排除Talos连接状态故障

目录

简介

本文档介绍如何解决安全防火墙FMC和FDM上的TALOS连接问题。

先决条件

要求

Cisco 建议您了解以下主题：

- Cisco Secure Firewall Management Center (FMC)
- Cisco Secure Firewall Device Manager (FDM)

- Cisco Secure Firewall Threat Defense (FTD)

使用的组件

本文档中的信息基于以下软件和硬件版本：

FMC版本7.6.0或7.7.0
FDM 7.6.0或7.7.0版
FTD版本7.6.0或7.7.0

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

思科安全防火墙管理中心(FMC)依靠客户端证书与思科Talos威胁情报服务建立安全连接。此身份验证对于FMC成功下载关键更新至关重要，这些更新包括URL信誉数据库(URLDB)、轻量级安全包(LSP)和其他丰富数据。

在正常操作条件下，此证书在软件安装期间预先调配，并设计为在接近到期日期时自动续订。但是，在某些思科安全防火墙FMC软件版本中存在一个已知问题，导致自动续订流程无法在2025年3月30日之后成功完成。发生这种情况时，FMC无法通过Talos进行身份验证，从而导致连接失败和无法检索更新的威胁情报。

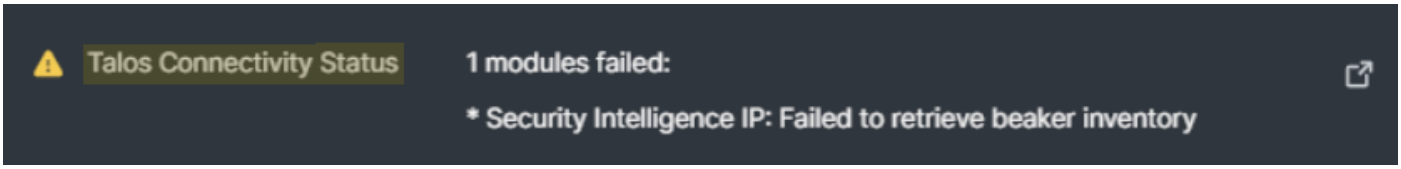
验证证书状态

FMC GUI

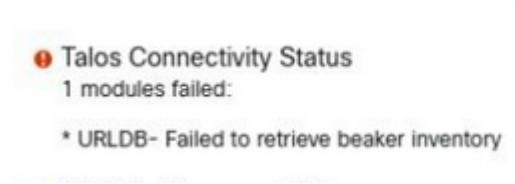
当客户端证书无法续订时，思科FMC会触发运行状况警报，通知管理员与思科Talos的通信中断。您可以通过导航到System > Health并查看Talos Connectivity Status部分来监控这些警报。

如果系统受到证书过期问题的影响，您通常会看到以下错误消息之一：

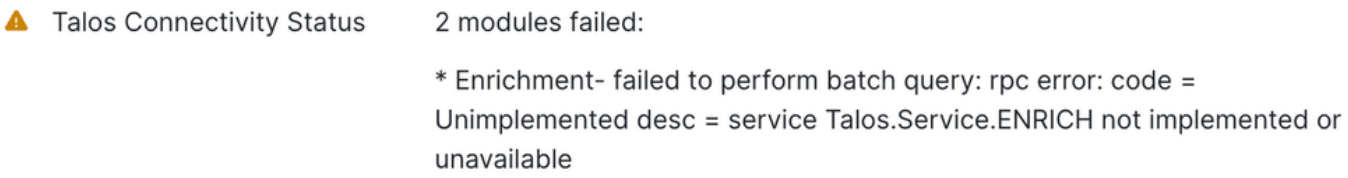
- “LSP — 无法检索烧杯库存”：



- "URLDB — 无法检索烧杯库存":



- "浓缩 — 无法执行批处理查询":



