Probleemoplossing voor SecureX-module - fouten voor beveiligde netwerkanalyse-integratie (voorheen Stealthwatch Enterprise)

Inhoud

Inleiding

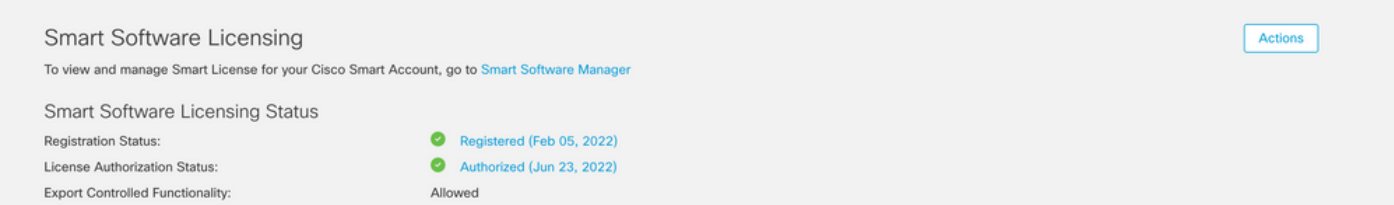
Dit document beschrijft hoe u problemen met SecureX Module-fouten kunt oplossen voor Secure Network Analytics-integratie.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Secure Network Analysis (SNA)-console
- Uw Secure Network Analytics-implementatie genereert security gebeurtenissen en alarmen zoals verwacht
- Uw SNA-console moet uitgaand verbinding kunnen maken met de Cisco-clouds: Noord-Amerikaanse clouds
- EU-wolken Azië (APJC)-wolken
- Uw SNA is geregistreerd in **slimme licenties.** Navigeren naar **Central Management > Slimme licentiëring**, zoals in de afbeelding:



- Aanbevolen wordt om dezelfde Smart Account/Virtual-account te gebruiken die u voor het SecureX-product gebruikt
- U hebt een account voor toegang tot SecureX. Om SecureX en bijbehorende tools te kunnen gebruiken, moet u een account hebben op de regionale cloud die u gebruikt

Opmerking: als u of uw organisatie al accounts heeft op uw regionale cloud, gebruik dan het account dat al bestaat. Maak geen nieuwe aan.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende softwareversies:

- Cisco Security Services Exchange (SSE)-console
- Secure Network Analytics v7.2.1 of hoger
- SecureX-console

Opmerking: de account in elke console moet beheerdersrechten hebben om een wijziging uit te voeren.

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.

Achtergrondinformatie

Cisco SecureX is het platform in de Cisco-cloud dat u helpt bij het detecteren, onderzoeken en en reageren op bedreigingen en de geaggregeerde gegevens van meerdere producten en bronnen. Dankzij deze integratie kunt u deze taken uitvoeren in Secure Network Analytics (voorheen Stealthwatch):

- Gebruik Secure Network Analytics (getoond als Stealthwatch) op de SecureX-controller dashboard om de belangrijkste operationele parameters te bewaken
- Gebruik het menu SecureX om naar uw andere Cisco-beveiligingssoftware en naar een externe switch te draaien integraties
- Toegang bieden tot uw SecureX-lint
- Verzend Secure Network Analytics-alarmen naar de Cisco SecureX-bedreigingsrespons (voorheen Cisco Threat Response) Private Intelligence Store
- Toestaan dat SecureX Security Events aanvraagt via Secure Network Analytics voor verrijking de onderzoekscontext in bedreigingsresponsstromen

Raadpleeg hier de meest recente integratiegids voor SecureX en Secure Network Analytics.

Fouten in Secure Network Analysis Module

Dit document helpt bij het oplossen van deze foutmeldingen in de Secure Network Analysis Integration Module:

- #1 foutenvoorbeeld

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

- #2 foutenvoorbeeld

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

SNA CLI-inlogmethoden

Er zijn twee gebruikersrollen om via SSH in te loggen op SNA CLI

- wortel
- Sysadmin

U moet inloggen via SSH met het IP-adres van het apparaat en de gebruikersrol ***Root***. (U hebt beperkte acties als ***Sysadmin*** gebruikersrol)

Problemen oplossen

> **Opmerking**: de probleemoplossing die in dit document wordt vermeld, **moet worden uitgevoerd en gecontroleerd** door een Cisco TAC-engineer. Open een case om de juiste assistentie te krijgen van het Cisco TAC Support team.

herstart SSE- en CTR-services

Stap 1. Als SecureX SNA-module een van de foutmeldingen activeert, meldt u zich via SSH aan bij het SNA-apparaat als de Root-gebruiker.

