Risoluzione dei problemi di split-brain sul failover ASA

Sommario

Introduzione

In questo documento viene descritto come risolvere i problemi più comuni degli split-brain (split-brain) incontrati con le coppie di dispositivi Cisco Adaptive Security Appliance (ASA) Failover o Firepower Threat Defense (FTD) High Availability (HA).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza del funzionamento della coppia di alta disponibilità ASA/FTD (failover) - Informazioni sul failover.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware e si applica a tutte le implementazioni ASA/FTD supportate in failover.

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.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Che cos'è Split-Brain?

Lo split-brain è uno scenario in cui le unità di un'HA ASA/FTD non sono in grado di rilevarsi a vicenda sulla rete e quindi assumono entrambe il ruolo attivo. In questo modo, entrambe le unità avranno lo stesso indirizzo IP e lo stesso indirizzo MAC dell'interfaccia e potrebbero causare gravi incoerenze nella rete con conseguente perdita dei servizi.

Per verificare se l'elevata disponibilità è in modalità split-brain, eseguire il comando **show failover state** su entrambe le unità e verificare se entrambe le caselle sono attive.

Un esempio di cervello diviso:

Unità principale:

```
ciscoasa1/act/pri# show failover state

State Last Failure Reason Date/Time
This host - Primary
 Active None
Other host - Secondary
Failed Comm Failure 02:39:43 UTC Jan 10 2022

====Configuration State===
 Sync Done - STANDBY
====Communication State==
```

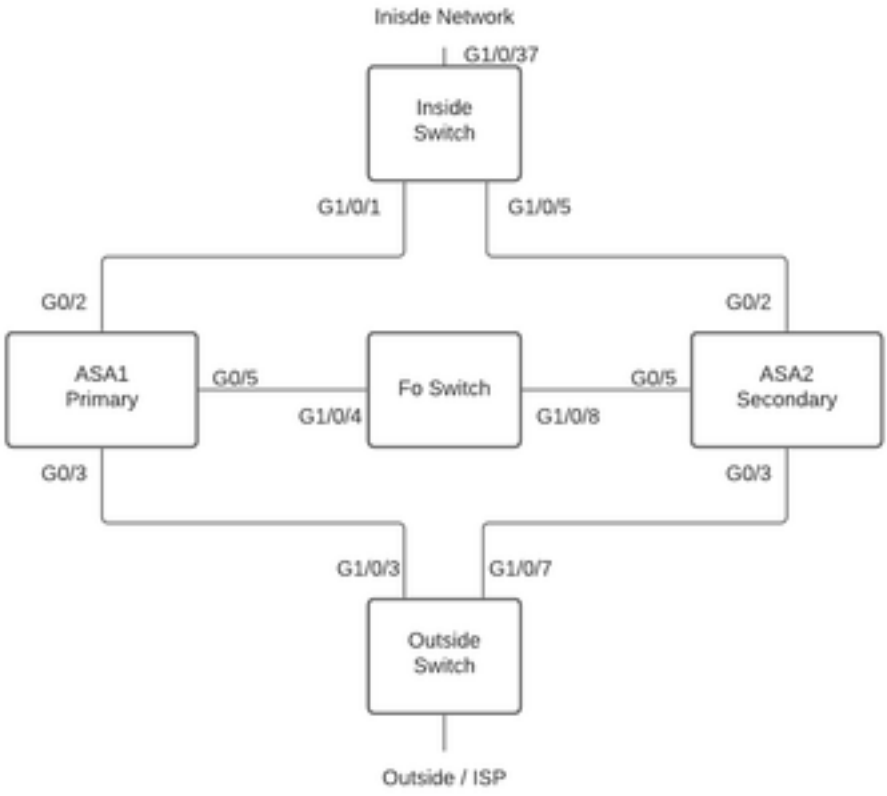
Unità secondaria:

```
ciscoasa2/act/sec# show failover state

State Last Failure Reason Date/Time
This host - Secondary
 Active None
Other host - Primary
Failed Comm Failure 02:39:40 UTC Jan 10 2022

====Configuration State===
  Sync Done
 Sync Done - STANDBY
====Communication State==
```

La separazione del cervello può causare un'interruzione se l'indirizzo MAC appreso per gli indirizzi IP attivi sui dispositivi collegati non è composto da tutte le unità. Si consideri ad esempio la topologia di rete:



Topologia lab

I VMAC sono stati assegnati all'interfaccia come segue, in modo da rendere la **tabella degli indirizzi mac** facilmente comprensibile:

```
Inside (G0/2)    : Active MAC    - 00c1.1000.aaaa
                         Standby MAC - 00c1.1000.bbbb

Outside (G0/4) : Active MAC    - 00c1.2000.aaaa

                         Standby MAC - 00c1.2000.bbbb
```

> **Nota:** se i VMAC non sono configurati, il dispositivo attivo usa sempre il MAC dell'interfaccia dell'unità primaria e il dispositivo standby prende il MAC secondario.

