排除Secure Network Analytics Integration（前身為Stealthwatch Enterprise）的SecureX模組錯誤

目錄

[簡介](#)
[必要條件](#)
[需求](#)
[採用元件](#)
[背景資訊](#)
[安全網路分析模組錯誤](#)
[SNA CLI登入方法](#)
[疑難排解](#)
[重新啟動SSE和CTR服務](#)
[配置SMC的FQDN](#)
[驗證](#)
[相關資訊](#)

簡介

本文檔介紹如何對Secure Network Analytics Integration的SecureX模組錯誤進行故障排除。

必要條件

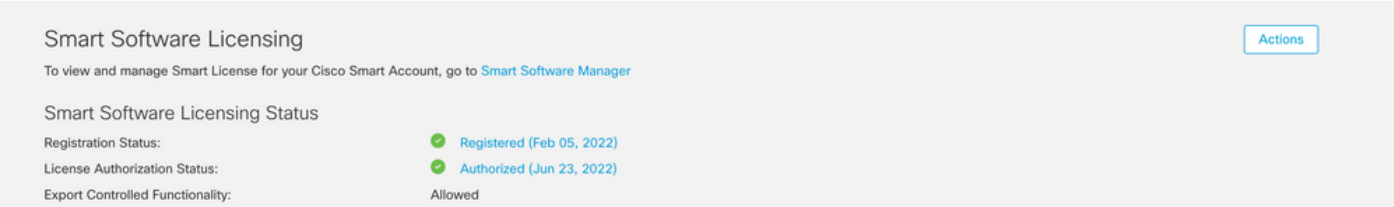
需求

思科建議您瞭解以下主題：

- 安全網路分析(SNA)主控台
- 您的Secure Network Analytics部署會按預期生成安全事件和警報
- 您的SNA控制檯需要能夠連線出站到Cisco雲: 北美雲

- 歐盟雲 亞洲(APJC)雲

- 您的SNA已在智慧許**可中註冊。導覽至Central Management > Smart Licensing**，如下圖所示：



- 建議使用用於SecureX產品的同一智慧帳戶/虛擬帳戶
- 您有一個帳戶可以訪問SecureX。為了使用SecureX和相關工具，您需要在您使用的區域雲上擁有一個帳戶

注意：如果您或您的組織已在您的區域雲上擁有帳戶，請使用已經存在的帳戶。不要新建一個。

採用元件

本檔案中的資訊是根據以下軟體版本：

- 思科安全服務交換(SSE)主控台
- 安全網路分析v7.2.1或更高版本
- SecureX控制檯

注意：每個控制檯中的帳戶必須具有管理員許可權才能執行更改。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

Cisco SecureX是思科雲中的平台，可幫助您檢測、調查、 分析和響應威脅，並使用從多個產品和來源。 此整合使您能夠在Secure Network Analytics(以前稱為 Stealthwatch):

- 在SecureX上使用安全網路分析（顯示為Stealthwatch）磁貼 用於監控關鍵運營指標的儀表板
- 利用SecureX選單轉到您的其他思科安全和第三方 整合
- 提供對您的SecureX功能區的訪問
- 向Cisco SecureX威脅響應傳送安全網路分析警報 （前身為Cisco Threat Response）Private Intelligence Store
- 允許SecureX從Secure Network Analytics請求安全事件以豐富 威脅響應工作流中的調查上下文

請參閱此處的最新SecureX和安全網路分析整合指南。

安全網路分析模組錯誤

本檔案將幫助對安全網路分析整合模組上的以下任何錯誤訊息進行疑難排解：

- 錯誤示例#1

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

- 錯誤示例#2

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

SNA CLI登入方法

有兩個使用者角色可通過SSH登入到SNA CLI

- 根
- Sysadmin

您需要使用裝置IP地址和***根***使用者角色通過SSH登入。(作為Sysadmin使用者角色，您***的操***作有限)

疑難排解

> **注意**：本文檔中提到的故障排**除必須由**Cisco **TAC工**程師執行並監督。請建立案例，以從Cisco TAC支援團隊取得適當的協助。

重新啟動SSE和CTR服務

步驟1.如果SecureX SNA模組觸發任何錯誤消息，請以Root使用者身份通過SSH登入到SNA裝置。

步驟2.運行以下命令以重新啟動**sse-connector**和**ctr-integration**服務：

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

步驟3.運行此命令以驗證服務狀態：

```
docker ps
```

服務必須顯示**UP**狀態（此外，您還可以看到服務啟動/重新啟動時的狀態時間變化），如下圖所示：

```
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
```

