Dépannage de l'état de connectivité Talos

Table des matières

Introduction

Ce document décrit comment dépanner les problèmes de connectivité TALOS sur Secure Firewall FMC et FDM.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

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

- Cisco Secure Firewall Threat Defense (FTD)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

FMC version 7.6.0 ou 7.7.0
FDM version 7.6.0 ou 7.7.0
FTD version 7.6.0 ou 7.7.0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Le Cisco Secure Firewall Management Center (FMC) s'appuie sur un certificat côté client pour établir une connexion sécurisée avec les services de renseignements sur les menaces de Cisco Talos. Cette authentification est essentielle pour que le FMC puisse télécharger avec succès les mises à jour critiques, notamment les bases de données de réputation d'URL (URLDB), les packages de sécurité légers (LSP) et d'autres données d'enrichissement.

Dans des conditions de fonctionnement normales, ce certificat est pré-provisionné lors de l'installation du logiciel et est conçu pour être renouvelé automatiquement à la date d'expiration. Cependant, un problème connu dans certaines versions du logiciel Cisco Secure Firewall FMC empêche le processus de renouvellement automatique de se terminer après le 30 mars 2025. Dans ce cas, le FMC ne peut pas s'authentifier auprès de Talos, ce qui entraîne des pannes de connectivité et l'incapacité à récupérer des informations actualisées sur les menaces.

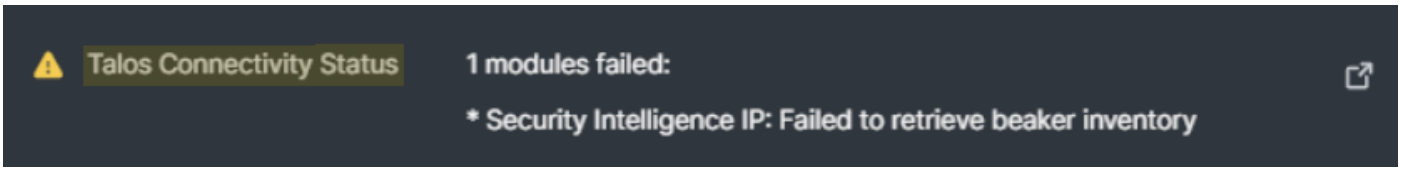
Vérification du statut du certificat

Interface graphique FMC

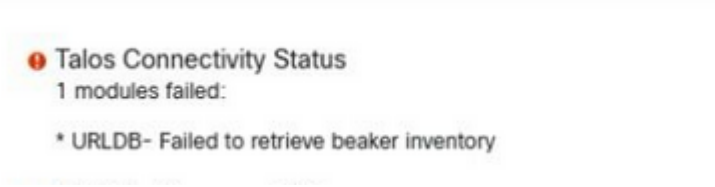
Lorsque le certificat côté client ne se renouvelle pas, Cisco FMC déclenche des alertes d'intégrité pour informer les administrateurs de l'interruption de la communication avec Cisco Talos. Vous pouvez surveiller ces alertes en accédant à System > Health et en consultant la section Talos Connectivity Status.

Si votre système est affecté par le problème d'expiration du certificat, vous voyez généralement l'un des messages d'erreur suivants :

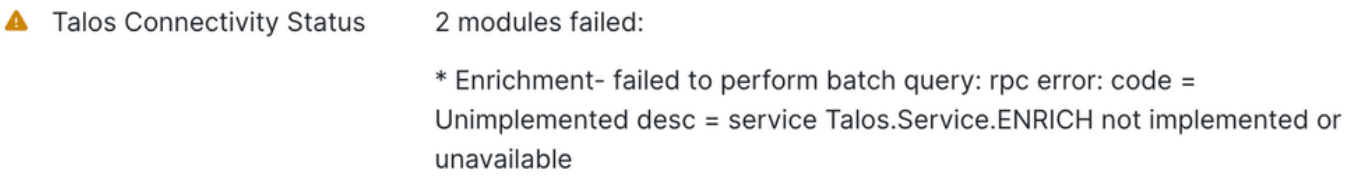
- "LSP - Echec de la récupération de l'inventaire du bécher" :



- "URLDB - Echec de la récupération de l'inventaire du bécher" :



- "Enrichissement - Echec de l'exécution de la requête par lots" :