Stap 2. Voer de volgende opdrachten uit om de **sse-connector-** en **ctr-**integratieservices opnieuw te starten:

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

Stap 3. Voer deze opdracht uit om de servicestatus te controleren:

```
docker ps
```

De services moeten de status **UP** tonen (ook kunt u de statustijdwijzigingen zien wanneer de service wordt gestart/opnieuw opgestart), zoals in de afbeelding:

Stap 4. Verfris de SNA Module tegels in SecureX portaal, begint het dashboard de juiste SNA

gegevens te tonen.

Configureer de FQDN van de SCM

Als het opnieuw starten van **sse-connector** en **ctr-integratie** services niet oplossen van het probleem, navigeer dan naar de locatie**/lancope/var/logs/containers** en voer deze opdracht uit:

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

Controleer of u deze foutmelding in de logbestanden krijgt:

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

Als de regel bestaat, moet u het bestand **docker-compose.yml** bewerken om deze fout te herstellen.

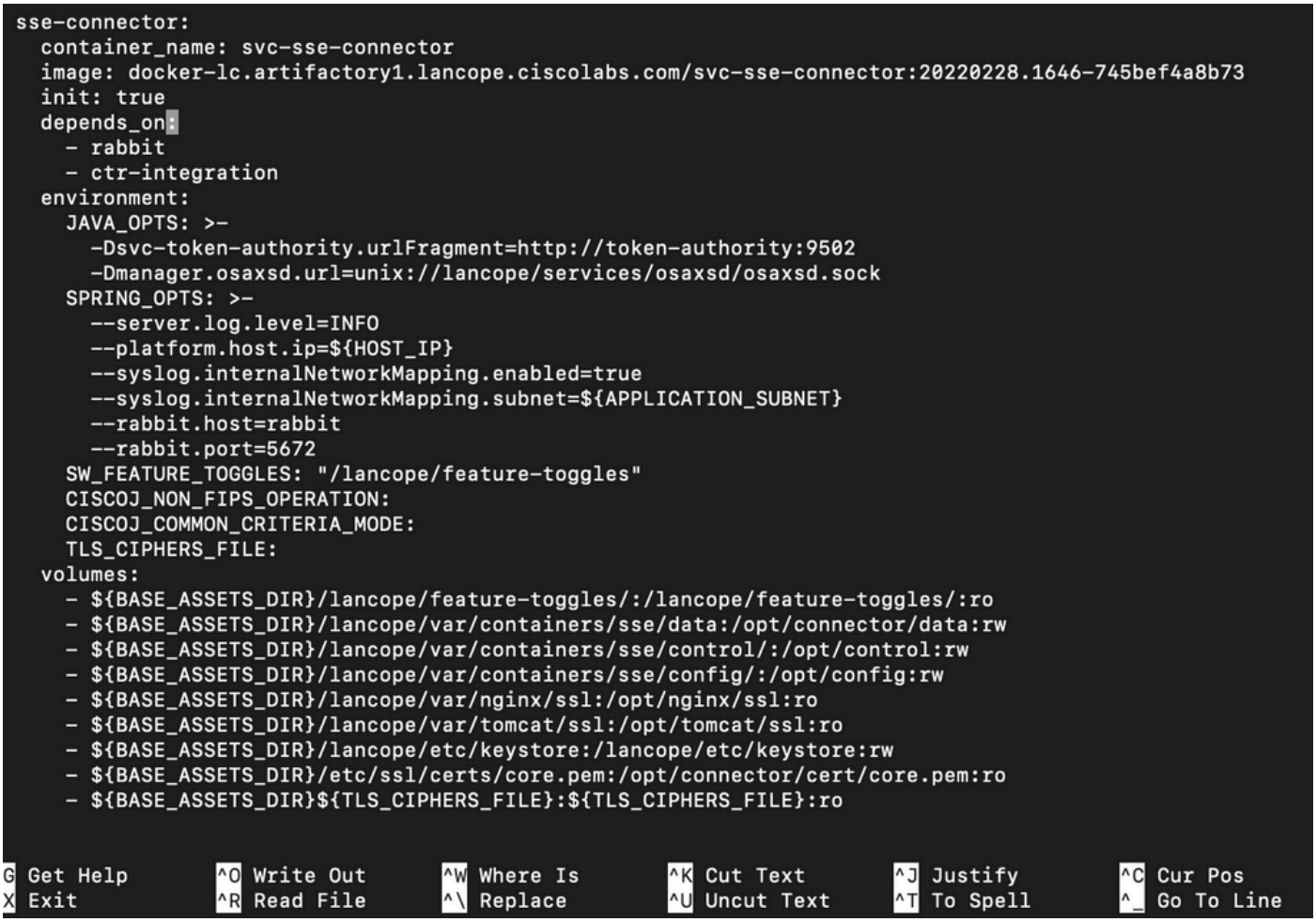
Stap 1. Navigeer in **/lancope/manifests/**path en lokaliseer **docker-compose.yml** bestand, zoals in de afbeelding:

```
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
```

