Solución de problemas de estado de conectividad Talos

Contenido

Introducción

Este documento describe cómo resolver problemas de conectividad TALOS en Secure Firewall FMC y FDM.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Secure Firewall Management Center (FMC)

- Cisco Secure Firewall Device Manager (FDM)

- Cisco Secure Firewall Threat Defence (FTD)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

FMC versión 7.6.0 o 7.7.0
FDM versión 7.6.0 o 7.7.0
FTD versión 7.6.0 o 7.7.0

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Cisco Secure Firewall Management Center (FMC) se basa en un certificado del cliente para establecer una conexión segura con los servicios de inteligencia de amenazas de Cisco Talos. Esta autenticación es esencial para que el FMC descargue correctamente las actualizaciones críticas, incluidas las bases de datos de reputación de URL (URLDB), los paquetes de seguridad ligeros (LSP) y otros datos de enriquecimiento.

En condiciones de funcionamiento normales, este certificado se suministra previamente durante la instalación del software y está diseñado para renovarse automáticamente a medida que se aproxima su fecha de vencimiento. Sin embargo, un problema conocido en determinadas versiones del software Cisco Secure Firewall FMC impide que el proceso de renovación automática se complete correctamente después del 30 de marzo de 2025. Cuando esto sucede, el FMC no puede autenticarse con Talos, lo que provoca fallos de conectividad y la incapacidad de recuperar la inteligencia de amenazas actualizada.

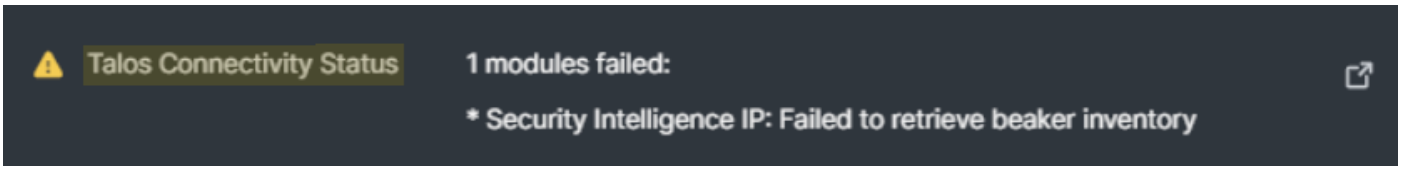
Verificación del estado del certificado

GUI de FMC

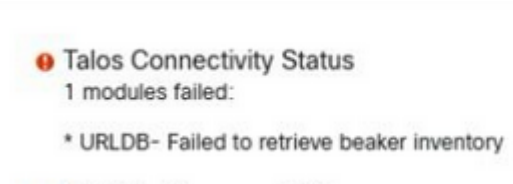
Cuando el certificado del cliente no se renueva, Cisco FMC activa alertas de estado para notificar a los administradores de la interrupción en la comunicación con Cisco Talos. Puede supervisar estas alertas navegando hasta System > Health y revisando la sección Talos Connectivity Status.

Si el problema de expiración del certificado afecta al sistema, normalmente verá uno de estos mensajes de error:

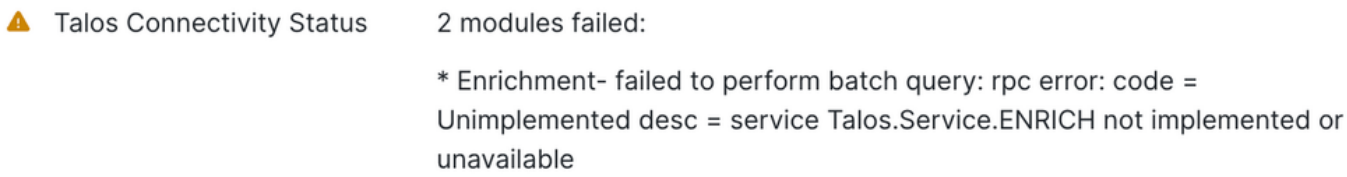
- "LSP - Fallo al recuperar el inventario del vaso de precipitados":



- "URLDB - No se pudo recuperar el inventario del vaso de precipitados":



- "Enriquecimiento - Fallo al realizar la consulta por lotes":



CLI de FMC

Para determinar si su dispositivo FMC está afectado por este problema, acceda al modo experto y ejecute el comando para verificar la fecha de vencimiento actual del certificado del lado del 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

En el resultado del comando, busque la sección Validity. El campo No después de indica la fecha

de vencimiento actual del certificado. Si esta fecha ya ha pasado o se acerca, el proceso de renovación ha fallado y es necesario reiniciar el servicio manualmente para iniciar la renovación del certificado.

