Risoluzione dei problemi relativi agli errori del modulo SecureX per l'integrazione Secure Network Analytics (in precedenza Stealthwatch Enterprise)

Sommario

Introduzione

In questo documento viene descritto come risolvere i problemi relativi agli errori del modulo SecureX per l'integrazione Secure Network Analytics.

Prerequisiti

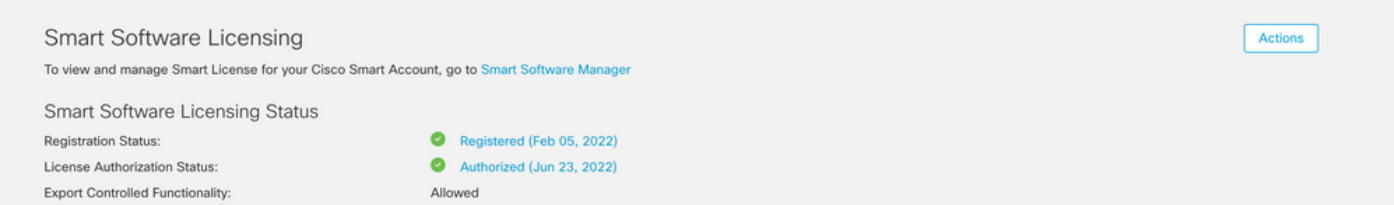
Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Console Secure Network Analytics (SNA)
- La distribuzione di Secure Network Analytics genera eventi di sicurezza e allarmi come previsto
- La console SNA deve essere in grado di connettersi in uscita ai cloud Cisco: Nuvole in Nord America

- Nuvole UE Nuvole in Asia (APJC)

- La SNA è registrata in **Smart Licensing. Passare a Gestione centrale > Smart Licensing**, come mostrato nell'immagine:



- Si consiglia di utilizzare lo stesso Smart Account/account virtuale utilizzato per il prodotto SecureX
- Si dispone di un account per accedere a SecureX. Per utilizzare SecureX e gli strumenti associati, è necessario disporre di un account nel cloud regionale utilizzato

Nota: se l'utente o l'organizzazione dispone già di account nel cloud regionale, utilizzare l'account già esistente. Non crearne uno nuovo.

Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni software:

- Console Cisco Security Services Exchange (SSE)
- Secure Network Analytics v7.2.1 o versioni successive
- Console SecureX

Nota: per eseguire una modifica, l'account in ogni console deve disporre di diritti di amministratore.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Cisco SecureX è la piattaforma del cloud Cisco che consente di rilevare, analizzare, analizzare e rispondere alle minacce e utilizzare i dati aggregati di più prodotti e fonti. Questa integrazione consente di eseguire queste attività in Secure Network Analytics (in precedenza Stealthwatch):

- Utilizza le tessere di Secure Network Analytics (visualizzate come Stealthwatch) su SecureX dashboard per monitorare le metriche operative chiave
- Utilizzare il menu SecureX per eseguire il pivot su altri prodotti Cisco Security e di terze parti integrazioni
- Accesso alla barra multifunzione SecureX
- Invia allarmi di analisi della rete sicura alla risposta alle minacce Cisco SecureX (in precedenza Cisco Threat Response) Archivio privato di intelligence
- Consenti a SecureX di richiedere eventi di protezione da Secure Network Analytics per l'arricchimento il contesto dell'indagine nei flussi di lavoro di risposta alle minacce

Fare riferimento alla più recente Guida all'integrazione di SecureX e Secure Network Analytics qui.

Errori del modulo Secure Network Analytics

Questo documento aiuta a risolvere i problemi relativi a uno di questi messaggi di errore nel modulo di integrazione Secure Network Analytics:

- Esempio di errore n. 1

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

- Esempio di errore n. 2

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

Metodi di login alla SNA CLI

Per accedere tramite SSH alla CLI della SNA, è necessario avere due ruoli utente

- Radice
- Sysadmin

Ènecessario eseguire l'accesso tramite SSH con l'indirizzo IP del dispositivo e il ruolo dell'utente ***root***. (azioni limitate come ruolo utente ***Sysadmin***)

Risoluzione dei problemi

> **Nota**: la risoluzione dei problemi descritta in questo documento **deve essere eseguita e supervisionata** da un tecnico Cisco TAC. Apri una richiesta per ottenere l'assistenza appropriata dal team di supporto Cisco TAC.

Riavvia i servizi SSE e CTR

Passaggio 1. Se il modulo SNA SecureX genera uno dei messaggi di errore, eseguire il login tramite SSH al dispositivo SNA come utente root.

Passaggio 2. Eseguire i comandi successivi per riavviare i servizi **sse-connector** e **ctr-integration**:

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

Passaggio 3. Eseguire questo comando per verificare lo stato dei servizi:

```
docker ps
```

I servizi devono mostrare lo stato **UP** (inoltre, è possibile visualizzare le modifiche dell'ora di avvio/riavvio del servizio), come mostrato nell'immagine:

Passaggio 4. Aggiornare i riquadri del modulo SNA nel portale SecureX, il dashboard inizia a visualizzare i dati SNA corretti.

