

Fehlerbehebung: SNMP Polling und falsche Schnittstellendetails für SNA

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurationen](#)

[Hintergrundinformationen](#)

[Fehlerbehebung](#)

[Falsche Schnittstellennamen](#)

[Exporter oder Schnittstellen fehlen](#)

[Verbindungsprobleme](#)

[Möglichkeit zur Abfrage von Exporteuren durch Validate Manager \(SMC\)](#)

[Generieren Sie eine Paketerfassung auf dem SMC unter Verwendung der IP-Adresse eines Exporteurs.](#)

[SNMP-Polling-Einstellungen überprüfen](#)

[Live-Fehlerbehebung für SNMP Polling](#)

[Testen von SNMP Polling von einem anderen Gerät](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird die Fehlerbehebung bei fehlenden Exportschnittstellen in Secure Network Analytics beschrieben.

Voraussetzungen

- Cisco empfiehlt grundlegendes SNMP-Polling
- Cisco empfiehlt grundlegende Kenntnisse im Bereich Secure Network Analytics (SNA/StealthWatch).

Anforderungen

- SNA Manager ab Version 7.4.1
- SNA Flow Collector in Version 7.4.1 oder höher
- Exporter sendet NetFlow aktiv an SNA

Verwendete Komponenten

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 kennen

- SNA Manager ab Version 7.4.1
- SNA Flow Collector in Version 7.4.1 oder höher
- SNMPwalk-Software
- Wireshark-Software

Konfigurationen

- Gerätekonfiguration: Die Exporteure müssen so konfiguriert werden, dass sie SNMP-Zugriff zulassen. Dazu gehört die Konfiguration der SNMP-Einstellungen auf jedem Gerät, einschließlich der Einrichtung von SNMP Community Strings, Zugriffskontrolllisten (ACLs) und der Definition der zu verwendenden SNMP-Version
- SNMP Polling Configuration on SNA (SNMP-Polling-Konfiguration für SNA): Nach erfolgreicher Konfiguration der Exporteure wird SNMP Polling auf dem SMC standardmäßig mithilfe voreingestellter Parameter aktiviert. Es ist wichtig, die erforderlichen Details für die Exporteure bereitzustellen, z. B. SNMP-Community-Strings und SNMP-Versionen, um sicherzustellen, dass der Abfragemechanismus optimal funktioniert.

Hintergrundinformationen

SNA bietet umfassende Statusberichte für Schnittstellen sowie die Möglichkeit, Schnittstellennamen für Exporteure anzuzeigen, die NetFlow-Daten aktiv an einen Flow Collector übertragen. Diese Schnittstellendetails werden angezeigt, wenn Sie über die Manager-Webbenutzeroberfläche zum Menü Investigate -> Interfaces (Untersuchen -> Schnittstellen) navigieren.

Interface Status (Since Reset Hour)

INTERFACE	EXPORTER	CURRENT UTILIZATION	CURRENT TRAFFIC	MAXIMUM UTILIZATION	MAX TRAFFIC	DIRECTION	SPEED
▶ GigabitEthernet1	0.01%	66.59 Kbps	0.18%	1.78 Mbps	INBOUND	1 Gbps
▶ GigabitEthernet1	0%	27.96 Kbps	0.29%	2.9 Mbps	OUTBOUND	1 Gbps
▶ GigabitEthernet2	4.31%	43.13 Mbps	12.22%	122.23 Mbps	INBOUND	1 Gbps
▶ GigabitEthernet2	0%	30.51 Kbps	0.02%	154.43 Kbps	OUTBOUND	1 Gbps
▶ GigabitEthernet3	0.01%	110.63 Kbps	0.29%	2.93 Mbps	INBOUND	1 Gbps
▶ GigabitEthernet3	0.01%	56.49 Kbps	0.04%	396.24 Kbps	OUTBOUND	1 Gbps
▶ GigabitEthernet4	0%	3.52 Kbps	0.06%	594.94 Kbps	INBOUND	1 Gbps
▶ GigabitEthernet4	0.01%	70.79 Kbps	0.18%	1.8 Mbps	OUTBOUND	1 Gbps
▶ GigabitEthernet5	0%	346 bps	0%	2.82 Kbps	INBOUND	1 Gbps

Fehlerbehebung

Falsche Schnittstellennamen

Falls der generierte Bericht eine "ifindex-#" anzeigt, die nicht Ihren Exporterschnittstellen entspricht, deutet dies auf ein potenzielles Konfigurationsproblem mit SNMP-Polling entweder auf

dem SMC oder auf dem Exporteur selbst hin. In diesem Beispiel habe ich ein offensichtliches Problem mit dem SNMP Polling eines bestimmten Exporteurs hervorgehoben.

