Solución de problemas de fuentes de amenazas externas Principales razones del error

Contenido

[Introducción](#)
[Prerequisites](#)
[Componentes Utilizados](#)
[Motivo de los errores:](#)
[El servicio ETF está deshabilitado o no hay una clave de característica válida para el servicio](#)
[Error al establecer una nueva conexión: [Error110] Connection Timed Out](#)
[Motivo del error: "400"](#)
[Error de HTTP: error de autenticación del código de estado 401](#)
[Error de taxi: error de HTTP: código de estado 404 Recurso solicitado no disponible](#)
[Motivo del error: "405"](#)
[Error de HTTP: código de estado 503 Servicio no disponible](#)
[NOT_FOUND: No se encuentra la colección solicitada](#)
[[SSL: CERTIFICATE_VERIFY_FAILED] Error en la verificación del certificado (_ssl.c:590)](#)
[Error de comparación de XML: no se encontró ningún elemento (línea 0)](#)
[Error al establecer una nueva conexión: [Error111] Conexión rechazada](#)
[Información Relacionada](#)

Introducción

En este documento se describen varios motivos para que se produzca un error durante la implementación de la fuente de amenazas externas, el análisis de errores y las acciones para su resolución.

Prerequisites

No hay requisitos específicos, por lo que Cisco recomienda que tenga conocimiento de estos temas:

- Cisco Secure Email Gateway (ESA)
- Fuentes sobre amenazas externas (ETF)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Secure Email Gateway (ESA) con software versión 12.x o posterior

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Motivo de los errores:

El servicio ETF está deshabilitado o no hay una clave de característica válida para el

servicio

<#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.
```

Solución

Asegúrese de lo siguiente:

1. La clave de característica ETF está instalada correctamente.
2. EULA aceptado y clave de característica habilitada globalmente.
3. Licencias aplicadas en el nivel de equipo.

Nota: Si hay un nivel de cluster, debe copiar la configuración en el nivel de máquina.

Error al establecer una nueva conexión: [Error 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',))
```

Nota: el tiempo de espera de la conexión normalmente indica un problema relacionado con la red, que impide que ESA obtenga una respuesta. Se recomiendan las comprobaciones de firewall/proxy y la captura de paquetes para un análisis más profundo.

Solución

1. Confirme que el firewall y el proxy no bloquean el tráfico.
   El proxy se puede comprobar en **GUI > Servicios de seguridad > Actualizaciones de servicios.**
2. Confirme la conectividad con la captura de paquetes. Vaya a **GUI > Ayuda y soporte técnico > Captura de paquetes.**

Sugerencia: cuando hay indicios de problemas relacionados con la red, es prudente ejecutar capturas de paquetes para confirmar que la conexión se ha establecido correctamente.

Motivo del error: "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
```

Nota: RFC7231 Error 400 (Solicitud incorrecta), indica que el servidor no puede o no procesa la solicitud debido a algo que se percibe como un error de cliente. La mayoría de las veces aparece debido a una sintaxis de solicitud incorrecta o a un entramado de mensaje de solicitud no válido.

Solución

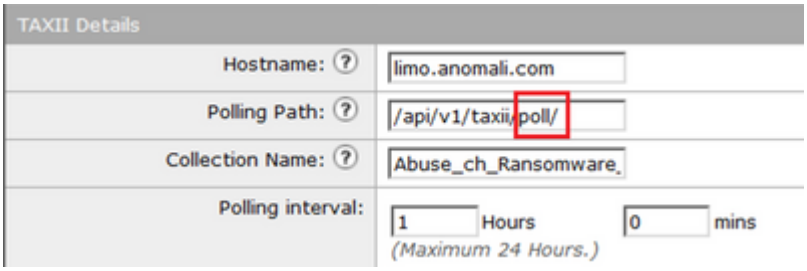
El error "400" indica que esta ruta de sondeo existe, pero apunta a un servicio diferente que ofrece el servidor TAXI.

1. Confirmar configuración de ruta de sondeo se configura con solicitud de sondeo y no con solicitud de detección.
2. Confirme que HTTPS está habilitado en **GUI > Políticas de correo > Administrador de fuentes de amenazas externas > Usar HTTPS.**

Precaución: Normalmente, este problema ocurre cuando la ruta de sondeo está mal configurada con la solicitud de detección, como: /api/v1/taxii/taxii-discovery-service/
La ruta de sondeo se puede configurar para utilizar la solicitud de sondeo para las fuentes, por ejemplo: /api/v1/taxii/poll

---

Nota: Diferencia entre la solicitud de sondeo y de descubrimiento:
- URL de sondeo es en realidad donde se consumen las fuentes de.
- URL del servicio de detección se utiliza para encontrar los servicios que ofrece el servicio de taxi.



Error de HTTP: error de autenticación del código de estado 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
```

