Dépannage des sources de menaces externes Principales raisons de l'échec

Table des matières

Introduction

Ce document décrit plusieurs causes d'échec lors de la mise en oeuvre du Flux de menaces externes, l'analyse des erreurs et les actions de résolution.

Conditions préalables

Il n'y a pas de conditions spécifiques, c'est pourquoi Cisco vous recommande de connaître les sujets suivants :

- Passerelle de messagerie sécurisée Cisco (ESA)
- Flux de menaces externes (ETF)

Composants utilisés

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

- Cisco Secure Email Gateway (ESA) exécutant le logiciel 12.x ou une version ultérieure

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 lâ€™incidence possible des commandes.

Raison des échecs :

Le service ETF est désactivé ou il n'existe pas de clé de fonction valide pour le service

<#root>

```
(Machine esa03.taclab.krk) (SERVICE)> tail threatfeeds

Press Ctrl-C to stop.
Wed Sep 8 16:15:26 2021 Info: THREAT_FEEDS: A delta poll is scheduled for the source: Test_Poll_Path
Machine: â€˜esa03.taclab.krk'. A failure was encountered for the source 'Test_Poll_Path'.

Reason for failure: The ETF service is either disabled or there is no valid feature key for the service.
```

Solution

Vérifiez les points suivants :

1. Clé de fonction ETF installée correctement.
2. CLUF accepté et clé de fonction activée globalement.
3. Licences appliquées au niveau machine.

Remarque : s'il existe un niveau de cluster, il doit copier le paramètre au niveau de l'ordinateur.

Échec de l'établissement d'une nouvelle connexion : [Erreur 110] Expiration de la connexion

```
(Machine esa03.taclab.krk) (SERVICE)> tail threatfeeds

Press Ctrl-C to stop.
Reason for failure: Taxii Error: HTTPSConnectionPool(host= otx.alienvault.comport, port=443): Max retrie
Failed to establish a new connection: [Errno 110] Connection timed out',))
```

Remarque : le délai d'attente de la connexion indique généralement un problème lié au réseau, qui empêche ESA d'obtenir une réponse. Les vérifications de pare-feu/proxy sont recommandées et la capture de paquets pour une analyse plus approfondie.

Solution

1. Vérifiez que le pare-feu et le proxy ne bloquent pas le trafic.
   Le proxy peut être vérifié sous **GUI > Security Services > Service Updates.**
2. Confirmez la connectivité avec la capture de paquets. Accédez à **GUI > Help and Support > Packet Capture.**

Conseil : en cas d'indications de problèmes liés au réseau, il est prudent d'exécuter des captures de paquets afin de vérifier que la connexion a été correctement établie.

Raison de l'échec : « 400 »

```
(Machine esa03.taclab.krk) (SERVICE)> grep "Sep 6 13:38" threatfeeds
Mon Sep 6 13:38:16 2021 Debug: THREAT_FEEDS: Failed to fetch observables from the source: Test_Poll_Path
Mon Sep 6 13:38:55 2021 Info: THREAT_FEEDS: The source 'Test_Poll_Path' is currently in a polling state
```

Remarque : l'erreur 400 (Requête incorrecte) RFC7231 indique que le serveur ne peut pas ou ne traite pas la requête en raison d'un élément perçu comme une erreur du client. La plupart du temps, il apparaît en raison d'une syntaxe de requête incorrecte ou d'un verrouillage de trame de message de requête non valide.

Solution

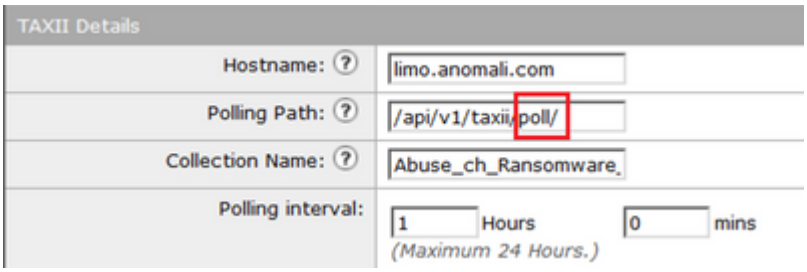
L'erreur « 400 » indique que ce chemin d'interrogation existe, mais qu'il pointe vers un service différent offert par le serveur TAXII.

1. Confirmez que la configuration du chemin d'interrogation est configurée avec une demande d'interrogation et non avec une demande de découverte.
2. Vérifiez que HTTPS est activé sous **GUI > Mail Policies > External Threat Feeds Manager > Use HTTPS.**

Attention : ce problème se produit généralement lorsque le chemin d'interrogation est mal configuré avec une requête de découverte, telle que : /api/v1/taxii/taxii-discovery-service/
Le chemin d'interrogation peut être configuré pour utiliser la requête d'interrogation pour les flux, par exemple : /api/v1/taxi/poll

---

Remarque : différence entre la demande d'interrogation et la demande de découverte :
- L'URL d'interrogation est en fait l'endroit où vous consommez les flux de.
- URL du service de découverte est utilisé pour trouver quels services le service de taxi offre.



