Controllo interfaccia di sincronizzazione FTD alta disponibilità firewall protetto non riuscito

Sommario

Problema

L'FTD in una coppia ad alta disponibilità (HA) era costantemente visualizzato in stato Failed. La sincronizzazione della configurazione tra i peer HA non è stata completata, nonostante la corretta connettività IP tra le unità. Si trattava di una nuova implementazione che eseguiva il software Cisco Secure Firewall Threat Defense, non ancora in produzione.

Il problema si è verificato dopo che l'unità primaria è stata spostata nella posizione finale e il relativo indirizzo IP di gestione è stato modificato senza prima interrompere la coppia HA. Il processo HA ha rilevato controlli dell'interfaccia non riusciti sulle interfacce dati monitorate, che hanno attivato la logica di valutazione dello stato HA per inserire l'unità primaria in un ruolo non riuscito.

Ambiente

- FTD HA Secure Firewall gestito da FMC
- Nuova distribuzione di un'attività di migrazione, non ancora in produzione

Risoluzione

La risoluzione implicava la rimozione delle interfacce dati selezionate dalla configurazione di monitoraggio dell'interfaccia HA per impedire il rilevamento di errori falsi.

Fasi di risoluzione dei problemi

1: I dati di risoluzione dei problemi hanno confermato errori di verifica dell'interfaccia HA sulle interfacce di dati monitorate, mentre la connettività peer HA (heartbeat e ping) è rimasta funzionante.

<#root>

```
device# show failover
Failover On
Failover unit Primary
Failover LAN Interface: FailOver Ethernet1/8 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 5 of 776 maximum
MAC Address Move Notification Interval not set
failover replication http
Version: Ours 9.20(2)121, Mate 9.20(2)121
Serial Number: Ours SERIAL#, Mate SERIAL#
Last Failover at: 17:14:25 UTC Mar 16 2026


This host: Primary - Failed

        Active time: 0 (sec)
        slot 0: FPR-1120 hw/sw rev (2.0/9.20(2)121) status (Up Sys)


Interface To-DC1-ACC (0.0.0.0): No Link (Waiting)
          Interface To-DC1-WAN (0.0.0.0): No Link (Waiting)


          Interface management (203.0.113.131/fe80::a610:b6ff:fe3d:e101): Normal (Monitored)
        slot 1: snort rev (1.0)  status (up)
        slot 2: diskstatus rev (1.0)  status (up)
    Other host: Secondary - Active
        Active time: 184688 (sec)


Interface To-DC1-ACC (0.0.0.0): No Link (Waiting)


          Interface To-DC1-WAN (10.230.2.2): Normal (Waiting)
          Interface management (203.0.113.130/fe80::6ae5:9eff:fee6:d681): Normal (Monitored)
        slot 1: snort rev (1.0)  status (up)
        slot 2: diskstatus rev (1.0)  status (up)
```

2: Confermato che le transizioni di stato HA si stavano verificando in base ai risultati del monitoraggio dell'interfaccia e non in base ai problemi di connettività del piano di gestione.

<#root>

```
device# show failover history
17:16:51 UTC Mar 16 2026
```

```
Standby Ready

Failed                      Interface check



This host:2
                                                    single_vf: To-DC1-ACC
                                                    single_vf: To-DC1-WAN

                                                    Other host:1
                                                    single_vf: To-DC1-ACC
```

Modifiche alla configurazione

1: La configurazione HA è stata aggiornata per escludere le interfacce dati interessate dal monitoraggio dello stato dell'interfaccia, evitando il rilevamento di errori falsi.

2: Dopo le modifiche della configurazione, l'FTD primario è passato correttamente allo stato Pronto per standby, confermando la corretta sincronizzazione dell'alta disponibilità e la stabilità dello stato.

3: Il test del failover HA è stato completato con i risultati previsti, convalidando la stabilità della configurazione HA dopo le modifiche.

Chiarimenti sul comportamento previsto

Di seguito sono riportati i comportamenti previsti e di progettazione osservati durante la risoluzione dei problemi:

- Nomi host duplicati su peer FTD: Entrambe le unità che visualizzano lo stesso nome host dovrebbero comportarsi in FTD HA, in quanto il nome host dell'unità attiva viene presentato a livello di sistema (indicato nella richiesta di miglioramento CSCwe31354)
- Proprietà indirizzo IP: Solo l'FTD attivo visualizza gli indirizzi IP attivi sulle interfacce dati, il che è previsto comportamento per progettazione per prevenire le condizioni di split-brain. Se non sono configurati indirizzi IP di standby dell'interfaccia, l'FTD pronto per la modalità standby sembra non avere indirizzi IP configurati sulle proprie interfacce.

Causa

L'FTD primario è stato contrassegnato come non riuscito a causa di errori del controllo di integrità dell'interfaccia ad alta disponibilità sulle interfacce dati monitorate. In questo caso, il peer con più interfacce operative rimane attivo. Questo comportamento è progettato in FTD High Availability ed è documentato nelle linee guida Cisco Secure Firewall HA. Il processo HA ha rilevato controlli dell'interfaccia non riusciti sulle interfacce dati monitorate, che hanno attivato la logica di valutazione dello stato HA per inserire l'unità primaria in un ruolo non riuscito.

Contenuto correlato

- Guida alla configurazione di Cisco Secure Firewall Device Manager - Alta disponibilità (failover)
- Supporto tecnico Cisco e download

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).