外部の脅威フィードのトラブルシューティング失敗の主な原因

内容

はじめに

このドキュメントでは、外部の脅威フィードの実装、エラー分析、および解決のためのアクション中に失敗するいくつかの理由について説明します。

前提条件

特別な要件はありません。そのため、次の項目に関する知識があることが推奨されます。

- Cisco Secure Email Gateway(ESA)
- 外部脅威フィード(ETF)

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ソフトウェア12.x以降のバージョンが稼働するCisco Secure Email Gateway(ESA)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始していま

す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

失敗の理由：

ETFサービスが無効になっているか、サービスに有効な機能キーがありません

<#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: ‘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.

解決方法

次の内容を確認してください。

1. ETF機能キーが正しくインストールされている。
2. EULAが承認され、機能キーがグローバルに有効になりました。
3. マシンレベルでライセンスを適用。

注：クラスタレベルがある場合は、設定をマシンレベルにコピーする必要があります。

新しい接続を確立できませんでした： [Errno 110]接続がタイムアウトしました

```
(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 retri
Failed to establish a new connection: [Errno 110] Connection timed out',))
```

注：接続タイムアウトは通常、ESAが応答を取得できないネットワーク関連の問題を示します。より詳細な分析を行うために、ファイアウォール/プロキシチェックとパケットキャプチャが推奨されます。

解決方法

1. ファイアウォールとプロキシがトラフィックをブロックしないことを確認します。
   プロキシは、GUI > Security Services > Service Updatesで確認できます。
2. パケットキャプチャで接続を確認します。GUI > Help and Support > Packet Captureの順に

移動します。

ヒント：ネットワーク関連の問題の兆候がある場合は、接続が正しく確立されていることを確認するためにパケットキャプチャを実行することが賢明です。

失敗の理由：「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
```

注:RFC7231 Error 400(Bad Request)は、クライアントエラーと見なされることによってサーバが要求を処理できない、または要求を処理しないことを示します。 ほとんどの場合、これは不正な要求シンタックスまたは無効な要求メッセージのフレーミングが原因で表示されます。

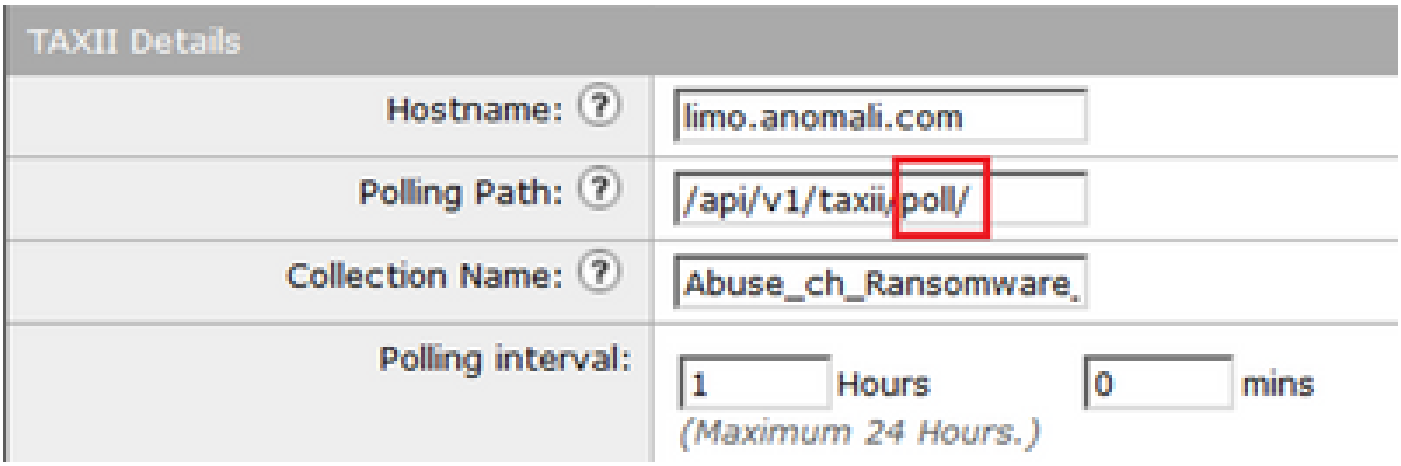
解決方法

エラー「400」は、このポーリングパスは存在するが、TAXIIサーバが提供する別のサービスを指していることを示しています。

1. ポーリングパスの設定が、ディスカバリ要求ではなくポーリング要求で設定されていることを確認します。
2. GUI > Mail Policies > External Threat Feeds Manager > Use HTTPSでHTTPSが有効になっていることを確認します。

注意：通常、この問題は、ポーリングパスが/api/v1/taxii/taxii-discovery-service/などの検出要求で誤って設定されている場合に発生します。
ポーリングパスは、フィードにポーリング要求を使用するように構成できます（例：/api/v1/taxii/poll）。

注：ポーリング要求と検出要求の違い：
- ポーリングURLは、実際にフィードを使用する場所です。
- ディスカバリサービスURLを使用して、Taxiiサービスが提供するサービスを検索します。



HTTPエラー：ステータスコード401認証エラー

