أستكشاف أخطاء موجز ويب للتهديدات الخارجية وإصلاحها أهم أسباب الفشل

المحتويات

المقدمة

المتطلبات الأساسية

المكونات المستخدمة

سبب الفشل:

مهلة الاتصال الجديد: انتهت مهلة الاتصال [Errno110] فشل الاتصال

سبب الفشل: "400"

خطأ HTTP: فشل مصادقة رمز الحالة 401

خطأ HTTP: المورد المطلوب لرمز الحالة 404 غير موجود :خطأ في بناء الجملة

سبب الفشل: "405"

خطأ HTTP: خدمة رمز الحالة 503 غير متوفرة

NOT_FOUND: تعذر العثور على المجموعة المطلوبة

[SSL: CERTIFICATE_VERIFY_FAILED] فشل التحقق من الشهادة (ssl.c:590)

خطأ في تحليل XML: لم يتم العثور على عنصر (السطر 0)

فشل الاتصال الجديد: تم رفض الاتصال [Errno111]

معلومات ذات صلة

المقدمة

يوضح هذا المستند العديد من أسباب الفشل أثناء تنفيذ موجز ويب التهديد الخارجي وتحليل الأخطاء والإجراءات الخاصة بالحل.

المتطلبات الأساسية

هناك ما من متطلب خاص، لذلك Cisco يوصي أن يتلقى أنت معرفة من هذا موضوع:

- عبارة البريد الإلكتروني الآمنة (ESA) من Cisco
- موجز ويب التهديد الخارجي (ETF)

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- عبارة البريد الإلكتروني الآمنة (ESA) من Cisco التي تشغل البرنامج 12.x أو الإصدار الأحدث

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة.

بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

سبب الفشل:

إما أن خدمة ETF معطلة أو ال يوجد مفتاح ميزة صالح للخدمة

<#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.
```

الحل

تأكد من:

1. تم تثبيت مفتاح ميزة ETF بشكل صحيح.
2. تم قبول EULA وتم تمكين مفتاح الميزة بشكل عام.
3. التاريخ المطبق على مستوى الجهاز.

ملاحظة: إذا كان هناك مستوى نظام مجموعة، فإنه يحتاج إلى نسخ الإعداد إلى مستوى جهاز.

فشل إنشاء اتصال جديد: انتهت مهلة الاتصال [Errno 110]

```
(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',))
```

ملاحظة: يشير انتهاء مهلة الاتصال عادة إلى مشكلة تتعلق بالشبكة، تمنع ESA من الحصول على إستجابة. يوصى بالقيام بعمليات التحقق من جدار الحماية/الوكيل والتقاط الحزم لمزيد من التحليل.

الحل

1. تأكيد جدار الحماية والوكيل ال يحجبان حركة المرور.
   يمكن التحقق من الوكيل تحت واجهة المستخدم الرسومية (GUI) > خدمات الأمان >

تحديثات الخدمة.
2. تأكيد الاتصال باستخدام التقاط الحزمة. انتقل إلى واجهة المستخدم الرسومية (GUI) > المساعدة والدعم > التقاط الحزمة.

تلميح: عندما تكون هناك مؤشرات على وجود مشاكل تتعلق بالشبكة، فمن الحكمة تشغيل التقاط الحزم لتأكيد إنشاء الاتصال بشكل صحيح.

سبب الفشل: "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
```

ملاحظة: يشير خطأ RFC7231 رقم 400 (طلب غير صحيح) إلى أن الخادم لا يمكنه معالجة الطلب أو أن لا يقوم بذلك بسبب خطأ في العميل. في معظم الأوقات التي يظهر فيها بسبب بناء جملة طلب غير صحيح، أو إعداد رسالة طلب غير صحيح.

