# أستكشاف أخطاء وحدة SecureX التنظيمية وإصلاحها لتكامل تحليلات الشبكة الآمنة (المعروفة سابقا باسم Stealthwatch Enterprise)

## المحتويات



## المقدمة

يوضح هذا المستند كيفية أستكشاف أخطاء وحدة SecureX التنظيمية وإصلاحها لتكامل تحليلات الشبكة الآمنة.

## المتطلبات الأساسية

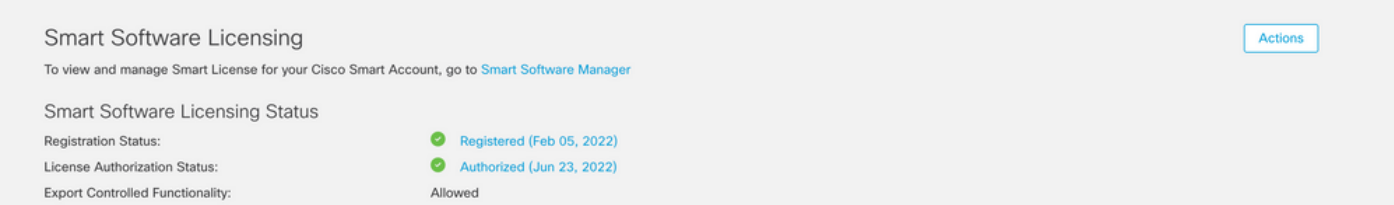
### المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- وحدة التحكم في تحليلات الشبكة الآمنة (SNA)
- يقوم نشر تحليلات الشبكة الآمنة بإنشاء أحداث الأمان والتنبيهات كما هو متوقع
- يجب أن تكون وحدة تحكم SNA الخاصة بك قادرة على الاتصال الصادر بسحابة Cisco: غيوم أمريكا الشمالية

- سحب الاتحاد الأوروبي سحب آسيا

- تم تسجيل SNA الخاص بك في **الترخيص الذكي. انتقل إلى الإدارة المركزية > الترخيص الذكي**، كما هو موضح في الصورة:




- يوصى باستخدام نفس الحساب الذكي/الحساب الظاهري الذي تستخدمه لمنتج SecureX
- لديك حساب للوصول إلى SecureX. لاستخدام SecureX والأدوات المرتبطة به، تحتاج إلى وجود حساب على السحابة الإقليمية التي تستخدمها

**ملاحظة:** إذا كان لديك بالفعل حسابات على مجموعة النظراء الإقليمية، فاستخدم الحساب الموجود بالفعل. لا تقم بإنشاء واحدة جديدة.

## المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج التالية:

- وحدة التحكم في تبادل خدمات الأمان (SSE) من Cisco
- Secure Network Analytics الإصدار 7.2.1 أو إصدار أحدث
- وحدة تحكم SecureX

**ملاحظة:** يجب أن يحتوي الحساب في كل وحدة تحكم على حقوق Administrator لإجراء تغييرات.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

# معلومات أساسية

Cisco SecureX هو النظام الأساسي في سحابة Cisco الذي يساعدك على اكتشاف الأخطاء والتحقيق فيها، تحليل التهديدات والاستجابة لها واستخدام البيانات المجمعة من منتجات متعددة و مصادر. يتيح لك هذا التكامل تنفيذ هذه المهام في تحليلات الشبكة الآمنة (سابقا) Stealthwatch):

- إستخدام تجانبات تحليلات الشبكة الآمنة (المعروضة ك Stealthwatch) على SecureX لوحة معلومات لمراقبة مقاييس العمليات الأساسية
- الاستفادة من قائمة SecureX للتحويل المحوري إلى أمان Cisco الآخر والوجهة الخارجية عمليات التكامل
- توفير الوصول إلى شريط SecureX
- إرسال تنبيهات تحليلات الشبكة الآمنة إلى إستجابة تهديد SecureX من Cisco (المعروفة سابقا باسم الاستجابة لتهديدات Cisco) مخزن المعلومات الاستخبارية الخاصة
- السماح ل SecureX بطلب أحداث الأمان من تحليلات الشبكة الآمنة لإثراء سياق التحقيق في عمليات سير العمل الخاصة بالاستجابة للتهديدات

يرجى الرجوع إلى أحدث دليل لتكامل تحليلات الشبكة الآمنة و Secure Network Analytics هنا.