Solución

Este código de error indica que carece de credenciales de autenticación válidas para el recurso de destino.

Confirme que las credenciales están configuradas correctamente.
También existe la opción de no configurar las credenciales de los usuarios.

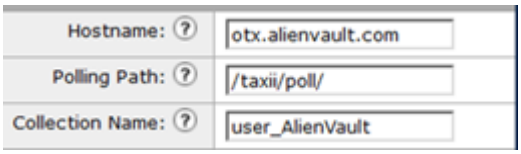
Error de taxi: error de HTTP: código de estado 404 Recurso solicitado no disponible

```
(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
```

> **Nota**: El código de estado 404 (No encontrado) indica que el servidor de origen no ha encontrado una representación actual para el recurso de destino o no está dispuesto a revelar que existe una. Esto revela que puede haber una dirección URL no válida y, en la mayoría de los casos, que no se encuentra la ruta de acceso del recurso.

Solución

Confirme la ruta de sondeo/nombre de la colección en el origen en la **GUI de** ESA> **Políticas de correo > Administrador de fuentes de amenazas externas > Elija el nombre de origen adecuado**.



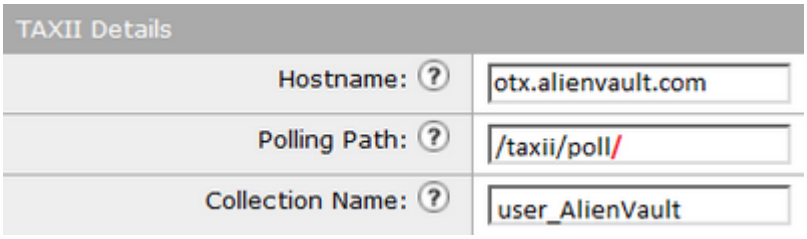
Motivo del error: "405"

```
(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
```

> **Nota**: Según RFC7231, el error 405 (método no permitido) indica que el servidor de origen conoce el método recibido en la línea de solicitud, pero el recurso de destino no lo admite.

Solución

Esto es un error de sintaxis debido a la barra diagonal "/" de la pista que falta al final de la ruta de sondeo. Agregue una barra inclinada al final de la ruta /taxi/poll/.



Error de HTTP: código de estado 503 Servicio no disponible

```
(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
```

> **Nota**: Según RFC7231, el error 503 "Servicio no disponible" es un código de estado de respuesta HTTP e indica que un servidor no puede gestionar temporalmente la solicitud.

Solución

El código de error indica un problema con el servidor TAXI de destino, que debe investigarse más a fondo. Esto puede ocurrir cuando el servidor está sobrecargado. Póngase en contacto con el proveedor para obtener más información.

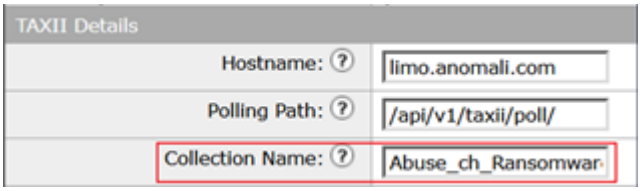
NOT_FOUND: No se encuentra la colección solicitada

```
(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
```

Solución

Este error indica que el nombre de la colección tiene la ortografía correcta; sin embargo, hay un problema en el servidor TAXI en la colección, que rechaza la solicitud.