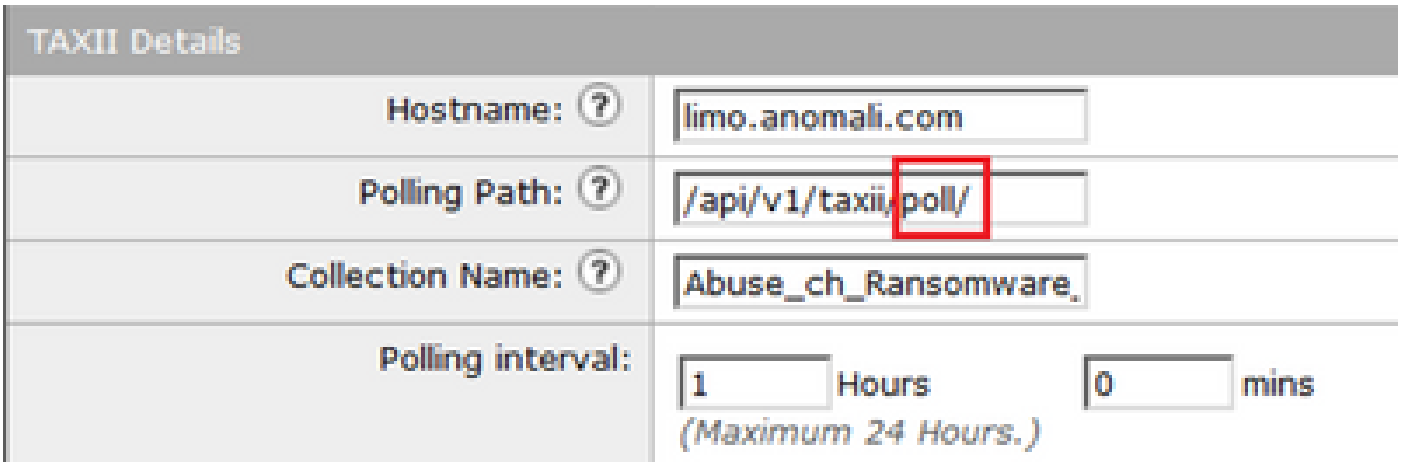
الحل

يشير الخطأ "400" إلى وجود مسار الاستقصاء هذا، ولكنه يشير إلى خدمة مختلفة يقدمها خادم TAXII.

1. تأكيد تكوين مسار التحقق يتم تكوينه بطلب الاستطلاع وليس طلب الاكتشاف.
2. تأكد من تمكين HTTPS تحت واجهة المستخدم الرسومية (GUI) > سياسات البريد > مدير موزع ويب التحديدات الخارجية > إستخدام HTTPS.

تحذير: عادة ما تحدث هذه المشكلة عندما يكون مسار القارعة مكونا بشكل غير صحيح مع طلب الاكتشاف، مثل: /api/v1/taxii/taxii-discovery-service/
يمكن تكوين مسار الاستقصاء لاستخدام طلب الاستقصاء لموزع ويب، على سبيل المثال: /api/v1/taxii/poll

ملاحظة: الفرق بين الاستطلاع وطلب الاكتشاف:
- عنوان URL الخاص بالقارعة وهو المكان الذي تستهلك منه موزع الويب.
- يتم إستخدام عنوان URL لخدمة Discovery للعثور على الخدمات التي تقدمها خدمة Taxii.



خطأ HTTP: فشل مصادقة رمز الحالة 401

```
(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
```

الحل

يشير رمز الخطأ هذا إلى أنه يفتقر إلى بيانات اعتماد مصادقة صالحة للمورد الهدف.

تأكد من تكوين بيانات الاعتماد بشكل صحيح.
هناك خيار أيضا ألا يتم تكوين بيانات الاعتماد للمستخدمين.

خطأ تاكسي: خطأ HTTP: المورد المطلوب لرمز الحالة 404 غير متوفر

```
(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
```

ملاحظة: يشير رمز حالة 404 (غير موجود) إلى أن الخادم الأصلي لم يعثر على تمثيل حالي للمورد الهدف، أو أنه غير مستعد للإفصاح عن وجود تمثيل. هذا يكشف أنه يمكن أن يكون هناك URL غير صالح وفي معظم الحالات، لم يتم العثور على مسار المورد.

الحل

تأكيد مسار القارع/اسم المجموعة على المصدر تحت ESA GUI> سياسات البريد > مدير موجز ويب التهديدات الخارجية > إختيار اسم المصدر المناسب.

