Fehlerbehebung bei externen Bedrohungs-Feeds Hauptgründe für Fehler

Inhalt

Einleitung

In diesem Dokument werden mehrere Gründe für das Versagen bei der Implementierung von External Threat Feed, Fehleranalysen und Maßnahmen zur Behebung beschrieben.

Voraussetzungen

Es gibt keine spezifischen Anforderungen. Daher empfiehlt Cisco, dass Sie über Kenntnisse in den folgenden Themen verfügen:

- Cisco Secure Email Gateway (ESA)
- Externe Bedrohungs-Feeds (ETF)

Verwendete Komponenten

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

- Cisco Secure Email Gateway (ESA) mit Software 12.x oder einer späteren Version

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.

Fehlerursache:

Der ETF-Dienst ist entweder deaktiviert oder es ist kein gültiger Feature-Schlüssel für den Dienst vorhanden.

<#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.
```

Lösung

Stellen Sie Folgendes sicher:

1. Der ETF-Feature-Schlüssel wurde ordnungsgemäß installiert.
2. EULA akzeptiert und Feature-Schlüssel global aktiviert.
3. Angewandte Lizenzen auf Computerebene.

Hinweis: Wenn eine Cluster-Ebene vorhanden ist, muss die Einstellung auf Computerebene kopiert werden.

Fehler beim Herstellen einer neuen Verbindung: [Errno 110] Zeitüberschreitung bei Verbindung.

```
(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',))
```

Hinweis: Ein Timeout bei der Verbindung weist in der Regel auf ein netzwerkbezogenes Problem hin, weshalb die ESA keine Antwort erhalten kann. Firewall-/Proxy-Prüfungen werden empfohlen, und die Paketerfassung dient der eingehenderen Analyse.

Lösung

1. Bestätigen Sie, dass Firewall und Proxy den Datenverkehr nicht blockieren.
   Der Proxy kann unter **GUI > Security Services > Service Updates** überprüft werden**.**
2. Bestätigen der Verbindung mit der Paketerfassung Navigieren Sie zu **GUI > Help and Support > Packet Capture.**

Tipp: Wenn es Anzeichen für Netzwerkprobleme gibt, ist es ratsam, die Paketerfassung auszuführen, um sicherzustellen, dass die Verbindung ordnungsgemäß hergestellt wurde.

Fehlerursache: "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
```

> **Hinweis:** RFC7231 Error 400 (Bad Request) gibt an, dass der Server die Anfrage aufgrund eines vermuteten Client-Fehlers nicht verarbeiten kann. Die meisten Male wird sie aufgrund einer fehlerhaften Anforderungssyntax oder eines ungültigen Framings von Anforderungsnachrichten angezeigt.

Lösung

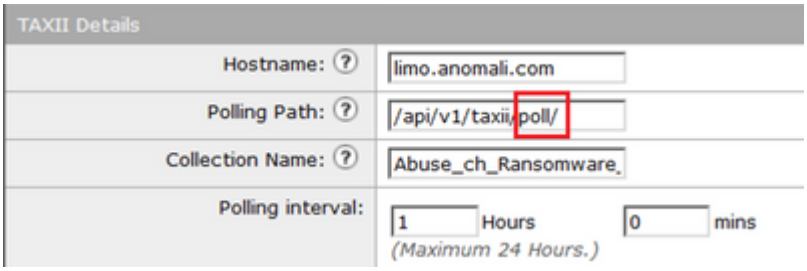
Der Fehler "400" gibt an, dass dieser Polling-Pfad vorhanden ist, verweist jedoch auf einen anderen Dienst, den der TAXII-Server anbietet.

1. Bestätigen Sie, dass die Polling Path-Konfiguration mit der Polling-Anforderung und nicht mit der Discovery-Anforderung konfiguriert ist.
2. Vergewissern Sie sich, dass HTTPS unter **GUI > Mail-Policys > External Threat Feeds Manager > HTTPS verwenden** aktiviert ist**.**

> **Achtung:** Normalerweise tritt dieses Problem auf, wenn der Polling-Pfad mit der Ermittlungsanforderung falsch konfiguriert ist, z. B.: /api/v1/taxii/taxii-discovery-service/
> Polling Path kann so konfiguriert werden, dass die Umfrageanforderung für die Feeds verwendet wird, z. B.: /api/v1/taxii/poll

---

> **Hinweis**: Unterschied zwischen Umfrage und Ermittlungsanfrage:
> - Die Polling-URL ist der Ort, von dem Sie die Feeds verwenden.
> - **Die** URL des Ermittlungsdienstes wird verwendet, um herauszufinden, welche Dienste der Taxidienst anbietet.