```
(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
```

解決方法

このエラーコードは、ターゲットリソースの有効な認証資格情報がないことを示します。

クレデンシャルが正しく設定されていることを確認します。
ユーザのクレデンシャルを設定しないオプションもあります。

Taxiiエラー： HTTPエラー：状態コード404要求されたリソースは利用できません

```
(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 a
Fri Aug 27 08:51:16 2021 Info: THREAT_FEEDS: Job failed with exception : Source: Test. Reason for failu
```

注：ステータスコード404(Not Found)は、オリジンサーバーがターゲットリソースの現在の表現を見つけられなかったこと、または存在することを公開しないことを示します。これは、無効なURLが存在する可能性があり、ほとんどの場合、リソースパスが原因で発生したことが見つからないことを示します。

解決方法

ESA GUI > Mail Policies > External Threat Feeds Manager > Choose the Proper Source Nameで、ソースのポーリングパス/コレクション名を確認します。

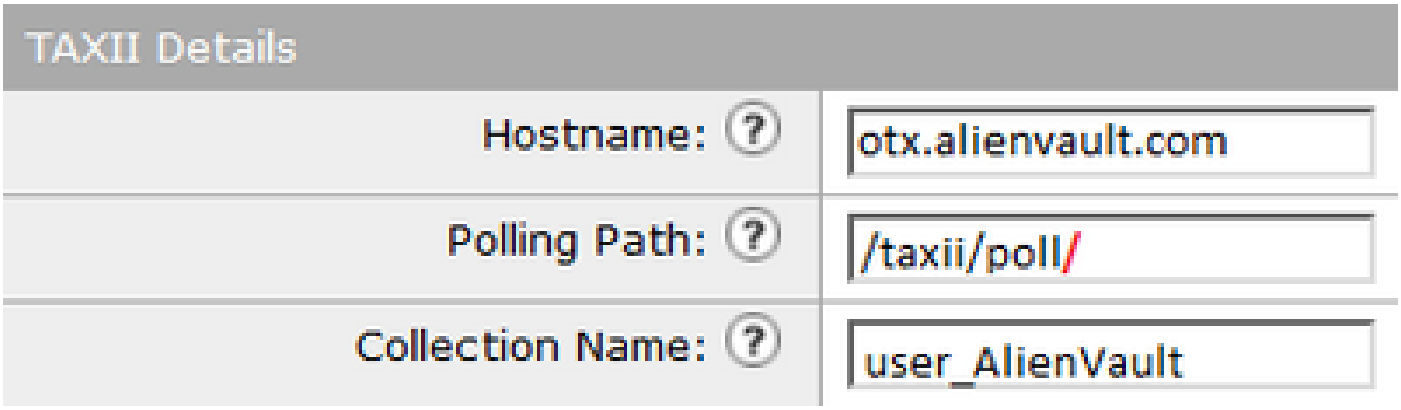
失敗の理由：「405」

