

Fehlerbehebung bei Hochverfügbarkeits-Kopplungsfehlern bei FDM

Inhalt

Problem

Die Hochverfügbarkeitspaarung zwischen zwei Cisco FirePOWER 1120-Appliances, auf denen FTD 7.4.2.4 ausgeführt wird, schlägt während der Anwendungssynchronisierung fehl, da der sekundäre Knoten aufgrund einer Nichtübereinstimmung des Lizenzregistrierungsmodus regelmäßig in den Status "Fehler" wechselt. Die aufgetretene Fehlermeldung lautet:

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

Der Befehl `show app-sync-history` zeigt wiederholte Fehler mit folgenden Meldungen an:

```
App Sync Status: FAILURE
```

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

Dieses Problem trat auf, nachdem beide Firewalls zurückgesetzt, die Konfigurationen aus dem Backup wiederhergestellt, die Software auf FTD-Version 7.4.2.4 aktualisiert, die VDB- und Snort-Versionen aktualisiert und die Lizenzen mit neuen Token erneut angewendet wurden. Die sekundäre Firewall befindet sich weiterhin im Status "Failed" (Ausgefallen), wodurch die HA-Funktion nicht vollständig ausgeführt wird und die Firewall-Redundanz beeinträchtigt wird.

Umwelt

- Cisco FirePOWER 1120 NGFW-Appliances für hohe Verfügbarkeit konfiguriert
- Firepower Threat Defense (FTD) Version 7.4.2.4-9

- Snort Inspection Engine: 3.1.53.2003-175
- VDB: 425.0
- Standortdatenbank: 2026-03-07-053
- Geräte, die vom Smart Licensing- in den PLR-Modus (Permanent License Reservation) umgewandelt werden
- Primäres Gerät versucht Cloud-Konnektivität nach PLR-Umwandlung
- Beide Geräte wurden aus dem Backup wiederhergestellt

Auflösung

Die Lösung besteht darin, die Nichtübereinstimmung des Lizenzregistrierungsmodus zwischen primärem und sekundärem Gerät zu identifizieren und zu korrigieren, die Cloud-Registrierung aufzuheben und eine vollständige Bereitstellung abzuschließen.

Schritt 1: Identifizieren der Nichtübereinstimmung des Lizenzregistrierungsmodus

Überprüfen Sie den Lizenzregistrierungsmodus auf beiden Geräten, indem Sie den App-Synchronisierungsverlauf aus bestimmten Fehlergründen überprüfen:

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

Die Ausgabe zeigt Fehler an und zeigt Folgendes an:

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

Phase 2: Cloud-Registrierung aufheben

Da das primäre Gerät nach der Umstellung von Smart Licensing auf den PLR-Modus noch eine

Cloud-Verbindung herstellen wollte, ist eine Cloud-Abmeldung erforderlich.

Konfigurieren Sie einen temporären Proxy in der FDM-Benutzeroberfläche (falls kein Proxy konfiguriert ist):

Navigieren Sie zur Registerkarte System Settings > See More > HTTP Proxy (Systemeinstellungen > Mehr anzeigen > HTTP-Proxy), und konfigurieren Sie vorübergehend einen Dummy-Proxy [dieser kann später entfernt werden].

SSH in das FTD-Gerät ein, und führen Sie das Connector-Skript aus:

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

Schritt 3: Port 8989-Konflikt lösen

Wenn das Connector-Skript mit diesem Fehler fehlschlägt:

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

Identifizieren und beenden Sie den Vorgang über Port 8989 (in der Regel Cisco Success Network):

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

Schritt 4: Vollständige Aufhebung der Cloud-Registrierung

Führen Sie das Connector-Skript erneut aus, nachdem Sie den Portkonflikt behoben haben:

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

Bei der erfolgreichen Ausführung muss die Ausgabe ähnlich wie folgt aussehen:

```
Starting connector
```

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

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

Gehen Sie zu FDM GUI, Systemeinstellungen > Cloud Services > Cloud Services und klicken Sie auf die Option zur Aufhebung der Registrierung. Stellen Sie sicher, dass das Gerät nicht für Cloud-Services registriert ist.

Schritt 5: Vollständige Bereitstellung und Wiederaufnahme der HA

Wenn nach der Cloud-Deregistrierung die HA-Paarung weiterhin fehlschlägt und derselbe Lizenzkonflikt auftritt, führen Sie über die FDM-Schnittstelle eine vollständige Bereitstellung auf dem aktiven Gerät durch.

Navigieren Sie zu Deploy > Deploy Now, und schließen Sie den Bereitstellungsprozess ab.

Wiederholen Sie nach Abschluss der Bereitstellung den HA-Vorgang. Die Geräte müssen erfolgreich ein Aktiv/Standby-HA-Paar mit verbundenen Schnittstellen bilden, die sich im Bereitschaftszustand befinden.

Schritt 6: HA-Status überprüfen

Bestätigen Sie die erfolgreiche HA-Bildung:

```
show failover
```

Die Ausgabe muss beide Einheiten im richtigen HA-Zustand bei erfolgreicher Synchronisierung anzeigen.

Ursache

Die Ursache hierfür war ein nicht übereinstimmender Lizenzregistrierungsmodus zwischen dem primären und sekundären Firepower 1120-Gerät. Die Geräte wurden vom Smart Licensing- in den PLR-Modus (Permanent License Reservation) umgewandelt. Das primäre Gerät versuchte jedoch weiterhin, eine Cloud-Verbindung herzustellen, was während der HA-Validierung zu einer Diskrepanz zwischen dem Compliance-Status des Lizenzagenten und des Exports führte. Dies führte zu wiederholten FDM/FIM-Validierungsfehlern während der Anwendungssynchronisierung. Darüber hinaus wurde die Cloud-Abmeldung anfänglich durch einen Konflikt auf Port 8989 blockiert, der mit dem Cisco Success Network zusammenhing. Eine Auflösung war erforderlich, bevor die Abmeldung fortgesetzt werden konnte.

Verwandte Inhalte

- [Permanente Lizenzen in Air-Gap Netzwerken anwenden](#)
- [Erneutes Image einer sicheren Firewall-Bedrohungsabwehr](#)
- [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.