Probleemoplossing Externe bedreigingen geeft belangrijkste redenen voor falen aan

Inhoud

Inleiding

In dit document worden verschillende redenen beschreven voor een storing tijdens de implementatie van de Externe Threat Feed, foutanalyse en maatregelen voor oplossing.

Voorwaarden

Er zijn geen specifieke vereisten. Cisco raadt u daarom aan deze onderwerpen te kennen:

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

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Software voor Cisco Secure Email Gateway (ESA) - 12.x of hoger

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Reden voor fouten:

De ETF-service is uitgeschakeld of er is geen geldige functiesleutel voor de 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.
```

Oplossing

Zorg ervoor dat:

1. De ETF-functiesleutel is correct geïnstalleerd.
2. EULA geaccepteerd en de functiesleutel is wereldwijd ingeschakeld.
3. Toegepaste licenties op machineniveau.

Opmerking: als er een clusterniveau is, moet het de instelling naar het niveau van de machine kopiëren.

Er is geen nieuwe verbinding tot stand gebracht: [Errno 110] Time-out verbinding

```
(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',))
```

Opmerking: Time-out bij verbinding duidt doorgaans op een probleem met betrekking tot het netwerk, dat ESA ervan weerhoudt een antwoord te krijgen. Firewall/Proxy-controles worden aanbevolen en pakketvastlegging voor diepere analyse.

Oplossing

1. Bevestig dat firewall en proxy het verkeer niet blokkeren.
   De proxy kan worden gecontroleerd onder **GUI > Security Services > Service Updates.**
2. Bevestig de connectiviteit met Packet Capture. Navigeren naar **GUI > Help en ondersteuning > Packet Capture.**

Tip: Wanneer er aanwijzingen zijn dat netwerk problemen veroorzaakt, is het verstandig om pakketopnamen uit te voeren om te bevestigen dat de verbinding goed tot stand is gebracht.

Reden voor falen: "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
```

Opmerking: RFC7231 Fout 400 (Slecht verzoek) geeft aan dat server het verzoek niet kan of niet verwerkt vanwege iets dat wordt gezien als een client fout. Meestal verschijnt het als gevolg van misvormde aanvraagsyntaxis, of ongeldige verzoekbericht framing.

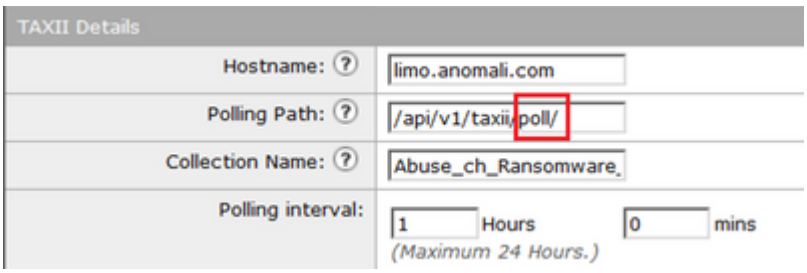
Oplossing

Fout "400" geeft aan dat dit opiniepeilingspad bestaat, maar wijst op een andere service die TAXII server biedt.

1. Bevestig dat de configuratie van het opiniepeilingspad is geconfigureerd met het verzoek om opiniepeiling en niet met het verzoek om detectie.
2. Bevestig dat HTTPS is ingeschakeld onder **GUI > Mail Policies > Externe Threat Feeds Manager > Gebruik HTTPS.**

Waarschuwing: dit probleem treedt doorgaans op wanneer het opiniepad verkeerd is ingesteld met een zoekverzoek, zoals: /api/v1/taxii/taxii-discovery-service/
Polling Path kan worden geconfigureerd om Poll request for the feeds te gebruiken, bijvoorbeeld: /api/v1/taxii/poll

Opmerking: verschil tussen opiniepeiling en detectieaanvraag:
- Polling URL is eigenlijk waar u de feeds van verbruikt.
- Detectieservice URL wordt gebruikt om de diensten te vinden die de Taxii-service biedt.



HTTP-fout: statuscode 401 verificatiefout

```
(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
```

Oplossing

Deze foutcode geeft aan dat er geen geldige verificatiereferenties zijn voor de doelbron.

Bevestig dat Credentials correct worden geconfigureerd.
Er is ook een optie om referenties voor gebruikers niet te configureren.

