Troubleshooting de SLIC Channel Down System Alarm

Contenido

Introducción

Este documento describe cómo resolver problemas de alarmas del sistema "SLIC Channel Down" de Secure Network Analytics (SNA).

Prerequisites

Requirements

Cisco recomienda que tenga conocimientos básicos de SNA.

SLIC significa "Stealthwatch Labs Intelligence Center"

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

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.

Procedimiento

La alarma "SLIC Channel Down" se activa cuando SNA Manager no puede obtener actualizaciones de fuentes de los Threat Intelligence Servers, anteriormente SLIC. Para entender mejor qué causó la

interrupción de las actualizaciones de la fuente, proceda como se indica a continuación:

1. Conéctese al Administrador SNA a través de SSH e inicie sesión con **root** credenciales.
2. Analice la **/lancope/var/smc/log/smc-core.log** archivo y buscar los registros del tipo **SlicFeedGetter**.

Una vez que encuentre los registros relevantes, continúe con la siguiente sección dado que hay múltiples condiciones que pueden causar que esta alarma se active.

Registros de errores comunes

Los registros de errores más comunes que se ven en la **smc-core.log** relacionados con la alarma de caída de canal SLIC son:

â€ƒ

Tiempo de espera de conexión agotado

<#root>

```
2023-01-03 22:43:28,533 INFO [SlicFeedGetter] Performing request to get Threat Feed update file.
2023-01-03 22:43:28,592 INFO [SlicFeedGetter] Threat Feed Host 'lancope.flexnetoperations.com' resolves
2023-01-03 22:43:28,592 INFO [SlicFeedGetter] Threat Feed URL: /control/lncp/LancopeDownload?token=20190
2023-01-03 22:45:39,604
```

ERROR [SlicFeedGetter] Getting Threat Feed update failed with exception.

org.apache.http.conn.HttpHostConnectException: Connect to lancope.flexnetoperations.com:443 [lancope.fle

â€ƒ

No se puede encontrar una ruta de certificación válida para el destino solicitado

<#root>

```
2023-01-04 00:27:50,497 INFO [SlicFeedGetter] Performing request to get Threat Feed update file.
2023-01-04 00:27:50,502 INFO [SlicFeedGetter] Threat Feed Host 'lancope.flexnetoperations.com' resolves
2023-01-04 00:27:50,502 INFO [SlicFeedGetter] Threat Feed URL: /control/lncp/LancopeDownload?token=20190
2023-01-04 00:27:51,239
```

ERROR [SlicFeedGetter] Getting Threat Feed update failed with exception.

javax.net.ssl.SSLHandshakeException: PKIX path building failed: sun.security.provider.certpath.SunCertPa

Fallo de enlace

<#root>

```
2023-01-02 20:00:49,427 INFO [SlicFeedGetter] Performing request to get Threat Feed update file.
```

```
2023-01-02 20:00:49,433 INFO [SlicFeedGetter] Threat Feed Host 'lancope.flexnetoperations.com' resolves
2023-01-02 20:00:49,433 INFO [SlicFeedGetter] Threat Feed URL: /control/lncp/LancopeDownload?token=20190
```

2023-01-02 20:00:50,227 ERROR [SlicFeedGetter] Getting Threat Feed update failed with exception.

javax.net.ssl.SSLHandshakeException: Handshake failed

Pasos a seguir

Las actualizaciones de la fuente de inteligencia de amenazas pueden interrumpirse debido a diferentes condiciones. Lleve a cabo los siguientes pasos de validación para asegurarse de que el administrador SNA cumple los requisitos.

Paso 1. Validar estado de licencia inteligente

Desplácese hasta **Central Management > Smart Licensing** y garantizar que el estado de la licencia de fuente de amenazas es **Authorized.**

â€ƒ

Paso 2. Comprobar la resolución del sistema de nombres de dominio (DNS)

Asegúrese de que el administrador SNA pueda resolver correctamente la dirección IP para **lancope.flexnetoperations.com** and esdhttp.flexnetoperations.com

â€ƒ

Paso 3. Verificar la conectividad con los servidores de fuentes de inteligencia de amenazas

Asegúrese de que el Administrador de SNA tenga acceso a Internet y de que se permita la conectividad con los Servidores de inteligencia de amenazas que se enumeran a continuación:

Puerto y Protocolo	Fuente	Destino
443/TCP	Administrador SNA	esdhttp.flexnetoperations.com lancope.flexnetoperations.com

---

> **Nota**: Si el administrador SNA no tiene permiso para tener acceso directo a Internet, asegúrese de que la configuración de proxy para el acceso a Internet esté en su lugar.

â€ƒ

Paso 4. Desactivar inspección/descifrado de capa de conexión segura (SSL)

Los errores segundo y tercero descritos en la **Common Error Logs** puede producirse cuando el Administrador de SNA no recibe el certificado de identidad correcto o la cadena de confianza correcta utilizada por los

servidores de fuente de inteligencia de amenazas. Para evitarlo, asegúrese de que no se realiza ninguna inspección/descifrado SSL en toda la red (mediante firewalls o servidores proxy compatibles) para las conexiones entre el administrador SNA y los servidores de inteligencia de amenazas enumerados en la **Verify Connectivity to the Threat Intelligence Feed Servers** sección.

Si no está seguro de si se realiza la inspección/descifrado SSL en la red, puede recopilar una captura de paquetes entre la dirección IP del administrador SNA y la dirección IP de los servidores de inteligencia de amenazas y analizar la captura para verificar el certificado recibido. Para ello, realice lo siguiente:

1. Conéctese al Administrador SNA por SSH e inicie sesión con **root** credenciales.
2. Ejecute uno de los dos comandos que se enumeran a continuación (el comando a ejecutar depende de si el administrador SNA utiliza o no un servidor proxy para el acceso a Internet):

```
tcpdump -w /lancope/var/tcpdump/slic_issue.pcap -nli eth0 host 64.14.29.85
tcpdump -w /lancope/var/tcpdump/slic_issue2.pcap -nli eth0 host [IP address of Proxy Server]
```

3. Deje que la captura se ejecute durante 2-3 minutos y luego detenerlo.
4. Transfiera el archivo generado fuera del Administrador de SNA para su análisis. Esto se puede conseguir con el protocolo de copia segura (SCP).

â€ƒ

Defectos relacionados

Hay un defecto conocido que puede afectar la conexión a los servidores SLIC:

- La comunicación SMC SLIC puede agotar el tiempo de espera y fallar si el puerto de destino 80 está bloqueado. Consulte Cisco bug ID CSCwe08331

Información Relacionada

- Para obtener asistencia adicional, póngase en contacto con el Technical Assistance Center (TAC). Se necesita un contrato de soporte válido: Contactos de soporte a nivel mundial de Cisco.
- También puede visitar Cisco Security Analytics Community aquí.
- Soporte Técnico y Documentación - Cisco Systems

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).