Errore dell'interfaccia di gestione FTD dopo l'aggiornamento da 7.4.3 a 7.6.4

Sommario

Problema

Dopo l'aggiornamento di una coppia Cisco Secure Firewall 3130 Threat Defense (FTD) High Availability (HA) dalla versione 7.4.3 alla versione 7.6.4, l'unità primaria ha riportato un errore al 99% nel centro di gestione del firewall e non ha risposto. L'unità secondaria è stata aggiornata ed è diventata attiva nella coppia HA. L'unità primaria non risponde alle connessioni SSH e il CCP non è in grado di comunicare con essa.

Al termine dell'indagine, è stato osservato questo errore critico su FXOS:

```
Critical  F1000398 2026-08-14T20:52:06.297     58437 [FSM:FAILED]: out-of-band interface configuration(
```

I registri di aggiornamento FTD hanno indicato che l'aggiornamento è stato effettivamente completato (completato al 100%), ma il servizio SFTunnel non è stato avviato correttamente, impedendo la comunicazione tra FTD e FMC. Il dispositivo poteva eseguire il ping tra se stesso, il suo gateway e l'unità FTD peer, ma non poteva raggiungere i CCP che risiedevano su subnet diverse.

Ambiente

- Cisco Secure Firewall 3130 - Coppia HA di Threat Defense
- Versione originale del software: FTD 7.4.3
- Versione software di destinazione: FTD 7.6.4 (build 69)
- Cisco Firepower Extensible Operating System (FX-OS) v2.16.1 (build 147)

- Interfaccia di gestione configurata con indirizzamento IP statico
- Server FMC situati su subnet diverse dalla rete di gestione FTD

Risoluzione

Il problema è stato risolto riconfigurando completamente l'interfaccia di gestione sull'unità FTD interessata. Sono stati eseguiti i seguenti passaggi:

Passaggio 1: Connettersi all'FTD tramite l'accesso alla console perché SSH non funzionava.

Passaggio 2: Verificare lo stato di completamento dell'aggiornamento controllando i registri di aggiornamento:

```
root@device:/ngfw/var/log/sf/Cisco_FTD_SSP_FP3K_Upgrade-7.6.4# cat status.log
```

Passaggio 3: Confermare l'errore dell'interfaccia di gestione su FXOS:

```
device# show fault
```

Passaggio 4: Provare a risolvere i problemi di base riconfigurando l'indirizzo IP di gestione (il problema non è stato risolto).

Passaggio 5: Eseguire un riavvio a freddo (il problema non è stato risolto).

Passaggio 6: Disabilitare completamente l'interfaccia management0 dalla CLI FTD:

```
configure network management-interface disable management0
```

Passaggio 7: Riattivare l'interfaccia management0:

```
configure network management-interface enable management0
```

Passaggio 8: Riconfigurare le impostazioni di rete per l'interfaccia di gestione:

```
configure network ipv4 manual <ip_address> <netmask> <gateway>
```

Passaggio 9: Verificare che gli allarmi FXOS siano stati cancellati e che l'FTD sia ora in grado di eseguire il ping del CCP:

```
root@device:/# ping <FMC_IP_address>
```

Passaggio 10: Riavviare il servizio SFTunnel utilizzando lo script manage_procs.pl:

```
manage_procs.pl restart sftunnel
```

Passaggio 11: Verifica connettività tunnel SFT:

```
root@device:/# sftunnel_status.pl
```

Passaggio 12: Testare la funzionalità di failover per garantire il corretto funzionamento delle operazioni HA.

Dopo aver completato questi passaggi, l'FTD è stato in grado di comunicare correttamente con il FMC e tutti i test di connettività e failover hanno avuto esito positivo. L'aggiornamento dell'aggiornamento dell'aggiornamento rapido può quindi essere applicato senza problemi.

Causa

La causa principale è stata un errore dell'interfaccia di gestione di inizializzare correttamente dopo l'aggiornamento FTD da 7.4.3 a 7.6.4, nonostante il completamento del processo di aggiornamento. Errore della macchina a stati finiti (FSM) di configurazione dell'interfaccia di gestione fuori banda durante il processo di aggiornamento. L'interfaccia di gestione non è in grado di stabilire la connettività corretta. Questo comportamento è stato documentato nell'ID bug Cisco CSCww08417.

Questo problema è simile ai problemi segnalati in precedenza con ID bug Cisco CSCwj04154 e ID bug Cisco CSCwa69303, ma si verifica in condizioni diverse. L'errore dell'interfaccia di gestione ha creato una falsa impressione di errore di aggiornamento al 99% di completamento, quando in realtà l'aggiornamento era stato completato correttamente ma la connettività di gestione era interrotta.

Contenuto correlato

- Cisco Bug ID CSCww08417 - L'avvio dell'interfaccia di gestione FTD potrebbe non riuscire dopo l'aggiornamento
- Guida alla compatibilità di Cisco 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).