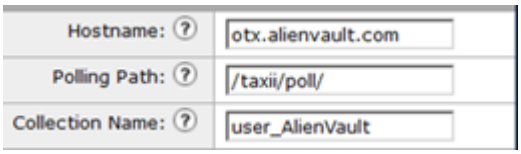
Taxii Fout: HTTP Fout: Status Code 404 Aangevraagde bron niet beschikbaar

```
(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
```

> **Opmerking**: De 404 (niet gevonden) statuscode geeft aan dat de oorspronkelijke server geen huidige representatie voor de doelbron heeft gevonden, of niet bereid is te onthullen dat er een bestaat. Dit onthult dat er een Ongeldige URL kan zijn en in de meeste gevallen, dat de voorvallen toe te schrijven aan middel weg niet wordt gevonden.

Oplossing

Bevestig de naam van het stempelpad/de verzameling op de bron onder ESA **GUI> Mail Policies > Externe Threat Feeds Manager > Kies de juiste bronnaam**.



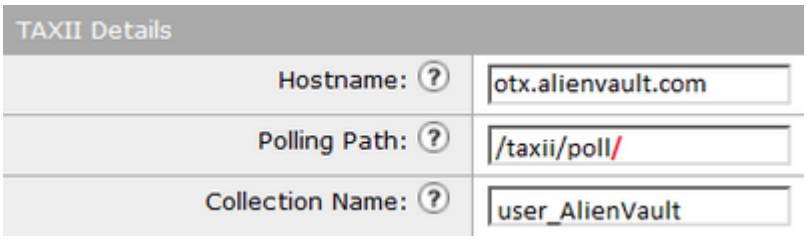
Reden voor falen: "405"

```
(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
```

> **Opmerking**: Per RFC7231 geeft Fout 405 (Methode niet toegestaan) aan dat de methode die wordt ontvangen in de aanvraagregel bekend is bij de oorsprongserver, maar niet wordt ondersteund door de doelbron.

Oplossing

Dit is een Syntax fout vanwege de ontbrekende Trail "/" Slash aan het einde van het opiniepeilingspad. Slash aan het einde van het pad /taxii/poll/ toevoegen.



HTTP-fout: statuscode 503 service niet beschikbaar

```
(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
```

Opmerking: per RFC7231 is fout 503 "Service niet beschikbaar" een HTTP-responsstatuscode en geeft aan dat een server tijdelijk niet in staat is om het verzoek te verwerken.

Oplossing

Foutcode geeft een probleem aan met de TAXI-server van bestemming, dat verder onderzocht moet worden. Dit kan gebeuren als de server is overbelast. Neem contact op met de leverancier voor meer informatie.

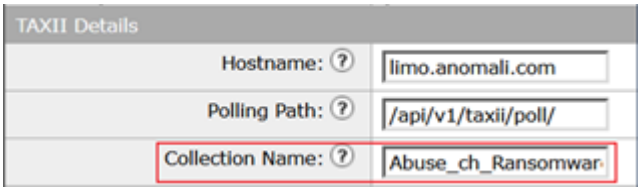
NOT_found: De gevraagde verzameling kon niet worden gevonden

```
(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
```

Oplossing

Deze fout geeft aan dat de Collectienaam de juiste spelling heeft, maar er is een probleem op TAXII server onder Collection, die het verzoek afwijst.

Mogelijke oorzaak kan een verlooptimer zijn op Collectienaam.
Neem contact op met de leverancier om deze inconsistentie te controleren.



[SSL: CERTIFICAAT_VERIFY_MISLUKT] Certificaat controleren mislukt (_ssl.c:590)

<#root>

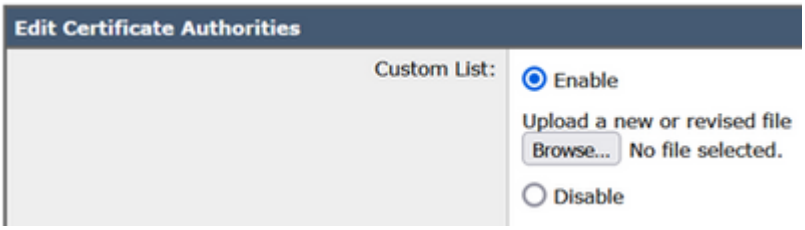
```
(Machine esa03.taclab.krk) (SERVICE)> grep "Sep 8 16:35" threatfeeds
Wed Sep 8 16:35:26 2021 Info: THREAT_FEEDS: A delta poll is scheduled for the source: ETF_Source_Name
Wed Sep 8 16:35:33 2019 Warning: THREAT_FEEDS: Unable to fetch the observables from the source: ETF_Sou
```

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

Oplossing

Deze fout duidt op een certificaatfout.

