Troubleshoot SecureX Module Errors for Secure Network Analytics Integration (Formerly Stealthwatch Enterprise)

Contents

Introduction

This document describes how to troubleshoot SecureX Module Errors for Secure Network Analytics Integration.

Prerequisites

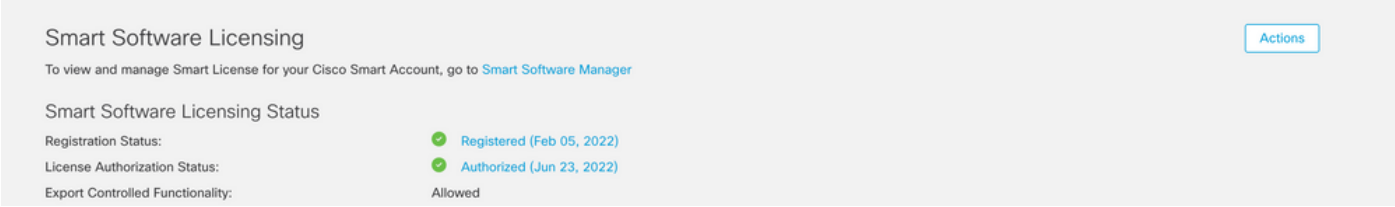
Requirements

Cisco recommends that you have knowledge of these topics:

- Secure Network Analytics (SNA) Console
- Your Secure Network Analytics deployment generates security events and Alarms as expected
- Your SNA Console needs to be able to connect outbound to the Cisco clouds: North America clouds

- EU clouds Asia (APJC) clouds

- Your SNA is Registered in **Smart Licensing.** Navigate to **Central Management > Smart Licensing**, as shown in the image:



- It is recommended to use the same Smart Account/Virtual Account that you use for the SecureX product
- You have an account to access SecureX. In order to use SecureX and associated tools, you need to have an account on the regional cloud you use

  Note: If you or your organization already have accounts on your regional cloud, use the account that already exists. Do not create a new one.

Components Used

The information in this document is based on these software versions:

- Cisco Security Services Exchange (SSE) console
- Secure Network Analytics v7.2.1 or later
- SecureX Console

  Note: The account in every console must have Administrator rights in order to perform a change.

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.

Background Information

Cisco SecureX is the platform in the Cisco cloud that helps you detect, investigate, analyze, and respond to threats and use the data aggregated from multiple products and sources. This integration enables you to do these tasks in Secure Network Analytics (formerly Stealthwatch):

- Use Secure Network Analytics (shown as Stealthwatch) tiles on the SecureX dashboard to monitor key operational metrics
- Utilize the SecureX menu to pivot to your other Cisco Security and third-party integrations
- Provide access to your SecureX ribbon
- Send Secure Network Analytics Alarms to the Cisco SecureX threat response (formerly Cisco Threat Response) Private Intelligence Store
- Allow SecureX to request Security Events from Secure Network Analytics to enrich the investigation context in threat response workflows

Please refer to the latest SecureX and Secure Network Analytics Integration Guide here.

Secure Network Analytics Module Errors

This document helps to troubleshoot any of these error messages on the Secure Network Analytics Integration Module:

- Error example #1

```
"Module Error: Stealthwatch Enterprise remote-server-error: {:error (not (map? a-
java.lang.String))} [:invalid-server-response]"
```

- Error example #2

```
"There was an unexpected error in the module"
```

SNA CLI Login Methods

There are two user roles in order to log in via SSH into SNA CLI

- Root
- Sysadmin

You need to log in via SSH with the device IP address and ***Root*** user role. (You have limited actions as ***Sysadmin*** user role)

Troubleshoot

> **Note**: The troubleshoot mentioned in this document **must be performed and supervised** by a Cisco TAC engineer. Please open a case in order to get the proper assistance from the Cisco TAC Support team.

Restart SSE and CTR services

Step 1. If SecureX SNA Module triggers any of the error messages, log in via SSH into the SNA device as the Root user.

