Risoluzione dei problemi relativi al cluster Firepower Threat Defense (FTD)

Sommario

Introduzione

In questo documento viene descritta la risoluzione dei problemi di installazione di un cluster in Firepower Next-Generation Firewall (NGFW).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti (per i collegamenti, vedere la sezione Informazioni correlate):

- Architettura della piattaforma Firepower
- Configurazione e funzionamento del cluster Firepower
- Familiarità con la CLI di FTD e Firepower eXtensible Operating System (FXOS)
- Registri NGFW/data plane
- NGFW/data plane packet-tracer
- Acquisizioni FXOS/data plane

Componenti usati

- HARDWARE: Firepower 4125
- Software: 6.7.0 (Build 65) - piano dati 9.15(1)

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

La maggior parte degli argomenti trattati in questo documento è applicabile anche alla risoluzione dei problemi dei cluster ASA (Adaptive Security Appliance).

Configurazione

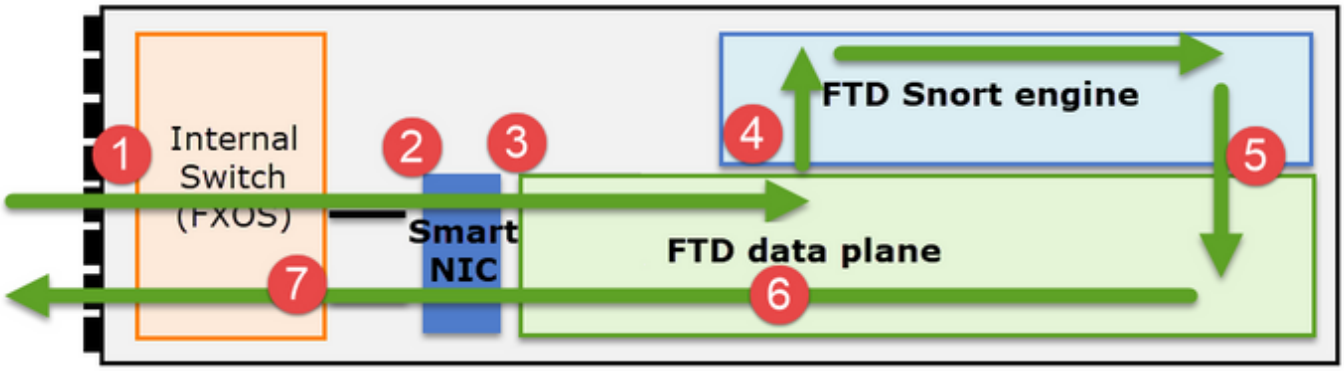
La parte relativa alla configurazione di una distribuzione cluster è illustrata nelle guide alla configurazione di FMC e FXOS:

- Clustering per Firepower Threat Defense
- Implementazione di un cluster per Firepower Threat Defense per la scalabilità e l'alta disponibilità

Nozioni di base sui cluster

Architettura NGFW

È importante comprendere in che modo Firepower serie 41xx o 93xx gestisce i pacchetti in transito:



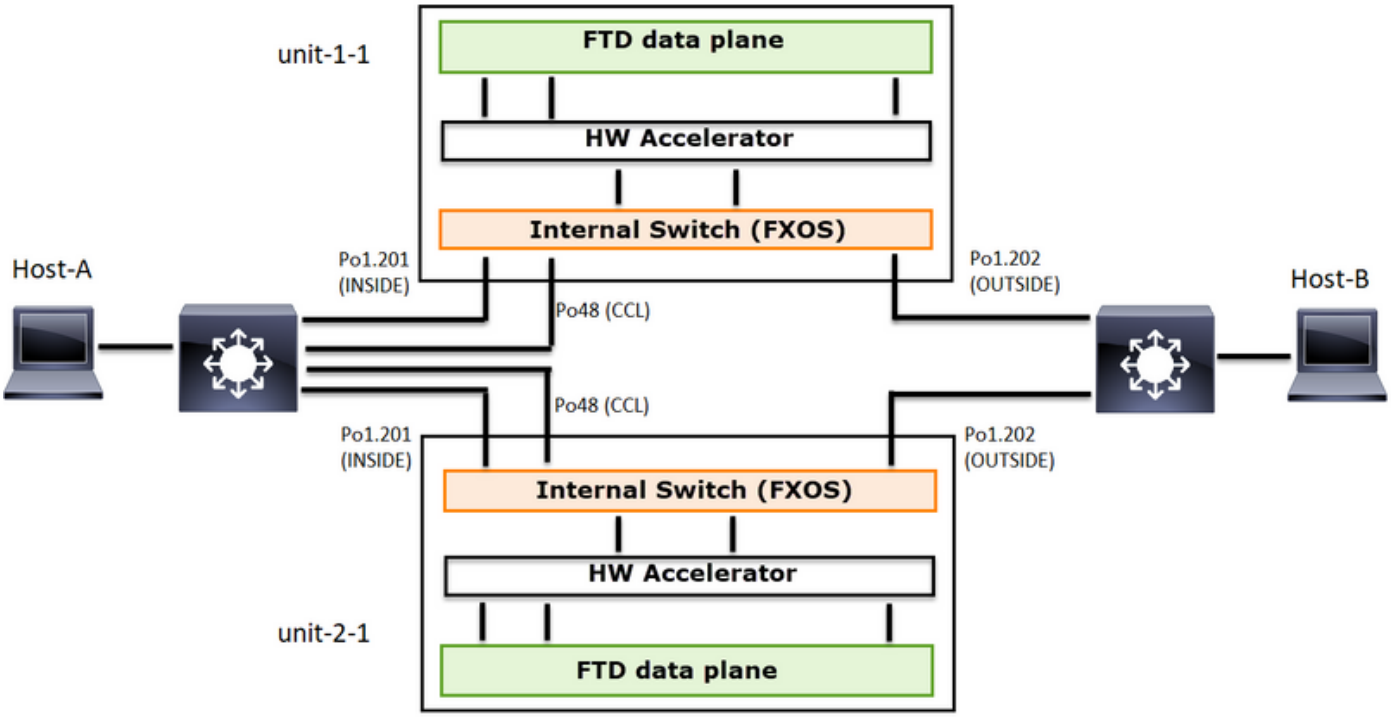
1. Un pacchetto entra nell'interfaccia in entrata e viene gestito dallo switch interno dello chassis.
2. Il pacchetto passa attraverso la Smart NIC. Se il flusso è scaricato (accelerazione hardware), il pacchetto viene gestito esclusivamente dalla Smart NIC e quindi inviato nuovamente alla rete.
3. Se il pacchetto non è scaricato, entra nel piano dati FTD che esegue principalmente i controlli L3/L4.
4. Se la politica lo richiede, il pacchetto viene ispezionato dal motore Snort (principalmente l'ispezione L7).
5. Il motore Snort restituisce un verdetto (ad esempio, allow o block) per il pacchetto.
6. Il data plane scarta o inoltra il pacchetto in base al verdetto di Snort.
7. Il pacchetto attraversa lo chassis attraverso lo switch interno dello chassis.

Acquisizioni cluster

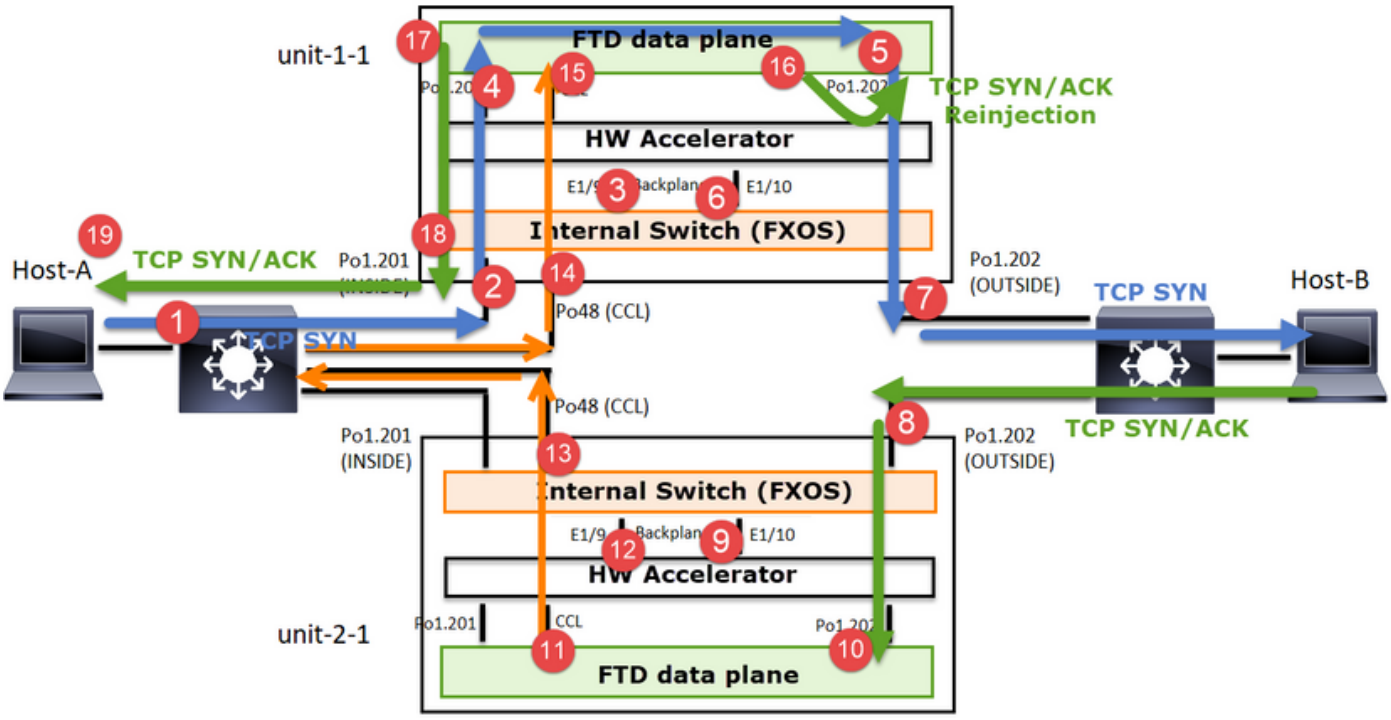
Le appliance Firepower forniscono più punti di acquisizione che forniscono visibilità sui flussi di transito. Quando si esegue la risoluzione dei problemi e si attivano le acquisizioni cluster, le principali problematiche sono:

- Il numero di acquisizioni aumenta con l'aumentare del numero di unità nel cluster.
- È necessario essere consapevoli del modo in cui il cluster gestisce un flusso specifico per poter tenere traccia del pacchetto attraverso il cluster.

Il diagramma mostra un cluster a 2 unità (ad esempio, FP941xx/FP9300):



In caso di connessione TCP asimmetrica stabilita, uno scambio SYN, SYN/ACK TCP ha il seguente aspetto:



Inoltra traffico

1. TCP SYN viene inviato dall'host A all'host B.
2. TCP SYN arriva sullo chassis (uno dei membri di Po1).
3. Il TCP SYN viene inviato al piano dati attraverso una delle interfacce backplane dello chassis (ad esempio, E1/9, E1/10, ecc.).
4. TCP SYN arriva sull'interfaccia in entrata del piano dati (Po1.201/INSIDE). In questo esempio, l'unità 1-1 assume la proprietà del flusso, esegue la randomizzazione ISN (Initial

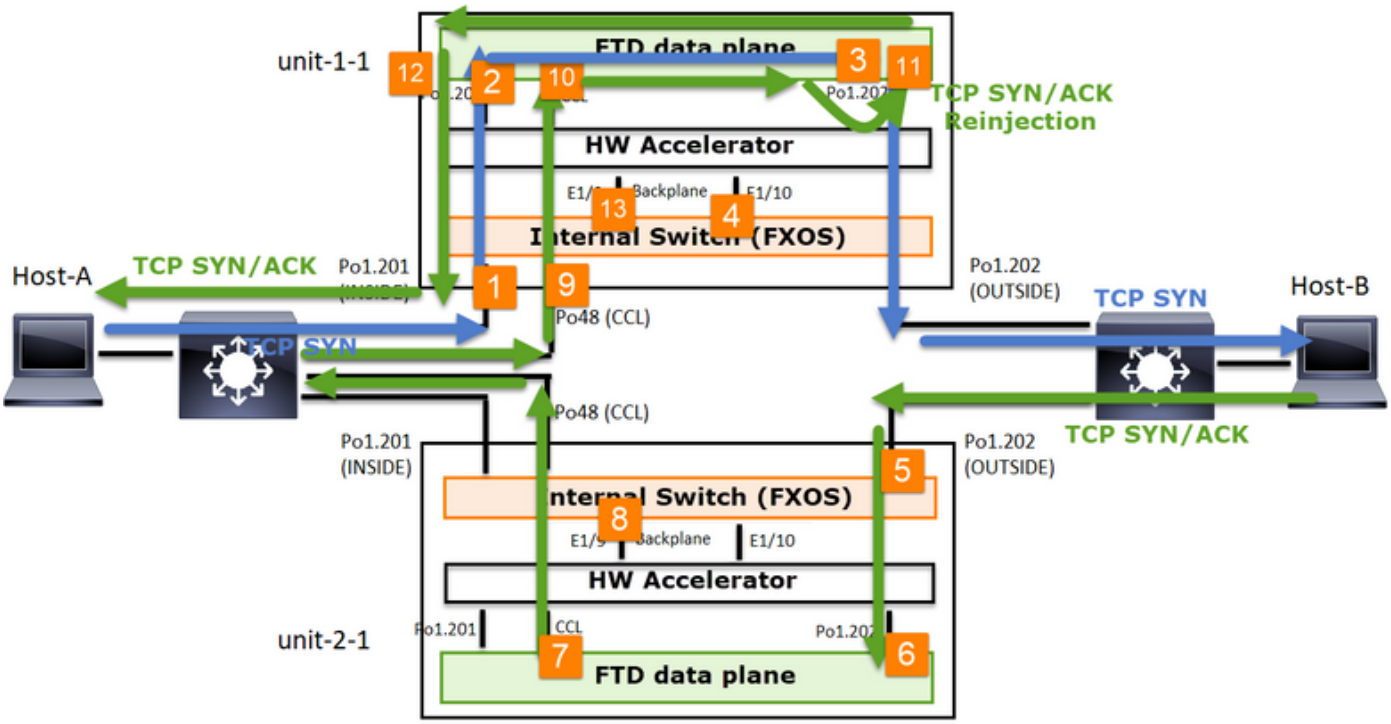
Sequence Number) e codifica le informazioni sulla proprietà (cookie) nel numero Seq.
5. TCP SYN viene inviato fuori da Po1.202/OUTSIDE (interfaccia di uscita del piano dati).
6. TCP SYN arriva su una delle interfacce backplane dello chassis (ad esempio, E1/9, E1/10, ecc.).
7. TCP SYN viene inviato dall'interfaccia fisica dello chassis (uno dei membri di Po1) verso l'host B.

Traffico di ritorno

8. TCP SYN/ACK viene inviato dall'host-B e arriva all'unità-2-1 (uno dei membri di Po1).
9. TCP SYN/ACK viene inviato al piano dati attraverso una delle interfacce backplane dello chassis (ad esempio, E1/9, E1/10, ecc.).
10. TCP SYN/ACK arriva sull'interfaccia in entrata del data plane (Po1.202/OUTSIDE).
11. TCP SYN/ACK viene inviato da Cluster Control Link (CCL) verso l'unità 1-1. Per impostazione predefinita, ISDN è abilitato. Pertanto, il server d'inoltro trova le informazioni sul proprietario per i TCP SYN+ACK senza il coinvolgimento del director. Per altri pacchetti o quando ISDN è disattivato, viene interrogato il director.
12. TCP SYN/ACK arriva su una delle interfacce backplane dello chassis (ad esempio, E1/9, E1/10 e così via).
13. TCP SYN/ACK viene inviato dall'interfaccia fisica dello chassis (uno dei membri di Po48) all'unità 1-1.
14. TCP SYN/ACK arriva sull'unità 1-1 (uno dei membri di Po48).
15. TCP SYN/ACK viene inoltrato attraverso una delle interfacce backplane dello chassis all'interfaccia del canale della porta CCL del piano dati (nameif cluster).
16. Il piano dati reindirizza il pacchetto TCP SYN/ACK all'interfaccia del piano dati Po1.202/OUTSIDE.
17. TCP SYN/ACK viene inviato fuori da Po1.201/INSIDE (data plane exit interface) verso HOST-A.
18. Il TCP SYN/ACK attraversa una delle interfacce backplane dello chassis (ad esempio, E1/9, E1/10 e così via) ed egredisce uno dei membri di Po1.
19. TCP SYN/ACK arriva sull'host-A.

Per ulteriori informazioni su questo scenario, vedere la sezione correlata in Casi di studio sull'istituzione di connessioni cluster.

In base a questo scambio di pacchetti, tutti i possibili punti di acquisizione del cluster sono:



Per il traffico di inoltro (ad esempio, TCP SYN), acquisire su:

1. L'interfaccia fisica dello chassis (ad esempio, membri Po1). Questa acquisizione viene configurata dall'interfaccia utente di Gestione chassis (CM) o dalla CLI di Gestione chassis.
2. Interfaccia in entrata del piano dati (ad esempio, Po1.201 INSIDE).
3. Interfaccia di uscita del piano dati (ad esempio, Po1.202 OUTSIDE).
4. Interfacce backplane chassis. Su FP4100 ci sono 2 interfacce backplane. Su FP9300 sono disponibili 6 (2 per modulo). Poiché non si conosce l'interfaccia a cui il pacchetto arriva, è necessario abilitare l'acquisizione su tutte le interfacce.

Per il traffico di ritorno (ad esempio, TCP SYN/ACK) acquisire su:

5. L'interfaccia fisica dello chassis (ad esempio, membri Po1). Questa acquisizione viene configurata dall'interfaccia utente di Gestione chassis (CM) o dalla CLI di Gestione chassis.
6. Interfaccia in entrata del piano dati (ad esempio, Po1.202 OUTSIDE).
7. Poiché il pacchetto viene reindirizzato, il punto di acquisizione successivo è il CCL del piano dati.
8. Interfacce backplane chassis. Anche in questo caso, abilitare l'acquisizione su entrambe le interfacce.
9. Interfacce membro CCL dello chassis dell'unità 1-1.
10. Interfaccia CCL del piano dati (nome del cluster).
11. Interfaccia in ingresso (Po1.202 OUTSIDE). Questo è il pacchetto reiniettato da CCL al piano dati.
12. Interfaccia di uscita del piano dati (ad esempio, Po1.201 INSIDE).
13. Interfacce backplane chassis.

Come abilitare le acquisizioni del cluster

Acquisizioni FXOS

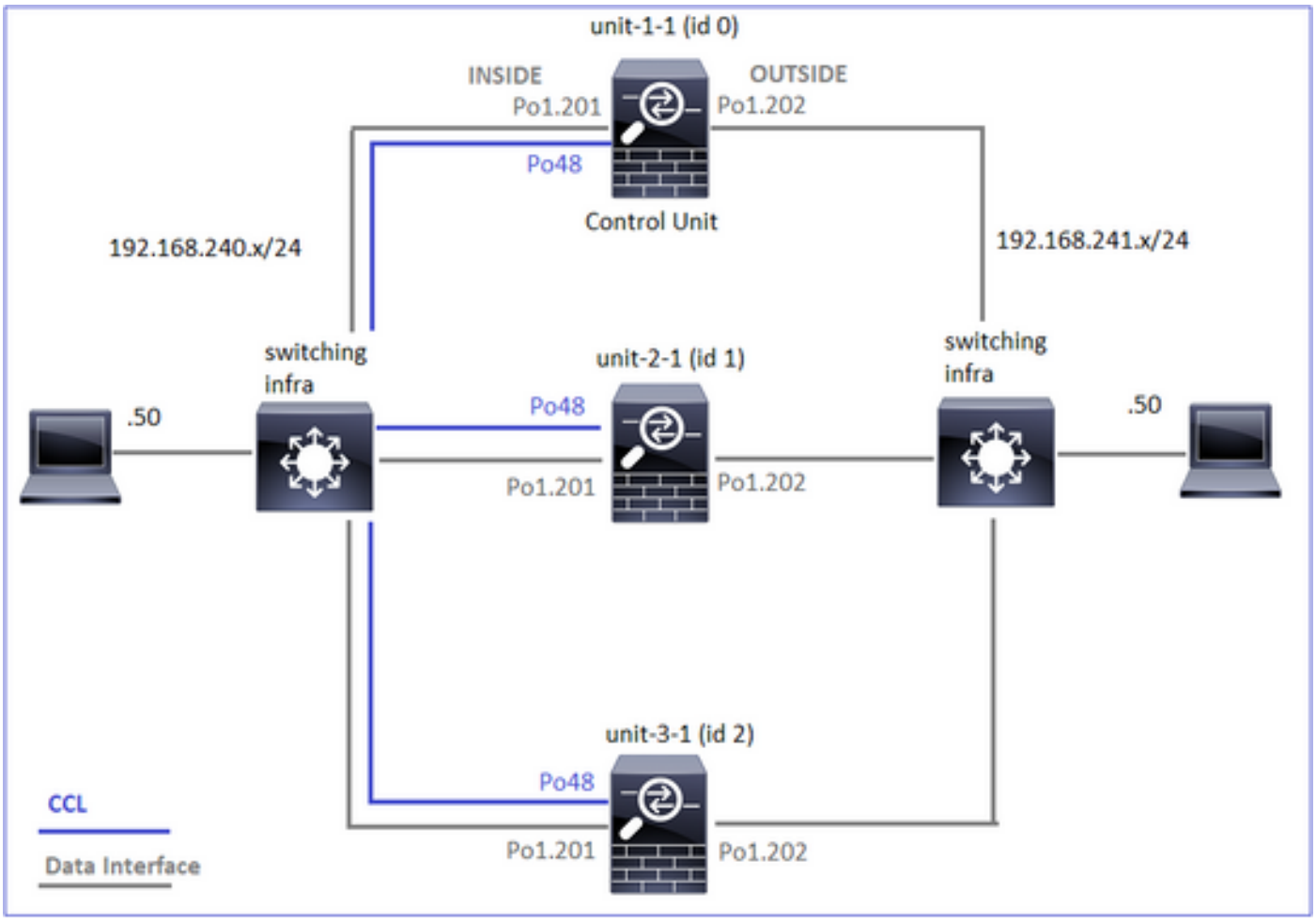
Il processo è descritto nella guida alla configurazione di FXOS: Acquisizione pacchetti

Nota: Le acquisizioni FXOS possono essere effettuate solo in entrata dal punto di vista dello switch interno.

Acquisizioni di Data Plane

Per abilitare l'acquisizione in tutti i membri del cluster, si consiglia di utilizzare il comando cluster exec.

Si consideri un cluster a 3 unità:



Per verificare se sono presenti acquisizioni attive in tutte le unità cluster, utilizzare questo comando:

<#root>

```
firepower#
cluster exec show capture

unit-1-1(LOCAL):*******************************************************

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

```
unit-3-1:************************************************************
firepower#
```

Per abilitare l'acquisizione di un piano dati su tutte le unità in Po1.201 (INSIDE):

<#root>

```
firepower#
```

cluster exec capture CAPI interface INSIDE

Per aumentare il buffer di acquisizione, si consiglia di specificare un filtro di acquisizione e, nel caso si preveda un traffico elevato:

<#root>

```
firepower#
```

cluster exec capture CAPI buffer 33554432 interface INSIDE match tcp host 192.168.240.50 host 192.168.24

Verifica

<#root>

```
firepower#
```

cluster exec show capture

```
unit-1-1(LOCAL):*********************************************************
capture CAPI type raw-data buffer 33554432 interface INSIDE [Capturing - 5140 bytes]
  match tcp host 192.168.240.50 host 192.168.241.50 eq www

unit-2-1:************************************************************
capture CAPI type raw-data buffer 33554432 interface INSIDE [Capturing - 260 bytes]
  match tcp host 192.168.240.50 host 192.168.241.50 eq www

unit-3-1:************************************************************
capture CAPI type raw-data buffer 33554432 interface INSIDE [Capturing - 0 bytes]
  match tcp host 192.168.240.50 host 192.168.241.50 eq www
```

Per visualizzare il contenuto di tutte le clip (questo output può essere molto lungo):

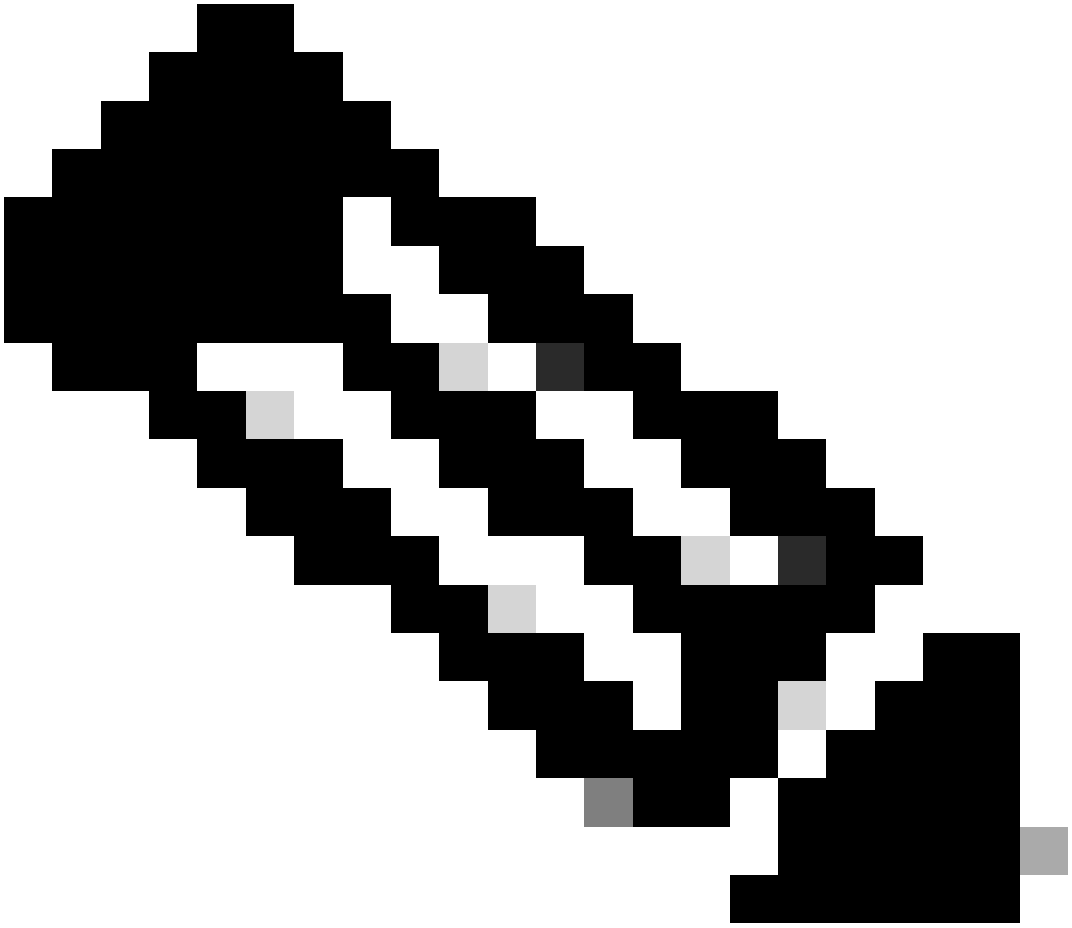
<#root>

```
firepower#
```

```
terminal pager 24


firepower#
cluster exec show capture CAPI


unit-1-1(LOCAL):*******************************************************
21 packets captured

1: 11:33:09.879226 802.1Q vlan#201 P0 192.168.240.50.45456 > 192.168.241.50.80: S 2225395909:2225395909
2: 11:33:09.880401 802.1Q vlan#201 P0 192.168.241.50.80 > 192.168.240.50.45456: S 719653963:719653963(0
3: 11:33:09.880691 802.1Q vlan#201 P0 192.168.240.50.45456 > 192.168.241.50.80: . ack 719653964 win 229
4: 11:33:09.880783 802.1Q vlan#201 P0 192.168.240.50.45456 > 192.168.241.50.80: P 2225395910:2225396054

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

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

Acquisisci tracce

Per vedere come vengono gestiti i pacchetti in entrata dal piano dati su ciascuna unità, usare la parola chiave trace. In questo modo si tracciano i primi 50 pacchetti in entrata. È possibile tracciare fino a 1000 pacchetti in entrata.



Nota: Se all'interfaccia sono state applicate più acquisizioni, è possibile tracciare un singolo pacchetto una sola volta.

Per tracciare i primi 1000 pacchetti in entrata sull'interfaccia OUTSIDE su tutte le unità cluster:

<#root>

```
firepower#
```

```
cluster exec cap CAPO int OUTSIDE buff 33554432 trace trace-count 1000 match tcp host 192.168.240.50 hos
```

Una volta acquisito il flusso di interesse, è necessario accertarsi di tracciare i pacchetti di interesse su ciascuna unità. L'importante da ricordare è che un pacchetto specifico può essere #1 sull'unità-1-1, ma #2 su un'altra unità, e così via.

Nell'esempio, si può vedere che il SYN/ACK è il pacchetto n. 2 sull'unità 2-1, ma il pacchetto n. 1

sull'unità 3-1:

<#root>

```
firepower#
cluster exec show capture CAPO | include S.*ack

unit-1-1(LOCAL):*********************************************************
1: 12:58:31.117700 802.1Q vlan#202 P0 192.168.240.50.45468 > 192.168.241.50.80: S 441626016:441626016(0
2: 12:58:31.118341 802.1Q vlan#202 P0 192.168.241.50.80 > 192.168.240.50.45468:
S
 301658077:301658077(0)
ack
 441626017 win 28960 <mss 1460,sackOK,timestamp 1125686319 1115330849,nop,wscale 7>

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

unit-3-1:*********************************************************
1: 12:58:31.111429 802.1Q vlan#202 P0 192.168.241.50.80 > 192.168.240.50.45468:
S
 301658077:301658077(0)
ack
 441626017 win 28960 <mss 1460,sackOK,timestamp 1125686319 1115330849,nop,wscale 7>
```

Per tracciare il pacchetto 2 (SYN/ACK) sull'unità locale:

<#root>

```
firepower#
cluster exec show cap CAPO packet-number 2 trace

unit-1-1(LOCAL):*********************************************************

2: 12:58:31.118341 802.1Q vlan#202 P0 192.168.241.50.80 > 192.168.240.50.45468:
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
...
```

Per tracciare lo stesso pacchetto (SYN/ACK) sull'unità remota:

<#root>

```
firepower#
```

cluster exec unit unit-3-1 show cap CAPO packet-number 1 trace

```
1: 12:58:31.111429 802.1Q vlan#202 P0 192.168.241.50.80 > 192.168.240.50.45468:
```

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
...
```

Acquisizione CCL

Per abilitare l'acquisizione sul collegamento CCL (su tutte le unità):

<#root>

```
firepower#
```

cluster exec capture CCL interface cluster

```
unit-1-1(LOCAL):*******************************************************

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

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

Rifiuta Nascondi

Per impostazione predefinita, un'acquisizione abilitata su un'interfaccia dati del piano dati mostra tutti i pacchetti:

- Quelli che arrivano dalla rete fisica
- Quelli che vengono reiniettati dalla CCL

Se non si desidera visualizzare i pacchetti reiniettati, usare l'opzione reinject-hide. Ciò può essere utile se si desidera verificare se un flusso è asimmetrico:

```
<#root>

firepower#

cluster exec capture CAPI_RH reinject-hide interface INSIDE match tcp host 192.168.240.50 host 192.168.2
```

Questa acquisizione mostra solo ciò che l'unità locale riceve effettivamente sull'interfaccia specifica direttamente dalla rete fisica e non dalle altre unità del cluster.

Cadute ASP

Se si desidera verificare la presenza di perdite software per un flusso specifico, è possibile abilitare l'acquisizione asp-drop. Se non si conosce il motivo della perdita su cui concentrarsi, utilizzare la parola chiave all. Inoltre, se non si è interessati al payload del pacchetto, è possibile specificare la parola chiave headers-only. In questo modo è possibile acquisire un numero di pacchetti da 20 a 30 volte superiore:

```
<#root>

firepower#

cluster exec cap ASP type asp-drop all buffer 33554432 headers-only


unit-1-1(LOCAL):**********************************************************

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

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

È inoltre possibile specificare gli IP di interesse nell'acquisizione ASP:

```
<#root>

firepower#

cluster exec cap ASP type asp-drop all buffer 33554432 headers-only


match ip host 192.0.2.100 any
```

Cancella un'acquisizione

Cancellare il buffer di qualsiasi acquisizione eseguita in tutte le unità cluster. In questo modo le acquisizioni non vengono interrotte, ma vengono cancellati solo i buffer:

<#root>

```
firepower#
cluster exec clear capture /all

unit-1-1(LOCAL):*********************************************************
unit-2-1:*********************************************************
unit-3-1:*********************************************************
```

Interrompere un'acquisizione

Esistono due modi per arrestare un'acquisizione attiva su tutte le unità cluster. In seguito sarà possibile riprendere l'attività.

Modo 1

<#root>

```
firepower#
cluster exec cap CAPI stop

unit-1-1(LOCAL):*********************************************************
unit-2-1:*********************************************************
unit-3-1:*********************************************************
```

Per riprendere

<#root>

```
firepower#
cluster exec no capture CAPI stop

unit-1-1(LOCAL):*********************************************************
unit-2-1:*********************************************************
unit-3-1:*********************************************************
```

Modo 2

<#root>

```
firepower#
cluster exec no capture CAPI interface INSIDE

unit-1-1(LOCAL):*********************************************************
unit-2-1:*********************************************************
unit-3-1:*********************************************************
```

Per riprendere

<#root>

```
firepower#
cluster exec capture CAPI interface INSIDE

unit-1-1(LOCAL):*********************************************************
unit-2-1:*********************************************************
unit-3-1:*********************************************************
```

Raccogli un'acquisizione

Esistono diversi modi per esportare un'acquisizione.

Modo 1 - A un server remoto

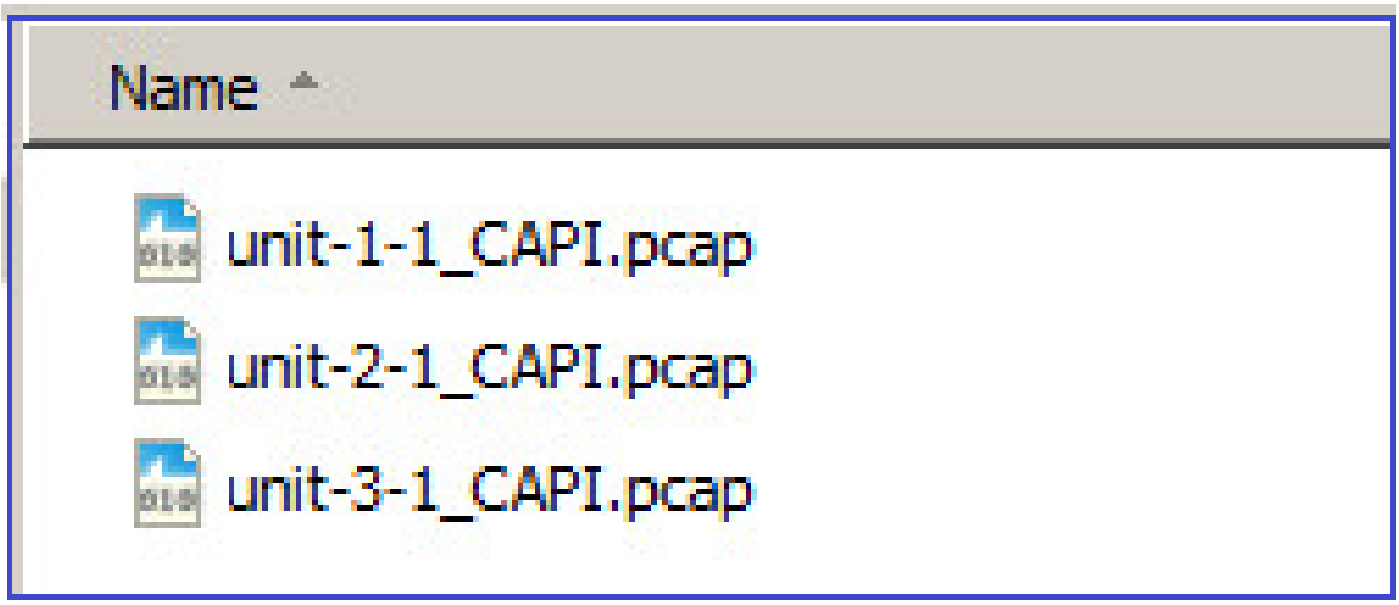
Ciò consente di caricare un'acquisizione dal piano dati su un server remoto (ad esempio, TFTP). I nomi di acquisizione vengono modificati automaticamente per riflettere l'unità di origine:

<#root>

```
firepower#
cluster exec copy /pcap capture:CAPI tftp://192.168.240.55/CAPI.pcap

unit-1-1(LOCAL):*********************************************************
Source capture name [CAPI]?
Address or name of remote host [192.168.240.55]?
```

```
Destination filename [CAPI.pcap]?

INFO: Destination filename is changed to unit-1-1_CAPI.pcap !!!!!!!

81 packets copied in 0.40 secs

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

INFO: Destination filename is changed to unit-2-1_CAPI.pcap !