Stap 2. Voer deze opdracht uit om **docker-compose.yml-**bestand te bewerken:

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

U kunt de voorkeursmethode gebruiken om deze te bewerken (Nano of Vim) om naar de details van de **connector-connector** te zoeken, zoals in de afbeelding:



Stap 3. Navigeer naar de **SPRING_OPTS**-regel en voeg de volgende opdrachtregel toe:

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

De **smc_hostname** is de FQDN van uw SNA, zoals in de afbeelding:

```
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
```

Stap 4. Sla de nieuwe wijziging op en voer deze opdracht uit:

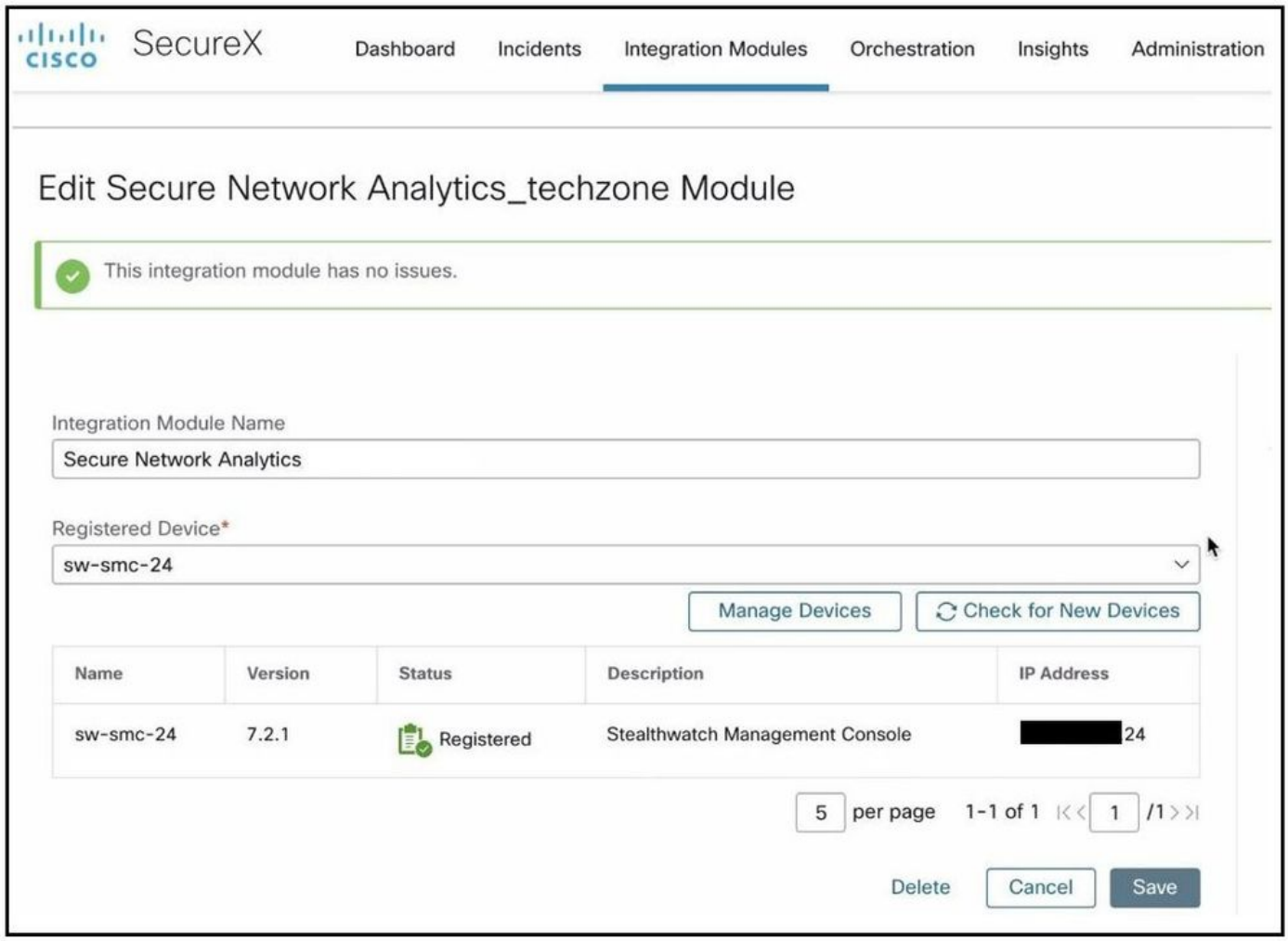
```
docker-compose up -d sse-connector
```