Step 2. Run the next commands in order to restart **sse-connector** and **ctr-integration** services:

```
docker restart svc-sse-connector docker restart svc-ctr-integration
```

Step 3. Run this command to verify services status:

```
docker ps
```

The services must show **UP** status (also, you can see the status time changes when the service is started/restarted), as shown in the image:

```
tac-smc-cds-sal:~# docker ps
CONTAINER ID        IMAGE                                                                                    COMMAND                  CREATED             STATUS              PORTS
NAMES
72b0513a3133        docker-lc.artifactory1.lancope.ciscolabs.com/svc-sse-connector:20220223.1826-50494327f47e   "/opt/connector/star…"   7 weeks ago         Up 10 seconds       8989/tcp, 12826/tcp
svc-sse-connector
21a19b529f47        docker-lc.artifactory1.lancope.ciscolabs.com/svc-ctr-integration:20220110.0948-948bd5d4e9be   "/opt/bin/start.sh"      7 weeks ago         Up About a minute   12825/tcp
```

Step 4. Refresh the SNA Module tiles in SecureX portal, the dashboard starts to show the proper SNA data.

Configure the FQDN of the SMC

If restart **sse-connector** and **ctr-integration** services do not fix the issue, please navigate to the location **/lancope/var/logs/containers** and run this command:

```
cat the svc-sse-connector.log
```

Verify if you get this error message in the logs:

```
docker/svc-sse-connector[1193]: time="2021-05-26T09:19:20.921548198Z" level=info
msg="[FlowID:<FLOW_UUID>;MsgID:<MSG_UUID>] HTTP command [/ctr/health] with cmdID [<UUID>]
failed: Post https://X.X.X.X/ctr/health: x509: cannot validate certificate for X.X.X.X because
it doesn't contain any IP SANs"
```

If the line exists, you need to edit the **docker-compose.yml** file in order to fix this error.

Step 1. Navigate into **/lancope/manifests/** path and locate **docker-compose.yml** file, as shown in the image:

```
tac-smc-cds-sal:~# cd /lancope/manifests/
tac-smc-cds-sal:/lancope/manifests# ls
configure-env  docker-compose.detections.yml  docker-compose.prod.yml    docker-compose.utils.yml       docker-compose.yml     plugins
detections     docker-compose.forensics.yml   docker-compose.static.yml  docker-compose.visibility.yml  generate-product-info  util
```

Step 2. Run this command in order to edit **docker-compose.yml** file:

```
cat docker-compose.yml
```

You can use your preferred method to edit it (Nano or Vim) in order to search the container **sse-connector** details, as shown in the image:

```
sse-connector:
  container_name: svc-sse-connector
  image: docker-lc.artifactory1.lancope.ciscolabs.com/svc-sse-connector:20220228.1646-745bef4a8b73
  init: true
  depends_on:
    - rabbit
    - ctr-integration
  environment:
    JAVA_OPTS: >-
      -Dsvc-token-authority.urlFragment=http://token-authority:9502
      -Dmanager.osaxsd.url=unix://lancope/services/osaxsd/osaxsd.sock
    SPRING_OPTS: >-
      --server.log.level=INFO
      --platform.host.ip=${HOST_IP}
      --syslog.internalNetworkMapping.enabled=true
      --syslog.internalNetworkMapping.subnet=${APPLICATION_SUBNET}
      --rabbit.host=rabbit
      --rabbit.port=5672
    SW_FEATURE_TOGGLES: "/lancope/feature-toggles"
    CISCOJ_NON_FIPS_OPERATION:
    CISCOJ_COMMON_CRITERIA_MODE:
    TLS_CIPHERS_FILE:
  volumes:
    - ${BASE_ASSETS_DIR}/lancope/feature-toggles/:/lancope/feature-toggles/:ro
    - ${BASE_ASSETS_DIR}/lancope/var/containers/sse/data:/opt/connector/data:rw
    - ${BASE_ASSETS_DIR}/lancope/var/containers/sse/control/:/opt/control:rw
    - ${BASE_ASSETS_DIR}/lancope/var/containers/sse/config/:/opt/config:rw
    - ${BASE_ASSETS_DIR}/lancope/var/nginx/ssl:/opt/nginx/ssl:ro
    - ${BASE_ASSETS_DIR}/lancope/var/tomcat/ssl:/opt/tomcat/ssl:ro
    - ${BASE_ASSETS_DIR}/lancope/etc/keystore:/lancope/etc/keystore:rw
    - ${BASE_ASSETS_DIR}/etc/ssl/certs/core.pem:/opt/connector/cert/core.pem:ro
    - ${BASE_ASSETS_DIR}${TLS_CIPHERS_FILE}:${TLS_CIPHERS_FILE}:ro

G Get Help     ^O Write Out    ^W Where Is     ^K Cut Text     ^J Justify      ^C Cur Pos
X Exit         ^R Read File    ^\ Replace      ^U Uncut Text   ^T To Spell     ^_ Go To Line
```