Interfaces (152)

Filter by Device

Interface Status (Since Reset Hour)

INTERFACE	EXPORTER	CURRENT UTILIZATION	CURRENT TRAFFIC	MAXIMUM UTILIZATION	MAX TRAFFIC	DIRECTION	SPEED
ifindex-5 ...	192.168.99.4 ...	90.93%	909.27 Mbps	162.76%	1.63 Gbps	INBOUND	1 Gbps
ifindex-8 ...	192.168.99.4 ...	85.71%	857.08 Mbps	85.71%	857.08 Mbps	OUTBOUND	1 Gbps
ifindex-26 ...	192.168.99.4 ...	85.71%	857.08 Mbps	85.71%	857.08 Mbps	INBOUND	1 Gbps
ifindex-3 ...	192.168.99.4 ...	80.46%	804.6 Mbps	82.07%	820.69 Mbps	INBOUND	1 Gbps
ifindex-25 ...	192.168.99.4 ...	79.06%	790.63 Mbps	80.29%	802.94 Mbps	OUTBOUND	1 Gbps
ifindex-16 ...	192.168.99.4 ...	79.06%	790.63 Mbps	80.29%	802.94 Mbps	INBOUND	1 Gbps
ifindex-13 ...	192.168.99.4 ...	53.29%	532.87 Mbps	94.85%	948.5 Mbps	OUTBOUND	1 Gbps
ifindex-24 ...	192.168.99.4 ...	53.29%	532.87 Mbps	94.85%	948.5 Mbps	INBOUND	1 Gbps
ifindex-0 ...	192.168.99.4 ...	0.43%	4.29 Mbps	2.58%	25.84 Mbps	OUTBOUND	1 Gbps
TenGigabitEthernet1/0/38 ...	192.168.99.4 ...	0.32%	3.17 Mbps	0.98%	9.77 Mbps	INBOUND	1 Gbps
ifindex-0 ...	192.168.99.4 ...	0.13%	1.28 Mbps	0.37%	3.66 Mbps	OUTBOUND	1 Gbps
ifindex-0 ...	192.168.99.4 ...	0.12%	1.18 Mbps	2.77%	27.74 Mbps	OUTBOUND	1 Gbps
GigabitEthernet1/0/1 ...	192.168.99.4 ...	0.1%	1 Mbps	0.32%	3.19 Mbps	INBOUND	1 Gbps
ifindex-0 ...	192.168.99.2 ...	0.06%	573.21 Kbps	1.29%	12.92 Mbps	OUTBOUND	1 Gbps
TenGigabitEthernet1/0/1 ...	192.168.99.5 ...	0.05%	531.31 Kbps	0.29%	2.86 Mbps	INBOUND	1 Gbps
TenGigabitEthernet1/0/37 ...	192.168.99.1 ...	0.05%	503.01 Kbps	2.02%	20.15 Mbps	INBOUND	1 Gbps
TenGigabitEthernet1/0/1 ...	192.168.99.2 ...	0.04%	354.1 Kbps	1.25%	12.5 Mbps	INBOUND	1 Gbps

Exporter oder Schnittstellen fehlen

Die Überprüfung von Vorlagen ist für die NetFlow-Datenverarbeitung von großer Bedeutung. Insbesondere wird sichergestellt, dass die vom Exporteur empfangene NetFlow-Vorlage alle erforderlichen Felder enthält, die für eine erfolgreiche Decodierung und Verarbeitung durch den Flow Collector erforderlich sind. Wenn keine gültige Vorlage gefunden wird, werden die zugehörigen Flows von der Decodierung ausgeschlossen, sodass sie nicht in der Schnittstellenliste aufgeführt sind.

Wenn die erwarteten Exporter/Schnittstellen nicht in der Schnittstellenliste angezeigt werden, sollten Sie die Vorlage für die eingehenden NetFlow-Daten überprüfen. Um die NetFlow-Vorlage zu überprüfen, kann auf der Flow Collector-Seite eine Paketerfassung erstellt werden, die die IP-Adresse des Exporteurs angibt, von dem NetFlow abgerufen wird, indem "x.x.x.x" geändert wird:

- Melden Sie sich bei Flow Collector über SSH oder eine Konsole mit Root-Anmeldeinformationen an.
- Führen Sie eine Paketerfassung vom betreffenden Export-IP- und NetFlow-Port aus:

```
tcpdump -s0 -v -nnn -i eth0 host x.x.x.x and port 2055 -w /lancope/var/admin/tmp/
```

.pcap

- Kopieren Sie die Paketerfassung von der Appliance auf eine Workstation, auf der die Wireshark-Anwendung installiert ist. Verwenden Sie dabei Ihre bevorzugte Methode (Beispiel: SCP, SFTP).
- Öffnen Sie die Paketerfassung mit Wireshark, und überprüfen Sie die Vorlage und die Daten, die der Exporteur an den Flow Collector sendet.