Tabella indirizzi MAC sullo switch quando HA è integro:

```
Switch#show mac address-table

Mac Address Table
-------------------------------------------
Vlan Mac Address Type Ports
---- ----------- -------- -----
100 00c1.1000.aaaa DYNAMIC Gi1/0/5
100 00c1.1000.bbbb DYNAMIC Gi1/0/1
300 00c1.64bc.c508 DYNAMIC Gi1/0/4
300 00d7.8f38.8424 DYNAMIC Gi1/0/8
200 00c1.2000.aaaa DYNAMIC Gi1/0/7
200 00c1.2000.bbbb DYNAMIC Gi1/0/3
```

In caso di guasto del collegamento di failover, l'unità attiva deve rimanere attiva e la modalità

standby deve rimanere attiva. Quando un'unità non riceve tre messaggi HELLO consecutivi sul collegamento di failover, invia messaggi LANTEST su ogni interfaccia dati, incluso il collegamento di failover, per verificare se il peer risponde o meno. L'azione che l'ASA esegue dipende dalla risposta dell'altra unità.

Le azioni possibili sono:

- Se l'ASA riceve una risposta sul collegamento di failover, non esegue il failover.
- Se l'ASA non riceve una risposta sul collegamento di failover, ma riceve una risposta sull'interfaccia dati, l'unità non esegue il failover. Il collegamento di failover è contrassegnato come non riuscito. È necessario ripristinare il collegamento di failover il prima possibile perché l'unità non può eseguire il failover in modalità standby mentre il collegamento di failover è inattivo.
- Se l'ASA non riceve una risposta su nessuna interfaccia, l'unità di standby passa alla modalità attiva e classifica l'altra unità come guasta. Questo porterà ad uno scenario di split-brain.

In questa fase, tutte le interfacce dati su entrambi i firewall funzioneranno come se fossero l'unità attiva. Pertanto, le interfacce sul firewall attivo e in standby useranno lo stesso indirizzo IP e MAC. La tabella degli indirizzi MAC risulterà incoerente a causa di una voce arp non elaborabile e pertanto si verificherà un'interruzione delle attività.

> **Nota:** Failover Link è responsabile della comunicazione di questi dati tra la coppia di failover: stato dell'unità (attivo/standby), messaggi Hello, stato del collegamento di rete, scambio di indirizzi MAC, replica e sincronizzazione della configurazione.

Come prepararsi in modo proattivo ai problemi di failover

Per prepararsi in modo proattivo contro una condizione di cervello diviso:

- Essere nella release d'oro consigliata da Cisco - In alcune condizioni, la separazione del cervello può anche essere causata da problemi come una perdita di memoria. L'utilizzo delle versioni consigliate da Cisco consente di ridurre notevolmente l'esposizione a situazioni di questo tipo.
- Topologia di rete: è consigliabile che le interfacce dati e i collegamenti di failover dispongano di percorsi diversi per ridurre il rischio di errori di tutte le interfacce contemporaneamente.
- Utilizzare un'interfaccia di canale della porta per l'interfaccia di failover. Se sul firewall sono presenti interfacce inutilizzate, associarle in modo da formare un canale della porta e utilizzarlo come collegamento di failover. In questo modo verrà aumentata l'affidabilità del collegamento e verrà rimosso un Single Point of Failure (SPOF).
- Assicurarsi che l'interfaccia di failover non abbia una latenza eccessiva - Come indicato nella guida alla configurazione dell'ASA "Per ottenere prestazioni ottimali con il failover su lunga distanza, la latenza per il collegamento di stato deve essere inferiore a 10 millisecondi e non superiore a 250 millisecondi. Se la latenza è superiore a 10 millisecondi, si verificherà un calo delle prestazioni dovuto alla ritrasmissione dei messaggi di failover."
- Regolare i valori Timer polling/Timer di attesa in base all'implementazione. Non esiste un approccio unico per tutti i timer di failover. In generale, un timer basso può causare failover non necessari (soprattutto se si verifica una certa latenza) e un valore troppo alto può causare un aumento del tempo necessario per il failover. che determinerà notevoli failover. Il valore del

