All data interfaces have been shutdown due to clustering being disabled. To recover either enable clustering or remove
cluster group configuration.

WARNING: Unit unit-3-1 is not reachable in CCL jumbo frame ICMP test, please check cluster interface and switch MTU
configuration
WARNING: Unit unit-3-1 is not reachable in CCL jumbo frame ICMP test, please check cluster interface and switch MTU
configuration
```

```
FTD-Cluster-RRB-1# show cluster history
20:49:57 CET Dec 21 2023
MASTER                MASTER                Event: Cluster unit unit-3-1 state
                                            is SLAVE_COLD

20:49:57 CET Dec 21 2023
MASTER                MASTER                Event: Cluster unit unit-3-1 state
                                            is SLAVE_APP_SYNC

20:49:59 CET Dec 21 2023
MASTER                MASTER                Event: Cluster new slave enrollment
                                            is on hold for app 1 for
                                            1800 s

20:50:07 CET Dec 21 2023
MASTER                MASTER                Event: CCL MTU test to unit unit-3-1
                                            failed
```

CCL jumbo frame ICMP - MTU test failing.

Ticket #5 – Troubleshooting MTU

```
FTD-Cluster-RRB-1# ping 10.99.2.1 size 1600
Type escape sequence to abort.
Sending 5, 1600-byte ICMP Echos to 10.99.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

Ping test to unit 2-1 working

```
FTD-Cluster-RRB-1# ping 10.99.3.1 size 1600
Type escape sequence to abort.
Sending 5, 1600-byte ICMP Echos to 10.99.3.1, timeout is 2 seconds:
?????
Success rate is 0 percent (0/5)
```

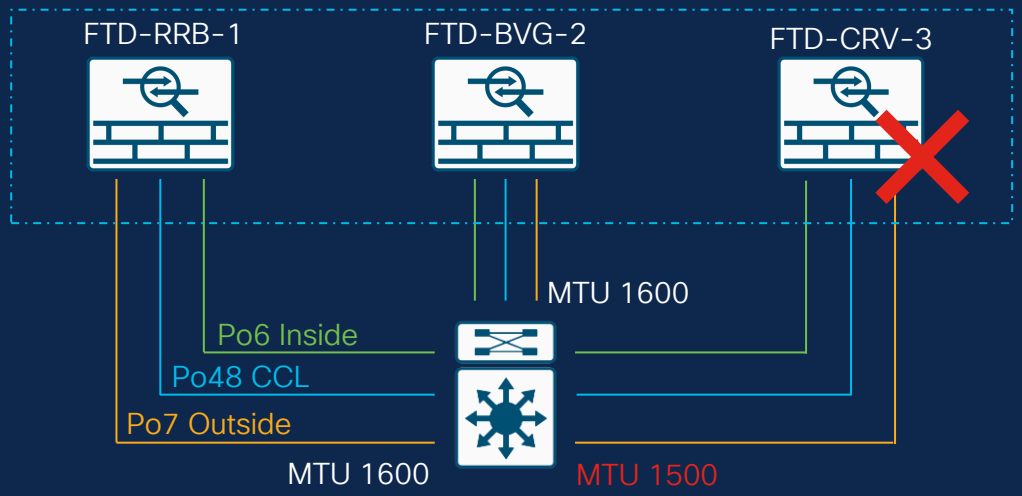
Ping test to unit 3-1 not-working

Cluster exec used to check CCL MTU

```
FTD-Cluster-RRB-1# cluster exec show interface detail
unit-1-1(LOCAL):*******************************************************
Interface Port-channel48 "cluster", is up, line protocol is up
  Hardware is EtherSVI, BW 1000 Mbps, DLY 10 usec
        Description: Clustering Interface
        MAC address 0015.c500.018f, MTU 1600
        IP address 10.99.1.1, subnet mask 255.255.0.0
unit-2-1:*******************************************************
Interface Port-channel48 "cluster", is up, line protocol is up
  Hardware is EtherSVI, BW 1000 Mbps, DLY 10 usec
        Description: Clustering Interface
        MAC address 0015.c500.028f, MTU 1600
        IP address 10.99.2.1, subnet mask 255.255.0.0
FTD-Cluster-CRV-3# show int detail
Interface Port-channel48 "cluster", is up, line protocol is up
  Hardware is EtherSVI, BW 1000 Mbps, DLY 10 usec
        Description: Clustering Interface
        MAC address 0015.c500.038f, MTU 1600
        IP address 10.99.3.1, subnet mask 255.255.0.0
```

Ticket #5 – Troubleshooting MTU

```
GIANT-SNORTY-CORE1#show int po41
Port-channel41 is up, line protocol is up (connected)
  Hardware is EtherChannel, address is 0021.a03d.e666 (bia
0021.a03d.e666)
  MTU 1600 bytes, BW 2000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 1000Mb/s, media type is unknown
GIANT-SNORTY-CORE1#show int po43
Port-channel43 is up, line protocol is up (connected)
  Hardware is EtherChannel, address is 0021.a03d.e660 (bia
0021.a03d.e660)
  MTU 1600 bytes, BW 2000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 1000Mb/s, media type is unknown
GIANT-SNORTY-CORE1#show int po45
Port-channel45 is up, line protocol is up (connected)
  Hardware is EtherChannel, address is 0021.a03d.e648 (bia
0021.a03d.e648)
  MTU 1500 bytes, BW 2000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 1000Mb/s, media type is unknown
```



Champ Tip 16 – MTU on CCL must always match between the switch and FTD. CCL MTU needs to be 100+ bytes more than data interfaces MTU.