HTTP-Fehler: Statuscode 401 - Authentifizierungsfehler

```
(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
```

Lösung

Dieser Fehlercode weist darauf hin, dass keine gültigen Authentifizierungsinformationen für die Zielressource vorhanden sind.

Bestätigen Sie, dass die Anmeldeinformationen richtig konfiguriert sind.
Es gibt auch eine Option, keine Anmeldeinformationen für Benutzer zu konfigurieren.

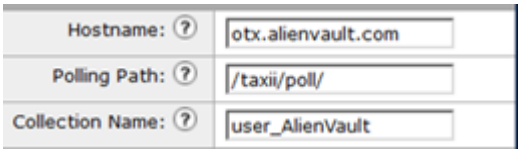
Taxifehler: HTTP-Fehler: Statuscode 404 Angeforderte Ressource nicht verfügbar

```
(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
```

> **Hinweis**: Der Statuscode 404 (Nicht gefunden) gibt an, dass der Ursprungsserver keine aktuelle Darstellung für die Zielressource gefunden hat oder nicht bereit ist, diese anzugeben. Dies zeigt, dass es eine ungültige URL geben kann und in den meisten Fällen, dass der Fehler aufgrund von Ressourcenpfad nicht gefunden wurde.

Lösung

Bestätigen Sie Polling Path/Collection Name auf der Quelle unter ESA **GUI> Mail Policies > External Threat Feeds Manager > Wählen Sie den richtigen Quellnamen aus**.



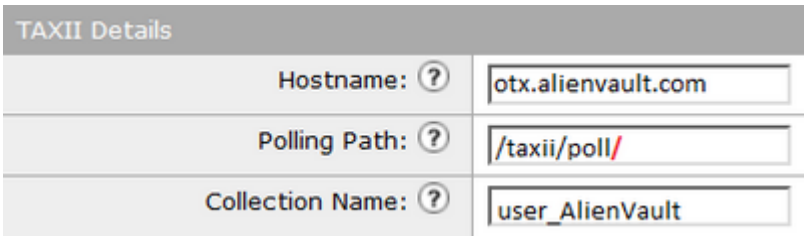
Fehlerursache: "405"

```
(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
```

> **Hinweis:** Laut RFC7231 gibt Fehler 405 (Methode nicht zulässig) an, dass die in der Anforderungszeile empfangene Methode vom Ursprungsserver bekannt ist, aber von der Zielressource nicht unterstützt wird.

Lösung

Dies ist ein Syntaxfehler aufgrund des fehlenden Schrägstrichs "/" am Ende des Polling-Pfads.
Trail Slash am Ende des Pfades /taxii/poll/ hinzufügen.



HTTP-Fehler: Statuscode 503 Dienst nicht verfügbar

```
(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
```

> **Hinweis**: Laut RFC 7231 ist error 503 "Service Unavailable" ein HTTP-Antwortstatuscode, der angibt, dass ein Server die Anforderung vorübergehend nicht verarbeiten kann.

Lösung

Der Fehlercode weist auf ein Problem mit dem Ziel-TAXII-Server hin, das weiter untersucht werden muss. Dies kann passieren, wenn der Server überlastet ist. Wenden Sie sich für weitere Informationen an den Anbieter.

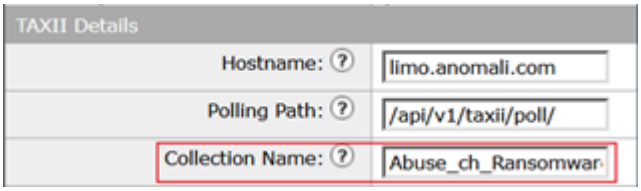
NOT_FOUND: Die angeforderte Sammlung konnte nicht gefunden werden.

```
(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
```

Lösung

Dieser Fehler weist darauf hin, dass der Name der Sammlung die richtige Schreibweise hat. Es liegt jedoch ein Problem auf dem TAXII-Server unter Sammlung vor, wodurch die Anforderung zurückgewiesen wird.

Mögliche Ursache könnte ein Ablaufzeitgeber für den Sammlungsnamen sein.
Wenden Sie sich an den Anbieter, um diese Art von Inkonsistenz zu prüfen.



