Fehlerbehebung bei Fehlern des SecureX-Moduls für die Integration von sicheren Netzwerkanalysen (ehemals StealthWatch Enterprise)

Inhalt

Einleitung

In diesem Dokument wird die Fehlerbehebung bei SecureX-Modulfehlern für die Integration von Secure Network Analytics beschrieben.

Voraussetzungen

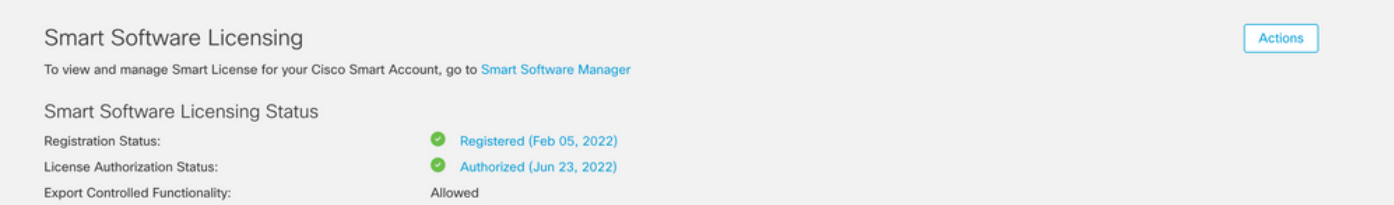
Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Secure Network Analytics (SNA)-Konsole
- Ihre Secure Network Analytics-Bereitstellung generiert erwartungsgemäß Sicherheitsereignisse und Alarme.
- Die SNA-Konsole muss eine ausgehende Verbindung mit den Cisco Clouds herstellen können: Nordamerika Clouds

- EU-Clouds Asien (APJC) Clouds

- Ihre SNA ist in **Smart Licensing** registriert. Navigieren Sie zu **Central Management > Smart Licensing**, wie in der Abbildung dargestellt:



- Es wird empfohlen, denselben Smart Account/Virtual Account zu verwenden, den Sie für das SecureX-Produkt verwenden.
- Sie haben ein Konto für den Zugriff auf SecureX. Um SecureX und die zugehörigen Tools verwenden zu können, benötigen Sie ein Konto in der regionalen Cloud, die Sie verwenden.

Hinweis: Wenn Sie oder Ihr Unternehmen bereits über Konten in Ihrer regionalen Cloud verfügen, verwenden Sie das bereits vorhandene Konto. Erstellen Sie keine neue.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen:

- Cisco Security Services Exchange (SSE)-Konsole
- Secure Network Analytics v7.2.1 oder spätere Version
- SecureX-Konsole

Hinweis: Das Konto in jeder Konsole muss über Administratorrechte verfügen, um eine Änderung vornehmen zu können.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Hintergrundinformationen

Cisco SecureX ist die Plattform in der Cisco Cloud, mit der Sie Bedrohungen analysieren, darauf reagieren und die aus mehreren Produkten zusammengetragenen Daten nutzen und Quellen. Diese Integration ermöglicht Ihnen, diese Aufgaben in Secure Network Analytics (ehemals StealthWatch):

- Verwenden Sie Secure Network Analytics-Kacheln (dargestellt als StealthWatch) auf SecureX. Dashboard zur Überwachung der wichtigsten Betriebskennzahlen
- Wechseln Sie mithilfe des SecureX-Menüs zu Ihren anderen Cisco Security-Lösungen und zu Lösungen von Drittanbietern. Integrationen
- Zugriff auf Ihre SecureX-Multifunktionsleiste
- Senden von Warnmeldungen zu sicheren Netzwerkanalysen an die Cisco SecureX-Bedrohungsreaktion (ehemals Cisco Threat Response) Privater Informationsspeicher
- SecureX kann Sicherheitsereignisse von Secure Network Analytics anfordern, um diese anzureichern den Untersuchungskontext in Threat-Response-Workflows

Weitere Informationen finden Sie hier im aktuellen SecureX and Secure Network Analytics Integration Guide.

