Risoluzione dei problemi dei feed di minacce esterne Principali motivi dell'errore

Sommario

Introduzione

In questo documento vengono descritte diverse cause di errore durante l'implementazione del feed delle minacce esterne, l'analisi degli errori e le azioni per la risoluzione.

Prerequisiti

Non sono previsti requisiti specifici, quindi Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Secure Email Gateway (ESA)
- Feed di minacce esterne (ETF)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Secure Email Gateway (ESA) con software versione 12.x o successive

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Motivo degli errori:

Il servizio ETF è disabilitato o non esiste una chiave di funzionalità valida per il servizio

<#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.

Soluzione

Accertarsi che:

1. Chiave della funzionalità ETF installata correttamente.
2. EULA accettato e chiave di funzionalità attivata a livello globale.
3. Licenze applicate a livello di computer.

Nota: se è presente un livello cluster, è necessario copiare l'impostazione nel livello computer.

Impossibile stabilire una nuova connessione: [Errore 110] Timeout della connessione

```
(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',))
```

Nota: il timeout della connessione in genere indica un problema di rete che impedisce a ESA di ricevere una risposta. Si consiglia di controllare il firewall e il proxy e di acquisire i pacchetti per un'analisi più approfondita.

Soluzione

1. Verificare che il firewall e il proxy non blocchino il traffico.
   Il proxy può essere controllato in GUI > Security Services > Service Updates (Servizi di sicurezza > Aggiornamenti servizi).
2. Confermare la connettività con Packet Capture. Selezionare GUI > Help and Support > Packet Capture.

Suggerimento: quando vi sono indicazioni di problemi relativi alla rete, è prudente eseguire l'acquisizione dei pacchetti per verificare che la connessione sia stata stabilita correttamente.

Motivo dell'errore: "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
```

Nota: RFC7231 Errore 400 (Richiesta non valida) indica che il server non può o non elabora la richiesta a causa di un errore del client. Nella maggior parte dei casi è dovuto a sintassi di richiesta non valida o frame di messaggi di richiesta non validi.

Soluzione

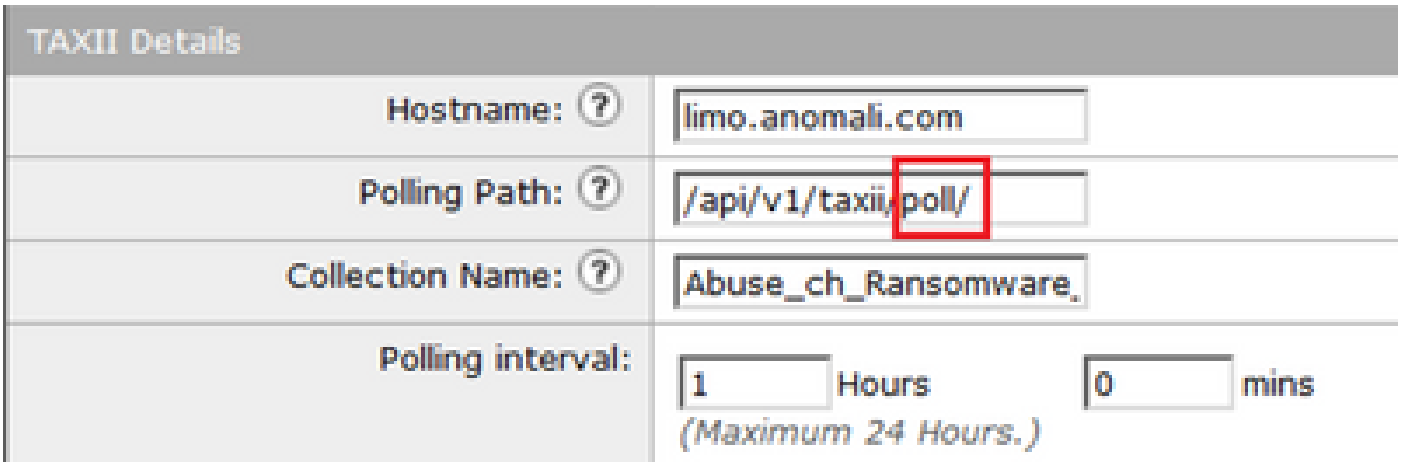
L'errore "400" indica che il percorso di polling esiste, ma punta a un servizio diverso offerto dal server TAXII.

1. Confermare che la configurazione del percorso di polling sia configurata con la richiesta di polling e non con la richiesta di individuazione.
2. Confermare che HTTPS è abilitato in GUI > Mail Policies > External Threat Feeds Manager > Use HTTPS.

Attenzione: questo problema si verifica in genere quando il percorso di polling non è configurato correttamente con la richiesta di individuazione, ad esempio: /api/v1/taxii/taxii-discovery-service/
È possibile configurare il percorso di polling in modo da utilizzare la richiesta di polling per i feed, ad esempio /api/v1/taxii/poll

---

Nota: differenza tra la richiesta di polling e la richiesta di individuazione:
- L'URL di polling è l'indirizzo da cui vengono utilizzati i feed.
- L'URL del servizio di individuazione viene utilizzato per individuare i servizi offerti dal servizio Taxi.



Errore HTTP: codice di stato 401, errore di autenticazione