```
(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. Rea
```

注:RFC7231によると、エラー405 (メソッドが許可されていません) は、要求行で受信したメソッドが元のサーバに認識されていても、ターゲットリソースでサポートされていないことを示しています。

解決方法

これは、ポーリングパスの最後にトレール「/」スラッシュがないために発生する構文エラーです。
パス/taxii/poll/の最後にトレイルスラッシュを追加します。



HTTPエラー：ステータスコード503 Service Unavailable

```
(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. Reaso
Sun Nov 10 13:45:22 2020 Info: THREAT_FEEDS: A delta poll is scheduled for the source: ETF_Source_Name
```

注:RFC7231によると、エラー503「Service Unavailable」はHTTP応答のステータスコードで、サーバが一時的に要求を処理できないことを示します。

解決方法

エラーコードは、宛先TAXIIサーバの問題を示しています。この問題をさらに調査する必要があります。
これは、サーバが過負荷のときに発生する可能性があります。詳細については、ベンダーにお問い合わせください。

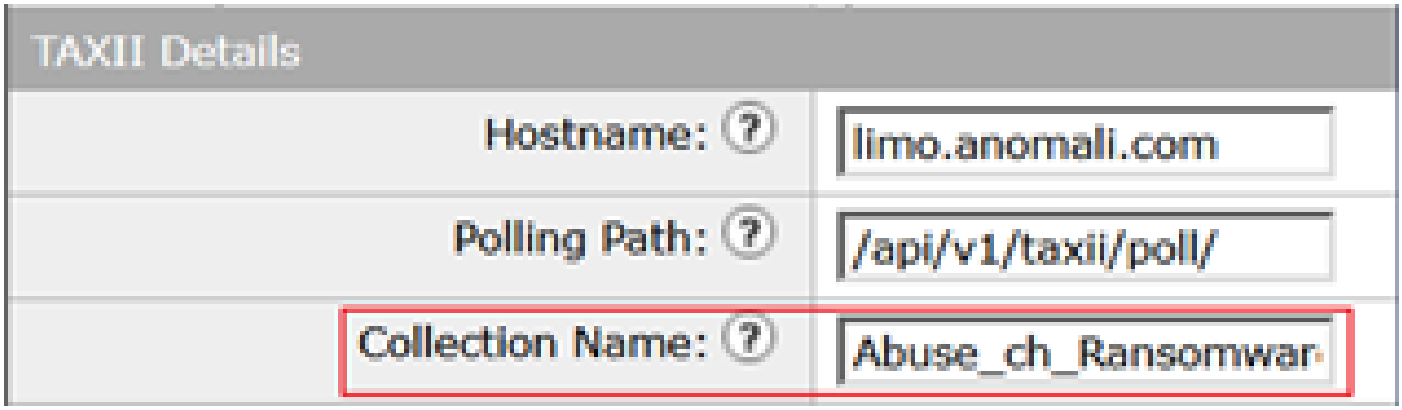
NOT_FOUND：要求されたコレクションが見つかりませんでした