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

INFO: Destination filename is changed to unit-3-1_CAPI.pcap !
```

I file pcap caricati:



Modo 2 - Recupera le clip dal CCP

Questo metodo è applicabile solo all'FTD. Innanzitutto, copiare l'acquisizione sul disco FTD:

<#root>

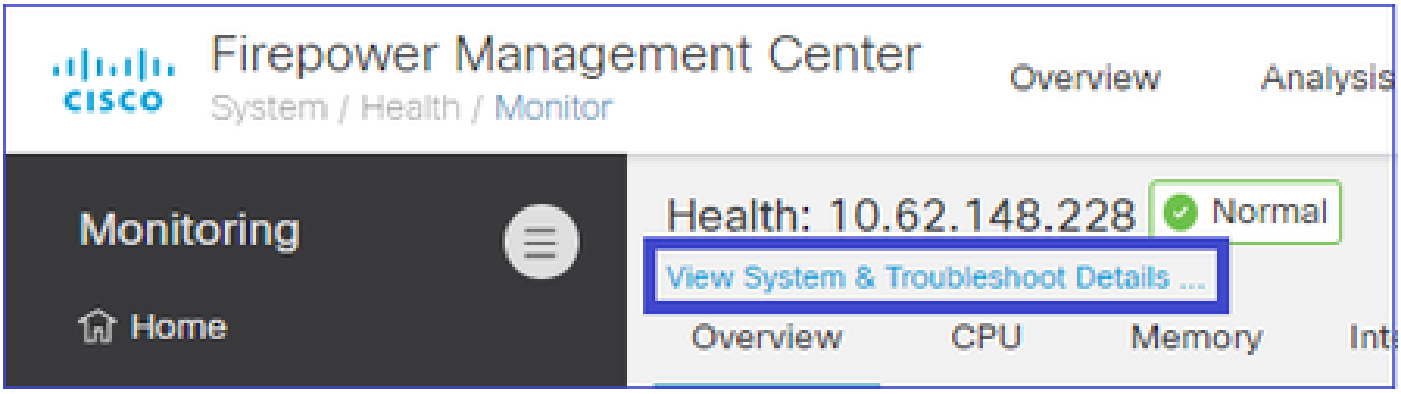
```
firepower#

cluster exec copy /pcap capture:CAPI disk0:CAPI.pcap


unit-1-1(LOCAL):****************************************************

Source capture name [CAPI]?

Destination filename [CAPI.pcap]?
!!!!!
```

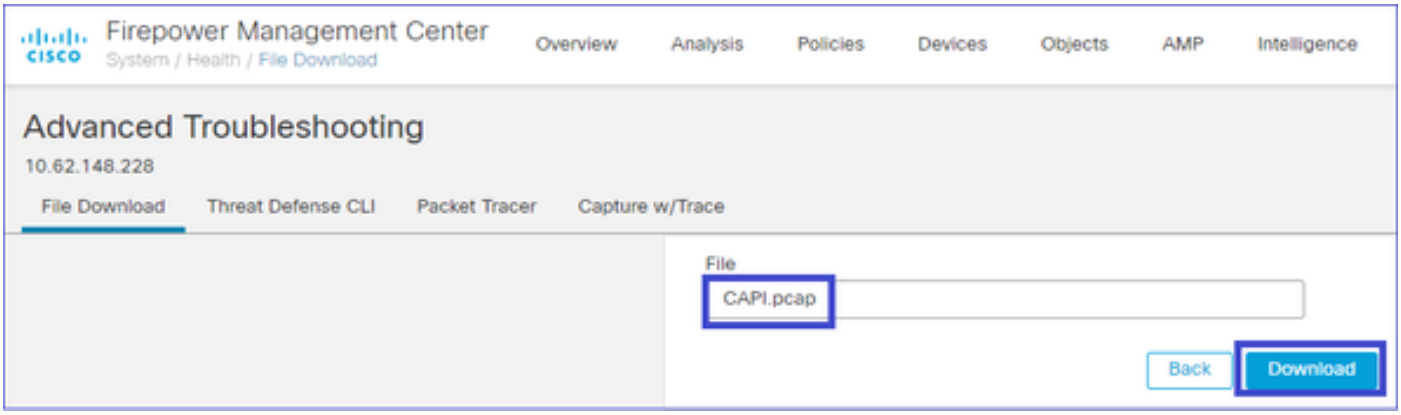
```
62 packets copied in 0.0 secs
```

In modalità Expert, copiare il file dalla directory /mnt/disk0/ alla directory /ngfw/var/common/:

```
<#root>

>

expert

admin@firepower:~$

cd /mnt/disk0

admin@firepower:/mnt/disk0$

sudo cp CAPI.pcap /ngfw/var/common
```

Infine, su FMC passare alla sezione Sistema > Integrità > Monitor. Scegliere Visualizza dettagli di sistema e risoluzione dei problemi > Risoluzione dei problemi avanzata e recuperare il file di acquisizione:





Eliminare un'acquisizione

Per rimuovere un'acquisizione da tutte le unità cluster, utilizzare questo comando:

```
<#root>

firepower#

cluster exec no capture CAPI


unit-1-1(LOCAL):*******************************************************

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

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

Flussi scaricati

Su FP41xx/FP9300 i flussi possono essere scaricati su HW Accelerator in modo statico (ad esempio, le regole Fastpath) o dinamico. Per ulteriori informazioni sull'offload del flusso, consultare questo documento:

https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212321-clarify-the-firepower-threat-defense-acc.html#anc22

Se un flusso viene scaricato, solo pochi pacchetti passano attraverso il piano dati FTD. Il resto viene gestito dall'acceleratore hardware (Smart NIC).

Dal punto di vista dell'acquisizione, ciò significa che se si abilitano solo le acquisizioni a livello di piano dati FTD, non si vedranno tutti i pacchetti che passano attraverso il dispositivo. In questo caso, è necessario abilitare anche le acquisizioni a livello di chassis FXOS.

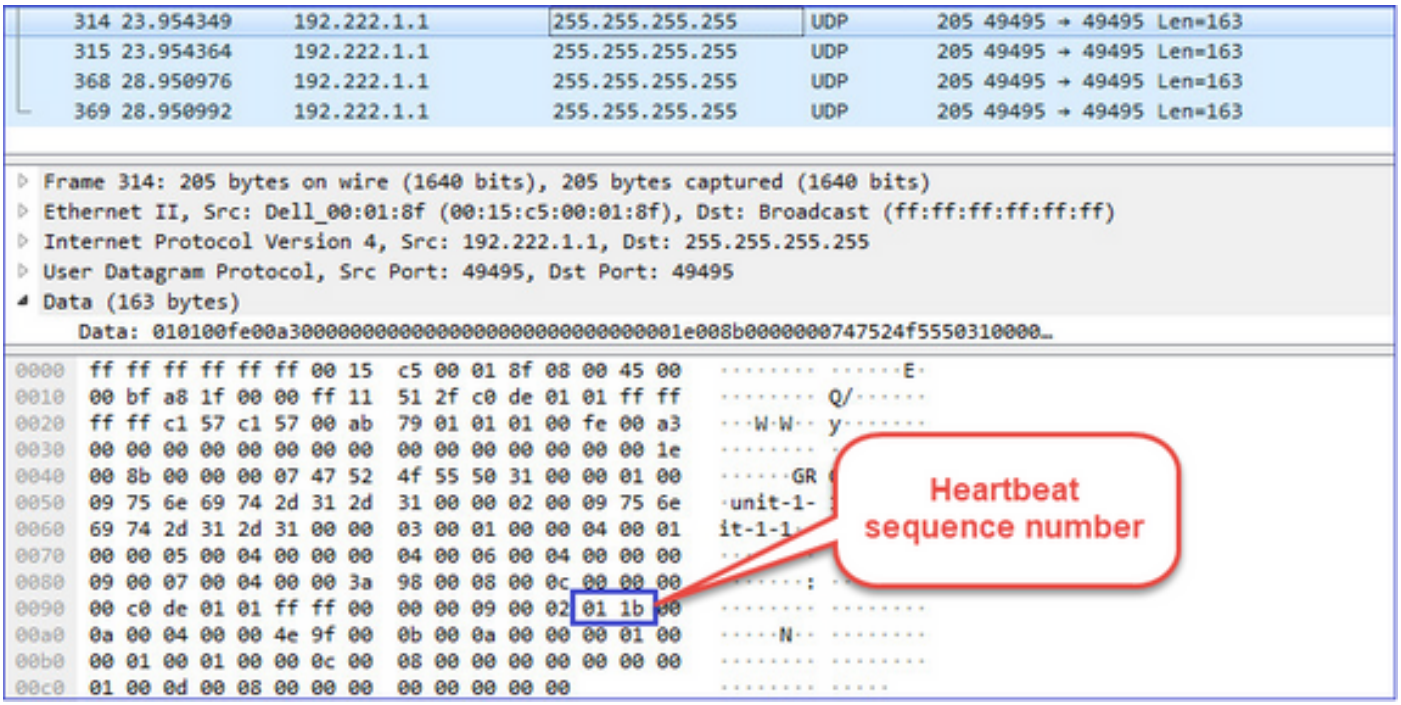
Messaggi CCL (Cluster Control Link)

Se si esegue un'acquisizione nella CCL, si noterà che le unità del cluster scambiano diversi tipi di messaggi. Le aree di interesse sono:

Protocollo	Descrizione
UDP 49495	Heartbeat del cluster (keepalive) · Trasmissione L3 (255.255.255.255) · Questi pacchetti vengono inviati da ogni unità cluster a 1/3 del valore del tempo di attesa per il controllo dello stato. · Notare che non tutti i pacchetti UDP 49495 rilevati nell'acquisizione sono heartbeat · Gli heartbeat contengono un numero di sequenza.

UDP 4193	Messaggi sul percorso dati del protocollo di controllo del cluster · Unicast · Questi pacchetti contengono informazioni (metadati) sul proprietario del flusso, sul director, sul proprietario del backup e così via. Alcuni esempi: · Quando viene creato un nuovo flusso, il proprietario invia un messaggio di aggiunta cluster al director · Quando un flusso viene terminato, il proprietario invia un messaggio di "eliminazione del cluster" al director
Pacchetti di dati	Pacchetti di dati appartenenti ai vari flussi di traffico che attraversano il cluster

Heartbeat del cluster



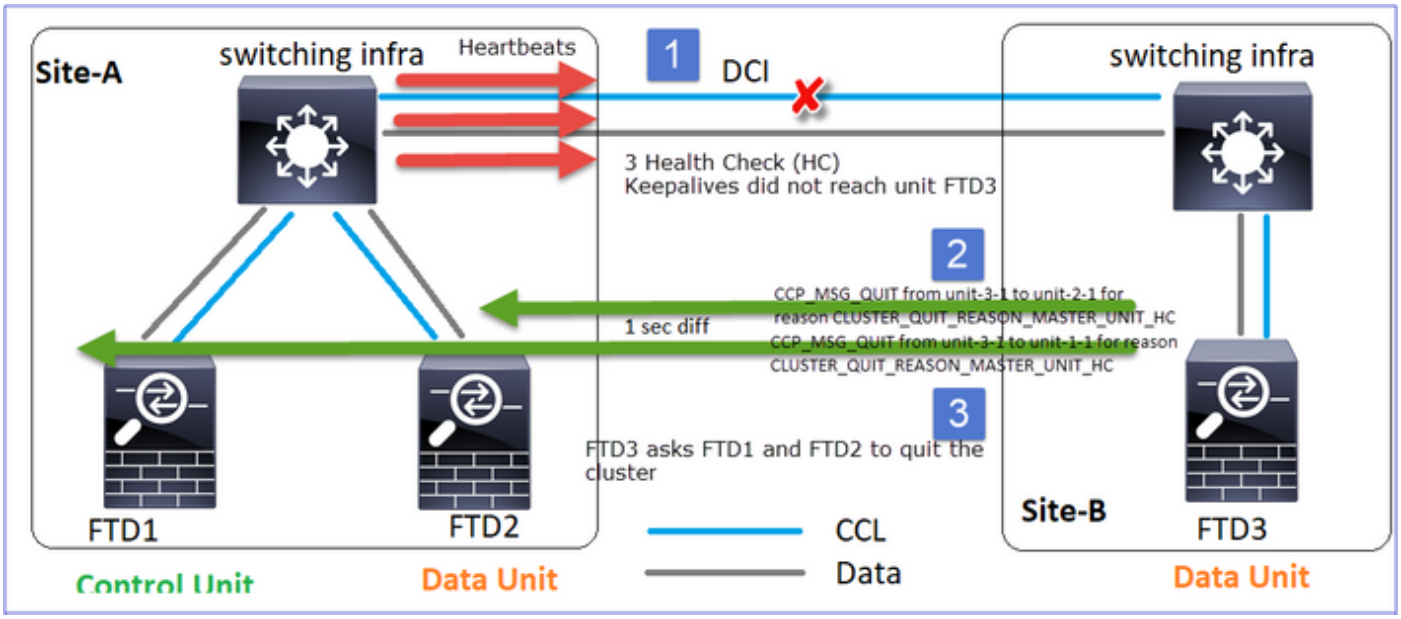
Messaggi CCP (Cluster Control Point)

Oltre ai messaggi di heartbeat, sono disponibili numerosi messaggi di controllo del cluster scambiati tramite la CCL in scenari specifici. Alcuni di essi sono messaggi unicast mentre altri sono trasmissioni.

CLUSTER_QUIT_REASON_PRIMARY_UNIT_HC

Ogni volta che un'unità perde 3 messaggi heartbeat consecutivi dal nodo di controllo, genera un messaggio CLUSTER_QUIT_REASON_PRIMARY_UNIT_HC sul CCL. Questo messaggio:

- È un unicast.
- e viene inviato a ciascuna delle unità con un intervallo di 1 sec.
- Quando un'unità riceve questo messaggio, esce dal cluster (DISABLED) e si unisce nuovamente.

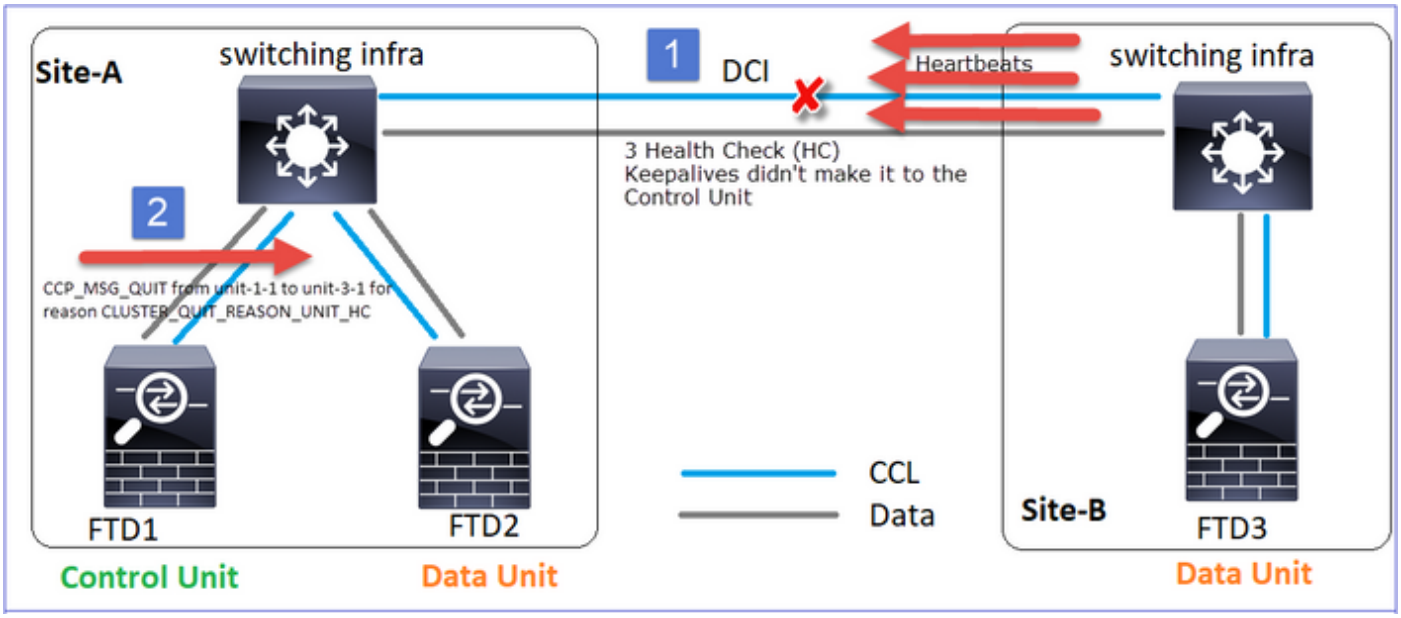


D. Qual è lo scopo di CLUSTER_QUIT_REASON_PRIMARY_UNIT_HC?

A. Dal punto di vista dell'unità-3-1 (Sito-B), perde la connessione sia all'unità-1-1 che all'unità-2-1 dal sito A, quindi deve rimuoverli dal suo elenco dei membri il prima possibile, altrimenti può perdere il pacchetto se l'unità-2-1 è ancora nel suo elenco dei membri e l'unità-2-1 si presenta come il direttore di una connessione, e la query del flusso all'unità-2-1 non riesce.

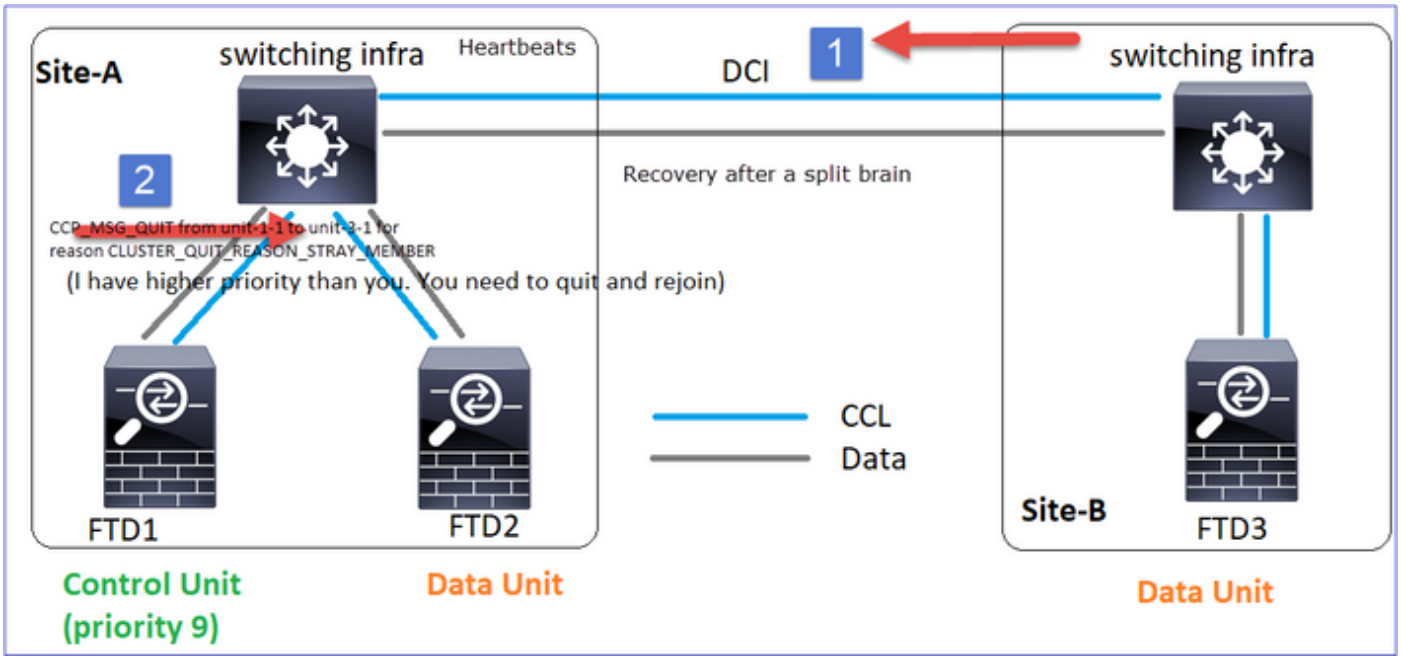
CLUSTER_QUIT_REASON_UNIT_HC

Ogni volta che il nodo di controllo perde 3 messaggi heartbeat consecutivi da un nodo di dati, invia il messaggio CLUSTER_QUIT_REASON_UNIT_HC sulla CCL. Questo messaggio è unicast.



CLUSTER_QUIT_REASON_STRAY_MEMBER

Quando una partizione divisa si riconnette con una partizione peer, il nuovo nodo di dati viene trattato come membro isolato dall'unità di controllo dominante e riceve un messaggio di uscita CCP con il motivo CLUSTER_QUIT_REASON_STRAY_MEMBER.



CLUSTER_QUIT_MEMBER_DROP

Messaggio broadcast generato da un nodo dati e inviato come broadcast. Quando un apparecchio riceve questo messaggio, passa allo stato DISABLED. Inoltre, l'auto-rejoin non decolla:

<#root>

firepower#

show cluster info trace | include DROPOUT

Nov 04 00:22:54.699 [DBUG]Receive CCP message: CCP_MSG_QUIT from unit-3-1 to unit-1-1 for reason

CLUSTER_QUIT_MEMBER_DROPOUT

Nov 04 00:22:53.699 [DBUG]Receive CCP message: CCP_MSG_QUIT from unit-3-1 to unit-2-1 for reason

CLUSTER_QUIT_MEMBER_DROPOUT

La cronologia del cluster mostra quanto segue:

<#root>

PRIMARY DISABLED Received control message DISABLE (

member dropout announcement

)

Meccanismo di verifica dello stato del cluster (HC)

Considerazioni principali

- Ogni unità cluster invia un heartbeat ogni 1/3 del valore del tempo di attesa per il controllo dello stato a tutte le altre unità (broadcast 255.255.255.255) e utilizza la porta UDP 49495 come trasporto sul CCL.
- Ogni unità cluster tiene traccia in modo indipendente di ogni altra unità con un timer di polling e un valore di conteggio polling.
- Se un'unità cluster non riceve alcun pacchetto (heartbeat o pacchetto dati) da un'unità peer del cluster entro un intervallo di heartbeat, aumenta il valore del conteggio polling.
- Quando il valore del conteggio di polling per un'unità peer del cluster diventa 3, il peer viene considerato inattivo.
- Ogni volta che si riceve un heartbeat, viene controllato il relativo numero di sequenza e nel caso in cui la differenza con l'heartbeat ricevuto in precedenza sia diversa da 1, il contatore di rilascio dell'heartbeat aumenta di conseguenza.
- Se il contatore Conteggio polling per un peer del cluster è diverso da 0 e il peer riceve un pacchetto, il contatore viene reimpostato su 0.

Utilizzare questo comando per controllare i contatori di integrità del cluster:

<#root>

```
firepower#
```

show cluster info health details

```
----------------------------------------------------------------------------------
|                Unit (ID)| Heartbeat| Heartbeat|   Average|   Maximum|      Poll|
|                         |     count|     drops|  gap (ms)| slip (ms)|     count|
----------------------------------------------------------------------------------
|            unit-2-1 ( 1)|       650|         0|      4999|         1|         0|
|            unit-3-1 ( 2)|       650|         0|      4999|         1|         0|
----------------------------------------------------------------------------------
```

Descrizione delle colonne principali

Colonna	Descrizione
Unità (ID)	ID del peer del cluster remoto.
Conteggio heartbeat	Numero di heartbeat ricevuti dal peer remoto tramite CCL.

Cadute di heartbeat	Numero di heartbeat mancati. Questo contatore viene calcolato in base al numero di sequenza di heartbeat ricevuto.
Distanza media	Intervallo di tempo medio degli heartbeat ricevuti.
Conteggio sondaggi	Quando questo contatore diventa 3, l'unità viene rimossa dal cluster. L'intervallo di query di polling è uguale all'intervallo di heartbeat, ma viene eseguito in modo indipendente.

Per reimpostare i contatori, utilizzare questo comando:

<#root>

```
firepower#
clear cluster info health details
```

D. Come verificare la frequenza del battito cardiaco?

A. Controllare il valore medio dell'intervallo:

<#root>

```
firepower#
show cluster info health details

-------------------------------------------------------------------------------
|                Unit (ID)| Heartbeat| Heartbeat|
Average
|   Maximum|      Poll|
|                         |     count|     drops|
gap (ms)
| slip (ms)|     count|
-------------------------------------------------------------------------------
|            unit-2-1 ( 1)|      3036|         0|
999
|         1|         0|
-------------------------------------------------------------------------------
```

D. Come è possibile modificare il tempo di attesa del cluster su FTD?

A. Uso di FlexConfig

D. Chi diventa il nodo di controllo dopo uno split-brain?

A. L'unità con la priorità più alta (numero più basso):

<#root>

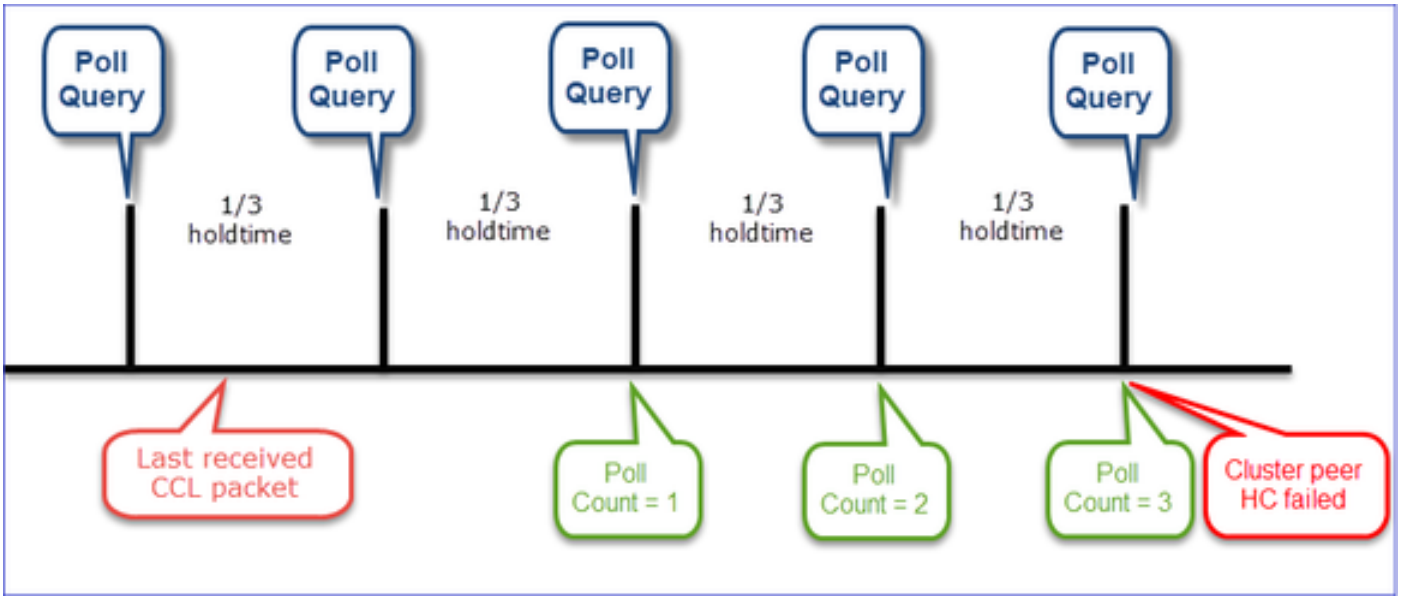
```
firepower#
```

```
show run cluster | include priority
```

```
priority 9
```

Per ulteriori informazioni, vedere lo scenario di errore 1 relativo alla conversione del tipo di dati.

Visualizzazione del meccanismo HC del cluster



Timer indicativi: Il valore minimo e il valore massimo dipendono dall'ultimo arrivo del pacchetto CCL ricevuto.

Tempo di attesa	Verifica query di polling (frequenza)	Tempo di rilevamento minimo	Tempo di rilevamento massimo
3 sec (impostazione predefinita)	Circa 1 sec	~3,01 sec	~3,99 sec

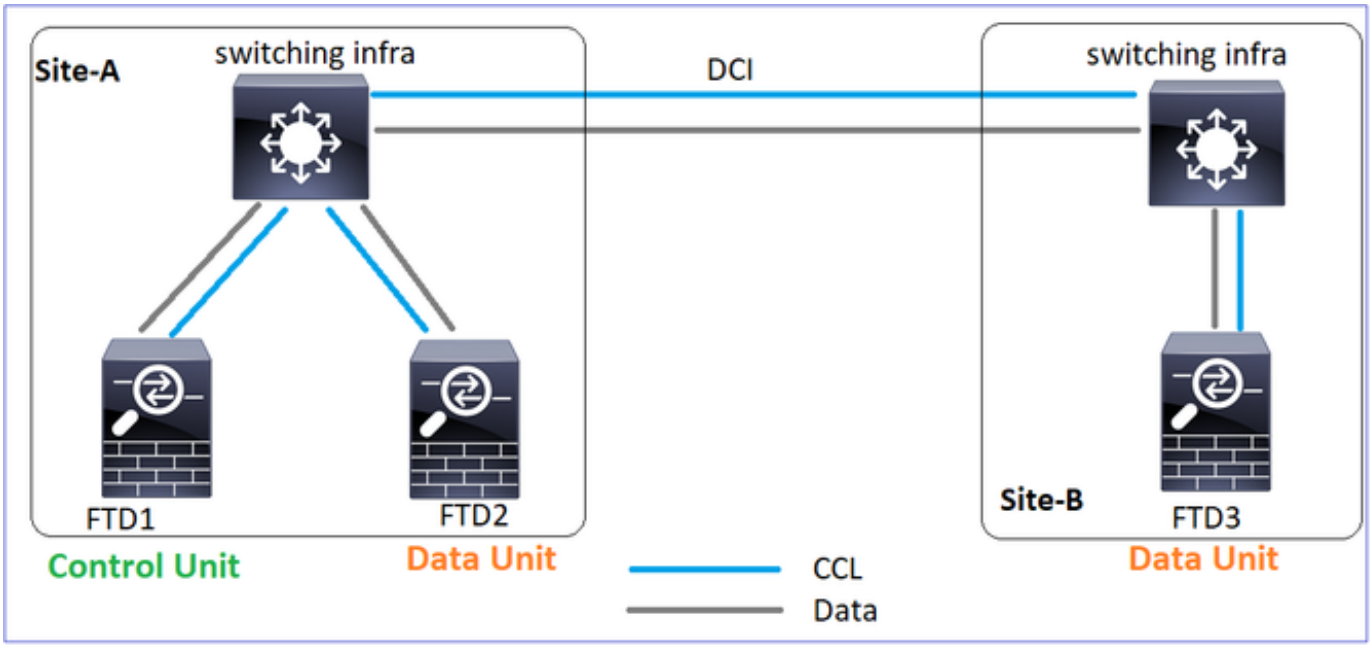
4 sec.	~1,33 sec	~4,01 sec	Circa 5,32 sec
5 sec.	~1,66 sec	Circa 5,01 sec	~6,65 sec
6 sec.	Circa 2 sec	~6,01 sec	~7,99 sec
7 sec.	~2,33 sec	Circa 7,01 sec	~9,32 sec
8 sec	~2,66 sec	Circa 8,01 sec	Circa 10,65 sec

Scenari di errore HC del cluster

Gli obiettivi di questa sezione sono illustrare:

- Diversi scenari di errore HC del cluster.
- Correlazione tra i diversi log e output di comando.

Topologia



Configurazione cluster

Unità-1-1	Unità-2-1
`cluster group GROUP1`	`cluster group GROU`

```
key *****
local-unit unit-1-1
cluster-interface Port-channel48 ip 10.17.1.1 255.255.0.0
priority 9
health-check holdtime 3
health-check data-interface auto-rejoin 3 5 2
health-check cluster-interface auto-rejoin unlimited 5 1
health-check system auto-rejoin 3 5 2
health-check monitor-interface debounce-time 500
site-id 1
enable
```

```
key *****
local-unit unit-2-
cluster-interface
priority 17
health-check holdt
health-check data-
health-check clust
health-check syste
health-check monit
site-id 1
enable
```

Stato cluster

Unità-1-1	Unità-2-1
<#root> firepower# **show cluster info** Cluster GROUP1: On Interface mode: spanned **This is "unit-1-1" in state PRIMARY** ID : 0 Site ID : 1 Version : 9.12(2)33 Serial No.: FCH22247LNK CCL IP : 10.17.1.1 CCL MAC : 0015.c500.018f Last join : 20:25:36 UTC Nov 1 2020 Last leave: 20:25:28 UTC Nov 1 2020 Other members in the cluster: **Unit "unit-3-1" in state secondary** ID : 1 Site ID : 2 Version : 9.12(2)33 Serial No.: FCH22247MKJ CCL IP : 10.17.3.1 CCL MAC : 0015.c500.038f Last join : 20:58:45 UTC Nov 1 2020 Last leave: 20:58:37 UTC Nov 1 2020	<#root> firepower# **show cluster info** Cluster GROUP1: On Interface mode: spanned **This is "unit-2-1" in state SECONDARY** ID : 2 Site ID : 1 Version : 9.12(2)33 Serial No.: FCH23157Y9N CCL IP : 10.17.2.1 CCL MAC : 0015.c500.028 Last join : 20:44:46 UTC Last leave: 20:44:38 UTC Other members in the cluster: **Unit "unit-1-1" in state PRIMARY** ID : 0 Site ID : 1 Version : 9.12(2)33 Serial No.: FCH22247LNK CCL IP : 10.17.1.1 CCL MAC : 0015.c500.018 Last join : 20:25:36 UTC Last leave: 20:25:28 UTC

Unit "unit-2-1" in state SECONDARY ID : 2 Site ID : 1 Version : 9.12(2)33 Serial No.: FCH23157Y9N CCL IP : 10.17.2.1 CCL MAC : 0015.c500.028f Last join : 20:44:45 UTC Nov 1 2020 Last leave: 20:44:38 UTC Nov 1 2020	**Unit "unit-3-1" in state SECONDARY** ID : 1 Site ID : 2 Version : 9.12(2)33 Serial No.: FCH22247MKJ CCL IP : 10.17.3.1 CCL MAC : 0015.c500.038 Last join : 20:58:45 UTC Last leave: 20:58:37 UTC

Scenario 1

Perdita di comunicazione CCL per circa 4+ sec in entrambe le direzioni.

Prima dell'errore

FTD1	FTD2	FTD3
Sito-A	Sito-A	Sito-B
Nodo di controllo	Nodo dati	Nodo dati

Dopo il ripristino (nessuna modifica nei ruoli delle unità)

FTD1	FTD2	FTD3
Sito-A	Sito-A	Sito-B
Nodo di controllo	Nodo dati	Nodo dati

Analisi

Errore (comunicazione CCL persa).

Messaggio della console del piano dati sull'unità 3-1:

<#root>

```
firepower#
WARNING: dynamic routing is not supported on management interface when cluster interface-mode is 'spann
If dynamic routing is configured on any management interface, please remove it.


Cluster unit unit-3-1 transitioned from SECONDARY to PRIMARY


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.
```

Registri di traccia cluster unità 1-1:

<#root>

```
firepower#

show cluster info trace | include unit-3-1


Nov 02 09:38:14.239 [INFO]Notify chassis de-bundle port for blade unit-3-1, stack 0x000055a8918307fb 0x
Nov 02 09:38:14.239 [INFO]FTD - CD proxy received state notification (DISABLED) from unit unit-3-1
Nov 02 09:38:14.239

[DBUG]Send CCP message to all: CCP_MSG_QUIT from unit-1-1 to unit-3-1 for reason CLUSTER_QUIT_MEMBER_DRO


Nov 02 09:38:14.239 [INFO]Notify chassis de-bundle port for blade unit-3-1, stack 0x000055a8917eb596 0x
Nov 02 09:38:14.239

[DBUG]Send CCP message to id 1: CCP_MSG_QUIT from unit-1-1 to unit-3-1 for reason CLUSTER_QUIT_REASON_UN


Nov 02 09:38:14.239 [CRIT]Received heartbeat event 'SECONDARY heartbeat failure' for member unit-3-1 (I
```

Spaccato

Unità-1-1	Unità-2-1

```
<#root>

firepower#

show cluster info


Cluster GROUP1: On
    Interface mode: spanned


This is "unit-1-1" in state PRIMARY


        ID        : 0
        Site ID   : 1
        Version   : 9.12(2)33
        Serial No.: FCH22247LNK
        CCL IP    : 10.17.1.1
        CCL MAC   : 0015.c500.018f
        Last join : 20:25:36 UTC Nov 1 2020
        Last leave: 20:25:28 UTC Nov 1 2020
Other members in the cluster:
    Unit "unit-2-1" in state SECONDARY
        ID        : 2
        Site ID   : 1
        Version   : 9.12(2)33
        Serial No.: FCH23157Y9N
        CCL IP    : 10.17.2.1
        CCL MAC   : 0015.c500.028f
        Last join : 20:44:45 UTC Nov 1 2020
        Last leave: 20:44:38 UTC Nov 1 2020
```

```
<#root>

firepower#

show cluster info


Cluster GROUP1: On
    Interface mode: spanned
    This is "unit-2-1" in state SE
        ID        : 2
        Site ID   : 1
        Version   : 9.12(2)33
        Serial No.: FCH23157Y9N
        CCL IP    : 10.17.2.1
        CCL MAC   : 0015.c500.028f
        Last join : 20:44:46 UTC N
        Last leave: 20:44:38 UTC N
Other members in the cluster:


Unit "unit-1-1" in state PRIMARY


        ID        : 0
        Site ID   : 1
        Version   : 9.12(2)33
        Serial No.: FCH22247LNK
        CCL IP    : 10.17.1.1
        CCL MAC   : 0015.c500.018f
        Last join : 20:25:36 UTC N
        Last leave: 20:25:28 UTC N
```

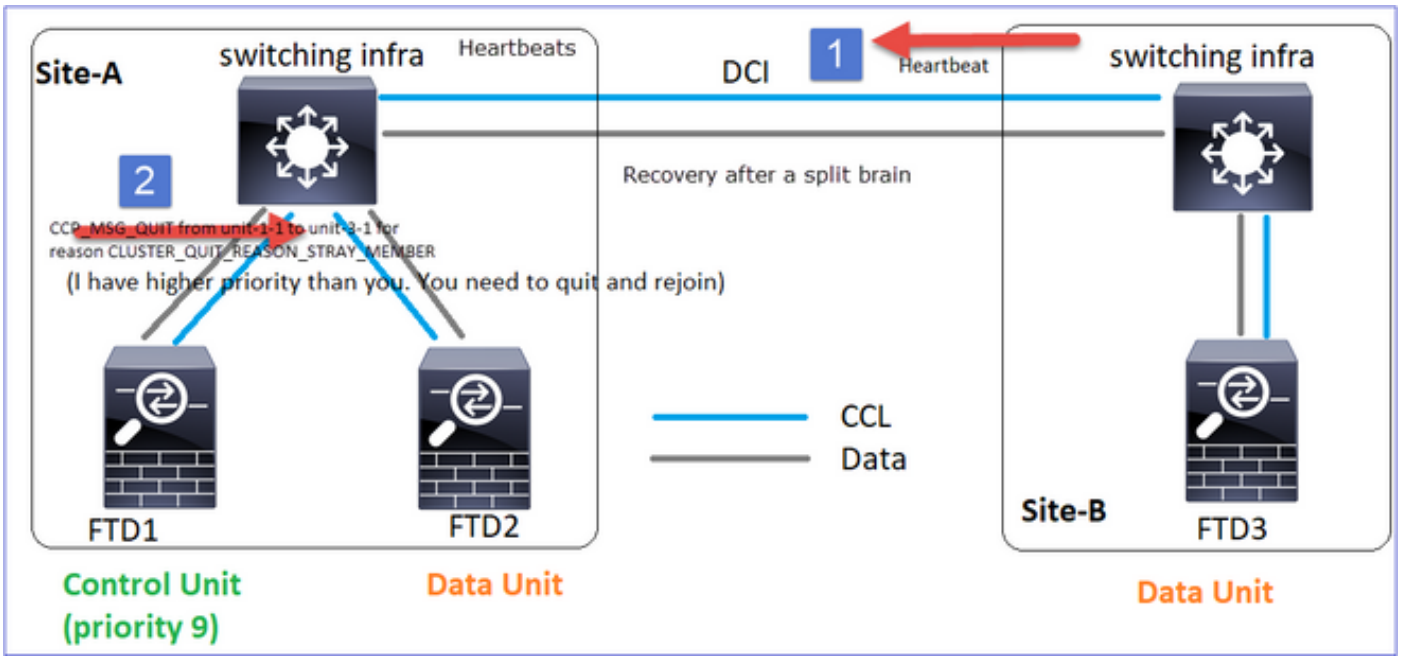
Cronologia cluster

Unità-1-1	Unità-2-1	Unità-3-1
Nessun evento	Nessun evento	<#root> 09:38:16 UTC Nov 2 2020 **SECONDARY PRIMARY_POST_CONFIG Primary relinqui** 09:38:17 UTC Nov 2 2020 PRIMARY_POST_CONFIG Primary Primary post config

Ripristino comunicazioni CCL

L'unità 1-1 rileva il nodo di controllo corrente e, poiché l'unità 1-1 ha priorità più alta, invia all'unità 3-1 un messaggio CLUSTER_QUIT_REASON_STRAY_MEMBER per attivare un nuovo processo di selezione. Alla fine, unit-3-1 si ricongiunge come nodo dati.