Ejemplo:

<#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
```

Troubleshoot

1. Identifique su situación

Versión del software	ID de bug asociado	Causa principal
7.6.0 o 7.7.0	ID de bug de Cisco CSCwo63951	Expiración del certificado/Fallo de conectividad
7.6.1+ o 7.7.10+	ID de bug de Cisco CSCwr23982	Configuración de registro/licencias (por ejemplo, Air-Gap).

2. Resolución de problemas para las versiones 7.6.0 y 7.7.0

Síntomas

Además de las alertas de estado mencionadas anteriormente, observará estos comportamientos:

- Errores del administrador de tareas de FDM: "Falló la actualización de nube de Snort 3: No hay respuesta del servidor de actualización o se agota el tiempo de espera de la conexión."
- Entradas de registro: Errores en /ngfw/var/log/messages que indican: Error al conectar con el túnel (UUID), error: No conectado.
- Estado: Actualizaciones estancadas en la interfaz de usuario: La pantalla Preferencias de filtrado de URL muestra "Aún no actualizado".

Solución temporal

Para restaurar los servicios inmediatamente, reinicie los procesos necesarios a través del modo Experto:

Paso 1. Acceda a la CLI e ingrese al modo experto.

Paso 2. Ejecute los comandos:

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

Nota: Esta solución alternativa activa un certificado válido solo para cinco días. Debe repetir este proceso cada cinco días hasta que se aplique una corrección permanente.

Resolución permanente

Para resolver este problema de forma permanente, asegúrese de que se cumplen estas

condiciones:

Paso 1. Verifique la conectividad: Asegúrese de que el dispositivo tiene acceso saliente a https://api-sse.cisco.com. Para ello, acceda a la CLI de FMC, entre en el modo experto y ejecute los comandos:

Paso 1.1. Resolución de DNS de prueba:

<#root>

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

nslookup api-sse.cisco.com

Paso 1.2. Probar el acceso al puerto TCP:

<#root>

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

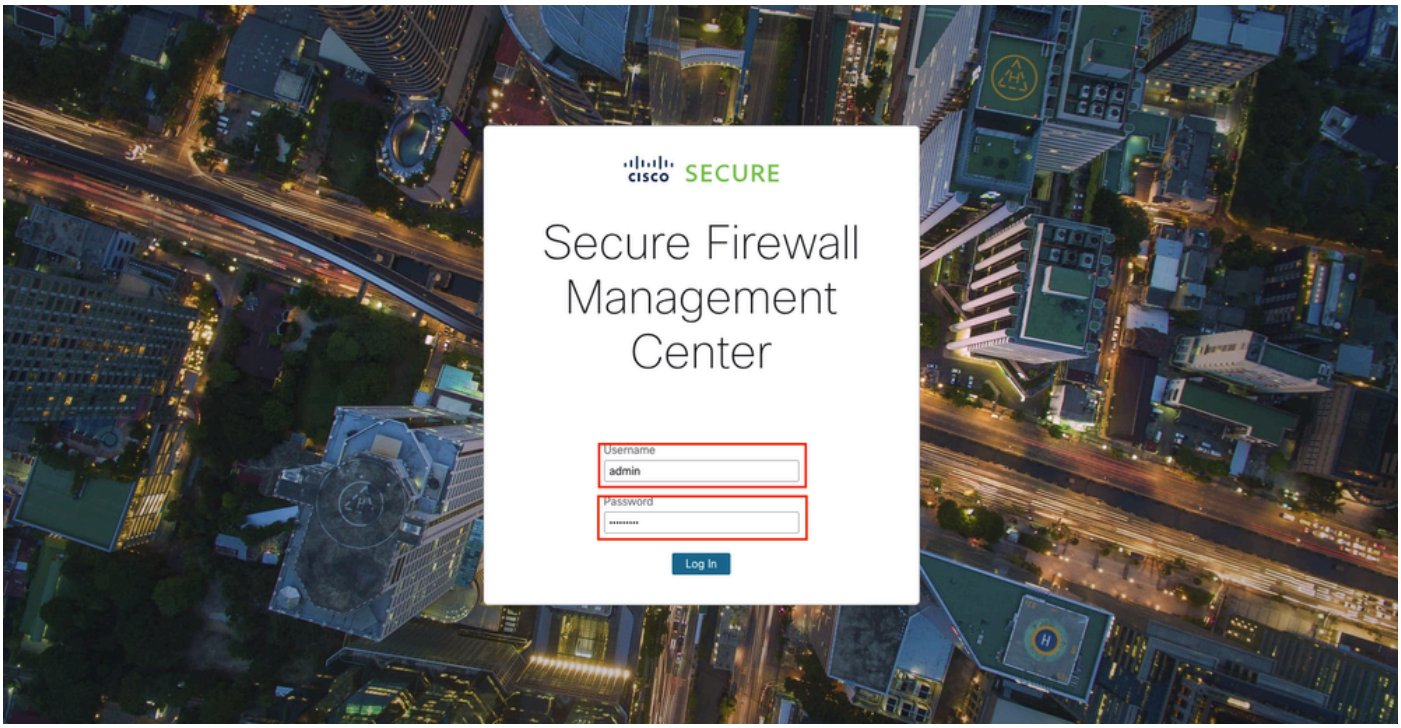
telnet api-sse.cisco.com 443

Nota: Compruebe que se permite el acceso HTTPS (TCP 443) saliente a https://api-sse.cisco.com a través de todos los firewalls ascendentes, proxies o dispositivos de seguridad.

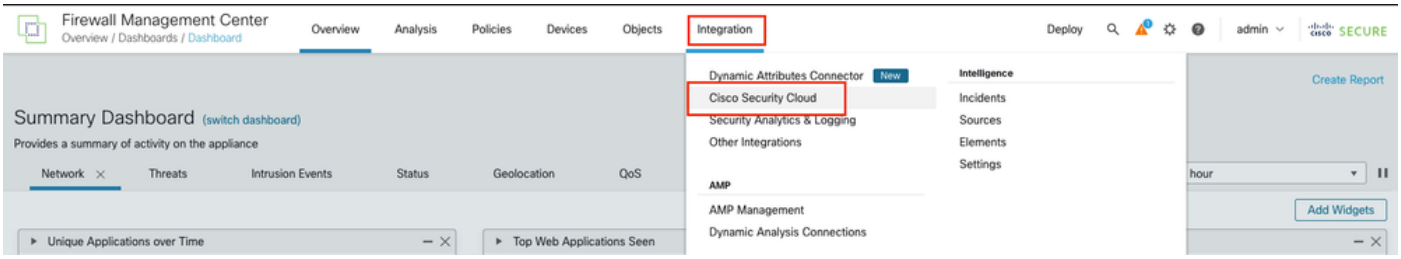
Paso 2. Habilitar telemetría: Asegúrese de que la telemetría de Customer Success Network (CSN) esté activada para que SSEConnector pueda obtener un nuevo certificado. Para activar el CSN en el FMC, siga estos pasos:

Paso 2.1. Inicie sesión en la GUI del CSP abriendo un navegador web y navegando hasta la URL del CSP (por ejemplo: https://<FMC_IP_or_Hostname>). Introduzca su nombre de usuario y contraseña para acceder al

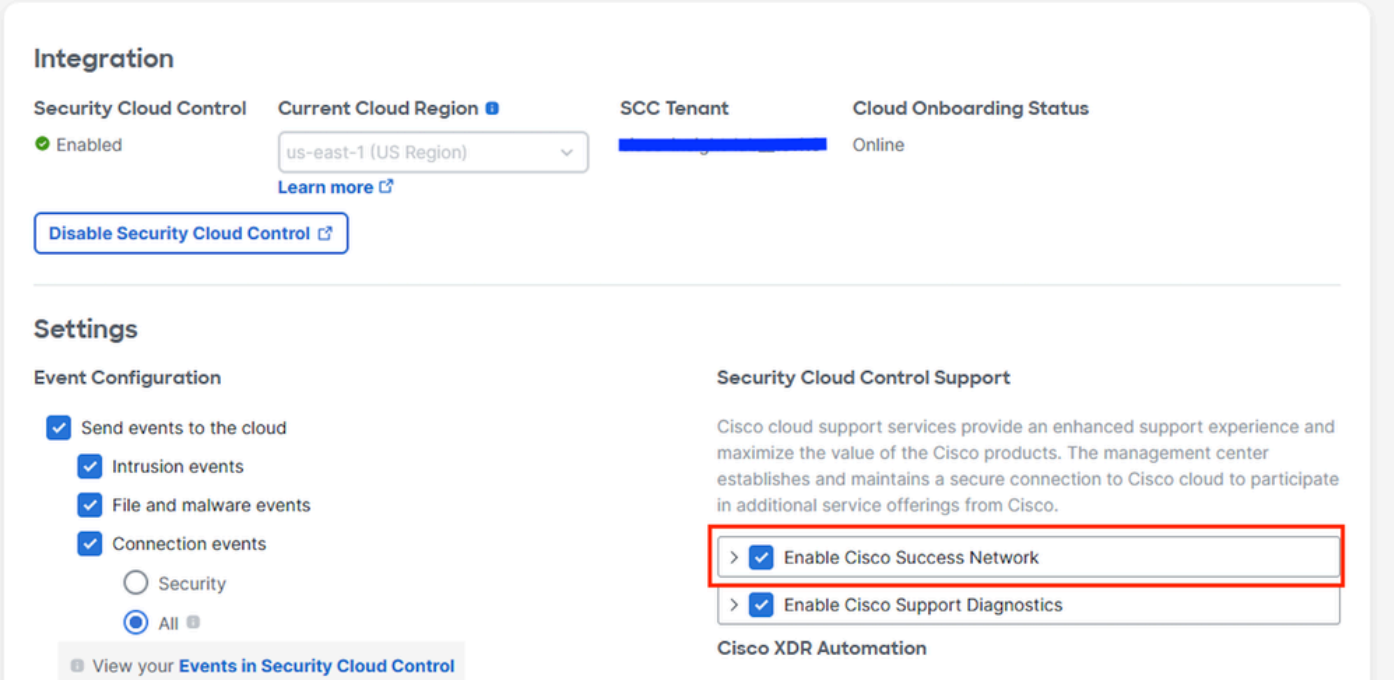
Interfaz GUI de FMC.



Paso 2.2. Navegue hasta Cisco Success Network Settings: En el menú principal, seleccione Integration > Cisco Security Cloud.



Paso 2.3. Busque y active la opción denominada Cisco Success Network: Para ello, marque la casilla de verificación Enable Cisco Success Network para activar la telemetría.



Paso 3. Instalar actualizaciones: Instale GeoDB 2025-04-03-094 o VDB 406 (o posterior). Esto activa la instalación de un nuevo certificado de 365 días.