CLI FMC

Pour déterminer si votre appliance FMC est affectée par ce problème, accédez au mode expert et exécutez la commande pour vérifier la date d'expiration actuelle du certificat côté 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
```

Dans le résultat de la commande, recherchez la section Validité. Le champ Not After indique la date d'expiration actuelle du certificat. Si cette date est déjà dépassée ou approche, le processus de renouvellement a échoué et un redémarrage manuel du service est nécessaire pour lancer le renouvellement du certificat.

Exemple :

<#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
```

Dépannage

1. Identifiez votre scénario

Version du logiciel	ID de bogue associé	Cause principale
7.6.0 ou 7.7.0	ID de bogue Cisco CSCwo63951	Expiration du certificat / Échec de la connectivité
7.6.1+ ou 7.7.10+	ID de bogue Cisco CSCwr23982	Configuration de l'enregistrement/de la licence (par exemple, à entrefer).

2. Dépannage des versions 7.6.0 et 7.7.0

Symptômes

Au-delà des alertes de santé mentionnées précédemment, vous observez ces comportements :

- Erreurs du Gestionnaire des tâches FDM : "Echec de la mise à jour du cloud Snort 3 : Aucune réponse du serveur de mise à jour ou délai de connexion."
- Entrées du journal : Erreurs dans /ngfw/var/log/messages indiquant : Echec de la connexion au tunnel (UUID), erreur : Non connecté.
- État : Mises à jour stagnantes dans l'interface utilisateur : L'écran Préférences de filtrage des URL affiche « Pas encore mis à jour ».

Contournement temporaire

Pour restaurer les services immédiatement, redémarrez les processus requis via le mode Expert :

Étape 1. Accédez à l’interface de ligne de commande et passez en mode expert.

Étape 2. Exécutez les commandes :

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

Remarque : Cette solution de contournement déclenche un certificat valide pendant seulement cinq jours. Vous devez répéter ce processus tous les cinq jours jusqu'à ce qu'une correction permanente soit appliquée.

Résolution Permanente

Pour résoudre définitivement ce problème, assurez-vous que les conditions suivantes sont remplies :

Étape 1. Vérification de la connectivité : Assurez-vous que l'appliance dispose d'un accès sortant à https://api-sse.cisco.com. Pour ce faire, accédez à l'interface de ligne de commande du FMC,

passez en mode expert et exécutez les commandes suivantes :

Étape 1.1. Test de la résolution DNS :

<#root>

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

nslookup api-sse.cisco.com

Étape 1.2. Test de l’accès au port TCP :