Date	Source	Destination	Protocol	Length	Info	Dst Port
19:35:07.222163	10.10.10.1	10.10.10.2	CFLOW	1416	total: 3 (v9) records Obs-Domain-ID= 257 [Data-Template:2856] [Option...	
19:35:07.222299	10.10.10.1	10.10.10.2	CFLOW	1416	total: 27 (v9) records Obs-Domain-ID= 257 [Data:2856]	
19:35:07.222377	10.10.10.1	10.10.10.2	CFLOW	1416	total: 27 (v9) records Obs-Domain-ID= 257 [Data:2856]	
19:35:07.222385	10.10.10.1	10.10.10.2	CFLOW	1416	total: 27 (v9) records Obs-Domain-ID= 257 [Data:2856]	
19:35:07.222388	10.10.10.1	10.10.10.2	CFLOW	1416	total: 27 (v9) records Obs-Domain-ID= 257 [Data:2856]	
19:35:07.222462	10.10.10.1	10.10.10.2	CFLOW	1416	total: 27 (v9) records Obs-Domain-ID= 257 [Data:2856]	

```

Frame 1: 182 bytes on wire (1456 bits), 182 bytes captured (1456 bits)
Ethernet II, Src: Cisco_94:b4:fc (8c:60:4f:94:b4:fc), Dst: VMware_84:49:4f (00:50:56:84:49:4f)
Internet Protocol Version 4, Src: 10.10.10.1, Dst: 10.10.10.2
User Datagram Protocol, Src Port: 23384, Dst Port: 2055
Cisco NetFlow/IPFIX
  Version: 9
  Count: 3
  SysUptime: 6981.285000000 seconds
  Timestamp: Jul 20, 2021 15:23:50.000000000 Eastern Daylight Time
  FlowSequence: 226153525
  SourceId: 257
  FlowSet 1 [id=0] (Data Template): 2856
    FlowSet Id: Data Template (V9) (0)
    FlowSet Length: 68
      Template (Id = 2856, Count = 15)
        Template Id: 2856
        Field Count: 15
        Field (1/15): BYTES
        Field (2/15): PKTS
        Field (3/15): OUTPUT_SNMP
        Field (4/15): IP_DST_ADDR
        Field (5/15): SRC_VLAN
        Field (6/15): IP_TOS
        Field (7/15): IPv4 ID
        Field (8/15): FRAGMENT_OFFSET
        Field (9/15): IP_SRC_ADDR
        Field (10/15): L4_DST_PORT
        Field (11/15): L4_SRC_PORT
        Field (12/15): PROTOCOL
        Field (13/15): FIRST_SWITCHED
  
```

Vergewissern Sie sich, dass die NetFlow-Vorlage die 9 erforderlichen Felder verwendet. Der genaue Name dieser Vorlagenfelder kann je nach Exportertyp variieren. Lesen Sie deshalb die Dokumentation zu dem von Ihnen konfigurierten Exportertyp:

- IP-Quelladresse
- Ziel-IP-Adresse
- Quell-Port
- Ziel-Port
- Layer-4-Protokoll
- Byte-Anzahl
- Paketanzahl

- Flow-Startzeit
- Flow-Endzeit

Um Schnittstellen korrekt anzuzeigen, fügen Sie bitte auch Folgendes hinzu:


- Schnittstellenausgang
- Schnittstelleneingang


Hier sehen Sie ein Beispiel für eine Vorlagen-Paketerfassung von einem bestimmten Exportgerät.

