Identificar e Solucionar Problemas do Alarme de Sistema de Canal SLIC Desativado

Contents

Introduction

Este documento descreve como solucionar problemas de alarmes do sistema "Canal SLIC Desativado" do Secure Network Analytics (SNA).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento básico de SNA.

SLIC significa "Stealthwatch Labs Intelligence Center"

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Procedimento

O alarme "Canal SLIC desativado" é acionado quando o Gerenciador SNA não consegue obter atualizações de feed dos Threat Intelligence Servers, anteriormente SLIC. Para entender melhor o que causou a interrupção das atualizações do feed, faça o seguinte:

1. Conecte-se ao SNA Manager via SSH e faça login com **root** credenciais.
2. Analise a **/lancope/var/smc/log/smc-core.log** arquivo e procurar os logs do tipo **SlicFeedGetter.**

Depois de encontrar os logs relevantes, continue na próxima seção, considerando que há várias condições que podem fazer com que esse alarme seja disparado.

Logs de erro comuns

Os logs de erros mais comuns vistos no **smc-core.log** relacionados ao alarme SLIC Channel Down são:

â€ƒ

Tempo limite da conexão esgotado

<#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

Não é possível localizar um caminho de certificação válido para o 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

Falha no handshake

<#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
```

Etapas para executar

As atualizações do feed de inteligência de ameaças podem ser interrompidas devido a condições diferentes. Execute as próximas etapas de validação para garantir que seu SNA Manager atenda aos requisitos.

Etapa 1. Validar Status do Smart Licensing

Navegue até **Central Management > Smart Licensing** e garantir que o status da licença do Threat Feed seja **Authorized.**

â€ƒ

Etapa 2. Verificar a Resolução do Sistema de Nomes de Domínio (DNS)

Certifique-se de que o Gerenciador SNA possa resolver com êxito o endereço IP para **lancope.flexnetoperations.com** and esdhttp.flexnetoperations.com

â€ƒ

Etapa 3. Verifique a conectividade com os servidores de feed de inteligência de ameaças

Verifique se o Gerenciador SNA tem acesso à Internet e se a conectividade com os servidores de inteligência de ameaças listados a seguir tem permissão:

Porta e protocolo	Fonte	Destino
443/TCP	Gerenciador SNA	esdhttp.flexnetoperations.com lancope.flexnetoperations.com

---

> **Observação**: se o Gerenciador SNA não tiver permissão para ter acesso direto à Internet, verifique se a configuração do Proxy para acesso à Internet está em vigor.

â€ƒ

Etapa 4. Desabilitar Inspeção/Descriptografia de SSL

O segundo e o terceiro erros descritos no **Common Error Logs** pode ocorrer quando o Gerenciador do SNA não recebe o certificado de identidade correto ou a cadeia de confiança correta usada pelos servidores de feed de inteligência de ameaças. Para evitar isso, certifique-se de que nenhuma Inspeção/Descriptografia SSL seja executada em sua rede (por Firewalls ou servidores proxy compatíveis) para conexões entre o SNA Manager e os servidores de inteligência de ameaças listados no **Verify Connectivity to the Threat Intelligence Feed Servers** seção.

Se você não tiver certeza se a Inspeção/Descriptografia SSL é executada em sua rede, você pode coletar uma

captura de pacote entre o endereço IP do SNA Manager e o endereço IP do Threat Intelligence Servers e analisar a captura para verificar o certificado recebido. Para isso, faça o seguinte:

1. Conecte-se ao Gerenciador SNA pelo SSH e faça login com **root** credenciais.
2. Execute um dos dois comandos listados a seguir (o comando a ser executado depende se o gerenciador SNA usa ou não um servidor proxy para acesso à 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. Deixe a captura ser executada por 2-3 minutos e, em seguida, pare-a.
4. Transfira o arquivo gerado para fora do Gerenciador SNA para análise. Isso pode ser feito com o Secure Copy Protocol (SCP).

â€*f*

Defeitos relacionados

Há um defeito conhecido que pode afetar a conexão com os servidores SLIC:

- A comunicação SMC SLIC pode expirar e falhar se a porta de destino 80 estiver bloqueada. Consulte o bug da Cisco ID CSCwe08331

Informações Relacionadas

- Para obter assistência adicional, entre em contato com o Technical Assistance Center (TAC). É necessário um contrato de suporte válido: Contatos de suporte da Cisco no mundo inteiro.
- Você também pode visitar a Comunidade de Análise de Segurança da Cisco aqui.
- Suporte Técnico e Documentação - Cisco Systems

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.