Step 3. Navigate to **SPRING_OPTS** line and add the next command line:

```
--context.custom.service.relay=smc_hostname
```

The **smc_hostname** is the FQDN of your SNA, as shown in the image:

```
container_name: svc-sse-connector
image: docker-lc.artifactory1.lancope.ciscolabs.com/svc-sse-connector:20220223.1826-50494327f47e
init: true
depends_on:
  - rabbit
  - ctr-integration
environment:
  JAVA_OPTS: >-
    -Dsvc-token-authority.urlFragment=http://token-authority:9502
    -Dmanager.osaxsd.url=unix://lancope/services/osaxsd/osaxsd.sock
  SPRING_OPTS: >-
    --server.log.level=INFO
    --platform.host.ip=${HOST_IP}
    --syslog.internalNetworkMapping.enabled=true
    --syslog.internalNetworkMapping.subnet=${APPLICATION_SUBNET}
    --rabbit.host=rabbit
    --rabbit.port=5672
    --context.custom.service.relay=tac-securex-sna
  SW_FEATURE_TOGGLES: "/lancope/feature-toggles"
  CISCOJ_NON_FIPS_OPERATION:
  CISCOJ_COMMON_CRITERIA_MODE:
  TLS_CIPHERS_FILE:
volumes:
  - ${BASE_ASSETS_DIR}/lancope/feature-toggles/:/lancope/feature-toggles/:ro
  - ${BASE_ASSETS_DIR}/lancope/var/containers/sse/data:/opt/connector/data:rw
  - ${BASE_ASSETS_DIR}/lancope/var/containers/sse/control/:/opt/control:rw
  - ${BASE_ASSETS_DIR}/lancope/var/containers/sse/config/:/opt/config:rw
  - ${BASE_ASSETS_DIR}/lancope/var/nginx/ssl:/opt/nginx/ssl:ro
  - ${BASE_ASSETS_DIR}/lancope/var/tomcat/ssl:/opt/tomcat/ssl:ro
  - ${BASE_ASSETS_DIR}/lancope/etc/keystore:/lancope/etc/keystore:rw
  - ${BASE_ASSETS_DIR}/etc/ssl/certs/core.pem:/opt/connector/cert/core.pem:ro
  - ${BASE_ASSETS_DIR}${TLS_CIPHERS_FILE}:${TLS_CIPHERS_FILE}:ro
```

Step 4. Save the new change and run this command:

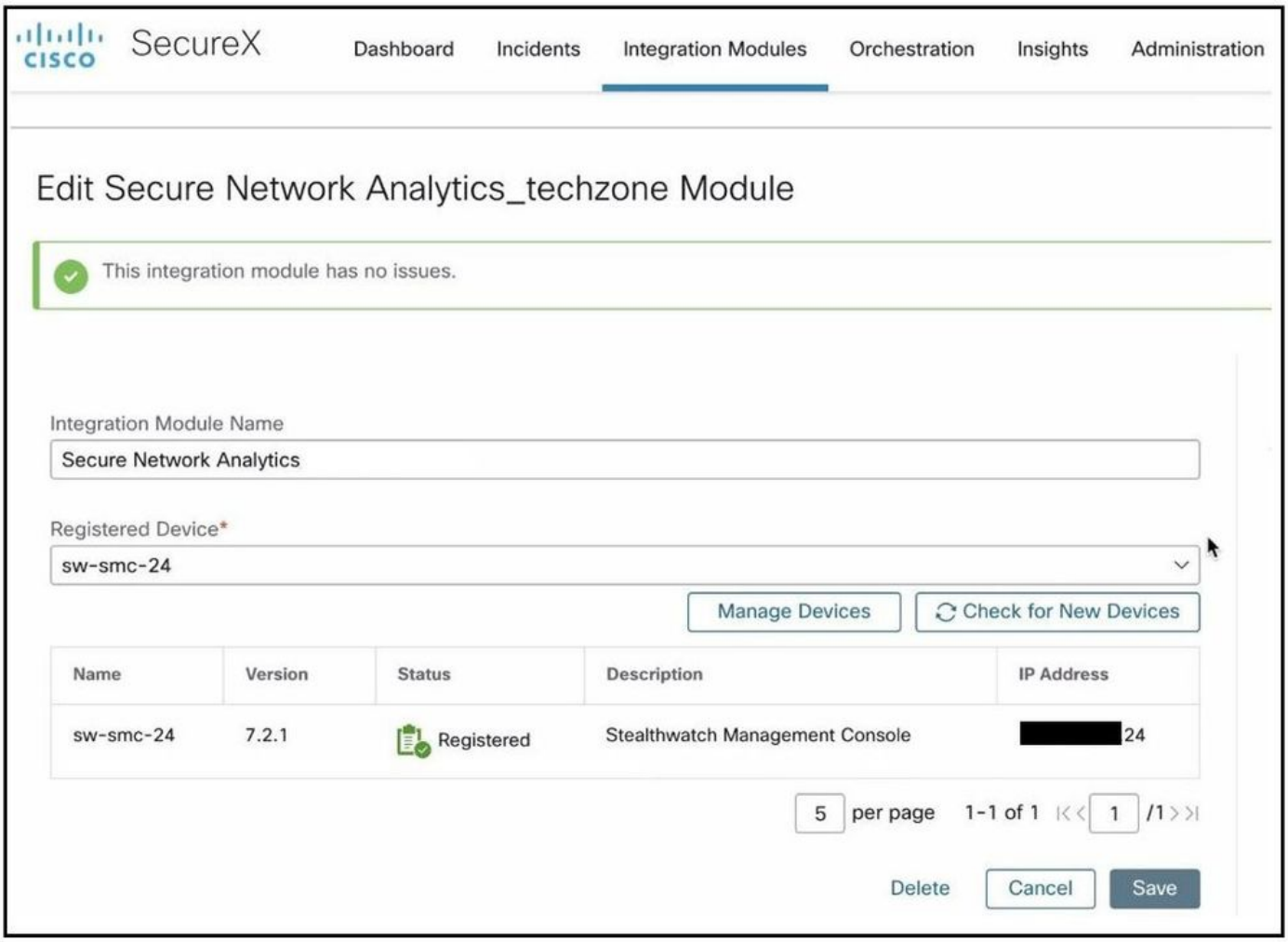
```
docker-compose up -d sse-connector
```

It recreates the **docker-compose.yml** file with the proper SNA details, the output must show ***done*** status, as shown in the image:

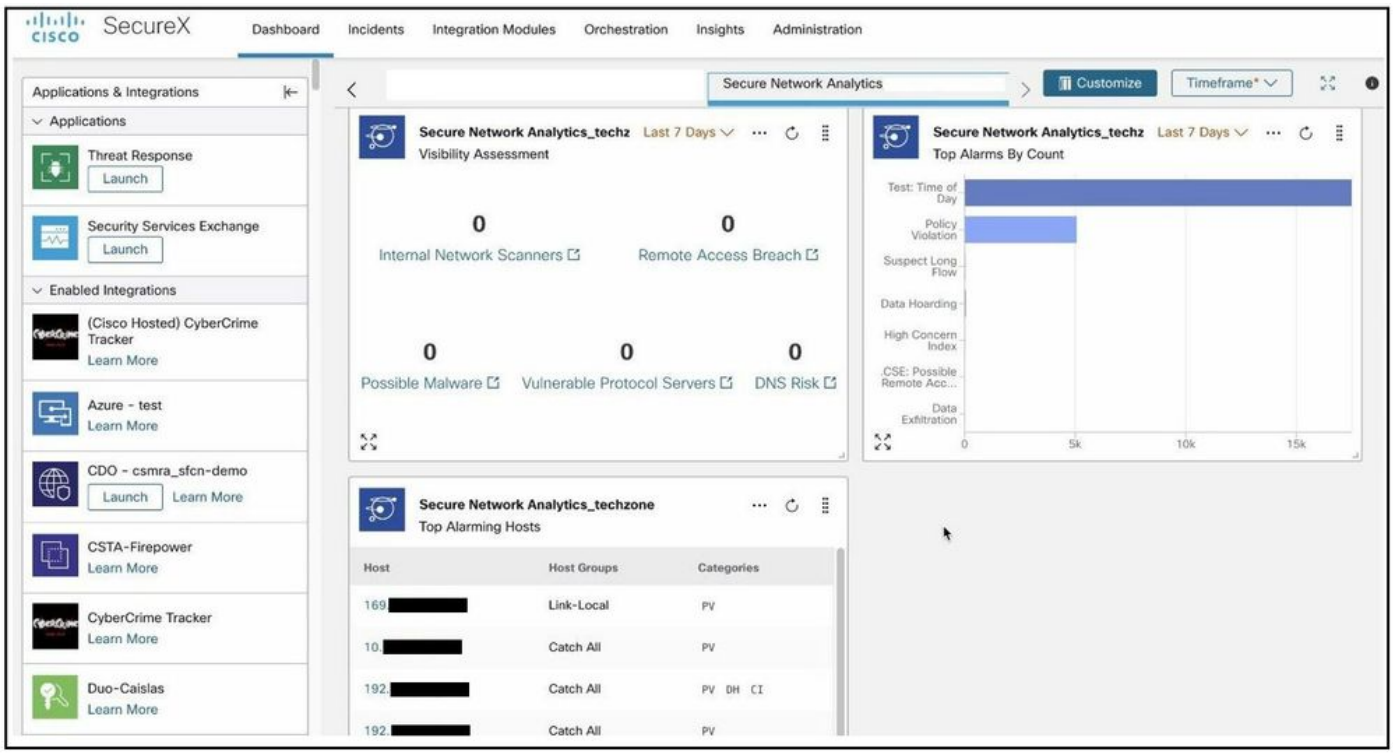
```
tac-smc-cds-sal:/lancope/manifests# docker-compose up -d sse-connector
WARNING: The BASE_ASSETS_DIR variable is not set. Defaulting to a blank string.
Starting sw-header ...
svc-central-management is up-to-date
Starting sw-configuration ...
Starting sw-login         ...
sw-rabbitmq is up-to-date
svc-sw-policy is up-to-date
static-assets is up-to-date
cta-smc is up-to-date
svc-sw-reporting is up-to-date
Starting lc-landing-page  ...
svc-legacy-auth is up-to-date
svc-cm-agent is up-to-date
Starting sw-header        ... done
Starting sw-configuration ... done
Starting sw-login         ... done
Starting lc-landing-page  ... done
nginx is up-to-date
svc-ctr-integration is up-to-date
Recreating svc-sse-connector ... done
```

Verify

From the SecureX portal, verify the SNA device is registered properly and the module has no issues, as shown in the image:



Refresh the SNA Module tiles, the dashboard start to show the proper SNA data, as shown in the image:



Related Information

- **If you use Secure Cloud Analytics, you can find more information in this Document**
- **Secure Network Analytics - System Configuration Guide 7.4.1 here .**
- **Technical Support & Documentation - Cisco Systems**