排除外部威胁源的故障主要原因

目录

简介

本文档介绍外部威胁源实施过程中发生故障的几种原因、错误分析和解决操作。

先决条件

没有特定要求，因此Cisco建议您了解以下主题：

- 思科安全邮件网关(ESA)
- 外部威胁源(ETF)

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行软件12.x或更高版本的思科安全邮件网关(ESA)

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

失败原因：

ETF服务已禁用或没有有效的服务功能密钥

<#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.
```

解决方案

请确保：

1. ETF功能密钥已正确安装。
2. EULA已接受，功能密钥已全局启用。
3. 已在计算机级别应用许可证。

注：如果存在集群级别，则需要将设置复制到计算机级别。

无法建立新连接：[错误110]连接超时

```
(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',))
```

注意：连接超时通常表示与网络相关的问题，这会阻止ESA获得响应。建议进行防火墙/代理检查并捕获数据包，以便进行更深入的分析。

解决方案

1. 确认防火墙和代理不阻止流量。
   可以在GUI > Security Services > Service Updates下检查代理。
2. 通过数据包捕获确认连接。导航到GUI > Help and Support > Packet Capture。

提示：当出现网络相关问题的迹象时，谨慎的做法是运行数据包捕获，以确认连接已正确建立。

失败原因：“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_Pat
Mon Sep 6 13:38:55 2021 Info: THREAT_FEEDS: The source 'Test_Poll_Path' is currently in a polling state
```

注意:RFC7231 Error 400（错误请求），表示服务器无法或不处理该请求，因为某些事件被视为客户端错误。 大多数情况下，出现该错误的原因在于请求语法格式不正确或请求消息帧无效。

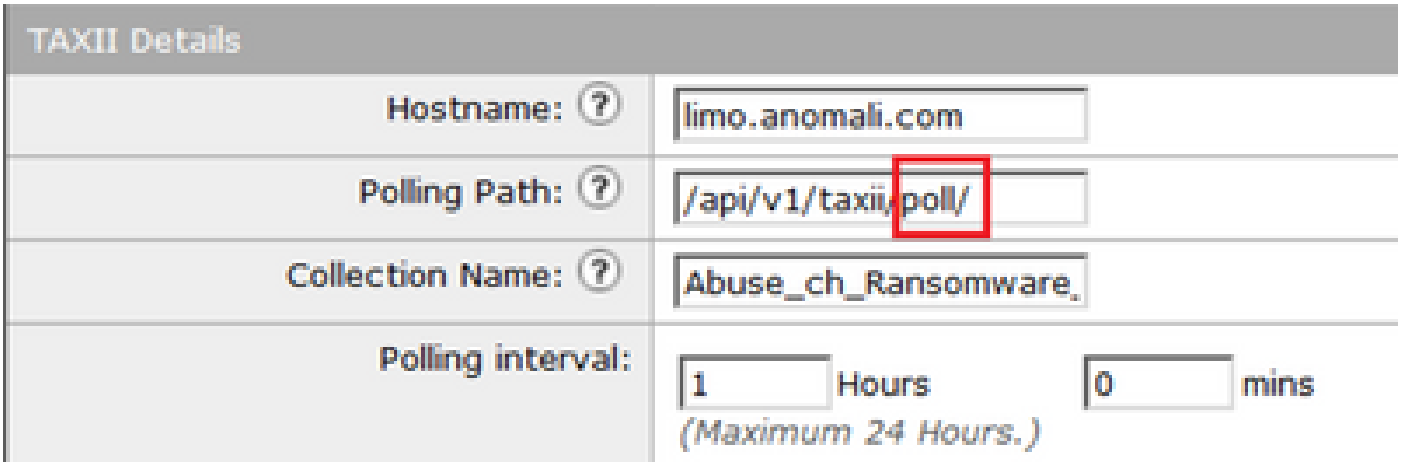
解决方案

错误“400”表示存在此轮询路径，但它指向TAXII服务器提供的其他服务。

1. 确认使用轮询请求而不是发现请求配置了轮询路径配置。
2. 在GUI > Mail Policies > External Threat Feeds Manager > Use HTTPS下启用确认HTTPS。

注意：通常，当轮询路径配置有发现请求时（例如：/api/v1/taxii/taxii-discovery-service/）会发生此问题
轮询路径可以配置为对源使用轮询请求，例如：/api/v1/taxii/poll

注意：轮询和发现请求之间的差异：
-轮询URL实际上就是您使用源的位置。
-发现服务URL用于查找Taxii服务提供的服务。



HTTP错误：状态代码401身份验证失败

```
(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
```

