Dépannage de l'alarme SLIC Channel Down System

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Procédure
  - Journaux d'erreurs courants
    - Délai de connexion dépassé
    - Impossible de trouver un chemin de certification valide vers la cible demandée
    - Échec de la connexion
  - Étapes de correction
    - Étape 1 : validation de l'état des licences Smart
    - Étape 2 : vérification de la résolution DNS (Domain Name System)
    - Étape 3. Vérification de la connectivité aux serveurs Threat Intelligence Feed
    - Étape 4 : désactivation de l'inspection/du déchiffrement SSL (Secure Socket Layer)
- Défauts associés
- Informations connexes

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. Accédez à Central Management en vous connectant à Manager (dans le champ d'adresse de votre navigateur, tapez https:// et l'adresse IP de l'appliance. Appuyez sur Entrée.)
2. Dans le menu principal, sélectionnez Configure **>** Global **>** Central Management.
3. Cliquez sur l'icône de sélection de l'appliance.
4. Sélectionnez Afficher les statistiques du matériel.
5. Dans le menu principal, sélectionnez Support **>** Browse Files
6. Sur la page Browse Files, sélectionnez smc **>** logs **>** et cliquez sur smc-core.log.
7. Un nouvel onglet s'ouvre avec le contenu smc-core.log. Vérifiez ce fichier en recherchant les**SlicFeedGetter** journaux.

Journaux d'erreurs courants

Les journaux d'erreurs les plus courants dans les**smc-core.log** rapports associés à l'alarme de canal hors service SLIC sont les suivants :

Délai de connexion dépassé

```
2026-01-01 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.fl
```

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

```
2026-01-01 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.SunCertP
```

Échec de la connexion

```
2026-01-01 20:00:50,227 ERROR [SlicFeedGetter] Getting Threat Feed update failed with exception.
javax.net.ssl.SSLHandshakeException: Handshake failed
```

Étapes de correction

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 : validation de 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 SNA Manager n'est pas autorisé à avoir un accès direct à Internet, assurez-vous que la configuration du proxy pour l'accès à Internet est en place.

Étape 4 : désactivation de l’inspection/du 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 :

Pour créer un utilisateur de capture de paquets, utilisez la console de l'appliance (SystemConfig) en tant qu'utilisateur sysadmin.

1. Connectez-vous à l'appliance en tant que sysadmin.
2. Sélectionnez Advanced > Packet Capture. S'il n'existe aucune capture de paquet existante, vous accédez directement au menu de configuration de capture de paquet. Si vous disposez déjà de captures de paquets, sélectionnez Create (Créer) pour créer une nouvelle capture de paquets.
3. Entrez un numéro de port TCP ou UDP dans le champ Port Filter. Le port peut être la source ou la destination. Vous pouvez laisser ce champ vide pour définir le filtre sur « Tout ». SLIC utilise une connexion tcp/443. Par conséquent, saisissez 443 dans ce champ.
4. Dans le champ Durée (900 secondes max), spécifiez le nombre de secondes pour effectuer la capture de paquets.

   

   Remarque : Veillez à entrer une durée raisonnable, car un fichier de capture extrêmement volumineux peut potentiellement consommer tout l'espace disponible sur le disque dur de l'appliance. Ce champ fonctionne avec le paramètre Packets (Paquets). La capture s'exécute jusqu'à ce que la durée ou le nombre de paquets soit atteint.

5. Dans le champ Packets (100 000 max), spécifiez le nombre de paquets à capturer avant de mettre fin à la capture. Ce champ fonctionne avec le paramètre Durée. La capture s'exécute jusqu'à ce que la durée ou le nombre de paquets soit atteint.
6. Cliquez sur OK pour démarrer la capture de paquets.

   

   Conseil : Pour arrêter brusquement une capture de paquet, vous pouvez généralement appuyer sur Ctrl+C.

Pour afficher les fichiers de capture de paquets, téléchargez-les et affichez-les localement. Les fichiers sont stockés dans /lancope/var/tcpdump.

Vous pouvez vous connecter directement à l'appliance ou y accéder via l'inventaire du Gestionnaire central > Afficher les statistiques de l'appliance. Accédez à Support > Browse Files pour télécharger la capture de paquets.

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.