Ticket #5 – Summary

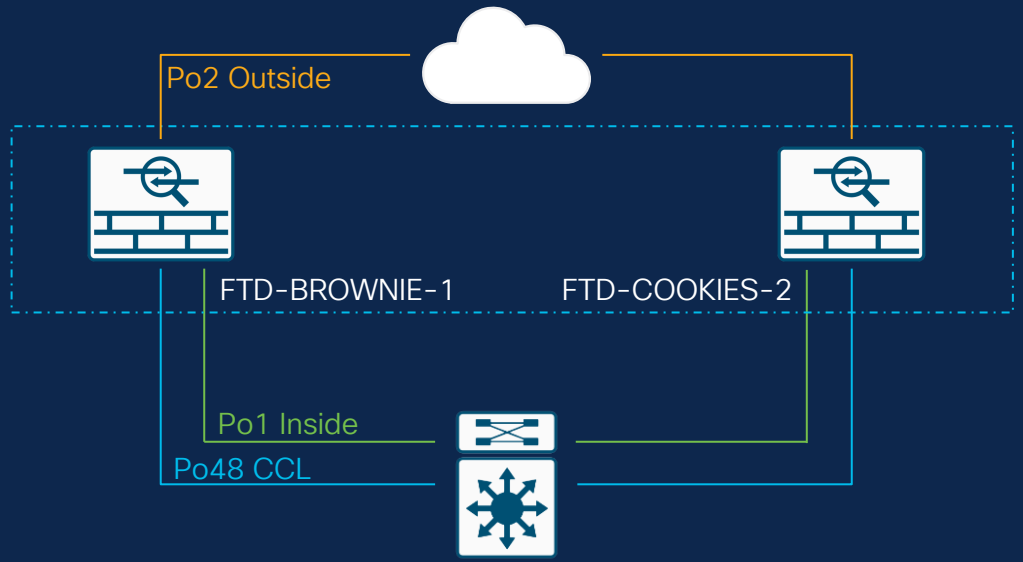
- After replacement, unit 3-1 was unable to join the cluster.
- After investigating configuration was OK on cluster units, however Control Unit reported:
  - Unit-3-1: CCL MTU test failed.
- Misconfigured MTU was identified on switch side.
- After setting right value unit 3-1 device was able to join the cluster and FMC.

Ticket Report #6

Ticket #6 – PAT/Internet Access Report

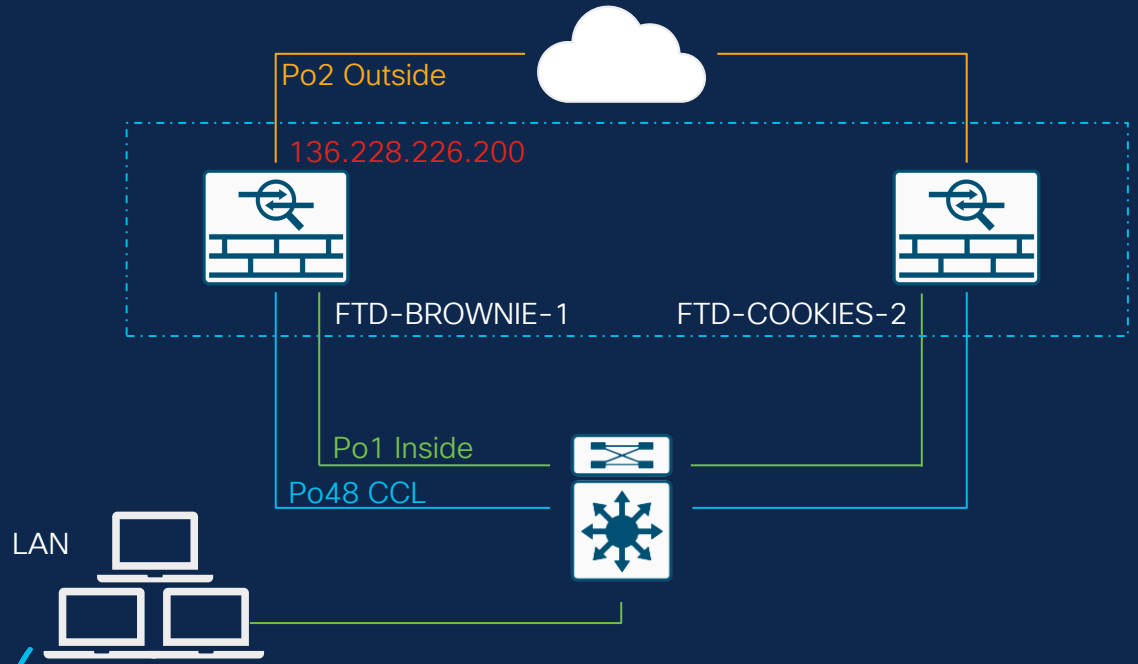
Customer Symptom:

- Giant Snorty company recently acquired Tiny Snort company which have a two-unit cluster.
- Devices are running 6.6 version and connectivity issues to internet have been reported with and without PAT pool configured.



Ticket #6 – Without PAT Pool

- Public IP is assigned to Control Unit. None available for Data Unit.
- Traffic received by Data Unit to the internet is forwarded through CCL to Control Unit which can cause overhead or CCL congestion.