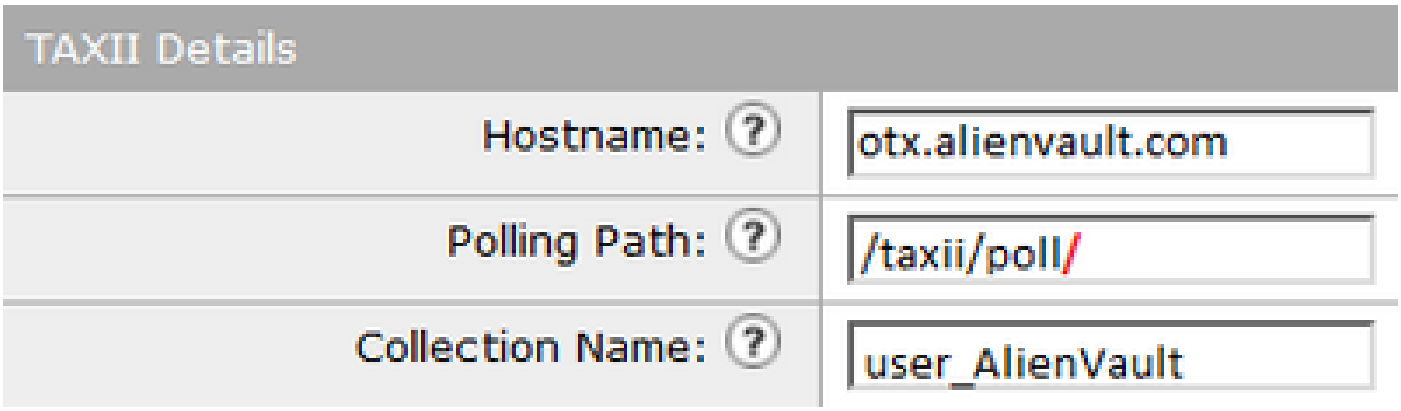
سبب الفشل: "405"

```
(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
```

ملاحظة: في RFC7231، يشير الخطأ 405 (الطريقة غير مسموح بها) إلى أن الطريقة المستلمة في سطر الطلب معروفة بواسطة الخادم الأصلي، ولكنها غير مدعومة من قبل المورد الهدف.

الحل

هذا خطأ في بناء الجملة بسبب شرطة المسار "/" المفقودة في نهاية مسار القارع.
إضافة شرطة المسار في نهاية المسار /taxii/poll/.



خطأ HTTP: خدمة رمز الحالة 503 غير متوفرة

```
(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
```

ملاحظة: وفقا لمعيار RFC7231، يمثل الخطأ 503 "الخدمة غير المتوفرة" رمز حالة إستجابة HTTP ويشير إلى أن الخادم غير قادر بشكل مؤقت على معالجة الطلب.

الحل

يشير رمز الخطأ إلى وجود مشكلة في خادم TAXII الوجهة، والتي يجب التحقيق فيها أكثر. قد يحدث ذلك عندما يتم تحميل الخادم فوق طاقته. اتصل بالمورد للحصول على مزيد من المعلومات.

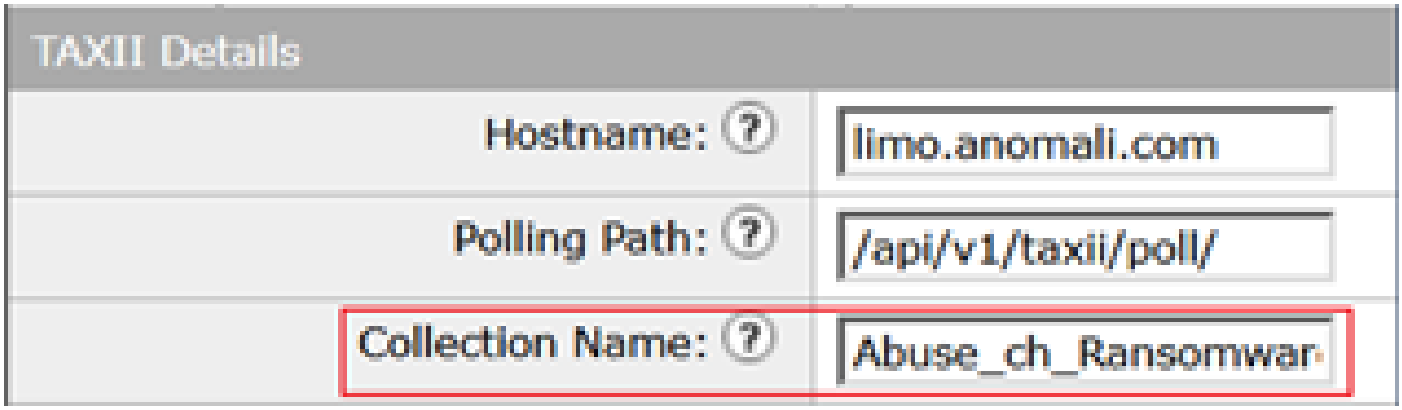
NOT_FOUND: تعذر العثور على المجموعة المطلوبة

```
(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
```

الحل

يشير هذا الخطأ إلى أن اسم المجموعة له الإعلام الصحيح، ومع ذلك، هناك مشكلة في خادم TAXII ضمن Collection، والتي ترفض الطلب.

