Solucionar problemas de status de conectividade do Talos

Contents

Introdução

Este documento descreve como solucionar problemas de conectividade do TALOS no FMC e no FDM do Secure Firewall.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Secure Firewall Management Center (FMC)

- Gerenciador de dispositivos do Cisco Secure Firewall (FDM)

- Defesa contra ameaças (FTD) do Cisco Secure Firewall

Componentes Utilizados

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

FMC versão 7.6.0 ou 7.7.0
FDM versão 7.6.0 ou 7.7.0
FTD versão 7.6.0 ou 7.7.0

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.

Informações de Apoio

O Cisco Secure Firewall Management Center (FMC) conta com um certificado do lado do cliente para estabelecer uma conexão segura com os serviços de inteligência contra ameaças do Cisco Talos. Essa autenticação é essencial para que o FMC faça o download de atualizações críticas com êxito, incluindo URL Reputation Databases (URLDBs), Lightweight Security Packages (LSPs) e outros dados de enriquecimento.

Em condições normais de operação, esse certificado é pré-provisionado durante a instalação do software e é projetado para ser renovado automaticamente quando a data de expiração estiver próxima. No entanto, um problema conhecido em determinadas versões do software FMC do firewall seguro da Cisco impede que o processo de renovação automática seja concluído com êxito após 30 de março de 2025. Quando isso acontece, o FMC não pode autenticar com o Talos, o que leva a falhas de conectividade e à incapacidade de recuperar informações atualizadas sobre ameaças.

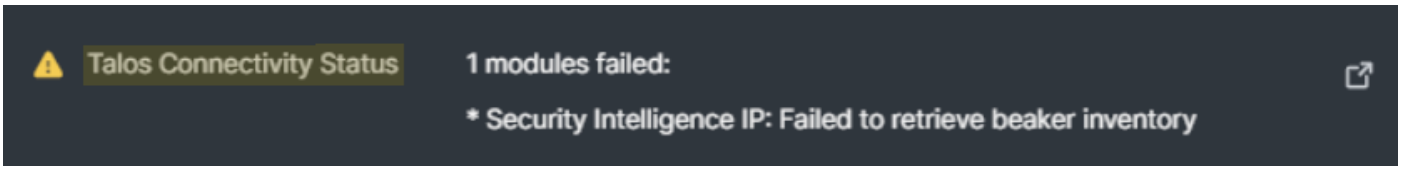
Verificando o status do certificado

GUI do FMC

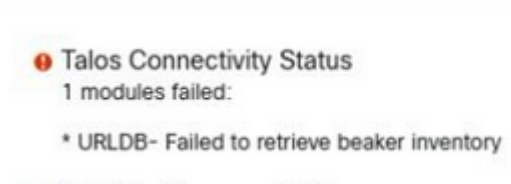
Quando o certificado do lado do cliente não é renovado, o Cisco FMC aciona alertas de integridade para notificar os administradores da interrupção na comunicação com o Cisco Talos. Você pode monitorar esses alertas navegando até System > Health e revisando a seção Status de conectividade do Talos.

Se o sistema for afetado pelo problema de expiração do certificado, você normalmente verá uma destas mensagens de erro:

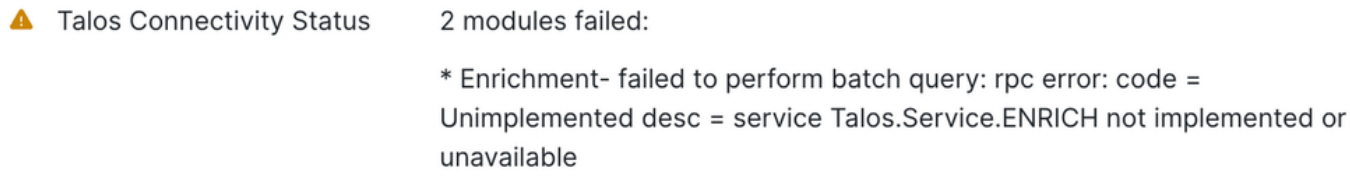
- "LSP - Falha ao recuperar inventário do copo":



- "URLDB - Falha ao recuperar inventário do copo":



- "Enriquecimento - Falha ao executar consulta em lotes":



CLI FMC

Para determinar se o seu dispositivo FMC é afetado por esse problema, acesse o modo especialista e execute o comando para verificar a data de expiração atual do certificado do lado do cliente:

<#root>

```
expert
sudo su
//type the 'FMC CLI admin password'
```

sudo openssl x509 --in /var/sf/beaker3/securefirewall-dev-prod-01_prod.pem --text

Na saída do comando, localize a seção Validade. O campo Não Depois indica a data de

vencimento atual do certificado. Se essa data já tiver passado ou estiver se aproximando, o processo de renovação falhou e é necessário reiniciar o serviço manualmente para iniciar a renovação do certificado.