FMC CLI

要确定您的FMC设备是否受到此问题的影响，请访问expert mode并运行命令以验证客户端证书的当前到期日期：

<#root>

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

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

在命令输出中，找到Validity部分。Not After字段指示证书的当前到期日期。如果此日期已过或即将到期，续订流程失败，需要手动重新启动服务以启动证书续订。

示例：

<#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

故障排除

1.确定您的场景

软件版本	关联的Bug ID	主要原因
7.6.0 或 7.7.0	Cisco Bug ID CSCwo63951	证书过期/连接故障
7.6.1+或7.7.10+	Cisco Bug ID CSCwr23982	注册/许可配置（例如，气隙）。

2.版本7.6.0和7.7.0的故障排除

症状

除了前面提到的运行状况警报，您还会观察到以下行为：

- FDM任务管理器错误："Snort 3云更新失败：没有来自更新服务器的响应或连接超时。"
- 日志条目：/ngfw/var/log/messages中的错误指示：无法连接到隧道(UUID)，错误：未连接.
- 状态:UI中的停滞更新：URL过滤首选项屏幕显示"尚未更新"。

临时解决方法

要立即恢复服务，请通过专家模式重新启动所需的进程：

步骤1.访问CLI并进入专家模式。

步骤2.运行以下命令：

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

注意：此解决方法触发有效期只有五天的证书。您必须每五天重复此过程，直到应用永久修复为止。

永久解决方案

要永久解决此问题，请确保满足以下条件：

步骤1.检验连通性：确保设备对https://api-sse.cisco.com具有出站访问权限。为此，请访问FMC CLI，进入专家模式，然后运行以下命令：

步骤1.1.测试DNS解析：

<#root>

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

nslookup api-sse.cisco.com
```

步骤1.2.测试TCP端口访问：

<#root>

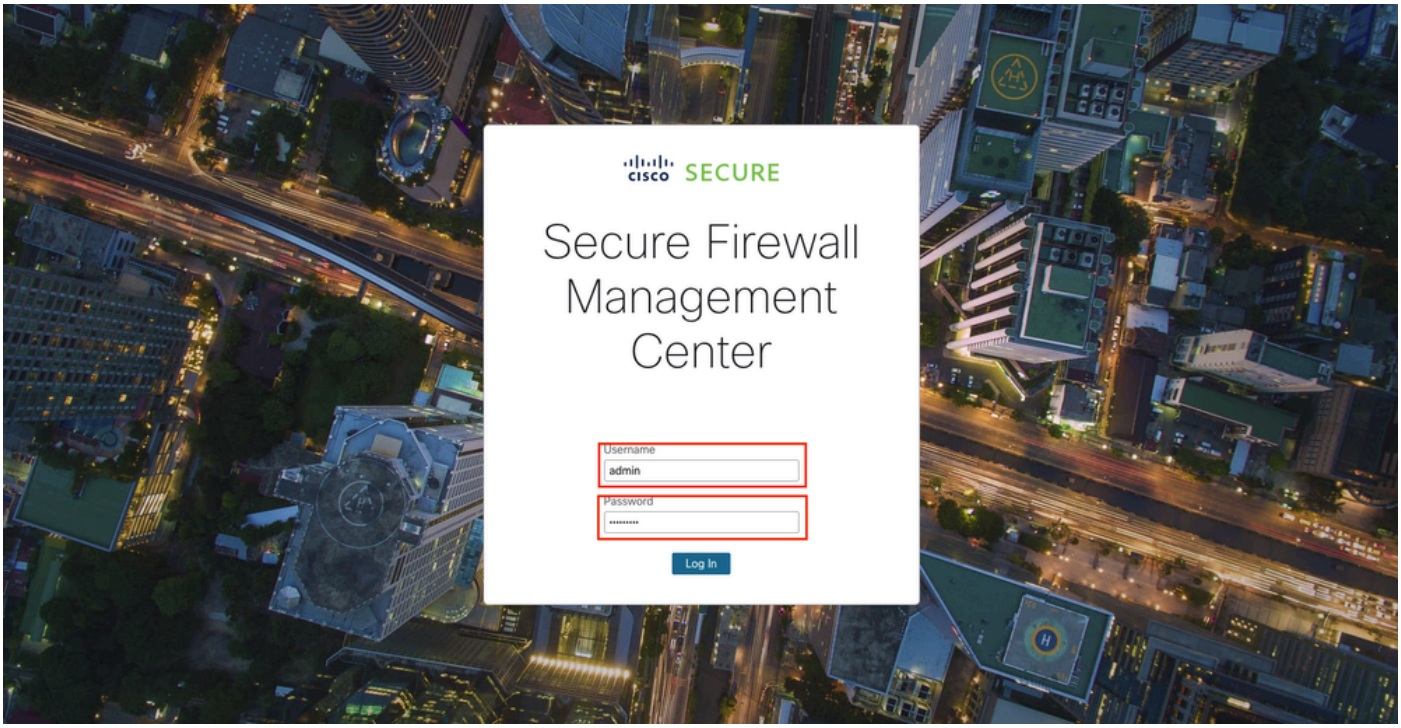
```
 expert
sudo su
//type the 'FMC CLI admin password'