Quando una partizione divisa si riconnette con una partizione peer, il nodo di dati viene trattato come membro isolato dal nodo di controllo dominante e riceve un messaggio di uscita CCP con un motivo di CLUSTER_QUIT_REASON_STRAY_MEMBER.



<#root>

```
Unit-3-1 console logs show:
```

Cluster unit unit-3-1 transitioned from PRIMARY to DISABLED

```
The 3DES/AES algorithms require a Encryption-3DES-AES activation key.
```

Detected Cluster Primart.

```
Beginning configuration replication from Primary.
WARNING: Local user database is empty and there are still 'aaa' commands for 'LOCAL'.
..
Cryptochecksum (changed): a9ed686f 8e2e689c 2553a104 7a2bd33a
End configuration replication from Primary.
```

Cluster unit unit-3-1 transitioned from DISABLED to SECONDARY

Entrambe le unità (unità-1-1 e unità-3-1) vengono visualizzate nei relativi registri cluster:

<#root>

```
firepower#
show cluster info trace | include retain

Nov 03 21:20:23.019 [CRIT]Found a split cluster with both unit-1-1 and unit-3-1 as primary units. Prima
Nov 03 21:20:23.019 [CRIT]Found a split cluster with both unit-1-1 and unit-3-1 as primary units. Prima
```

Esistono anche messaggi syslog generati per lo split-brain:

```
<#root>
firepower#
show log | include 747016

Nov 03 2020 21:20:23: %FTD-4-747016: Clustering: Found a split cluster with both unit-1-1 and unit-3-1 a
Nov 03 2020 21:20:23: %FTD-4-747016: Clustering: Found a split cluster with both unit-1-1 and unit-3-1 a
```

Cronologia cluster

Unità-1-1	Unità-2-1	Unità-3-1
Nessun evento	Nessun evento	<#root> 09:47:33 UTC Nov 2 2020 **Primary DISABLED Detected a splitted cluster** 09:47:38 UTC Nov 2 2020 DISABLED ELECTION Enabled from CLI 09:47:38 UTC Nov 2 2020 ELECTION SECONDARY_COLD Received cluster contro 09:47:38 UTC Nov 2 2020 SECONDARY_COLD SECONDARY_APP_SYNC Client progression 09:48:18 UTC Nov 2 2020 SECONDARY_APP_SYNC SECONDARY_CONFIG SECONDARY applicat 09:48:29 UTC Nov 2 2020 SECONDARY_CONFIG SECONDARY_FILESYS Configuration repl 09:48:30 UTC Nov 2 2020 SECONDARY_FILESYS SECONDARY_BULK_SYNC Client progression 09:48:54 UTC Nov 2 2020 SECONDARY_BULK_SYNC **SECONDARY** Client progression done

Scenario 2

Perdita di comunicazione CCL per circa 3-4 sec in entrambe le direzioni.

Prima dell'errore

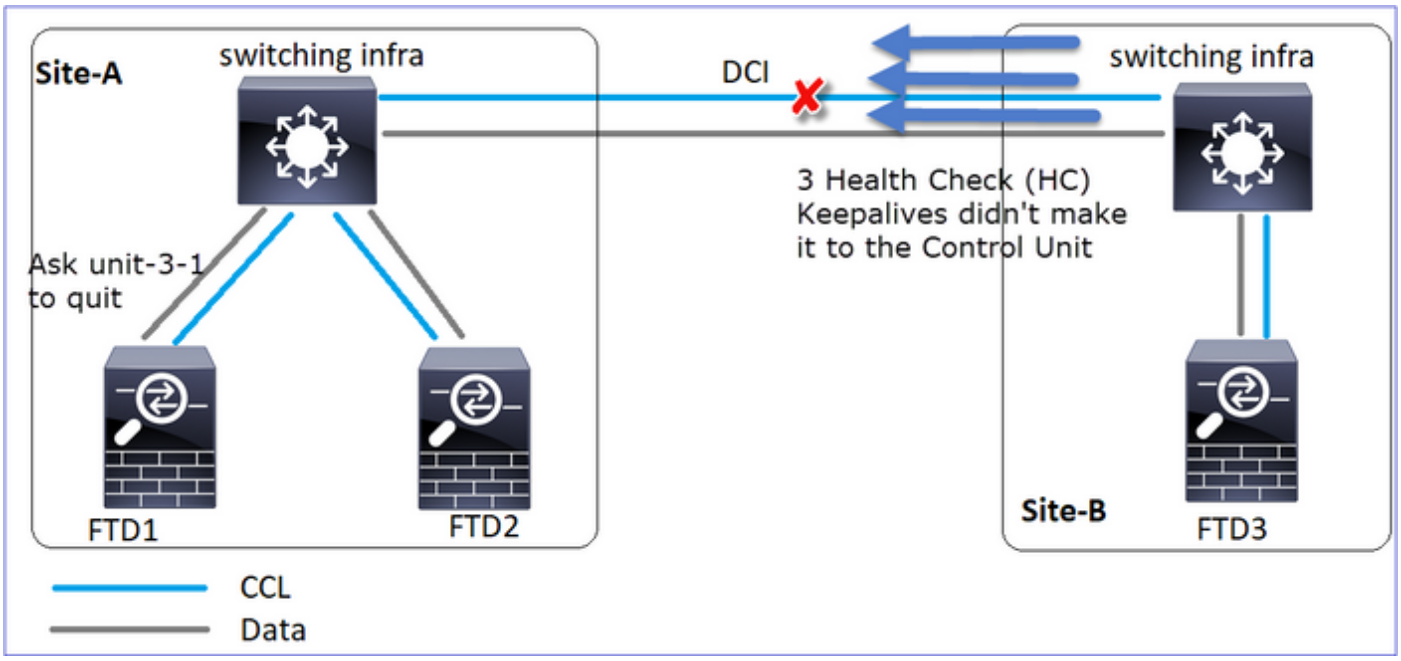
FTD1	FTD2	FTD3
Sito-A	Sito-A	Sito-B
Nodo di controllo	Nodo dati	Nodo dati

Dopo il ripristino (nessuna modifica nei ruoli delle unità)

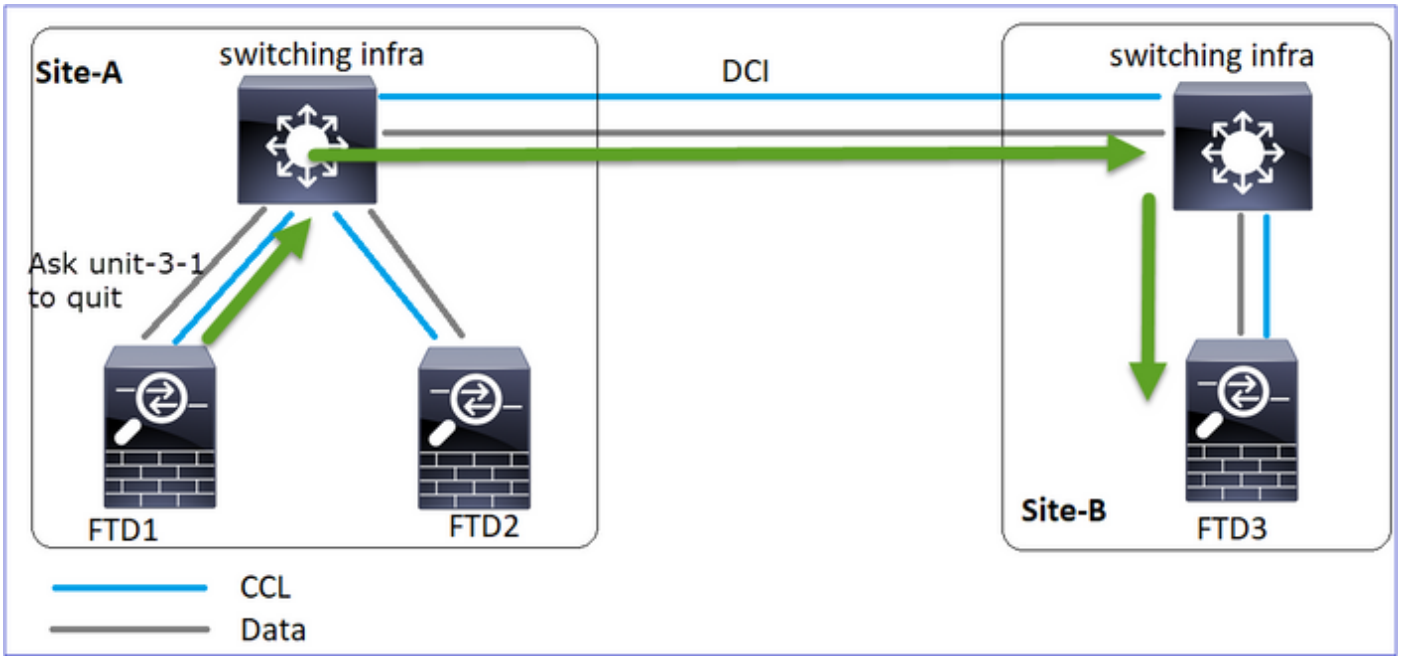
FTD1	FTD2	FTD3
Sito-A	Sito-A	Sito-B
Nodo di controllo	Nodo dati	Nodo dati

Analisi

Evento 1 Il nodo di controllo perde 3 HC dall'unità 3-1 e invia un messaggio all'unità 3-1 per lasciare il cluster.



Evento 2 La CCL si è ripresa molto velocemente e il messaggio CLUSTER_QUIT_REASON_STRAY_MEMBER dal nodo di controllo è arrivato sul lato remoto. L'unità 3-1 passa direttamente alla modalità DISABLED e non è presente la funzione split-brain



Nell'unità 1-1 (controllo) è possibile vedere:

<#root>

```
firepower#
Asking SECONDARY unit unit-3-1 to quit because it failed unit health-check.
```

Forcing stray member unit-3-1 to leave the cluster

Nell'unità 3-1 (nodo dati) vengono visualizzati:

<#root>

```
firepower#
```

Cluster disable

```
 is performing cleanup..done.
All data interfaces have been shutdown due to clustering being disabled. To recover either enable clust
```

Cluster unit unit-3-1 transitioned from SECONDARY to DISABLED

L'unità cluster 3-1 è passata a uno stato DISABLED e, una volta ripristinata la comunicazione CCL, viene nuovamente aggiunta come nodo dati:

```
<#root>

firepower#

show cluster history


20:58:40 UTC Nov 1 2020

SECONDARY                  DISABLED              Received control message DISABLE (stray member)


20:58:45 UTC Nov 1 2020
DISABLED              ELECTION              Enabled from CLI
20:58:45 UTC Nov 1 2020
ELECTION              SECONDARY_COLD            Received cluster control message
20:58:45 UTC Nov 1 2020
SECONDARY_COLD            SECONDARY_APP_SYNC        Client progression done
20:59:33 UTC Nov 1 2020
SECONDARY_APP_SYNC        SECONDARY_CONFIG          SECONDARY application configuration sync done
20:59:44 UTC Nov 1 2020
SECONDARY_CONFIG          SECONDARY_FILESYS         Configuration replication finished
20:59:45 UTC Nov 1 2020
SECONDARY_FILESYS         SECONDARY_BULK_SYNC       Client progression done
21:00:09 UTC Nov 1 2020

SECONDARY_BULK_SYNC       SECONDARY

                Client progression done
```

Scenario 3

Perdita di comunicazione CCL per circa 3-4 sec in entrambe le direzioni.

Prima del fallimento.

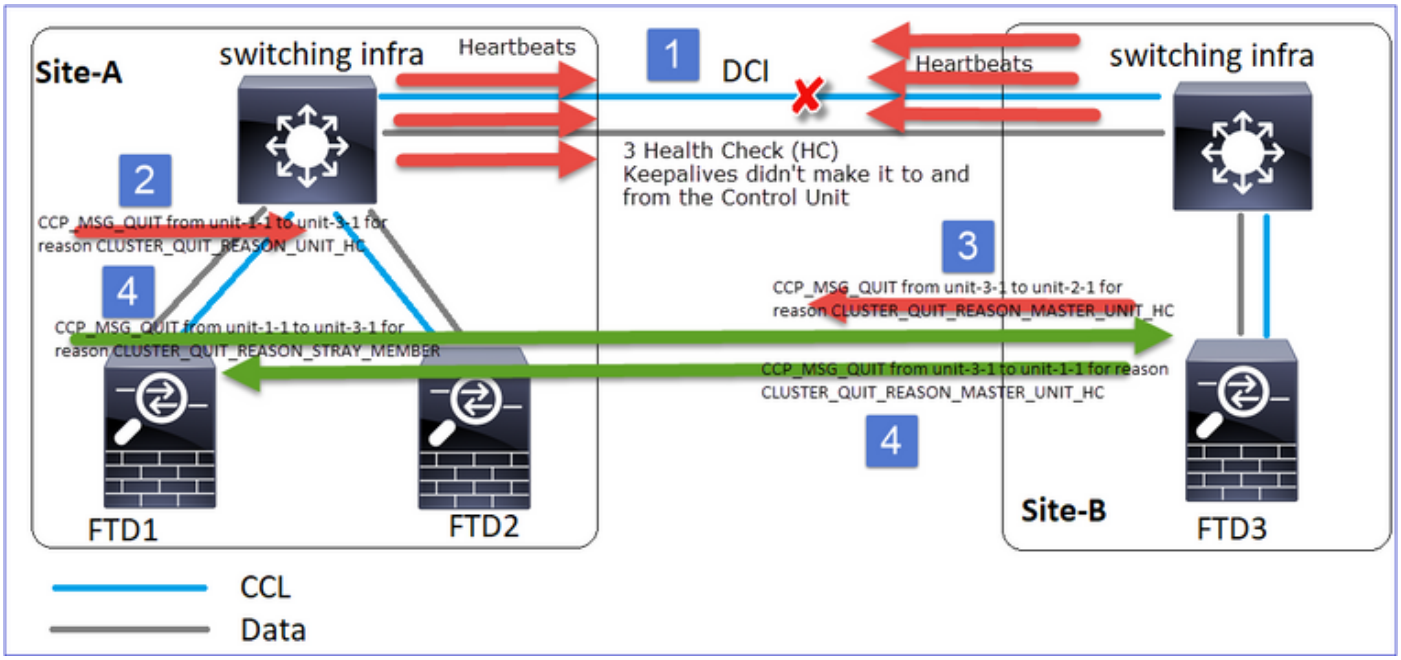
FTD1	FTD2	FTD3
Sito-A	Sito-A	Sito-B
Nodo di controllo	Nodo dati	Nodo dati

Dopo il ripristino (il nodo di controllo è stato modificato).

FTD1	FTD2	FTD3
Sito-A	Sito-A	Sito-B

Nodo dati	Nodo di controllo	Nodo dati

Analisi



1. CCL si abbassa.
2. L'unità 1-1 non riceve messaggi 3 HC dall'unità 3-1 e invia un messaggio QUIT all'unità 3-1. Questo messaggio non raggiunge mai l'unità 3-1.
3. L'unità 3-1 invia un messaggio QUIT all'unità 2-1. Questo messaggio non raggiunge mai l'unità 2-1.

Recupero CCL.

4. L'unità-1-1 vede che l'unità-3-1 si è annunciata come nodo di controllo e invia il messaggio QUIT_REASON_STRAY_MEMBER all'unità-3-1. Quando l'unità-3-1 ottiene questo messaggio passa allo stato DISABLED. Allo stesso tempo, l'unità 3-1 invia un messaggio QUIT_REASON_PRIMARY_UNIT_HC all'unità 1-1 e gli chiede di uscire. Una volta che l'unità 1-1 riceve questo messaggio, passa allo stato DISABLED.

Cronologia cluster

Unità-1-1
<#root> 19:53:09 UTC Nov 2 2020 **PRIMARY DISABLED** Received control message DISABLE (primary unit health check failure)

```
19:53:13 UTC Nov 2 2020
DISABLED              ELECTION         Enabled from CLI
19:53:13 UTC Nov 2 2020
ELECTION              SECONDARY_COLD       Received cluster control message
19:53:13 UTC Nov 2 2020
SECONDARY_COLD            SECONDARY_APP_SYNC   Client progression done
19:54:01 UTC Nov 2 2020
SECONDARY_APP_SYNC        SECONDARY_CONFIG     SECONDARY application configur
19:54:12 UTC Nov 2 2020
SECONDARY_CONFIG          SECONDARY_FILESYS    Configuration replication fini
19:54:13 UTC Nov 2 2020
SECONDARY_FILESYS         SECONDARY_BULK_SYNC  Client progression done
19:54:37 UTC Nov 2 2020
SECONDARY_BULK_SYNC

      SECONDARY

           Client progression done
```

Scenario 4

Perdita di comunicazione CCL per circa 3-4 sec

Prima dell'errore

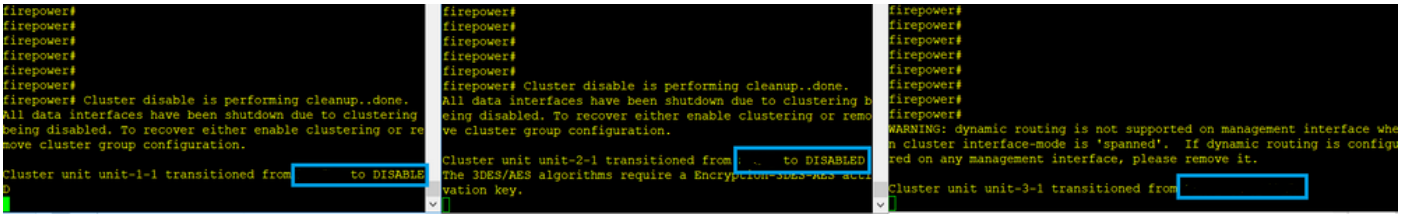
FTD1	FTD2	FTD3
Sito-A	Sito-A	Sito-B
Nodo di controllo	Nodo dati	Nodo dati

Dopo il ripristino (il nodo di controllo ha modificato i siti)

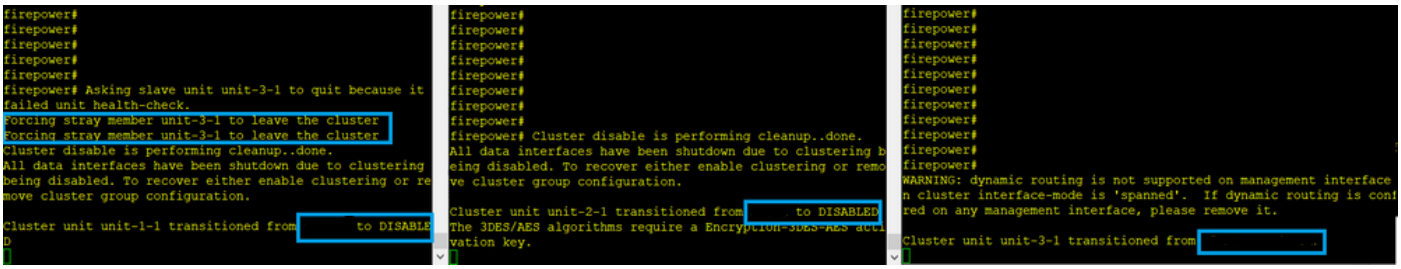
FTD1	FTD2	FTD3
Sito-A	Sito-A	Sito-B
Nodo dati	Nodo dati	Nodo di controllo

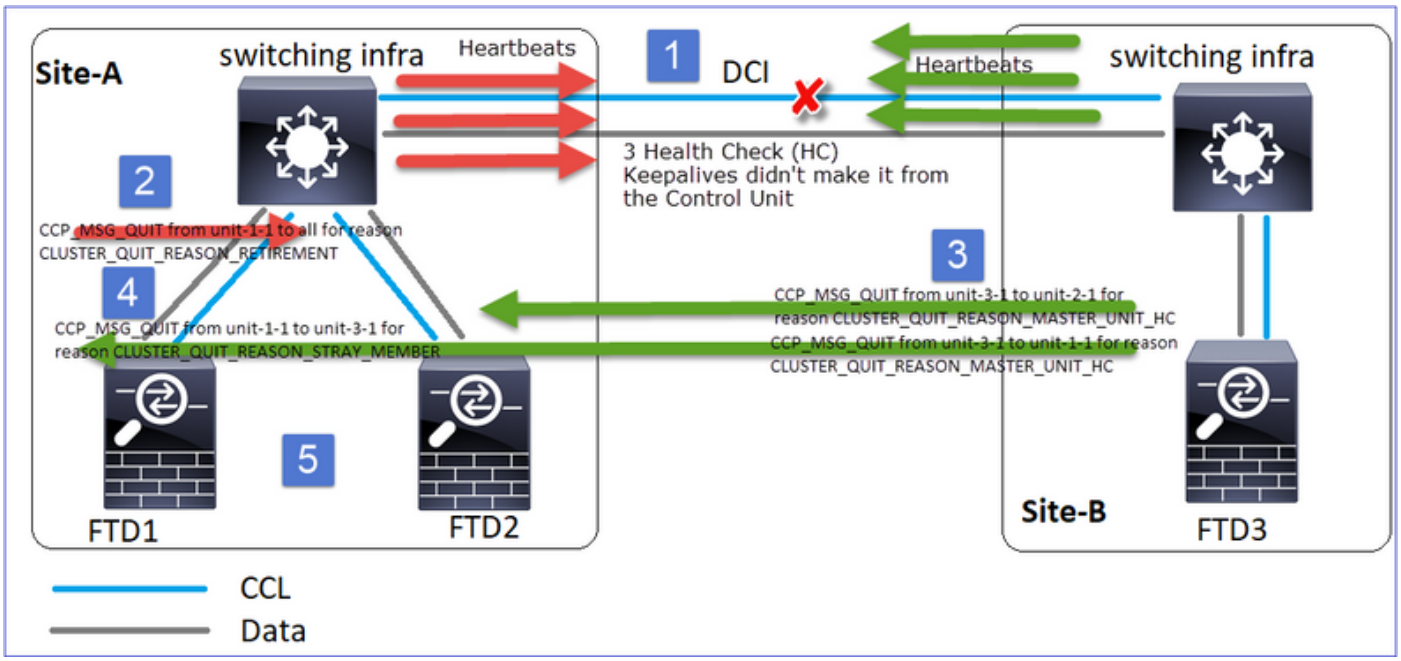
Analisi

Il fallimento

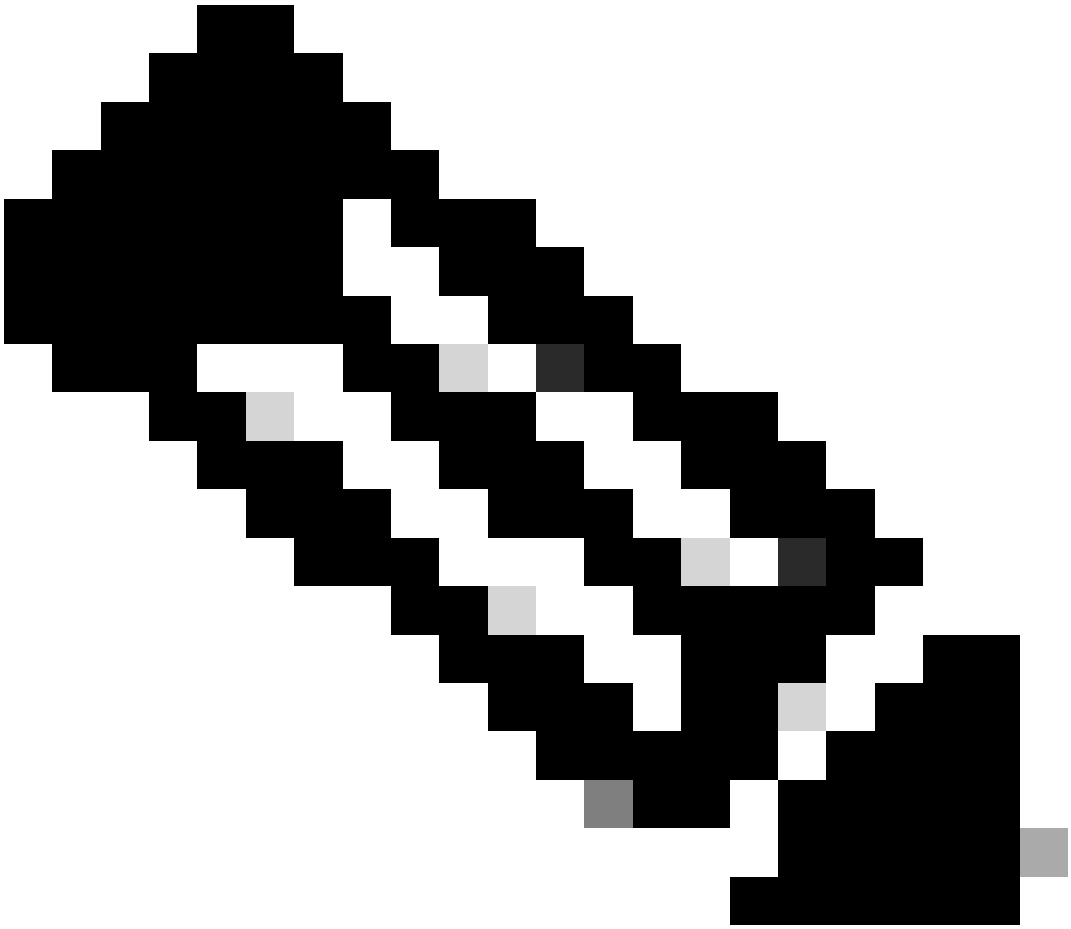


Un gusto diverso dello stesso errore. In questo caso, l'unità-1-1 non ha ricevuto messaggi 3 HC dall'unità-3-1, e una volta che ha ricevuto un nuovo keepalive, ha cercato di buttare fuori l'unità-3-1 con l'uso di un messaggio STRAY, ma il messaggio non è mai arrivato all'unità-3-1:





1. CCL diventa unidirezionale per alcuni secondi. L'unità 3-1 non riceve messaggi 3 HC dall'unità 1-1 e diventa un nodo di controllo.
2. L'unità 2-1 invia un messaggio CLUSTER_QUIT_REASON_RETIREMENT (broadcast).
3. L'unità 3-1 invia un messaggio QUIT_REASON_PRIMARY_UNIT_HC all'unità 2-1. L'unità 2-1 lo riceve e chiude il cluster.
4. L'unità 3-1 invia un messaggio QUIT_REASON_PRIMARY_UNIT_HC all'unità 1-1. L'unità 1-1 lo riceve e chiude il cluster. Recupero CCL.
5. Le unità 1-1 e 2-1 si uniscono nuovamente al cluster come nodi di dati.



> Nota: Se nel passo 5 la CCL non si riprende, nel sito A l'FTD1 diventa il nuovo nodo di controllo e, dopo il recupero della CCL, vince la nuova scelta.

Messaggi syslog sull'unità 1-1:

<#root>

```
firepower#
```

show log | include 747

```
Nov 03 2020 23:13:08: %FTD-7-747005: Clustering: State machine notify event CLUSTER_EVENT_MEMBER_STATE
Nov 03 2020 23:13:09: %FTD-4-747015: Clustering: Forcing stray member unit-3-1 to leave the cluster
Nov 03 2020 23:13:09: %FTD-7-747005: Clustering: State machine notify event CLUSTER_EVENT_MEMBER_STATE
Nov 03 2020 23:13:10: %FTD-4-747015: Clustering: Forcing stray member unit-3-1 to leave the cluster
Nov 03 2020 23:13:10: %FTD-6-747004: Clustering:
```

State machine changed from state PRIMARY to DISABLED

```
Nov 03 2020 23:13:12: %FTD-7-747006: Clustering: State machine is at state DISABLED
Nov 03 2020 23:13:12: %FTD-7-747005: Clustering: State machine notify event CLUSTER_EVENT_MY_STATE (sta
Nov 03 2020 23:13:18: %FTD-6-747004: Clustering: State machine changed from state ELECTION to ONCALL
```

Log di traccia del cluster sull'unità 1-1:

<#root>

```
firepower#
```

show cluster info trace | include QUIT

```
Nov 03 23:13:10.789 [DBUG]Send CCP message to all: CCP_MSG_QUIT from unit-1-1 for reason CLUSTER_QUIT_R
Nov 03 23:13:10.769 [DBUG]
```

Receive CCP message: CCP_MSG_QUIT from unit-3-1 to unit-1-1 for reason CLUSTER_QUIT_REASON_PRIMARY_UNIT_

```
Nov 03 23:13:10.769 [DBUG]Send CCP message to id 1: CCP_MSG_QUIT from unit-1-1 to unit-3-1 for reason C
Nov 03 23:13:09.789 [DBUG]Receive CCP message: CCP_MSG_QUIT from unit-2-1 for reason CLUSTER_QUIT_REASO
Nov 03 23:13:09.769 [DBUG]Send CCP message to id 1: CCP_MSG_QUIT from unit-1-1 to unit-3-1 for reason C
Nov 03 23:13:08.559 [DBUG]Send CCP message to all: CCP_MSG_QUIT from unit-1-1 to unit-3-1 for reason CL
Nov 03 23:13:08.559 [DBUG]Send CCP message to id 1: CCP_MSG_QUIT from unit-1-1 to unit-3-1 for reason C
```

Messaggi syslog sull'unità 3-1:

<#root>

```
firepower#
```

show log | include 747

```
Nov 03 2020 23:13:09: %FTD-7-747005: Clustering: State machine notify event CLUSTER_EVENT_MEMBER_STATE
Nov 03 2020 23:13:10: %FTD-7-747005: Clustering: State machine notify event CLUSTER_EVENT_MEMBER_STATE
Nov 03 2020 23:13:10: %FTD-6-747004: Clustering:
```

State machine changed from state SECONDARY to PRIMARY

```
Nov 03 2020 23:13:10: %FTD-6-747004: Clustering: State machine changed from state PRIMARY_FAST to PRIMA
Nov 03 2020 23:13:10: %FTD-6-747004: Clustering: State machine changed from state PRIMARY_DRAIN to PRIM
Nov 03 2020 23:13:10: %FTD-6-747004: Clustering: State machine changed from state PRIMARY_CONFIG to PRI
Nov 03 2020 23:13:10: %FTD-7-747006: Clustering: State machine is at state PRIMARY_POST_CONFIG
```

```
Nov 03 2020 23:13:10: %FTD-6-747004: Clustering: State machine changed from state PRIMARY_POST_CONFIG t
Nov 03 2020 23:13:10: %FTD-7-747006: Clustering:
```

State machine is at state PRIMARY

Cronologia cluster

Unità-1-1
<#root> 23:13:13 UTC Nov 3 2020 **PRIMARY DISABLED Received control message DISABLE** **(primary unit health check failure)** 23:13:18 UTC Nov 3 2020 DISABLED ELECTION Enabled from CLI 23:13:18 UTC Nov 3 2020 ELECTION ONCALL Received cluster control message 23:13:23 UTC Nov 3 2020 ONCALL ELECTION Received cluster control message … 23:14:48 UTC Nov 3 2020 ONCALL ELECTION Received cluster control message 23:14:48 UTC Nov 3 2020 ELECTION SECONDARY_COLD Received cluster control message 23:14:48 UTC Nov 3 2020 SECONDARY_COLD SECONDARY_APP_SYNC Client progression done 23:15:36 UTC Nov 3 2020 SECONDARY_APP_SYNC SECONDARY_CONFIG SECONDARY application configuration sync done 23:15:48 UTC Nov 3 2020 SECONDARY_CONFIG SECONDARY_FILESYS Configuration replication finished 23:15:49 UTC Nov 3 2020 SECONDARY_FILESYS SECONDARY_BULK_SYNC Client progression done 23:16:13 UTC Nov 3 2020 SECONDARY_BULK_SYNC **SECONDARY** Client progression done

Scenario 5

Prima dell'errore

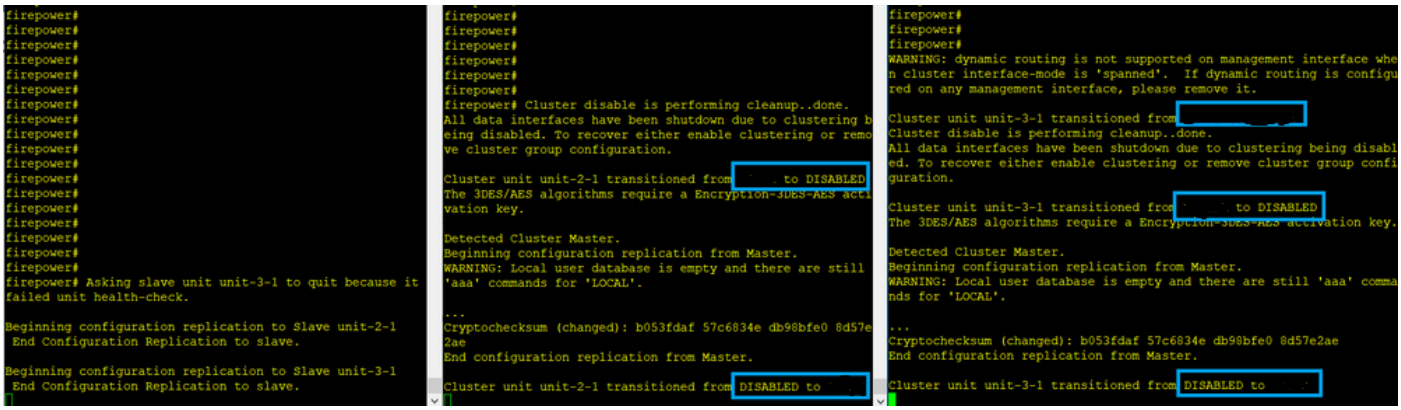
FTD1	FTD2	FTD3

Sito-A	Sito-A	Sito-B
Nodo di controllo	Nodo dati	Nodo dati

Dopo il ripristino (nessuna modifica)

FTD1	FTD2	FTD3
Sito-A	Sito-A	Sito-B
Nodo di controllo	Nodo dati	Nodo dati

Il fallimento



L'unità 3-1 ha inviato messaggi QUIT sia all'unità 1-1 che all'unità 2-1, ma, a causa di problemi di connettività, solo l'unità 2-1 ha ricevuto il messaggio QUIT.

Registri di traccia cluster unità 1-1:

<#root>

```
firepower#
```

show cluster info trace | include QUIT

```
Nov 04 00:52:10.429 [DBUG]Receive CCP message: CCP_MSG_QUIT from unit-3-1 for reason CLUSTER_QUIT_REASO
Nov 04 00:51:47.059 [DBUG]Receive CCP message: CCP_MSG_QUIT from unit-2-1 for reason CLUSTER_QUIT_REASO
Nov 04 00:51:45.429 [DBUG]Send CCP message to all: CCP_MSG_QUIT from unit-1-1 to unit-3-1 for reason CL
Nov 04 00:51:45.429 [DBUG]Send CCP message to unit-3-1(1): CCP_MSG_QUIT from unit-1-1 to unit-3-1 for r
```

Registri di traccia cluster unità 2-1:

<#root>

firepower#

show cluster info trace | include QUIT

Nov 04 00:52:10.389 [DBUG]Receive CCP message: CCP_MSG_QUIT from unit-3-1 for reason CLUSTER_QUIT_REASO
Nov 04 00:51:47.019 [DBUG]Send CCP message to all: CCP_MSG_QUIT from unit-2-1 for reason CLUSTER_QUIT_R
Nov 04 00:51:46.999 [DBUG]

Receive CCP message: CCP_MSG_QUIT from unit-3-1 to unit-2-1 for reason CLUSTER_QUIT_REASON_PRIMARY_UNIT_

Nov 04 00:51:45.389 [DBUG]Receive CCP message: CCP_MSG_QUIT from unit-1-1 to unit-3-1 for reason CLUSTE

Cronologia cluster

Unità-1-1	Unità-2-1
Nessun evento	<#root> 00:51:50 UTC Nov 4 2020 **SECONDARY DISABLED Received control message DISABLE** **(primary unit health check failure)** 00:51:54 UTC Nov 4 2020 DISABLED ELECTION Enabled from CLI 00:51:54 UTC Nov 4 2020 ELECTION SECONDARY_COLD Received cluster control message 00:51:54 UTC Nov 4 2020 SECONDARY_COLD SECONDARY_APP_SYNC Client progression done 00:52:42 UTC Nov 4 2020 SECONDARY_APP_SYNC SECONDARY_CONFIG SECONDARY application configu sync done 00:52:54 UTC Nov 4 2020 SECONDARY_CONFIG SECONDARY_FILESYS Configuration replication fir 00:52:55 UTC Nov 4 2020 SECONDARY_FILESYS SECONDARY_BULK_SYNC Client progression done 00:53:19 UTC Nov 4 2020 SECONDARY_BULK_SYNC **SECONDARY** Client progression done

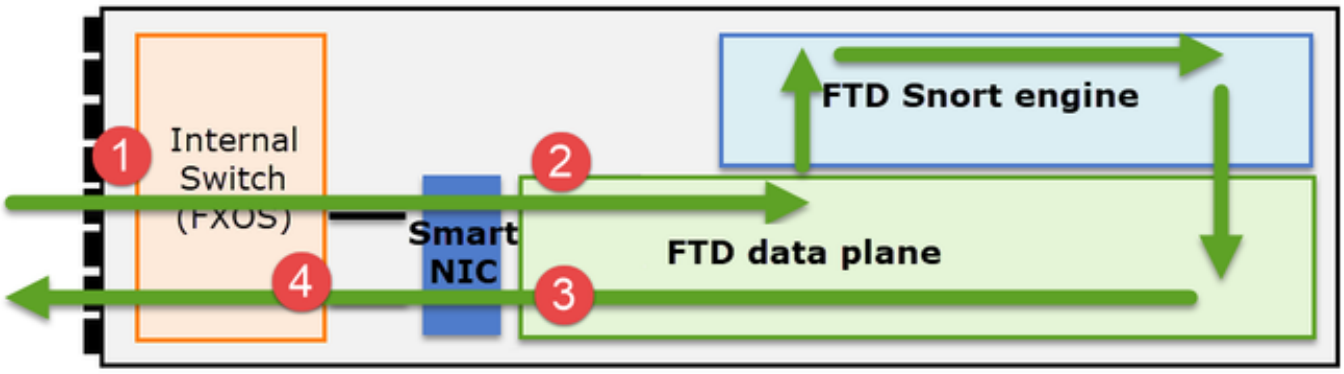
Installazione connessione Data Plane cluster

Punti di acquisizione NGFW

NGFW fornisce funzionalità di acquisizione su questi punti:

- Switch interno per chassis (FXOS)
- motore del piano dati FTD
- FTD Motore Snort

Quando si risolvono i problemi relativi ai percorsi dati in un cluster, nella maggior parte dei casi vengono utilizzati i punti di acquisizione acquisiti dal motore del piano dati FXOS e FTD.



