Dépannage de l'alarme SLIC Channel Down System

Table des matières

Introduction

Ce document décrit comment dépanner les alarmes système « SLIC Channel Down » de Secure Network Analytics (SNA).

Conditions préalables

Exigences

Cisco vous recommande d'avoir des connaissances de base sur l'architecture SNA.

SLIC signifie « StealthWatch Labs Intelligence Center »

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Procédure

L'alarme « SLIC Channel Down » est déclenchée lorsque le SNA Manager ne parvient pas à obtenir les mises à jour de flux des serveurs Threat Intelligence, anciennement SLIC. Pour mieux comprendre ce qui a provoqué l'interruption des mises à jour du flux, procédez comme suit :

1. Connectez-vous à SNA Manager via SSH et connectez-vous avec des informations d' **root** identification.

    - Analysez le **/lancope/var/smc/log/smc-core.log** fichier et recherchez les journaux de type **SlicFeedGetter**.

Une fois que vous avez trouvé les journaux appropriés, passez à la section suivante, car plusieurs conditions peuvent déclencher cette alarme.

Journaux d'erreurs courants

Les journaux d'erreurs les plus courants dans la **smc-core.log** relative à l'alarme SLIC Channel Down sont les suivants :

Délai de connexion dépassé

<#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

Impossible de trouver un chemin de certification valide vers la cible demandée

<#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

Échec de la connexion

<#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
```

Étapes à effectuer

Les mises à jour du flux Threat Intelligence peuvent être interrompues en raison de conditions différentes. Suivez les étapes de validation suivantes pour vous assurer que votre SNA Manager répond aux exigences.

Étape 1. Valider l'état des licences Smart

Naviguez jusqu'à **Central Management > Smart Licensing** et vérifiez que l'état de la licence Threat Feed est **Authorized**.

Étape 2. Vérification de la résolution DNS (Domain Name System)

Assurez-vous que le SNA Manager est en mesure de résoudre l'adresse IP pour **lancope.flexnetoperations.com**
and esdhttp.flexnetoperations.com

Étape 3. Vérification de la connectivité aux serveurs Threat Intelligence Feed

Assurez-vous que SNA Manager dispose d'un accès Internet et que la connectivité aux serveurs Threat Intelligence Servers répertoriés ci-dessous est autorisée :

Port et protocole	Source	Destination
443/TCP	Gestionnaire SNA	esdhttp.flexnetoperations.com lancope.flexnetoperations.com

Remarque : si le gestionnaire SNA n'est pas autorisé à disposer d'un accès Internet direct, assurez-vous que la configuration du proxy pour l'accès Internet est en place.

Étape 4. Désactiver l'inspection/le déchiffrement SSL (Secure Socket Layer)

Les deuxième et troisième erreurs décrites dans la **Common Error Logs** section peuvent se produire lorsque le SNA Manager ne reçoit pas le certificat d'identité correct ou la chaîne de confiance correcte utilisée par les serveurs Threat Intelligence Feed. Pour éviter cela, assurez-vous qu'aucune inspection/décryptage SSL n'est effectuée sur votre réseau (par des pare-feu ou des serveurs proxy compatibles) pour les connexions entre le SNA Manager et les serveurs Threat Intelligence répertoriés dans la **Verify Connectivity to the Threat Intelligence Feed Servers** section.

Si vous n'êtes pas sûr que l'inspection/le déchiffrement SSL est effectué sur votre réseau, vous pouvez collecter une capture de paquets entre l'adresse IP de SNA Manager et l'adresse IP des serveurs Threat Intelligence et analyser la capture pour vérifier le certificat reçu. Pour cela, procédez comme suit :

1. Connectez-vous à SNA Manager par SSH et connectez-vous avec des informations d'**root** identification.
2. Exécutez l’une des deux commandes suivantes (la commande à exécuter dépend du fait que le gestionnaire SNA utilise ou non un serveur

proxy pour l’accès 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. Laissez la capture s'exécuter pendant 2-3 minutes, puis arrêtez-la.
4. Transférez le fichier généré hors de SNA Manager pour analyse. Cela peut être réalisé avec le protocole Secure Copy Protocol (SCP).

Défauts associés

Il existe un défaut connu qui peut affecter la connexion aux serveurs SLIC :

- La communication SMC SLIC peut expirer et échouer si le port de destination 80 est bloqué. Voir ID de bogue Cisco CSCwe08331

Informations connexes

- Pour obtenir de l'aide supplémentaire, veuillez contacter le Centre d'assistance technique (TAC). Un contrat d'assistance valide est requis : Cisco Worldwide Support Contacts.
- Vous pouvez également visiter la communauté Cisco Security Analytics ici.
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.