قد يكون السبب المحتمل مؤقت انتهاء صلاحية على اسم المجموعة.
اتصل بالمورد للتحقق من عدم التناسق هذا.



[SSL: CERTIFICATE_VERIFY_FAILED] فشل التحقق من الشهادة (_ssl.c:590)

<#root>

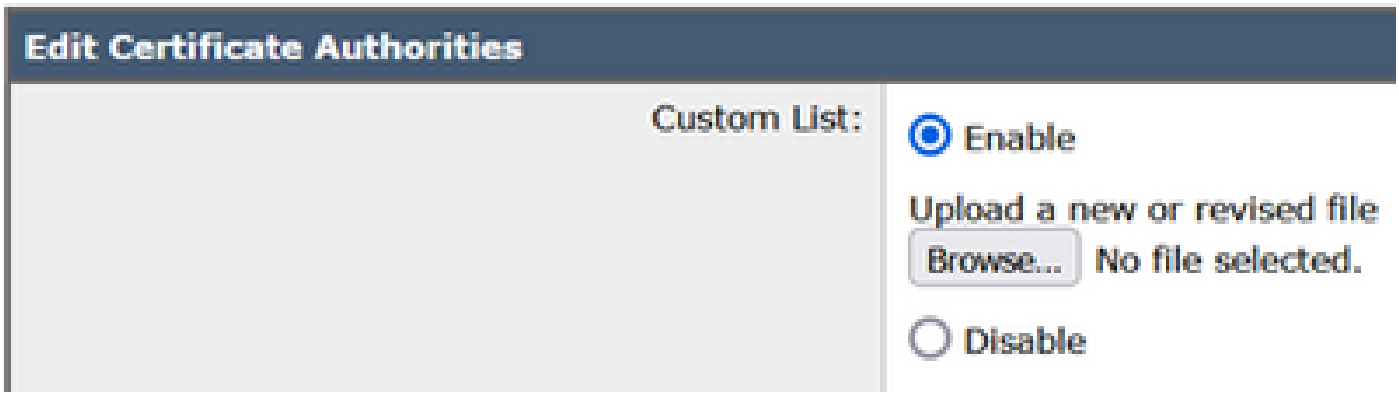
```
(Machine esa03.taclab.krk) (SERVICE)> grep "Sep 8 16:35" threatfeeds
Wed Sep 8 16:35:26 2021 Info: THREAT_FEEDS: A delta poll is scheduled for the source: ETF_Source_Name
Wed Sep 8 16:35:33 2019 Warning: THREAT_FEEDS: Unable to fetch the observables from the source: ETF_Sou

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

الحل

يشير هذا الخطأ إلى فشل الشهادة.

لحل المشكلة، قم باستيراد الشهادة في قائمة المرجع المصدق (CA).
انتقل إلى واجهة المستخدم الرسومية (GUI) > الشبكة > الشهادات > تحرير الإعدادات > قائمة مخصصة >
أختر تمكين الوضع وتحميل الشهادة.



خطأ في تحليل XML: لم يتم العثور على عنصر (السطر 0)

<#root>

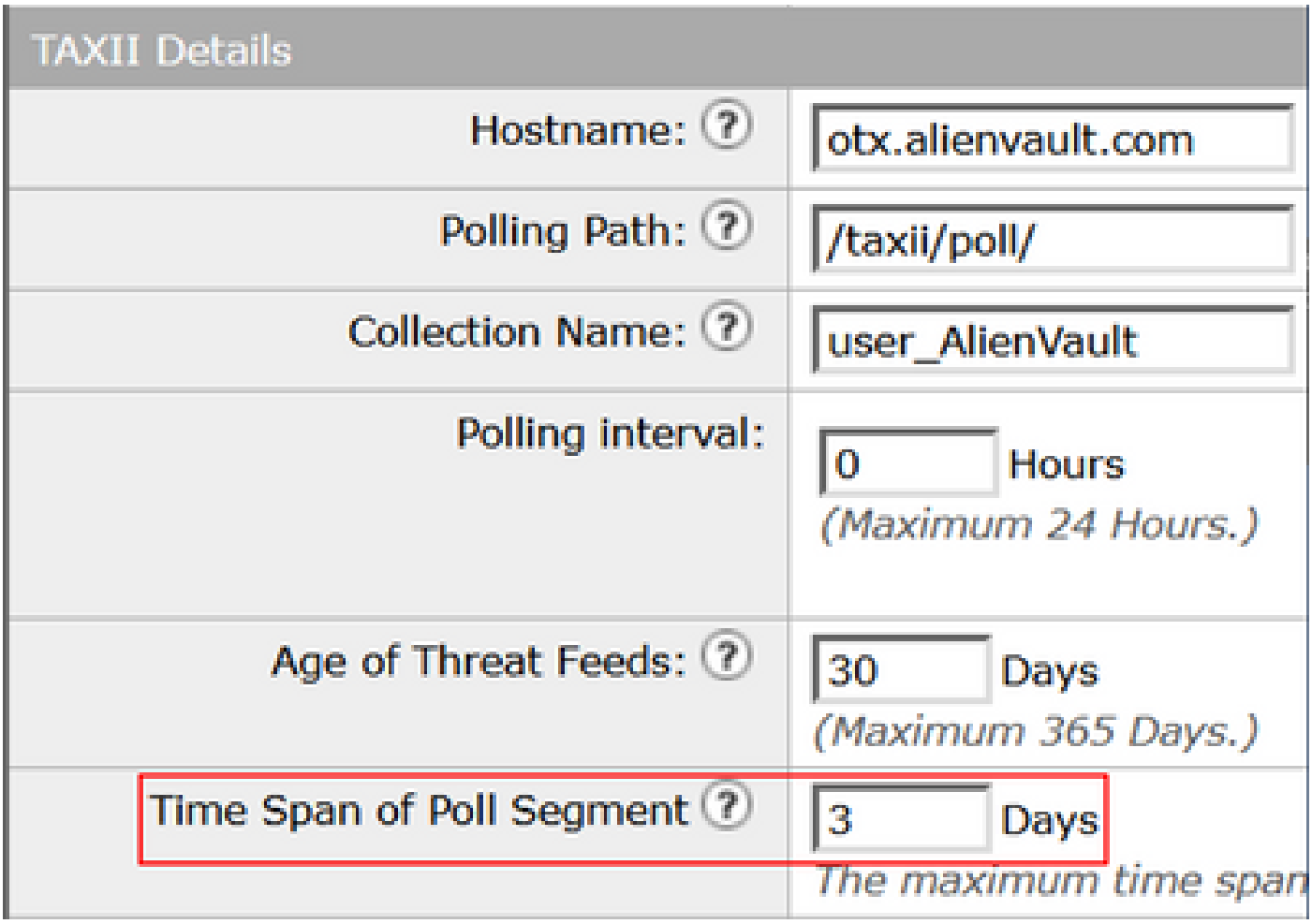
```
(Machine esa03.taclab.krk) (SERVICE)> grep "Aug 21 02:39" threatfeeds
Fri Aug 21 02:39:37 2021 Warning: THREAT_FEEDS: Unable to fetch the observables from the source: ETF_So
Fri Aug 21 02:39:37 2021 Info: THREAT_FEEDS: Job failed with exception : Source: ETF_Source_Name.