```
(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
```

Soluzione

Questo codice di errore indica la mancanza di credenziali di autenticazione valide per la risorsa di destinazione.

Verificare che le credenziali siano configurate correttamente.
È inoltre possibile non configurare le credenziali per gli utenti.

Errore Taxi: errore HTTP: codice di stato 404. Risorsa richiesta non disponibile

```
(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
```

Nota: il codice di stato 404 (Non trovato) indica che il server di origine non ha trovato una rappresentazione corrente per la risorsa di destinazione o non è disposto a rivelarne l'esistenza. Ciò indica che può esistere un URL non valido e, nella maggior parte dei casi, che il problema si è verificato a causa del percorso della risorsa non trovato.

Soluzione

Confermare il percorso di polling/nome della raccolta sull'origine in ESA GUI> Mail Policies > External Threat Feeds Manager > Scegliere il nome di origine appropriato.

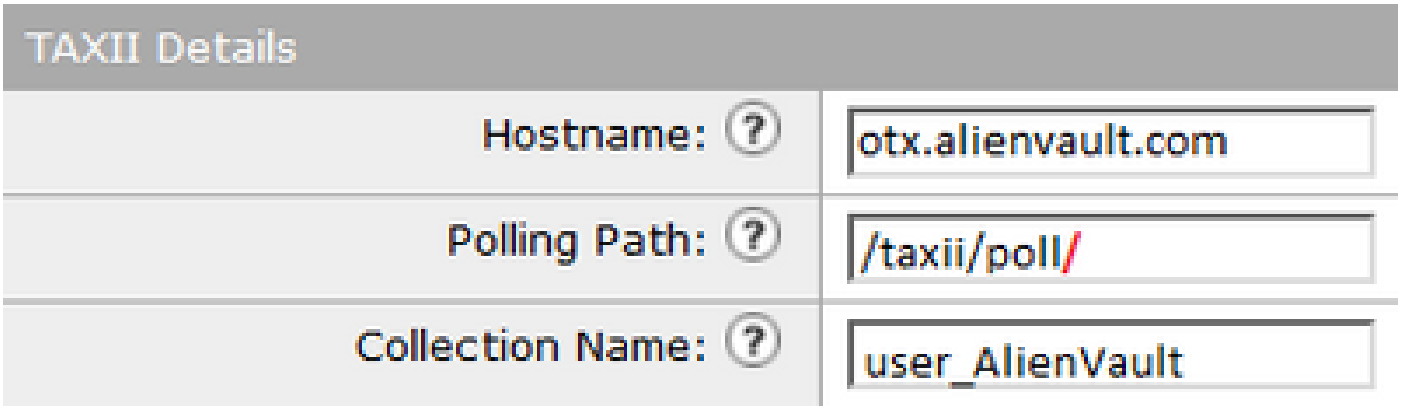
Motivo dell'errore: "405"