Erreur HTTP : code d'état 401 - échec d'authentification

```
(Machine esa03.taclab.krk) (SERVICE)> grep "Sep 8 16:35" threatfeeds
Wed Sep 8 16:35:39 2021 Debug: THREAT_FEEDS: Updating the timestamp: 2021-09-08 16:31:36.071684 for the
Wed Sep 8 16:35:39 2021 Info: THREAT_FEEDS: Job failed with exception : Source: ETF_Source_Name. Reason
```

Solution

Ce code d'erreur indique qu'il manque des informations d'authentification valides pour la ressource cible.

Vérifiez que les informations d'identification sont correctement configurées.

Il est également possible de ne pas configurer les informations d'identification des utilisateurs.

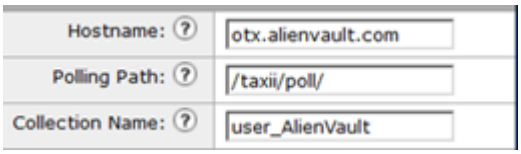
Erreur de taxi : Erreur HTTP : Code d'état 404 Ressource demandée non disponible

```
(Machine esa03.taclab.krk) (SERVICE)> grep "Aug 27 08:51" threatfeeds
Fri Aug 27 08:51:16 2021 Warning: THREAT_FEEDS: Unable to fetch the observables from the source: Test af
Fri Aug 27 08:51:16 2021 Info: THREAT_FEEDS: Job failed with exception : Source: Test. Reason for failur
```

> **Remarque** : le code d'état 404 (introuvable) indique que le serveur d'origine n'a pas trouvé de représentation actuelle pour la ressource cible ou n'est pas disposé à en divulguer une. Cela indique qu'il peut y avoir une URL non valide et, dans la plupart des cas, que le problème s'est produit en raison du chemin de la ressource est introuvable.

Solution

Confirmez le chemin d'interrogation/nom de la collection sur la source sous ESA **GUI> Politiques de messagerie > Gestionnaire des sources de menaces externes > Choisissez le nom de la source approprié**.



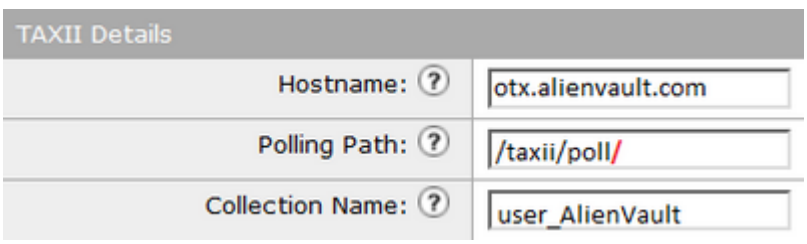
Raison de l'échec : « 405 »

```
(Machine esa03.taclab.krk) (SERVICE)> grep "Sep 13 00:2" threatfeeds
Mon Sep 13 00:20:21 2021 Debug: THREAT_FEEDS: Failed to fetch observables from the source: Anomali. Reas
```

> **Remarque** : selon RFC7231, l'erreur 405 (Method Not Allowed) indique que la méthode reçue dans la ligne de requête est connue du serveur d'origine, mais non prise en charge par la ressource cible.

Solution

Il s'agit d'une erreur de syntaxe due à la barre oblique « / » manquante à la fin du chemin d'interrogation. Ajouter la barre oblique à la fin du chemin /taxi/poll/.



Erreur HTTP : Service de code d'état 503 indisponible

```
(Machine esa03.taclab.krk) (SERVICE)> grep "Nov 10 13:45" threatfeeds
Sun Nov 10 13:45:21 2020 Info: THREAT_FEEDS: Job failed with exception : Source: ETF_Source_Name. Reason
Sun Nov 10 13:45:22 2020 Info: THREAT_FEEDS: A delta poll is scheduled for the source: ETF_Source_Name
```

> **Remarque** : selon RFC7231, l'erreur 503 « Service indisponible » est un code d'état de réponse HTTP qui indique qu'un serveur est temporairement incapable de traiter la requête.

Solution

Le code d'erreur indique un problème avec le serveur TAXII de destination, qui doit être étudié plus en détail.
Cela peut se produire lorsque le serveur est surchargé. Pour plus d'informations, contactez le fournisseur.

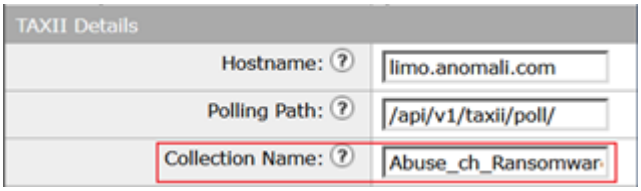
NOT_FOUND : impossible de trouver la collection demandée

```
(Machine esa03.taclab.krk) (SERVICE)> grep "Sep 7 12:53" threatfeeds
Tue Sep 7 12:53:16 2021 Warning: THREAT_FEEDS: Unable to fetch the observables from the source: Test_Pol
Tue Sep 7 12:53:16 2021 Debug: THREAT_FEEDS: Updating the timestamp: 2021-09-07 12:49:12.648625 for the
```

Solution

Cette erreur indique que le nom de la collection est correctement orthographié. Cependant, un problème se produit sur le serveur TAXII sous Collection, qui rejette la demande.