解决方案

此错误代码表明它缺少目标资源的有效身份验证凭据。

确认凭证配置正确。
还有一个选项不为用户配置凭证。

Taxii错误： HTTP错误：状态代码404请求的资源不可用

```
(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:404（未找到）状态代码表示源服务器没有找到目标资源的当前表示形式，或者不愿意透露该表示形式存在。这表明，可能存在无效的URL，在大多数情况下，找不到由于资源路径而发生的情况。

解决方案

在ESA GUI > Mail Policies > External Threat Feeds Manager > Choose the proper Source Name下，确认源上的轮询路径/收集名称。

失败原因：“405”

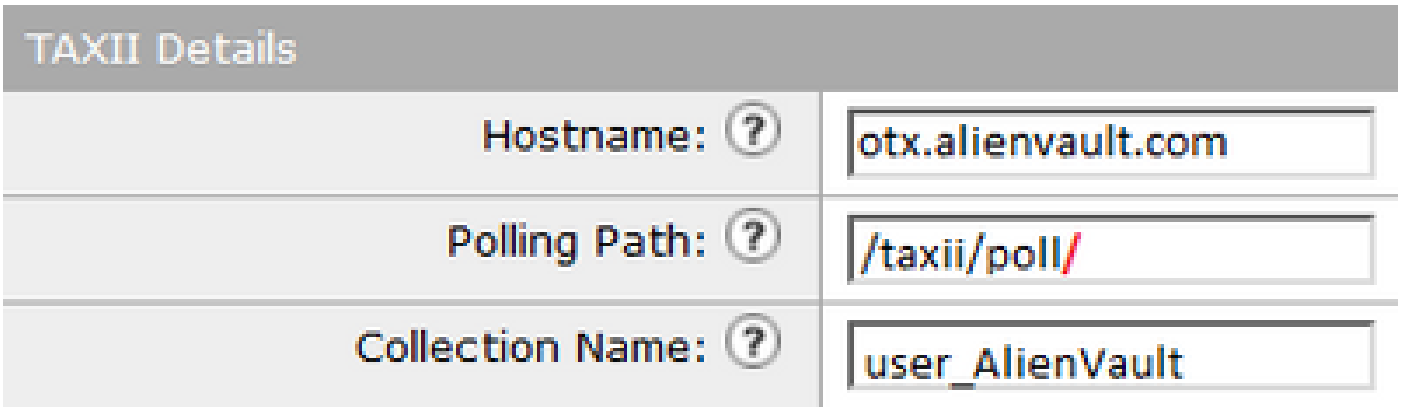
```
(Machine esa03.taclab.krk) (SERVICE)> grep "Sep 13 00:2" threatfeeds
Mon Sep 13 00:20:21 2021 Debug: THREAT_FEEDS: Failed to fetch observables from the source: Anomali. Rea
```

注：根据RFC7231，错误405(Method Not Allowed)表示在请求行中接收的方法是源服务器已知的，但目标资源不支持该方法。

解决方案

由于轮询路径末尾缺少跟踪线“/”斜线，这是一个语法错误。

在路径/taxii/poll/的末尾添加轨迹斜线。



HTTP错误：状态代码503服务不可用

```
(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：根据RFC7231，错误503“Service Unavailable”是HTTP响应状态代码，表示服务器暂时无法处理请求。

解决方案

错误代码表明目标TAXII服务器出现问题，需要进一步调查。
当服务器过载时可能会发生这种情况。请联系供应商以了解更多信息。

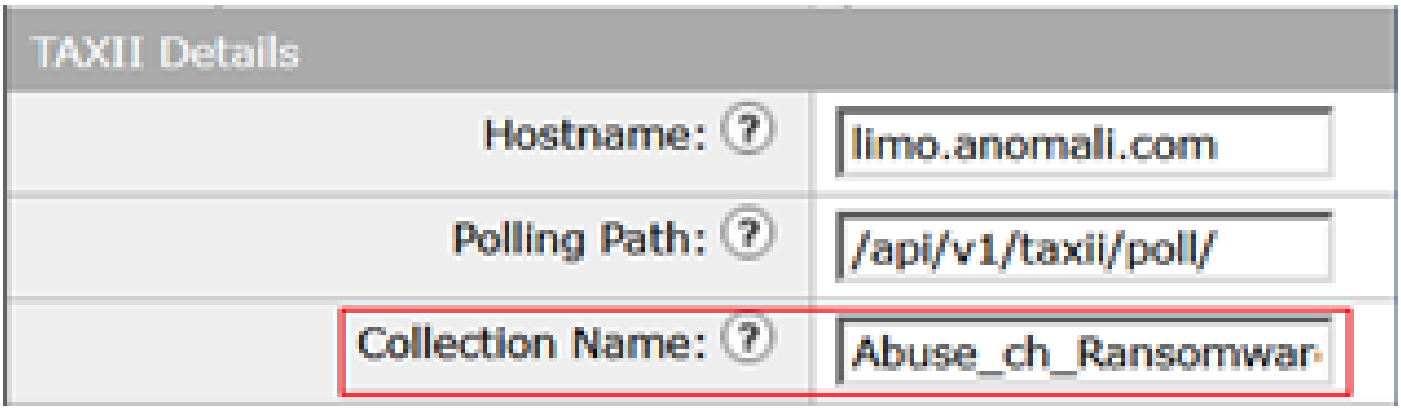
NOT_FOUND：找不到请求的集合

```
(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
```