```
(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
```

Nota: in base a RFC7231, l'errore 405 (metodo non consentito) indica che il metodo ricevuto nella riga di richiesta è noto al server di origine, ma non è supportato dalla risorsa di destinazione.

Soluzione

Errore di sintassi causato dalla barra "/" di riepilogo mancante alla fine del percorso di polling. Aggiungere una barra alla fine del percorso /taxii/poll/.



Errore HTTP: codice di stato 503, servizio non disponibile

```
(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
```

Nota: in base a RFC7231, l'errore 503 "Service Unavailable" (Servizio non disponibile) è un codice di stato della risposta HTTP e indica che un server non è temporaneamente in grado di gestire la richiesta.

Soluzione

Il codice di errore indica un problema con il server TAXII di destinazione, che deve essere esaminato ulteriormente.
Questo problema può verificarsi quando il server è sovraccarico. Per ulteriori informazioni, contattare il fornitore.

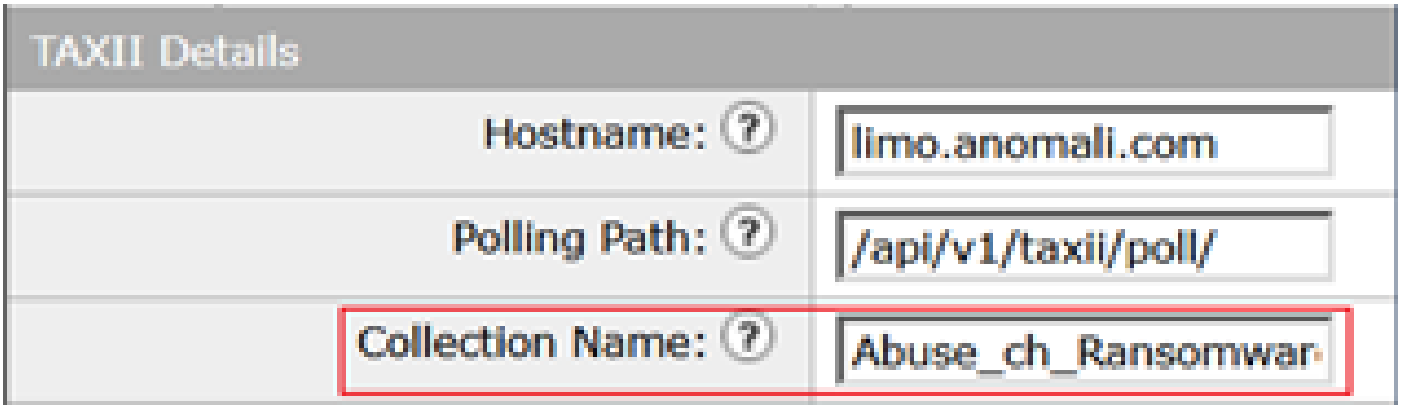
NOT_FOUND: impossibile trovare la raccolta richiesta

