Fehlerbehebung - Alarm "SLIC Channel Down System"

Inhalt

Einleitung

In diesem Dokument wird die Fehlerbehebung bei Systemwarnungen für Secure Network Analytics (SNA) "SLIC Channel Down" beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über grundlegende SNA-Kenntnisse verfügen.

SLIC steht für "StealthWatch Labs Intelligence Center"

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Vorgehensweise

Der Alarm "SLIC Channel Down" wird ausgelöst, wenn der SNA Manager keine Feed-Updates von den Threat Intelligence Servern (ehemals SLIC) abrufen kann. Um besser zu verstehen, was die Unterbrechung

der Feed-Updates verursacht hat, gehen Sie wie folgt vor:

1. Stellen Sie über SSH eine Verbindung zum SNA-Manager her, und melden Sie sich an mit **root** Anmeldeinformationen.
2. Analysieren Sie die **/lancope/var/smc/log/smc-core.log** Datei und suchen Sie nach den Protokollen vom Typ **SlicFeedGetter.**

Fahren Sie nach dem Auffinden der relevanten Protokolle mit dem nächsten Abschnitt fort, da mehrere Bedingungen vorliegen, die dazu führen können, dass dieser Alarm ausgelöst wird.

Häufige Fehlerprotokolle

Die häufigsten Fehlerprotokolle, die im **smc-core.log** für den Alarm "SLIC Channel Down" sind:

â€ƒ

Zeitüberschreitung bei Verbindung

<#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

Es wurde kein gültiger Zertifizierungspfad zum angeforderten Ziel gefunden.

<#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

Handshake fehlgeschlagen

<#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

Durchzuführende Schritte

Die Aktualisierungen des Threat Intelligence Feed können aufgrund unterschiedlicher Bedingungen unterbrochen werden. Führen Sie die nächsten Validierungsschritte durch, um sicherzustellen, dass Ihr SNA Manager die Anforderungen erfüllt.

Schritt 1: Smart Licensing-Status überprüfen

Navigieren Sie zu **Central Management > Smart Licensing** und stellen Sie sicher, dass der Status der Threat Feed-Lizenz **Authorized.**

â€ƒ

Schritt 2: DNS-Auflösung (Domain Name System) überprüfen

Stellen Sie sicher, dass der SNA Manager die IP-Adresse für **lancope.flexnetoperations.com**
and esdhttp.flexnetoperations.com

â€ƒ

Schritt 3: Verbindung zu den Threat Intelligence Feed-Servern überprüfen

Stellen Sie sicher, dass der SNA Manager über Internetzugriff verfügt und dass die Verbindung zu den als Nächstes aufgeführten Threat Intelligence Servern zulässig ist:

Port und Protokoll	Quelle	Ziel
443 TCP	SNA-Manager	esdhttp.flexnetoperations.com lancope.flexnetoperations.com

---

> **Hinweis**: Wenn der SNA Manager keinen direkten Internetzugriff hat, stellen Sie sicher, dass die Proxy-Konfiguration für den Internetzugriff eingerichtet ist.

â€ƒ

Schritt 4: SSL-Überprüfung/Entschlüsselung deaktivieren

Der zweite und der dritte Fehler werden im **Common Error Logs** kann auftreten, wenn der SNA Manager nicht

das richtige Identitätszertifikat oder die richtige Vertrauenskette erhält, die von den Threat Intelligence Feed-Servern verwendet wird. Um dies zu verhindern, müssen Sie sicherstellen, dass im gesamten Netzwerk (durch geeignete Firewalls oder Proxy-Server) keine SSL-Überprüfung/Entschlüsselung für Verbindungen zwischen dem SNA Manager und den Threat Intelligence-Servern durchgeführt wird, die im **Verify Connectivity to the Threat Intelligence Feed Servers** Abschnitt.

Wenn Sie sich nicht sicher sind, ob die SSL-Überprüfung/Entschlüsselung in Ihrem Netzwerk durchgeführt wird, können Sie eine Paketerfassung zwischen der IP-Adresse des SNA Managers und der IP-Adresse des Threat Intelligence Servers durchführen und die Erfassung analysieren, um das empfangene Zertifikat zu überprüfen. Gehen Sie hierzu wie folgt vor:

1. Stellen Sie über SSH eine Verbindung zum SNA-Manager her, und melden Sie sich an mit **root** Anmeldeinformationen.
2. Führen Sie einen der beiden als Nächstes aufgeführten Befehle aus (der auszuführende Befehl hängt davon ab, ob der SNA-Manager einen Proxyserver für den Internetzugriff verwendet):

```
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. Lassen Sie die Aufnahme für 2-3 Minuten laufen und dann stoppen Sie es.
4. Übertragen Sie die generierte Datei zur Analyse aus dem SNA Manager. Dies ist über das Secure Copy Protocol (SCP) möglich.

â€ƒ

Verwandte Fehler

Es gibt einen bekannten Fehler, der sich auf die Verbindung zu SLIC-Servern auswirken kann:

- Die SMC SLIC-Kommunikation kann aufgrund einer Zeitüberschreitung fehlschlagen, wenn der Zielport 80 blockiert wird. Siehe Cisco Bug-ID CSCwe08331

Zugehörige Informationen

- Weitere Unterstützung erhalten Sie vom Technical Assistance Center (TAC). Ein gültiger Supportvertrag ist erforderlich: Weltweiter Kontakt zum Cisco Support.
- Besuchen Sie auch die Cisco Security Analytics Community hier.
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.