1. Acquisizione FXOS in entrata sull'interfaccia fisica
2. Acquisizione in ingresso FTD nel motore del piano dati
3. Acquisizione in uscita FTD nel motore del piano dati
4. Acquisizione in entrata FXOS sull'interfaccia del backplane

Per ulteriori informazioni sulle acquisizioni NGFW, consultare questo documento:

Nozioni di base sui ruoli del flusso di unità del cluster

Le connessioni possono essere stabilite tramite un cluster in diversi modi, a seconda di fattori quali:

- Tipo di traffico (TCP, UDP, ecc.)
- Algoritmo di bilanciamento del carico configurato sullo switch adiacente
- Funzionalità configurate sul firewall
- Condizioni di rete (ad esempio, frammentazione IP, ritardi della rete e così via)

Ruolo Flusso	Descrizione	Contrassegno/i

Proprietario	In genere, l'unità che riceve inizialmente la connessione	UIO
Direttore	Unità che gestisce le richieste di ricerca del proprietario dai server d'inoltro.	Y
Proprietario backup	Finché il director non è la stessa unità del proprietario, il director è anche il proprietario del backup. Se il proprietario sceglie se stesso come director, viene scelto un proprietario di backup separato.	Y (se la directory è anche il proprietario del backup) y (se la directory non è il proprietario del backup)
Inoltro	Unità che inoltra i pacchetti al proprietario	z
Proprietario frammento	Unità che gestisce il traffico frammentato	-
Backup dello chassis	In un cluster tra chassis, quando i flussi di director/backup e proprietari sono di proprietà delle unità dello stesso chassis, un'unità in uno degli altri chassis diventa un backup/director secondario. Questo ruolo è specifico per i cluster tra chassis di Firepower serie 9300 con più di un blade.	s

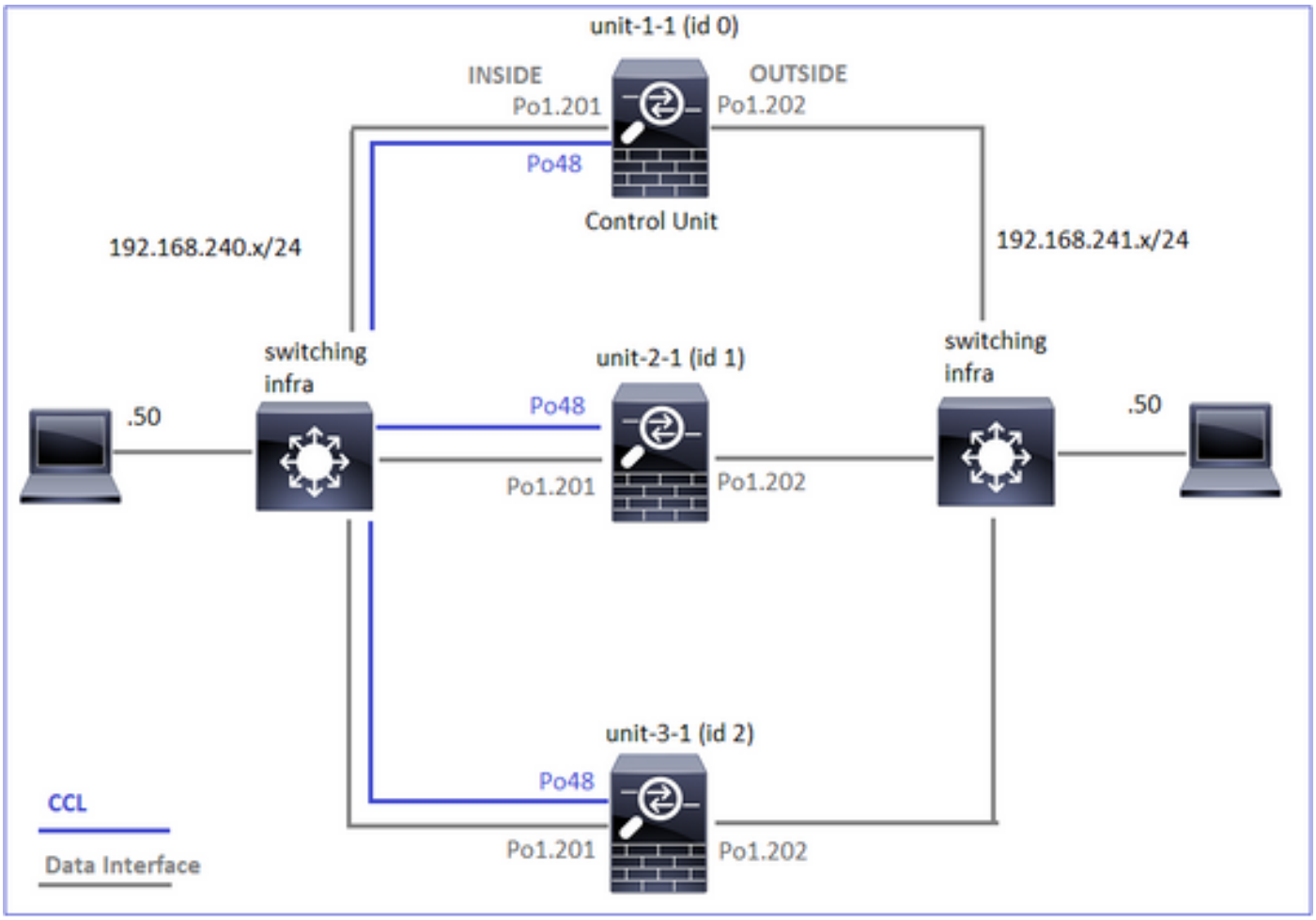
- Per ulteriori informazioni, consultare la sezione correlata nella Guida alla configurazione (vedere i collegamenti nelle Informazioni correlate)
- In scenari specifici (vedere la sezione studi di casi) alcuni flag non sono sempre visualizzati.

Casi aziendali relativi all'istituzione di connessioni cluster

Nella sezione successiva vengono illustrati vari casi aziendali che dimostrano alcuni dei modi in cui è possibile stabilire una connessione tramite un cluster. Gli obiettivi sono i seguenti:

- Acquisire familiarità con i diversi ruoli delle unità.
- Dimostrare come è possibile correlare i vari output del comando.

Topologia



ID e unità cluster:

Unità-1-1	Unità-2-1
<#root> Cluster GROUP1: On Interface mode: spanned **This is "unit-1-1" in state PRIMARY** **ID : 0** Site ID : 1 Version : 9.15(1) Serial No.: FCH22247LNK CCL IP : 10.17.1.1 CCL MAC : 0015.c500.018f Last join : 02:24:43 UTC Nov 27 2020	<#root> **Unit "unit-2-1" in state SECO** **ID : 1** Site ID : 1 Version : 9.15(1) Serial No.: FCH23157Y9N CCL IP : 10.17.2.1 CCL MAC : 0015.c500.02 Last join : 02:04:19 UTC Last leave: N/A

Last leave: N/A	

Acquisizioni cluster abilitate:

```
cluster exec cap CAPI int INSIDE buffer 33554432 match tcp host 192.168.240.50 host 192.168.241.50 eq 8
cluster exec cap CAPO int OUTSIDE buffer 33554432 match tcp host 192.168.240.50 host 192.168.241.50 eq
cluster exec cap CAPI_RH reinject-hide int INSIDE buffer 33554432 match tcp host 192.168.240.50 host 19
cluster exec cap CAPO_RH reinject-hide int OUTSIDE buffer 33554432 match tcp host 192.168.240.50 host 1
cluster exec cap CCL int cluster buffer 33554432
```

Nota: Questi test sono stati eseguiti in un ambiente lab con traffico minimo attraverso il cluster. Nella produzione, cercare di usare filtri di acquisizione il più possibile specifici (ad esempio, la porta di destinazione e, quando possibile, la porta di origine) per ridurre al minimo il "rumore" nelle riprese.

Caso di studio 1. Traffico simmetrico (il proprietario è anche il direttore)

Osservazione 1. Le clip reject-hide mostrano i pacchetti solo sull'unità 1-1. Ciò significa che il flusso in entrambe le direzioni ha attraversato l'unità 1-1 (traffico simmetrico):

<#root>

```
firepower#
```

cluster exec show cap

```
unit-1-1(LOCAL):*******************************************************
capture CCL type raw-data interface cluster [Capturing - 33513 bytes]
capture CAPI type raw-data buffer 33554432 trace interface INSIDE [Buffer Full - 33553914 bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq 80
capture CAPO type raw-data buffer 33554432 trace interface OUTSIDE [Buffer Full - 33553914 bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq 80
capture CAPI_RH type raw-data
```

reinject-hide

```
 buffer 33554432 interface INSIDE [Buffer Full -
```

33553914 bytes

```
]
match tcp host 192.168.240.50 host 192.168.241.50 eq 80
capture CAPO_RH type raw-data
```

reinject-hide

```
 buffer 33554432 interface OUTSIDE [Buffer Full -
```

33553914 bytes

```
]
match tcp host 192.168.240.50 host 192.168.241.50 eq 80
```

```
unit-2-1:************************************************************
capture CCL type raw-data interface cluster [Capturing - 23245 bytes]
capture CAPI type raw-data buffer 33554432 trace interface INSIDE [Capturing - 0 bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq 80
capture CAPO type raw-data buffer 33554432 trace interface OUTSIDE [Capturing - 0 bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq 80
capture CAPI_RH type raw-data
reinject-hide
 buffer 33554432 interface INSIDE [Capturing -
0 bytes
]
match tcp host 192.168.240.50 host 192.168.241.50 eq 80
capture CAPO_RH type raw-data
reinject-hide
 buffer 33554432 interface OUTSIDE [Capturing -
0 bytes
]
match tcp host 192.168.240.50 host 192.168.241.50 eq 80

unit-3-1:************************************************************
capture CCL type raw-data interface cluster [Capturing - 24815 bytes]
capture CAPI type raw-data buffer 33554432 trace interface INSIDE [Capturing - 0 bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq 80
capture CAPO type raw-data buffer 33554432 trace interface OUTSIDE [Capturing - 0 bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq 80
capture CAPI_RH type raw-data
reinject-hide
 buffer 33554432 interface INSIDE [Capturing -
0 bytes
]
match tcp host 192.168.240.50 host 192.168.241.50 eq 80
capture CAPO_RH type raw-data
reinject-hide
 buffer 33554432 interface OUTSIDE [Capturing -
0 bytes
]
match tcp host 192.168.240.50 host 192.168.241.50 eq 80
```

Osservazione 2. Analisi del flag di connessione per il flusso con porta di origine 45954

<#root>

```
firepower#
cluster exec show conn
```

```
unit-1-1(LOCAL):*******************************************************
22 in use, 25 most used
Cluster:
fwd connections: 0 in use, 1 most used
dir connections: 0 in use, 122 most used
centralized connections: 0 in use, 0 most used
VPN redirect connections: 0 in use, 0 most used
Inspect Snort:
preserve-connection: 1 enabled, 0 in effect, 2 most enabled, 1 most in effect

TCP OUTSIDE 192.168.241.50:80 INSIDE 192.168.240.50:
```

45954

```
, idle 0:00:00, bytes 487413076,
```

flags UIO N1

```
unit-2-1:*************************************************************
22 in use, 271 most used
Cluster:
fwd connections: 0 in use, 2 most used
dir connections: 0 in use, 2 most used
centralized connections: 0 in use, 0 most used
VPN redirect connections: 0 in use, 0 most used
Inspect Snort:
preserve-connection: 1 enabled, 0 in effect, 249 most enabled, 0 most in effect

unit-3-1:*************************************************************
17 in use, 20 most used
Cluster:
fwd connections: 1 in use, 2 most used
dir connections: 1 in use, 127 most used
centralized connections: 0 in use, 0 most used
VPN redirect connections: 0 in use, 0 most used
Inspect Snort:
preserve-connection: 0 enabled, 0 in effect, 1 most enabled, 0 most in effect

TCP OUTSIDE 192.168.241.50:443 NP Identity Ifc 192.168.240.50:39698, idle 0:00:23, bytes 0, flags z
TCP OUTSIDE 192.168.241.50:80 INSIDE 192.168.240.50:
```

45954

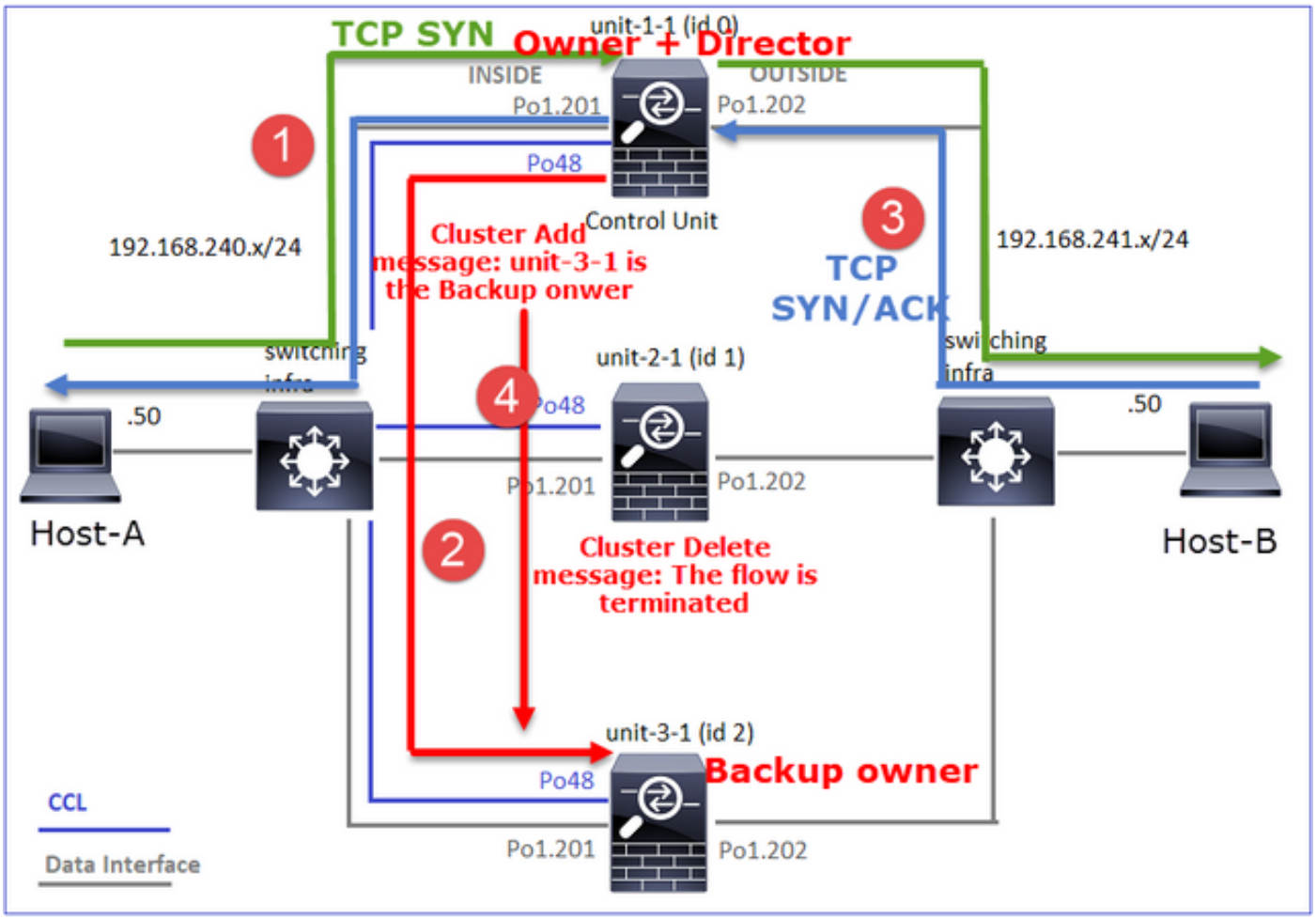
```
, idle 0:00:06, bytes 0,
```

flags y

Unità	Contrassegna	Nota
Unità-1-1	UIO	· Proprietario flusso: l'unità gestisce il flusso · Direttore - Poiché l'unità 3-1 ha "y" e non "Y", ciò implica che l'unità 1-1 è stata scelta come direttore per questo flusso. Pertanto, poiché è anche il proprietario, un'altra unità (in questo caso l'unità 3-1) è stata scelta come proprietario del backup

Unità-2-1	-	-
Unità-3-1	y	L'unità è proprietaria di un backup

Ciò può essere visualizzato come:



1. Il pacchetto TCP SYN arriva dall'host A all'unità 1 1. L'unità 1 1 diventa il proprietario del flusso.
2. Anche l'unità 1-1 viene selezionata come director di flusso. Pertanto, seleziona anche l'unità 3-1 come proprietario del backup (messaggio di aggiunta cluster).
3. Il pacchetto TCP SYN/ACK arriva dall'host-B all'unità-3-1. Il flusso è simmetrico.
4. Una volta terminata la connessione, il proprietario invia un messaggio di eliminazione del cluster per rimuovere le informazioni sul flusso dal proprietario del backup.

Osservazione 3. La cattura con traccia indica che entrambe le direzioni attraversano solo l'unità 1-1.

Passaggio 1. Identificare il flusso e i pacchetti di interesse in tutte le unità cluster in base alla porta di origine:

<#root>

```
firepower#
cluster exec show capture CAPI | i 45954


unit-1-1(LOCAL):*******************************************************
1: 08:42:09.362697 802.1Q vlan#201 P0 192.168.240.50.45954 > 192.168.241.50.80: S 992089269:992089269(0)
2: 08:42:09.363521 802.1Q vlan#201 P0 192.168.241.50.80 > 192.168.240.50.45954: S 4042762409:4042762409
3: 08:42:09.363827 802.1Q vlan#201 P0 192.168.240.50.45954 > 192.168.241.50.80: . ack 4042762410 win 22
…
unit-2-1:*******************************************************

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

<#root>

```
firepower#
cluster exec show capture CAPO | i 45954


unit-1-1(LOCAL):*******************************************************
1: 08:42:09.362987 802.1Q vlan#202 P0 192.168.240.50.45954 > 192.168.241.50.80: S 2732339016:2732339016
2: 08:42:09.363415 802.1Q vlan#202 P0 192.168.241.50.80 > 192.168.240.50.45954: S 3603655982:3603655982
3: 08:42:09.363903 802.1Q vlan#202 P0 192.168.240.50.45954 > 192.168.241.50.80: . ack 3603655983 win 22
…
unit-2-1:*******************************************************

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

Passaggio 2. Poiché si tratta di una traccia di flusso TCP, i pacchetti di handshake a 3 vie. Come si può vedere in questo output, l'unità-1-1 è il proprietario. Per semplicità, le fasi di analisi non pertinenti sono omesse:

<#root>

```
firepower#
show cap CAPI packet-number 1 trace


25985 packets captured
1: 08:42:09.362697 802.1Q vlan#201 P0 192.168.240.50.
45954
 > 192.168.241.50.80:
S
 992089269:992089269(0) win 29200 <mss 1460,sackOK,timestamp 495153655 0,nop,wscale 7>
...
Phase: 4
```

Type: CLUSTER-EVENT

Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'INSIDE'

Flow type: NO FLOW

I (0) got initial, attempting ownership.

Phase: 5

Type: CLUSTER-EVENT

Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'INSIDE'
Flow type: NO FLOW

I (0) am becoming owner

...

Traffico di ritorno (TCP SYN/ACK):

<#root>

firepower#

show capture CAPO packet-number 2 trace

25985 packets captured
2: 08:42:09.363415 802.1Q vlan#202 P0 192.168.241.50.80 > 192.168.240.50.45954:

S

3603655982:3603655982(0)

ack

2732339017 win 28960 <mss 1460,sackOK,timestamp 505509125 495153655,nop,wscale 7>
...
Phase: 3

Type: FLOW-LOOKUP

```
Subtype:
Result: ALLOW
Config:
Additional Information:
```

Found flow with id 9364, using existing flow

Osservazione 4. I syslog del piano dati FTD mostrano la creazione e la terminazione della connessione su tutte le unità:

<#root>

```
firepower#
```

cluster exec show log | include 45954

unit-1-1

```
(LOCAL):*******************************************************
Dec 01 2020 08:42:09: %FTD-6-302013:
```

Built inbound TCP connection 9364

```
 for INSIDE:192.168.240.50/45954 (192.168.240.50/45954) to OUTSIDE:192.168.241.50/80 (192.168.241.50/80)
Dec 01 2020 08:42:18: %FTD-6-302014:
```

Teardown TCP connection 9364

```
 for INSIDE:192.168.240.50/45954 to OUTSIDE:192.168.241.50/80 duration 0:00:08 bytes 1024000440 TCP FIN

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

unit-3-1

```
:*************************************************************
Dec 01 2020 08:42:09: %FTD-6-302022:
```

Built backup stub TCP connection

```
 for INSIDE:192.168.240.50/45954 (192.168.240.50/45954) to OUTSIDE:192.168.241.50/80 (192.168.241.50/80)
Dec 01 2020 08:42:18: %FTD-6-302023:
```

Teardown backup TCP connection

```
 for INSIDE:192.168.240.50/45954 to OUTSIDE:192.168.241.50/80 duration 0:00:08 forwarded bytes 0 Cluste
```

Caso di studio 2. Traffico simmetrico (proprietario diverso dal director)

- Come il caso di studio n. 1, ma in questo caso di studio il proprietario di un flusso è un'unità diversa da quella del direttore.
- Tutti i risultati sono simili al caso di studio n. 1. La differenza principale rispetto al caso di studio n. 1 è il flag "Y" che sostituisce il flag "y" dello scenario 1.

Osservazione 1. Il proprietario è diverso dal direttore.

Analisi del flag di connessione per il flusso con la porta di origine 46278.

<#root>

firepower#

cluster exec show conn

unit-1-1(LOCAL):***
23 in use, 25 most used
Cluster:
fwd connections: 0 in use, 1 most used
dir connections: 0 in use, 122 most used
centralized connections: 0 in use, 0 most used
VPN redirect connections: 0 in use, 0 most used
Inspect Snort:
preserve-connection: 2 enabled, 0 in effect, 4 most enabled, 1 most in effect

TCP OUTSIDE 192.168.241.50:80 INSIDE 192.168.240.50:

46278

, idle 0:00:00, bytes 508848268, flags

UIO N1

TCP OUTSIDE 192.168.241.50:80 INSIDE 192.168.240.50:46276, idle 0:00:03, bytes 0, flags aA N1

unit-2-1:***
21 in use, 271 most used
Cluster:
fwd connections: 0 in use, 2 most used
dir connections: 0 in use, 2 most used
centralized connections: 0 in use, 0 most used
VPN redirect connections: 0 in use, 0 most used
Inspect Snort:
preserve-connection: 0 enabled, 0 in effect, 249 most enabled, 0 most in effect

unit-3-1:***
17 in use, 20 most used
Cluster:
fwd connections: 1 in use, 5 most used
dir connections: 1 in use, 127 most used
centralized connections: 0 in use, 0 most used
VPN redirect connections: 0 in use, 0 most used
Inspect Snort:
preserve-connection: 0 enabled, 0 in effect, 1 most enabled, 0 most in effect

TCP OUTSIDE 192.168.241.50:80 NP Identity Ifc 192.168.240.50:46276, idle 0:00:02, bytes 0, flags z
TCP OUTSIDE 192.168.241.50:80 INSIDE 192.168.240.50:

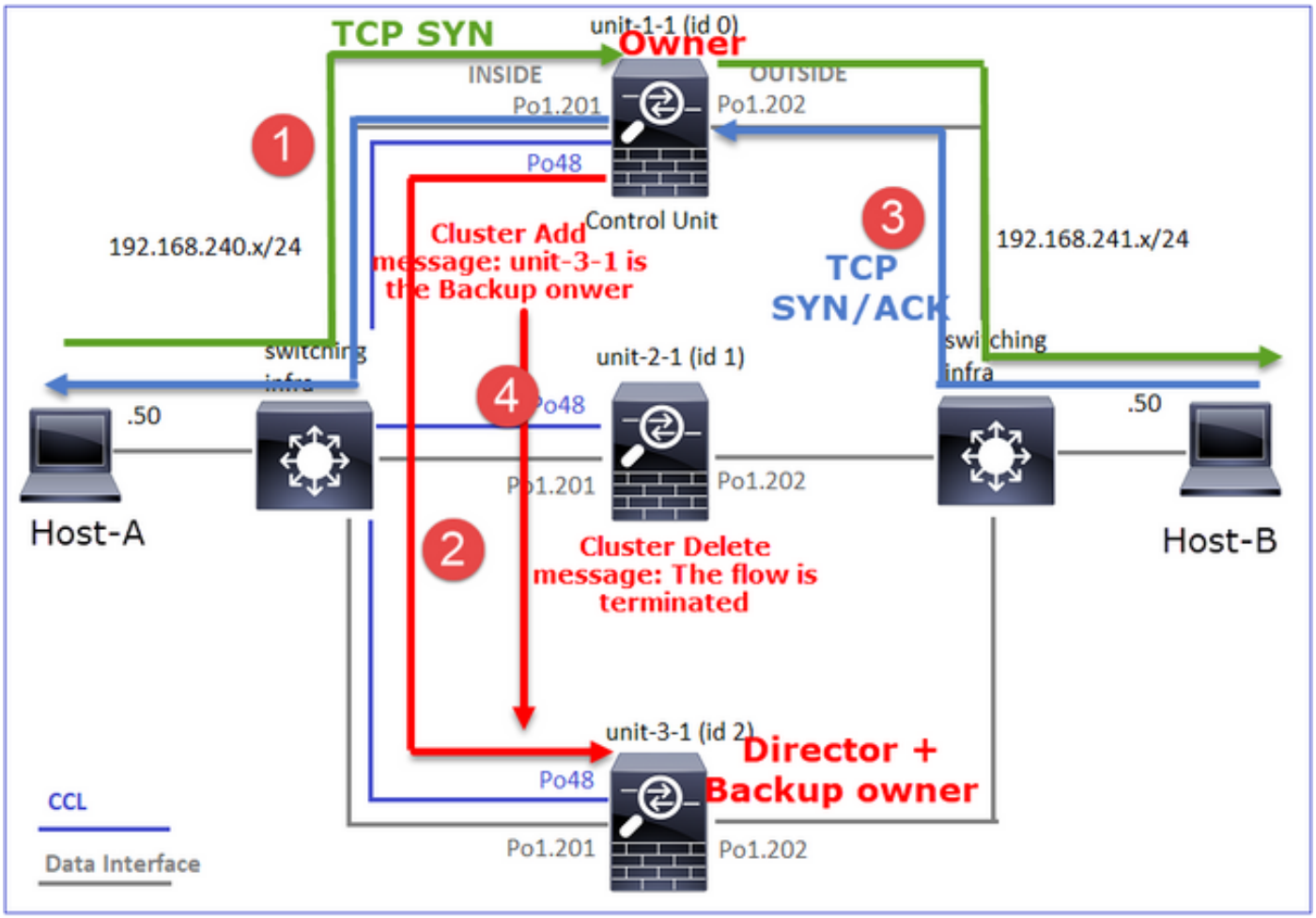
46278

, idle 0:00:06, bytes 0,

flags Y

Unità	Contrassegna	Nota
Unità-1-1	UIO	· Proprietario flusso: l'unità gestisce il flusso
Unità-2-1	-	-
Unità-3-1	Y	· Direttore e proprietario del backup - Unità 3-1 ha il flag Y (Direttore).

Ciò può essere visualizzato come:



1. Il pacchetto TCP SYN arriva dall'host A all'unità 1 1. L'unità 1 1 diventa il proprietario del flusso.
2. L'unità 3-1 viene selezionata come director di flusso. L'unità 3-1 è anche il proprietario del backup (messaggio "cluster add" su UDP 4193 su CCL).
3. Il pacchetto TCP SYN/ACK arriva dall'host-B all'unità-3-1. Il flusso è simmetrico.
4. Una volta terminata la connessione, il proprietario invia al CCL un messaggio di eliminazione del cluster su UDP 4193 per rimuovere le informazioni sul flusso dal proprietario del backup.

Osservazione 2. La cattura con traccia indica che entrambe le direzioni attraversano solo l'unità 1-

1

Passaggio 1. Utilizzare lo stesso approccio utilizzato nello studio di applicazione 1 per identificare il flusso e i pacchetti di interesse in tutte le unità cluster in base alla porta di origine:

```
<#root>

firepower#

cluster exec show cap CAPI | include 46278



unit-1-1

(LOCAL):*******************************************************
3: 11:01:44.841631 802.1Q vlan#201 P0 192.168.240.50.46278 > 192.168.241.50.80:

S

 1972783998:1972783998(0) win 29200 <mss 1460,sackOK,timestamp 503529072 0,nop,wscale 7>
4: 11:01:44.842317 802.1Q vlan#201 P0 192.168.241.50.80 > 192.168.240.50.46278:

S

 3524167695:3524167695(0)

ack

 1972783999 win 28960 <mss 1380,sackOK,timestamp 513884542 503529072,nop,wscale 7>
5: 11:01:44.842592 802.1Q vlan#201 P0 192.168.240.50.46278 > 192.168.241.50.80: . ack 3524167696 win 22
…
unit-2-1:*************************************************************

unit-3-1:*************************************************************
firepower#
```

Acquisizione sull'interfaccia ESTERNA:

```
<#root>


firepower#

cluster exec show cap CAPO | include 46278



unit-1-1

(LOCAL):*******************************************************
3: 11:01:44.841921 802.1Q vlan#202 P0 192.168.240.50.46278 > 192.168.241.50.80:

S

 2153055699:2153055699(0) win 29200 <mss 1380,sackOK,timestamp 503529072 0,nop,wscale 7>
4: 11:01:44.842226 802.1Q vlan#202 P0 192.168.241.50.80 > 192.168.240.50.46278:

S
```

```
 3382481337:3382481337(0)

ack

 2153055700 win 28960 <mss 1460,sackOK,timestamp 513884542 503529072,nop,wscale 7>
5: 11:01:44.842638 802.1Q vlan#202 P0 192.168.240.50.46278 > 192.168.241.50.80: . ack 3382481338 win 22

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

unit-3-1:*************************************************************
firepower#
```

Passaggio 2. Concentrazione sui pacchetti in entrata (TCP SYN e TCP SYN/ACK):

<#root>

```
firepower#

cluster exec show cap CAPI packet-number 3 trace


unit-1-1(LOCAL):*********************************************************

824 packets captured

3: 11:01:44.841631 802.1Q vlan#201 P0 192.168.240.50.46278 > 192.168.241.50.80:

S

 1972783998:1972783998(0) win 29200 <mss 1460,sackOK,timestamp 503529072 0,nop,wscale 7>
…

Phase: 4


Type: CLUSTER-EVENT


Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'INSIDE'
Flow type: NO FLOW


I (0) got initial, attempting ownership.



Phase: 5
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'INSIDE'
Flow type: NO FLOW
```

```
I (0) am becoming owner
```

Tracciare il SYN/ACK sull'unità 1-1:

```
<#root>

firepower#

cluster exec show cap CAPO packet-number 4 trace


unit-1-1(LOCAL):*******************************************************

4: 11:01:44.842226 802.1Q vlan#202 P0 192.168.241.50.80 > 192.168.240.50.

46278

:

S

 3382481337:3382481337(0)

ack

 2153055700 win 28960 <mss 1460,sackOK,timestamp 513884542 503529072,nop,wscale 7>
Phase: 3
Type: FLOW-LOOKUP
Subtype:
Result: ALLOW
Config:
Additional Information:


Found flow with id 9583, using existing flow
```

Osservazione 3. I syslog del piano dati FTD mostrano la creazione e la terminazione della connessione sul proprietario e sul proprietario del backup:

```
<#root>

firepower#

cluster exec show log | include 46278


unit-1-1(LOCAL):*******************************************************
Dec 01 2020 11:01:44: %FTD-6-302013:

Built inbound TCP connection

 9583 for INSIDE:192.168.240.50/46278 (192.168.240.50/46278) to OUTSIDE:192.168.241.50/80 (192.168.241.
Dec 01 2020 11:01:53: %FTD-6-302014:

Teardown TCP connection

 9583 for INSIDE:192.168.240.50/46278 to OUTSIDE:192.168.241.50/80 duration 0:00:08 bytes 1024001808 TC
```

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

unit-3-1:**************************************************************
Dec 01 2020 11:01:44: %FTD-6-302022:

Built director stub TCP connection

 for INSIDE:192.168.240.50/46278 (192.168.240.50/46278) to OUTSIDE:192.168.241.50/80 (192.168.241.50/80)
Dec 01 2020 11:01:53: %FTD-6-302023:

Teardown director TCP connection

 for INSIDE:192.168.240.50/46278 to OUTSIDE:192.168.241.50/80 duration 0:00:08 forwarded bytes 0 Cluste
```

Caso di studio 3. Traffico asimmetrico (il director inoltra il traffico).