```
(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
```

Soluzione

Questo errore indica che il nome della raccolta è stato digitato correttamente. Tuttavia, si è verificato un problema nel server TAXII in Raccolta, che rifiuta la richiesta.

Possibile causa: un timer di scadenza per il nome della raccolta.
Contattare il fornitore per verificare questo tipo di incoerenze.



[SSL: CERTIFICATE_VERIFY_FAILED] Verifica certificato non riuscita (_ssl.c:590)

<#root>

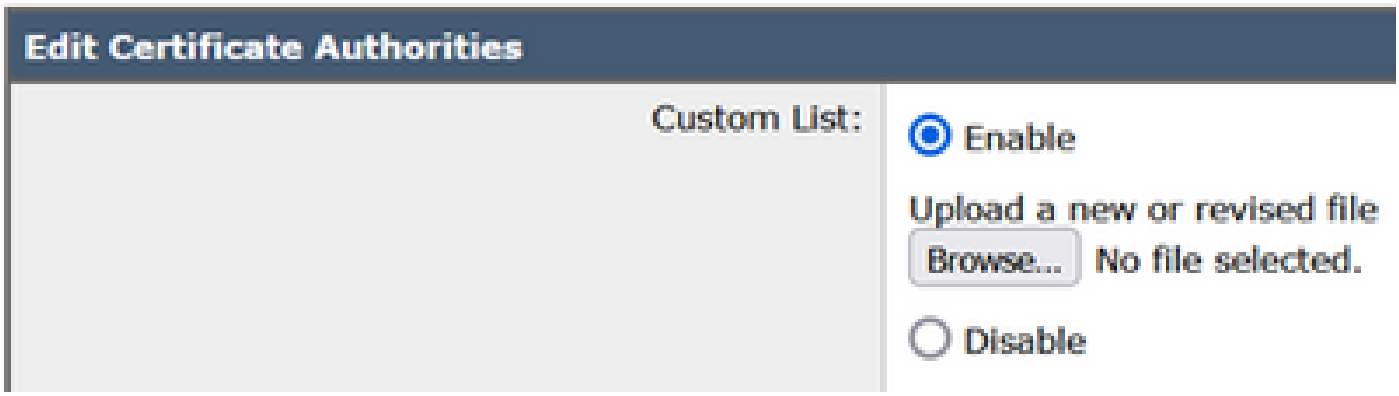
```
(Machine esa03.taclab.krk) (SERVICE)> grep "Sep 8 16:35" threatfeeds
Wed Sep 8 16:35:26 2021 Info: THREAT_FEEDS: A delta poll is scheduled for the source: ETF_Source_Name
Wed Sep 8 16:35:33 2019 Warning: THREAT_FEEDS: Unable to fetch the observables from the source: ETF_Sou
```

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

Soluzione

Questo errore indica un errore del certificato.

Per risolvere il problema, importare il certificato nell'elenco delle Autorità di certificazione (CA). Selezionare GUI > Rete > Certificati > Modifica impostazioni > Elenco personalizzato > Scegliere Abilita modalità e caricare il certificato.



Errore di analisi XML: nessun elemento trovato (riga 0)

<#root>

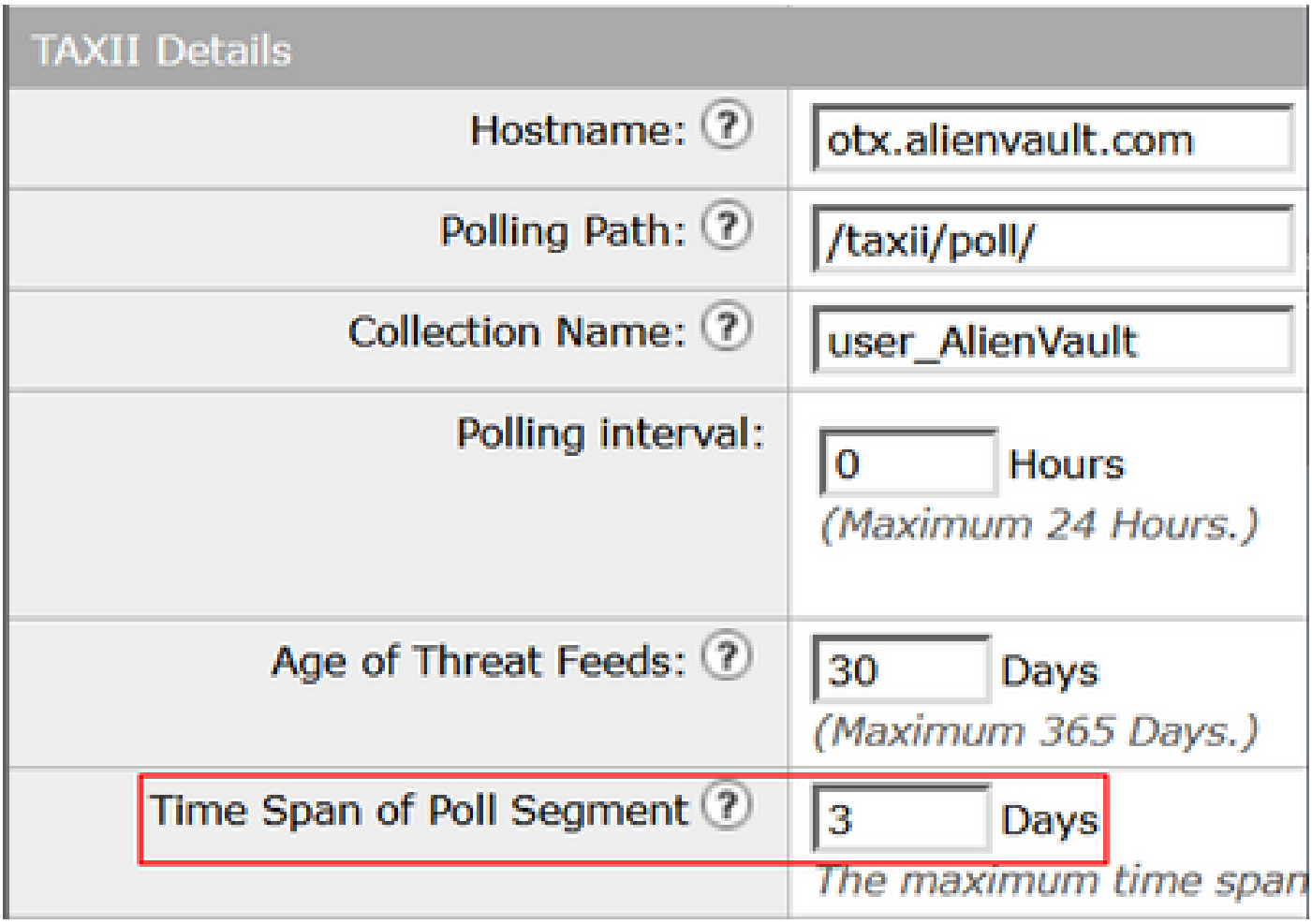
```
(Machine esa03.taclab.krk) (SERVICE)> grep "Aug 21 02:39" threatfeeds
Fri Aug 21 02:39:37 2021 Warning: THREAT_FEEDS: Unable to fetch the observables from the source: ETF_So
Fri Aug 21 02:39:37 2021 Info: THREAT_FEEDS: Job failed with exception : Source: ETF_Source_Name.