Configurare l'FQDN di SMC

Se il riavvio di **sse-connector** e **ctr-integration** services non risolve il problema, passare alla posizione **/lancope/var/logs/containers** ed eseguire questo comando:

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

Verificare se nei log viene visualizzato questo messaggio di errore:

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

Se la riga esiste, è necessario modificare il file **docker-compose.yml** per correggere l'errore.

Passaggio 1. Individuare il percorso **/lancope/manifests/** e individuare il file **docker-compose.yml**, come mostrato nell'immagine:

```
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
```

Passaggio 2. Eseguire questo comando per modificare il file **docker-compose.yml**:

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

Èpossibile utilizzare il metodo preferito per modificarlo (Nano o Vim) per cercare i dettagli del **connettore** dell'**asse del** contenitore, come mostrato nell'immagine:

```
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
```

Passaggio 3. Passare alla riga **SPRING_OPTS** e aggiungere la riga di comando successiva:

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

smc_hostname è il nome di dominio completo (FQDN) della SNA, come mostrato nell'immagine:

```
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
```

Passaggio 4. Salvare la nuova modifica ed eseguire questo comando:

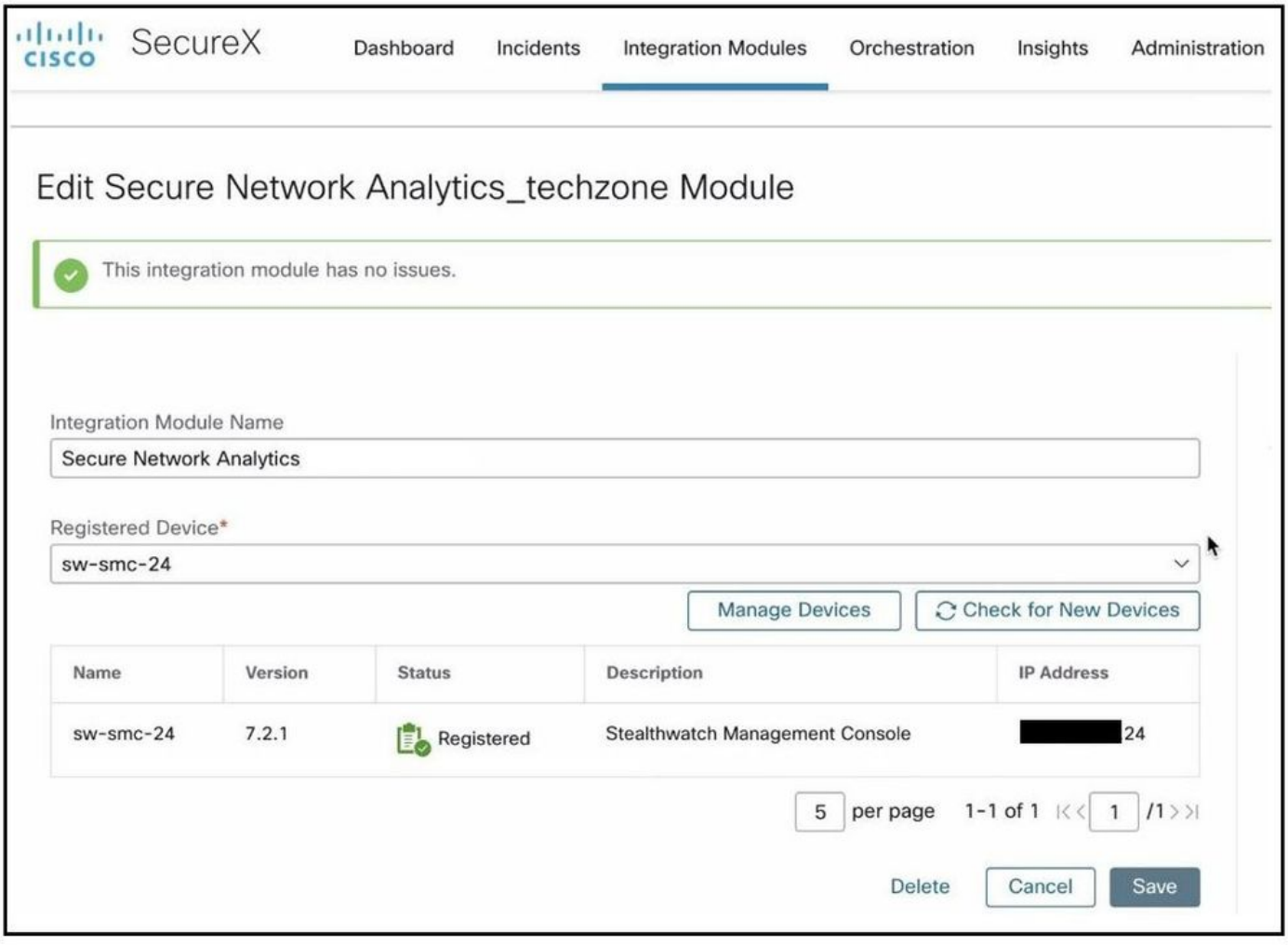
```
docker-compose up -d sse-connector
```