Ticket #6 – Without PAT Pool

```
FTD-BROWNIE-1# show nat pool cluster
IP Outside:Giant-Snorty-PATPool 136.228.226.200, owner unit-1-1, backup unit-2-1
```

Information about PAT pool owner/backup

```
FTD-BROWNIE-1# show xlate
TCP PAT from Inside:172.16.100.30/31733 to Outside:136.228.226.200/31733 flags ri idle 0:00:07 timeout 0:00:30
TCP PAT from Inside:172.16.100.31/35883 to Outside:136.228.226.200/35883 flags ri idle 0:00:04 timeout 0:00:30
```

Use show xlate command to check translations

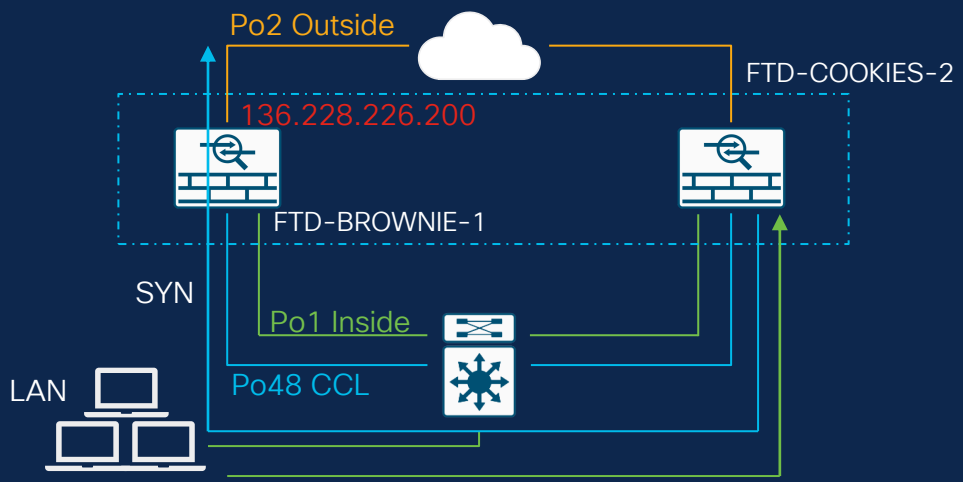
```
FTD-BROWNIE-1#
Phase: 4
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Additional Information:
Input interface: 'Inside'
Flow type: NO FLOW
I (0) got initial, attempting ownership.
Phase: 5
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Additional Information:
Input interface: 'Inside'
Flow type: NO FLOW
I (0) am becoming owner
```

Control Unit capture trace shows unit becoming connection Owner

Ticket #6 – Without PAT Pool

```
FTD-COOKIES-2#
Phase: 4
Type: CLUSTER-EVENT
Result: ALLOW
Additional Information:
Input interface: 'Inside'
Flow type: NO FLOW
I (1) got initial, attempting ownership.
.
Phase: 5
Type: CLUSTER-EVENT
Result: ALLOW
Additional Information:
Input interface: 'Inside'
Flow type: NO FLOW
I (1) am becoming owner
.
Phase: 10
Type: CLUSTER-EVENT
Result: ALLOW
Config:
Additional Information:
Input interface: 'Inside'
Flow type: NO FLOW
NAT: I (1) am redirecting packet to
master (0) for PAT.
```

Champ Tip 17 – PAT pool size must be always equal or bigger that the number of cluster units.



Data Unit capture trace shows unit attempting connection ownership, but redirects to control unit

Ticket #6 - With PAT Pool

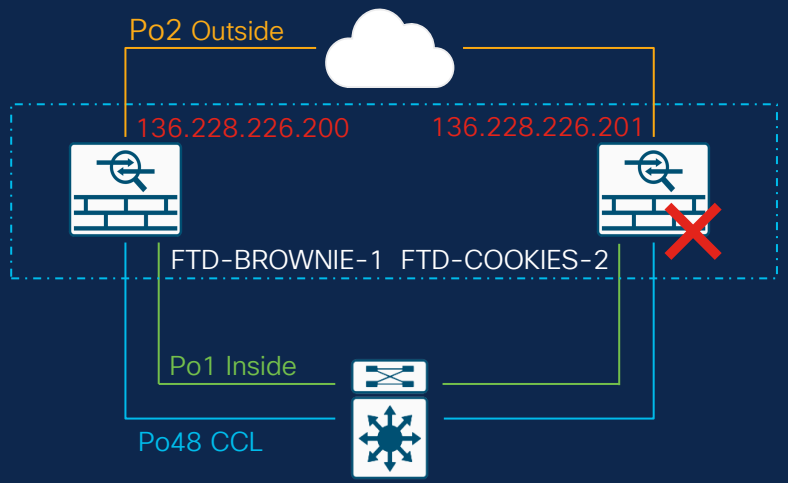
```
FTD-BROWNIE-1# show nat pool cluster
IP Outside:Giant-Snorty-PATPool 136.228.226.200, owner unit-1-1, backup unit-2-1
IP Outside:Giant-Snorty-PATPool 136.228.226.201, owner unit-2-1, backup unit-1-1
```

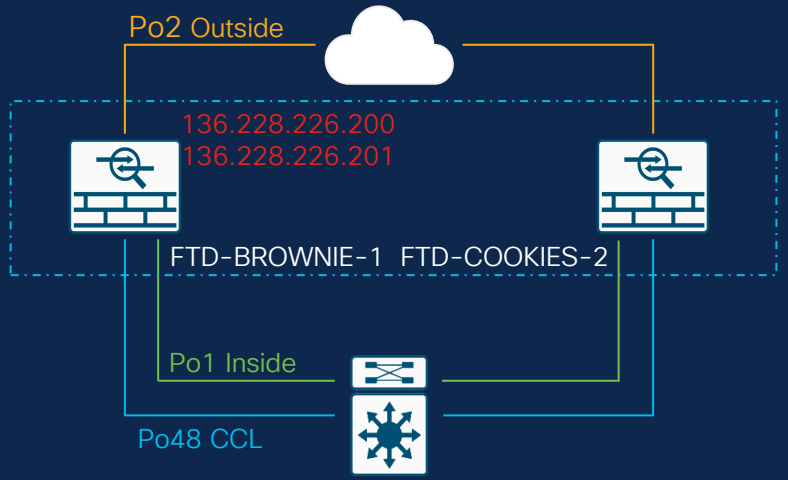
```
FTD-BROWNIE-1# show nat pool cluster
IP Outside:Giant-Snorty-PATPool 136.228.226.200, owner unit-1-1, backup unit-2-1
IP Outside:Giant-Snorty-PATPool 136.228.226.201, owner unit-1-1, backup unit-2-1
```