timer di attesa deve essere 5x valore del timer di polling.
- Configurazione di un indirizzo MAC virtuale per le interfacce - In una condizione in cui "l'unità secondaria si avvia senza rilevare l'unità primaria, l'unità secondaria diventa l'unità attiva e utilizza i propri indirizzi MAC perché non conosce gli indirizzi MAC dell'unità primaria. Quando l'unità primaria diventa disponibile, l'unità secondaria (attiva) cambia gli indirizzi MAC in quelli dell'unità primaria, causando un'interruzione nel traffico di rete. Allo stesso modo, se si cambia l'unità principale con il nuovo hardware, viene utilizzato un nuovo indirizzo MAC." Gli indirizzi MAC virtuali proteggono da questa interruzione, in quanto gli indirizzi MAC attivi sono noti all'unità secondaria all'avvio e rimangono gli stessi nel caso di nuovo hardware dell'unità primaria. Se non si configurano indirizzi MAC virtuali, potrebbe essere necessario cancellare le tabelle ARP sui router connessi per ripristinare il flusso del traffico". Per ulteriori informazioni, vedere Indirizzi MAC e indirizzi IP in Failover.
- Inviare i log ASA/FTD di entrambe le unità a un server Syslog esterno. Questo passaggio è più adatto alla manutenzione dei problemi.

Possibili motivi per la separazione del cervello

Come già accennato, lo split-brain si verifica quando la comunicazione tra le interfacce di collegamento di failover è inattiva (in modo unidirezionale o bidirezionale). I motivi più comuni sono:

- Problemi L1 - Cavo/SFP/Interfaccia guasto
- Problema su un dispositivo intermedio
- Mancanza di memoria o di risorse CPU sull'appliance ASA/FTD **Nota:** il motore ASA/LAN usa 1550 byte di blocchi di memoria per memorizzare i pacchetti per l'elaborazione. Se il numero di blocchi liberi di queste dimensioni si esaurisce, l'ASA/FTD non sarà più in grado di elaborare i pacchetti di failover. Eseguire il comando **show block** per verificare se il blocco è stato esaurito.

Procedura di risoluzione dei problemi - Diagramma di flusso

Per risolvere i problemi relativi a uno Scenario a cervello diviso, utilizzare questo diagramma di flusso a partire dalla casella **Main** (Principale). Ci sono alcuni problemi che potrebbero non essere risolvibili qui. In questi casi, vengono forniti collegamenti al supporto tecnico Cisco. Per aprire una richiesta di assistenza, è necessario disporre di un contratto di assistenza valido.

> **Nota:** nelle distribuzioni FTD, i passaggi in questo grafico devono essere seguiti da "**system support diagnostics-cli**".