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

注意：验证所有上游防火墙、代理或安全设备是否允许对https://api-sse.cisco.com的出站HTTPS(TCP 443)访问。

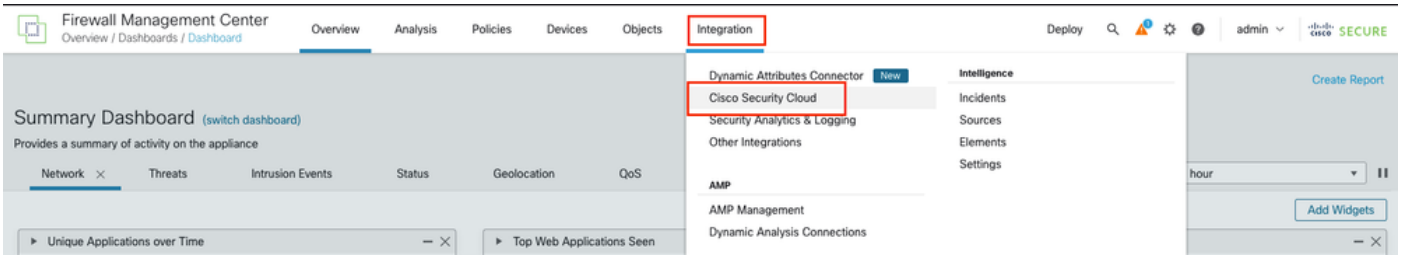
步骤2.启用遥测：确保已启用客户成功网络(CSN)遥感勘测，以便SSEConnector可以获取新证书。要在FMC上启用CSN，请执行以下步骤：

第2.1步：打开Web浏览器并导航到FMC URL，登录到FMC GUI(例如：https://<FMC_IP_or_Hostname>)。 输入您的用户名和密码以访问