## أخطاء وحدات تحليلات الشبكة الآمنة

يساعد هذا المستند في استكشاف أخطاء أي من رسائل الخطأ هذه وإصلاحها على الوحدة النمطية لتكامل تحليلات الشبكة الآمنة:

- مثال الخطأ #1

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

- مثال الخطأ #2

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

## طرق تسجيل دخول SNA CLI

هناك دوران للمستخدمين لتسجيل الدخول عبر SSH إلى واجهة سطر الأوامر لـ SNA

- جذر
- سياسي

تحتاج إلى تسجيل الدخول عبر SSH باستخدام عنوان IP للجهاز ودور ***المستخدم الجذري***. (لديك إجراءات محدودة كـ دور مستخدم ***Sysadmin***)

# استكشاف الأخطاء وإصلاحها

> **ملاحظة: يجب إجراء** أستكشاف الأخطاء وإصلاحها المذكورة في هذا المستند **والإشراف** عليها بواسطة مهندس Cisco TAC. يرجى فتح حالة للحصول على المساعدة المناسبة من فريق دعم Cisco TAC.

## إعادة تشغيل خدمات SSE و CTR

الخطوة 1. إذا كانت الوحدة النمطية SecureX SNA تقوم بتشغيل أي من رسائل الخطأ، فقم بتسجيل الدخول عبر SSH إلى جهاز SNA كمستخدم جذري.

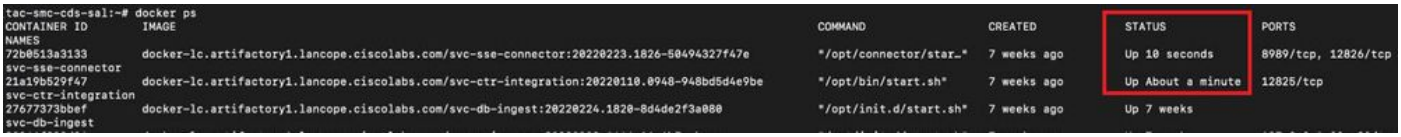
الخطوة 2. قم بتشغيل الأوامر التالية لإعادة تشغيل **sse-connector** وخدمات **دمج CTR**:

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

الخطوة 3. قم بتشغيل هذا الأمر للتحقق من حالة الخدمات:

```
docker ps
```

يجب أن تظهر الخدمات حالة **UP** (أيضا، يمكنك أن ترى تغير حالة الوقت عند بدء الخدمة/إعادة تشغيلها)، كما هو موضح في الصورة:




الخطوة 4. تحديث تجانبات وحدة SNA النمطية في مدخل SecureX، تبدأ لوحة المعلومات في

عرض بيانات SNA المنسبة.

## تكوين FQDN ل SMC

إذا لم تقم إعادة تشغيل **sse-connector** و**CTR-integration** بإصلاح المشكلة، فيرجى الانتقال إلى الموقع **/lancope/var/log/containers** وتشغيل هذه الأمر:

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

تحقق من الحصول على رسالة الخطأ هذه في السجلات:

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

إذا كان البند موجودا، تحتاج إلى تحرير ملف **docker-compose.yml** لإصلاح هذا الخطأ.

الخطوة 1. انتقل إلى **/lancope/manifest/**path وحدد موقع ملف **docker-compose.yml** ، كما هو موضح في الصورة:


الخطوة 2. قم بتشغيل هذا الأمر لتحرير ملف **docker-compose.yml**:

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

يمكنك إستخدام الطريقة المفضلة لديك لتحريرها (نانو أو فيم) للبحث في تفاصيل **موصل sse** الحاوية، كما هو موضح في الصورة:

```
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
```

الخطوة 3. انتقل إلى سطر **SPRING_OPTS** وأضف سطر الأوامر التالي:

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

يعد **smc_hostname** FQDN الخاص بـ SNA، كما هو موضح في الصورة:

```
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
```

الخطوة 4. احفظ التغيير الجديد وقم بتشغيل هذا الأمر:

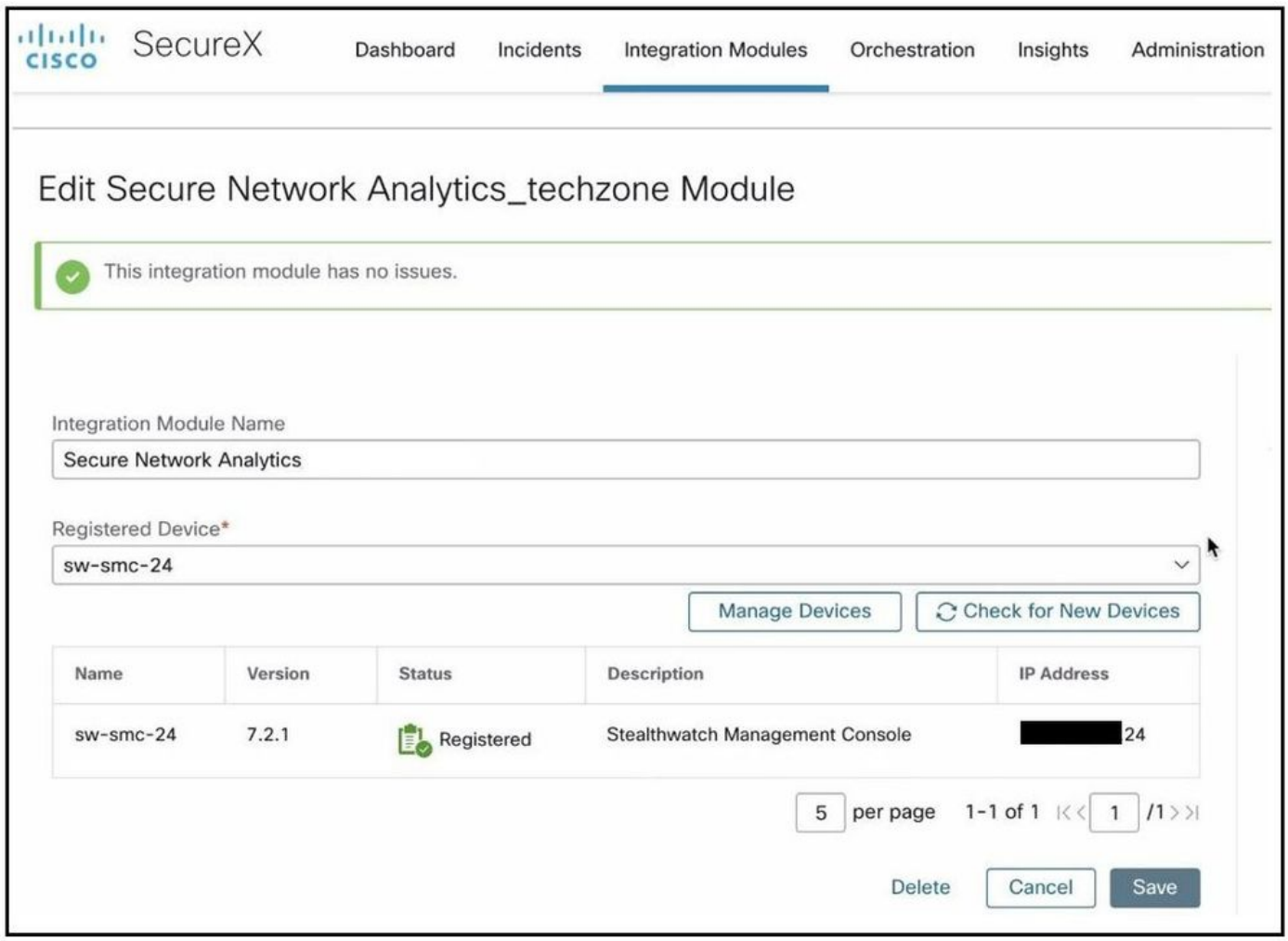
```
docker-compose up -d sse-connector
```

وهو يعني ملف **docker-compose.yml** مع التفاصيل المناسبة SNA، الإنتاج يجب أن يظهر *مرت* الحالة، كما هو موضح في الصورة:

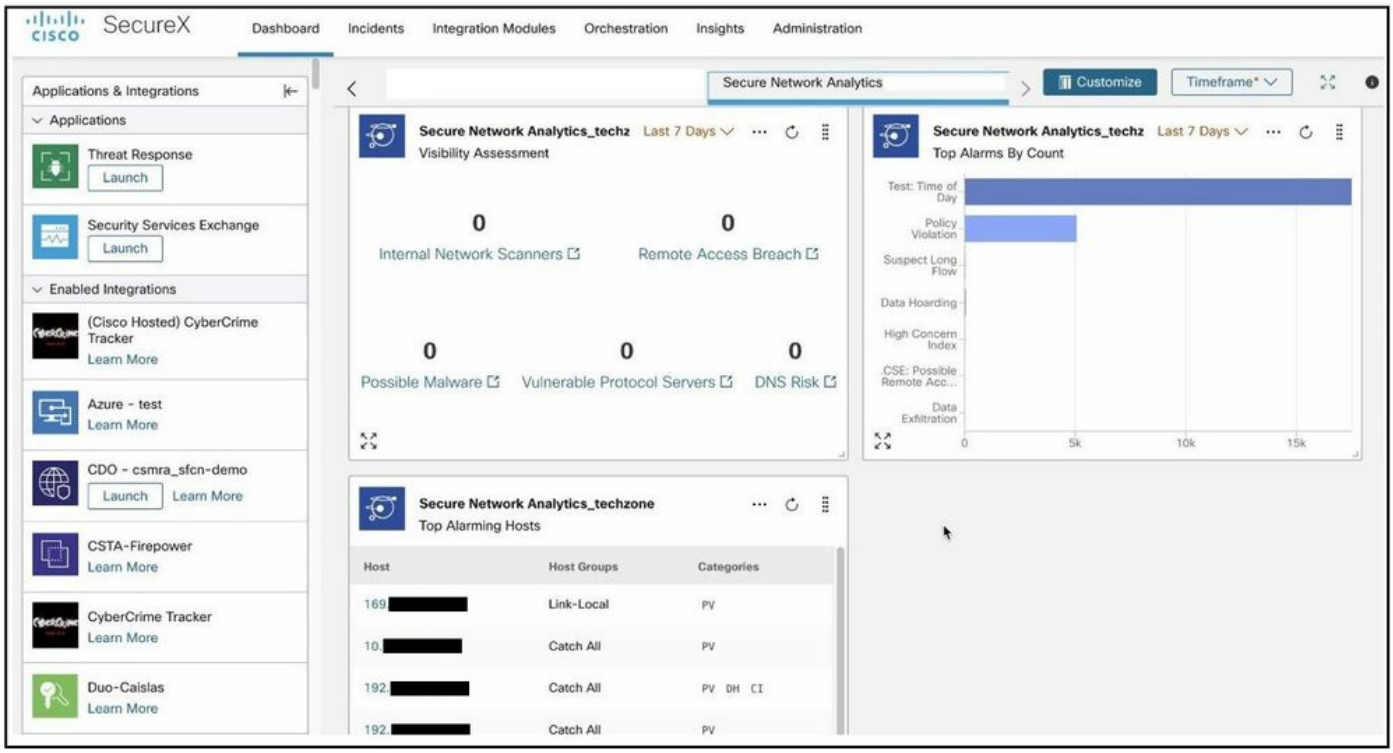
```
tac-smc-cds-sal:/lancope/manifests# docker-compose up -d sse-connector
WARNING: The BASE_ASSETS_DIR variable is not set. Defaulting to a blank string.
Starting sw-header ...
svc-central-management is up-to-date
Starting sw-configuration ...
Starting sw-login         ...
sw-rabbitmq is up-to-date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

# التحقق من الصحة

من بوابة SecureX، تحقق من تسجيل جهاز SNA بشكل صحيح ومن عدم وجود مشاكل في الوحدة النمطية، كما هو موضح في الصورة:




تحديث تجانبات وحدة SNA النمطية، تبدأ لوحة المعلومات في إظهار بيانات SNA المناسبة، كما هو موضح في الصورة:




## معلومات ذات صلة

- إذا كنت تستخدم تحليلات الشبكة الآمنة، فيمكنك العثور على مزيد من المعلومات في هذه المستند
- تحليلات الشبكة الآمنة - دليل تكوين النظام 7. 4. 1 هنا .
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).