Het creëert het bestand **docker-compose.yml** met de juiste SNA details, de output moet *gedaan* status tonen, zoals in de afbeelding:

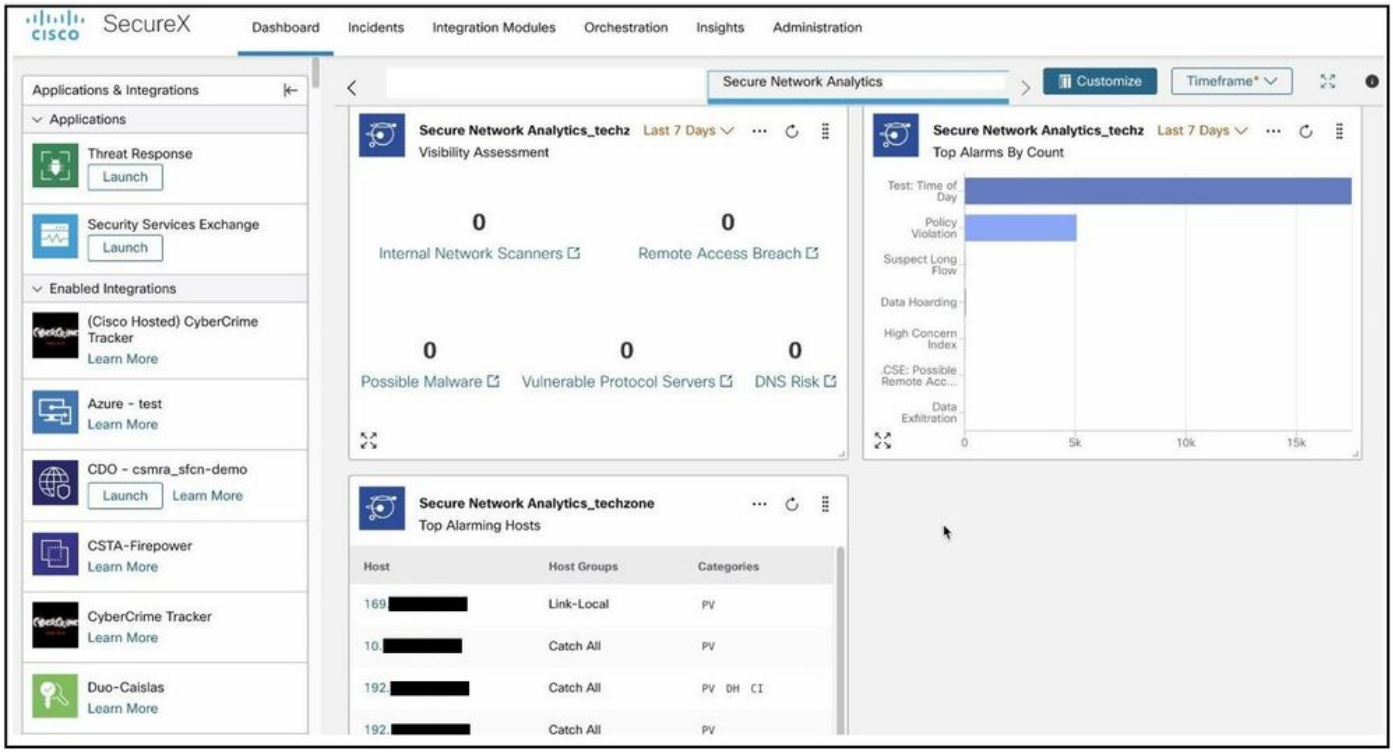
```
[tac-smc-cds-sal:/lancope/manifests# docker-compose up -d sse-connector
WARNING: The BASE_ASSETS_DIR variable is not set. Defaulting to a blank string.
Starting sw-header ...
svc-central-management is up-to-date
Starting sw-configuration ...
Starting sw-login         ...
sw-rabbitmq is up-to-date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

Verifiëren

Controleer vanuit het SecureX-portal of het SNA-apparaat correct is geregistreerd en of de module geen problemen heeft, zoals in de afbeelding:



Verfris de tegels van de SNA Module, begint het dashboard om de juiste SNA gegevens, zoals aangetoond in het beeld te tonen:



Gerelateerde informatie

- Als u Secure Cloud Analytics gebruikt, vindt u meer informatie in dit document
- Secure Network Analytics - Handleiding voor systeemconfiguratie 7.4.1. hier.
- Technische ondersteuning en documentatie – 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.