```

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

Soluzione

Ridurre il valore Time Span del segmento di polling dalla configurazione ESA a 3-4 giorni.

Nota: si tratta di un'incoerenza con i server Anomali per alcuni feed specifici, in cui non viene inviato alcun flag di fine dati per arrestare i feed.
In questo caso, l'ESA configurata con una fonte ETF di Anomali non è in grado di eseguire il polling dei dati per un periodo di tempo di 5 giorni.
Una soluzione valida consiste nel ridurre il valore Time Span del segmento di polling dalla configurazione ESA.



Impossibile stabilire una nuova connessione: [Errore 111] Connessione rifiutata

<#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',))
```

Nota: "Connessione rifiutata" indica che il client non può connettersi alla porta sul server in esecuzione. Questo si verifica in genere quando il server resta in ascolto sulla porta errata o quando la porta non è disponibile.

Soluzione

1. Utilizzare il comando telnet o netstat dalla CLI per verificare che la porta appropriata sia in ascolto.
2. Verificare che il firewall non blocchi la porta.
3. Verificare che non vi siano porte configurate in modo errato/porte non aggiornate nel servizio in esecuzione.

Informazioni correlate

- Guide per l'utente finale di Cisco Email Security Appliance
- Cosa sono STIX e TAXII
- RFC 2741 - Codici di errore
- Feed minacce esterne del workshop TAC

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).