Troubleshoot SLIC Channel Down System Alarm

Contents

Introduction

This document describes how to troubleshoot Secure Network Analytics (SNA) "SLIC Channel Down" system alarms.

Prerequisites

Requirements

Cisco recommends that you have basic SNA knowledge.

SLIC stands for "Stealthwatch Labs Intelligence Center"

Components Used

This document is not restricted to specific software and hardware versions.

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. If your network is live, ensure that you understand the potential impact of any command.

Procedure

The "SLIC Channel Down" alarm is triggered when the SNA Manager is unable to get feed updates from the Threat Intelligence Servers, formerly SLIC. To better understand what caused the feed updates to be interrupted, proceed as follows:

1. Connect to the SNA Manager via SSH and log in with **root** credentials.
2. Analyze the **/lancope/var/smc/log/smc-core.log** file and search for the logs of type **SlicFeedGetter**.

Once you find the relevant logs, continue to the next section given that there are multiple conditions that can cause this alarm to get triggered.

Common Error Logs

The most common error logs seen in the **smc-core.log** related to the SLIC Channel Down alarm are:

â€ƒ

Connection Timed Out

<#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

Unable to Find Valid Certification Path to Requested Target

<#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 Failed

<#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

Steps to Perform

The Threat Intelligence Feed updates can be interrupted due to different conditions. Perform the next validation steps to ensure your SNA Manager meets the requirements.

Step 1. Validate Smart Licensing Status

Navigate to **Central Management > Smart Licensing** and ensure that the status of the Threat Feed License is **Authorized.**

â€ƒ

Step 2. Verify Domain Name System (DNS) Resolution

Ensure that the SNA Manager is successfully able to resolve the IP Address for **lancope.flexnetoperations.com** and esdhttp.flexnetoperations.com

â€ƒ

Step 3. Verify Connectivity to the Threat Intelligence Feed Servers

Ensure that the SNA Manager has Internet access and that connectivity to the Threat Intelligence Servers listed next is allowed:

Port and Protocol	Source	Destination
443/TCP	SNA Manager	esdhttp.flexnetoperations.com lancope.flexnetoperations.com

---

> **Note**: If the SNA Manager is not allowed to have direct internet access, please ensure that the Proxy configuration for internet access is in place.

â€ƒ

Step 4. Disable Secure Socket Layer (SSL) Inspection/Decryption

The second and third errors described in the **Common Error Logs** section can occur when the SNA Manager does not receive the correct identity certificate or the correct trust chain used by the Threat Intelligence Feed servers. To prevent this, ensure that no SSL Inspection/Decryption is performed across your network (by capable Firewalls or Proxy Servers) for connections between the SNA Manager and the Threat Intelligence servers listed in the **Verify Connectivity to the Threat Intelligence Feed Servers** section.

If you are unsure if SSL Inspection/Decryption is performed in your network, you can collect a packet capture between the SNA Manager IP address and the Threat Intelligence Servers IP address and analyze the capture to verify the certificate received. For this, perform as follows:

1. Connect to the SNA Manager by SSH and log in with **root** credentials.

2. Run one of the two commands listed next (the command to run depends on whether the SNA manager uses a proxy server for internet access or not):

```
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. Let the capture run for 2-3 minutes and then stop it.
4. Transfer the generated file out of the SNA Manager for analysis. This can be accomplished with Secure Copy Protocol (SCP).

â€ƒ

Related Defects

There is one known defect that can impact the connection to SLIC servers:

- SMC SLIC communication can timeout and fail if destination port 80 is blocked. See Cisco bug ID CSCwe08331

Related Information

- For additional assistance, please contact the Technical Assistance Center (TAC). A valid support contract is required: Cisco Worldwide Support Contacts.
- You can also visit the Cisco Security Analytics Community here.
- Technical Support & Documentation - Cisco Systems