Fehlerbehebung: Talos-Verbindungsstatus

Inhalt

Einleitung

In diesem Dokument wird die Behebung von TALOS-Verbindungsproblemen bei Secure Firewall FMC und FDM beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Secure Firewall Management Center (FMC)
- Cisco Secure Firewall Device Manager (FDM)

- Cisco Secure Firewall Threat Defense (FTD)

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

FMC Version 7.6.0 oder 7.7.0
FDM Version 7.6.0 oder 7.7.0
FTD-Version 7.6.0 oder 7.7.0

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Das Cisco Secure Firewall Management Center (FMC) baut auf einem Client-seitigen Zertifikat auf, um eine sichere Verbindung mit den Cisco Talos Threat Intelligence Services herzustellen. Diese Authentifizierung ist für das FMC unerlässlich, um wichtige Updates wie URL-Reputationsdatenbanken (URLDBs), Lightweight Security Packages (LSPs) und andere Anreicherungsdaten erfolgreich herunterzuladen.

Unter normalen Betriebsbedingungen wird dieses Zertifikat während der Softwareinstallation vorab bereitgestellt und soll sich automatisch erneuern, sobald es abläuft. Ein bekanntes Problem in bestimmten Versionen der Cisco Secure Firewall FMC-Software verhindert jedoch, dass die automatische Verlängerung nach dem 30. März 2025 erfolgreich abgeschlossen werden kann. In diesem Fall kann sich das FMC nicht bei Talos authentifizieren, was zu Verbindungsfehlern und der Unmöglichkeit führt, aktualisierte Bedrohungsinformationen abzurufen.

Überprüfen des Zertifikatsstatus

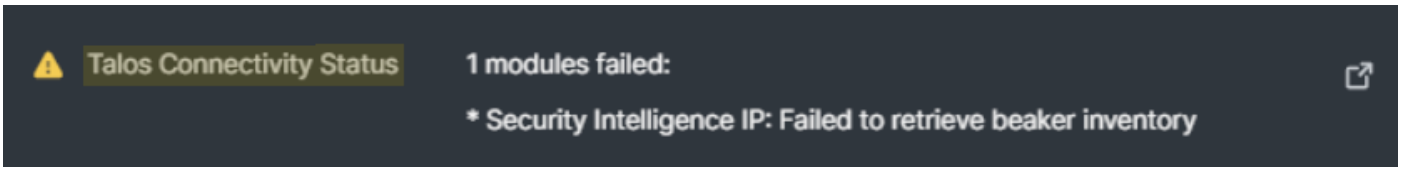
FMC-GUI

Wenn das clientseitige Zertifikat nicht erneuert werden kann, löst das Cisco FMC Integritätswarnungen aus, um Administratoren über die Unterbrechung der Kommunikation mit Cisco Talos zu informieren. Sie können diese Warnungen überwachen, indem Sie zu System > Health (System > Zustand) navigieren und den Abschnitt Talos Connectivity Status (Talos-Verbindungsstatus) überprüfen.

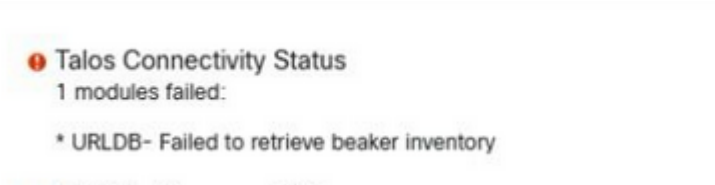
Wenn das Problem mit dem Ablauf des Zertifikats Ihr System beeinträchtigt, wird in der Regel eine

der folgenden Fehlermeldungen angezeigt:

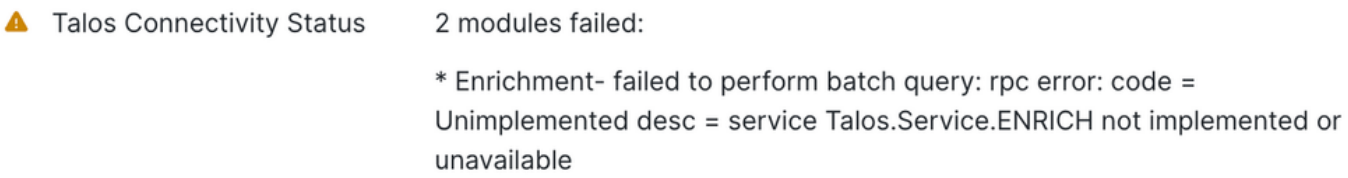
- "LSP - Fehler beim Abrufen des Becherbestands":



- "URLDB - Becherbestand konnte nicht abgerufen werden":



- "Anreicherung - Batchabfrage konnte nicht durchgeführt werden":



FMC-CLI

Um festzustellen, ob sich das Problem auf Ihre FMC-Appliance auswirkt, wechseln Sie in den Expertenmodus, und führen Sie den Befehl aus, um das aktuelle Ablaufdatum des clientseitigen Zertifikats zu überprüfen:

<#root>

```
expert
sudo su
//type the 'FMC CLI admin password'

sudo openssl x509 --in /var/sf/beaker3/securefirewall-dev-prod-01_prod.pem --text
```

Suchen Sie in der Befehlsausgabe nach dem Abschnitt Validity (Gültigkeit). Das Feld Nicht nach gibt das aktuelle Ablaufdatum des Zertifikats an. Wenn dieses Datum bereits verstrichen ist oder

näher rückt, ist der Verlängerungsprozess fehlgeschlagen, und ein manueller Neustart des Service ist erforderlich, um die Erneuerung des Zertifikats einzuleiten.

Beispiel:

<#root>

```
> expert
>sudo su
//type the 'FMC CLI admin password'
openssl x509 --in /var/sf/beaker3/securefirewall-dev-prod-01_prod.pem --text
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 46240369 (0x2c19271)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, ST = California, L = San Jose, O = Cisco Systems Inc., OU = Security, CN = Keym
```

Validity

```
Not Before: Jan 30 22:32:39 2024 GMT
```

Not After :

```
 Mar 30 22:32:39 2025 GMT
        Subject: CN = SFW76EVAL-prod-01, C = US, ST = California, L = San Jose, O = Cisco, OU = Securit
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
```

Fehlerbehebung

1. Identifizieren Sie Ihr Szenario

Software-Version	Zugehörige Bug-ID	Hauptursache
7.6.0 oder 7.7.0	Cisco Bug-ID CSCwo63951	Ablauf des Zertifikats/Verbindungsfehler
7.6.1+ oder 7.7.10+	Cisco Bug-ID CSCwr23982	Konfiguration der Registrierung/Lizenzierung (z. B. Air-Gap).

2. Fehlerbehebung für die Versionen 7.6.0 und 7.7.0

Symptome

Zusätzlich zu den oben erwähnten Warnmeldungen können Sie folgende Verhaltensweisen beobachten:

- FDM-Task-Manager-Fehler: "Fehler beim Cloud-Update für Snort 3: Keine Antwort vom Aktualisierungsserver oder Verbindungszeitüberschreitung."
- Protokolleinträge: Fehler in /ngfw/var/log/messages: Failed to connect to tunnel (UUID), error: Keine Verbindung.
- Status: Stagnierende Updates in der Benutzeroberfläche: Der Bildschirm "Voreinstellungen für die URL-Filterung" zeigt "Noch nicht aktualisiert" an.

Temporäre Problemumgehung

Um die Services sofort wiederherzustellen, starten Sie die erforderlichen Prozesse über den Expertenmodus neu:

Schritt 1: Rufen Sie die CLI auf, und wechseln Sie in den Expertenmodus.

Schritt 2: Führen Sie die folgenden Befehle aus:

```
expert
sudo su
//type the 'FMC CLI admin password'
pmtool restartbyid talosAgent
pmtool restartbyid beaker3
```

Anmerkung: Diese Problemumgehung löst ein Zertifikat aus, das nur fünf Tage gültig ist. Sie müssen diesen Vorgang alle fünf Tage wiederholen, bis eine dauerhafte Lösung angewendet wurde.