Ricrea il file **docker-compose.yml** con i dettagli SNA appropriati, l'output deve mostrare lo stato ***fatto***, come mostrato nell'immagine:

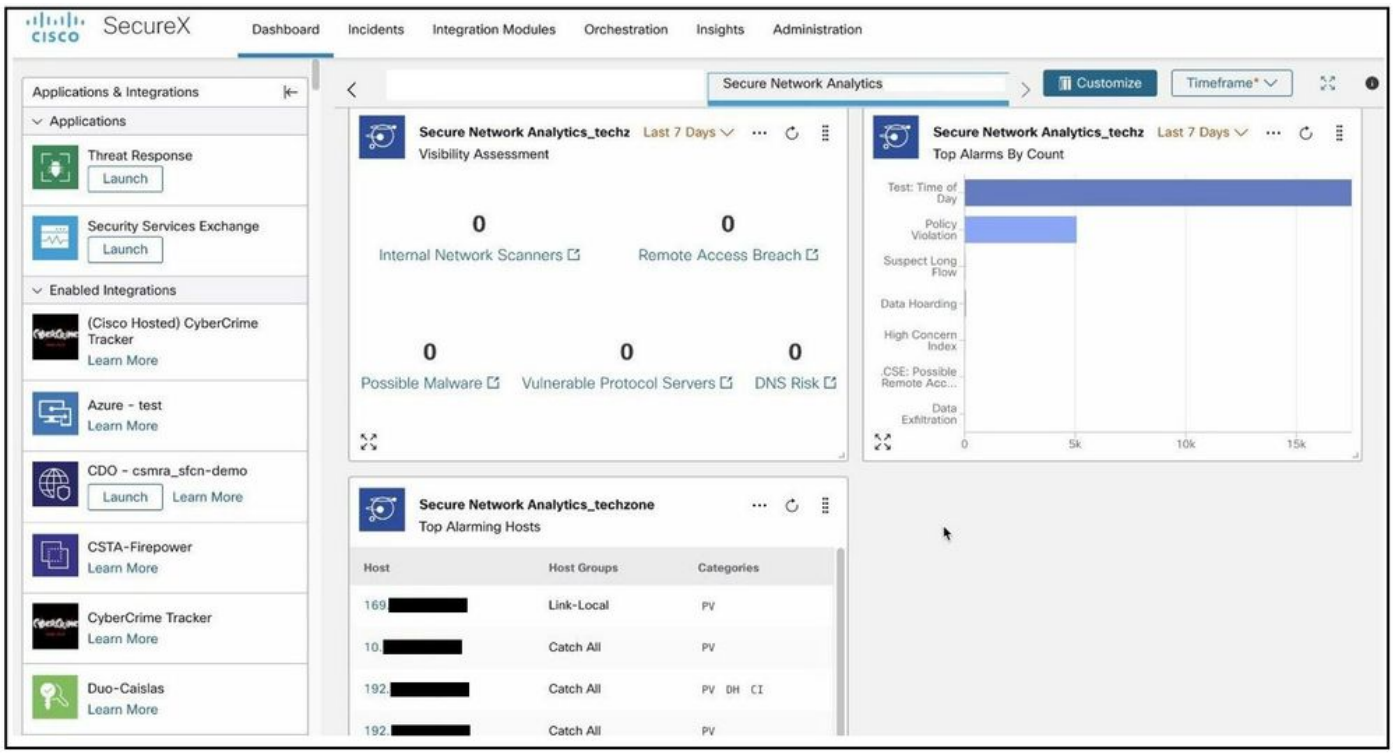
```
tac-smc-cds-sal:/lancope/manifests# docker-compose up -d sse-connector
WARNING: The BASE_ASSETS_DIR variable is not set. Defaulting to a blank string.
Starting sw-header ...
svc-central-management is up-to-date
Starting sw-configuration ...
Starting sw-login         ...
sw-rabbitmq is up-to-date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

Verifica

Dal portale SecureX, verificare che il dispositivo SNA sia registrato correttamente e che il modulo non presenti problemi, come mostrato nell'immagine:



Aggiornare i riquadri del modulo SNA, il dashboard inizia a visualizzare i dati SNA corretti, come mostrato nell'immagine:



Informazioni correlate

- Se utilizzi Secure Cloud Analytics, puoi trovare ulteriori informazioni in questo documento
- Secure Network Analytics - Guida alla configurazione del sistema 7.4.1 qui .
- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).