步驟4.刷新SecureX門戶中的SNA模組磁貼，儀表板開始顯示正確的SNA資料。

配置SMC的FQDN

如果重新啟動**sse-connector**和**ctr-integration**服務未解決問題，請導航到位置**/lancope/var/logs/containers**，然後運行以下命令：

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

驗證日誌中是否顯示以下錯誤消息：

```
docker/svc-sse-connector[1193]: time="2021-05-26T09:19:20.921548198Z" level=info msg="[FlowID:
```

如果該行存在，您需要編輯**docker-compose.yml**檔案以修復此錯誤。

步驟1.導覽至**/lancope/manifests/**path，然後找到**docker-compose.yml**檔案，如下圖所示：

```
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
```

步驟2.運行此命令可編輯**docker-compose.yml**檔案：

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

您可以使用首選方法編輯它（Nano或Vim），以便搜尋容器**sse-connector**詳細資訊，如下圖所示：

```
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
```

步驟3.導覽至SPRING_OPTS行，然後新增下一個命令列：

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

smc_hostname是SNA的FQDN，如下圖所示：

```
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
```

步驟4.儲存新更改並運行以下命令：

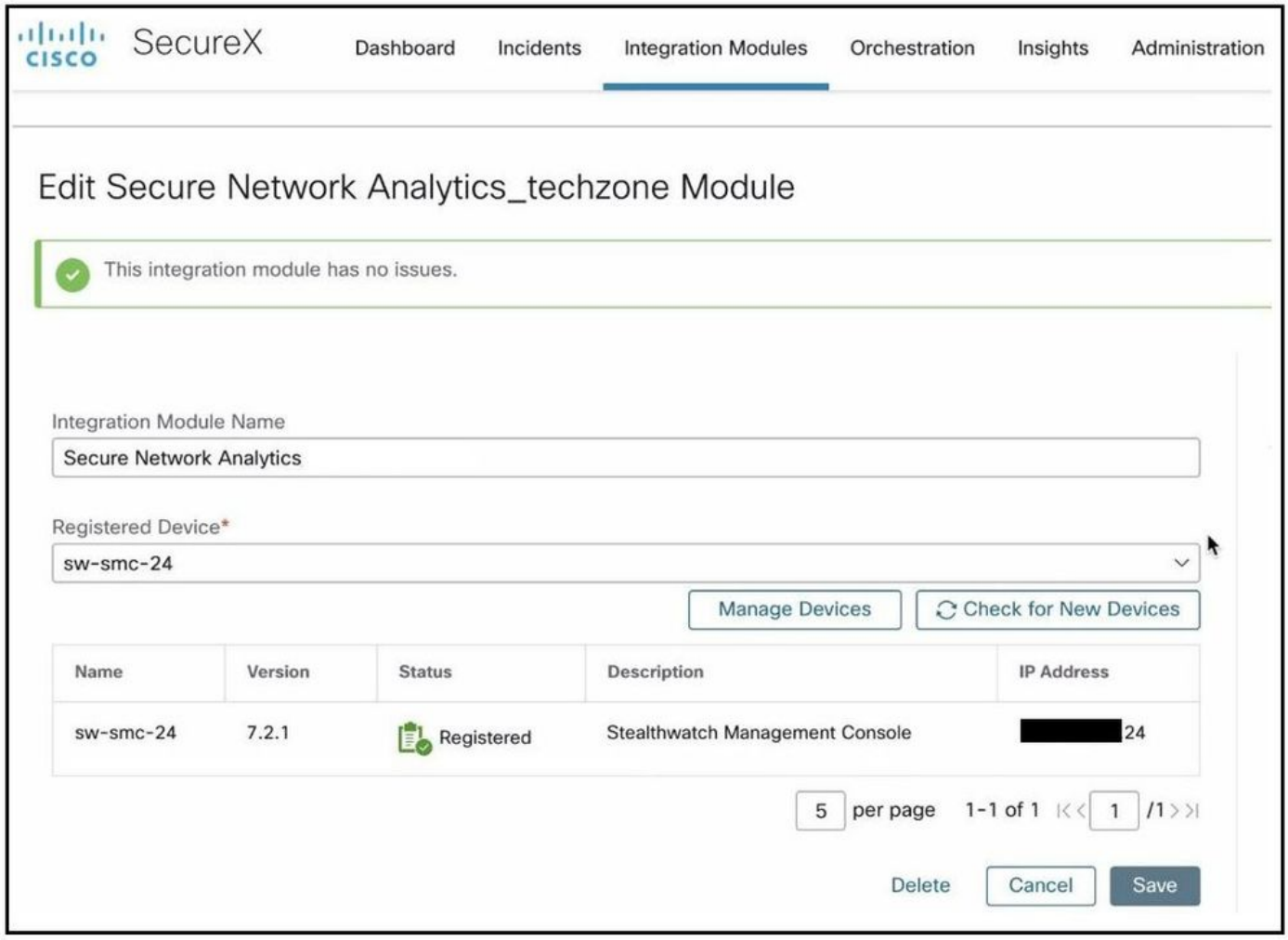
```
docker-compose up -d sse-connector
```