Ständige Entschließung

Um dieses Problem dauerhaft zu beheben, stellen Sie sicher, dass die folgenden Bedingungen erfüllt sind:

Schritt 1: Überprüfen der Verbindung: Stellen Sie sicher, dass die Appliance ausgehenden Zugriff auf https://api-sse.cisco.com hat. Rufen Sie dazu die FMC-CLI auf, wechseln Sie in den Expertenmodus, und führen Sie die folgenden Befehle aus:

Schritt 1.1. DNS-Auflösung testen:

<#root>

```
expert
sudo su
//type the 'FMC CLI admin password'
```

nslookup api-sse.cisco.com

Schritt 1.2. Test des TCP-Portzugriffs:

<#root>

```
 expert
sudo su
//type the 'FMC CLI admin password'
```

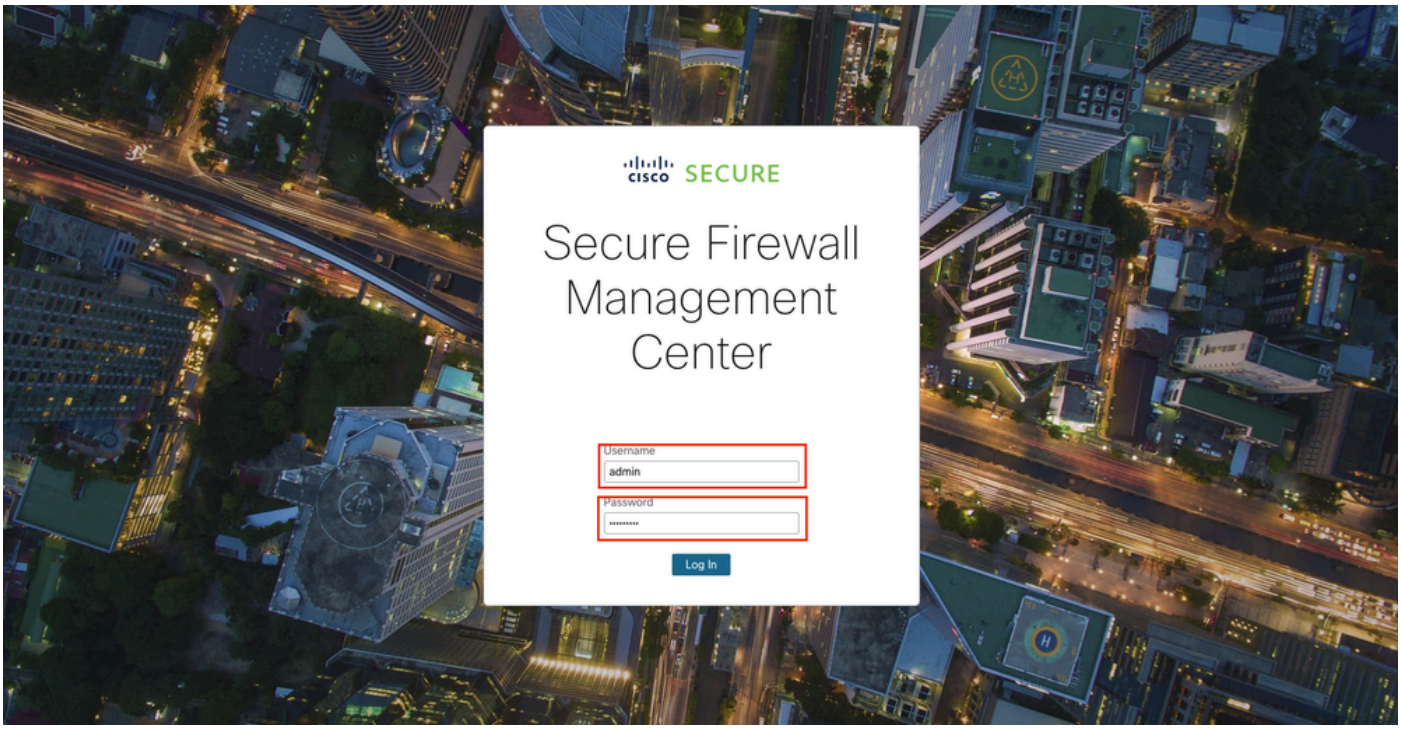
telnet api-sse.cisco.com 443

Anmerkung: Überprüfen Sie, ob der ausgehende HTTPS-Zugriff (TCP 443) auf https://api-sse.cisco.com über alle Upstream-Firewalls, Proxys oder Sicherheitsgeräte zugelassen ist.

