Principais motivos para a falha do Troubleshooting de Feeds de Ameaças Externas

Contents

Introdução

Este documento descreve vários motivos para falha durante a implementação do External Threat Feed, análise de erros e ações para resolução.

Pré-requisitos

Não há requisitos específicos, portanto a Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Secure Email Gateway (ESA)
- Feeds de ameaças externas (ETF)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Secure Email Gateway (ESA) executando o software 12.x ou versão posterior

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Motivo das falhas:

O serviço ETF está desativado ou não há uma chave de recurso válida para o serviço

<#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.
```

Solução

Assegure que:

1. Chave de recurso ETF instalada corretamente.
2. EULA aceito e chave de recurso habilitada globalmente.
3. Licenças aplicadas no nível da máquina.

Observação: se houver um nível de cluster, ele precisará copiar a configuração no nível da máquina.

Falha ao Estabelecer uma Nova Conexão: [Erro 110] Tempo Limite da Conexão Esgotado

```
(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',))
```

Observação: o tempo limite da conexão normalmente indica um problema relacionado à rede, o que impede que o ESA obtenha uma resposta. As verificações de firewall/proxy são recomendadas e a captura de pacotes é recomendada para uma análise mais profunda.

Solução

1. Confirme se o Firewall e o Proxy não bloqueiam o tráfego.
   O proxy pode ser verificado em **GUI > Serviços de segurança > Atualizações de serviço.**
2. Confirme a conectividade com a Captura de pacotes. Navegue até **GUI > Ajuda e suporte > Captura de pacotes.**

Dica: quando há indicações de problemas relacionados à rede, é prudente executar capturas de pacotes para confirmar se a conexão foi estabelecida corretamente.

Motivo da falha: "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
```

Observação: o erro 400 (solicitação incorreta) do RFC7231 indica que o servidor não pode ou não processa a solicitação devido a algo que é considerado um erro do cliente. Na maioria das vezes, ele aparece devido a sintaxe de solicitação malformada ou enquadramento de mensagem de solicitação inválido.

Solução

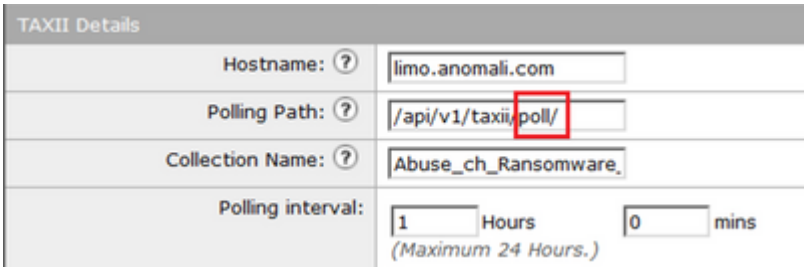
O erro "400" indica que esse caminho de polling existe, mas aponta para um serviço diferente que o servidor TAXII oferece.

1. Confirme se a Configuração do Caminho de Sondagem está configurada com a solicitação de Sondagem e não com a solicitação de Descoberta.
2. Confirme se o HTTPS está habilitado em **GUI > Políticas de e-mail > Gerenciador de feeds de ameaças externas > Usar HTTPS.**

Cuidado: normalmente esse problema ocorre quando o Caminho de Sondagem está configurado incorretamente com a solicitação de descoberta, como: /api/v1/taxii/taxii-discovery-service/
O caminho de sondagem pode ser configurado para usar a solicitação de sondagem para os feeds, por exemplo: /api/v1/taxii/poll

---

Observação: Diferença entre solicitação de pesquisa e descoberta:
- A URL de pesquisa é de onde você consome os feeds.
- A URL do Discovery Service é usada para localizar quais serviços o serviço Taxii oferece.