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

الحل

قلل القيمة الفترة الزمنية لمقطع الاستطلاع من تكوين ESA إلى 3-4 أيام.

ملاحظة: يعد هذا الأمر غير متناسق مع خوادم Anomali لبعض موجز الويب المحدد، حيث لا يتم إرسال علامة نهاية البيانات إلى إقفاف موجز الويب.
في هذه الحالة، لا يمكن لـ ESA الذي تم تكوينه باستخدام مصدر ETF من Anomali، استيراد البيانات لفترة زمنية تزيد عن 5 أيام.
قد يكون الحل البديل الصحيح هو تقليل القيمة الفترة الزمنية لمقطع الاستطلاع من تكوين ESA.



فشل إنشاء اتصال جديد: تم رفض اتصال [Errno 111]

<#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',))
```

ملاحظة: يشير "رفض الاتصال" إلى أنه يتعذر على العميل الاتصال بالمنفذ على الخادم الجاري تشغيله. عادة، يحدث ذلك عندما يستمع الخادم إلى المنفذ الخاطئ، أو عندما لا يكون المنفذ متوفرا.

الحل

1. أستخدم الأمر telnet أو netstat عبر واجهة سطر الأوامر (CLI) للتحقق من أن المنفذ المناسب هو الاستماع.
2. تحقق من عدم حظر جدار الحماية للمنفذ.
3. تأكد من عدم وجود منفذ Misconfiguration/ Stale على الخدمة قيد التشغيل.

معلومات ذات صلة

- أدلة المستخدم النهائي لجهاز أمان البريد الإلكتروني من Cisco
- ما هو ستاكس وتاكسي
- المعيار RFC2741 - رموز الأخطاء
- موجز التحديثات الخارجية الخاصة بورشة عمل TAC

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).