解决方案

此错误表示集合名称拼写正确，但TAXII服务器在集合下存在问题，拒绝该请求。

可能的原因是收集名称上的过期计时器。
请与供应商联系以检查此类不一致情况。



[SSL: CERTIFICATE_VERIFY_FAILED]证书验证失败(_ssl.c:590)

<#root>

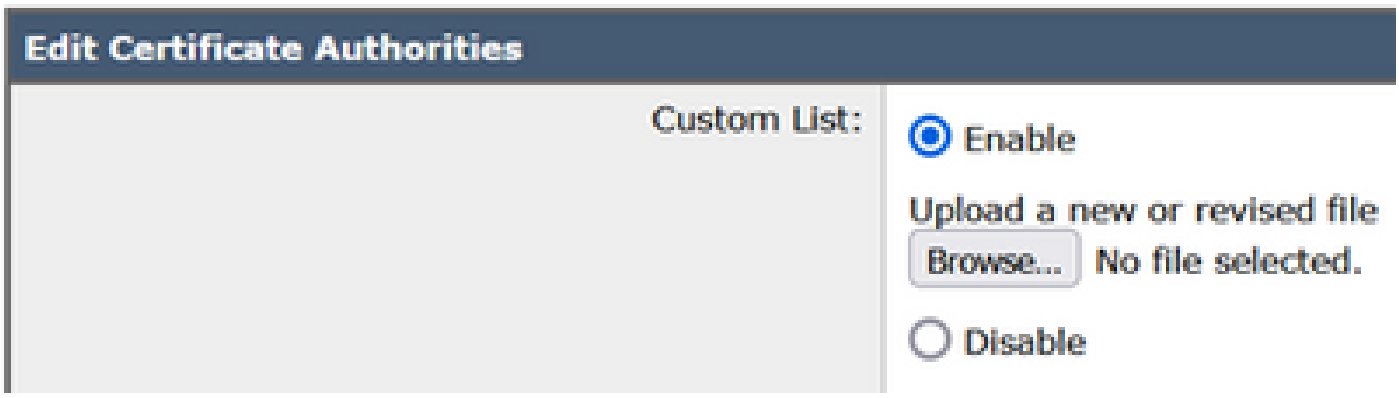
```
(Machine esa03.taclab.krk) (SERVICE)> grep "Sep 8 16:35" threatfeeds
Wed Sep 8 16:35:26 2021 Info: THREAT_FEEDS: A delta poll is scheduled for the source: ETF_Source_Name
Wed Sep 8 16:35:33 2019 Warning: THREAT_FEEDS: Unable to fetch the observables from the source: ETF_Sou
```

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

解决方案

此错误表示证书失败。

要解决此问题，请导入证书颁发机构(CA)列表中的证书。
导航到GUI > Network > Certificates > Edit Settings > Custom List >
选择Enable模式并上传证书。



