Troubleshoot External Threat Feeds Top Reasons for Failure

Contents

Introduction

This document describes several reasons for failure during External Threat Feed implementation, error analysis and actions for resolution.

Prerequisites

There are no specific requirements, hence Cisco recommends that you have knowledge of these topics:

- Cisco Secure Email Gateway (ESA)
- External Threat Feeds (ETF)

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Secure Email Gateway (ESA) running software 12.x or later version

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. If your network is live, ensure that you understand the potential impact of any command.

Reason For Failures:

The ETF Service is Either Disabled or There is no Valid Feature Key for 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

Ensure that:

1. ETF Feature key installed properly.
2. EULA accepted and Feature key enabled globally.
3. Applied licenses on machine level.

Note: If there is a cluster-level, then it needs to copy the setting into machine level.

Failed to Establish a New Connection: [Errno 110] Connection Timed Out

```
(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',))
```

Note: Connection timed out typically indicates a network related issue, which prevents ESA to get a response. Firewall/ Proxy checks are recommended and packet capture for deeper analysis.

Solution

1. Confirm Firewall and Proxy do not block the traffic.
   Proxy can be checked under **GUI > Security Services > Service Updates.**
2. Confirm connectivity with Packet Capture. Navigate to **GUI > Help and Support > Packet Capture.**

Tip: When there are indications of network relates issues, it is prudent to run packet captures in order to confirm that connection has been established properly.

Reason for Failure: "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
```

Note: RFC7231 Error 400 (Bad Request), indicates that server cannot or does not process the request due to something that is perceived to be a client error. Most of the times it appears due to malformed request syntax, or invalid request message framing.

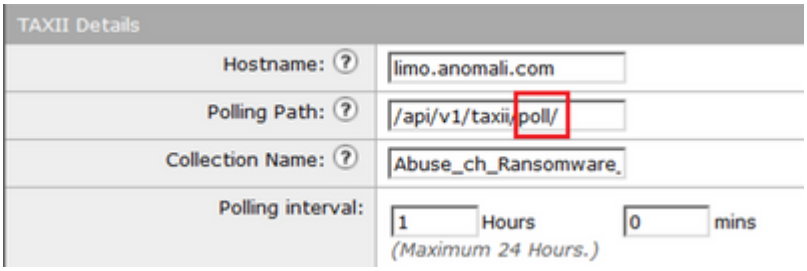
Solution

Error "400â€ indicates that this Polling Path exists, but it points to a different service that TAXII server offers.

1. Confirm Polling Path Configuration is configured with Poll request and not Discovery request.
2. Confirm HTTPS is enabled under **GUI > Mail Policies > External Threat Feeds Manager > Use HTTPS.**

Caution: Typically this issue occurs when Polling Path is misconfigured with discover request, such as: /api/v1/taxii/taxii-discovery-service/
Polling Path can be configured to use Poll request for the feeds, for instance: /api/v1/taxii/poll

Note: Difference between Poll and Discovery request:
- Polling URL is actually where you consume the feeds from.
- Discovery Service URL is used to find what services the Taxii service offers.



HTTP Error: Status Code 401 Authentication Failure

```
(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

This error code indicates that it lacks valid authentication credentials for the target resource.

Confirm that Credentials are configured properly.
There is an option also not to configure credentials for users.

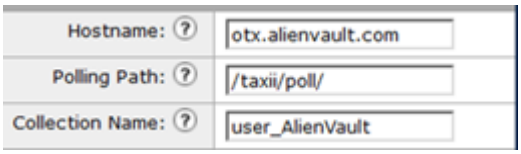
Taxii Error: HTTP Error: Status Code 404 Requested Resource not Available

```
(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 failu
```

Note: The 404 (Not Found) status code indicates that the origin server did not find a current representation for the target resource, or is not willing to disclose that one exists. This reveals that there can be an Invalid URL and in majority of the cases, that the occurred due to resource path is not found.

Solution

Confirm Polling Path/Collection Name on the Source under ESA **GUI> Mail Policies > External Threat Feeds Manager > Choose the proper Source Name**.



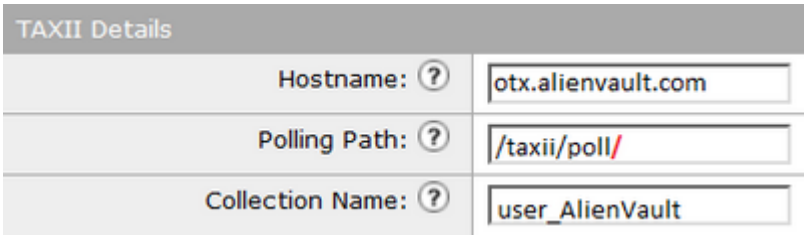
Reason for Failure: "405"

```
(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
```

Note: Per RFC7231, Error 405 (Method Not Allowed) indicates that the method received in the request-line is known by the origin server, but not supported by the target resource.

Solution

This is a Syntax Error due to the missing Trail â€œ/â€ Slash at the end of the Polling Path.
Add trail Slash at the end of the path /taxii/poll/.