Fehler des Moduls für sichere Netzwerkanalysen

Dieses Dokument unterstützt Sie bei der Behebung einer dieser Fehlermeldungen auf dem Secure Network Analytics Integration Module:

- Fehlerbeispiel #1

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

- Fehlerbeispiel #2

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

SNA CLI-Anmeldemethoden

Es gibt zwei Benutzerrollen für die Anmeldung über SSH bei der SNA-CLI.

- Wurzel
- Sysadmin

Sie müssen sich über SSH mit der IP-Adresse des Geräts und der ***Root-***Benutzerrolle anmelden. (Sie haben begrenzte Aktionen als ***Sysadmin-***Benutzerrolle)

Fehlerbehebung

> **Hinweis**: Die in diesem Dokument beschriebene Fehlerbehebung **muss** von einem Cisco TAC-Techniker **durchgeführt und überwacht werden**. Öffnen Sie ein Ticket, um die richtige Unterstützung vom Cisco TAC-Support-Team zu erhalten.

SSE- und CTR-Services neu starten

Schritt 1: Wenn das SecureX SNA-Modul eine der Fehlermeldungen auslöst, melden Sie sich über SSH beim SNA-Gerät als Root-Benutzer an.

Schritt 2: Führen Sie die nächsten Befehle aus, um **sse-connector** und **ctr-integration** services neu zu starten:

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

Schritt 3: Führen Sie diesen Befehl aus, um den Dienststatus zu überprüfen:

```
docker ps
```

Die Dienste müssen den **UP-**Status anzeigen (Sie können auch die Statuszeitänderungen sehen, wenn der Dienst gestartet/neu gestartet wird), wie im Bild gezeigt:

```
tac-smc-cds-sal:~# docker ps
CONTAINER ID        IMAGE                                                                                  COMMAND                  CREATED             STATUS              PORTS                     NAMES
72b0513a3133        docker-lc.artifactory1.lancope.ciscolabs.com/svc-sse-connector:20220223.1826-58494327f47e   "/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
```

Schritt 4: Aktualisieren Sie die Kacheln des SNA-Moduls im SecureX-Portal. Das Dashboard zeigt

dann die richtigen SNA-Daten an.

Konfigurieren des FQDN des SMC

Wenn der Neustart **von sse-connector** und **ctr-integration** services das Problem nicht behebt, navigieren Sie zum Speicherort/**lancope/var/logs/container** und führen den folgenden Befehl aus:

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

Überprüfen Sie, ob die folgende Fehlermeldung in den Protokollen angezeigt wird:

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

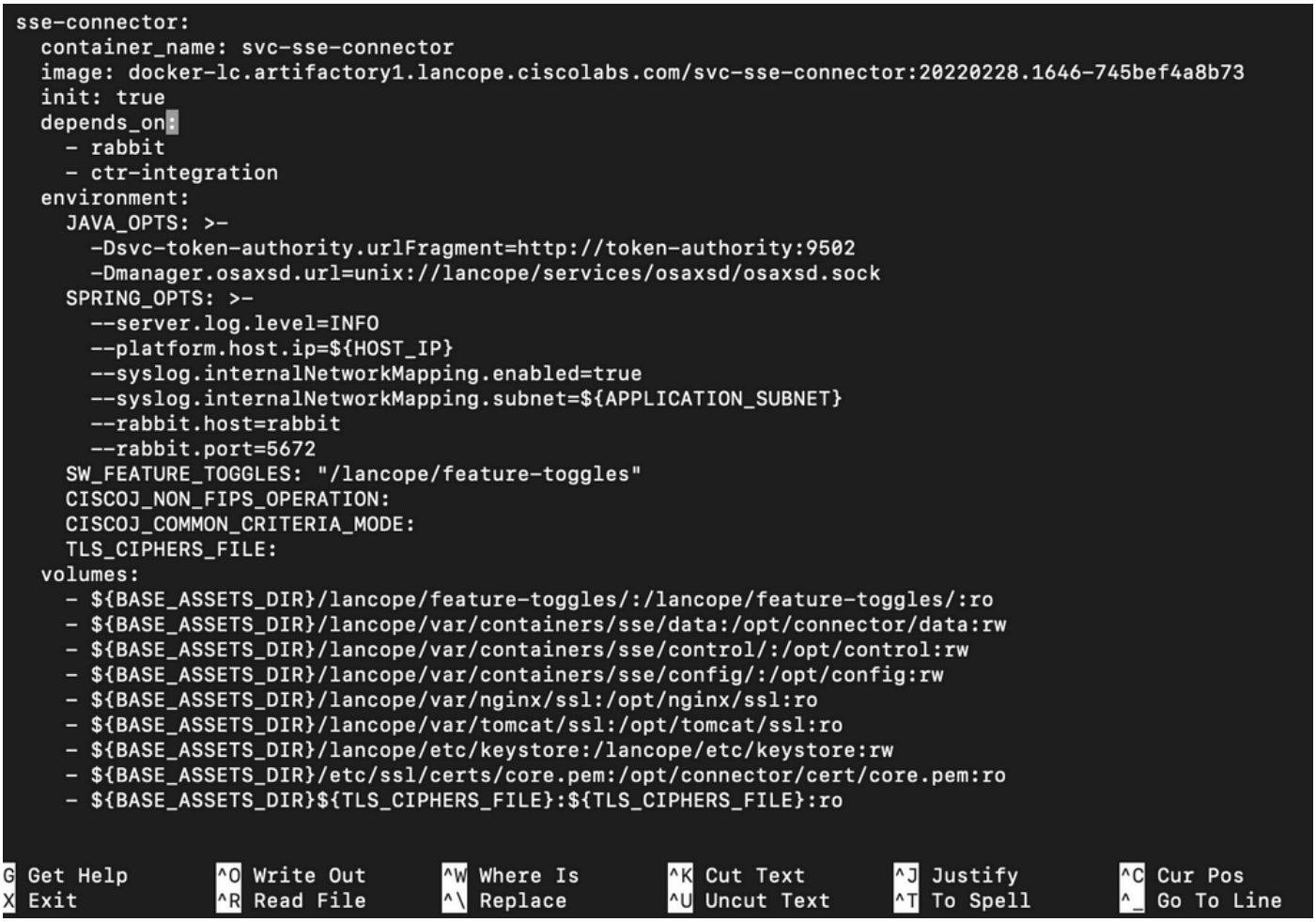
Wenn die Zeile existiert, müssen Sie die Datei **docker-compose.yml** bearbeiten, um diesen Fehler zu beheben.

Schritt 1: Navigieren Sie in **/lancope/manifests/**path, und suchen Sie die Datei **docker-compose.yml**, wie im Bild gezeigt:

Schritt 2: Führen Sie diesen Befehl aus, um die Datei **docker-compose.yml** zu bearbeiten:

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

Sie können Ihre bevorzugte Methode verwenden, um sie zu bearbeiten (Nano oder Vim), um die Container-**Sse-Connector-**Details zu durchsuchen, wie im Bild gezeigt:



Schritt 3: Navigieren Sie zur Zeile **SPRING_OPTS**, und fügen Sie die nächste Befehlszeile hinzu:

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

Der **smc_hostname** ist der FQDN Ihrer SNA, wie im Bild gezeigt:

```
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
```

Schritt 4: Speichern Sie die neue Änderung, und führen Sie den folgenden Befehl aus:

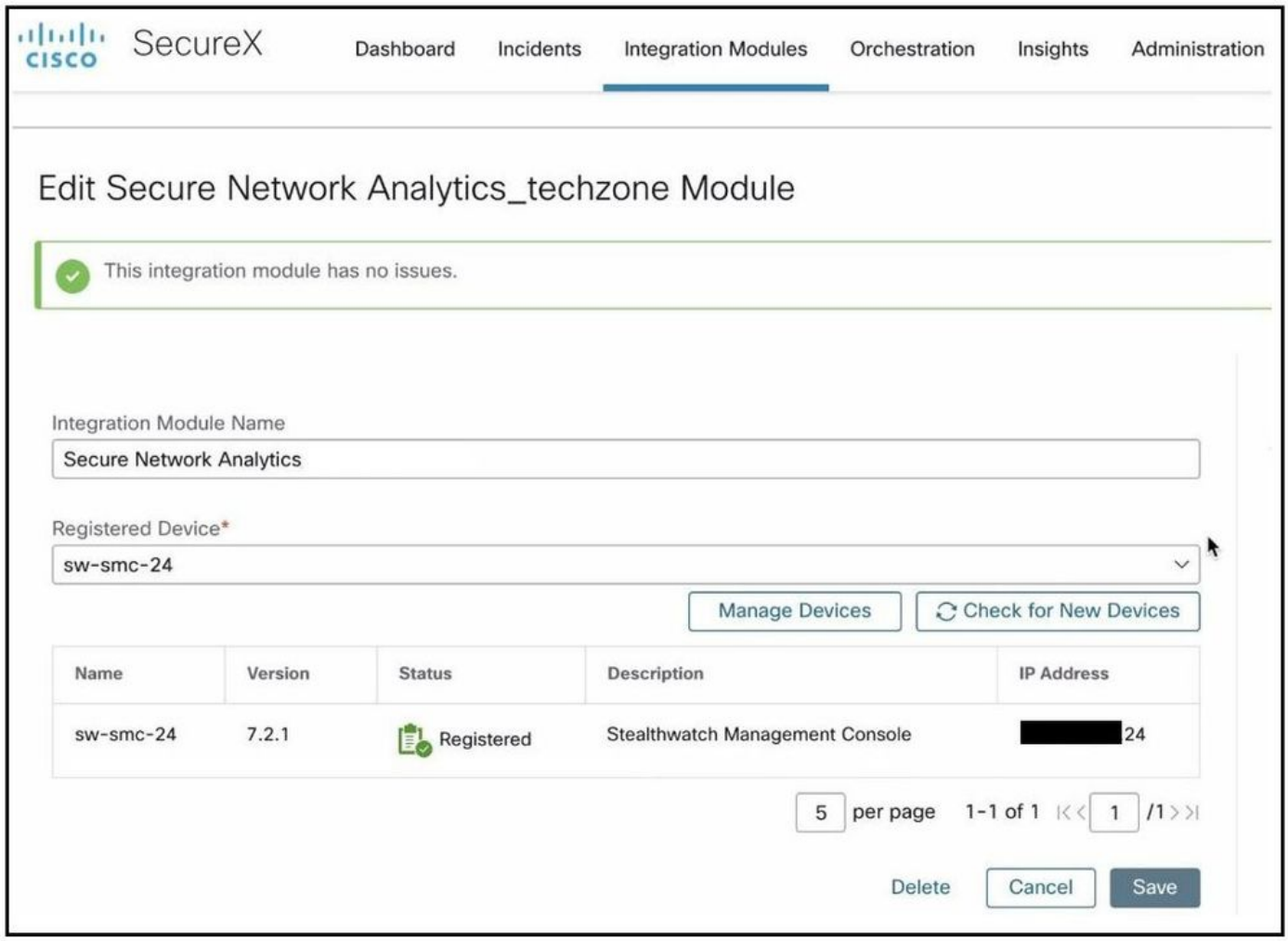
```
docker-compose up -d sse-connector
```

Es stellt die Datei **docker-compose.yml** mit den richtigen SNA-Details wieder her. Die Ausgabe muss den Status ***done*** anzeigen, wie im Bild gezeigt:

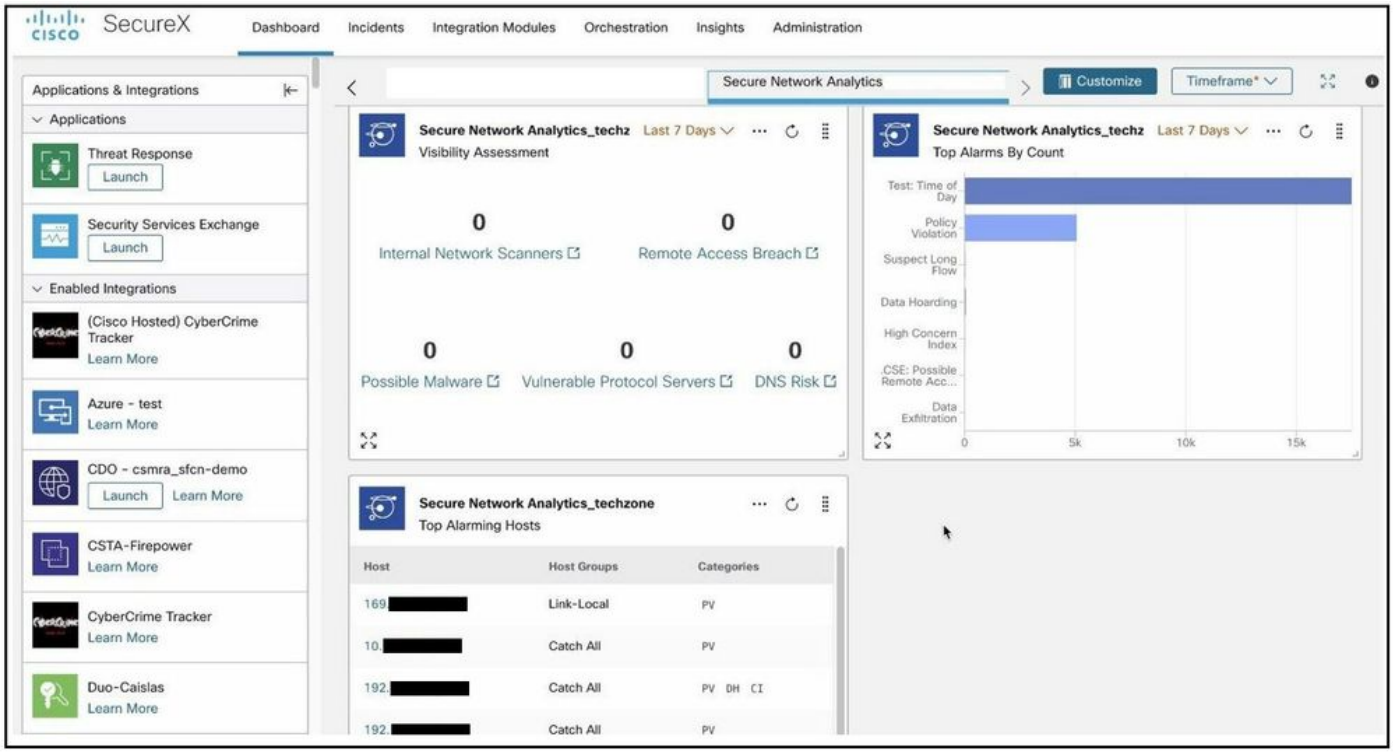
```
[tac-smc-cds-sal:/lancope/manifests# docker-compose up -d sse-connector
WARNING: The BASE_ASSETS_DIR variable is not set. Defaulting to a blank string.
Starting sw-header ...
svc-central-management is up-to-date
Starting sw-configuration ...
Starting sw-login         ...
sw-rabbitmq is up-to-date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

Überprüfung

Vergewissern Sie sich im SecureX-Portal, dass das SNA-Gerät ordnungsgemäß registriert ist und das Modul problemlos funktioniert, wie in der Abbildung gezeigt:



Aktualisieren Sie die Kacheln des SNA-Moduls. Das Dashboard zeigt dann die richtigen SNA-Daten an, wie im Bild gezeigt:



Zugehörige Informationen

- Wenn Sie Secure Cloud Analytics verwenden, finden Sie weitere Informationen in diesem Dokument
- Sichere Netzwerkanalysen - Leitfaden zur Systemkonfiguration 7.4.1 finden Sie hier .
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.