Balanced PAT allocation on units

Allocation become imbalanced, even when Data unit is back online

Workaround: Add more IP's to PAT pool or clear xlates for one IP.





FTD Clustering PAT Improvements (6.7+)

- IP's are not distributed entirely to a single cluster member.
- PAT IP's split in port blocks and evenly distributed on members.
- IP stickiness is also used.

```
object network Giant-Snorty-PATPool
 range 136.228.226.2 136.228.226.4
```

```
nat (Inside,Outside) after-auto source dynamic Giant-Snorty-LAN pat-pool
Giant-Snorty-PATPool
```

```
FTD-Cluster-RRB-1# show nat pool cluster summary
port-blocks count display order: total, unit-1-1, unit-2-1, unit-3-1
Codes: ^ - reserve, # - reclaimable
IP Outside:Giant-Snorty-PATPool 136.228.226.2 (126 - 32 / 31 / 32) ^ 31 # 0
IP Outside:Giant-Snorty-PATPool 136.228.226.3 (126 - 32 / 31 / 32) ^ 31 # 0
IP Outside:Giant-Snorty-PATPool 136.228.226.4 (126 - 32 / 31 / 32) ^ 31 # 0
```

Reserved port block

Available ports per IP
64512

Total port blocks per IP
64512/512 = 126

FTD Clustering PAT Improvements

```
FTD-Cluster-RRB-1# show nat pool cluster
IP Outside:Giant-Snorty-PATPool 136.228.226.2
          [1024-1535], owner unit-1-1, backup unit-2-1
          [1536-2047], owner unit-1-1, backup unit-2-1
          [2048-2559], owner unit-1-1, backup unit-2-1
          [2560-3071], owner unit-1-1, backup unit-2-1
          [3072-3583], owner unit-1-1, backup unit-2-1
        [17920-18431], owner unit-2-1, backup unit-3-1
        [18432-18943], owner unit-2-1, backup unit-3-1
        [18944-19455], owner unit-2-1, backup unit-3-1
        [19456-19967], owner unit-2-1, backup unit-3-1
        [19968-20479], owner unit-2-1, backup unit-3-1
        [20480-20991], owner unit-2-1, backup unit-3-1
        [33280-33791], owner unit-3-1, backup unit-1-1
        [33792-34303], owner unit-3-1, backup unit-1-1
        [34304-34815], owner unit-3-1, backup unit-1-1
        [34816-35327], owner unit-3-1, backup unit-1-1
        [35328-35839], owner unit-3-1, backup unit-1-1
        [35840-36351], owner unit-3-1, backup unit-1-1
        [36352-36863], owner unit-3-1, backup unit-1-1
        [36864-37375], owner unit-3-1, backup unit-1-1
        [49664-50175], owner <RESERVED>, backup <RESERVED>
        [50176-50687], owner <RESERVED>, backup <RESERVED>
        [50688-51199], owner <RESERVED>, backup <RESERVED>
        [51200-51711], owner <RESERVED>, backup <RESERVED>
        [51712-52223], owner <RESERVED>, backup <RESERVED>
```

Blocks with Owner 1-1 Backup 2-1

Blocks with Owner 2-1 Backup 3-1

Blocks with Owner 3-1 Backup 1-1

Reserved Blocks

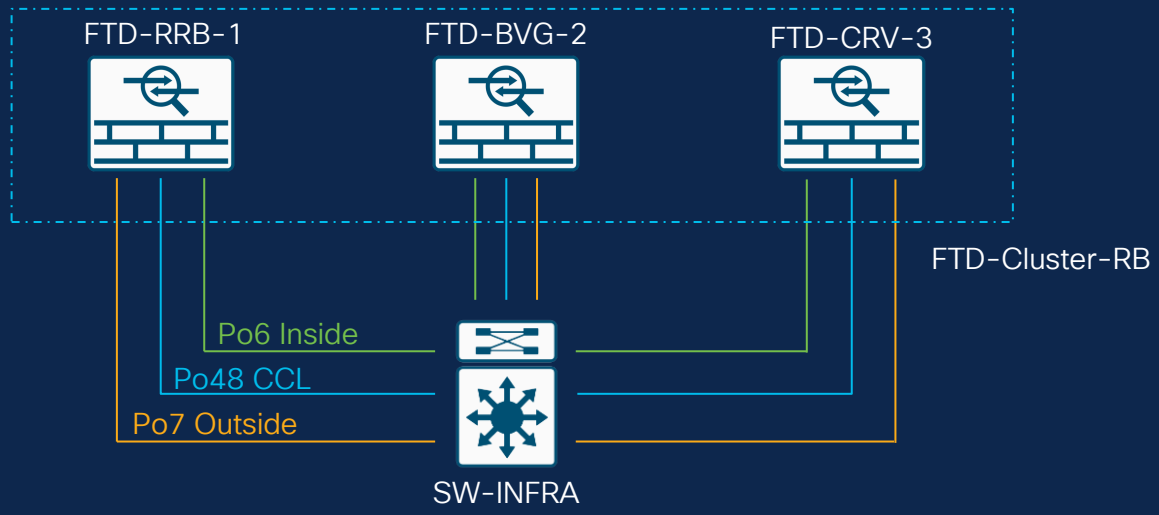
Ticket #6 – Summary

- Issues were seen in connectivity to the internet when using single IP address for PAT or with PAT pool when one unit was rebooted/kicked out from cluster.
- Devices are running FTD 6.6 version.
- Solution was to add additional IP addresses to the PAT pool or clear xlates for one IP after imbalance is detected.
- Version 6.7+ offers re-design for PAT-related limitations.