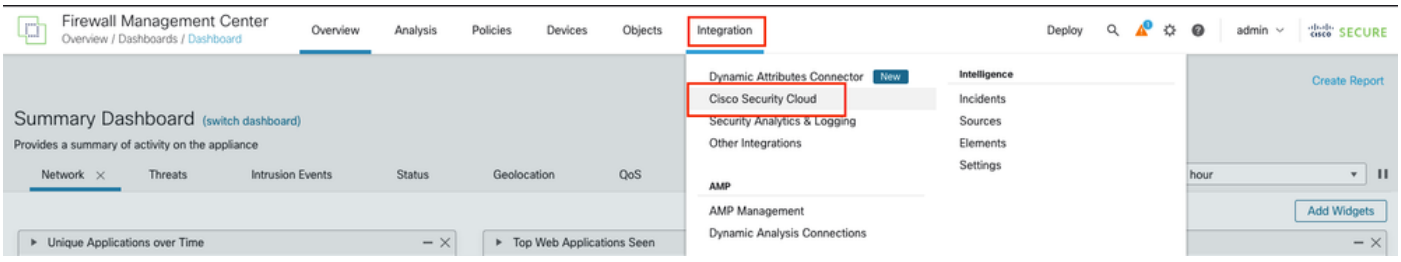
Schritt 2. Telemetrie aktivieren: Stellen Sie sicher, dass die CSN-Telemetrie aktiviert ist, damit der SSEConnector ein neues Zertifikat erhalten kann. Um CSN auf dem FMC zu aktivieren, gehen Sie wie folgt vor:

Schritt 2.1. Melden Sie sich an der FMC-GUI an, indem Sie einen Webbrowser öffnen und zur FMC-URL navigieren (z. B.: https://<FMC_IP_or_Hostname>). Geben Sie Ihren Benutzernamen und Ihr Kennwort ein, um auf das

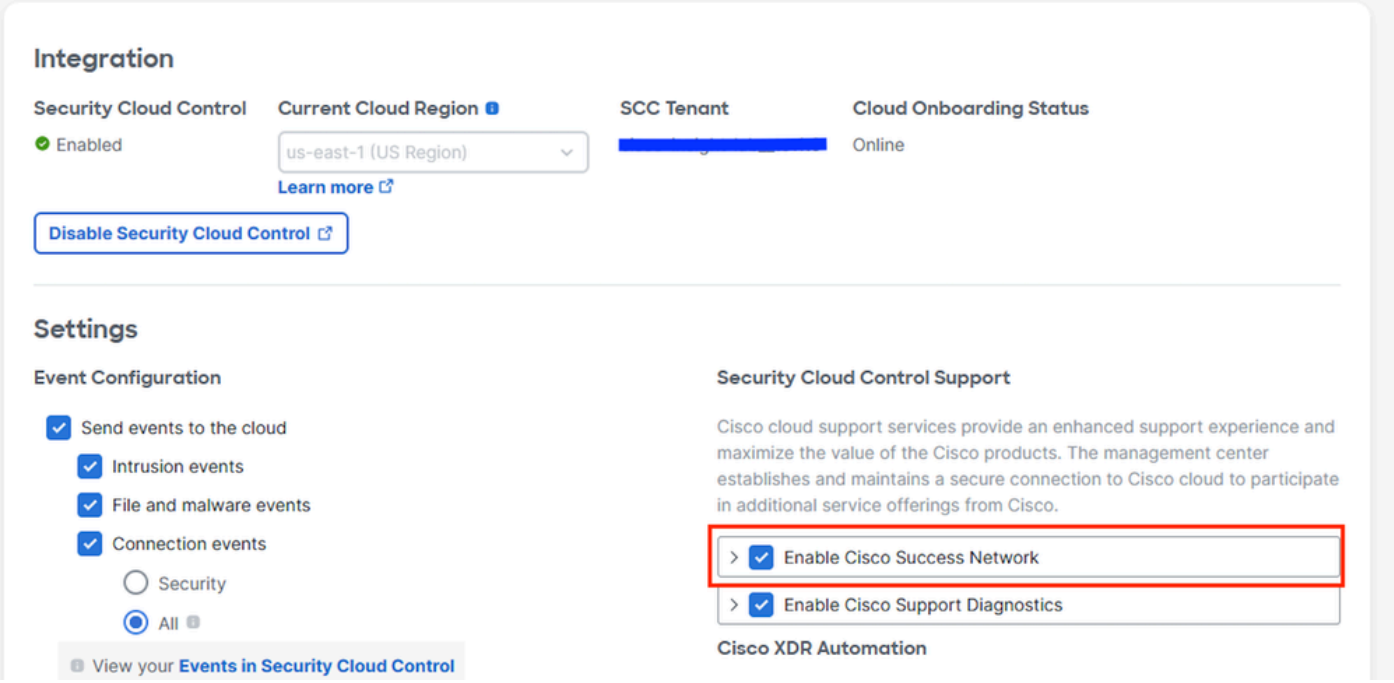
FMC-GUI-Schnittstelle.