```
(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_Po
Tue Sep 7 12:53:16 2021 Debug: THREAT_FEEDS: Updating the timestamp: 2021-09-07 12:49:12.648625 for the
```

解決方法

このエラーは、コレクション名のスペルが正しいことを示していますが、コレクションのTAXIIサーバに要求を拒否する問題があります。

コレクション名の有効期限タイマーが原因である可能性があります。
この種の不整合を確認するには、ベンダーにお問い合わせください。



[SSL: CERTIFICATE_VERIFY_FAILED]証明書の検証に失敗しました(_ssl.c:590)

<#root>

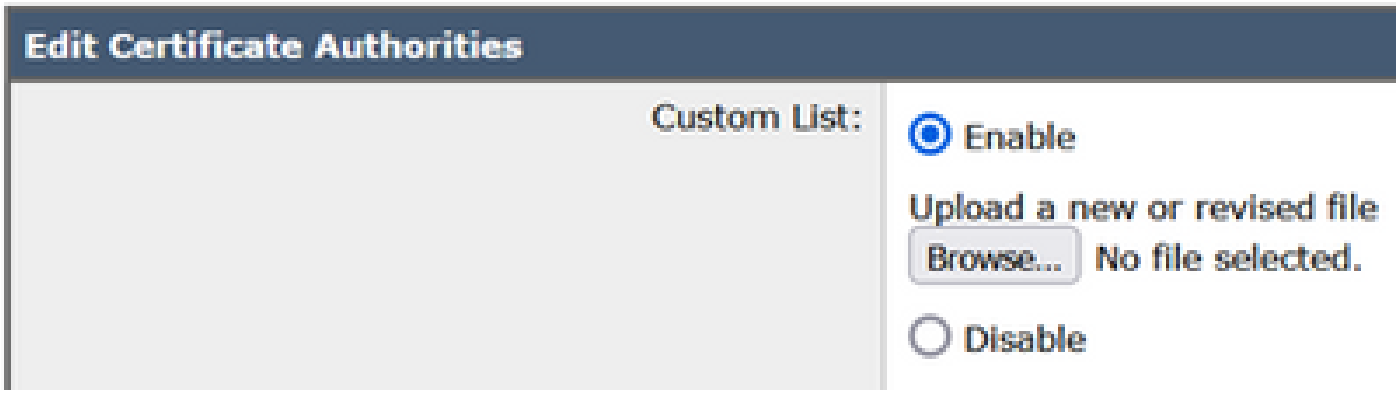
```
(Machine esa03.taclab.krk) (SERVICE)> grep "Sep 8 16:35" threatfeeds
Wed Sep 8 16:35:26 2021 Info: THREAT_FEEDS: A delta poll is scheduled for the source: ETF_Source_Name
Wed Sep 8 16:35:33 2019 Warning: THREAT_FEEDS: Unable to fetch the observables from the source: ETF_Sou
```

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

解決方法

このエラーは、証明書の障害を示します。

この問題を解決するには、認証局(CA)リストの証明書をインポートします。
GUI > Network > Certificates > Edit Settings > Custom Listの順に移動します。
Enableモードを選択し、証明書をアップロードします。



XML解析エラー：要素が見つかりません（行0）

<#root>

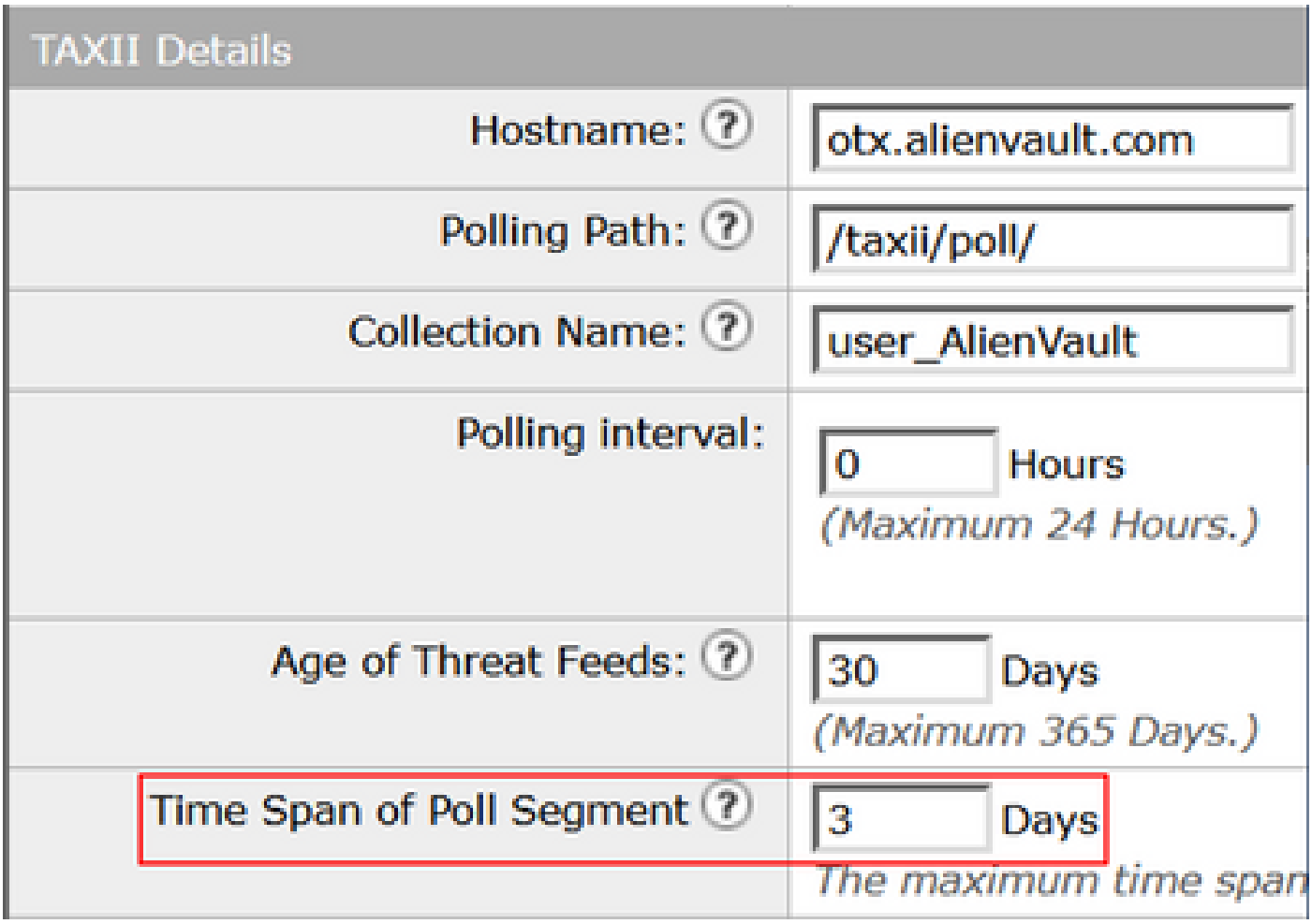
```
(Machine esa03.taclab.krk) (SERVICE)> grep "Aug 21 02:39" threatfeeds