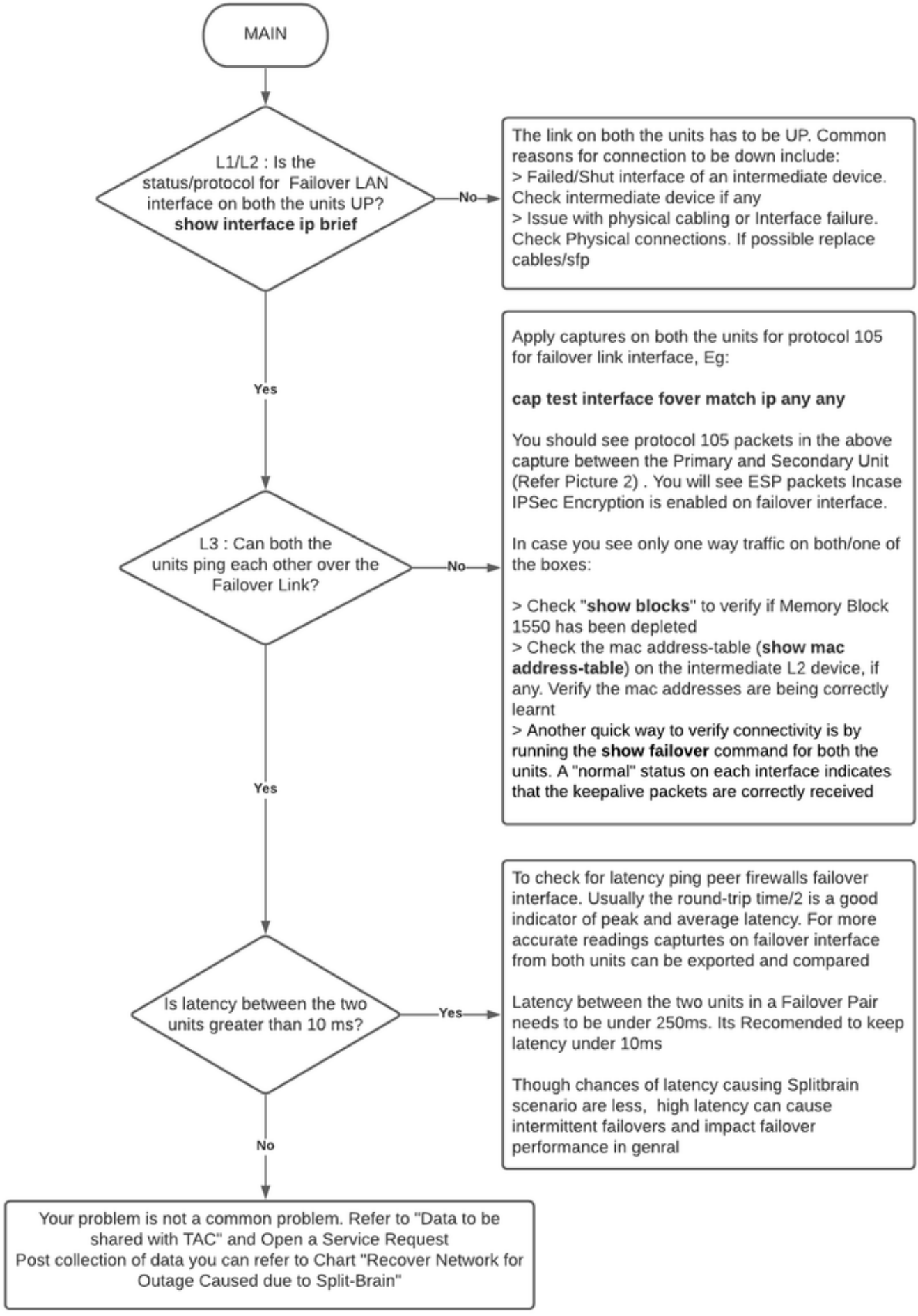


Diagramma di flusso per la risoluzione dei problemi

Ripristino di emergenza da split-brain

Per ripristinare la rete da uno split-brain è necessario assicurarsi che il traffico colpisca solo uno dei due firewall, cioè, gli indirizzi MAC appresi per gli IP attivi devono tutti puntare a una singola unità. A tale scopo, è possibile disabilitare il failover sull'unità o tagliarla completamente dalla rete.

1. Disabilitare il failover sull'unità che non trasmette il traffico: Sulla piattaforma ASA, dalla CLI, passare al terminale di configurazione e immettere il comando **no failover**.Su Piattaforma FTD, in modalità Clish, immettere il comando **configure high-availability suspend**.
2. Per l'appliance ASA, chiudere le interfacce dati. Per FTD, chiudere le interfacce sul dispositivo collegato. In alternativa, è possibile disconnettere fisicamente le interfacce. È inoltre possibile spegnere il dispositivo, ma in questo modo non sarà possibile gestirlo. Per ulteriori informazioni, consultare la guida alla configurazione del dispositivo.

   Nota: se si verificano problemi di connettività anche dopo aver eseguito le operazioni descritte, è probabile che i dispositivi collegati dispongano di voci arp non aggiornate. Controllare le voci arp sui dispositivi upstream e downstream. Per risolvere il problema, è possibile scaricare i pacchetti o forzare l'ASA/FTD a inviare un pacchetto garp per l'IP dell'interfaccia con il problema. A tale scopo, eseguire il comando in modalità abilitazione (per FTD in Sistema supporta diagnostics-cli) - **debug menu ipaddrutl 6 <indirizzo ip interfaccia>**.

   Attenzione: Se si apre una richiesta di assistenza con TAC per problemi relativi alla separazione dei cervelli, condividere le informazioni indicate nella sezione **Dati da raccogliere per la richiesta di assistenza TAC** in questo documento.

Dati da condividere con TAC

Condividere i dati menzionati se è necessario aprire una richiesta di assistenza TAC.

1. Diagramma topologico che mostra l'ASA/FTD-HA e le sue connessioni fisiche con i dispositivi adiacenti (incluse le interfacce di failover).
2. Output per **mostrare il supporto tecnico** su ASA o il file sulla risoluzione dei problemi su piattaforme con FTD.
3. Registri di sistema con indicazione dell'ora per +/- 5 minuti quando si è verificato il problema.
4. File di risoluzione dei problemi FXOS, se l'hardware è un accessorio FPR.

Per generare file con la risoluzione dei problemi per FTD o FXOS, consultare il documento sulla risoluzione dei problemi relativi alle procedure di generazione file di Firepower. Aprire TAC SR.