Nota: Alta disponibilidad (HA). En un par HA, el proceso SSEConnector no se ejecuta en la unidad en espera. Para actualizar el FMC en espera, realice un cambio de función para que el modo en espera se active y, a continuación, instale la actualización de VDB o GeoDB necesaria.

---

3. Resolución de problemas para las versiones 7.6.1+ y 7.7.10+

Este problema suele producirse en entornos sin registro estándar de Cisco Security Cloud (CSC), como los que utilizan licencias de evaluación, SSM en las instalaciones, PLR o SLR.

Funciones afectadas

- Actualizaciones automáticas/manuales del paquete de seguridad ligero (LSP).
- Actualizaciones de contenido de base de datos de filtrado de URL y búsquedas en la nube.
- Enriquecimiento de Talos de eventos de conexión.

Acciones recomendadas

1. Entorno estándar: Registre el FMC mediante Integration > Cisco Security Cloud. El registro activa automáticamente una nueva descarga de certificado en 30 minutos.

2. Actualizaciones manuales: Si las actualizaciones automáticas fallan, descargue el último LSP manualmente desde software.cisco.com e instálelo directamente en el FMC.

3. Entornos con brechas de aire: Si su red no tiene acceso a Internet, el módulo de estado de conectividad de Talos se vuelve irrelevante. En este escenario, inhabilite este módulo específico dentro de su política de salud aplicada.

Información Relacionada

- Para obtener asistencia adicional, póngase en contacto con el centro de asistencia técnica Cisco Technical Assistance Center (TAC). Se necesita un contrato de asistencia válido: Contactos de asistencia globales de Cisco.

- Soporte y descargas de Cisco: Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).