Erro HTTP: falha de autenticação do código de status 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
```

Solução

Este código de erro indica que ele não tem credenciais de autenticação válidas para o recurso de destino.

Confirme se as Credenciais estão configuradas corretamente.
Há também uma opção de não configurar credenciais para usuários.

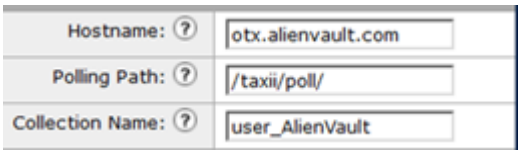
Erro de imposto: Erro HTTP: Código de Status 404 Recurso Solicitado Não Disponível

```
(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
```

> **Observação**: o código de status 404 (Não Encontrado) indica que o servidor de origem não encontrou uma representação atual para o recurso de destino ou não está disposto a divulgar que existe uma. Isso revela que pode haver um URL inválido e, na maioria dos casos, que o ocorreu devido ao caminho do recurso não foi encontrado.

Solução

Confirme o caminho de pesquisa/nome da coleção na origem em ESA **GUI> Políticas de e-mail > Gerenciador de feeds de ameaças externas > Escolha o nome de origem apropriado**.



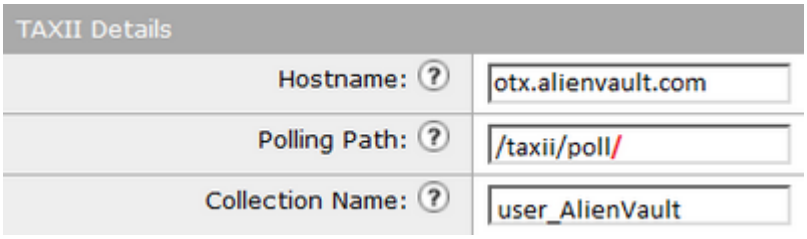
Motivo da falha: "405"

```
(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
```

> **Observação**: de acordo com RFC7231, o erro 405 (método não permitido) indica que o método recebido na linha de solicitação é conhecido pelo servidor de origem, mas não é suportado pelo recurso de destino.

Solução

Este é um erro de sintaxe devido à barra de trilha "/" ausente no final do caminho de pesquisa.
Adicionar barra de trilha no final do caminho /taxii/poll/.



Erro HTTP: Código de Status 503 Serviço Indisponível

```
(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
```

> **Observação**: de acordo com RFC7231, o erro 503 "Serviço indisponível" é um código de status de resposta HTTP e indica que um servidor não pode tratar temporariamente a solicitação.

Solução

O código de erro indica um problema com o servidor TAXII de destino, que precisa ser investigado mais a fundo.
Isso pode acontecer quando o servidor está sobrecarregado. Entre em contato com o Fornecedor para obter mais informações.

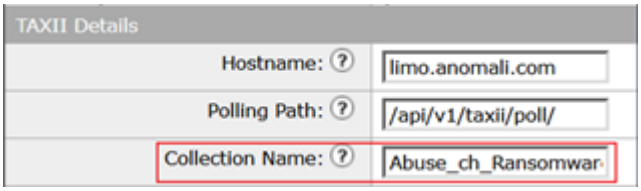
NOT_FOUND: Não foi possível localizar a coleção solicitada

