Risoluzione dei problemi relativi allo stato di connettività di Talos

Sommario

Introduzione

In questo documento viene descritto come risolvere i problemi di connettività di TALOS in Secure Firewall FMC e FDM.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Secure Firewall Management Center (FMC)

- Cisco Secure Firewall Device Manager (FDM)

- Cisco Secure Firewall Threat Defense (FTD)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

FMC versione 7.6.0 o 7.7.0
FDM versione 7.6.0 o 7.7.0
FTD versione 7.6.0 o 7.7.0

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Il Cisco Secure Firewall Management Center (FMC) si basa su un certificato sul lato client per stabilire una connessione sicura con i servizi Cisco Talos Threat Intelligence. Questa autenticazione è essenziale per consentire al FMC di scaricare correttamente gli aggiornamenti critici, inclusi i database URL Reputation (URLDB), i pacchetti LSP (Lightweight Security Packages) e altri dati di arricchimento.

In condizioni operative normali, il presente certificato viene predisposto durante l'installazione del software ed è progettato per essere rinnovato automaticamente quando si avvicina alla data di scadenza. Tuttavia, un problema noto in alcune versioni del software Cisco Secure Firewall FMC impedisce il corretto completamento del processo di rinnovo automatico dopo il 30 marzo 2025. Quando ciò accade, la FMC non può autenticarsi con Talos, causando problemi di connettività e l'impossibilità di recuperare informazioni aggiornate sulle minacce.

Verifica dello stato del certificato

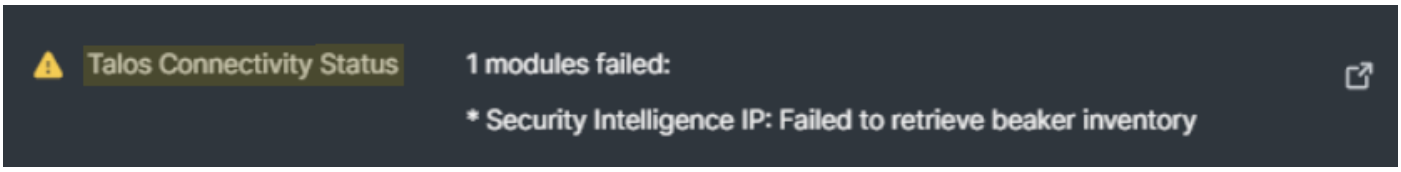
GUI FMC

Quando il rinnovo del certificato sul lato client non riesce, Cisco FMC attiva avvisi di integrità per notificare agli amministratori l'interruzione nella comunicazione con Cisco Talos. Per monitorare questi allarmi, selezionare Sistema > Stato ed esaminare la sezione Stato connettività talos.

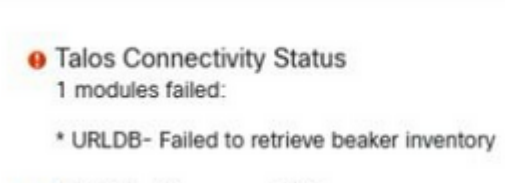
Se il problema relativo alla scadenza del certificato influisce sul sistema, viene in genere

visualizzato uno dei messaggi di errore seguenti:

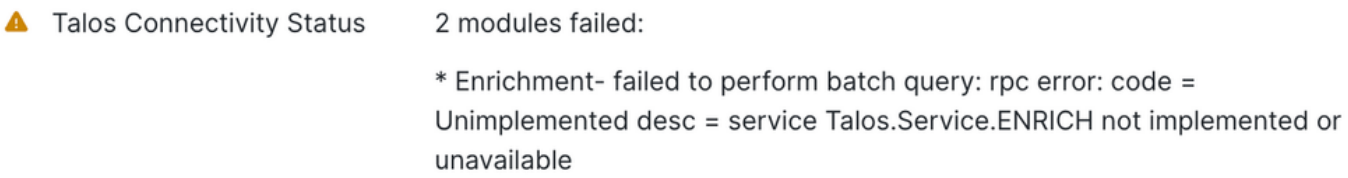
- "LSP - Impossibile recuperare l'inventario del becher":



- "URLDB - Impossibile recuperare l'inventario del becher":



- "Arricchimento - Impossibile eseguire query batch":



CLI FMC

Per determinare se l'accessorio FMC è interessato dal problema, accedere in modalità Expert ed eseguire il comando per verificare la data di scadenza corrente del certificato sul lato client:

<#root>

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

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

Nell'output del comando, trovare la sezione Validità. Il campo Non dopo indica la data di scadenza corrente del certificato. Se la data è già trascorsa o si sta avvicinando, il processo di rinnovo non è riuscito ed è necessario riavviare manualmente il servizio per avviare il rinnovo del certificato.