Ticket Report #7

Ticket #7 – Data Plane Issues Report

- Customer Symptom:
  - Sometimes there are connectivity issues for certain traffic through the cluster.
  - Need some guidance on how to troubleshoot such scenarios.



Ticket #7 – Data Plane Troubleshoot

Champ Tip 18

- Collect as much details as possible about flow(s) affected.
- Identify 5-Tuple (Source/Destination IP/Port + Protocol).
- Identify interfaces and units involved in traffic forwarding.

Source IP – 172.18.201.99
Destination IP – 18.239.18.70
Source Port - X
Destination Port - 443
Protocol - TCP
Ingress Interface - Inside
Egress Interface - Outside
Units Involved – Unit 1-1 & 2-1

Ticket #7 – Packet Captures

```
FTD-Cluster-RRB-1# cluster exec show capture
unit-1-1(LOCAL):***************


unit-2-1:**********************


unit-3-1:**********************
```

Champ Tip 19 – Enable captures on all cluster units using **cluster exec** commands.

```
FTD-Cluster-RRB-1# cluster exec capture IN buffer 33554432 interface Inside match tcp host 172.18.201.99 host
18.239.18.70 eq 443
FTD-Cluster-RRB-1# cluster exec show capture
unit-1-1(LOCAL):******************************************************
capture IN type raw-data buffer 33554432 interface Inside [Capturing - 1260 bytes]
  match tcp host 172.18.201.99 host 18.239.18.70 eq https


unit-2-1:******************************************************
capture IN type raw-data buffer 33554432 interface Inside [Capturing - 0 bytes]
  match tcp host 172.18.201.99 host 18.239.18.70 eq https


unit-3-1:******************************************************
capture IN type raw-data buffer 33554432 interface Inside [Capturing - 0 bytes]
  match tcp host 172.18.201.99 host 18.239.18.70 eq https
FTD-Cluster-RRB-1#
```

Ticket #7 - Packet Captures

```
FTD-Cluster-RRB-1# cluster exec show capture IN
unit-1-1(LOCAL):*******************************************************
10 packets captured

1: 10:23:12.879226 802.1Q vlan#201 P0 172.18.201.99.31349 > 18.239.18.70.443: S 2225395909:2225395909(0) win 29200 <mss
1460,sackOK,timestamp 1110209649 0,nop,wscale 7>
2: 10:23:12.880401 802.1Q vlan#201 P0 18.239.18.70.443 > 172.18.201.99.31349: S 719653963:719653963(0) ack 2225395910 win
28960 <mss 1380,sackOK,timestamp 1120565119 1110209649,nop,wscale 7>
3: 10:23:12.880691 802.1Q vlan#201 P0 172.18.201.99.31349 > 18.239.18.70.443: . ack 719653964 win 229 <nop,nop,timestamp
1110209650 1120565119>
4: 10:23:12.880783 802.1Q vlan#201 P0 172.18.201.99.31349 > 18.239.18.70.443: P 2225395910:2225396054(144) ack 719653964
win 229 <nop,nop,timestamp 1110209650 1120565119>

unit-2-1:*********************************************************
0 packet captured
0 packet shown

unit-3-1:*********************************************************
0 packet captured
0 packet shown
```

Traffic is only seen on Control unit 1-1

Ticket #7 – Packet Captures Options

Champ Tip 20 – Trace option allows to see how the unit handle ingress traffic, by default only the first ingress 50 packets are traced but it can be configured up to 1000.

```
FTD-Cluster-RRB-1# cluster exec capture OUT interface Outside buffer 33554432 trace trace-count 1000 match tcp host
136.228.226.2 host 18.239.18.70 eq 443

FTD-Cluster-RRB-1# cluster exec show capture OUT
unit-1-1(LOCAL):*******************************************************
1: 09:28:12.117700 802.1Q vlan#202 P0 136.228.226.2.31349 > 18.239.18.70.443: S 441626016:441626016(0) win 29200 <mss
1380,sackOK,timestamp 1115330849 0,nop,wscale 7>
2: 09:28:12.118341 802.1Q vlan#202 P0 18.239.18.70.443 > 136.228.226.2.31349: S 301658077:301658077(0) ack 441626017 win
28960 <mss 1460,sackOK,timestamp 1125686319 1115330849,nop,wscale 7>

unit-2-1:*******************************************************

unit-3-1:*******************************************************
1: 09:28:12.111429 802.1Q vlan#202 P0 18.239.18.70.443 > 136.228.226.2.31349: S 301658077:301658077(0) ack 441626017 win
28960 <mss 1460,sackOK,timestamp 1125686319 1115330849,nop,wscale 7>
```

Champ Tip 21 – Same packet can have different numbers on different units. Check timestamps to understand packet flow.

