排除SLIC通道關閉系統警報故障

目錄

簡介

本檔案介紹如何對安全網路分析(SNA)「SLIC通道關閉」系統警報進行疑難排解。

必要條件

需求

思科建議您瞭解基本SNA知識。

SLIC代表「Stealthwatch Labs Intelligence Center」

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

程式

當SNA管理器無法從威脅情報伺服器（以前稱為SLIC）獲取源更新時，會觸發「SLIC通道關閉」警報。要更好地瞭解導致源更新中斷的原因，請按照以下步驟操作：

1. 通過SSH連線到SNA管理器並使用 **root** 憑證。
2. 分析 **/lancope/var/smc/log/smc-core.log** 檔案並搜尋型別的日誌 **SlicFeedGetter**.

找到相關日誌後，假設存在多種情況可觸發此警報，請繼續下一部分。

常見錯誤日誌

在中看到的最常見的錯誤日誌 **smc-core.log** 與SLIC Channel Down警報相關的有：

連線超時

<#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
```

無法找到所請求目標的有效證書路徑

<#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
```

握手失敗

<#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
```

要執行的步驟

威脅情報源更新可能由於不同情況而中斷。執行下面的驗證步驟以確保SNA Manager符合要求。

步驟 1.驗證智慧許可狀態

導航至 **Central Management > Smart Licensing** 並確保威脅源許可證的狀態為 **Authorized.**

步驟 2.驗證網域名稱系統(DNS)解析

確保SNA管理器能夠成功解析 **lancope.flexnetoperations.com** and esdhttp.flexnetoperations.com

步驟 3.驗證與威脅情報源伺服器的連線

確保SNA Manager可以訪問Internet，並允許連線到下面列出的威脅情報伺服器：

埠和協定	來源	目的地
443/TCP	SNA管理員	esdhttp.flexnetoperations.com lancope.flexnetoperations.com

註：如果不允許使用SNA管理器直接訪問網際網路，請確保網際網路訪問的代理配置已就緒。

步驟 4.禁用安全套接字層(SSL)檢查/解密

中介紹的第二和第三項錯誤 **Common Error Logs** 部分，當SNA Manager未收到由Threat Intelligence Feed伺服器使用的正確身份證書或正確信任鏈時。要防止發生這種情況，請確保您的網路（通過功能強大的防火牆或代理伺服器）上未對SNA Manager和中列出的威脅情報伺服器之間的連線執行SSL檢查/解密 **Verify Connectivity to the Threat Intelligence Feed Servers** 部分。

如果您不確定是否在您的網路中執行SSL檢查/解密，可以收集SNA Manager IP地址和Threat Intelligence Servers IP地址之間的資料包捕獲，並分析該捕獲以驗證收到的證書。為此，請執行以

下操作：

1.通過SSH連線到SNA管理器，並使用 **root** 憑證。
2.運行下面列出的兩個命令之一（要運行的命令取決於SNA管理器是否使用代理伺服器進行網際網路訪問）：

```
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.讓捕獲運行2-3分鐘，然後停止。
4.將生成的檔案從SNA Manager中傳輸出來進行分析。這可以通過安全複製協定(SCP)來實現。

相關缺陷

有一個已知缺陷可能會影響到SLIC伺服器的連線：

- 如果目標埠80被阻止，SMC SLIC通訊可能會超時並失敗。請參閱思科錯誤ID CSCwe08331

相關資訊

- 如需其他協助，請聯絡技術支援中心(TAC)。需要有效的支援合約： 思科全球支援聯絡人.
- 您還可以在此處訪問思科安全分析社群。
- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。