Risoluzione dei problemi relativi all'allarme del sistema SLIC Channel Down

Sommario

Introduzione

In questo documento viene descritto come risolvere i problemi relativi agli allarmi di sistema "SLIC Channel Down" di Secure Network Analytics (SNA).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza base della SNA.

SLIC sta per "Stealthwatch Labs Intelligence Center"

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Procedura

L'allarme "SLIC Channel Down" viene attivato quando SNA Manager non è in grado di ricevere gli aggiornamenti dei feed dai Threat Intelligence Server, in precedenza SLIC. Per comprendere meglio la

causa dell'interruzione degli aggiornamenti dei feed, procedere come segue:

1. Collegarsi a SNA Manager tramite SSH e accedere con **root** credenziali.
2. Analizzare **/lancope/var/smc/log/smc-core.log** e cercare i log di tipo **SlicFeedGetter.**

Una volta trovati i registri rilevanti, procedere alla sezione successiva, dato che ci sono diverse condizioni che possono causare l'attivazione di questo allarme.

Log degli errori comuni

I log degli errori più comuni visualizzati nel **smc-core.log** rispetto all'allarme SLIC Channel Down sono:

â€ƒ

Timeout della connessione

<#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

Impossibile trovare un percorso di certificazione valido per la destinazione richiesta

<#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 non riuscito

<#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
```

Passi da eseguire

Gli aggiornamenti del feed di Threat Intelligence possono essere interrotti a causa di condizioni diverse. Eseguire i passaggi di convalida successivi per verificare che SNA Manager soddisfi i requisiti.

Passaggio 1. Convalida stato licenze Smart

Passa a **Central Management > Smart Licensing** e accertarsi che lo stato della licenza per mangimi a rischio sia **Authorized.**

â€ƒ

Passaggio 2. Verifica risoluzione DNS (Domain Name System)

Accertarsi che SNA Manager sia in grado di risolvere correttamente l'indirizzo IP per **lancope.flexnetoperations.com** and esdhttp.flexnetoperations.com

â€ƒ

Passaggio 3. Verifica della connettività ai server feed di Threat Intelligence

Verificare che SNA Manager disponga di accesso a Internet e che sia consentita la connettività ai server di Threat Intelligence elencati di seguito:

Porta e protocollo	Origine	Destinazione
443/TCP	Gestione SNA	esdhttp.flexnetoperations.com lancope.flexnetoperations.com

---

> **Nota**: se a SNA Manager non è consentito l'accesso diretto a Internet, verificare che sia presente la configurazione proxy per l'accesso a Internet.

â€ƒ

Passaggio 4. Disabilita controllo/decrittografia SSL (Secure Sockets Layer)

Il secondo e il terzo errore descritti nel **Common Error Logs** Questa sezione può verificarsi quando Gestione SNA non riceve il certificato di identità corretto o la catena di attendibilità corretta utilizzata dai server dei feed di Threat Intelligence. Per evitare questo inconveniente, accertarsi che non venga eseguita alcuna ispezione/decrittografia SSL sulla rete (da parte di firewall o server proxy compatibili) per le connessioni tra SNA Manager e i server Threat Intelligence elencati nella **Verify Connectivity to the Threat Intelligence Feed Servers**

sezione.

Se non si è certi che l'ispezione/decrittografia SSL venga eseguita nella rete, è possibile raccogliere un'acquisizione di pacchetto tra l'indirizzo IP di SNA Manager e l'indirizzo IP dei server Threat Intelligence e analizzare l'acquisizione per verificare il certificato ricevuto. A tale scopo, effettuare le seguenti operazioni:

1. Connettersi a SNA Manager tramite SSH e accedere con **root** credenziali.
2. Eseguire uno dei due comandi elencati di seguito (il comando da eseguire dipende dal fatto che il gestore SNA utilizzi o meno un server proxy per l'accesso 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. Lasciare in esecuzione l'acquisizione per 2-3 minuti, quindi arrestarla.
4. Trasferire il file generato fuori da SNA Manager per l'analisi. A tale scopo, è possibile utilizzare SCP (Secure Copy Protocol).

â€*f*

Difetti correlati

Esiste un difetto noto che può influire sulla connessione ai server SLIC:

- La comunicazione SLIC SMC può scadere e non riuscire se la porta di destinazione 80 è bloccata. Vedere l'ID bug Cisco CSCwe0831

Informazioni correlate

- Per ulteriore assistenza, contattare il Technical Assistance Center (TAC). È necessario un contratto di supporto valido: Contatti del supporto Cisco internazionali.
- Qui è possibile anche visitare la Cisco Security Analytics Community.
- Documentazione e supporto tecnico â€“ Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).