Ticket #7 – Packet Captures Trace Option

```
FTD-Cluster-RRB-1# cluster exec show cap OUT packet-number 2 trace
unit-1-1(LOCAL):*******************************************************

2: 09:28:12.118341 802.1Q vlan#202 P0 18.239.18.70.443 > 136.228.226.2.31349: S 301658077:301658077(0) ack 441626017 win
28960 <mss 1460,sackOK,timestamp 1125686319 1115330849,nop,wscale 7>
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

FTD-Cluster-RRB-1# cluster exec unit unit-3-1 show cap OUT packet-number 1 trace

1: 09:28:12.111429 802.1Q vlan#202 P0 18.239.18.70.443 > 136.228.226.2.31349: S 301658077:301658077(0) ack 441626017 win
28960 <mss 1460,sackOK,timestamp 1125686319 1115330849,nop,wscale 7>
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list
```

Ticket #7 – CCL/ASP Packet Captures

```
FTD-Cluster-RRB-1# cluster exec capture CCLCAP interface cluster headers-only
unit-1-1(LOCAL):*********************************************************

unit-2-1:*********************************************************

unit-3-1:*********************************************************
```

Configure CCL captures on all units.

Champ Tip 22 – Data interface captures shows all packets by default (Ones that reach the interface from the network + Reinjected packets from CCL.

Use reinject-hide option to not see reinjected packets. (Useful to verify asymmetry). headers-only option is useful when packet payload is of no interest.

In addition, asp-drop captures are useful to check if certain flow has software drops.

```
FTD-Cluster-RRB-1# cluster exec cap ASPDROP type asp-drop all buffer 33554432
unit-1-1(LOCAL):*********************************************************

unit-2-1:*********************************************************

unit-3-1:*********************************************************
```

Configure ASP drop captures on all units.

Ticket #7 – ASP Packet Captures

- Can be used to check main reasons behind flows or packets drops.
- Troubleshooting approach goes as follows:

1. Clear ASP drop counters → 2. Run ASP drop few times to identify high counter → 3. Configure drop-specific captures

```
FTD-Cluster-RRB-1# show asp drop

Frame drop:
  Flow is being freed (flow-being-freed)                  21
  Unexpected packet (unexpected-packet)                   13
  No route to host (no-route)                        1045842
  Reverse-path verify failed (rpf-violated)           625454
  Flow is denied by configured rule (acl-drop)       1491856
  First TCP packet not SYN (tcp-not-syn)               15005
  TCP failed 3 way handshake (tcp-3whs-failed)           112
FP L2 rule drop (l2_acl)                             974637
  Interface is down (interface-down)                      8
  Dispatch queue tail drops (dispatch-queue-limit)      231

Last clearing: Never
Flow drop:
Last clearing: Never
```

Drop reasons + Counters

```
FTD-Cluster-RRB-1 # cap ASP type asp-drop no-route
FTD-Cluster-RRB-1 # show cap ASP

2 packets captured

   1: 14:41:05.029325       172.18.100.100.33448 > 172.19.220.100.53:
udp 39 Drop-reason: (no-route) No route to host, Drop-location: frame
0x000055d135ca7895 flow (NA)/NA
   2: 14:41:05.029386       172.18.100.100.33448 > 172.19.220.100.53:
udp 39 Drop-reason: (no-route) No route to host, Drop-location: frame
0x000055d135ca7895 flow (NA)/NA
2 packets shown
```

Capture with reason + Packets captured

Ticket #7 – Copying Packet Captures

```
FTD-Cluster-RRB-1# cluster exec copy /pcap capture:IN disk0:/IN.pcap
unit-1-1(LOCAL):*********************************************************
Source capture name [IN]?
Destination filename [IN.pcap]?
!
unit-2-1:*********************************************************
!
unit-3-1:*********************************************************
!
FTD-Cluster-RRB-1# cluster exec dir
unit-1-1(LOCAL):*********************************************************
Directory of disk0:/
536878169  -rwx  24           13:00:41 Jan 04 2024  IN.pcap

204800524288 bytes total (189498900480 bytes free/92% free)

unit-2-1:*********************************************************
Directory of disk0:/
536898414  -rwx  24           13:00:41 Jan 04 2024  IN.pcap

204800524288 bytes total (189751681024 bytes free/92% free)

unit-3-1:*********************************************************
Directory of disk0:/
537408304  -rwx  24           13:00:29 Jan 04 2024  IN.pcap

204800524288 bytes total (190179241984 bytes free/92% free)
```

Copy contents of packet captures to disk0 of each unit. On expert are under /mnt/disk0/ folder

Besides Champ Tip 13, files can also be directly copied to external servers like TFTP.

IN.pcap can be seen on directory of each unit

Ticket #7 – Additional Commands Dataplane

```
FTD-Cluster-RRB-1# show logging
%FTD-6-747004: Clustering: State machine changed from state SLAVE_CONFIG to SLAVE_FILESYS
%FTD-6-747004: Clustering: State machine changed from state SLAVE_FILESYS to SLAVE_BULK_SYNC
%FTD-7-747005: Clustering: State machine notify event CLUSTER_EVENT_MEMBER_IFC_STATE
%FTD-7-747005: Clustering: State machine notify event CLUSTER_EVENT_MEMBER_IFC_STATE
%FTD-7-747005: Clustering: State machine notify event CLUSTER_EVENT_MEMBER_IFC_STATE
%FTD-7-747005: Clustering: State machine notify event CLUSTER_EVENT_MEMBER_IFC_STATE
```

Syslog

```
> system support trace
Enable firewall-engine-debug too? [n]: y
Please specify an IP protocol: tcp
Please specify a client IP address: 172.18.201.99
Please specify a client port:
Please specify a server IP address: 18.239.18.70
Please specify a server port: 443
Monitoring packet tracer and firewall debug messages
```