Schritt 2.2: Navigieren Sie zu Cisco Success Network Settings: Wählen Sie im Hauptmenü Integration > Cisco Security Cloud aus.



Schritt 2.3. Suchen und aktivieren Sie die Option mit der Bezeichnung Cisco Success Network: Aktivieren Sie dazu das Kontrollkästchen Enable Cisco Success Network to activate the telemetry.



Schritt 3: Installieren von Updates: Installieren Sie GeoDB 2025-04-03-094 oder VDB 406 (oder höher). Dies löst die Installation eines neuen 365-Tage-Zertifikats aus.

Anmerkung: Hohe Verfügbarkeit In einem HA-Paar wird der SSEConnector-Prozess nicht auf dem Standby-Gerät ausgeführt. Um das Standby-FMC zu aktualisieren, führen Sie einen Rollenschalter aus, sodass das Standby-FMC aktiviert wird, und installieren Sie dann das erforderliche VDB- oder GeoDB-Update.

---

3. Fehlerbehebung für die Versionen 7.6.1+ und 7.7.10+

Dieses Problem tritt in der Regel in Umgebungen auf, in denen keine Cisco Security Cloud (CSC)-Standardregistrierung erfolgt, wie z. B. Umgebungen, in denen Evaluierungslizenzen, SSM On-Prem, PLR oder SLR verwendet werden.

Betroffene Funktionen

- Automatische/manuelle Aktualisierungen des LSP (Lightweight Security Package)
- URL-Filterung, Aktualisierung von Datenbankinhalten und Cloud-Suche.
- Talos Bereicherung von Verbindungsereignissen.

Empfohlene Maßnahmen

1. Standardumgebung: Registrieren Sie das FMC über Integration > Cisco Security Cloud. Durch die Registrierung wird innerhalb von 30 Minuten automatisch ein neues Zertifikat heruntergeladen.

2. Manuelle Aktualisierungen: Wenn die automatischen Updates fehlschlagen, laden Sie den neuesten LSP manuell von software.cisco.com herunter, und installieren Sie ihn direkt auf dem FMC.

3. Air-Gap Umgebungen: Wenn Ihr Netzwerk keinen Internetzugang hat, ist das Statusmodul für den Talos-Verbindungsstatus irrelevant. Deaktivieren Sie in diesem Szenario dieses Modul innerhalb der angewendeten Integritätsrichtlinie.

Zugehörige Informationen

- Weitere Unterstützung erhalten Sie vom Cisco Technical Assistance Center (TAC). Ein gültiger Support-Vertrag ist erforderlich: Cisco Worldwide Support Contacts

- Cisco Support und Downloads: 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.