Exemplo:

<#root>

```
> expert
>sudo su
//type the 'FMC CLI admin password'
openssl x509 --in /var/sf/beaker3/securefirewall-dev-prod-01_prod.pem --text
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 46240369 (0x2c19271)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, ST = California, L = San Jose, O = Cisco Systems Inc., OU = Security, CN = Keym
```

Validity

Not Before: Jan 30 22:32:39 2024 GMT

Not After :

Mar 30 22:32:39 2025 GMT

```
        Subject: CN = SFW76EVAL-prod-01, C = US, ST = California, L = San Jose, O = Cisco, OU = Securit
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
```

Troubleshooting

1. Identifique seu cenário

Versão de software	ID do bug associado	Causa principal
7.6.0 ou 7.7.0	ID de bug da Cisco CSCwo63951	Expiração do certificado / Falha de conectividade
7.6.1+ ou 7.7.10+	ID de bug da Cisco CSCwr23982	Configuração de registro/licenciamento (por exemplo, air-gapped).

2. Solução de problemas para as versões 7.6.0 e 7.7.0

Sintomas

Além dos alertas de integridade mencionados anteriormente, você observa estes comportamentos:

- Erros do FDM Task Manager: "Falha na atualização da nuvem do Snort 3: Sem resposta do servidor de atualização ou tempo limite da conexão."
- Entradas de log: Erros em /ngfw/var/log/messages indicando: Falha ao conectar ao túnel (UUID), erro: Não conectado.
- Status: Atualizações estagnadas na interface do usuário: A tela Preferências de filtragem de URL exibe "Ainda não atualizado".

Solução temporária

Para restaurar os serviços imediatamente, reinicie os processos necessários por meio do modo avançado:

Etapa 1. Acesse a CLI e entre no modo especialista.

Etapa 2. Execute os comandos:

```
expert
sudo su
//type the 'FMC CLI admin password'
pmtool restartbyid talosAgent
pmtool restartbyid beaker3
```

Note: Essa solução alternativa aciona um certificado válido por apenas cinco dias. Você deve repetir esse processo a cada cinco dias até que uma correção permanente seja aplicada.

Resolução Permanente

Para resolver esse problema permanentemente, verifique se estas condições foram atendidas:

Etapa 1. Verificar a Conectividade: Verifique se o equipamento tem acesso de saída a https://api-sse.cisco.com. Para fazer isso, acesse a CLI do FMC, entre no modo especialista e execute os comandos:

Etapa 1.1. Testar a resolução DNS:

<#root>

```
expert
sudo su
//type the 'FMC CLI admin password'

nslookup api-sse.cisco.com
```

Etapa 1.2. Testar o acesso à porta TCP:

<#root>

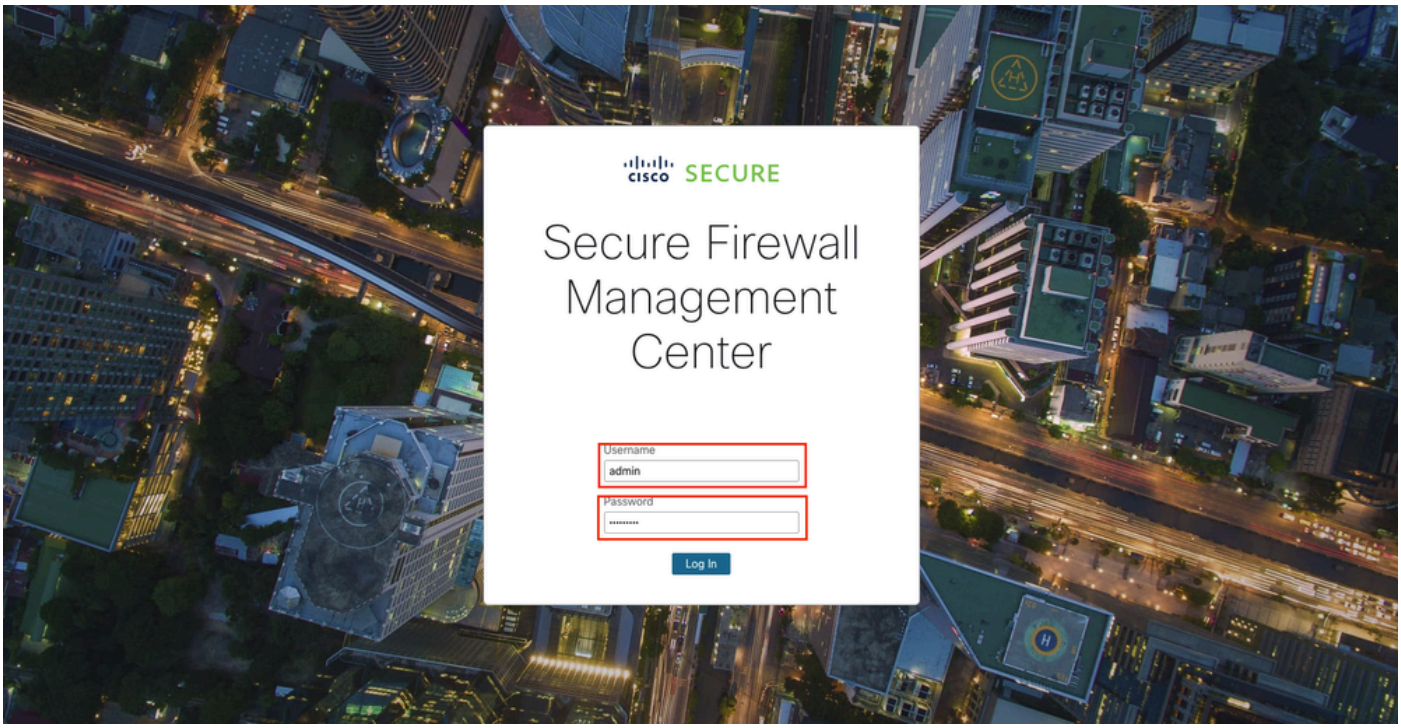
```
 expert
sudo su
//type the 'FMC CLI admin password'

telnet api-sse.cisco.com 443
```

Note: Verifique se o acesso HTTPS de saída (TCP 443) a https://api-sse.cisco.com é permitido através de todos os firewalls, proxies ou dispositivos de segurança de upstream.

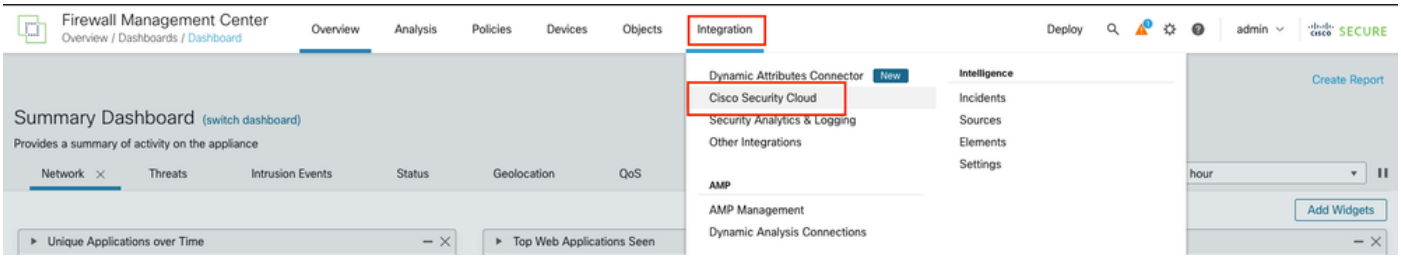
Etapa 2. Ativar a telemetria: Verifique se a telemetria da CSN (Customer Success Network) está habilitada para que o SSEConnector possa obter um novo certificado. Para ativar o CSN no FMC, siga estas etapas:

Passo 2.1. Inicie a sessão na interface gráfica do usuário do FMC abrindo um navegador da Web e navegando até a URL do FMC (por exemplo: https://<FMC_IP_or_Hostname>). Insira seu nome de usuário e senha para acessar o