<#root>

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

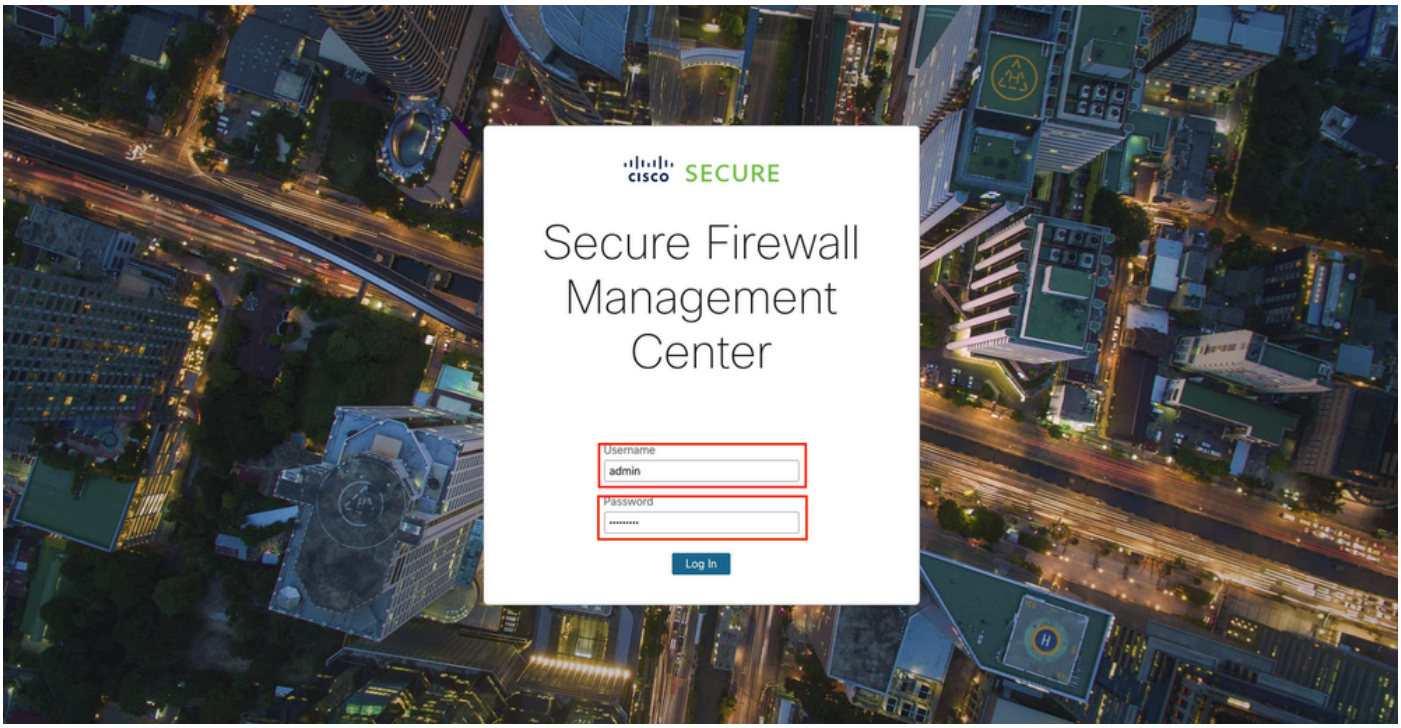
telnet api-sse.cisco.com 443

Remarque : Vérifiez que l'accès HTTPS sortant (TCP 443) à https://api-sse.cisco.com est autorisé via tous les pare-feu, proxys ou périphériques de sécurité en amont.

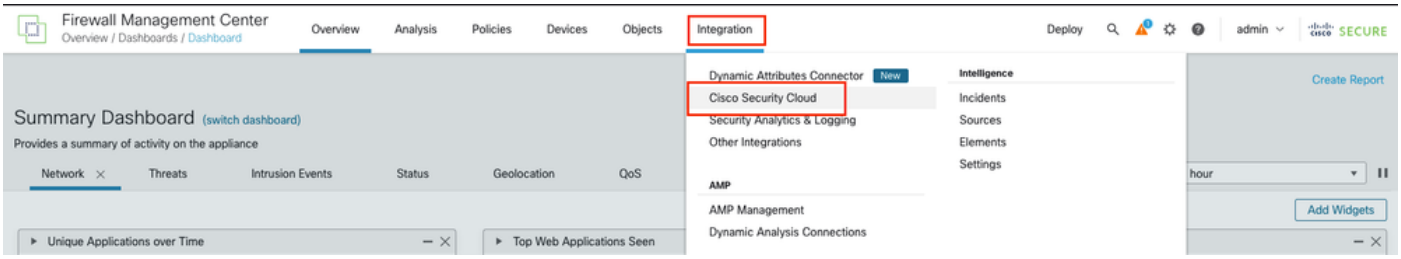
Étape 2. Activer la télémétrie : Assurez-vous que la télémétrie CSN (Customer Success Network) est activée pour que le connecteur SEC puisse obtenir un nouveau certificat. Pour activer CSN sur le FMC, procédez comme suit :

Étape 2.1. Connectez-vous à l’interface graphique FMC en ouvrant un navigateur Web et en accédant à l’URL FMC (par exemple : https://<FMC_IP_or_Hostname>). Entrez votre nom d'utilisateur et votre mot de passe pour accéder