Voer het Certificaat in de lijst van de certificeringsinstantie (CA) in om de kwestie op te lossen.
Navigeer naar **GUI > Netwerk > Certificaten > Instellingen bewerken > Aangepaste lijst >**
Kies de modus **Inschakelen** en het certificaat uploaden.



XML Parising-fout: geen element gevonden (regel 0)

<#root>

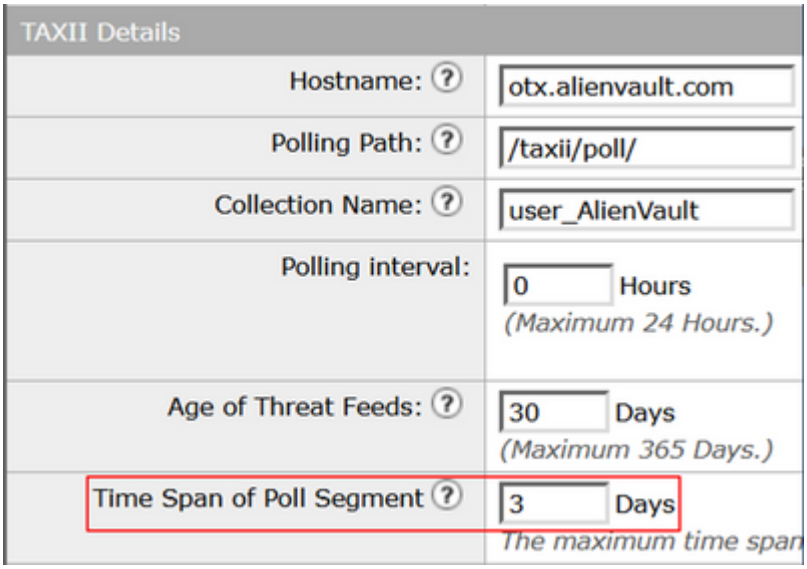
```
(Machine esa03.taclab.krk) (SERVICE)> grep "Aug 21 02:39" threatfeeds
Fri Aug 21 02:39:37 2021 Warning: THREAT_FEEDS: Unable to fetch the observables from the source: ETF_Sou
Fri Aug 21 02:39:37 2021 Info: THREAT_FEEDS: Job failed with exception : Source: ETF_Source_Name.
```

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

Oplossing

Verminder de waarde tijdspanne van Poll Segment van ESA configuratie tot 3-4 dagen.

> **Opmerking**: dit is een inconsistentie met Anomali-servers voor bepaalde specifieke feeds, waarbij geen einde van data-vlag wordt verzonden om de feeds te stoppen.
> In dit geval kan een ESA dat is geconfigureerd met een ETF-bron uit Anomali, de gegevens niet over een periode van meer dan vijf dagen opvragen.
> Een geldige tijdelijke oplossing zou zijn de waarde tijdspanne van Poll Segment van ESA configuratie te verminderen.



Geen nieuwe verbinding tot stand brengen: [fout 111] verbinding geweigerd

<#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',))
```

> **Opmerking**: "Verbinding geweigerd" geeft aan dat client geen verbinding kan maken met de poort op de actieve server. Meestal gebeurt dit wanneer de server inluistert op de verkeerde poort, of wanneer de poort niet beschikbaar is.

Oplossing

1. Gebruik de opdracht **Telnet** of **netstat** via CLI om te controleren of de juiste poort luistert.
2. Controleer of de firewall de poort niet blokkeert.
3. Zorg ervoor dat er geen Port MisConfiguration/Stale-poort is bij een actieve service.

Gerelateerde informatie

- Cisco e-mail security applicatie eindgebruikershandleidingen
- Wat zijn STIX en TAXII
- RFC2741 - Foutcodes
- TAC Workshop externe bedreigingen

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.