Esempio:

<#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
```

Risoluzione dei problemi

1. Identificare lo scenario

Versione del software	ID bug associato	Causa principale
7.6.0 o 7.7.0	ID bug Cisco CSCwo63951	Scadenza certificato/errore di connettività
7.6.1+ o 7.7.10+	ID bug Cisco CSCwr23982	Registrazione/configurazione delle licenze (ad esempio, con intercapedine).

2. Risoluzione dei problemi per le versioni 7.6.0 e 7.7.0

Sintomi

Oltre agli avvisi sullo stato di salute menzionati in precedenza, si osservano questi comportamenti:

- Errori di Task Manager FDM: "Aggiornamento cloud Snort 3 non riuscito: Nessuna risposta dal server di aggiornamento o timeout della connessione."
- Voci di registro: Errori in /ngfw/var/log/messages indicanti: Failed to connect to tunnel (UUID), error: Non connesso.
- Stato: Aggiornamenti stagnanti nell'interfaccia utente: Nella schermata Preferenze filtro URL viene visualizzato "Non ancora aggiornato".

Soluzione temporanea

Per ripristinare immediatamente i servizi, riavviare i processi necessari tramite la modalità Expert:

Passaggio 1. Accedere alla CLI e accedere alla modalità Expert.

Passaggio 2. Eseguire i comandi:

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

Nota: Questa soluzione attiva un certificato valido solo per cinque giorni. È necessario ripetere questa procedura ogni cinque giorni fino a quando non viene applicata una correzione permanente.

Risoluzione permanente

Per risolvere il problema in modo permanente, verificare che siano soddisfatte le seguenti condizioni:

Passaggio 1. Verificare la connettività: Verificare che l'accessorio disponga dell'accesso in uscita a https://api-sse.cisco.com. A tale scopo, accedere alla CLI di FMC, accedere in modalità Expert

ed eseguire i comandi:

Passaggio 1.1. Verifica della risoluzione DNS:

<#root>

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

nslookup api-sse.cisco.com
```

Passaggio 1.2. Verifica dell'accesso alla porta TCP:

<#root>

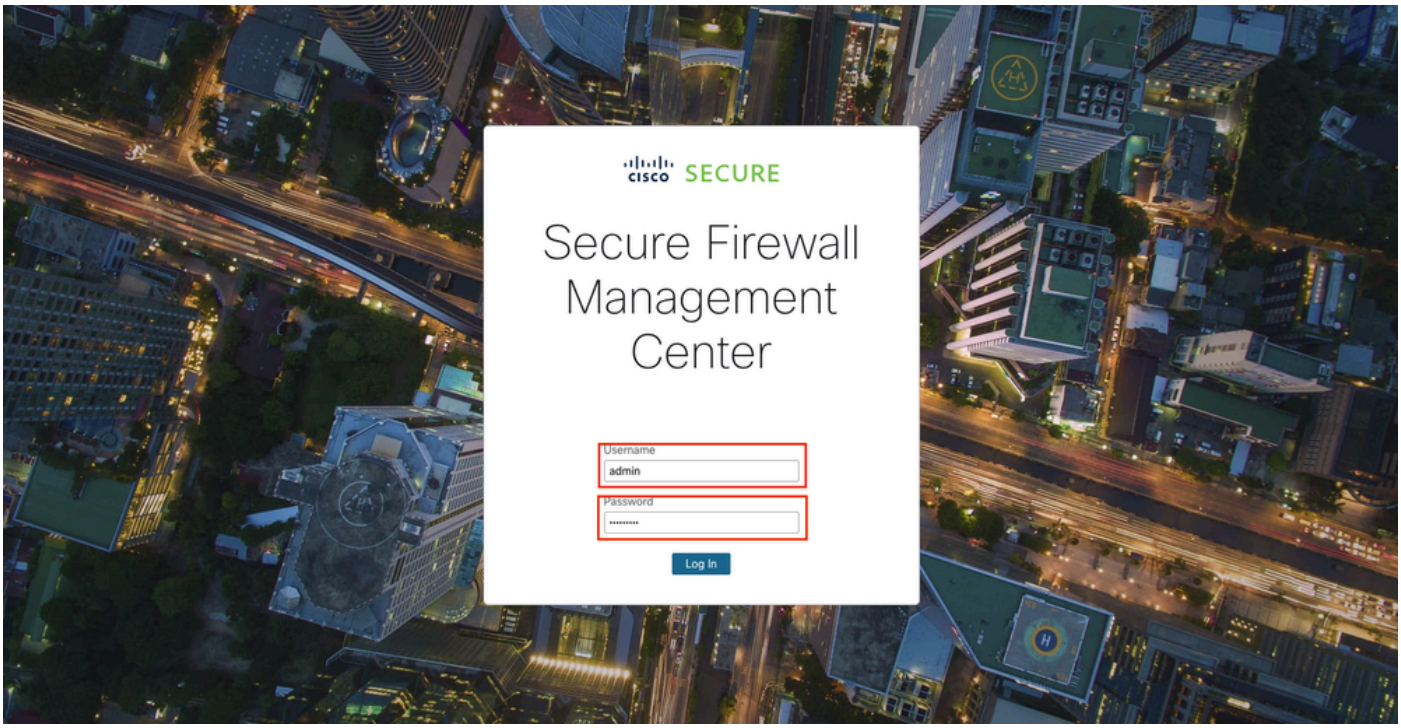
```
 expert
sudo su
//type the 'FMC CLI admin password'

telnet api-sse.cisco.com 443
```