XML解析错误：未找到元素（第0行）

<#root>

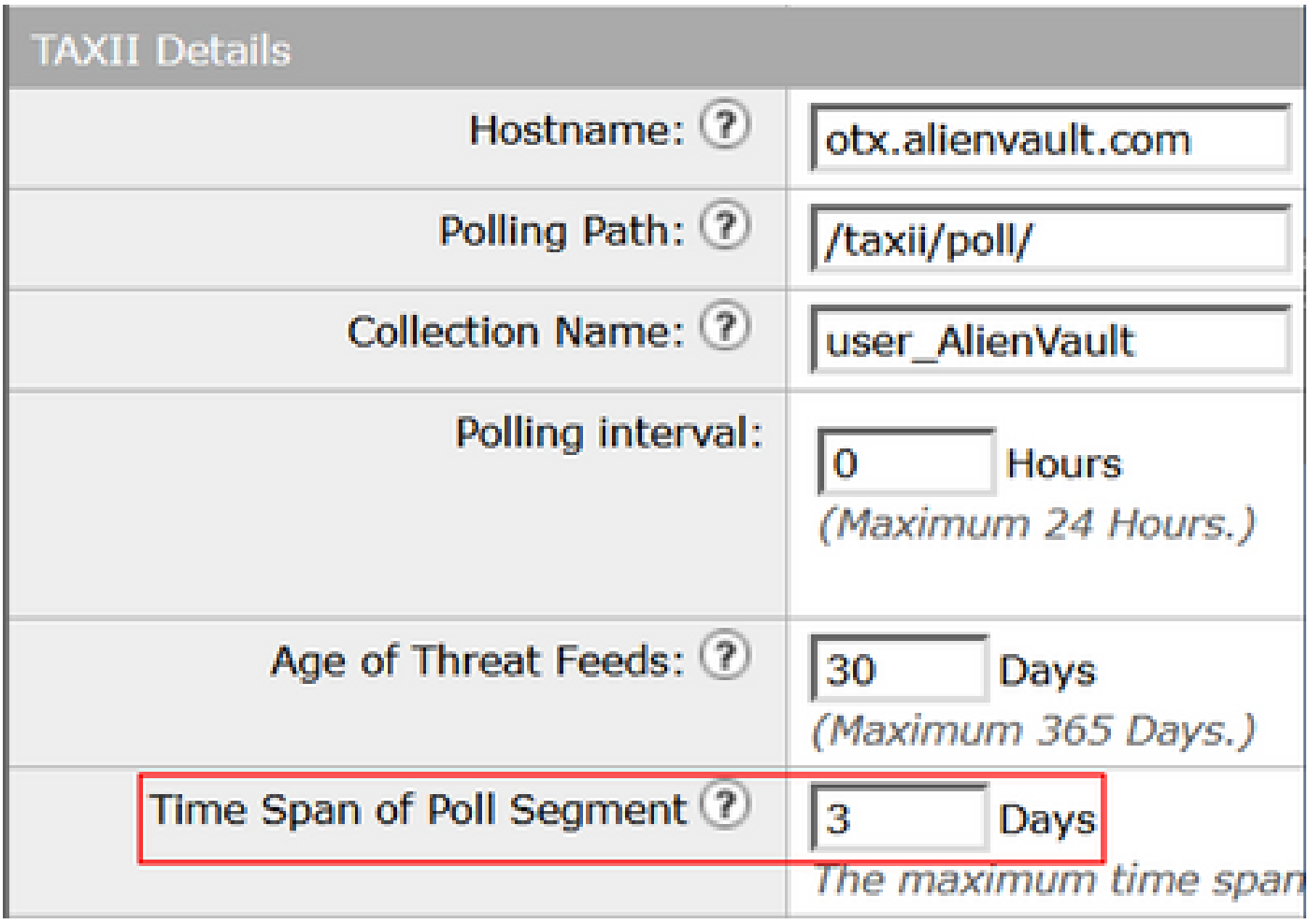
```
(Machine esa03.taclab.krk) (SERVICE)> grep "Aug 21 02:39" threatfeeds
Fri Aug 21 02:39:37 2021 Warning: THREAT_FEEDS: Unable to fetch the observables from the source: ETF_So
Fri Aug 21 02:39:37 2021 Info: THREAT_FEEDS: Job failed with exception : Source: ETF_Source_Name.
```

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

解决方案

将ESA配置的轮询段时间跨度值减少到3-4天。

注意：对于某些特定源，这与Anomali服务器不一致，在这些源中不会发送数据结束标记来停止源。
在这种情况下，配置了Anomali的ETF源的ESA无法轮询超过5天时间跨度的数据。
有效的解决方法是减少ESA配置中的轮询段的时间跨度(Time Span)。



无法建立新连接：[错误11]连接被拒绝

<#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',))
```

注意：“连接被拒绝”表示客户端无法连接到正在运行的服务器上的端口。通常，当服务器在错误的端口上侦听或端口不可用时会出现这种情况。

解决方案

1. 通过CLI使用telnet或netstat命令验证适当的端口是否处于侦听状态。
2. 验证防火墙是否未阻止端口。
3. 确保运行的服务没有端口配置错误/端口陈旧。

相关信息

- 思科邮件安全设备最终用户指南
- 什么是STIX和TAXII
- RFC2741 — 错误代码
- TAC研讨会外部威胁源

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。