System support trace + firewall engine debug

Show xlate + Show conn

```
FTD-Cluster-RRB-1# show xlate
TCP PAT from Inside:172.18.201.99/37634 to Outside:136.228.226.2/37634 flags ri idle 0:00:04 timeout
0:00:30
FTD-Cluster-RRB-1# show conn
unit-1-1(LOCAL):**********************************************************
TCP Outside 18.239.18.70:443 Inside 172.18.201.99:37634, idle 0:00:00, bytes 487413076, flags UIO N1
unit-3-1:**********************************************************
TCP Outside 18.239.18.70:443 Inside 172.18.201.99:36634, idle 0:00:06, bytes 0, flags y
```

Ticket #7 – Summary

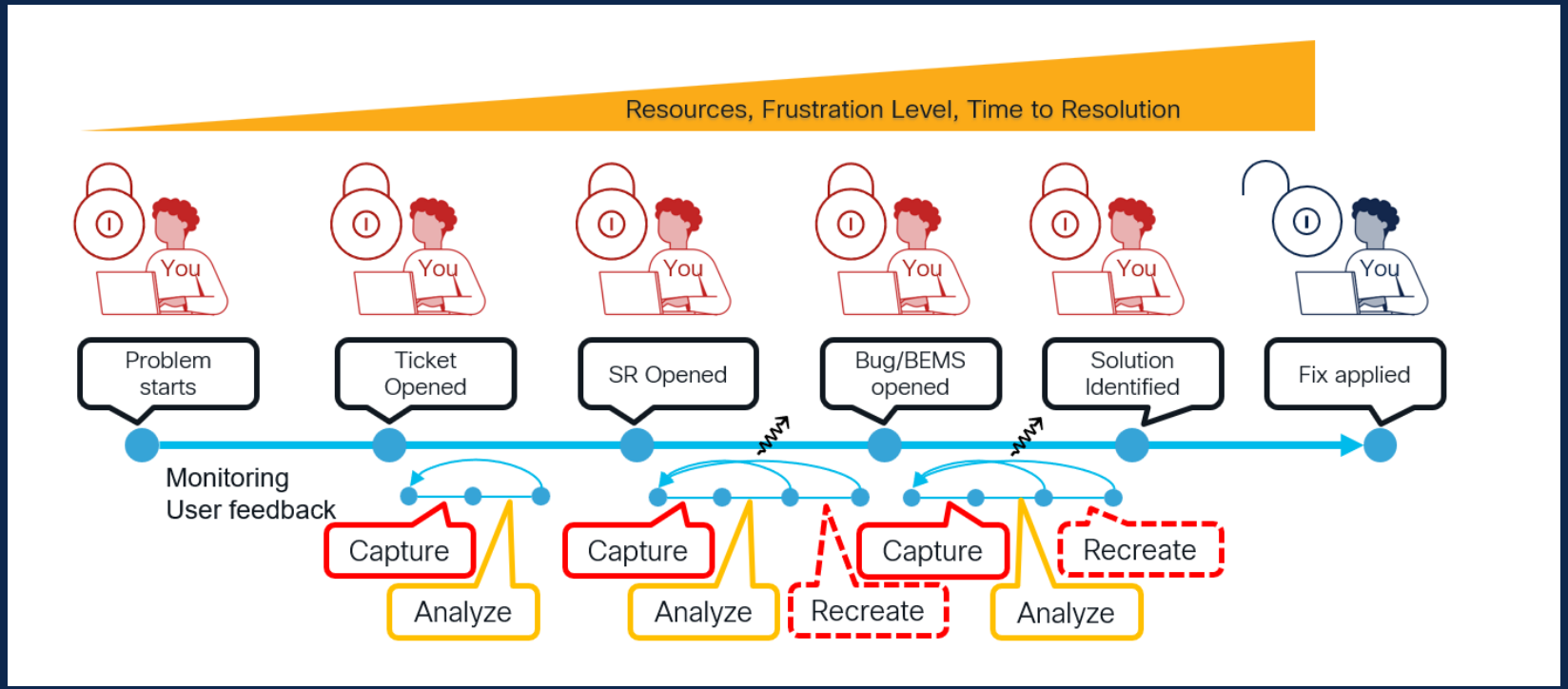
- When having data plane related issues, make sure to identify the traffic affected details.
- Using captures with trace and syslog can be extremely useful to understand traffic flow and detect missing packets.
- CCL/ASP packet captures, along with checking connections and xlates comes handy in troubleshooting process.

Champ Tip 23 – Packet captures can have impact on device performance. Once troubleshooting is completed, proceed to delete them.

Ticket Reports Complete

RADKit

The Churn in Issue Lifecycle



Remote Automation Development Kit (RADKit)

- RADKit is a Software Development Kit (SDK): a set of ready-to-use tools and Python modules allowing efficient and scalable interactions with local or remote equipment to eliminate 50% of total time spent in problem solving lifecycle.