Fri Aug 21 02:39:37 2021 Warning: THREAT_FEEDS: Unable to fetch the observables from the source: ETF_So
Fri Aug 21 02:39:37 2021 Info: THREAT_FEEDS: Job failed with exception : Source: ETF_Source_Name.

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

解決方法

ESA設定のTime Span of Poll Segment値を3 ~ 4日に減らします。

注：これは、特定のフィードに対するAnomaliサーバとの不整合であり、フィードを停止するためのEnd of Dataフラグが送信されません。
この場合、AnomaliからのETFソースを使用して設定されたESAは、5日間にわたってデータをポーリングできません。
有効な回避策は、ESA設定のTime Span of Poll Segmentの値を減らすことです。



新しい接続を確立できませんでした： [Errno 111]接続が拒否されました

<#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',))
```

注:「Connection refused」は、クライアントが実行中のサーバのポートに接続できないことを示します。通常、これは、サーバが誤ったポートで受信する場合や、ポートが使用できない場合に発生します。

解決方法

1. CLIからtelnetまたはnetstatコマンドを使用して、適切なポートがリッスンしていることを確認します。
2. ファイアウォールがポートをブロックしていないことを確認します。
3. 実行中のサービスにPort Misconfiguration/Stale portがないことを確認します。

関連情報

- Cisco E メール セキュリティ アプライアンス エンド ユーザ ガイド
- STIXとTAXIIとは
- RFC2741 – エラーコード
- TACワークショップ外部脅威フィード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。