Probleemoplossing voor SLIC Channel Down systeemalarmlampje

Inhoud

Inleiding

In dit document wordt beschreven hoe u systeemalarmen voor "SLIC Channel Down"-analyse van Secure Network Analytics (SNA) kunt oplossen.

Voorwaarden

Vereisten

Cisco raadt aan dat u over fundamentele SNA-kennis beschikt.

SLIC staat voor "Stealthwatch Labs Intelligence Center"

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Procedure

Het "SLIC Channel Down" alarm wordt geactiveerd wanneer de SNA Manager geen feed updates kan ontvangen van de Threat Intelligence Servers, voorheen SLIC. Om beter te begrijpen wat de onderbreking van de updates heeft veroorzaakt, gaat u als volgt te werk:

1. Verbinding maken met SNA Manager via SSH en inloggen met **root** referenties.
2. Het **/lancope/var/smc/log/smc-core.log** bestand en zoeken naar de logbestanden van het type **SlicFeedGetter.**

Zodra u de relevante logbestanden vindt, gaat u verder naar de volgende sectie omdat er meerdere omstandigheden zijn die ervoor kunnen zorgen dat dit alarm wordt geactiveerd.

Gemeenschappelijke foutenlogboeken

De meest voorkomende foutenlogboeken die in de **smc-core.log** gerelateerd aan het SLIC Channel Down alarm zijn:

â€ƒ

Time out verbinding

<#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

Kan geen geldig certificeringspad naar aangevraagd doel vinden

<#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

Handdruk is mislukt

<#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
```

Uit te voeren stappen

De updates van Threat Intelligence kunnen vanwege verschillende omstandigheden worden onderbroken. Voer de volgende validatiestappen uit om er zeker van te zijn dat uw SNA Manager aan de vereisten voldoet.

Stap 1. Slimme licentiestatus valideren

Naar navigeren **Central Management > Smart Licensing** en ervoor te zorgen dat de status van de bedreigingsvoedingsvergunning **Authorized.**

â€ƒ

Stap 2. Controleer de resolutie van Domain Name System (DNS)

Zorg ervoor dat de SNA Manager met succes het IP-adres kan oplossen voor **lancope.flexnetoperations.com** and esdhttp.flexnetoperations.com

â€ƒ

Stap 3. Controleer de connectiviteit met de Threat Intelligence Feed Servers

Zorg ervoor dat de SNA Manager toegang tot internet heeft en dat verbinding met de volgende Threat Intelligence Servers is toegestaan:

Poorten en protocollen	Bron	Bestemming
443/TCP-switch	SNA-beheer	esdhttp.flexnetoperations.com lancope.flexnetoperations.com

---

> **Opmerking**: Als de SNA Manager geen directe internettoegang mag hebben, zorg er dan voor dat de Proxy-configuratie voor internettoegang aanwezig is.

â€ƒ

Stap 4. SSL-inspectie (Secure Socket Layer) uitschakelen/decryptie

De tweede en de derde fout die in het **Common Error Logs** Deze sectie kan voorkomen wanneer de SNA Manager niet het juiste identiteitscertificaat of de juiste vertrouwensketen ontvangt die wordt gebruikt door de Threat Intelligence Feed servers. Om dit te voorkomen, dient u ervoor te zorgen dat er geen SSL-inspectie/decryptie wordt uitgevoerd over uw netwerk (door geschikte firewalls of proxyservers) voor

verbindingen tussen de SNA Manager en de Threat Intelligence-servers die in de **Verify Connectivity to the Threat Intelligence Feed Servers** doorsnede.

Als u niet zeker weet of SSL-inspectie/decryptie wordt uitgevoerd in uw netwerk, kunt u een pakketopname verzamelen tussen het IP-adres van SNA Manager en het IP-adres van Threat Intelligence Servers en de opname analyseren om het ontvangen certificaat te verifiëren. Voer hiervoor de volgende handelingen uit:

1. Verbind met de SNA Manager door SSH en log in met **root** referenties.
2. Voer een van de volgende twee opdrachten uit (de uit te voeren opdracht is afhankelijk van de vraag of de SNA-beheerder een proxyserver voor internettoegang gebruikt of niet):

```
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. Laat de opname 2 tot 3 minuten lopen en stop ermee.
4. Breng het gegenereerde bestand voor analyse naar de SNA Manager. Dit kan worden bereikt met Secure Copy Protocol (SCP).

â€ƒ

Verwante defecten

Er is één bekend defect dat gevolgen kan hebben voor de verbinding met SLIC-servers:

- SMC SLIC-communicatie kan uitvallen en mislukken als bestemmingshaven 80 is geblokkeerd. Zie Cisco bug-id CSCwe08331

Gerelateerde informatie

- Voor extra hulp kunt u contact opnemen met het Technical Assistance Center (TAC). Een geldig ondersteuningscontract is vereist: Ciscoâ€™s wereldwijde contactgegevens voor ondersteuning.
- U kunt hier ook de Cisco Security Analytics Community bezoeken.
- Technische ondersteuning en documentatie â€“ Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.