La causa posible podría ser un temporizador de vencimiento en el nombre de la colección.
Póngase en contacto con el proveedor para comprobar este tipo de incoherencia.



[SSL: CERTIFICATE_VERIFY_FAILED] Error en la verificación del certificado (_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)

Solución

Este error indica una falla de certificado.

Para resolver el problema, importe el certificado en la lista de entidades emisoras de certificados (CA).
Vaya a **GUI > Red > Certificados > Editar configuración > Lista personalizada >**
Elija el modo **Enable** y cargue el certificado.

Error de comparación de XML: no se encontró ningún elemento (línea 0)

<#root>

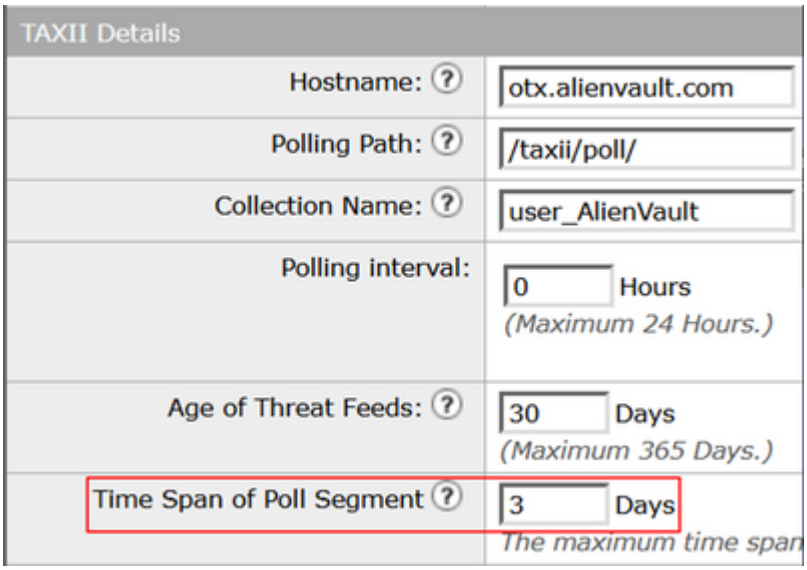
```
(Machine esa03.taclab.krk) (SERVICE)> grep "Aug 21 02:39" threatfeeds
Fri Aug 21 02:39:37 2021 Warning: THREAT_FEEDS: Unable to fetch the observables from the source: ETF_Sou
Fri Aug 21 02:39:37 2021 Info: THREAT_FEEDS: Job failed with exception : Source: ETF_Source_Name.
```

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

Solución

Reduzca el valor de Intervalo de tiempo del segmento de sondeo de la configuración de ESA a 3-4 días.

> **Nota**: Esto es una incoherencia con los servidores Anomali para algunas fuentes específicas, donde no se envía ningún indicador de fin de datos para detener las fuentes.
> En este caso, el ESA que está configurado con un origen ETF de Anomali, no puede sondear los datos durante un lapso de tiempo de más de 5 días.
> Una solución alternativa válida sería reducir el valor del intervalo de tiempo del segmento de sondeo de la configuración ESA.



Error al establecer una nueva conexión: [Error 111] Conexión rechazada

<#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 excee
```

Failed to establish a new connection: [Errno 111] Connection refused',))

> **Nota**: "Conexión rechazada" indica que el cliente no puede conectarse al puerto del servidor en ejecución. Normalmente, esto ocurre cuando el servidor escucha en el puerto incorrecto o cuando el puerto no está disponible.

Solución

1. Utilice el comando **telnet** o **netstat** a través de CLI para verificar que el puerto apropiado está escuchando.
2. Verifique que el firewall no bloquee el puerto.
3. Asegúrese de que no haya un error de configuración de puerto/puerto obsoleto en el servicio en ejecución.

Información Relacionada

- Guías para el usuario final de Cisco Email Security Appliance
- Qué son STIX y TAXI
- RFC2741: códigos de error
- Fuentes sobre amenazas externas del taller TAC

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).