Osservazione 1. Le catture di reject-hide mostrano pacchetti sulle unità 1-1 e 2-1 (flusso asimmetrico):

<#root>

```
firepower#

cluster exec show cap


unit-1-1(LOCAL):******************************************************
capture CCL type raw-data buffer 33554432 interface cluster [Buffer Full - 33554320 bytes]
capture CAPI type raw-data buffer 100000 trace interface INSIDE [Buffer Full - 98552 bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq www
capture CAPO type raw-data buffer 100000 trace interface OUTSIDE [Buffer Full - 98552 bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq www
capture CAPI_RH type raw-data

reinject-hide

 buffer 100000 interface

INSIDE

 [Buffer Full -

98552 bytes

]
match tcp host 192.168.240.50 host 192.168.241.50 eq www
capture CAPO_RH type raw-data

reinject-hide

 buffer 100000 interface

OUTSIDE

 [Buffer Full -

99932 bytes

]
match tcp host 192.168.240.50 host 192.168.241.50 eq www

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

```
capture CCL type raw-data buffer 33554432 interface cluster [Buffer Full - 33553268 bytes]
capture CAPI type raw-data buffer 100000 trace interface INSIDE [Capturing - 0 bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq www
capture CAPO type raw-data buffer 100000 trace interface OUTSIDE [Buffer Full - 99052 bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq www
capture CAPI_RH type raw-data reinject-hide buffer 100000 interface INSIDE [Capturing - 0 bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq www
capture CAPO_RH type raw-data
```

reinject-hide

```
 buffer 100000 interface
```

OUTSIDE

```
 [Buffer Full -
```

99052 bytes

```
]
match tcp host 192.168.240.50 host 192.168.241.50 eq www

unit-3-1:************************************************************
capture CCL type raw-data buffer 33554432 interface cluster [Capturing - 53815 bytes]
capture CAPI type raw-data buffer 100000 trace interface INSIDE [Capturing - 0 bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq www
capture CAPO type raw-data buffer 100000 trace interface OUTSIDE [Capturing - 658 bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq www
capture CAPI_RH type raw-data reinject-hide buffer 100000 interface INSIDE [Capturing - 0 bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq www
capture CAPO_RH type raw-data reinject-hide buffer 100000 interface OUTSIDE [Capturing - 658 bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq www
```

Osservazione 2. Analisi del flag di connessione per il flusso con porta di origine 46502.

<#root>

```
firepower#
```

cluster exec show conn

unit-1-1

```
(LOCAL):*****************************************************
23 in use, 25 most used
Cluster:
fwd connections: 0 in use, 1 most used
dir connections: 0 in use, 122 most used
centralized connections: 0 in use, 0 most used
VPN redirect connections: 0 in use, 0 most used
Inspect Snort:
preserve-connection: 2 enabled, 0 in effect, 4 most enabled, 1 most in effect

TCP OUTSIDE 192.168.241.50:80 INSIDE 192.168.240.50:
```

46502

```
, idle 0:00:00, bytes 448760236,
```

flags UIO N1

TCP OUTSIDE 192.168.241.50:80 INSIDE 192.168.240.50:46500, idle 0:00:06, bytes 0, flags aA N1

unit-2-1

:**********
21 in use, 271 most used
Cluster:
fwd connections: 0 in use, 2 most used
dir connections: 1 in use, 2 most used
centralized connections: 0 in use, 0 most used
VPN redirect connections: 0 in use, 0 most used
Inspect Snort:
preserve-connection: 0 enabled, 0 in effect, 249 most enabled, 0 most in effect

TCP OUTSIDE 192.168.241.50:80 INSIDE 192.168.240.50:

46502

, idle 0:00:00, bytes 0,

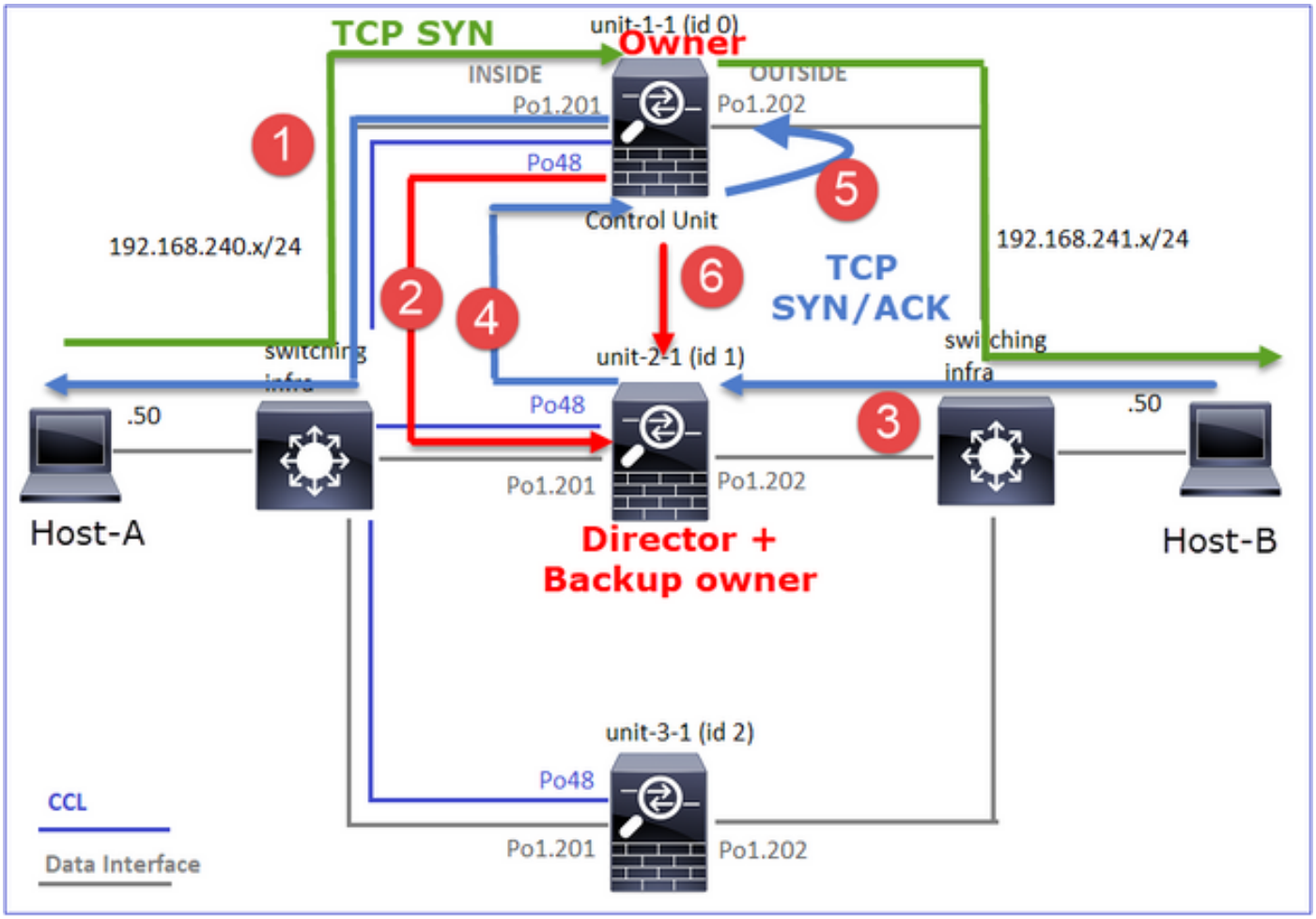
flags Y

unit-3-1:**********
17 in use, 20 most used
Cluster:
fwd connections: 1 in use, 5 most used
dir connections: 0 in use, 127 most used
centralized connections: 0 in use, 0 most used
VPN redirect connections: 0 in use, 0 most used
Inspect Snort:
preserve-connection: 0 enabled, 0 in effect, 1 most enabled, 0 most in effect

Unità	Contrassegna	Nota
Unità-1-1	UIO	· Proprietario flusso: l'unità gestisce il flusso.
Unità-2-1	Y	· Director - Poiché l'unità 2-1 ha il flag 'Y', ciò implica che l'unità 2-1 è stata scelta come director per questo flusso. · Proprietario del backup · Infine, sebbene non sia ovvio da questo output, dai risultati show capture e show log è evidente che l'unità 2-1 inoltra questo flusso al proprietario (anche se tecnicamente non è considerato un server d'inoltro in questo scenario). Nota: Un'unità non può essere sia director (flusso Y) che

		forwarder (flusso z). Questi due ruoli si escludono a vicenda. I director (flusso Y) possono comunque inoltrare il traffico. Vedere l'output del comando show log più avanti in questo caso di studio.
Unità-3-1	-	-

Ciò può essere visualizzato come:



1. Il pacchetto TCP SYN arriva dall'host A all'unità 1 1. L'unità 1 1 diventa il proprietario del flusso.
2. L'unità 2-1 viene selezionata come director di flusso e proprietario del backup. Il proprietario del flusso invia un messaggio unicast 'cluster add' su UDP 4193 per informare il proprietario del backup del flusso.
3. Il pacchetto TCP SYN/ACK arriva dall'host-B all'unità-2-1. Il flusso è asimmetrico.
4. L'unità 2-1 inoltra il pacchetto attraverso la CCL al proprietario (a causa del cookie SYN di TCP).
5. Il proprietario reinserisce il pacchetto sull'interfaccia OUTSIDE e quindi lo inoltra all'host-A.
6. Una volta terminata la connessione, il proprietario invia un messaggio di eliminazione del cluster per rimuovere le informazioni sul flusso dal proprietario del backup.

Osservazione 3. La cattura con traccia mostra il traffico asimmetrico e il reindirizzamento dall'unità

2-1 all'unità 1-1.

Passaggio 1. Identificare i pacchetti che appartengono al flusso di interesse (porta 46502):

<#root>

```
firepower#
```

cluster exec show capture CAPI | include 46502

```
unit-1-1(LOCAL):*******************************************************
3: 12:58:33.356121 802.1Q vlan#201 P0 192.168.240.50.46502 > 192.168.241.50.80: S 4124514680:4124514680
4: 12:58:33.357037 802.1Q vlan#201 P0 192.168.241.50.80 > 192.168.240.50.46502: S 883000451:883000451(0)
5: 12:58:33.357357 802.1Q vlan#201 P0 192.168.240.50.46502 > 192.168.241.50.80: . ack 883000452 win 229
unit-2-1:*************************************************************

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

Direzione di ritorno:

<#root>

```
firepower#
```

cluster exec show capture CAPO | include 46502

```
unit-1-1(LOCAL):*******************************************************
3: 12:58:33.356426 802.1Q vlan#202 P0 192.168.240.50.46502 > 192.168.241.50.80: S 1434968587:1434968587
4: 12:58:33.356915 802.1Q vlan#202 P0 192.168.241.50.80 > 192.168.240.50.46502: S 4257314722:4257314722
5: 12:58:33.357403 802.1Q vlan#202 P0 192.168.240.50.46502 > 192.168.241.50.80: . ack 4257314723 win 22

unit-2-1:*************************************************************
1: 12:58:33.359249 802.1Q vlan#202 P0 192.168.241.50.80 > 192.168.240.50.46502: S 4257314722:4257314722
2: 12:58:33.360302 802.1Q vlan#202 P0 192.168.241.50.80 > 192.168.240.50.46502: . ack 1434968736 win 23
3: 12:58:33.361004 802.1Q vlan#202 P0 192.168.241.50.80 > 192.168.240.50.46502: . 4257314723:4257316091
…

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

Passaggio 2. Tracciare i pacchetti. Per impostazione predefinita, vengono tracciati solo i primi 50 pacchetti in entrata. Per semplicità, le fasi di analisi non rilevanti vengono omesse.

Unità-1-1 (proprietario):

<#root>

```
firepower#
```

cluster exec show capture CAPI packet-number 3 trace

```
unit-1-1(LOCAL):*******************************************************
3: 12:58:33.356121 802.1Q vlan#201 P0 192.168.240.50.
```

46502

```
 > 192.168.241.50.80:
```

S

```
 4124514680:4124514680(0) win 29200 <mss 1460,sackOK,timestamp 510537534 0,nop,wscale 7>
...
Phase: 4
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'INSIDE'
Flow type: NO FLOW
```

I (0) got initial, attempting ownership.

```
Phase: 5
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'INSIDE'
Flow type: NO FLOW
```

I (0) am becoming owner

Unità-2-1 (server d'inoltro)

Il traffico di ritorno (TCP SYN/ACK). L'unità di interesse è l'unità 2-1 che è il director/proprietario del backup e inoltra il traffico al proprietario:

<#root>

```
firepower#
```

cluster exec unit unit-2-1 show capture CAPO packet-number 1 trace

```
1: 12:58:33.359249 802.1Q vlan#202 P0 192.168.241.50.80 > 192.168.240.50.
```

46502

```
: S 4257314722:4257314722(0) ack 1434968588 win 28960 <mss 1460,sackOK,timestamp 520893004 510537534,no
...
Phase: 4
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
```

```
Input interface: 'OUTSIDE'
Flow type: NO FLOW


I (1) got initial, attempting ownership.



Phase: 5
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'OUTSIDE'
Flow type: NO FLOW


I (1) am early redirecting to (0) due to matching action (-1).
```

Osservazione 4. I syslog del piano dati FTD mostrano la creazione e la terminazione della connessione su tutte le unità:

<#root>

```
firepower#

cluster exec show log | i 46502


unit-1-1(LOCAL):*******************************************************
Dec 01 2020 12:58:33: %FTD-6-302013:

B

uilt inbound TCP connection

 9742 for INSIDE:192.168.240.50/46502 (192.168.240.50/46502) to OUTSIDE:192.168.241.50/80 (192.168.241.
Dec 01 2020 12:59:02: %FTD-6-302014:

Teardown TCP connection

 9742 for INSIDE:192.168.240.50/46502 to OUTSIDE:192.168.241.50/80 duration 0:00:28 bytes 2048000440 TC

unit-2-1:*************************************************************
Dec 01 2020 12:58:33: %FTD-6-302022:

Built forwarder stub TCP connection

 for OUTSIDE:192.168.241.50/80 (192.168.241.50/80) to unknown:192.168.240.50/46502 (192.168.240.50/4650
Dec 01 2020 12:58:33: %FTD-6-302023:

Teardown forwarder TCP connection

 for OUTSIDE:192.168.241.50/80 to unknown:192.168.240.50/46502 duration 0:00:00 forwarded bytes 0 Forwa
Dec 01 2020 12:58:33: %FTD-6-302022:

Built director stub TCP connection

 for INSIDE:192.168.240.50/46502 (192.168.240.50/46502) to OUTSIDE:192.168.241.50/80 (192.168.241.50/80
Dec 01 2020 12:59:02: %FTD-6-302023:

Teardown director TCP connection
```

```
 for INSIDE:192.168.240.50/46502 to OUTSIDE:192.168.241.50/80 duration 0:00:28 forwarded bytes 20483163

unit-3-1:***********************************************************
firepower#
```

Caso di studio 4. Traffico asimmetrico (il proprietario è il director)

Osservazione 1. Le catture di reject-hide mostrano pacchetti sulle unità 1-1 e 2-1 (flusso asimmetrico):

<#root>

```
firepower#

cluster exec show cap


unit-1-1(LOCAL):*******************************************************
capture CCL type raw-data buffer 33554432 interface cluster [Buffer Full - 33554229 bytes]
capture CAPI type raw-data buffer 100000 trace interface INSIDE [Buffer Full - 98974 bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq www
capture CAPO type raw-data buffer 100000 trace interface OUTSIDE [Buffer Full - 98974 bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq www
capture CAPI_RH type raw-data

reinject-hide

 buffer 100000 interface

INSIDE

 [Buffer Full -

98974 bytes

]
match tcp host 192.168.240.50 host 192.168.241.50 eq www
capture CAPO_RH type raw-data

reinject-hide

 buffer 100000 interface

OUTSIDE

 [Buffer Full -

99924 bytes

]
match tcp host 192.168.240.50 host 192.168.241.50 eq www

unit-2-1:***********************************************************
capture CCL type raw-data buffer 33554432 interface cluster [Buffer Full - 33552925 bytes]
capture CAPI type raw-data buffer 100000 trace interface INSIDE [Capturing - 0 bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq www
capture CAPO type raw-data buffer 100000 trace interface OUTSIDE [Buffer Full - 99052 bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq www
capture CAPI_RH type raw-data reinject-hide buffer 100000 interface INSIDE [Capturing - 0 bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq www
capture CAPO_RH type raw-data
```

reinject-hide

 buffer 100000 interface OUTSIDE [Buffer Full -

99052 bytes

]
match tcp host 192.168.240.50 host 192.168.241.50 eq www

unit-3-1:**
capture CCL type raw-data buffer 33554432 interface cluster [Capturing - 227690 bytes]
capture CAPI type raw-data buffer 100000 trace interface INSIDE [Capturing - 0 bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq www
capture CAPO type raw-data buffer 100000 trace interface OUTSIDE [Capturing - 4754 bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq www
capture CAPI_RH type raw-data reinject-hide buffer 100000 interface INSIDE [Capturing - 0 bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq www
capture CAPO_RH type raw-data reinject-hide buffer 100000 interface OUTSIDE [Capturing - 0 bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq www

Osservazione 2. Analisi del flag di connessione per il flusso con porta di origine 46916.

<#root>

firepower#

 cluster exec show conn

unit-1-1

(LOCAL):**
23 in use, 25 most used
Cluster:
fwd connections: 0 in use, 1 most used
dir connections: 0 in use, 122 most used
centralized connections: 0 in use, 0 most used
VPN redirect connections: 0 in use, 0 most used
Inspect Snort:
preserve-connection: 1 enabled, 0 in effect, 4 most enabled, 1 most in effect

TCP OUTSIDE 192.168.241.50:80 INSIDE 192.168.240.50:

46916

, idle 0:00:00, bytes 414682616,

flags UIO N1

unit-2-1

:**
21 in use, 271 most used
Cluster:
fwd connections: 1 in use, 2 most used
dir connections: 0 in use, 2 most used

```
centralized connections: 0 in use, 0 most used
VPN redirect connections: 0 in use, 0 most used
Inspect Snort:
preserve-connection: 0 enabled, 0 in effect, 249 most enabled, 0 most in effect

TCP OUTSIDE 192.168.241.50:80 NP Identity Ifc 192.168.240.50:
```

46916

```
, idle 0:00:00, bytes 0,
```

flags z

unit-3-1

```
:************************************************************
17 in use, 20 most used
Cluster:
fwd connections: 0 in use, 5 most used
dir connections: 1 in use, 127 most used
centralized connections: 0 in use, 0 most used
VPN redirect connections: 0 in use, 0 most used
Inspect Snort:
preserve-connection: 0 enabled, 0 in effect, 1 most enabled, 0 most in effect

TCP OUTSIDE 192.168.241.50:80 INSIDE 192.168.240.50:
```

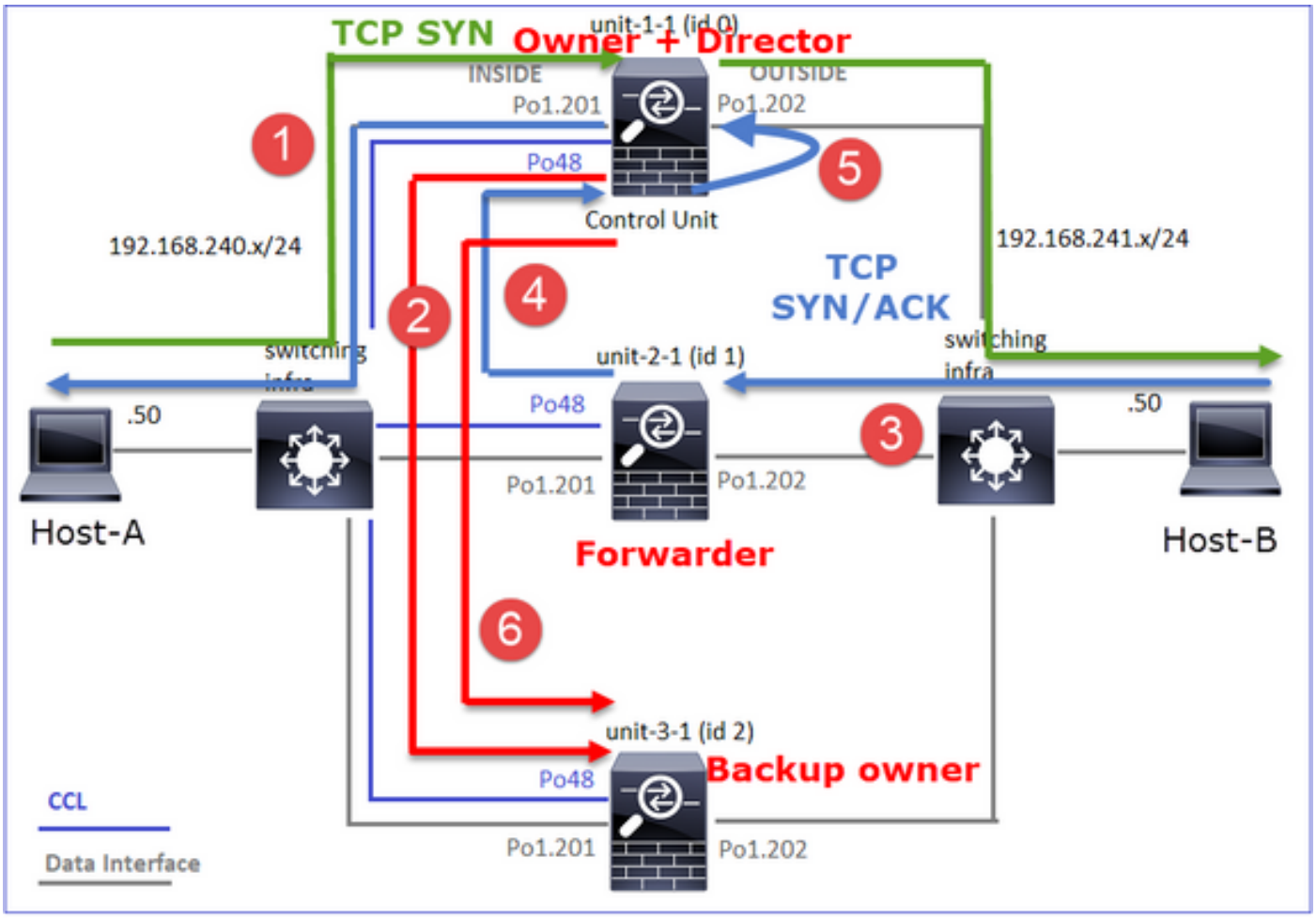
46916

```
, idle 0:00:04, bytes 0,
```

flags y

Unità	Contrassegna	Nota
Unità-1-1	UIO	· Proprietario flusso: l'unità gestisce il flusso · Direttore - Poiché l'unità 3-1 ha "y" e non "Y", ciò implica che l'unità 1-1 è stata scelta come direttore per questo flusso. Pertanto, poiché è anche il proprietario, un'altra unità (in questo caso l'unità 3-1) è stata scelta come proprietario del backup
Unità-2-1	z	· Inoltro
Unità-3-1	y	- Proprietario backup

Ciò può essere visualizzato come:



1. Il pacchetto TCP SYN arriva dall'host-A all'unità-1-1. L'unità-1-1 diventa il proprietario del flusso e viene selezionata come director.
2. L'unità 3-1 viene selezionata come proprietario del backup. Il proprietario del flusso invia un messaggio unicast 'cluster add' su UDP 4193 per informare il proprietario del backup del flusso.
3. Il pacchetto TCP SYN/ACK arriva dall'host-B all'unità-2-1. Il flusso è asimmetrico.
4. L'unità 2-1 inoltra il pacchetto attraverso la CCL al proprietario (a causa del cookie SYN di TCP).
5. Il proprietario reinserisce il pacchetto sull'interfaccia OUTSIDE e quindi lo inoltra all'host-A.
6. Una volta terminata la connessione, il proprietario invia un messaggio di eliminazione del cluster per rimuovere le informazioni sul flusso dal proprietario del backup.

Osservazione 3. La cattura con traccia mostra il traffico asimmetrico e il reindirizzamento dall'unità 2-1 all'unità 1-1.

Unità-2-1 (server d'inoltro)

```
<#root>

firepower#

cluster exec unit unit-2-1 show capture CAPO packet-number 1 trace

1: 16:11:33.653164 802.1Q vlan#202 P0 192.168.241.50.80 > 192.168.240.50.
```

46916

:

S

 1331019196:1331019196(0)

ack

 3089755618 win 28960 <mss 1460,sackOK,timestamp 532473211 522117741,nop,wscale 7>
...
Phase: 4
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'OUTSIDE'
Flow type: NO FLOW

I (1) got initial, attempting ownership.

Phase: 5
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'OUTSIDE'
Flow type: NO FLOW

I (1) am early redirecting to (0) due to matching action (-1).

Osservazione 4. I syslog del piano dati FTD mostrano la creazione e la terminazione della connessione su tutte le unità:

- Unit-1-1 (proprietario)
- Unità-2-1 (server d'inoltro)
- Unit-3-1 (proprietario del backup)

<#root>

firepower#

cluster exec show log | i 46916

unit-1-1(LOCAL):***
Dec 01 2020 16:11:33: %FTD-6-302013:

Built inbound TCP connection

 10023 for INSIDE:192.168.240.50/46916 (192.168.240.50/46916) to OUTSIDE:192.168.241.50/80 (192.168.241
Dec 01 2020 16:11:42: %FTD-6-302014:

Teardown TCP connection

```
 10023 for INSIDE:192.168.240.50/46916 to OUTSIDE:192.168.241.50/80 duration 0:00:09 bytes 1024010016 T

unit-2-1:************************************************************
Dec 01 2020 16:11:33: %FTD-6-302022:

Built forwarder stub TCP connection

 for OUTSIDE:192.168.241.50/80 (192.168.241.50/80) to unknown:192.168.240.50/46916 (192.168.240.50/4691
Dec 01 2020 16:11:42: %FTD-6-302023:

Teardown forwarder TCP connection

 for OUTSIDE:192.168.241.50/80 to unknown:192.168.240.50/46916 duration 0:00:09 forwarded bytes 1024009

unit-3-1:************************************************************
Dec 01 2020 16:11:33: %FTD-6-302022:

Built backup stub TCP connection

 for INSIDE:192.168.240.50/46916 (192.168.240.50/46916) to OUTSIDE:192.168.241.50/80 (192.168.241.50/80)
Dec 01 2020 16:11:42: %FTD-6-302023:

Teardown backup TCP connection

 for INSIDE:192.168.240.50/46916 to OUTSIDE:192.168.241.50/80 duration 0:00:09 forwarded bytes 0 Cluste
```

Caso di studio 5. Traffico asimmetrico (il proprietario è diverso dal director).

Osservazione 1. Le catture di reject-hide mostrano pacchetti sulle unità 1-1 e 2-1 (flusso asimmetrico):

<#root>

```
firepower#

cluster exec show cap



unit-1-1

(LOCAL):*****************************************************
capture CCL type raw-data buffer 33554432 interface cluster [Buffer Full - 33553207 bytes]
capture CAPI type raw-data buffer 100000 trace interface INSIDE [Buffer Full - 99396 bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq www
capture CAPO type raw-data buffer 100000 trace interface OUTSIDE [Buffer Full - 99224 bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq www
capture CAPI_RH type raw-data

reinject-hide

 buffer 100000 interface

INSIDE

 [Buffer Full -

99396 bytes

]
match tcp host 192.168.240.50 host 192.168.241.50 eq www
```

```
capture CAPO_RH type raw-data

reinject-hid

e buffer 100000 interface

OUTSIDE

 [Buffer Full -

99928 bytes

]
match tcp host 192.168.240.50 host 192.168.241.50 eq www



unit-2-1

:************************************************************
capture CCL type raw-data buffer 33554432 interface cluster [Buffer Full - 33554251 bytes]
capture CAPI type raw-data buffer 100000 trace interface INSIDE [Capturing - 0 bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq www
capture CAPO type raw-data buffer 100000 trace interface OUTSIDE [Buffer Full - 99052 bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq www
capture CAPI_RH type raw-data reinject-hide buffer 100000 interface INSIDE [Capturing - 0 bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq www
capture CAPO_RH type raw-data

reinject-hide

 buffer 100000 interface

OUTSIDE

 [Buffer Full -

99052 bytes

]
match tcp host 192.168.240.50 host 192.168.241.50 eq www

unit-3-1:************************************************************
capture CCL type raw-data buffer 33554432 interface cluster [Capturing - 131925 bytes]
capture CAPI type raw-data buffer 100000 trace interface INSIDE [Capturing - 0 bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq www
capture CAPO type raw-data buffer 100000 trace interface OUTSIDE [Capturing - 2592 bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq www
capture CAPI_RH type raw-data reinject-hide buffer 100000 interface INSIDE [Capturing - 0 bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq www
capture CAPO_RH type raw-data reinject-hide buffer 100000 interface OUTSIDE [Capturing - 0 bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq www
```

Osservazione 2. Analisi del flag di connessione per il flusso con porta di origine 46994:

```
<#root>

firepower#

cluster exec show conn
```

unit-1-1

(LOCAL):***
23 in use, 25 most used
Cluster:
fwd connections: 0 in use, 1 most used
dir connections: 0 in use, 122 most used
centralized connections: 0 in use, 0 most used
VPN redirect connections: 0 in use, 0 most used
Inspect Snort:
preserve-connection: 1 enabled, 0 in effect, 4 most enabled, 1 most in effect

TCP OUTSIDE 192.168.241.50:80 INSIDE 192.168.240.50:

46994

, idle 0:00:00, bytes 406028640,

flags UIO N1

unit-2-1

:**
22 in use, 271 most used
Cluster:
fwd connections: 1 in use, 2 most used
dir connections: 0 in use, 2 most used
centralized connections: 0 in use, 0 most used
VPN redirect connections: 0 in use, 0 most used
Inspect Snort:
preserve-connection: 0 enabled, 0 in effect, 249 most enabled, 0 most in effect

TCP OUTSIDE 192.168.241.50:80 NP Identity Ifc 192.168.240.50:

46994

, idle 0:00:00, bytes 0,

flags z

unit-3-1

:**
17 in use, 20 most used
Cluster:
fwd connections: 2 in use, 5 most used
dir connections: 1 in use, 127 most used
centralized connections: 0 in use, 0 most used
VPN redirect connections: 0 in use, 0 most used
Inspect Snort:
preserve-connection: 0 enabled, 0 in effect, 1 most enabled, 0 most in effect

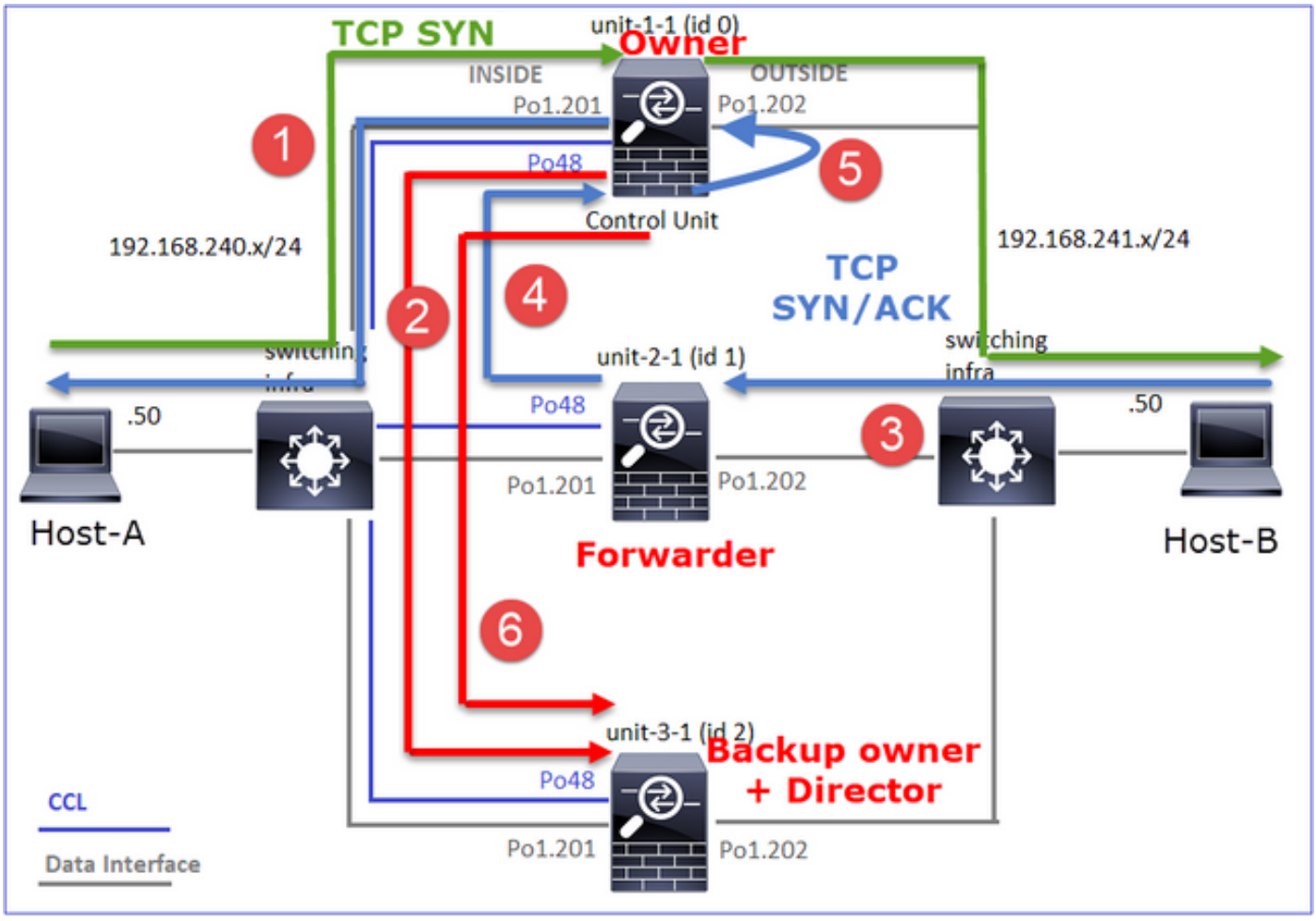
TCP OUTSIDE 192.168.241.50:80 INSIDE 192.168.240.50:

46994

```
, idle 0:00:05, bytes 0,
flags Y
```

Unità	Contrassegna	Nota
Unità-1-1	UIO	· Proprietario flusso: l'unità gestisce il flusso
Unità-2-1	z	· Inoltro
Unità-3-1	Y	· Proprietario del backup · Direttore

Ciò può essere visualizzato come:



1. Il pacchetto TCP SYN arriva dall'host A all'unità 1 1. L'unità 1 1 diventa il proprietario del flusso.
2. L'unità 3-1 viene scelta come director e proprietario del backup. Il proprietario del flusso invia

un messaggio unicast 'cluster add' su UDP 4193 per informare il proprietario del backup del flusso.
3. Il pacchetto TCP SYN/ACK arriva dall'host B all'unità 2-1. Il flusso è asimmetrico
4. L'unità 2-1 inoltra il pacchetto attraverso la CCL al proprietario (a causa del cookie SYN di TCP).
5. Il proprietario reinserisce il pacchetto sull'interfaccia OUTSIDE e quindi lo inoltra all'host-A.
6. Una volta terminata la connessione, il proprietario invia un messaggio di eliminazione del cluster per rimuovere le informazioni sul flusso dal proprietario del backup.

Osservazione 3. La cattura con traccia mostra il traffico asimmetrico e il reindirizzamento dall'unità 2-1 all'unità 1-1.

Unit-1-1 (proprietario)

<#root>

```
firepower#
```

cluster exec show cap CAPI packet-number 1 trace

```
unit-1-1(LOCAL):*******************************************************
…
Phase: 4
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'INSIDE'
Flow type: NO FLOW
```

I (0) got initial, attempting ownership.

```
Phase: 5
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'INSIDE'
Flow type: NO FLOW
```

I (0) am becoming owner

Unità-2-1 (server d'inoltro)

<#root>

```
firepower#
```

cluster exec unit unit-2-1 show cap CAPO packet-number 1 trace

1: 16:46:44.232074 802.1Q vlan#202 P0 192.168.241.50.80 > 192.168.240.50.

46994

: S 2863659376:2863659376(0) ack 2879616990 win 28960 <mss 1460,sackOK,timestamp 534583774 524228304,no
…
Phase: 4
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'OUTSIDE'
Flow type: NO FLOW

I (1) got initial, attempting ownership.

Phase: 5
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'OUTSIDE'
Flow type: NO FLOW

I (1) am early redirecting to (0) due to matching action (-1).

Osservazione 4. I syslog del piano dati FTD mostrano la creazione e la terminazione della connessione su tutte le unità:

- Unit-1-1 (proprietario)
- Unità-2-1 (server d'inoltro)
- Unità-3-1 (proprietario/director di backup)

<#root>

firepower#

cluster exec show log | i 46994

unit-1-1(LOCAL):***
Dec 01 2020 16:46:44: %FTD-6-302013:

Built inbound TCP connection

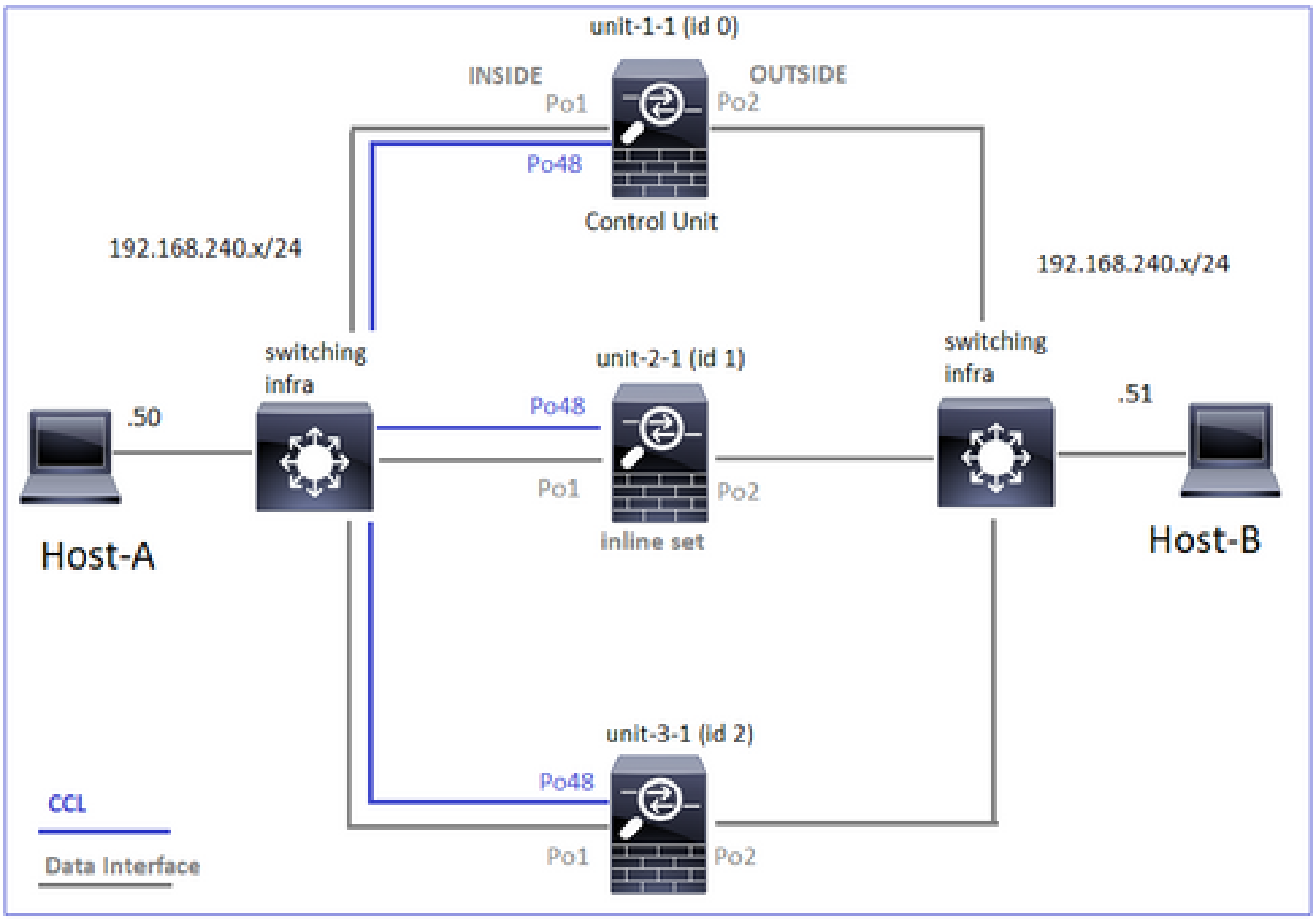
 10080 for INSIDE:192.168.240.50/46994 (192.168.240.50/46994) to OUTSIDE:192.168.241.50/80 (192.168.241
Dec 01 2020 16:46:53: %FTD-6-302014:

Teardown TCP connection

 10080 for INSIDE:192.168.240.50/46994 to OUTSIDE:192.168.241.50/80 duration 0:00:09 bytes 1024000440 T

```
unit-2-1:************************************************************
Dec 01 2020 16:46:44: %FTD-6-302022:

Built forwarder stub TCP connection

 for OUTSIDE:192.168.241.50/80 (192.168.241.50/80) to unknown:192.168.240.50/46994 (192.168.240.50/4699
Dec 01 2020 16:46:53: %FTD-6-302023:

Teardown forwarder TCP connection

 for OUTSIDE:192.168.241.50/80 to unknown:192.168.240.50/46994 duration 0:00:09 forwarded bytes 1024000

unit-3-1:************************************************************
Dec 01 2020 16:46:44: %FTD-6-302022:

Built director stub TCP connection

 for INSIDE:192.168.240.50/46994 (192.168.240.50/46994) to OUTSIDE:192.168.241.50/80 (192.168.241.50/80)
Dec 01 2020 16:46:53: %FTD-6-302023:

Teardown director TCP connection

 for INSIDE:192.168.240.50/46994 to OUTSIDE:192.168.241.50/80 duration 0:00:09 forwarded bytes 0 Cluste
```

Per i casi di studio successivi, la topologia utilizzata si basa su un cluster con insiemi inline:



Caso di studio 6. Traffico asimmetrico (Inline-set, il proprietario è il director)

Osservazione 1. Le immagini acquisite con la tecnica del reject-hide mostrano i pacchetti sulle unità 1-1 e 2-1 (flusso asimmetrico). Inoltre, il proprietario è l'unità-2-1 (ci sono pacchetti su entrambe le interfacce, INTERNA ed ESTERNA per le clip di reject-hide, mentre l'unità-1-1 ha solo su ESTERNA):

<#root>

firepower#

cluster exec show cap

unit-1-1

(LOCAL):**
capture CCL type raw-data buffer 33554432 interface cluster [Buffer Full - 33553253 bytes]
capture CAPO type raw-data trace interface OUTSIDE [Buffer Full - 523432 bytes]
match tcp host 192.168.240.50 host 192.168.240.51 eq www
capture CAPI type raw-data trace interface INSIDE [Capturing - 0 bytes]
match tcp host 192.168.240.50 host 192.168.240.51 eq www
capture CAPO_RH type raw-data

reinject-hide

interface

OUTSIDE

[Buffer Full -

523432 bytes

]
match tcp host 192.168.240.50 host 192.168.240.51 eq www
capture CAPI_RH type raw-data reinject-hide interface INSIDE [Capturing - 0 bytes]
match tcp host 192.168.240.50 host 192.168.240.51 eq www

unit-2-1

:**
capture CCL type raw-data buffer 33554432 interface cluster [Buffer Full - 33554312 bytes]
capture CAPO type raw-data trace interface OUTSIDE [Buffer Full - 523782 bytes]
match tcp host 192.168.240.50 host 192.168.240.51 eq www
capture CAPI type raw-data trace interface INSIDE [Buffer Full - 523782 bytes]
match tcp host 192.168.240.50 host 192.168.240.51 eq www
capture CAPO_RH type raw-data

reinject-hide

interface

OUTSIDE

[Buffer Full -

524218 bytes

]
match tcp host 192.168.240.50 host 192.168.240.51 eq www
capture CAPI_RH type raw-data

reinject-hide

interface

INSIDE

[Buffer Full -

523782 bytes]

match tcp host 192.168.240.50 host 192.168.240.51 eq www

unit-3-1:**********
capture CCL type raw-data buffer 33554432 interface cluster [Capturing - 53118 bytes]
capture CAPO type raw-data trace interface OUTSIDE [Capturing - 0 bytes]
match tcp host 192.168.240.50 host 192.168.240.51 eq www
capture CAPI type raw-data trace interface INSIDE [Capturing - 0 bytes]
match tcp host 192.168.240.50 host 192.168.240.51 eq www
capture CAPO_RH type raw-data reinject-hide interface OUTSIDE [Capturing - 0 bytes]
match tcp host 192.168.240.50 host 192.168.240.51 eq www
capture CAPI_RH type raw-data reinject-hide interface INSIDE [Capturing - 0 bytes]
match tcp host 192.168.240.50 host 192.168.240.51 eq www

Osservazione 2. Analisi del flag di connessione per il flusso con porta sorgente 51844.

<#root>

firepower#

cluster exec show conn addr 192.168.240.51

unit-1-1

(LOCAL):**********
30 in use, 102 most used
Cluster:
fwd connections: 1 in use, 1 most used
dir connections: 2 in use, 122 most used
centralized connections: 3 in use, 39 most used
VPN redirect connections: 0 in use, 0 most used
Inspect Snort:
preserve-connection: 0 enabled, 0 in effect, 4 most enabled, 1 most in effect

TCP OUTSIDE 192.168.240.51:80 NP Identity Ifc 192.168.240.50:

51844

, idle 0:00:00, bytes 0,

flags z

unit-2-1

:**********
23 in use, 271 most used

```
Cluster:
fwd connections: 0 in use, 2 most used
dir connections: 4 in use, 26 most used
centralized connections: 0 in use, 14 most used
VPN redirect connections: 0 in use, 0 most used
Inspect Snort:
preserve-connection: 0 enabled, 0 in effect, 249 most enabled, 0 most in effect

TCP OUTSIDE 192.168.240.51:80 INSIDE 192.168.240.50:
```

51844

```
, idle 0:00:00, bytes 231214400,
```

flags b N

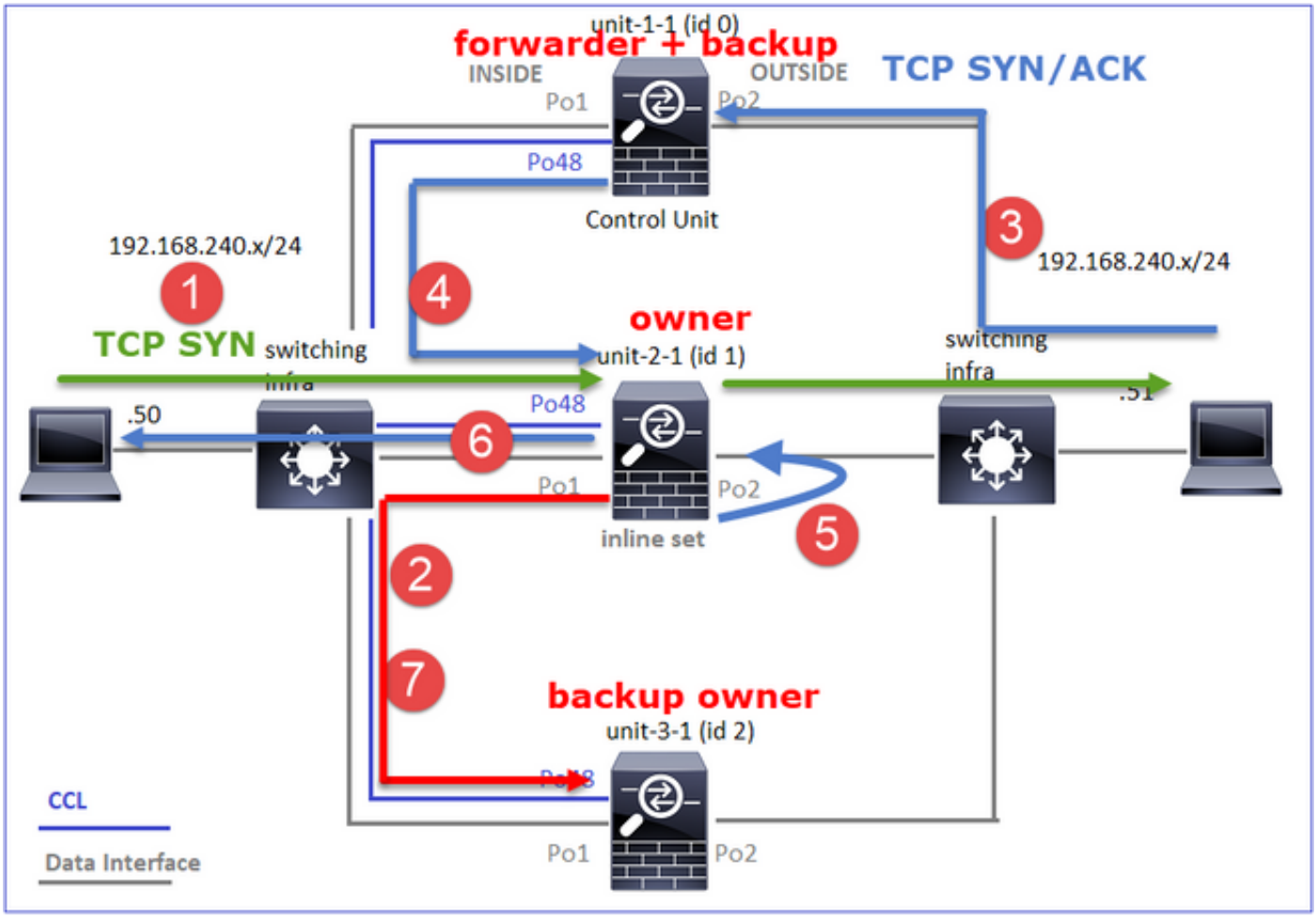
unit-3-1

```
:************************************************************
20 in use, 55 most used
Cluster:
fwd connections: 0 in use, 5 most used
dir connections: 1 in use, 127 most used
centralized connections: 0 in use, 24 most used
VPN redirect connections: 0 in use, 0 most used
Inspect Snort:
preserve-connection: 0 enabled, 0 in effect, 1 most enabled, 0 most in effect

TCP OUTSIDE 192.168.240.51:80 INSIDE 192.168.240.50:51844, idle 0:00:01, bytes 0,
```

flags y

Unità	Contrassegna	Nota
Unità-1-1	z	· Inoltro
Unità-2-1	b N	· Proprietario flusso: l'unità gestisce il flusso
Unità-3-1	y	· Proprietario del backup

Ciò può essere visualizzato come:



1. Il pacchetto TCP SYN arriva dall'host-A all'unità-2-1. L'unità-2-1 diventa il proprietario del flusso e viene selezionata come director.
2. L'unità 3-1 viene selezionata come proprietario del backup. Il proprietario del flusso invia un messaggio unicast 'cluster add' su UDP 4193 per informare il proprietario del backup del flusso.
3. Il pacchetto TCP SYN/ACK arriva dall'host-B all'unità-1-1. Il flusso è asimmetrico.
4. L'unità 1-1 inoltra il pacchetto attraverso la CCL al director (unità 2-1).
5. Anche l'unità 2-1 è proprietaria e reinserisce il pacchetto sull'interfaccia OUTSIDE.
6. L'unità 2-1 inoltra il pacchetto all'host A.
7. Una volta terminata la connessione, il proprietario invia un messaggio di eliminazione del cluster per rimuovere le informazioni sul flusso dal proprietario del backup.

Osservazione 3. La cattura con traccia mostra il traffico asimmetrico e il reindirizzamento dall'unità 1-1 all'unità 2-1.

Unità-2-1 (proprietario/direttore)

<#root>

```
firepower#
```

cluster exec unit unit-2-1 show cap CAPI packet-number 1 trace

```
1: 18:10:12.842912 192.168.240.50.51844 > 192.168.240.51.80:
```

S

```
 4082593463:4082593463(0) win 29200 <mss 1460,sackOK,timestamp 76258053 0,nop,wscale 7>
Phase: 1
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'INSIDE'
Flow type: NO FLOW
```

I (1) got initial, attempting ownership.

```
Phase: 2
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'INSIDE'
Flow type: NO FLOW
```

I (1) am becoming owner

Unità-1-1 (server d'inoltro)

<#root>

```
firepower#
```

cluster exec show cap CAPO packet-number 1 trace

```
unit-1-1(LOCAL):*******************************************************

1: 18:10:12.842317 192.168.240.51.80 > 192.168.240.50.51844: S 2339579109:2339579109(0) ack 4082593464 w
Phase: 1
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'OUTSIDE'
Flow type: NO FLOW
```

I (0) am asking director (1).

Traffico di ritorno (TCP SYN/ACK)

Unità-2-1 (proprietario/direttore)

<#root>

firepower#

cluster exec unit unit-2-1 show cap CAPO packet-number 2 trace

2: 18:10:12.843660 192.168.240.51.80 > 192.168.240.50.51844: S 2339579109:2339579109(0) ack 4082593464 w
Phase: 1
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'OUTSIDE'
Flow type: FULL

I (1) am owner, update sender (0).

Phase: 2
Type: FLOW-LOOKUP
Subtype:
Result: ALLOW
Config:
Additional Information:

Found flow with id 7109, using existing flow

Osservazione 4. I syslog del piano dati FTD mostrano la creazione e la terminazione della connessione su tutte le unità:

- Unit-1-1 (proprietario)
- Unità-2-1 (server d'inoltro)
- Unità-3-1 (proprietario/director di backup)

<#root>

firepower#

cluster exec show log | include 51844

unit-1-1(LOCAL):***
Dec 02 2020 18:10:12: %FTD-6-302022:

Built forwarder stub TCP connection

for OUTSIDE:192.168.240.51/80 (192.168.240.51/80) to unknown:192.168.240.50/51844 (192.168.240.50/5184
Dec 02 2020 18:10:22: %FTD-6-302023:

Teardown forwarder TCP connection

for OUTSIDE:192.168.240.51/80 to unknown:192.168.240.50/51844 duration 0:00:09 forwarded bytes 1024001

unit-2-1:***
Dec 02 2020 18:10:12: %FTD-6-302303:

Built TCP state-bypass connection

 7109 from INSIDE:192.168.240.50/51844 (192.168.240.50/51844) to OUTSIDE:192.168.240.51/80 (192.168.240
Dec 02 2020 18:10:22: %FTD-6-302304:

Teardown TCP state-bypass connection

 7109 from INSIDE:192.168.240.50/51844 to OUTSIDE:192.168.240.51/80 duration 0:00:09 bytes 1024001888 T

unit-3-1:**
Dec 02 2020 18:10:12: %FTD-6-302022:

Built backup stub TCP connection

 for INSIDE:192.168.240.50/51844 (192.168.240.50/51844) to OUTSIDE:192.168.240.51/80 (192.168.240.51/80
Dec 02 2020 18:10:22: %FTD-6-302023:

Teardown backup TCP connection

 for INSIDE:192.168.240.50/51844 to OUTSIDE:192.168.240.51/80 duration 0:00:09 forwarded bytes 0 Cluste

Caso di studio 7. Traffico asimmetrico (Inline-set, il proprietario è diverso dal director)

Il proprietario è l'unità 2-1 (ci sono pacchetti su entrambe le interfacce INSIDE ed OUTSIDE per le acquisizioni di reject-hide, mentre l'unità 3-1 ha solo su OUTSIDE):

<#root>

firepower#

cluster exec show cap

unit-1-1(LOCAL):**
capture CCL type raw-data buffer 33554432 interface cluster [Capturing - 13902 bytes]
capture CAPO type raw-data trace interface OUTSIDE [Capturing - 90 bytes]
match tcp host 192.168.240.50 host 192.168.240.51 eq www
capture CAPI type raw-data trace interface INSIDE [Capturing - 0 bytes]
match tcp host 192.168.240.50 host 192.168.240.51 eq www
capture CAPO_RH type raw-data reinject-hide interface OUTSIDE [Capturing - 0 bytes]
match tcp host 192.168.240.50 host 192.168.240.51 eq www
capture CAPI_RH type raw-data reinject-hide interface INSIDE [Capturing - 0 bytes]
match tcp host 192.168.240.50 host 192.168.240.51 eq www

unit-2-1

:**
capture CCL type raw-data buffer 33554432 interface cluster [Buffer Full - 33553936 bytes]
capture CAPO type raw-data trace interface OUTSIDE [Buffer Full - 523126 bytes]
match tcp host 192.168.240.50 host 192.168.240.51 eq www
capture CAPI type raw-data trace interface INSIDE [Buffer Full - 523126 bytes]
match tcp host 192.168.240.50 host 192.168.240.51 eq www
capture CAPO_RH type raw-data

reinject-hid

e

 interface

OUTSIDE

[Buffer Full -

524230 bytes

]
match tcp host 192.168.240.50 host 192.168.240.51 eq www
capture CAPI_RH type raw-data

reinject-hide

interface

INSIDE

[Buffer Full -

523126 bytes

]
match tcp host 192.168.240.50 host 192.168.240.51 eq www

unit-3-1

:**********
capture CCL type raw-data buffer 33554432 interface cluster [Buffer Full - 33553566 bytes]
capture CAPO type raw-data trace interface OUTSIDE [Buffer Full - 523522 bytes]
match tcp host 192.168.240.50 host 192.168.240.51 eq www
capture CAPI type raw-data trace interface INSIDE [Capturing - 0 bytes]
match tcp host 192.168.240.50 host 192.168.240.51 eq www
capture CAPO_RH type raw-data

reinject-hide

interface

OUTSIDE

[Buffer Full -

523432 bytes

]
match tcp host 192.168.240.50 host 192.168.240.51 eq www
capture CAPI_RH type raw-data reinject-hide interface INSIDE [Capturing - 0 bytes]
match tcp host 192.168.240.50 host 192.168.240.51 eq www

Osservazione 2. Analisi del flag di connessione per il flusso con porta sorgente 59210.

<#root>

firepower#

cluster exec show conn addr 192.168.240.51

unit-1-1

(LOCAL):**********

25 in use, 102 most used
Cluster:
fwd connections: 0 in use, 1 most used
dir connections: 2 in use, 122 most used
centralized connections: 0 in use, 39 most used
VPN redirect connections: 0 in use, 0 most used
Inspect Snort:
preserve-connection: 0 enabled, 0 in effect, 4 most enabled, 1 most in effect

TCP OUTSIDE 192.168.240.51:80 INSIDE 192.168.240.50:

59210

, idle 0:00:03, bytes 0,

flags Y

unit-2-1

:**********
21 in use, 271 most used
Cluster:
fwd connections: 0 in use, 2 most used
dir connections: 0 in use, 28 most used
centralized connections: 0 in use, 14 most used
VPN redirect connections: 0 in use, 0 most used
Inspect Snort:
preserve-connection: 0 enabled, 0 in effect, 249 most enabled, 0 most in effect

TCP OUTSIDE 192.168.240.51:80 INSIDE 192.168.240.50:

59210

, idle 0:00:00, bytes 610132872,

flags b N

unit-3-1

:**********
19 in use, 55 most used
Cluster:
fwd connections: 1 in use, 5 most used
dir connections: 0 in use, 127 most used
centralized connections: 0 in use, 24 most used
VPN redirect connections: 0 in use, 0 most used
Inspect Snort:
preserve-connection: 0 enabled, 0 in effect, 1 most enabled, 0 most in effect

TCP OUTSIDE 192.168.240.51:80 NP Identity Ifc 192.168.240.50:

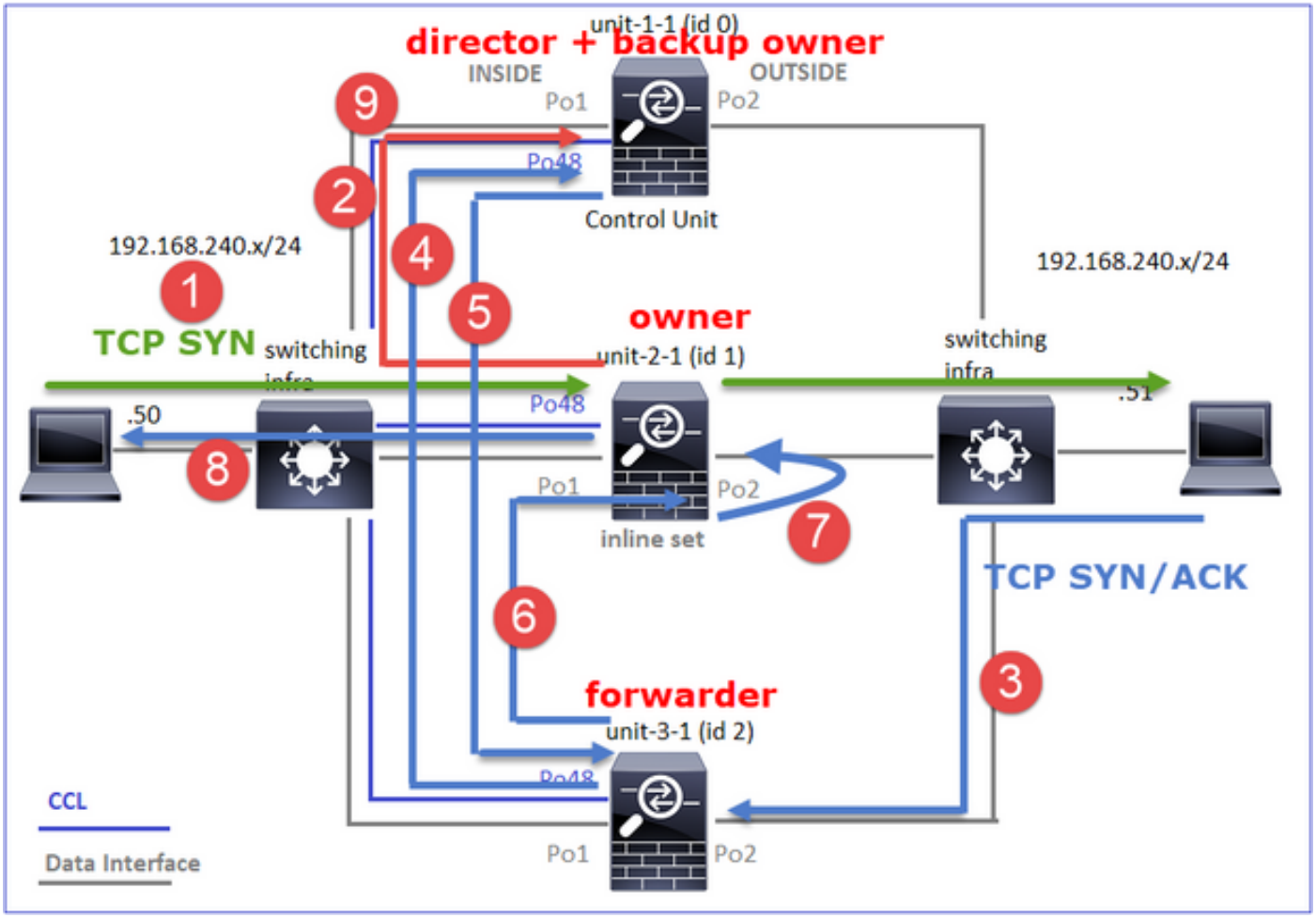
59210

, idle 0:00:00, bytes 0,

flags z

Unità	Contrassegna	Nota
Unità-1-1	Y	· Responsabile/Backup
Unità-2-1	b N	· Proprietario flusso: l'unità gestisce il flusso
Unità-3-1	z	· Inoltro

Ciò può essere visualizzato come:



1. Il pacchetto TCP SYN arriva dall'host-A all'unità-2-1. L'unità-2-1 diventa il proprietario del flusso e l'unità-1-1 viene selezionata come director
2. L'unità 1-1 è il proprietario del backup (in quanto è il director). Il proprietario del flusso invia un messaggio unicast 'cluster add' su UDP 4193 a. informare il proprietario del backup del flusso.
3. Il pacchetto TCP SYN/ACK arriva dall'host-B all'unità-3-1. Il flusso è asimmetrico.
4. L'unità 3-1 inoltra il pacchetto attraverso la CCL al director (unità 1-1).
5. L'unità 1-1 (direttore) sa che il proprietario è l'unità 2-1, invia il pacchetto al mittente (unità 3-1) e gli notifica che il proprietario è l'unità 2-1.

6. L'unità 3-1 invia il pacchetto all'unità 2-1 (proprietario).
7. L'unità 2-1 reinserisce il pacchetto sull'interfaccia OUTSIDE.
8. L'unità 2-1 inoltra il pacchetto all'host A.
9. Una volta terminata la connessione, il proprietario invia un messaggio di eliminazione del cluster per rimuovere le informazioni sul flusso dal proprietario del backup.

Nota: È importante che il passaggio 2 (pacchetto attraverso la CCL) venga eseguito prima del passaggio 4 (traffico di dati). In un caso diverso (ad esempio, race condition), il direttore non è a conoscenza del flusso. Pertanto, poiché si tratta di un set inline, inoltra il pacchetto verso la destinazione. Se le interfacce non sono in un set inline, il pacchetto di dati viene scartato.

Osservazione 3. La cattura con traccia mostra il traffico asimmetrico e gli scambi attraverso la CCL:

Traffico di inoltro (TCP SYN)

Unit-2-1 (proprietario)

<#root>

```
firepower#
```

cluster exec unit unit-2-1 show cap CAPI packet-number 1 trace

```
1: 09:19:49.760702 192.168.240.50.59210 > 192.168.240.51.80: S 4110299695:4110299695(0) win 29200 <mss
Phase: 1
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'INSIDE'
Flow type: NO FLOW
```

I (1) got initial, attempting ownership.

```
Phase: 2
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'INSIDE'
Flow type: NO FLOW
```

I (1) am becoming owner

Traffico di ritorno (TCP SYN/ACK)

L'unità 3-1 (ID 2 - mittente) invia il pacchetto attraverso la CCL all'unità 1-1 (ID 0 - regista).

<#root>

```
firepower#
cluster exec unit unit-3-1 show cap CAPO packet-number 1 trace


1: 09:19:49.760336 192.168.240.51.80 > 192.168.240.50.59210:
S
 4209225081:4209225081(0)
ack
 4110299696 win 28960 <mss 1460,sackOK,timestamp 567715984 130834570,nop,wscale 7>
Phase: 1
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'OUTSIDE'
Flow type: NO FLOW


I (2) am asking director (0).
```

Unit-1-1 (director) - Unit-1-1 (ID 0) sa che il proprietario del flusso è l'unit-2-1 (ID 1) e invia il pacchetto tramite CCL all'unit-3-1 (ID 2 - forwarder).

<#root>

```
firepower#
cluster exec show cap CAPO packet-number 1 trace


unit-1-1(LOCAL):*******************************************************

1: 09:19:49.761038 192.168.240.51.80 > 192.168.240.50.59210:
S
 4209225081:4209225081(0)
ack
 4110299696 win 28960 <mss 1460,sackOK,timestamp 567715984 130834570,nop,wscale 7>
Phase: 1
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
```

```
Additional Information:
Input interface: 'OUTSIDE'
Flow type: STUB
```

I (0) am director, valid owner (1), update sender (2).

L'unità 3-1 (ID 2 - mittente) ottiene il pacchetto tramite l'ACL e lo invia all'unità 2-1 (ID 1 - proprietario).

<#root>

```
firepower#
```

cluster exec unit unit-3-1 show cap CAPO packet-number 2 trace

```
...
2: 09:19:49.761008 192.168.240.51.80 > 192.168.240.50.59210:
```

S

```
 4209225081:4209225081(0) ack 4110299696 win 28960 <mss 1460,sackOK,timestamp 567715984 130834570,nop,w
Phase: 1
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'OUTSIDE'
Flow type: STUB
```

I (2) am becoming forwarder to (1), sender (0).

Il proprietario rifiuta e inoltra il pacchetto verso la destinazione:

<#root>

```
firepower#
```

cluster exec unit unit-2-1 show cap CAPO packet-number 2 trace

```
2: 09:19:49.775701 192.168.240.51.80 > 192.168.240.50.59210:
```

S

```
 4209225081:4209225081(0)
```

ack

```
 4110299696 win 28960 <mss 1460,sackOK,timestamp 567715984 130834570,nop,wscale 7>
Phase: 1
Type: CLUSTER-EVENT
Subtype:
```

```
Result: ALLOW
Config:
Additional Information:
Input interface: 'OUTSIDE'
Flow type: FULL
```

I (1) am owner, sender (2).

Osservazione 4. I syslog del piano dati FTD mostrano la creazione e la terminazione della connessione su tutte le unità:

- Unità-1-1 (director/proprietario del backup)
- Unit-2-1 (proprietario)
- Unità-3-1 (server d'inoltro)

<#root>

```
firepower#
```

cluster exec show log | i 59210

```
unit-1-1(LOCAL):*******************************************************
Dec 03 2020 09:19:49: %FTD-6-302022:
```

Built director stub TCP connection

```
 for INSIDE:192.168.240.50/59210 (192.168.240.50/59210) to OUTSIDE:192.168.240.51/80 (192.168.240.51/80)
Dec 03 2020 09:19:59: %FTD-6-302023:
```

Teardown director TCP connection

```
 for INSIDE:192.168.240.50/59210 to OUTSIDE:192.168.240.51/80 duration 0:00:09 forwarded bytes 0 Cluste

unit-2-1:*************************************************************
Dec 03 2020 09:19:49: %FTD-6-302303:
```

Built TCP state-bypass connection

```
 14483 from INSIDE:192.168.240.50/59210 (192.168.240.50/59210) to OUTSIDE:192.168.240.51/80 (192.168.240
Dec 03 2020 09:19:59: %FTD-6-302304:
```

Teardown TCP state-bypass connection

```
 14483 from INSIDE:192.168.240.50/59210 to OUTSIDE:192.168.240.51/80 duration 0:00:09 bytes 1024003336 T

unit-3-1:*************************************************************
Dec 03 2020 09:19:49: %FTD-6-302022:
```

Built forwarder stub TCP connection

```
 for OUTSIDE:192.168.240.51/80 (192.168.240.51/80) to unknown:192.168.240.50/59210 (192.168.240.50/5921
Dec 03 2020 09:19:59: %FTD-6-302023:
```

Teardown forwarder TCP connection

```
 for OUTSIDE:192.168.240.51/80 to unknown:192.168.240.50/59210 duration 0:00:09 forwarded bytes 1024003
```

Risoluzione dei problemi

Introduzione alla risoluzione dei problemi dei cluster

I problemi del cluster possono essere classificati in:

- Problemi del Control Plane (problemi relativi alla stabilità del cluster)
- Problemi relativi al Data Plane (problemi relativi al traffico di transito)

Problemi del Data Plane del cluster

Problemi comuni NAT/PAT

Considerazioni importanti sulla configurazione

- I pool PAT (Port Address Translation) devono disporre di un numero di IP pari almeno al numero di unità nel cluster, preferibilmente più IP rispetto ai nodi del cluster.
- I comandi di default di xlate per sessione devono essere mantenuti, a meno che non vi sia un motivo specifico per disabilitarli. Qualsiasi estensione PAT creata per una connessione in cui l'estensione per sessione è disabilitata viene sempre gestita dall'unità del nodo di controllo nel cluster, con conseguente riduzione delle prestazioni.

Utilizzo elevato dell'intervallo del pool PAT a causa del traffico proveniente da porte basse che causa lo squilibrio IP del cluster

L'FTD divide un IP PAT in intervalli e tenta di mantenere l'xlate nello stesso intervallo di origine. Nella tabella viene mostrato come una porta di origine viene convertita in una porta globale all'interno dello stesso intervallo di origine.

Porta originale Src	Translated Src Port
1-511	1-511
512-1023	512-1023
1024-65535	1024-65535

Quando un intervallo di porte di origine è pieno ed è necessario allocare un nuovo xlate di porta da tale intervallo, FTD passa all'IP successivo per allocare nuove conversioni per l'intervallo di porte di origine.

Sintomi

Problemi di connettività per il traffico NAT che attraversa il cluster

Verifica

<#root>

#

show nat pool

I log del data plane FTD mostrano l'esaurimento del pool PAT:

<#root>

Dec 9 09:00:00 192.0.2.10 FTD-FW %ASA-3-202010:

PAT pool exhausted. Unable to create TCP connection

 from Inside:192.0.2.150/49464 to Outside:192.0.2.250/20015
Dec 9 09:00:00 192.0.2.10 FTD-FW %ASA-3-202010:

PAT pool exhausted. Unable to create TCP connection

 from Inside:192.0.2.148/54141 to Outside:192.0.2.251/443

Attenuazione

Configurare l'intervallo di porte fisse NAT e includere le porte di riserva.

Inoltre, nella versione successiva alla 6.7/9.15.1 è possibile ottenere una distribuzione non bilanciata del blocco di porte solo quando i nodi lasciano o si uniscono al cluster con un traffico in background elevato soggetto a PAT. L'unico modo in cui viene ripristinato automaticamente è quando i blocchi delle porte vengono liberati per essere ridistribuiti tra i nodi.

Con la distribuzione basata su blocchi di porte, quando un nodo viene allocato con, ad esempio, 10 blocchi di porte come pb-1, pb-2 ... pb-10. Il nodo inizia sempre con il primo blocco di porte disponibile e alloca una porta casuale da esso fino allo scaricamento. L'allocazione viene spostata al blocco di porta successivo solo quando tutti i blocchi di porta fino a quel punto sono esauriti.

Ad esempio, se un host stabilisce 512 connessioni, l'unità alloca le porte mappate per tutte le 512 connessioni da pb-1 in modo casuale. Ora, con tutte queste 512 connessioni attive, quando l'host stabilisce la 513a connessione poiché pb-1 è esaurito, si sposta su pb-2 e alloca una porta casuale da esso. Anche in questo caso, su 513 connessioni, si presuppone che la decima connessione sia terminata e che sia stata cancellata una porta disponibile in pb-1. A questo punto, se l'host stabilisce la 514a connessione, l'unità cluster alloca una porta mappata da pb-1 e non da pb-2, in quanto pb-1 dispone ora di una porta libera (rilasciata come parte della decima rimozione della connessione).

È importante tenere presente che l'allocazione avviene a partire dal primo blocco di porte disponibile con porte libere, in modo che gli ultimi blocchi di porte siano sempre disponibili per la ridistribuzione in un sistema a carico normale. Inoltre, PAT viene generalmente utilizzato per connessioni di breve durata. La probabilità che un blocco di porte diventi disponibile in un periodo di tempo più breve è molto elevata. Pertanto, il tempo necessario per bilanciare la distribuzione del pool può migliorare con la distribuzione del pool basata su blocchi di porte.

Tuttavia, nel caso in cui tutti i blocchi di porte, da pb-1 a pb-10, siano esauriti o ciascun blocco di porte contenga una porta per una connessione di lunga durata, i blocchi di porte non vengono mai liberati rapidamente e vengono ridistribuiti. In tal caso, l'approccio meno dirompente consiste nel:

1. Identificare i nodi con blocchi di porte eccessivi (visualizzare il riepilogo dei cluster del pool nat).
2. Identificare i blocchi di porte meno utilizzati in tale nodo (visualizzare i dettagli ip <addr> del pool nat).
3. Cancellare gli xlate per tali blocchi di porte (cancellare xlate global <addr> gport 'start-end') per renderli disponibili per la ridistribuzione.

⚠ Avviso: L'operazione interrompe le connessioni interessate.

Impossibile accedere a siti Web a doppio canale (come webmail, banking, ecc.) o a siti Web SSO quando viene effettuato il reindirizzamento a una destinazione diversa.

Sintomi

Impossibile accedere ai siti Web a doppio canale (come webmail, siti Web bancari e così via). Quando un utente si connette a un sito Web che richiede al client di aprire un secondo socket/connessione e la seconda connessione viene sottoposta a hashing a un membro del cluster diverso da quello a cui è stato eseguito l'hashing della prima connessione e il traffico utilizza un pool IP PAT, il traffico viene reimpostato dal server quando riceve la connessione da un diverso indirizzo IP pubblico.

Verifica

Acquisire le immagini del cluster del piano dati per verificare come viene gestito il flusso di transito interessato. In questo caso, un reset TCP viene dal sito Web di destinazione.

Attenuazione (precedente alla 6.7/9.15.1)

- Verificare se nelle applicazioni multisessione vengono utilizzati più indirizzi IP mappati.
- Utilizzare il comando show nat pool cluster summary per verificare se il pool è distribuito uniformemente.
- Utilizzare il comando cluster exec show conn per verificare se il traffico è bilanciato correttamente.
- Utilizzare il comando show nat pool cluster ip <indirizzo>detail per controllare l'utilizzo del pool da parte di sticky IP.
- Abilitare syslog 305021 (6.7/9.15) per individuare le connessioni che non sono riuscite a

utilizzare sticky IP.
- Per risolvere il problema, aggiungere altri indirizzi IP al pool PAT o ottimizzare l'algoritmo di bilanciamento del carico sugli switch connessi.

Informazioni sull'algoritmo di bilanciamento del carico del canale etere:

- Per configurazioni diverse da FP9300 e se l'autenticazione avviene tramite un server: Regolare l'algoritmo di bilanciamento del carico del canale etere sullo switch adiacente da IP/porta di origine e IP/porta di destinazione a IP di origine e IP di destinazione.
- Per configurazioni diverse da FP9300 e se l'autenticazione avviene tramite più server: Regolare l'algoritmo di bilanciamento del carico del canale etere sullo switch adiacente da IP/porta di origine e IP/porta di destinazione a IP di origine.
- FP9300: Sullo chassis FP9300 l'algoritmo di bilanciamento del carico è fisso come source-dest-port source-dest-ip source-dest-mac e non può essere modificato. La soluzione, in questo caso, è usare FlexConfig per aggiungere comandi xlate per sessione deny alla configurazione FTD per forzare il traffico di alcuni indirizzi IP di destinazione (per le applicazioni problematiche/incompatibili) a essere gestito solo dal nodo di controllo nel cluster all'interno dello chassis. La soluzione viene fornita con questi effetti collaterali:
    - Nessun bilanciamento del carico del traffico convertito in modo diverso (tutto va al nodo di controllo).
    - Possibilità di esaurimento degli slot xlate (e conseguente impatto negativo sulla conversione NAT per altro traffico sul nodo di controllo).
    - Scalabilità ridotta del cluster all'interno dello chassis.

Prestazioni del cluster ridotte a causa di tutto il traffico inviato al nodo di controllo. Numero insufficiente di indirizzi IP PAT nei pool.

Sintomi

Il numero di IP PAT nel cluster non è sufficiente per allocare un IP libero ai nodi di dati. Di conseguenza, tutto il traffico soggetto alla configurazione PAT viene inoltrato al nodo di controllo per l'elaborazione.

Verifica

Utilizzare il comando show nat pool cluster per visualizzare le allocazioni di ciascuna unità e confermare che tutte possiedano almeno un indirizzo IP nel pool.

Attenuazione

Per le versioni precedenti alla 6.7/9.15.1, assicurarsi di avere un pool PAT di dimensioni almeno uguali al numero di nodi nel cluster. Nelle versioni successive alla 6.7/9.15.1 con il pool PAT, i blocchi di porte vengono allocati da tutti gli IP del pool PAT. Se l'utilizzo del pool PAT è molto elevato, il che porta ad esaurimento frequente del pool, è necessario aumentare le dimensioni del pool PAT (vedere la sezione Domande frequenti).

Prestazioni ridotte a causa di tutto il traffico inviato al nodo di controllo perché gli xlate non sono abilitati per sessione.

Sintomi

Molti flussi di backup UDP ad alta velocità vengono elaborati attraverso il nodo di controllo del cluster, con un conseguente impatto sulle prestazioni.

Introduzione

Un nodo di dati che utilizza PAT può elaborare solo connessioni che utilizzano xlate abilitate per sessione. Utilizzare il comando show run all xlate per verificare la configurazione di xlate per sessione.

Per sessione abilitata significa che l'estensione viene immediatamente disattivata quando la connessione associata viene disattivata. Ciò consente di migliorare le prestazioni delle connessioni al secondo quando le connessioni sono soggette a PAT. Le porte non per sessione rimangono attive per altri 30 secondi dopo l'interruzione della connessione associata e, se la velocità di connessione è sufficientemente alta, le porte TCP/UDP da 65 KB disponibili su ciascun IP globale possono essere usate in un breve periodo di tempo.

Per impostazione predefinita, tutto il traffico TCP è per xlate abilitato e solo il traffico DNS UDP è per sessione abilitato. Questo significa che tutto il traffico UDP non DNS viene inoltrato al nodo di controllo per l'elaborazione.

Verifica

Utilizzare questo comando per controllare la connessione e la distribuzione dei pacchetti tra le unità cluster:

<#root>