它會使用正確的SNA詳細資訊重新建立**docker-compose.yml**檔案，輸出必須顯示***done***狀態，如下圖所示：

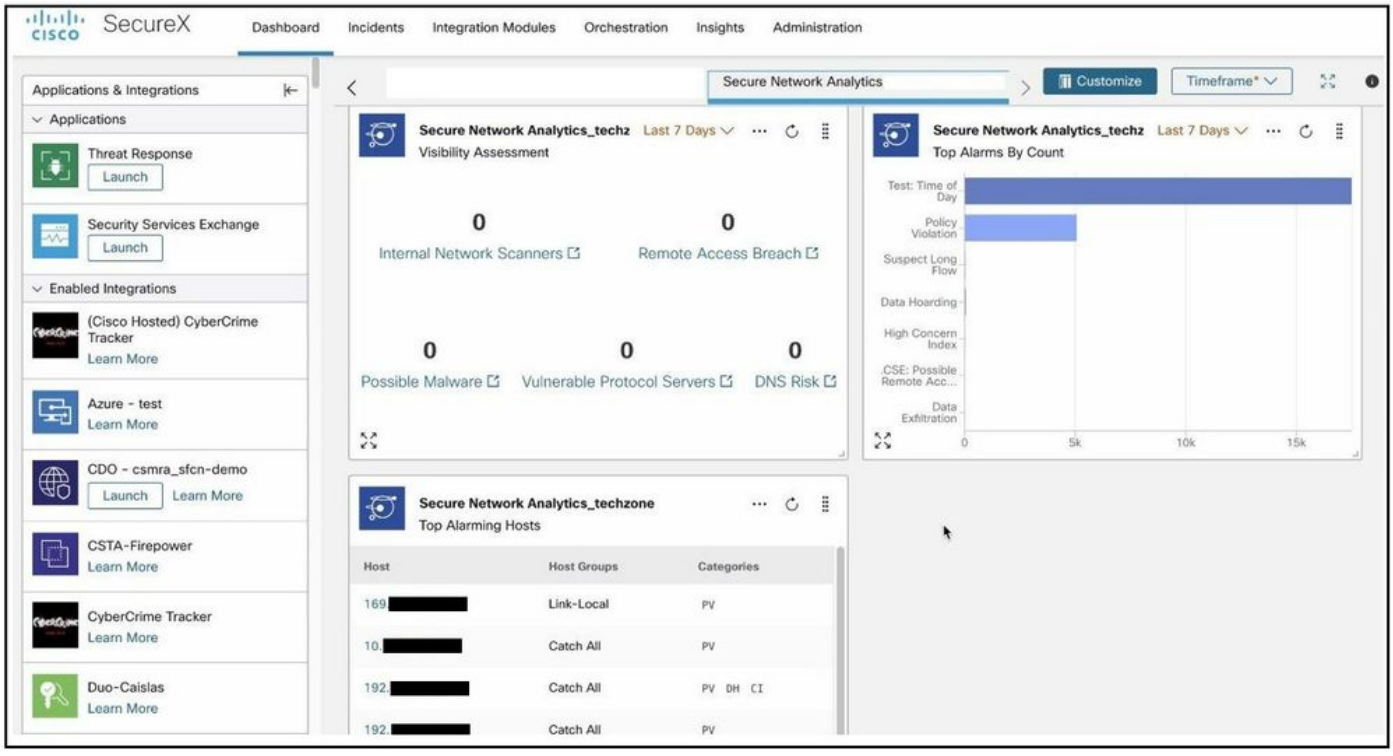
```
[tac-smc-cds-sal:/lancope/manifests# docker-compose up -d sse-connector
WARNING: The BASE_ASSETS_DIR variable is not set. Defaulting to a blank string.
Starting sw-header ...
svc-central-management is up-to-date
Starting sw-configuration ...
Starting sw-login         ...
sw-rabbitmq is up-to-date
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
```

驗證

在SecureX門戶上，驗證SNA裝置是否正確註冊，以及模組是否沒有任何問題，如下圖所示：



刷新SNA模組磁貼，儀表板開始顯示正確的SNA資料，如下圖所示：



相關資訊

- 如果您使用安全雲分析，則可以在本文檔中找到更多資訊
- 安全網路分析 — 系統配置指南 7.4.1這裡。
- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。