La cause possible peut être un minuteur d'expiration sur le nom de la collection.
Contactez le Fournisseur pour vérifier ce type d'incohérence.



[SSL : CERTIFICATE_VERIFY_FAILED] La vérification du certificat a échoué (_ssl.c : 590)

<#root>

```
(Machine esa03.taclab.krk) (SERVICE)> grep "Sep 8 16:35" threatfeeds
Wed Sep 8 16:35:26 2021 Info: THREAT_FEEDS: A delta poll is scheduled for the source: ETF_Source_Name
Wed Sep 8 16:35:33 2019 Warning: THREAT_FEEDS: Unable to fetch the observables from the source: ETF_Sou
```

Reason for failure: Taxii Error: [SSL: CERTIFICATE_VERIFY_FAILED] certificate verify failed (_ssl.c:590)

Solution

Cette erreur indique un échec du certificat.

Pour résoudre le problème, importez le certificat dans la liste de l'autorité de certification (CA).
Accédez à **GUI > Network > Certificates > Edit Settings > Custom List >**
Choisissez le mode **Enable** et téléchargez le certificat.

Erreur d'analyse XML : Aucun élément trouvé (ligne 0)

<#root>

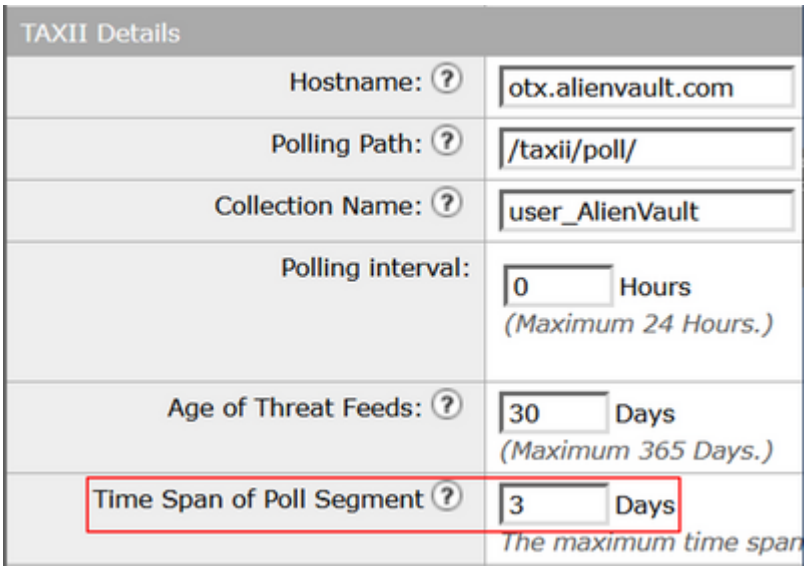
```
(Machine esa03.taclab.krk) (SERVICE)> grep "Aug 21 02:39" threatfeeds
Fri Aug 21 02:39:37 2021 Warning: THREAT_FEEDS: Unable to fetch the observables from the source: ETF_Sou
Fri Aug 21 02:39:37 2021 Info: THREAT_FEEDS: Job failed with exception : Source: ETF_Source_Name.
```

Reason for failure: Taxii Error: XML Parising Error: no element found (line 0)

Solution

Réduisez la valeur Durée du segment d'interrogation de la configuration ESA à 3-4 jours.

> **Remarque** : il s'agit d'une incohérence avec les serveurs Anomali pour certains flux spécifiques, où aucun indicateur de fin de données n'est envoyé pour arrêter les flux.
> Dans ce cas, ESA qui est configuré avec une source ETF d'Anomali, n'est pas en mesure d'interroger les données pendant une période de plus de 5 jours.
> Une solution de contournement valide serait de réduire la valeur Time Span of Poll Segment à partir de la configuration ESA.



Impossible d'établir une nouvelle connexion : [Erreur 111] Connexion refusée

<#root>

```
(Machine esa03.taclab.krk) (SERVICE)> tail threatfeeds

Press Ctrl-C to stop.
Reason for failure: Taxii Error: HTTPSConnectionPool(host=otx.alienvault.comport=443): Max retries exce
```

Failed to establish a new connection: [Errno 111] Connection refused',))

> **Remarque** : « Connexion refusée » indique que le client ne peut pas se connecter au port sur le serveur en cours d'exécution. En général, cela se produit lorsque le serveur écoute sur le mauvais port ou lorsque le port n'est pas disponible.

Solution

1. Utilisez la commande **telnet** ou **netstat** via CLI pour vérifier que le port approprié écoute.
2. Vérifiez que le pare-feu ne bloque pas le port.
3. Assurez-vous qu'il n'y a aucune erreur de configuration de port / port obsolète sur le service en cours.

Informations connexes

- Guides de l'utilisateur final du dispositif de sécurisation de messagerie Cisco
- Que sont STIX et TAXII
- RFC2741 - Codes d'erreur
- Flux de menaces externes de l'atelier TAC

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.