[SSL: CERTIFICATE_VERIFY_FAILED] Überprüfung des Zertifikats fehlgeschlagen (_ssl.c:590)

<#root>

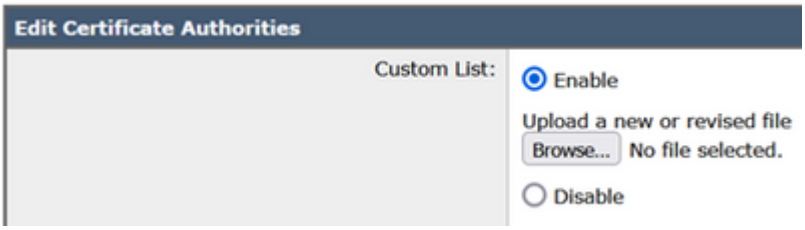
```
(Machine esa03.taclab.krk) (SERVICE)> grep "Sep 8 16:35" threatfeeds
Wed Sep 8 16:35:26 2021 Info: THREAT_FEEDS: A delta poll is scheduled for the source: ETF_Source_Name
Wed Sep 8 16:35:33 2019 Warning: THREAT_FEEDS: Unable to fetch the observables from the source: ETF_Sou
```

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

Lösung

Dieser Fehler weist auf einen Zertifikatfehler hin.

Importieren Sie das Zertifikat in die Liste der Zertifizierungsstellen, um das Problem zu beheben.
Navigieren Sie zu **GUI > Netzwerk > Zertifikate > Einstellungen bearbeiten > Benutzerdefinierte Liste >**
Wählen Sie den Modus **Aktivieren** aus, und laden Sie das Zertifikat hoch.



XML-Analysefehler: Kein Element gefunden (Zeile 0)

<#root>

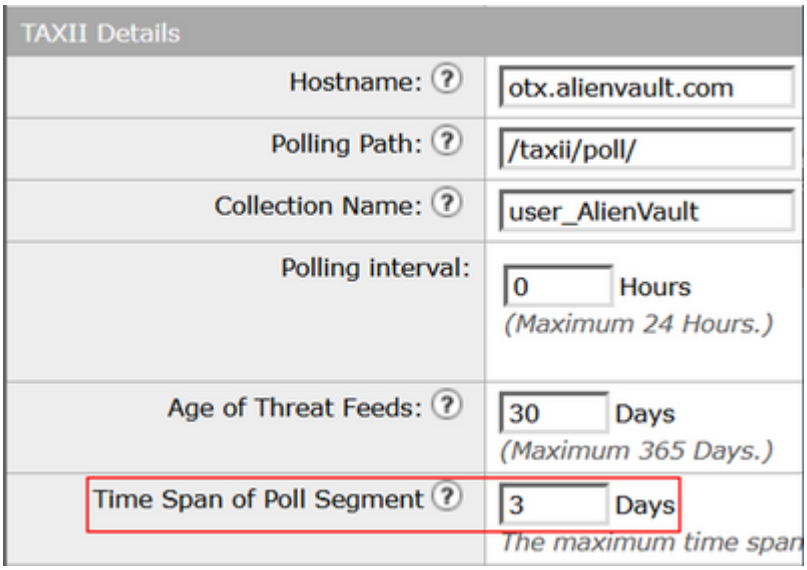
```
(Machine esa03.taclab.krk) (SERVICE)> grep "Aug 21 02:39" threatfeeds
Fri Aug 21 02:39:37 2021 Warning: THREAT_FEEDS: Unable to fetch the observables from the source: ETF_Sou
Fri Aug 21 02:39:37 2021 Info: THREAT_FEEDS: Job failed with exception : Source: ETF_Source_Name.
```

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

Lösung

Reduzieren Sie den Wert "Zeitspanne des Umfragesegments aus der ESA-Konfiguration" auf 3-4 Tage.

> **Hinweis**: Dies ist eine Inkonsistenz mit Anomali-Servern für einige spezifische Feeds, bei denen kein Ende der Daten-Flag gesendet wird, um die Feeds zu stoppen.
> In diesem Fall kann die ESA, die mit einer ETF-Quelle von Anomali konfiguriert ist, die Daten für einen Zeitraum von 5 Tagen nicht abfragen.
> Eine gültige Problemumgehung bestünde darin, den Wert "Time Span" (Zeitspanne) des Umfragesegments von der ESA-Konfiguration zu reduzieren.



Fehler beim Herstellen einer neuen Verbindung: [Fehler 111] Verbindung verweigert

<#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',))

> **Hinweis**: "Verbindung verweigert" zeigt an, dass der Client keine Verbindung mit dem Port des aktiven Servers herstellen kann. In der Regel geschieht dies, wenn der Server den falschen Port abhört oder der Port nicht verfügbar ist.

Lösung

1. Verwenden Sie den Befehl **telnet** oder **netstat** über die CLI, um zu überprüfen, ob der entsprechende Port abhört.
2. Vergewissern Sie sich, dass die Firewall den Port nicht blockiert.
3. Stellen Sie sicher, dass bei laufendem Service keine Port-Fehlkonfiguration/veralteter Port vorhanden ist.

Zugehörige Informationen

- Cisco Email Security Appliance - Benutzerhandbücher
- Was sind STIX und TAXII
- RFC2741 - Fehlercodes
- TAC-Workshop Feeds zu externen Bedrohungen

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.