- Rote Pfeile: erforderliche NetFlow-Felder
- Grüne Pfeile: SNMP-Felder

```
> User Datagram Protocol, Src Port: 51431, Dst Port: 2055
v Cisco NetFlow/IPFIX
  Version: 10
  Length: 120
  > Timestamp: Jun 20, 2023 00:24:38.000000000 CST
  FlowSequence: 41662155
  Observation Domain Id: 256
  v Set 1 [id=2] (Data Template): 260
    FlowSet Id: Data Template (V10 [IPFIX]) (2)
    FlowSet Length: 104
    v Template (Id = 260, Count = 24)
      Template Id: 260
      Field Count: 24
      > Field (1/24): IPv4 ID
      > Field (2/24): IP_SRC_ADDR ←
      > Field (3/24): IP_DST_ADDR ←
      > Field (4/24): IP_TOS
      > Field (5/24): IP_DSCP
      > Field (6/24): PROTOCOL ←
      > Field (7/24): IP TTL MINIMUM
      > Field (8/24): IP TTL MAXIMUM
      > Field (9/24): L4_SRC_PORT ←
      > Field (10/24): L4_DST_PORT ←
      > Field (11/24): TCP_FLAGS
      > Field (12/24): SRC_AS
      > Field (13/24): IP_SRC_PREFIX
      > Field (14/24): SRC_MASK
      > Field (15/24): INPUT_SNMP ←
      > Field (16/24): DST_AS
      > Field (17/24): IP_NEXT_HOP
      > Field (18/24): DST_MASK
      > Field (19/24): OUTPUT_SNMP ←
      > Field (20/24): DIRECTION
      > Field (21/24): BYTES ←
      > Field (22/24): PKTS ←
      > Field (23/24): FIRST_SWITCHED ←
      > Field (24/24): LAST_SWITCHED ←
```

 Hinweis: Der im Beispielbefehl aufgeführte Port kann je nach Exportkonfiguration variieren. Der Standardwert ist 2055.

 Hinweis: Halten Sie die Paketerfassung von 5-10 Minuten laufen, je nach Exporteur kann die

 Vorlage alle N Minuten gesendet werden, und Sie müssen diese Vorlage fangen, sodass der NetFlow richtig decodiert wird. Wenn die Vorlage nicht angezeigt wird, wiederholen Sie die Paketerfassung für einen längeren Zeitraum

Verbindungsprobleme

Konnektivität prüfen: Stellen Sie sicher, dass eine Verbindung zwischen der SNA Manager-Appliance und den Exporteuren besteht. Überprüfen Sie, ob die Exporteure über die StealthWatch-Verwaltungskonsole erreichbar sind, indem Sie deren IP-Adressen pingen. Treten Probleme mit der Netzwerkverbindung auf, beheben Sie diese entsprechend, und beheben Sie die Probleme.

Möglichkeit zur Abfrage von Exporteuren durch Validate Manager (SMC)

- Stellen Sie eine Verbindung zum SNA-Manager über SSH her, und melden Sie sich mit Root-Anmeldeinformationen an.
- Analysieren Sie die Datei `/lancope/var/smc/log/smc-configuration.log`, und suchen Sie nach den Protokollen vom Typ `ExporterSnmpSession`:

```
INFO [ExporterSnmpSession] SNMP polling for 10.1.0.253 took 0s
INFO [ExporterSnmpSession] SNMP polling for 10.1.0.253 took 0s
WARN [ExporterSnmpSession] SNMP polling for 10.10.0.254 failed: java.lang.Exception: timeout
INFO [ExporterSnmpSession] SNMP polling for 10.10.0.254 took 20s
WARN [ExporterSnmpSession] SNMP polling for 10.10.0.254 failed: java.lang.Exception: timeout
INFO [ExporterSnmpSession] SNMP polling for 10.10.0.254 took 20s
```

- In diesem Abfragebeispiel wurden keine Fehler für Exporteur 10.1.0.253 erkannt. Beim Exporter 10.1.0.254 trat jedoch zunächst eine Zeitüberschreitungsfehlermeldung auf, die anschließend jedoch nach einer Verzögerung von 20 Sekunden erfolgreich ausgeführt werden konnte.

Generieren Sie eine Paketerfassung auf dem SMC unter Verwendung der IP-Adresse eines Exporteurs.

- Melden Sie sich beim Manager-Knoten über SSH oder die Konsole mit Root-Anmeldeinformationen an.
- Ausgeführt:

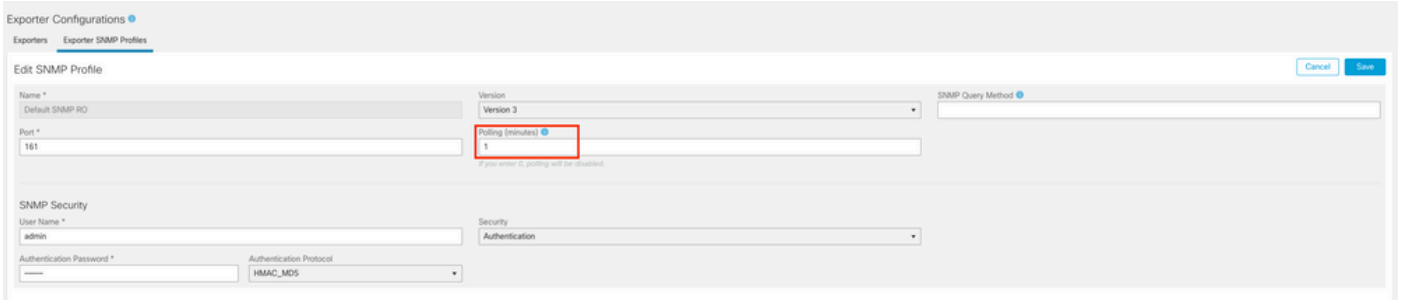
```
tcpdump -s0 -v -nnn -i [Interface] host [Exporter_IP_address] -w /lancope/var/admin/tmp/[file_name]
```