HTTP Error: Status Code 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. Reason
Sun Nov 10 13:45:22 2020 Info: THREAT_FEEDS: A delta poll is scheduled for the source: ETF_Source_Name
```

Note: Per RFC7231, error 503 "Service Unavailableâ€ is an HTTP response status code and indicates that a server is temporarily unable to handle the request.

Solution

Error code indicates an issue with destination TAXII server, which needs to be investigated further.
This could happen when server is overloaded. Contact Vendor for further information.

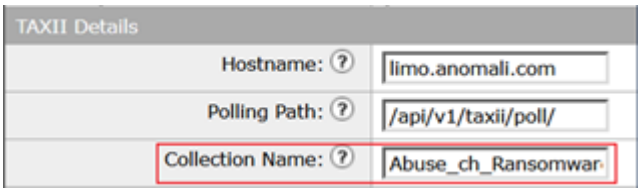
NOT_FOUND: The Requested Collection Could not be Found

```
(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

This error indicates that Collection name has the correct spelling, however, there is an issue on TAXII server under Collection, which rejects the request.

Possible cause could be an expiration timer on Collection Name.
Contact Vendor to check for this kind of inconsistency.



[SSL: CERTIFICATE_VERIFY_FAILED] Certificate Verify Failed (_ssl.c:590)

<#root>

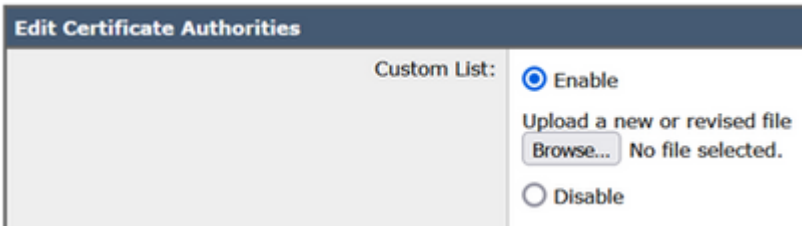
```
(Machine esa03.taclab.krk) (SERVICE)> grep "Sep 8 16:35" threatfeeds
Wed Sep 8 16:35:26 2021 Info: THREAT_FEEDS: A delta poll is scheduled for the source: ETF_Source_Name
Wed Sep 8 16:35:33 2019 Warning: THREAT_FEEDS: Unable to fetch the observables from the source: ETF_Sou
```

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

Solution

This error indicates Certificate failure.

To resolve the issue, import the Certificate in Certificate Authority (CA) list.
Navigate to **GUI > Network > Certificates > Edit Settings > Custom List >**
Choose **Enable** mode and upload the Certificate.



XML Parising Error: No Element Found (line 0)

<#root>

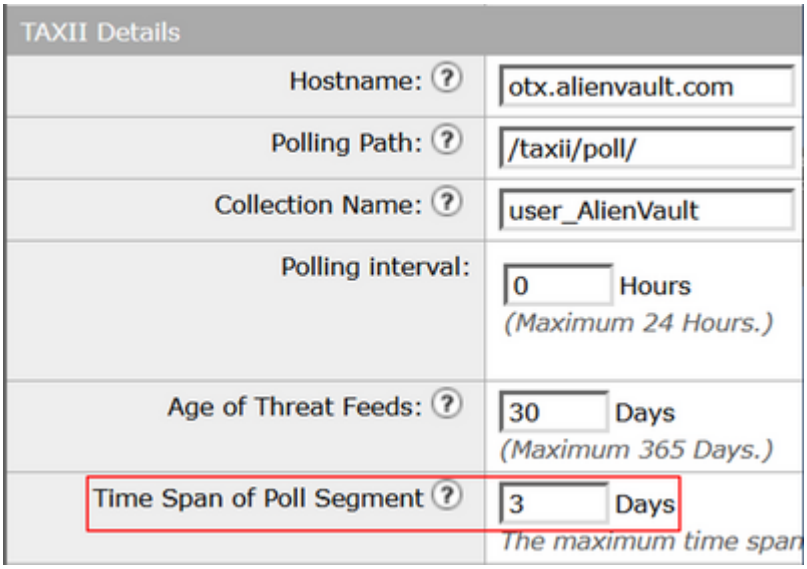
```
(Machine esa03.taclab.krk) (SERVICE)> grep "Aug 21 02:39" threatfeeds
Fri Aug 21 02:39:37 2021 Warning: THREAT_FEEDS: Unable to fetch the observables from the source: ETF_Sou
Fri Aug 21 02:39:37 2021 Info: THREAT_FEEDS: Job failed with exception : Source: ETF_Source_Name.
```

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

Solution

Reduce the value Time Span of Poll Segment from ESA configuration to 3-4 days.

> **Note**: This is an inconsistency with Anomali servers for some specific feeds, where no end of data flag is sent to stop the feeds.
> In this case, ESA that is configured with an ETF source from Anomali, is not able to poll data for a time span over 5 days.
> A valid workaround would be to reduce the value Time Span of Poll Segment from ESA configuration.



Failed to Establish a New Connection: [Errno 111] Connection Refused

<#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',))
```

> **Note**: "Connection refused" indicates that client cannot connect to the port on the running Server. Typically, this occurs when the server listens in on the wrong port, or port is unavailable.

Solution

1. Use **telnet** or **netstat** command via CLI to verify the appropriate port is listening.
2. Verify that Firewall does not block the port.
3. Ensure there is no Port Misconfiguration/ Stale port on running service.

Related Information

- Cisco Email Security Appliance End User Guides
- What are STIX and TAXII
- RFC2741 - Error Codes
- TAC Workshop External Threat Feeds