```
(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
```

Solução

Este erro indica que o nome da coleção tem a ortografia correta, no entanto, há um problema no servidor TAXII em Coleção, que rejeita a solicitação.

A possível causa pode ser um temporizador de expiração no Nome da Coleção.
Entre em contato com o fornecedor para verificar esse tipo de inconsistência.



[SSL: CERTIFICATE_VERIFY_FAILED] Falha na verificação do certificado (_ssl.c:590)

<#root>

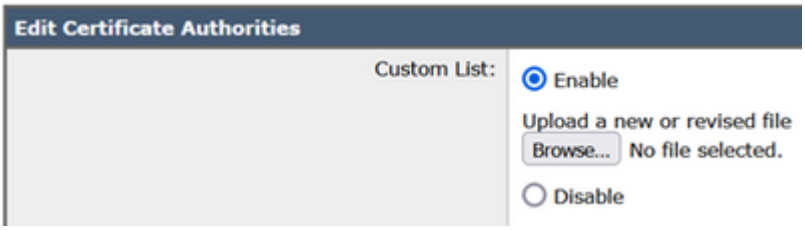
```
(Machine esa03.taclab.krk) (SERVICE)> grep "Sep 8 16:35" threatfeeds
Wed Sep 8 16:35:26 2021 Info: THREAT_FEEDS: A delta poll is scheduled for the source: ETF_Source_Name
Wed Sep 8 16:35:33 2019 Warning: THREAT_FEEDS: Unable to fetch the observables from the source: ETF_Sou
```

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

Solução

Este erro indica falha no certificado.

Para resolver o problema, importe o Certificado na lista de Autoridades de Certificação (CA).
Navegue até **GUI > Rede > Certificados > Editar configurações > Lista personalizada >**
Selecione o modo **Enable** e faça o upload do certificado.



Erro de análise de XML: nenhum elemento encontrado (linha 0)

<#root>

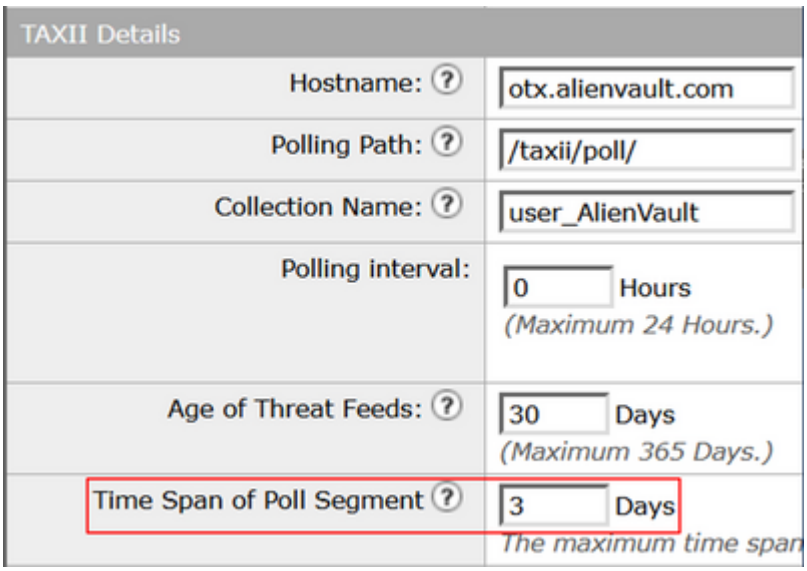
```
(Machine esa03.taclab.krk) (SERVICE)> grep "Aug 21 02:39" threatfeeds
Fri Aug 21 02:39:37 2021 Warning: THREAT_FEEDS: Unable to fetch the observables from the source: ETF_Sou
Fri Aug 21 02:39:37 2021 Info: THREAT_FEEDS: Job failed with exception : Source: ETF_Source_Name.
```

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

Solução

Reduza o valor do intervalo de tempo do segmento de pesquisa da configuração do ESA para 3 a 4 dias.

> **Observação**: isso é uma inconsistência com servidores Anomali para alguns feeds específicos, em que nenhum sinalizador de fim de dados é enviado para interromper os feeds.
> Nesse caso, o ESA configurado com uma fonte ETF da Anomali não pode pesquisar dados por um período de tempo superior a 5 dias.
> Uma solução alternativa válida seria reduzir o valor Time Span do segmento de pesquisa da configuração do ESA.



Falha ao estabelecer uma nova conexão: [Erro 111] Conexão recusada

<#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',))

> **Observação**: "Connection rejected" indica que o cliente não pode se conectar à porta no servidor em execução. Normalmente, isso ocorre quando o servidor escuta na porta errada ou quando a porta não está disponível.

Solução

1. Use o comando **telnet** ou **netstat** via CLI para verificar se a porta apropriada está escutando.
2. Verifique se o Firewall não bloqueia a porta.
3. Verifique se não há erro de configuração de porta ou porta obsoleta no serviço em execução.

Informações Relacionadas

- Guias do usuário final do Cisco Email Security Appliance
- O que são STIX e TAXII
- RFC2741 - Códigos de erro
- Feeds de ameaças externas do workshop do TAC

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.