Expedite your issue resolution when using it with Cisco TAC

Securely connect and interact with remote devices

Powerful and easy to use APIs for automations

Champ Cheat Sheet

Reference

LINA

show cluster info – Shows cluster information and roles.
show cluster history – Shows unit event history.
show cluster conn count – Shows overall and per-unit connections count.
show cluster xlate count – Shows overall and per-unit xlate count.
show cluster traffic – Shows overall and per-unit traffic statistics.
show cluster info trace – Shows additional details (debug) level of clustering.
show cluster resource usage – Shows overall and per-unit resource utilization.
show cluster cpu – Shows overall and per-unit cpu utilization.
show cluster memory – Shows overall and per-unit memory utilization.
show cluster info load-monitor – Shows general information about conns, buffer drops, memory and CPU.
show cluster info health – Shows general information about unit health (interfaces, disk, snort).
cluster exec capture <name> – To configure packet captures.
cluster exec show cap <name> – To check packet capture contents.
show cluster info conn-distribution – Shows information about connection distribution in cluster.
show cluster info packet-distribution – Show information about packet distribution in cluster.
show nat pool cluster summary – Shows PAT pool distribution.
show conn detail – Show details about connections.
show xlate detail – Show details about translations.
show asp drop – Check software drops

Champ Cheat Sheet

Reference

```
FXOS commands:
scope eth-uplink; scope fabric a; show port-channel
connect fxos
      show port-channel summary
      show lacp internal event-history interface ethernet <int>
      show port-channel database

Expert mode commands:
Disk
df -ha
ls -lah
find /ngfw -type f -exec du -Sh {} + | sort -rh | head -n 15
lsof | grep deleted

Snort Cores Location
Snort 2 -  /ngfw/var/data/cores/ or /ngfw/var/common/
Snort 3 -  /ngfw/var/log/crashinfo/ - /ngfw/var/data/cores/ - /ngfw/var/common/

FMC
Devices > Device Management > Cluster > General - To check cluster information and history from FMC.
Health > Monitor - Check cluster health and graphs.
```

Documentation

Configuration Guides:

https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/720/management-center-device-config-72.html

Clustering Troubleshooting Document:

https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/216745-troubleshoot-firepower-threat-defense-f.html

Radkit:

https://radkit.cisco.com/

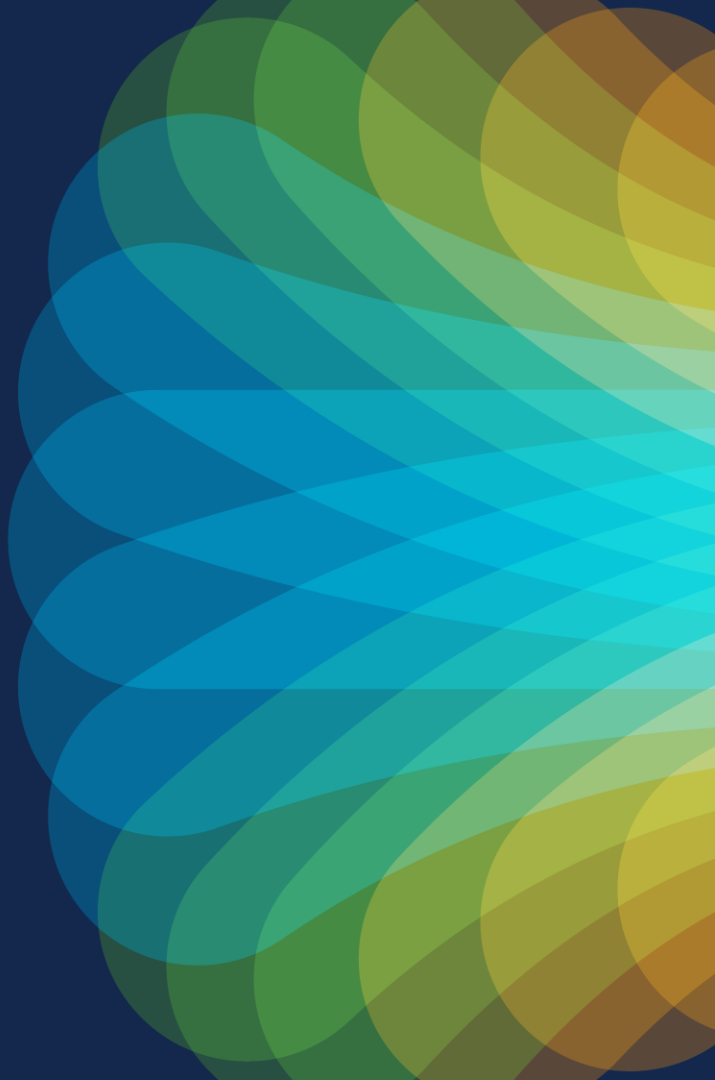
Compatibility Guide:

https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/compatibility/threat-defense-compatibility.html

FTD Syslog Messages:

https://www.cisco.com/c/en/us/td/docs/security/firepower/Syslogs/b_fptd_syslog_guide/about.html

Conclusion



Key Session Learnings

- Structured approach, Allies, Tools and Champ Tips can help to have a faster and more effective clustering troubleshooting.
- Monitor as much as possible with health monitoring.
- Make sure MTU is set properly.
  - Must be same on FTD and SW side.
  - For CCL MTU must be at least 100 bytes more than data interfaces.
- Take fast action when Split-Brain or kicked units is reported to avoid impact on the network or single device overload.
- There are hidden slides! – Additional theory, performance troubleshooting commands and Radkit, for offline review.

Continue your education

CTF booth at World of Solutions

Test your skills and earn Cisco CE Credits*

CTF is gamified Hands-On Cisco Technologies Labs!

* Ask at the booth for the qualifying missions

Continue your education

- Recommended Sessions
  - LABSEC-2550: Basic troubleshooting of data-path on Cisco Secure Firewall Threat Defense
  - LABSEC-2030: Cisco Secure Firewall Threat Defense Identity Based Firewall for VPN Remote Users – Configuration and Troubleshooting
  - BRKSEC-3533: Think Like a TAC Engineer: A guide to Cisco Secure Firewall most common pain points.


cisco
The bridge to possible
Thank you
cisco Live!


cisco Live!
Let's go