SLICチャネルダウンシステムアラームのトラブルシューティング

内容

概要

前提条件

- 要件
- 使用するコンポーネント

手順

- 一般的なエラーログ
  - 接続タイムアウト
  - 要求されたターゲットへの有効な証明パスが見つかりません
  - ハンドシェイク失敗
- 実行する手順
  - ステップ 1：スマートライセンスのステータスの検証
  - ステップ 2：ドメインネームシステム(DNS)解決の確認
  - ステップ 3：脅威インテリジェンスフィードサーバへの接続の確認
  - ステップ 4：Secure Socket Layer(SSL)インスペクション/復号化の無効化

関連する不具合

関連情報

概要

このドキュメントでは、Secure Network Analytics(SNA)の「SLIC Channel Down」システムアラームをトラブルシューティングする方法について説明します。

前提条件

要件

SNAに関する基本的な知識があることが推奨されます。

SLICは「StealthWatch Labs Intelligence Center」の略です。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して

ください。

手順

「SLIC Channel Down」アラームは、SNAマネージャがThreat Intelligence Server（以前のSLIC）からフィードアップデートを取得できない場合にトリガーされます。フィードの更新が中断された原因を詳しく理解するには、次の手順を実行します。

1. SSH経由でSNAマネージャに接続し、 **root** credentials.
2. ネットワークの **/lancope/var/smc/log/smc-core.log** タイプのログをファイルおよび検索します。**SlicFeedGetter**を参照。

関連するログが見つかったら、このアラームがトリガーされる原因となる条件が複数あることを考慮して、次のセクションに進みます。

一般的なエラーログ

最も一般的なエラーログは **smc-core.log** slicチャネルダウンアラームに関連するアラームは次のとおりです。

接続タイムアウト

<#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=2019
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

要求されたターゲットへの有効な証明パスが見つかりません

<#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=2019
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

ハンドシェイク失敗

<#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=2019
```

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

javax.net.ssl.SSLHandshakeException: Handshake failed

実行する手順

脅威インテリジェンスフィードの更新は、さまざまな状況によって中断される可能性があります。次の検証手順を実行して、SNAマネージャが要件を満たしていることを確認します。

ステップ 1：スマートライセンスのステータスの検証

移動先 **Central Management > Smart Licensing** 脅威フィードライセンスのステータスが **Authorized**を参照。

ステップ 2：ドメインネームシステム(DNS)解決の確認

SNAマネージャがIPアドレスを正常に解決できることを確認します。 **lancope.flexnetoperations.com** and esdhttp.flexnetoperations.com

ステップ 3：脅威インテリジェンスフィードサーバへの接続の確認

SNAマネージャがインターネットにアクセスできること、および次にリストされている脅威インテリジェンスサーバへの接続が許可されていることを確認します。

ポートおよびプロトコル	出典	宛先
443/TCP	SNAマネージャ	esdhttp.flexnetoperations.com

		lancope.flexnetoperations.com

注:SNAマネージャが直接インターネットアクセスを許可されていない場合は、インターネットアクセスのプロキシ設定が行われていることを確認してください。

ステップ 4：Secure Socket Layer(SSL)インスペクション/復号化の無効化

2番目と3番目のエラーについては、 **Common Error Logs** このセクションは、SNAマネージャが脅威インテリジェンスフィードサーバで使用される正しいID証明書または正しい信頼チェーンを受信しない場合に発生する可能性があります。これを防ぐには、SNAマネージャと **Verify Connectivity to the Threat Intelligence Feed Servers** 。

ネットワークでSSLインスペクション/復号化が実行されているかどうかわからない場合は、SNAマネージャのIPアドレスと脅威インテリジェンスサーバのIPアドレス間のパケットキャプチャを収集し、キャプチャを分析して受信した証明書を確認できます。そのためには、次の手順を実行します。

1. SSHでSNAマネージャに接続し、 **root** credentials.
2.次に示す2つのコマンドのいずれかを実行します（実行するコマンドは、SNAマネージャがインターネットアクセスにプロキシサーバを使用しているかどうかによって異なります）。

```
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.キャプチャを2 ~ 3分間実行してから停止します。
4.分析のために、生成されたファイルをSNAマネージャから転送します。これは、Secure Copy Protocol(SCP)を使用して実現できます。

関連する不具合

SLICサーバへの接続に影響を与える可能性がある既知の不具合が1つあります。

- 宛先ポート80がブロックされると、SMC SLIC通信がタイムアウトして失敗する可能性があります。Cisco Bug ID CSCwe08331を参照してください。

関連情報

- 詳細については、Technical Assistance Center(TAC)にお問い合わせください。有効なサポート契約が必要です。 各国のシスコ サポートの連絡先.
- また、ここからCisco Security Analytics Communityにアクセスすることもできます。
- テクニカル サポートとドキュメント - Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。