Nota: Verificare che l'accesso HTTPS (TCP 443) in uscita a https://api-sse.cisco.com sia consentito tramite tutti i firewall upstream, i proxy o i dispositivi di sicurezza.

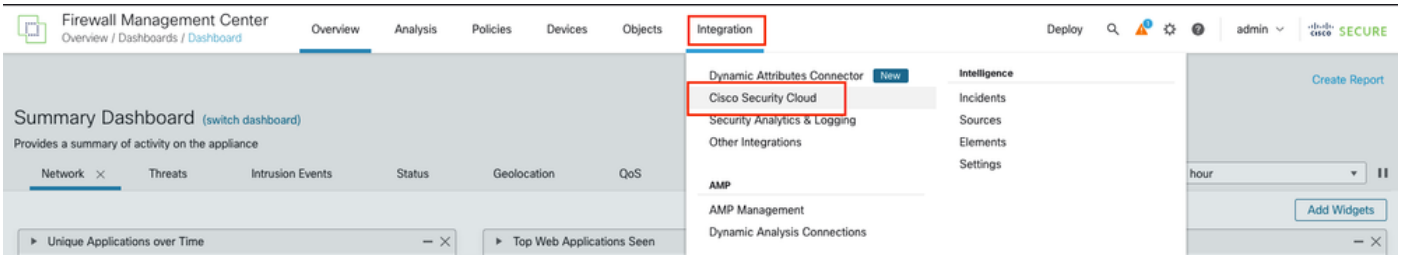
Passaggio 2. Abilitare la telemetria: Verificare che la telemetria CSN (Customer Success Network) sia abilitata in modo che SSEConnector possa ottenere un nuovo certificato. Per abilitare il CSN nel CCP, eseguire la procedura seguente:

Passaggio 2.1. Accedere all'interfaccia utente dell'FMC aprendo un browser Web e selezionando l'URL dell'FMC (ad esempio: https://<FMC_IP_or_Hostname>). Immettere il nome utente e la password per accedere al