```
firepower#
show cluster info conn-distribution

firepower#
show cluster info packet-distribution

firepower#
show cluster info load-monitor
```

Utilizzare il comando cluster exec show conn per verificare i nodi cluster proprietari delle connessioni UDP.

<#root>

```
firepower#
cluster exec show conn
```

Utilizzare questo comando per comprendere l'utilizzo del pool nei nodi del cluster.

<#root>

```
firepower#
cluster exec show nat pool ip
```

```
      | in UDP
```

Attenuazione

Configurare il PAT per sessione (comando enable udp per sessione) per il traffico di interesse (ad esempio, UDP). Per il protocollo ICMP, non è possibile modificare il protocollo PAT multisessione predefinito. In questo modo, il traffico ICMP viene gestito sempre dal nodo di controllo quando è configurato il protocollo PAT.

La distribuzione del pool PAT non è bilanciata quando i nodi lasciano o si uniscono al cluster.

Sintomi

- Problemi di connettività poiché l'allocazione IP di PAT può sbilanciarsi nel tempo a causa di unità che escono e si uniscono al cluster.
- Nella versione successiva alla 6.7/9.15.1, possono esserci casi in cui il nodo appena aggiunto non è in grado di ottenere un numero sufficiente di blocchi di porte. Un nodo privo di blocco porta reindirizza il traffico al nodo di controllo. Un nodo che dispone di almeno un blocco di porte gestisce il traffico e lo scarta una volta esaurito il pool.

Verifica

- I syslog del piano dati mostrano messaggi come:

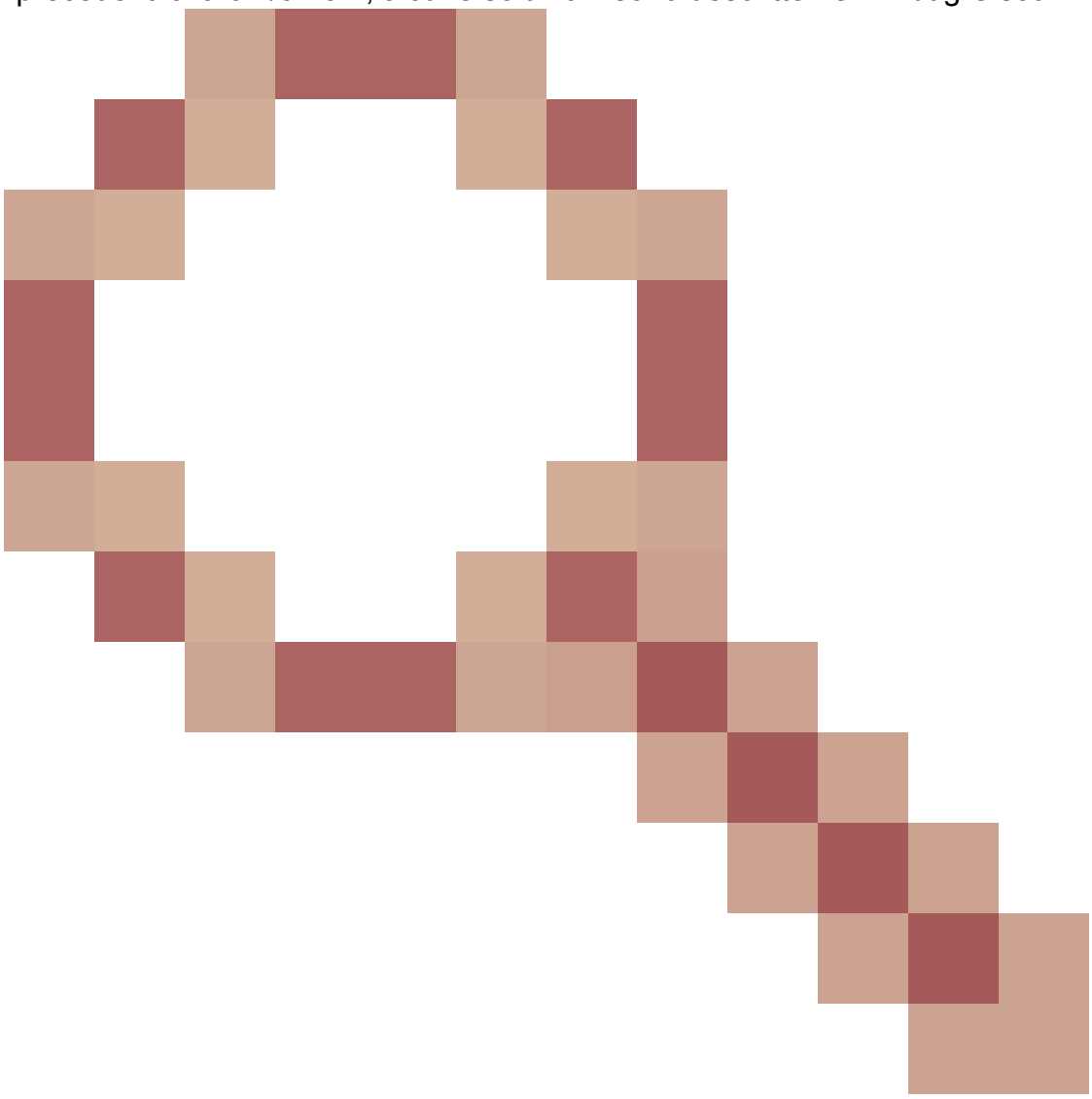
<#root>

```
%ASA-3-202010:
NAT pool exhausted. Unable to create TCP connection
 from inside:192.0.2.1/2239 to outside:192.0.2.150/80
```

- Utilizzare il comando show nat pool cluster summary per identificare la distribuzione del pool.
- Utilizzare il comando cluster exec show nat pool ip <addr>detail per comprendere l'utilizzo del pool tra i nodi del cluster.

Attenuazione

- Per le versioni precedenti alla 6.7/9.15.1, alcune soluzioni sono descritte nell'ID bug Cisco



CSCvd10530

.
- Nella versione successiva alla 6.7/9.15.1, usare il comando clear xlate global <ip> gport <start-end> per cancellare manualmente alcuni dei blocchi di porta sugli altri nodi per la ridistribuzione sui nodi richiesti.

Sintomi

Principali problemi di connettività per il traffico gestito dal cluster. Questo perché il piano dati FTD, per progetto, non invia GARP per gli indirizzi NAT globali.

Verifica

La tabella ARP dei dispositivi collegati direttamente mostra diversi indirizzi MAC dell'interfaccia

dati del cluster dopo una modifica del nodo di controllo:

<#root>

```
root@kali2:~/tests#
```

arp -a

```
? (192.168.240.1) at f4:db:e6:
```

33:44:2e

```
 [ether] on eth0
root@kali2:~/tests#
```

arp -a

```
? (192.168.240.1) at f4:db:e6:
```

9e:3d:0e

```
 [ether] on eth0
```

Attenuazione

Configurare l'indirizzo MAC statico (virtuale) sulle interfacce dati del cluster.

Connessioni soggette a errore PAT

Sintomi

Problemi di connettività per il traffico indirizzato dal cluster.

Verifica/mitigazione

- Verificare che la configurazione sia replicata correttamente.
- Verificare che il pool sia distribuito in modo uniforme.
- Verificare che la proprietà del pool sia valida.
- Nessun incremento contatore errori nel contatore del cluster show asp.
- Verificare che i flussi di server di inoltro/director siano stati creati con informazioni corrette.
- Convalida se gli elenchi di backup vengono creati, aggiornati e puliti come previsto.
- Convalida se gli assembly vengono creati e terminati in base al comportamento "per sessione".
- Abilitare "debug nat 2" per l'indicazione di eventuali errori. Nota, questo output può essere molto rumoroso, ad esempio:

<#root>

```
firepower#
```

debug nat 2

```
nat:
no free blocks available to reserve for 192.168.241.59, proto 17


nat: no free blocks available to reserve for 192.168.241.59, proto 17
nat: no free blocks available to reserve for 192.168.241.58, proto 17
nat: no free blocks available to reserve for 192.168.241.58, proto 17
nat: no free blocks available to reserve for 192.168.241.57, proto 17
```

Per interrompere il debug:

<#root>

```
firepower#
un all
```

- Abilitare la connessione e i syslog relativi a NAT per correlare le informazioni a una connessione non riuscita.

Miglioramenti dei percorsi di clustering ASA e FTD (dopo le versioni 9.15 e 6.7)

Cos'è cambiato?

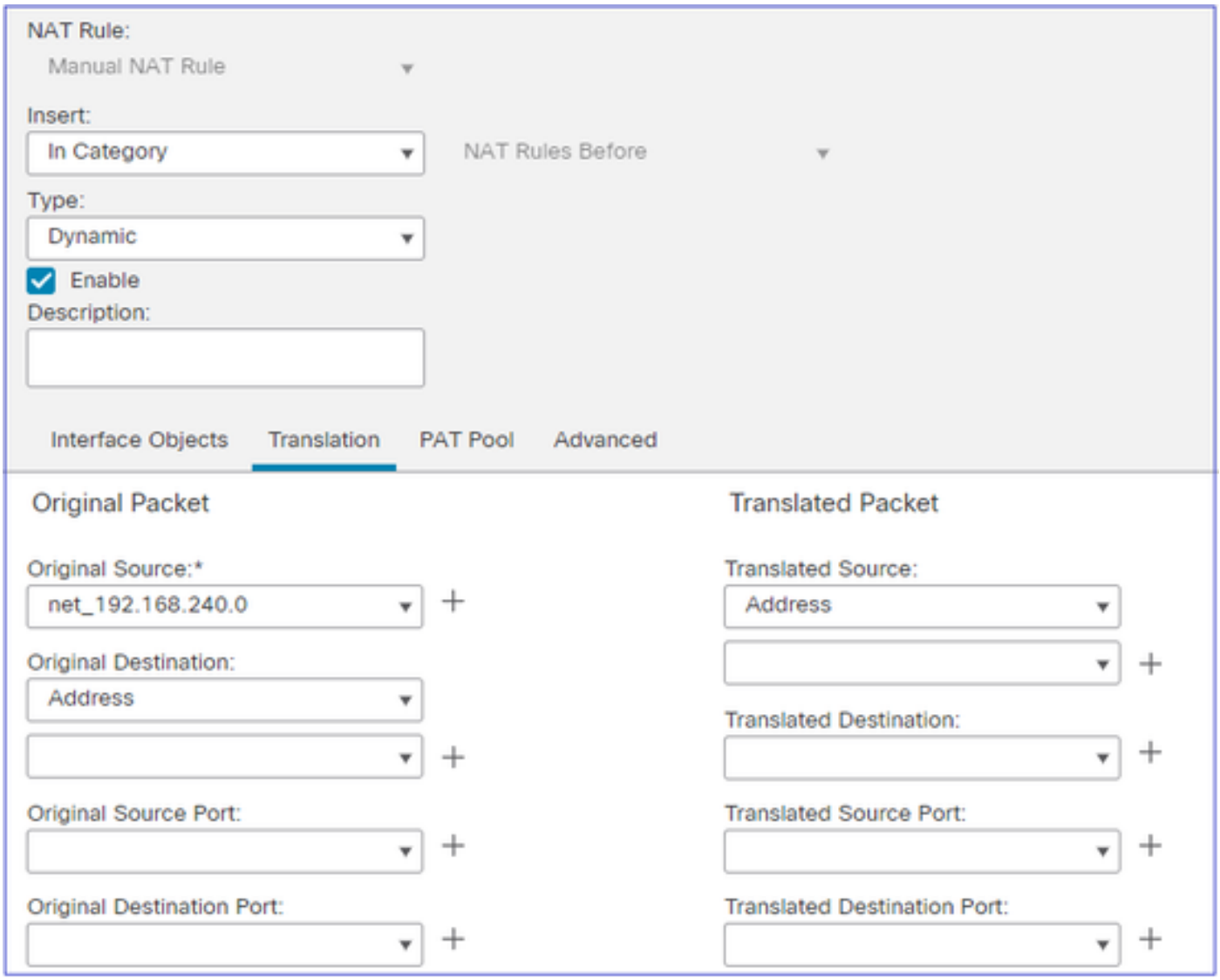
L'operazione PAT è stata riprogettata. I singoli indirizzi IP non vengono più distribuiti a ciascuno dei membri del cluster. Al contrario, gli IP PAT vengono suddivisi in blocchi di porte e distribuiti in modo uniforme (per quanto possibile) tra i membri del cluster, in combinazione con il funzionamento con IP stickiness.

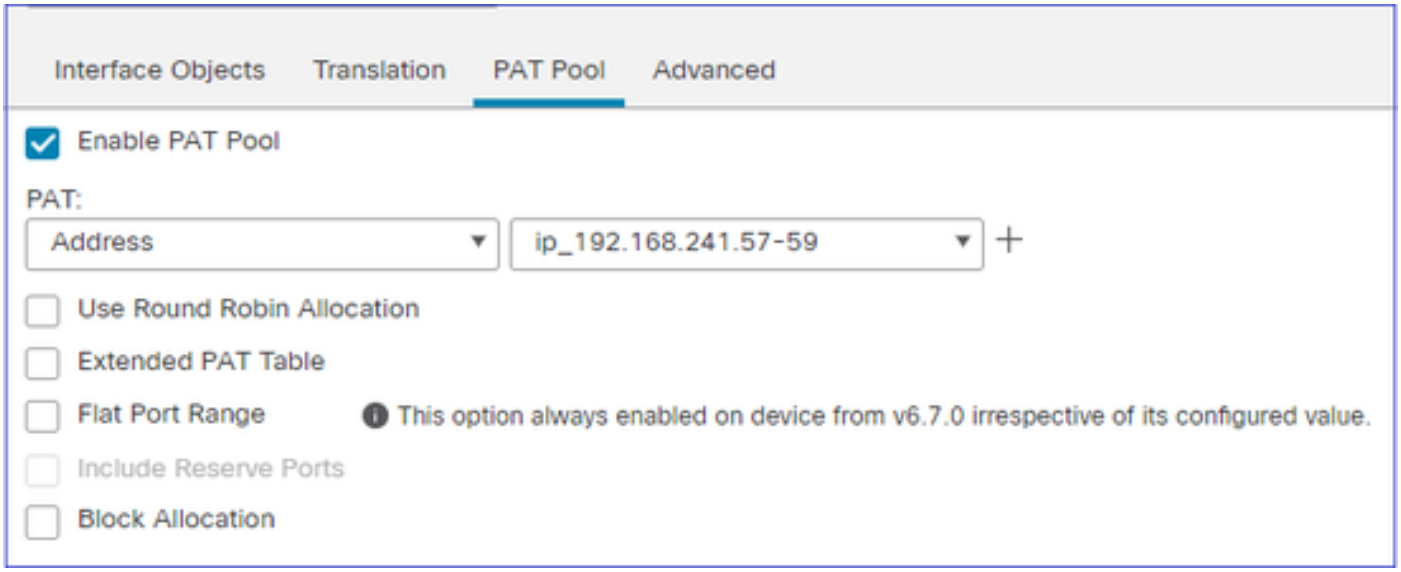
Il nuovo progetto risolve queste limitazioni (vedere la sezione precedente):

- Le applicazioni multisessione sono interessate dalla mancanza di persistenza IP a livello di cluster.
- Il requisito è disporre di un pool PAT di dimensioni almeno uguali al numero di nodi nel cluster.
- La distribuzione del pool PAT non è bilanciata quando i nodi lasciano o si uniscono al cluster.
- Nessun syslog per indicare lo squilibrio del pool PAT.

Da un punto di vista tecnico, anziché gli intervalli di porte predefiniti 1-511, 512-1023 e 1024-65535, ora è disponibile 1024-65535 come intervallo di porte predefinito per PAT. Questo intervallo predefinito può essere esteso in modo da includere l'intervallo di porte privilegiate 1-1023 per le porte PAT normali (opzione "include-reserve").

Questo è un esempio di configurazione di un pool PAT su FTD 6.7. Per ulteriori dettagli, consultare la relativa sezione nella Guida alla configurazione:





Ulteriori informazioni sulla risoluzione dei problemi relativi a PAT

Syslog del piano dati FTD (post 6.7/9.15.1)

Il syslog di annullamento della convalida della persistenza viene generato quando tutte le porte

sono esaurite nell'IP permanente su un nodo cluster e l'allocazione si sposta sul successivo IP disponibile con porte libere, ad esempio:

```
%ASA-4-305021: Ports exhausted in pre-allocated PAT pool IP 192.0.2.100 for host 198.51.100.100 Allocat
```

Un syslog di squilibrio del pool viene generato su un nodo quando si unisce al cluster e non ottiene alcuna o ineguale condivisione di blocchi di porte, ad esempio:

```
%ASA-4-305022: Cluster unit ASA-4 has been allocated 0 port blocks for PAT usage. All units should have
%ASA-4-305022: Cluster unit ASA-4 has been allocated 12 port blocks for PAT usage. All units should hav
```

Comandi show

Stato distribuzione pool

Nell'output di riepilogo del cluster del pool di porte show nat, per ogni indirizzo IP PAT non deve esistere una differenza di più di un blocco di porte tra i nodi in uno scenario di distribuzione bilanciato. Esempi di distribuzione bilanciata e non bilanciata di blocchi di porte.

<#root>

```
firepower#
```

show nat pool cluster summary

```
port-blocks count display order: total, unit-1-1, unit-2-1, unit-3-1
IP OUTSIDE:ip_192.168.241.57-59 192.168.241.57 (126 -
```

42 / 42 / 42

```
)
IP OUTSIDE:ip_192.168.241.57-59 192.168.241.58 (126 - 42 / 42 / 42)
IP OUTSIDE:ip_192.168.241.57-59 192.168.241.59 (126 - 42 / 42 / 42)
```

Distribuzione non bilanciata:

<#root>

```
firepower#
```

show nat pool cluster summary

```
port-blocks count display order: total, unit-1-1, unit-4-1, unit-2-1, unit-3-1
IP outside:src_map 192.0.2.100 (128 - 32 /
```

Stato proprietà pool

Nell'output del comando show nat pool cluster non deve essere presente un singolo blocco di porte con proprietario o backup come SCONOSCIUTO. Se presente, indica un problema con la comunicazione della proprietà del pool. Esempio:

<#root>

firepower#

show nat pool cluster | in

[3072-3583], owner unit-4-1, backup <

UNKNOWN

>
[56832-57343], owner <UNKNOWN>, backup <UNKNOWN>
[10240-10751], owner unit-2-1, backup <UNKNOWN>

Contabilizzazione delle allocazioni di porte in blocchi di porte

Il comando show nat pool è stato migliorato con opzioni aggiuntive per visualizzare informazioni dettagliate e output filtrato. Esempio:

<#root>

firepower#

show nat pool detail

TCP PAT pool INSIDE, address 192.168.240.1, range 1-1023, allocated 0
TCP PAT pool INSIDE, address 192.168.240.1, range 1024-65535, allocated 18
UDP PAT pool INSIDE, address 192.168.240.1, range 1-1023, allocated 0
UDP PAT pool INSIDE, address 192.168.240.1, range 1024-65535, allocated 20
TCP PAT pool OUTSIDE, address 192.168.241.1, range 1-1023, allocated 0
TCP PAT pool OUTSIDE, address 192.168.241.1, range 1024-65535, allocated 18
UDP PAT pool OUTSIDE, address 192.168.241.1, range 1-1023, allocated 0
UDP PAT pool OUTSIDE, address 192.168.241.1, range 1024-65535, allocated 20
UDP PAT pool OUTSIDE, address 192.168.241.58
range 1024-1535, allocated 512
range 1536-2047, allocated 512
range 2048-2559, allocated 512
range 2560-3071, allocated 512

```
...
unit-2-1:************************************************************
UDP PAT pool OUTSIDE, address 192.168.241.57
range 1024-1535, allocated 512 *
range 1536-2047, allocated 512 *
range 2048-2559, allocated 512 *
```

‘*’ indica che si tratta di un blocco di porte di cui è stato eseguito il backup

Per risolvere questo problema, utilizzare il comando clear xlate global <ip> gport <start-end> per cancellare manualmente alcuni dei blocchi di porte sugli altri nodi per la ridistribuzione sui nodi richiesti.

Ridistribuzione dei blocchi di porte attivata manualmente

- In una rete di produzione con traffico costante, quando un nodo esce dal cluster e vi si ricongiunge (probabilmente a causa di un traceback), possono verificarsi casi in cui non è in grado di ottenere una quota uguale del pool o, nel peggiore dei casi, non è in grado di ottenere alcun blocco di porta.
- Utilizzare il comando show nat pool cluster summary per identificare il nodo che possiede più blocchi di porte del necessario.
- Sui nodi proprietari di più blocchi di porte, utilizzare il comando show nat pool ip <addr>detail per individuare i blocchi di porte con il minor numero di allocazioni.
- Utilizzare il comando clear xlate global <address> gport <start-end> per cancellare le conversioni create da quei blocchi di porte in modo che diventino disponibili per la ridistribuzione nei nodi richiesti, ad esempio:

<#root>

```
firepower#
```

show nat pool detail | i 19968

```
        range 19968-20479, allocated 512
        range 19968-20479, allocated 512
        range 19968-20479, allocated 512
```

```
firepower#
```

clear xlate global 192.168.241.57 gport 19968-20479

```
INFO: 1074 xlates deleted
```

Domande frequenti (FAQ) per le versioni successive a 6.7/9.15.1 PAT

D. Se si dispone del numero di indirizzi IP disponibili per il numero di unità disponibili nel cluster, è comunque possibile utilizzare 1 indirizzo IP per unità come opzione?

R. Non più disponibile e non è possibile passare da uno schema di distribuzione di pool basato su

indirizzi IP a uno basato su blocchi di porte e viceversa.

Lo schema precedente di distribuzione del pool basato sull'indirizzo IP ha causato errori dell'applicazione multisessione in cui più connessioni (che fanno parte di una singola transazione dell'applicazione) da un host sono con bilanciamento del carico in nodi diversi del cluster e quindi convertite da diversi indirizzi IP mappati che portano al server di destinazione per vederle come originate da entità diverse.

Inoltre, con il nuovo schema di distribuzione basato su blocchi di porte, anche se ora è possibile lavorare con un solo indirizzo IP PAT, si consiglia sempre di disporre di un numero sufficiente di indirizzi IP PAT in base al numero di connessioni che devono essere gestite tramite PAT.

D. È ancora possibile disporre di un pool di indirizzi IP per il pool PAT per il cluster?

R. Sì. I blocchi di porte di tutti gli IP del pool di porte vengono distribuiti tra i nodi del cluster.

D. Se si utilizza un certo numero di indirizzi IP per il pool PAT, viene fornito lo stesso blocco di porte a ciascun membro per ciascun indirizzo IP?

R. No, ogni indirizzo IP è distribuito in modo indipendente.

D. Tutti i nodi cluster dispongono di tutti gli IP pubblici, ma solo di un sottoinsieme di porte? In questo caso, è garantito che ogni volta che l'IP di origine utilizza lo stesso IP pubblico?

R. È corretto, ogni IP PAT è parzialmente di proprietà di ogni nodo. Se un IP pubblico selezionato è esaurito su un nodo, viene generato un syslog che indica che l'IP permanente non può essere mantenuto e l'allocazione passa all'IP pubblico disponibile successivo. Sia che si tratti di un'installazione standalone, ad alta disponibilità o cluster, la persistenza dell'IP dipende sempre dalla disponibilità del pool.

D. È tutto basato su un singolo indirizzo IP nel pool di indirizzi IP, ma non è applicabile se vengono utilizzati più indirizzi IP nel pool di indirizzi IP?

R. Si applica anche a più indirizzi IP nel pool PAT. I blocchi di porte di ogni IP nel pool PAT vengono distribuiti tra i nodi del cluster. Ogni indirizzo IP nel pool PAT viene suddiviso tra tutti i membri del cluster. Pertanto, se si dispone di una classe C di indirizzi nel pool PAT, ogni membro del cluster dispone di pool di porte da ogni indirizzo del pool PAT.

D. Funziona con CGNAT?

R. Sì, anche CGNAT è supportato. CGNAT, noto anche come PAT di allocazione blocchi, ha una dimensione blocco predefinita di '512' che può essere modificata tramite Xlate block-allocation size CLI. Nel caso di PAT dinamico regolare (non CGNAT), la dimensione del blocco è sempre '512', che è fissa e non configurabile.

D. Se l'unità lascia il cluster, il nodo di controllo assegna l'intervallo di blocchi di porte ad altre unità o lo mantiene su se stesso?

R. Ogni blocco di porte ha un proprietario e un backup. Ogni volta che viene creato da un blocco

di porte, lo xlate viene replicato anche nel nodo di backup del blocco di porte. Quando un nodo esce dal cluster, il nodo di backup possiede tutti i blocchi di porte e tutte le connessioni correnti. Il nodo di backup, dal momento che è diventato il proprietario di questi blocchi di porte aggiuntivi, seleziona un nuovo backup per tali blocchi e replica tutti gli xl correnti in tale nodo per gestire gli scenari di errore.

D. Quali azioni possono essere intraprese sulla base di tale allerta per far rispettare la viscosità?

R: Ci sono due possibili ragioni per le quali non è possibile mantenere la vischiosità.

Motivo-1: Il traffico ha un errato bilanciamento del carico, a causa del quale uno dei nodi vede un numero di connessioni più alto di altri, il che porta a un particolare esaurimento degli indirizzi IP permanenti. È possibile risolvere questo problema se si è certi che il traffico sia distribuito in modo uniforme tra i nodi del cluster. Ad esempio, su un cluster FPR41xx, modificare l'algoritmo di bilanciamento del carico sugli switch connessi. Su un cluster FPR9300, verificare che il numero di blade sullo chassis sia uguale.

Motivo-2: L'utilizzo del pool PAT è molto elevato, il che porta ad esaurimento frequente del pool. Per risolvere questo problema, aumentare le dimensioni del pool PAT.

D. In che modo viene gestito il supporto della parola chiave estesa? Indica se visualizza un errore e impedisce l'aggiunta dell'intero comando NAT durante l'aggiornamento oppure rimuove la parola chiave estesa e visualizza un avviso?

A. L'opzione estesa PAT non è supportata in Cluster da ASA 9.15.1/FP 6.7 in avanti. l'opzione di configurazione non viene rimossa da CLI/ASDM/CSM/FMC. Quando viene eseguita la configurazione (direttamente o indirettamente tramite un aggiornamento), viene visualizzato un messaggio di avviso e la configurazione viene accettata, ma la funzionalità estesa di PAT non viene attivata.

D. Il numero di conversioni è uguale a quello delle connessioni simultanee?

R. In versioni precedenti alla 6.7/9.15.1, anche se era 1-65535, poiché le porte di origine non vengono mai usate molto nell'intervallo 1-1024, in realtà lo rende 1024-65535 (64512 conns). Nell'implementazione successiva alla 6.7/9.15.1 con il comportamento predefinito 'flat', è 1024-65535. Se invece si desidera utilizzare 1-1024, è possibile utilizzare l'opzione "include-reserve".

D. Se il nodo si unisce nuovamente al cluster, avrà come backup il vecchio nodo di backup e a tale nodo verrà assegnato il vecchio blocco di porta?

R. Dipende dalla disponibilità di blocchi di porte in quel momento. Quando un nodo esce dal cluster, tutti i relativi blocchi di porte vengono spostati nel nodo di backup. È quindi il nodo di controllo che accumula i blocchi di porte libere e li distribuisce ai nodi richiesti.

D. In caso di modifica dello stato del nodo di controllo, viene selezionato un nuovo nodo di controllo, l'allocazione del blocco PAT viene mantenuta o i blocchi di porta vengono riallocati in base al nuovo nodo di controllo?

R. Il nuovo nodo di controllo comprende quali blocchi sono stati allocati e quali sono liberi e inizia

da lì.

D. Il numero massimo di terminali è uguale al numero massimo di connessioni simultanee con questo nuovo comportamento?

R. Sì. Il numero massimo di xlate dipende dalla disponibilità delle porte PAT. Non ha nulla a che fare con il numero massimo di connessioni simultanee. Se si consente solo 1 indirizzo, è possibile stabilire 65535 connessioni. Se hai bisogno di più indirizzi IP, devi allocarne di più. Se il numero di indirizzi/porte è sufficiente, è possibile raggiungere il numero massimo di connessioni simultanee.

D. Qual è il processo di allocazione del blocco di porte quando viene aggiunto un nuovo membro del cluster? Cosa succede se viene aggiunto un membro del cluster a causa del riavvio?

R. I blocchi delle porte vengono sempre distribuiti dal nodo di controllo. I blocchi porte vengono allocati a un nuovo nodo solo quando sono presenti blocchi porte liberi. I blocchi di porte liberi indicano che nessuna connessione viene gestita tramite una porta mappata all'interno del blocco di porte.

Inoltre, al successivo join, ogni nodo ricalcola il numero di blocchi di cui è proprietario. Se un nodo contiene un numero di blocchi superiore a quello previsto, rilascia tali blocchi di porte aggiuntivi al nodo di controllo quando e come diventano disponibili. Il nodo di controllo li alloca quindi al nodo di dati appena unito.

D. Sono supportati solo i protocolli TCP e UDP o anche SCTP?

R. SCTP non è mai stato supportato con PAT dinamico. Per il traffico SCTP, si consiglia di utilizzare solo un NAT di oggetto di rete statico.

D. Se un nodo esaurisce le porte di blocco, elimina i pacchetti e non utilizza il successivo blocco IP disponibile?

R: No, non cala immediatamente. Utilizza i blocchi di porte disponibili dal successivo IP porta. Se tutti i blocchi di porte in tutti gli IP delle porte sono esauriti, il traffico viene interrotto.

D. Per evitare il sovraccarico del nodo di controllo in una finestra di aggiornamento del cluster, è preferibile selezionare un nuovo controllo manualmente in anticipo (ad esempio, a metà di un aggiornamento del cluster a 4 unità), anziché attendere che tutte le connessioni vengano gestite sul nodo di controllo?

R. Il controllo deve essere aggiornato per ultimo. Infatti, quando il nodo di controllo esegue la versione più recente, non avvia la distribuzione del pool a meno che tutti i nodi non eseguano la versione più recente. Inoltre, quando viene eseguito un aggiornamento, tutti i nodi di dati con una versione più recente ignorano i messaggi di distribuzione del pool da un nodo di controllo se esegue una versione precedente.

Per una descrizione dettagliata di questa operazione, considerare una distribuzione cluster con 4 nodi A, B, C e D con il controllo A. Di seguito sono riportati i passaggi tipici dell'aggiornamento hitless:

1. Scaricare una nuova versione su ognuno dei nodi.
2. Ricaricare l'unità "D". Tutte le connessioni, gli xl vengono spostati nel nodo di backup.
3. L'unità "D" si accende e:

r. Elabora la configurazione delle parti

b. Suddivide ciascun IP PAT in blocchi di porte

c. Con tutti i blocchi di porte in stato non assegnato

d. Ignora la versione precedente dei messaggi PAT del cluster ricevuti dal controllo

e. Reindirizza tutte le connessioni PAT a Primario.

4. Analogamente, visualizzare altri nodi con la nuova versione.

5. Ricaricare il comando "A" dell'unità. Poiché non è disponibile un backup per il controllo, tutte le connessioni esistenti vengono eliminate

6. Il nuovo controllo avvia la distribuzione dei blocchi di porte nel nuovo formato

7. L'unità "A" si ricongiunge ed è in grado di accettare e di intervenire sui messaggi di distribuzione del blocco di porte

Gestione dei frammenti

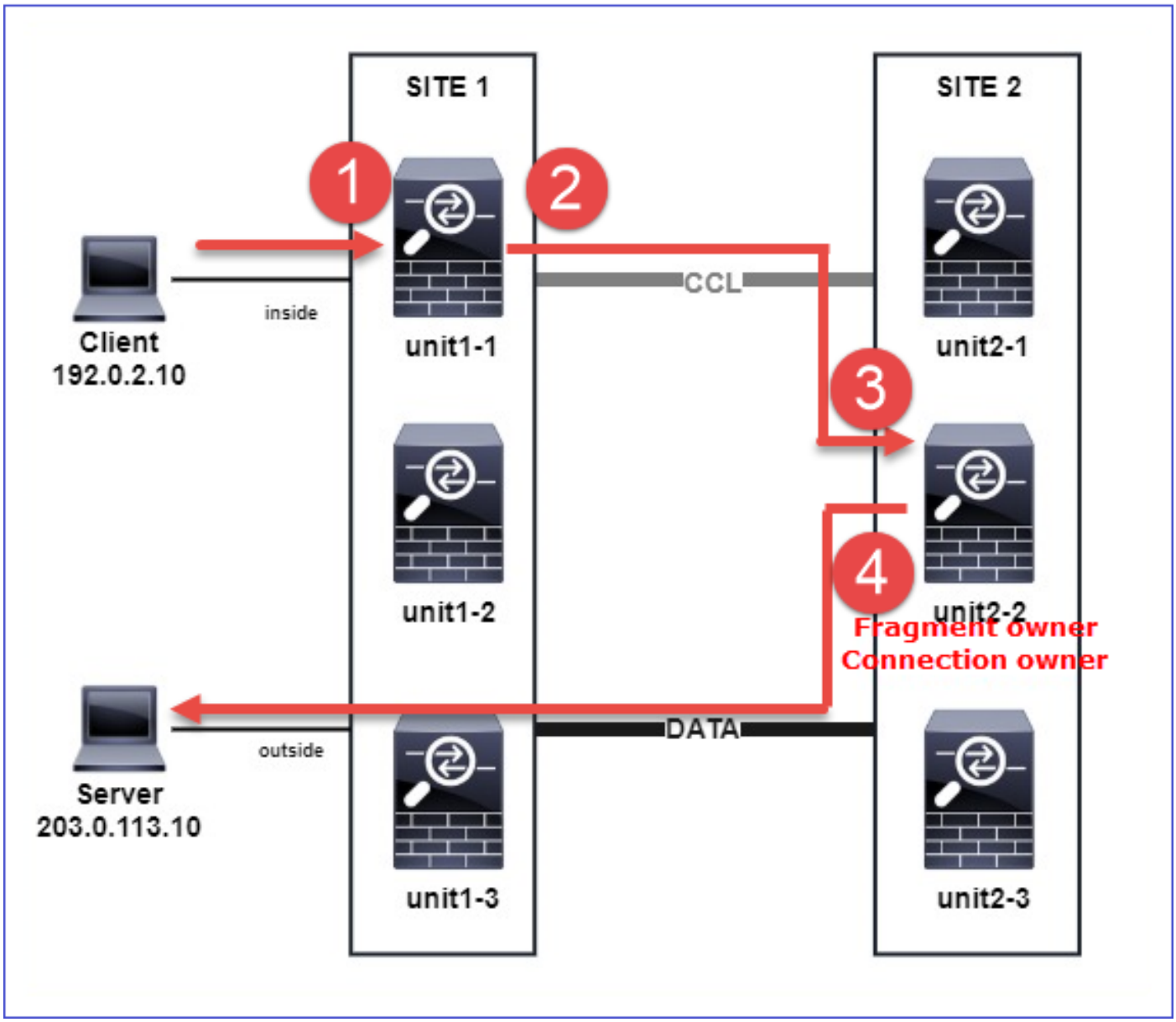
Sintomo

Nelle distribuzioni di cluster tra siti, i pacchetti frammentati che devono essere gestiti in un sito specifico (traffico locale del sito) possono ancora essere inviati alle unità di altri siti, in quanto uno di questi siti può avere il proprietario del frammento.

Nella logica del cluster è definito un ruolo aggiuntivo per le connessioni con pacchetti frammentati: proprietario del frammento.

Per i pacchetti frammentati, il proprietario del frammento viene determinato dalle unità del cluster che ricevono il frammento in base all'hash dell'indirizzo IP di origine, dell'indirizzo IP di destinazione e dell'ID del pacchetto. Tutti i frammenti vengono quindi inoltrati al proprietario tramite il collegamento di controllo del cluster. È possibile bilanciare il carico dei frammenti su unità cluster diverse perché solo il primo frammento include la 5-tupla utilizzata nell'hash di bilanciamento del carico dello switch. Gli altri frammenti non contengono le porte di origine e di destinazione e possono avere il bilanciamento del carico su altre unità del cluster. Il proprietario del frammento ricompone temporaneamente il pacchetto in modo da poter determinare il director in base a un hash dell'indirizzo IP di origine/destinazione e delle porte. Se si tratta di una nuova connessione, il proprietario del frammento diventa il proprietario della connessione. Se si tratta di una connessione esistente, il proprietario inoltra tutti i frammenti al proprietario della connessione tramite il collegamento di controllo del cluster. Il proprietario della connessione ricompone quindi tutti i frammenti.

Prendere in considerazione questa topologia con il flusso di una richiesta echo ICMP frammentata dal client al server:



Per comprendere l'ordine delle operazioni, sono disponibili acquisizioni di pacchetti a livello di cluster nelle interfacce di collegamento di controllo interno, esterno e cluster configurate con l'opzione trace. Inoltre, nell'interfaccia interna è configurata un'acquisizione di pacchetti con l'opzione reject-hide.

<#root>

```
firepower#
```

```
cluster exec capture capi interface inside trace match icmp any any
```

```
firepower#
```

```
cluster exec capture capir interface inside reinject-hide trace match icmp any any
```

```
firepower#
```

```
cluster exec capture capo interface outside trace match icmp any any

firepower#
cluster exec capture capccl interface cluster trace match icmp any any
```

Ordine delle operazioni nel cluster:

1. l'unità 1-1 nel sito 1 riceve i pacchetti di richiesta echo ICMP frammentati.

<#root>

```
firepower#
cluster exec show cap capir

unit-1-1(LOCAL)
:*******************************************************
2 packets captured

1: 20:13:58.227801 802.1Q vlan#10 P0 192.0.2.10 > 203.0.113.10 icmp: echo request

2: 20:13:58.227832 802.1Q vlan#10 P0

2 packets shown
```

2. l'unità 1-1 seleziona l'unità 2-2 nel sito 2 come proprietario del frammento e gli invia pacchetti frammentati.
L'indirizzo MAC di destinazione dei pacchetti inviati dall'unità 1-1 all'unità 2-2 è l'indirizzo MAC del collegamento CCL nell'unità 2-2.

<#root>

```
firepower#
show cap capccl packet-number 1 detail

7 packets captured
1: 20:13:58.227817
0015.c500.018f 0015.c500.029f
 0x0800 Length: 1509
```

192.0.2.10 > 203.0.113.10

 icmp: echo request (wrong icmp csum) (frag 46772:1475@0+) (ttl 3)
1 packet shown

firepower#

show cap capccl packet-number 2 detail

7 packets captured

2: 20:13:58.227832

0015.c500.018f 0015.c500.029f

 0x0800 Length: 637

192.0.2.10 > 203.0.113.10

 (

frag 46772

:603@1480) (ttl 3)
1 packet shown

firepower#

cluster exec show interface po48 | i MAC

unit-1-1(LOCAL):**********
MAC address 0015.c500.018f, MTU 1500
unit-1-2:**********
MAC address 0015.c500.019f, MTU 1500

unit-2-2

:**********

MAC address 0015.c500.029f, MTU 1500

unit-1-3:**********
MAC address 0015.c500.016f, MTU 1500
unit-2-1:**********
MAC address 0015.c500.028f, MTU 1500
unit-2-3:**********
MAC address 0015.c500.026f, MTU 1500

3. l'unità 2-2 riceve, ricompone i pacchetti frammentati e diventa il proprietario del flusso.

<#root>

```
firepower#
```

cluster exec unit unit-2-2 show capture capccl packet-number 1 trace

```
11 packets captured

1: 20:13:58.231845 192.0.2.10 > 203.0.113.10 icmp: echo request
Phase: 1
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'inside'
Flow type: NO FLOW
```

I (2) received a FWD_FRAG_TO_FRAG_OWNER from (0).