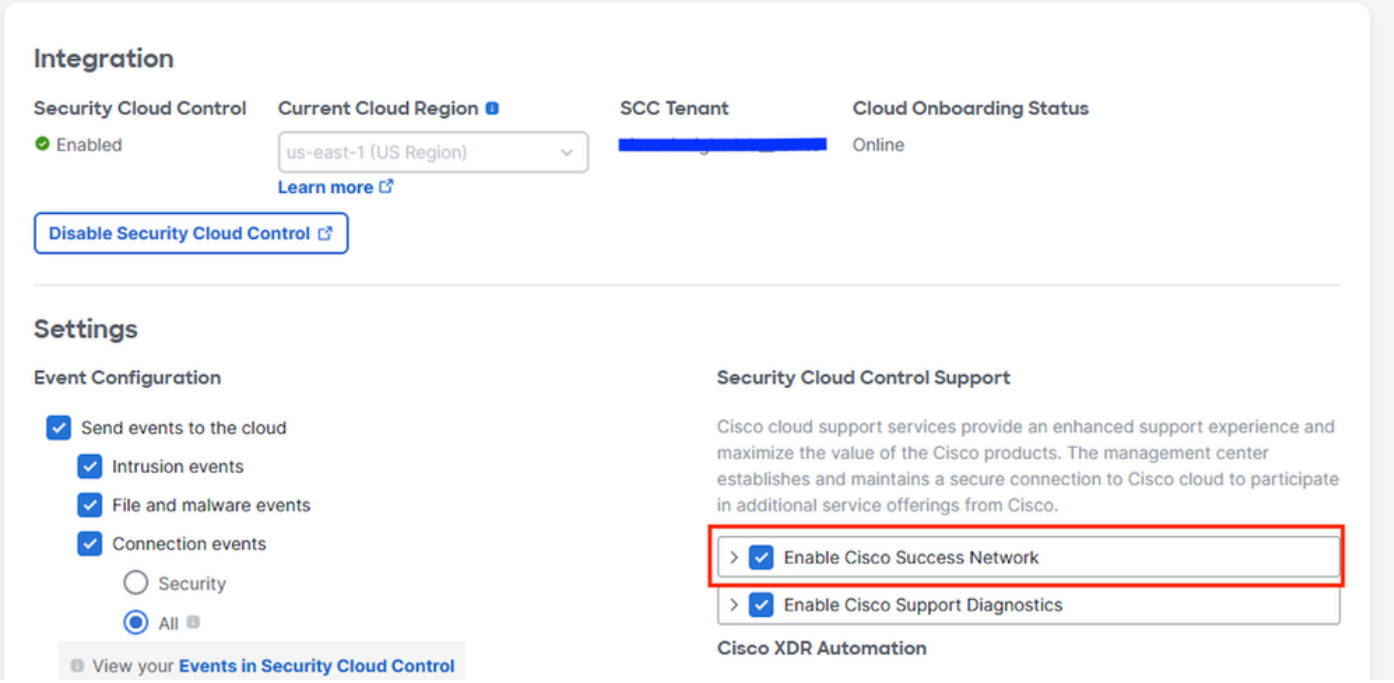
Interface GUI do FMC.



Etapa 2.2. Navegue até Cisco Success Network Settings: No menu principal, selecione Integration > Cisco Security Cloud.



Etapa 2.3. Localize e ative a opção Cisco Success Network: Para isso, marque a caixa Enable Cisco Success Network para ativar a telemetria.



Etapa 3. Instalar Atualizações: Instale o GeoDB 2025-04-03-094 ou VDB 406 (ou posterior). Isso dispara a instalação de um novo certificado de 365 dias.

Note: Alta disponibilidade (HA). Em um par HA, o processo do SSEConnector não é executado na unidade em standby. Para atualizar o FMC em espera, execute uma troca de função para que o FMC em espera fique ativo e instale a atualização necessária do VDB ou do GeoDB.

---

3. Solução de problemas para as versões 7.6.1+ e 7.7.10+

Esse problema geralmente ocorre em ambientes sem registro padrão do Cisco Security Cloud (CSC), como aqueles que usam licenças de avaliação, SSM On-Prem, PLR ou SLR.

Recursos afetados

- Atualizações automáticas/manuais do LSP (Lightweight Security Package).
- Atualizações de conteúdo de banco de dados de filtragem de URL e pesquisas na nuvem.
- Enriquecimento Talos de eventos de conexão.

Ações recomendadas

1. Ambiente Padrão: Registre o FMC via Integração > Cisco Security Cloud. O registro aciona automaticamente um novo download de certificado em 30 minutos.

2. Atualizações Manuais: Se as atualizações automáticas falharem, baixe manualmente o LSP mais recente de software.cisco.com e instale-o diretamente no FMC.

3. Ambientes Com Distorção De Ar: Se a sua rede não tiver acesso à Internet, o módulo de integridade Status de conectividade do Talos se tornará irrelevante. Neste cenário, desabilite este módulo específico na sua política de integridade aplicada.

Informações Relacionadas

- Para obter assistência adicional, entre em contato com o Cisco Technical Assistance Center (TAC). É necessário um contrato de suporte válido: Cisco Worldwide Support Contacts.

- Suporte e downloads da Cisco: Suporte técnico e downloads da Cisco

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.