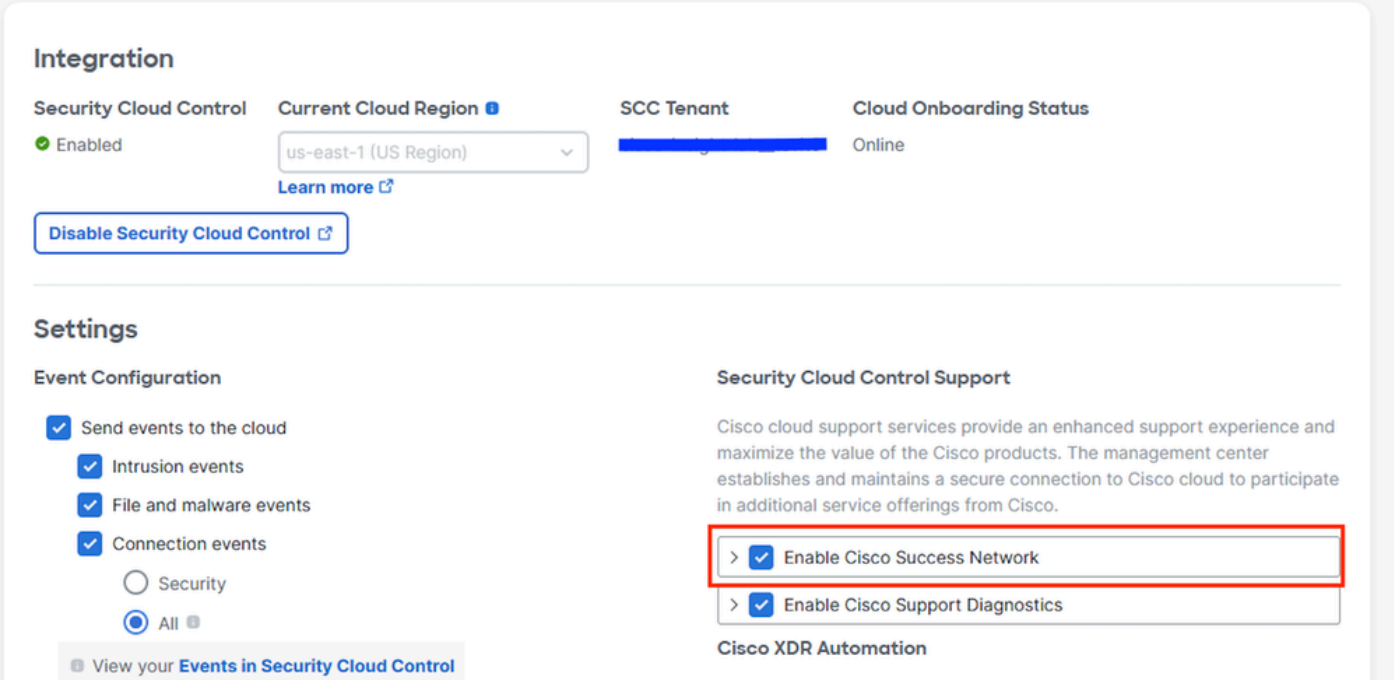
Interface GUI du FMC.



Étape 2.2. Accédez à Cisco Success Network Settings : Dans le menu principal, sélectionnez Integration > Cisco Security Cloud.



Étape 2.3. Rechercher et activer l'option intitulée Cisco Success Network : Pour cela, cochez la case Enable Cisco Success Network pour activer la télémétrie.



Étape 3. Installation des mises à jour : Installez GeoDB 2025-04-03-094 ou VDB 406 (ou version ultérieure). Cela déclenche l'installation d'un nouveau certificat de 365 jours.

Remarque : Haute disponibilité (HA). Dans une paire haute disponibilité, le processus SSEConnector ne s'exécute pas sur l'unité en veille. Pour mettre à jour le FMC de secours, effectuez un changement de rôle afin que le FMC de secours devienne actif, puis installez la mise à jour VDB ou GeoDB requise.

---

3. Dépannage des versions 7.6.1+ et 7.7.10+

Ce problème se produit généralement dans les environnements sans enregistrement CSC (Cisco Security Cloud) standard, tels que ceux utilisant des licences d'évaluation, SSM On-Prem, PLR ou SLR.

Fonctionnalités impactées

- Mises à jour LSP (Lightweight Security Package) automatiques/manuelles.
- Filtrage des URL, mises à jour de contenu de base de données et recherches cloud.
- Enrichissement Talos des événements de connexion.

Actions recommandées

1. Environnement standard : Enregistrez le FMC via Integration > Cisco Security Cloud. L'enregistrement déclenche automatiquement le téléchargement d'un nouveau certificat dans les 30 minutes.

2. Mises à jour manuelles Si les mises à jour automatiques échouent, téléchargez manuellement le dernier LSP à partir de software.cisco.com et installez-le directement sur le FMC.

3. Environnements à vide : Si votre réseau n'a pas d'accès à Internet, le module d'état de la connectivité Talos devient inutile. Dans ce scénario, désactivez ce module spécifique dans votre stratégie d'intégrité appliquée.

Informations connexes

- Pour obtenir de l'aide supplémentaire, contactez le centre d'assistance technique de Cisco. Un contrat d'assistance valide est requis : Cisco Worldwide Support Contacts.

- Assistance et téléchargements Cisco : Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.