

Risoluzione dei problemi relativi all'errore di associazione a elevata disponibilità in FDM

Sommario

Problema

L'accoppiamento ad alta disponibilità (HA, High Availability) tra due appliance Cisco Firepower 1120 con FTD 7.4.2.4 non riesce durante la sincronizzazione dell'applicazione e il nodo secondario entra sistematicamente in stato di errore a causa di una mancata corrispondenza della modalità di registrazione della licenza. Messaggio di errore specifico:

```
CD App Sync error FDM validation failure License registration mode mismatch between Primary and Secondary
```

Il comando `show app-sync-history` rivela errori ripetuti con messaggi come:

```
App Sync Status: FAILURE
```

```
Failed Reason: FDM validation failure - License agent compliance mismatch between Primary and Secondary
```

Il problema si è verificato dopo la reimpostazione dei firewall, il ripristino delle configurazioni dal backup, l'aggiornamento del software alla versione 7.4.2.4 FTD, l'aggiornamento delle versioni VDB e Snort e la riapplicazione delle licenze con token aggiornati. Il firewall secondario rimane in stato Non riuscito, impedendo il completamento dell'HA e influenzando sulla ridondanza del firewall.

Ambiente

- Appliance Cisco Firepower 1120 NGFW configurate per l'alta disponibilità
- Firepower Threat Defense (FTD) versione 7.4.2.4-9
- Motore di ispezione snort: 3.1.53.2003 — 175

- VDB: 425.0
- Database di georilevazione: 2026-03-07-053
- Dispositivi convertiti da Smart Licensing alla modalità PLR (Permanent License Reservation)
- Tentativo di connettività cloud da parte del dispositivo primario dopo la conversione PLR
- Entrambi i dispositivi ripristinati dal backup

Risoluzione

La risoluzione implica l'identificazione e la correzione della mancata corrispondenza della modalità di registrazione della licenza tra i dispositivi primario e secondario, l'annullamento della registrazione del cloud e il completamento di un'installazione completa.

Passaggio 1: Identificazione della mancata corrispondenza della modalità di registrazione della licenza

Verificare la modalità di registrazione della licenza su entrambi i dispositivi controllando app-sync-history per i motivi specifici dell'errore:

```
show app-sync-history
```

Nell'output vengono visualizzati errori che indicano:

```
FDM validation failure - License registration mode mismatch between Primary and Secondary node
```

Passaggio 2: Esegui annullamento registrazione cloud

Poiché il dispositivo primario stava ancora tentando la connettività cloud dopo la conversione da Smart Licensing alla modalità PLR, è necessario annullare la registrazione del cloud.

Configurare un proxy temporaneo nell'interfaccia utente di FDM (se non è configurato alcun proxy):

Selezionare Impostazioni di sistema > Ulteriori informazioni > scheda Proxy HTTP e configurare temporaneamente un proxy fittizio [che può essere rimosso in seguito].

SSH nel dispositivo FTD ed eseguire lo script del connettore:

```
ssh admin@<device-ip>
expert
sudo su
/ngfw/var/sf/bin/connector.sh
```

Passaggio 3: Conflitto risoluzione porta 8989

Se lo script del connettore ha esito negativo a causa di questo errore:

```
Error: listen tcp :8989: bind: address already in use
```

Identificare e terminare il processo utilizzando la porta 8989 (in genere Cisco Success Network):

```
netstat -tulpn | grep 8989
kill <pid>
```

Passaggio 4: Annullamento registrazione cloud completa

Rieseguire lo script del connettore dopo aver risolto il conflitto tra porte:

```
/ngfw/var/sf/bin/connector.sh
```

L'esecuzione deve avere un output simile al seguente:

Starting connector

INFO[0000] [firepower][functions.go:162 common:LogEnv] Environment variable: https_proxy=http://1xx.xx.

INFO[0000] [firepower][functions.go:162 common:LogEnv] Environment variable: http_proxy=http://1xx.xx.x

Andare a FDM GUI, System Settings > Cloud Services > Cloud Services e fare clic su unregister option (Annulla registrazione). Verificare che la registrazione del dispositivo sia stata annullata dai servizi cloud.

Passaggio 5: Esecuzione della distribuzione completa e ripresa di HA

Dopo l'annullamento della registrazione del cloud, se l'accoppiamento HA ha ancora esito negativo con lo stesso errore di mancata corrispondenza delle licenze, eseguire una distribuzione completa sull'unità attiva tramite l'interfaccia FDM.

Passare a Distribuisci > Distribuisci ora e completare il processo di distribuzione.

Una volta completata la distribuzione, riprovare la formazione HA. I dispositivi devono essere in grado di formare una coppia HA di standby attivo con interfacce connesse e in stato pronto.

Passaggio 6: Verifica stato HA

Confermare la corretta formazione HA:

```
show failover
```

L'output deve mostrare entrambe le unità in stati HA corretti con una corretta sincronizzazione.

Causa

La causa principale è una mancata corrispondenza della modalità di registrazione della licenza tra i dispositivi Firepower 1120 primario e secondario. I dispositivi sono stati convertiti dalla modalità

Smart Licensing alla modalità PLR (Permanent License Reservation); tuttavia, il dispositivo primario ha continuato a tentare la connettività cloud, determinando una mancata corrispondenza nello stato di conformità dell'agente di licenza/esportazione durante la convalida HA. Ciò ha comportato ripetuti errori di convalida di FDM/FIM durante la sincronizzazione dell'applicazione. Inoltre, l'annullamento della registrazione del cloud è stata inizialmente bloccata da un conflitto della porta 8989 relativo a Cisco Success Network, che ha richiesto una risoluzione prima di procedere con l'annullamento della registrazione.

Contenuto correlato

- [Applicazione di licenze permanenti su reti con interruzioni dell'aria](#)
- [Ricreare un'immagine di Secure Firewall Threat Defense](#)
- [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).