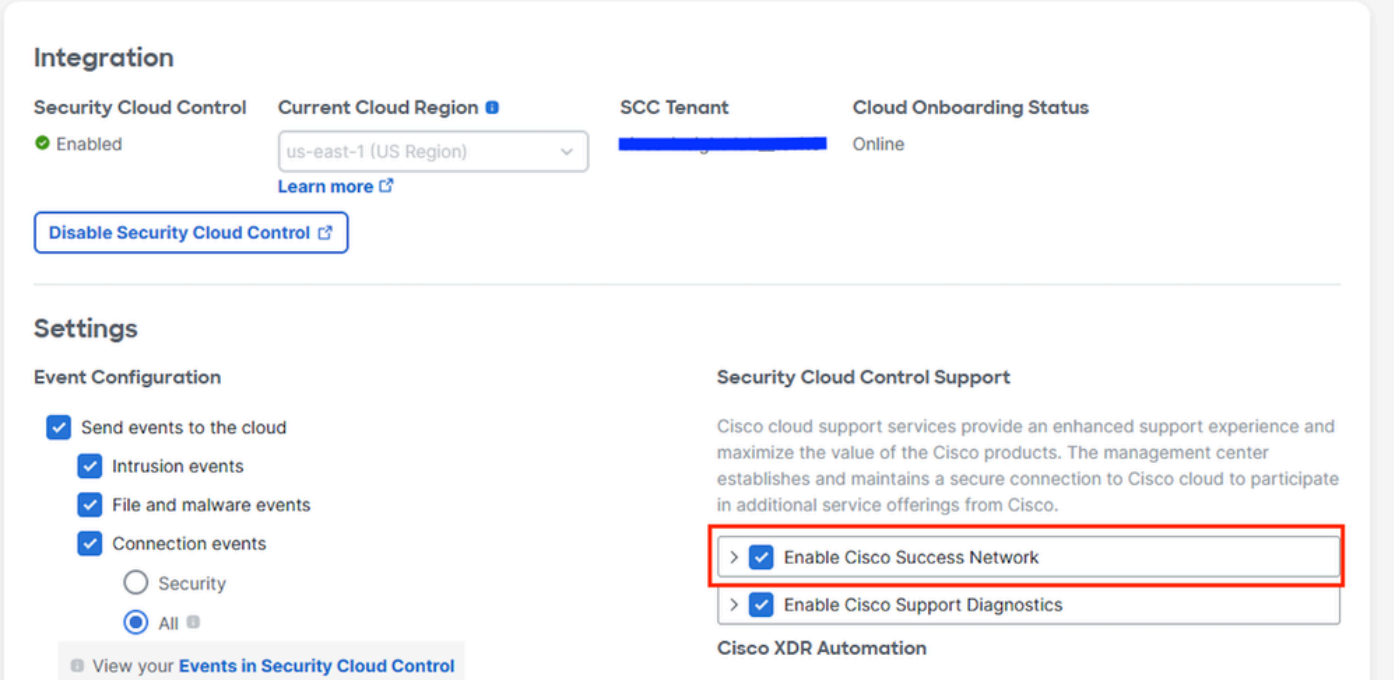
FMC GUI界面。



步骤2.2.导航至Cisco Success Network Settings:从主菜单中选择Integration> Cisco Security Cloud。



步骤2.3.查找并启用标记为Cisco Success Network的选项：为此，请选中Enable Cisco Success Network复选框以激活遥测。



步骤3.安装更新：安装GeoDB 2025-04-03-094或VDB 406（或更高版本）。 这会触发安装新的365天证书。

注意：高可用性(HA)。 在HA对中，SSEConnector进程不在备用设备上运行。要更新备用FMC，请执行角色切换以使备用变为活动状态，然后安装所需的VDB或GeoDB更新。

3.7.6.1+和7.7.10+版本的故障排除

此问题通常发生在没有标准思科安全云(CSC)注册的环境中，例如使用评估许可证、SSM内部部署、PLR或SLR的环境。

受影响的功能

- 自动/手动轻型安全包(LSP)更新。
- URL过滤数据库内容更新和云查找。
- Talos丰富连接事件。

推荐的操作

1.标准环境：通过集成>思科安全云注册。注册会在30分钟内自动触发新证书下载。

2.手动更新：如果自动更新失败，请从software.cisco.com手动下载最新的LSP并将其直接安装到FMC上。

3.气隙环境：如果您的网络无法访问Internet，则Talos连接状态运行状况模块变得无关紧要。在此场景中，在应用的运行状况策略中禁用此特定模块。

相关信息

- 如需获取其他帮助，请联系思科技术支持中心 (TAC)。联系时需要提供有效的支持合同：思科全球支持联系信息

- 思科支持和下载:思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。