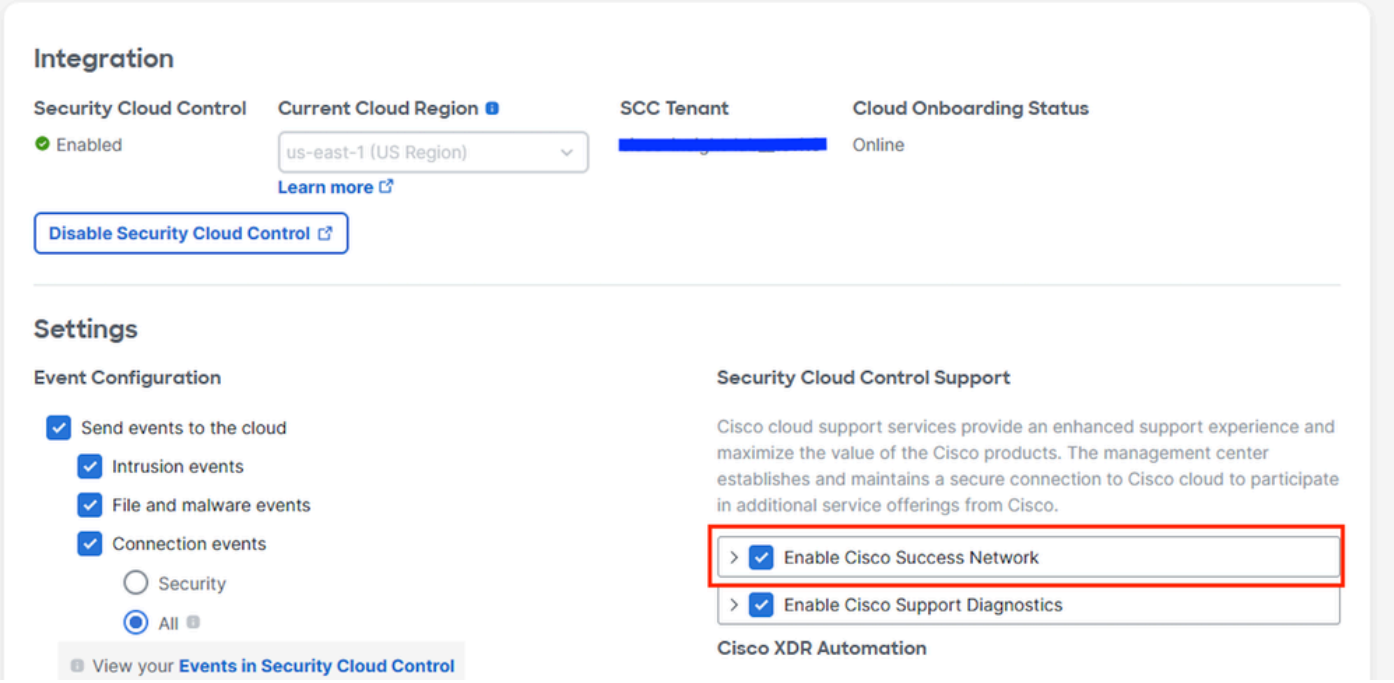
Interfaccia GUI FMC.



Passaggio 2.2. Passare a Cisco Success Network Settings: Dal menu principale, selezionare Integration > Cisco Security Cloud (Integrazione).



Passaggio 2.3. Individuare e abilitare l'opzione Cisco Success Network: Per questo motivo, selezionare la casella di controllo Abilita Cisco Success Network per attivare la telemetria.



Passaggio 3. Installare gli aggiornamenti: Installare GeoDB 2025-04-03-094 o VDB 406 (o versione successiva). In questo modo viene avviata l'installazione di un nuovo certificato valido 365 giorni.

Nota: Alta disponibilità (HA). In una coppia HA, il processo SSEConnector non viene eseguito sull'unità di standby. Per aggiornare il FMC in standby, eseguire un cambio di ruolo in modo che lo standby diventi attivo, quindi installare l'aggiornamento VDB o GeoDB richiesto.

---

3. Risoluzione dei problemi per le versioni 7.6.1+ e 7.7.10+

Questo problema si verifica in genere in ambienti senza registrazione Cisco Security Cloud (CSC) standard, ad esempio in ambienti che utilizzano licenze di valutazione, SSM On-Prem, PLR o SLR.

Caratteristiche interessate

- Aggiornamenti LSP (Lightweight Security Package) automatici/manuali.
- Filtro URL: aggiornamenti del contenuto del database e ricerche cloud.
- Talos arricchisce gli eventi di connessione.

Azioni consigliate

1. Ambiente standard: Registrare il CCP tramite Integration > Cisco Security Cloud. La registrazione attiva automaticamente il download di un nuovo certificato entro 30 minuti.

2. Aggiornamenti manuali: Se gli aggiornamenti automatici hanno esito negativo, scaricare manualmente l'ultimo provider di servizi di traduzione da software.cisco.com e installarlo direttamente nel FMC.

3. Ambienti con intercapedine ad aria: Se la rete non dispone di un accesso a Internet, il modulo di stato della connettività di Talos diventa irrilevante. In questo scenario, disabilitare questo modulo specifico all'interno del criterio di integrità applicato.

Informazioni correlate

- Per ulteriore assistenza, contattare il Cisco Technical Assistance Center (TAC). È necessario un contratto di supporto valido: Contatti del supporto Cisco internazionali.

- Supporto e download Cisco: 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).