FTD-Verwaltungsschnittstellenfehler nach Upgrade von 7.4.3 auf 7.6.4

Inhalt

Problem

Nach dem Upgrade eines Cisco Secure Firewall 3130 Threat Defense (FTD) High Availability (HA)-Paares von Version 7.4.3 auf 7.6.4 schien die primäre Einheit mit 99 % Vollendung im Firewall Management Center (FMC) zu fehlschlagen und reagierte nicht mehr. Die sekundäre Einheit wurde erfolgreich aktualisiert und im HA-Paar aktiviert. Die primäre Einheit reagierte nicht auf SSH-Verbindungen, und das FMC konnte nicht mit ihr kommunizieren.

Bei der Untersuchung wurde dieser kritische Fehler auf FXOS beobachtet:

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

Die FTD-Upgrade-Protokolle zeigten, dass das Upgrade tatsächlich erfolgreich abgeschlossen wurde (100 % abgeschlossen), aber der SFTunnel-Service nicht richtig startete, wodurch die Kommunikation zwischen FTD und FMC behindert wurde. Das Gerät konnte sich selbst, sein Gateway und die FTD-Einheit des Peers pingen, konnte jedoch die FMCs nicht erreichen, die sich in verschiedenen Subnetzen befanden.

Umwelt

- Cisco Secure Firewall 3130 Threat Defense - HA-Paar
- Original-Softwareversion: FTD 7.4.3
- Zielversion der Software: FTD 7.6.4 (Build 69)
- Cisco FirePOWER Extensible Operating System (FX-OS) v2.16.1 (Build 147)

- Managementschnittstelle mit statischer IP-Adressierung
- FMC-Server in verschiedenen Subnetzen des FTD-Managementnetzwerks

Auflösung

Das Problem wurde durch eine vollständige Neukonfiguration der Verwaltungsschnittstelle der betroffenen FTD-Einheit behoben. Diese Schritte wurden ausgeführt:

Schritt 1: Verbindung zum FTD über Konsolenzugriff, da SSH nicht funktionierte

Phase 2: Überprüfen Sie den Status des Upgrade-Abschlusses, indem Sie die Upgrade-Protokolle überprüfen:

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

Schritt 3: Bestätigen Sie den Management-Schnittstellenfehler auf FXOS:

```
device# show fault
```

Schritt 4: Versuchen Sie eine grundlegende Fehlerbehebung, indem Sie die Management-IP-Adresse neu konfigurieren (dadurch wurde das Problem nicht behoben).

Schritt 5: Führen Sie einen Kaltstart durch (das Problem konnte dadurch nicht behoben werden).

Schritt 6: Deaktivieren Sie die Schnittstelle management0 über die FTD-CLI vollständig:

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

Schritt 7: Aktivieren Sie die Schnittstelle management0 erneut:

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

Schritt 8: Konfigurieren Sie die Netzwerkeinstellungen für die Verwaltungsschnittstelle neu:

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

Schritt 9: Vergewissern Sie sich, dass die FXOS-Warnungen gelöscht wurden und der FTD nun den FMC pingen kann:

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

Phase 10: Starten Sie den SFTunnel-Dienst mit dem Managed_procs.pl-Skript neu:

```
manage_procs.pl restart sftunnel
```

Phase 11: Überprüfen der SFTunnel-Verbindung:

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

Phase 12: Testen Sie die Failover-Funktionalität, um sicherzustellen, dass die HA-Vorgänge ordnungsgemäß funktionieren.

Nach Abschluss dieser Schritte konnte die FTD ordnungsgemäß mit dem FMC kommunizieren, und alle Verbindungs- und Failover-Tests waren erfolgreich. Das Hotfix-Upgrade konnte dann ohne Probleme angewendet werden.

Ursache

Die Hauptursache war, dass die Verwaltungsschnittstelle nach dem FTD-Upgrade von 7.4.3 auf 7.6.4 nicht ordnungsgemäß initialisiert wurde, obwohl der Upgrade-Prozess erfolgreich abgeschlossen wurde. Der FSM (Finite State Machine) für die Out-of-Band-Managementschnittstellenkonfiguration ist während des Upgrade-Vorgangs fehlgeschlagen, sodass die Managementschnittstelle keine ordnungsgemäße Verbindung herstellen konnte. Dieses Verhalten wurde unter der Cisco Bug-ID CSCww08417 dokumentiert.

Dieses Problem ähnelt den bereits gemeldeten Fehlern Cisco Bug-ID CSCwj04154 und Cisco Bug-ID CSCwa69303, tritt jedoch unter anderen Bedingungen auf. Der Ausfall der Managementschnittstelle vermittelte den falschen Eindruck eines Upgrade-Fehlers bei 99 % Abschluss, als das Upgrade tatsächlich erfolgreich abgeschlossen war, aber die Managementverbindung unterbrochen wurde.

Verwandte Inhalte

- Cisco Bug-ID CSCww08417 - FTD-Management-Schnittstelle kann nach Upgrade möglicherweise nicht gestartet werden
- Kompatibilitätsleitfaden für Cisco Secure Firewall Threat Defense
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.