```
Phase: 2
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'inside'
```

Flow type: NO FLOW

I (2) have reassembled a packet and am processing it.

```
Phase: 3
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 4
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 5
Type: ROUTE-LOOKUP
Subtype: No ECMP load balancing
Result: ALLOW
Config:
Additional Information:
```

```
Destination is locally connected. No ECMP load balancing.
Found next-hop 203.0.113.10 using egress ifc outside(vrfid:0)

Phase: 6
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'inside'
```

Flow type: NO FLOW

I (2) am becoming owner

```
Phase: 7
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced trust ip any any rule-id 268435460 event-log flow-end
access-list CSM_FW_ACL_ remark rule-id 268435460: PREFILTER POLICY: igasimov_prefilter1
access-list CSM_FW_ACL_ remark rule-id 268435460: RULE: r1
Additional Information:

...

Phase: 19
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 1719, packet dispatched to next module

...

Result:
input-interface: cluster(vrfid:0)
input-status: up
input-line-status: up
output-interface: outside(vrfid:0)
output-status: up
output-line-status: up
```

Action: allow

```
1 packet shown
firepower#
```

cluster exec unit unit-2-2 show capture capccl packet-number 2 trace

```
11 packets captured

2: 20:13:58.231875
Phase: 1
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'inside'


Flow type: NO FLOW



I (2) received a FWD_FRAG_TO_FRAG_OWNER from (0).



Result:
input-interface: cluster(vrfid:0)
input-status: up
input-line-status: up
Action: allow

1 packet shown
```

4. l'unità 2-2 consente i pacchetti in base ai criteri di sicurezza e li invia, tramite l'interfaccia esterna, dal sito 2 al sito 1.

<#root>

```
firepower#

cluster exec unit unit-2-2 show cap capo



2 packets captured



1: 20:13:58.232058 802.1Q vlan#20 P0 192.0.2.10 > 203.0.113.10 icmp: echo request



2: 20:13:58.232058 802.1Q vlan#20 P0
```

Osservazioni/avvertenze

- A differenza del ruolo di director, il proprietario del frammento non può essere localizzato all'interno di un particolare sito. Il proprietario del frammento è determinato dall'unità che in origine riceve i pacchetti frammentati di una nuova connessione e può trovarsi in qualsiasi

sito.

- Poiché anche il proprietario di un frammento può diventare il proprietario della connessione, per inoltrare i pacchetti all'host di destinazione deve essere in grado di risolvere l'interfaccia di uscita e di trovare gli indirizzi IP e MAC dell'host di destinazione o dell'hop successivo. In questo modo, si presume che gli hop successivi debbano essere anche raggiungibili dall'host di destinazione.
- Per ricomporre i pacchetti frammentati, l'ASA/FTD mantiene un modulo di riassemblaggio del frammento IP per ciascuna interfaccia con nome. Per visualizzare i dati operativi del modulo di riassemblaggio del frammento IP, usare il comando show fragment:
  <#root>

  ```
  Interface: inside
  Configuration:

  Size: 200

  , Chain: 24, Timeout: 5, Reassembly: virtual
  Run-time stats: Queue: 0, Full assembly: 0
  Drops: Size overflow: 0, Timeout: 0,
  Chain overflow: 0, Fragment queue threshold exceeded: 0,
  Small fragments: 0, Invalid IP len: 0,
  Reassembly overlap: 0, Fraghead alloc failed: 0,
  SGT mismatch: 0, Block alloc failed: 0,
  Invalid IPV6 header: 0, Passenger flow assembly failed: 0
  ```

  Nelle distribuzioni cluster, il proprietario del frammento o il proprietario della connessione inseriscono i pacchetti frammentati nella coda. La dimensione della coda di frammenti è limitata dal valore del contatore Dimensione (per impostazione predefinita 200) configurato con il comando fragment size <size> <nameif>. Quando le dimensioni della coda di frammenti raggiungono i 2/3 della dimensione, la soglia della coda di frammenti viene considerata superata e tutti i nuovi frammenti che non fanno parte della catena di frammenti corrente vengono scartati. In questo caso, la soglia della coda dei frammenti superata viene incrementata e viene generato il messaggio syslog FTD-3-209006.

<#root>

```
firepower#

show fragment inside


Interface: inside

    Configuration:

Size: 200

, Chain: 24, Timeout: 5, Reassembly: virtual
    Run-time stats:

Queue: 133

, Full assembly: 0
    Drops: Size overflow: 0, Timeout: 8178,
           Chain overflow: 0,
```

```
Fragment queue threshold exceeded: 40802

,
           Small fragments: 0, Invalid IP len: 0,
           Reassembly overlap: 9673, Fraghead alloc failed: 0,
           SGT mismatch: 0, Block alloc failed: 0,
           Invalid IPV6 header: 0, Passenger flow assembly failed: 0


%FTD-3-209006: Fragment queue threshold exceeded, dropped TCP fragment from 192.0.2.10/21456 to 203.0.11
```

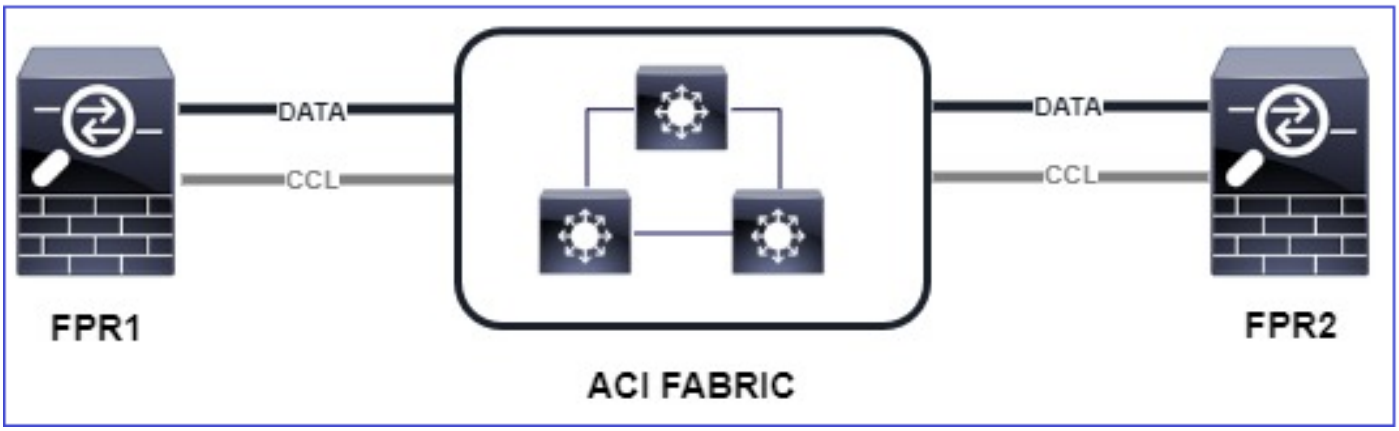
Per risolvere il problema, aumentare le dimensioni in Firepower Management Center > Dispositivi > Gestione dispositivi > [Modifica dispositivo] > Interfacce > [Interfaccia] > Avanzate > Configurazione protezione > Ignora impostazione predefinita frammento, salvare la configurazione e distribuire i criteri. Monitorare quindi il contatore Coda nell'output del comando show fragment e l'occorrenza del messaggio syslog FTD-3-209006.

Problemi ACI

Problemi di connettività intermittenti nel cluster dovuti alla verifica del checksum L4 attivo nel POD ACI

Sintomo

- Problemi di connettività intermittenti tramite il cluster ASA/FTD implementato in un POD ACI.
- Se nel cluster è presente solo un'unità, i problemi di connettività non vengono rilevati.
- I pacchetti inviati da un'unità cluster a una o più altre unità nel cluster non sono visibili in FXOS e nelle acquisizioni dei piani dati delle unità di destinazione.



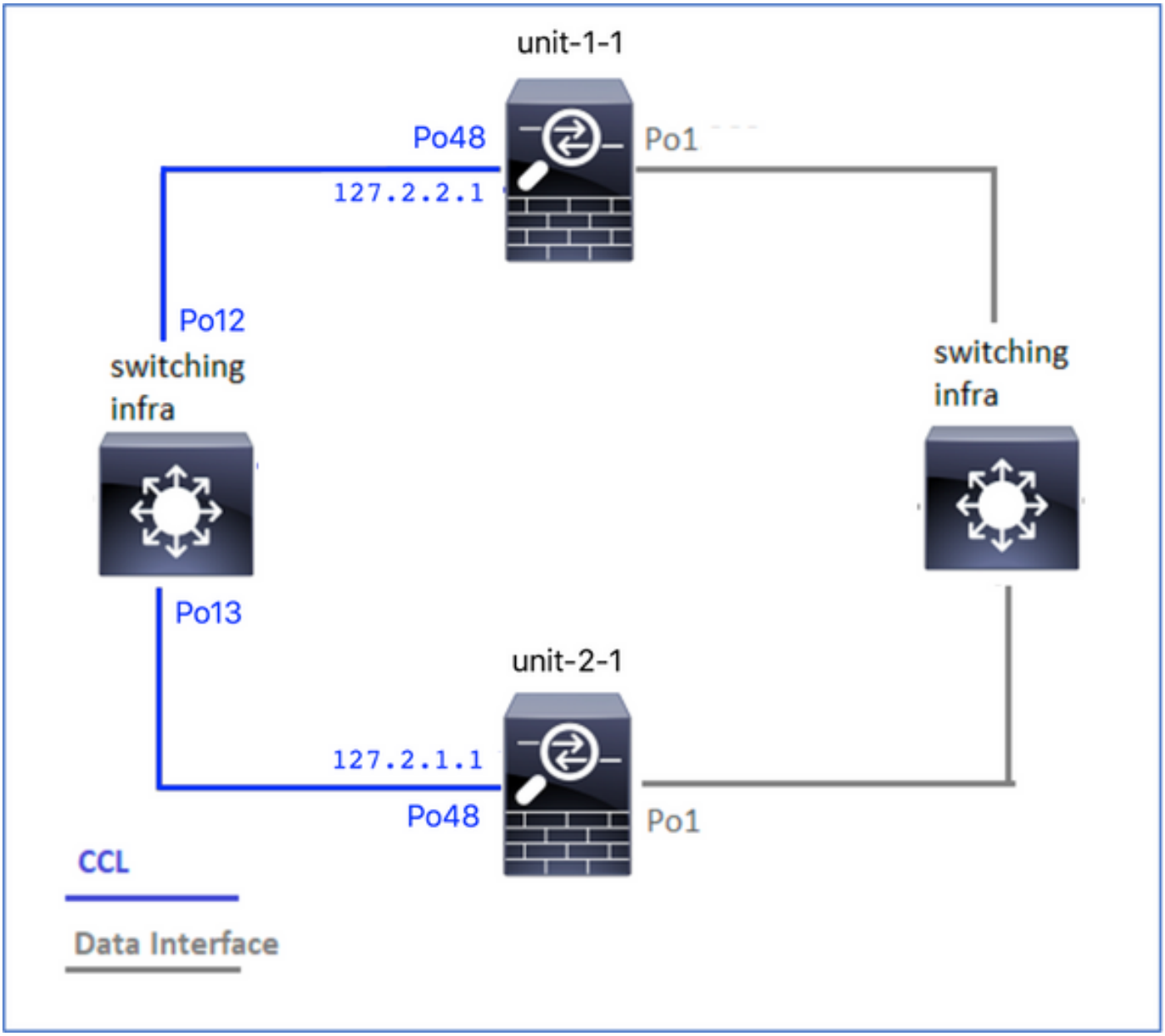
Attenuazione

- Il traffico reindirizzato sul collegamento di controllo del cluster non dispone di un checksum L4 corretto e questo è il comportamento previsto. Gli switch nel percorso del collegamento di controllo del cluster non devono verificare il checksum L4. Gli switch che verificano il checksum L4 possono causare l'eliminazione del traffico. Controllare la configurazione dello switch ACI fabric e verificare che non venga eseguito alcun checksum L4 sui pacchetti ricevuti o inviati tramite il collegamento di controllo del cluster.

Problemi del Control Plane del cluster

Impossibile aggiungere l'unità al cluster

Dimensioni MTU su CCL



Sintomi

Impossibile aggiungere l'unità al cluster. Viene visualizzato il seguente messaggio:

```
The SECONDARY has left the cluster because application configuration sync is timed out on this unit. Di
Cluster disable is performing cleanup..done.
Unit unit-2-1 is quitting due to system failure for 1 time(s) (last failure is SECONDARY application co
All data interfaces have been shutdown due to clustering being disabled. To recover either enable clust
```

Verifica/mitigazione

- Utilizzare il comando show interface sull'FTD per verificare che l'MTU sull'interfaccia del collegamento di controllo del cluster sia superiore di almeno 100 byte all'MTU dell'interfaccia dati:

<#root>

firepower#

show interface

Interface

Port-channel1

 "

Inside

", is up, line protocol is up
  Hardware is EtherSVI, BW 40000 Mbps, DLY 10 usec
    MAC address 3890.a5f1.aa5e,

MTU 9084

Interface

 Port-channel48

 "

cluster

", is up, line protocol is up
  Hardware is EtherSVI, BW 40000 Mbps, DLY 10 usec
    Description: Clustering Interface
    MAC address 0015.c500.028f,

MTU 9184

    IP address 127.2.2.1, subnet mask 255.255.0.

- Eseguire il ping attraverso la CCL, con l'opzione size, per verificare che la MTU della CCL sia configurata correttamente su tutti i dispositivi del percorso.

<#root>

firepower#

ping 127.2.1.1 size 9184

- Usare il comando show interface sullo switch per verificare la configurazione MTU

<#root>

Switch#

show interface

port-channel12

 is up
admin state is up,
  Hardware: Port-Channel, address: 7069.5a3a.7976 (bia 7069.5a3a.7976)

MTU 9084

bytes, BW 40000000 Kbit , DLY 10 usec

port-channel13

 is up
admin state is up,
  Hardware: Port-Channel, address: 7069.5a3a.7967 (bia 7069.5a3a.7967)

MTU 9084

bytes, BW 40000000 Kbit , DLY 10 use

Interfaccia Non Corrispondente Tra Le Unità Cluster

Sintomi

Impossibile aggiungere l'unità al cluster. Viene visualizzato il seguente messaggio:

```
Interface mismatch between cluster primary and joining unit unit-2-1. unit-2-1 aborting cluster join.
Cluster disable is performing cleanup..done.
Unit unit-2-1 is quitting due to system failure for 1 time(s) (last failure is Internal clustering erro
All data interfaces have been shutdown due to clustering being disabled. To recover either enable clust
```

Verifica/mitigazione

Accedere alla GUI di FCM su ciascuno chassis, passare alla scheda Interfacce e verificare se tutti i membri del cluster hanno la stessa configurazione di interfaccia:

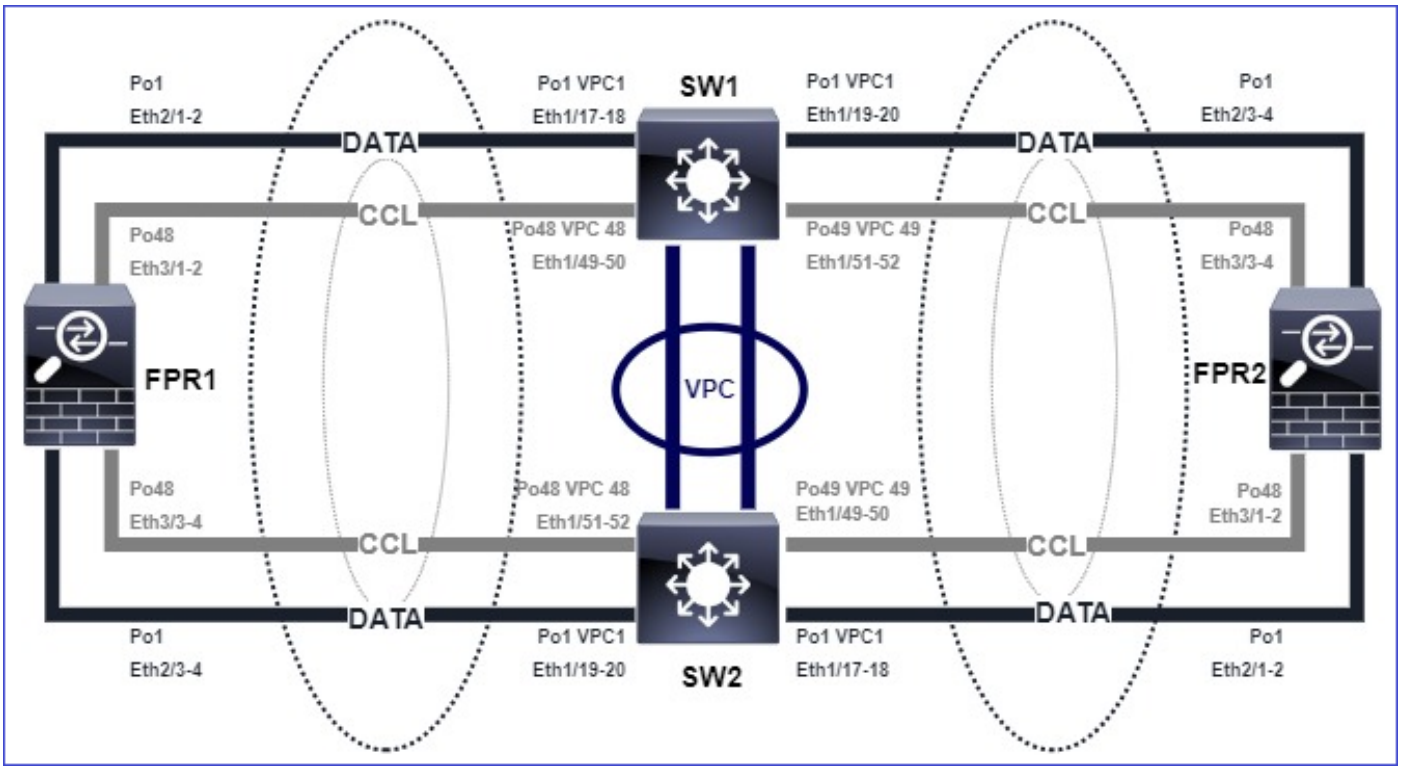
- Interfacce assegnate al dispositivo logico
- Velocità di amministrazione delle interfacce
- Amministrazione - duplex delle interfacce
- Stato interfaccia

Problema dell'interfaccia Data/Port-Channel

Separazione dei cervelli dovuta a problemi di raggiungibilità sulla CCL

Sintomo

Nel cluster sono presenti più unità di controllo. Supponiamo di avere questa topologia:



Chassis 1:

<#root>

```
firepower# show cluster info
```

```
Cluster ftd_cluster1: On
Interface mode: spanned
```

```
This is "unit-1-1" in state PRIMARY
```

```
ID : 0
Site ID : 1
Version : 9.15(1)
Serial No.: FLM2103TU5H
CCL IP : 127.2.1.1
CCL MAC : 0015.c500.018f
Last join : 07:30:25 UTC Dec 14 2020
Last leave: N/A
Other members in the cluster:
Unit "unit-1-2" in state SECONDARY
```

```
ID : 1
Site ID : 1
Version : 9.15(1)
Serial No.: FLM2103TU4D
CCL IP : 127.2.1.2
CCL MAC : 0015.c500.019f
Last join : 07:30:26 UTC Dec 14 2020
Last leave: N/A
Unit "unit-1-3" in state SECONDARY
ID : 3
Site ID : 1
Version : 9.15(1)
Serial No.: FLM2102THJT
CCL IP : 127.2.1.3
CCL MAC : 0015.c500.016f
Last join : 07:31:49 UTC Dec 14 2020
Last leave: N/A
```

Chassis 2:

<#root>

```
firepower# show cluster info
```

```
Cluster ftd_cluster1: On
Interface mode: spanned
```

```
This is "unit-2-1" in state PRIMARY
```

```
ID : 4
Site ID : 1
Version : 9.15(1)
Serial No.: FLM2103TUN1
CCL IP : 127.2.2.1
CCL MAC : 0015.c500.028f
Last join : 11:21:56 UTC Dec 23 2020
Last leave: 11:18:51 UTC Dec 23 2020
Other members in the cluster:
Unit "unit-2-2" in state SECONDARY
ID : 2
Site ID : 1
Version : 9.15(1)
Serial No.: FLM2102THR9
CCL IP : 127.2.2.2
CCL MAC : 0015.c500.029f
Last join : 11:18:58 UTC Dec 23 2020
Last leave: 22:28:01 UTC Dec 22 2020
Unit "unit-2-3" in state SECONDARY
ID : 5
Site ID : 1
Version : 9.15(1)
Serial No.: FLM2103TUML
CCL IP : 127.2.2.3
CCL MAC : 0015.c500.026f
Last join : 11:20:26 UTC Dec 23 2020
```

```
Last leave: 22:28:00 UTC Dec 22 2020
```

Verifica

- Utilizzare il comando ping per verificare la connettività tra gli indirizzi IP del collegamento di controllo del cluster (CCL) delle unità di controllo:

<#root>

```
firepower# ping 127.2.1.1
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 127.2.1.1, timeout is 2 seconds:
```

```
?????
Success rate is 0 percent (0/5)
```

- Controllare la tabella ARP:

<#root>

```
firepower# show arp
```

```
cluster 127.2.2.3 0015.c500.026f 1
cluster 127.2.2.2 0015.c500.029f 1
```

- Nelle unità di controllo, configurare e controllare le acquisizioni sulle interfacce CCL:

<#root>

```
firepower# capture capccl interface cluster
firepower# show capture capccl | i 127.2.1.1
```

```
2: 12:10:57.652310 arp who-has 127.2.1.1 tell 127.2.2.1
41: 12:11:02.652859 arp who-has 127.2.1.1 tell 127.2.2.1
74: 12:11:07.653439 arp who-has 127.2.1.1 tell 127.2.2.1
97: 12:11:12.654018 arp who-has 127.2.1.1 tell 127.2.2.1
126: 12:11:17.654568 arp who-has 127.2.1.1 tell 127.2.2.1
151: 12:11:22.655148 arp who-has 127.2.1.1 tell 127.2.2.1
174: 12:11:27.655697 arp who-has 127.2.1.1 tell 127.2.2.1
```

Attenuazione

- Verificare che le interfacce canale porta CCL siano collegate a interfacce canale porta

separate sullo switch.
- Se sugli switch Nexus vengono utilizzati canali porte virtuali (vPC), verificare che le interfacce canale porta CCL siano collegate a vPC diversi e che la configurazione vPC non presenti uno stato di coerenza non riuscito.
- Verificare che le interfacce porta-canale CCL si trovino nello stesso dominio di broadcast e che la VLAN CCL sia stata creata e autorizzata sulle interfacce.

Di seguito viene riportato un esempio di configurazione dello switch:

```
<#root>

Nexus#

show run int po48-49



interface port-channel48
description FPR1

switchport access vlan 48



vpc 48



interface port-channel49
description FPR2

switchport access vlan 48



vpc 49



Nexus#

 show vlan id 48



VLAN Name Status Ports
---- ----------- --------- -------------------------------

48 CCL active Po48, Po49, Po100, Eth1/53, Eth1/54



VLAN Type Vlan-mode
---- ----- ----------
48 enet CE
```

```
1  Po1  up success success 10,20


48 Po48 up success success 48



49 Po49 up success success 48
```

<#root>

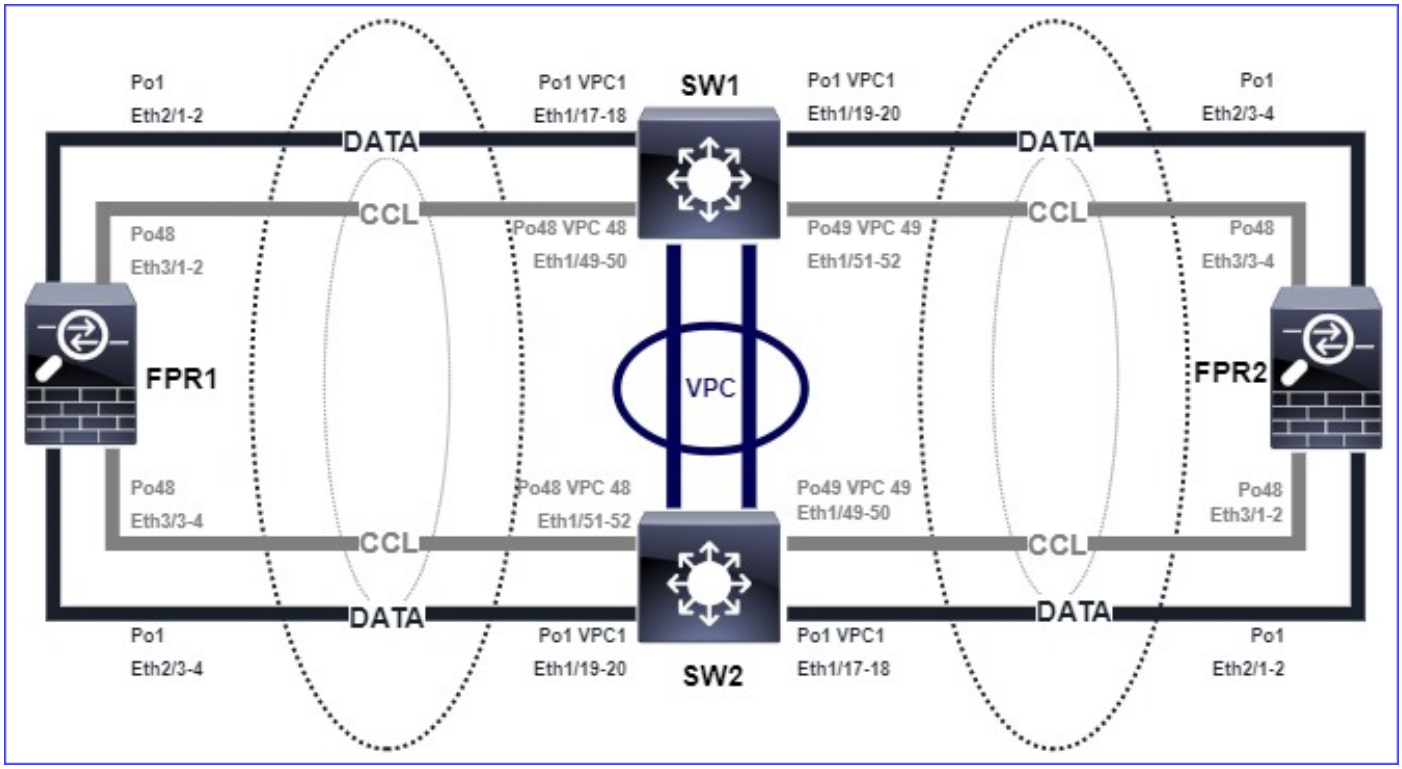
```
Nexus1#

show vpc brief


Legend:
(*) - local vPC is down, forwarding via vPC peer-link

vPC domain id : 1
Peer status : peer adjacency formed ok
vPC keep-alive status : peer is alive
Configuration consistency status : success


Per-vlan consistency status : success



Type-2 consistency status : success


vPC role : primary
Number of vPCs configured : 3
Peer Gateway : Disabled
Dual-active excluded VLANs : -
Graceful Consistency Check : Enabled
Auto-recovery status : Disabled
Delay-restore status : Timer is off.(timeout = 30s)
Delay-restore SVI status : Timer is off.(timeout = 10s)

vPC Peer-link status
---------------------------------------------------------------------
id Port Status Active vlans
-- ---- ------ --------------------------------------------------
1 Po100 up 1,10,20,48-49,148

vPC status
----------------------------------------------------------------------------
id Port Status Consistency Reason Active vlans
-- ---- ------ ----------- ------ ------------
1 Po1 up success success 10,20


48 Po48 up success success 48



49 Po49 up success success 48
```

Cluster disabilitato a causa di interfacce del canale della porta dati sospese

Sintomo

Una o più interfacce del canale della porta dati sono sospese. Quando un'interfaccia dati abilitata a livello amministrativo viene sospesa, tutte le unità cluster nello stesso chassis vengono eliminate dal cluster a causa di un errore del controllo di integrità dell'interfaccia.

Supponiamo di avere questa topologia:



Verifica

- Controllare la console dell'unità di controllo:

<#root>

```
firepower#
Beginning configuration replication to
```

SECONDARY unit-2-2

```
End Configuration Replication to SECONDARY.
Asking SECONDARY unit
```

unit-2-2

```
 to quit because it
```

failed interface health

```
 check 4 times (last failure on
```

Port-channel1

). Clustering must be manually enabled on the unit to rejoin.

- Controllare l'output dei comandi show cluster history e show cluster info trace module hc nelle unità interessate:

<#root>

```
firepower# Unit is kicked out from cluster because of interface health check failure.
Cluster disable is performing cleanup..done.
All data interfaces have been shutdown due to clustering being disabled. To recover either enable clust

Cluster unit unit-2-1 transitioned from SECONDARY to DISABLED


firepower#
```

show cluster history

```
==========================================================================
From State To State Reason
==========================================================================

12:59:37 UTC Dec 23 2020
ONCALL SECONDARY_COLD Received cluster control message

12:59:37 UTC Dec 23 2020
SECONDARY_COLD SECONDARY_APP_SYNC Client progression done

13:00:23 UTC Dec 23 2020
SECONDARY_APP_SYNC SECONDARY_CONFIG SECONDARY application configuration sync done

13:00:35 UTC Dec 23 2020
SECONDARY_CONFIG SECONDARY_FILESYS Configuration replication finished

13:00:36 UTC Dec 23 2020
SECONDARY_FILESYS SECONDARY_BULK_SYNC Client progression done
```

13:01:35 UTC Dec 23 2020

SECONDARY_BULK_SYNC DISABLED Received control message DISABLE (interface health check failure)

<#root>

```
firepower#
```

show cluster info trace module hc

```
Dec 23 13:01:36.636 [INFO]cluster_fsm_clear_np_flows: The clustering re-enable timer is started to expi
Dec 23 13:01:32.115 [INFO]cluster_fsm_disable: The clustering re-enable timer is stopped.
```

Dec 23 13:01:32.115 [INFO]Interface Port-channel1 is down

- Controllare l'output del comando show port-channel summary nella shell dei comandi fxos:

<#root>

```
FPR2(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-Channel Type Protocol Member Ports

--------------------------------------------------------------------------------
```

1 Po1(SD) Eth LACP Eth2/1(s) Eth2/2(s) Eth2/3(s) Eth2/4(s)

```
48 Po48(SU) Eth LACP Eth3/1(P) Eth3/2(P) Eth3/3(P) Eth3/4(P)
```

Attenuazione

- Verificare che tutti gli chassis abbiano lo stesso nome e la stessa password del gruppo cluster.
- Verificare che le interfacce del canale della porta dispongano di interfacce fisiche membro abilitate dall'amministratore con la stessa configurazione duplex/velocità in tutti gli chassis e gli switch.
- Nei cluster interni al sito, verificare che la stessa interfaccia porta-canale dati in tutti gli chassis sia collegata alla stessa interfaccia porta-canale sullo switch.
- Se negli switch Nexus vengono utilizzati canali di porte virtuali (vPC), verificare che la configurazione vPC non presenti uno stato di coerenza non riuscito.
- Nei cluster interni al sito, assicurarsi che la stessa interfaccia del canale della porta dati in tutti gli chassis sia collegata allo stesso vPC.

Problemi di stabilità del cluster

Traceback FXOS

Sintomo

L'unità lascia il cluster.

Verifica/mitigazione

- Utilizzare il comando show cluster history per verificare quando l'unità ha lasciato il cluster

<#root>

```
firepower#
show cluster history
```

- Utilizzare questi comandi per verificare se FXOS dispone di un traceback

<#root>

```
FPR4150#
connect local-mgmt

FPR4150 (local-mgmt)#
dir cores
```

- Raccogliere il file di base generato nel momento in cui l'unità ha lasciato il cluster e fornirlo a TAC.

Disco pieno

Se l'utilizzo del disco nella partizione /ngfw di un'unità cluster raggiunge il 94%, l'unità esce dal cluster. Il controllo dell'utilizzo del disco viene eseguito ogni 3 secondi:

<#root>

```
> show disk

Filesystem Size Used Avail Use% Mounted on
rootfs 81G 421M 80G 1% /
devtmpfs 81G 1.9G 79G 3% /dev
tmpfs 94G 1.8M 94G 1% /run
tmpfs 94G 2.2M 94G 1% /var/volatile
/dev/sda1 1.5G 156M 1.4G 11% /mnt/boot
/dev/sda2 978M 28M 900M 3% /opt/cisco/config
/dev/sda3 4.6G 88M 4.2G 3% /opt/cisco/platform/logs
/dev/sda5 50G 52M 47G 1% /var/data/cores
/dev/sda6 191G 191G 13M
100% /ngfw

cgroup_root 94G 0 94G 0% /dev/cgroups
```

In questo caso, l'output show cluster history visualizza:

<#root>

```
15:36:10 UTC May 19 2021
PRIMARY Event: Primary unit unit-1-1 is quitting
                    due to
```

diskstatus

```
 Application health check failure, and
                    primary's application state is down
```

o

```
14:07:26 CEST May 18 2021
SECONDARY DISABLED Received control message DISABLE (application health check failure)
```

Un altro modo per verificare l'errore è:

<#root>

```
firepower#
```

show cluster info health

```
Member ID to name mapping:
0 - unit-1-1(myself) 1 - unit-2-1

               0   1
Port-channel48 up up
Ethernet1/1 up up
Port-channel12 up up
Port-channel13 up up

Unit overall            healthy healthy
Service health status:
                        0       1
```

diskstatus (monitor on) down down

```
snort (monitor on)      up      up
Cluster overall         healthy
```

Inoltre, se il disco è circa il 100%, l'unità potrebbe avere difficoltà a unirsi al cluster finché non viene liberato spazio su disco.

Protezione da overflow

Ogni 5 minuti ogni unità cluster controlla l'utilizzo della CPU e della memoria nell'unità locale e peer. Se l'utilizzo è superiore alle soglie di sistema (CPU LINA 50% o memoria LINA 59%), viene visualizzato un messaggio informativo in:

- Syslog (FTD-6-748008)
- File log/cluster_trace.log, ad esempio:

<#root>

```
firepower#

more log/cluster_trace.log | i CPU


May 20 16:18:06.614 [INFO][

CPU load 87%

 | memory load 37%] of module 1 in chassis 1 (unit-1-1) exceeds overflow protection threshold [

CPU 50% | Memory 59%

]. System may be oversubscribed on member failure.
May 20 16:18:06.614 [INFO][CPU load 87% | memory load 37%] of chassis 1 exceeds overflow protection thr
May 20 16:23:06.644 [INFO][CPU load 84% | memory load 35%] of module 1 in chassis 1 (unit-1-1) exceeds
```

Il messaggio indica che in caso di guasto di un'unità, le altre risorse dell'unità possono essere sovrascritte.

Modalità semplificata

Comportamento nelle versioni FMC precedenti alla 6.3

- Ogni nodo del cluster viene registrato singolarmente in FMC.
- In FMC verrà quindi creato un cluster logico.
- Per ogni aggiunta di nuovi nodi cluster, è necessario registrare manualmente il nodo.

FMC post-6.3

- La funzionalità della modalità semplificata consente di registrare l'intero cluster in FMC in un unico passaggio (è sufficiente registrare un nodo qualsiasi del cluster).

Gestione minima supportata	Dispositivi gestiti	Versione minima dispositivo gestito supportato richiesta	Note
CCP 6.3	Cluster FTD solo su	6.2.0	Questa è solo una

	FP9300 e FP4100		funzionalità di FMC

Avviso: Una volta che il cluster è stato formato su FTD, è necessario attendere l'avvio della registrazione automatica. Non è necessario provare a registrare manualmente i nodi del cluster (Aggiungi dispositivo), ma utilizzare l'opzione Riconcilia.

Sintomo

Errori di registrazione del nodo

- Se la registrazione del nodo di controllo ha esito negativo per qualsiasi motivo, il cluster viene eliminato da FMC.

Attenuazione

Se la registrazione del nodo di dati non riesce per un motivo qualsiasi, sono disponibili due opzioni:

1. Per ogni distribuzione nel cluster, FMC verifica se sono presenti nodi del cluster da registrare e avvia la registrazione automatica per tali nodi.
2. Nella scheda Riepilogo cluster è disponibile l'opzione Riconcilia (collegamento Dispositivi > Gestione dispositivi > scheda Cluster > Visualizza stato cluster). Una volta attivata l'azione Riconcilia, FMC avvia la registrazione automatica dei nodi da registrare.

Informazioni correlate

- Clustering per Firepower Threat Defense
- Cluster ASA per chassis Firepower 4100/9300
- Informazioni sul clustering sullo chassis Firepower 4100/9300
- Immersione profonda nel clustering di Firepower NGFW - BRKSEC-3032
- Analisi delle acquisizioni di Firepower Firewall per la risoluzione efficace dei problemi di rete

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).