- Exportieren Sie die Paketerfassung von der Appliance mit der bevorzugten Methode (Beispiel: SCP, SFTP).
- Öffnen der Paketerfassung mit Wireshark zum Anzeigen der erfolgreichen Abrufversuche
 - Anfrage vom SMC:

Live-Fehlerbehebung für SNMP Polling

Navigieren Sie in der Webbenutzeroberfläche zu Configure -> Exporters -> Exporter SNMP Profiles.

- Stellen Sie Polling (Minuten) vorübergehend auf 1 (Minute) ein.



The screenshot shows the 'Edit SNMP Profile' configuration page. The 'Polling (minutes)' field is highlighted with a red box and contains the value '1'. Other fields include Name (Default SNMP RD), Port (161), Version (Version 3), User Name (admin), and Authentication Protocol (HMAC_MD5).

- Melden Sie sich bei SMC über SSH oder eine Konsole mit Root-Anmeldeinformationen an.
- Navigieren Sie zu diesem Ordner:

```
cd /lancope/var/smc/log
```

- Ausgeführt:

```
tail -f smc-configuration.log
```

- Für SNMPv3 lautet eine gängige Fehlermeldung:

```
failed: java.lang.IllegalArgumentException: USM passphrases must be at least 8 bytes long (RFC3414)
```

- Vergewissern Sie sich, dass das Authentifizierungskennwort im SNMP-Profil auf mindestens 8 Zeichen eingestellt ist.
- Sobald die Live-Fehlerbehebung abgeschlossen ist, setzen Sie die Polling-Konfiguration (in Minuten) für den Exporteur oder dessen Konfigurationsvorlage auf den vorherigen Wert zurück.

Testen von SNMP Polling von einem anderen Gerät

SNMP-Polling testen: Manuelles Initiieren einer SNMP-Abfrage von einem lokalen Computer an ein bestimmtes Netzwerkgerät und Überprüfen, ob eine Antwort eingeht. Dies kann mithilfe von SNMP-Polling-Tools oder Dienstprogrammen wie SNMPwalk erfolgen. Überprüfen Sie, ob das Netzwerkgerät mit den angeforderten SNMP-Daten antwortet. Wenn keine Antwort erfolgt, weist dies auf ein Problem mit der SNMP-Konfiguration oder -Verbindung hin.

- Ersetzen Sie auf Ihrem lokalen Computer mit SNMPwalk-Software "x.x.x.x" als Export-IP, und führen Sie es auf der Kommandozeile aus:

```
snmpwalk -v2c -c public x.x.x.x
```

- -v2c: gibt die zu verwendende SNMP-Version an
- -c: legt den Community-String fest

```

% snmpwalk -v2c -c public 1
SNMPv2-MIB::sysDescr.0 = STRING: Cisco IOS Software [Amsterdam], Virtual XE Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version 17.3.4a, RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2021 by Cisco Systems, Inc.
Compiled Tue 20-Jul-21 04:
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.9.1.1537
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (373833542) 43 days, 6:25:35.42
SNMPv2-MIB::sysContact.0 =
SNMPv2-MIB::sysName.0 = STRING:
SNMPv2-MIB::sysLocation.0 = STRING: cxlabs
SNMPv2-MIB::sysServices.0 = INTEGER: 78
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (0) 0:00:00.00
IF-MIB::ifNumber.0 = INTEGER: 10
IF-MIB::ifIndex.1 = INTEGER: 1
IF-MIB::ifIndex.2 = INTEGER: 2
IF-MIB::ifIndex.3 = INTEGER: 3
IF-MIB::ifIndex.4 = INTEGER: 4
IF-MIB::ifIndex.5 = INTEGER: 5
IF-MIB::ifIndex.6 = INTEGER: 6
IF-MIB::ifIndex.7 = INTEGER: 7
IF-MIB::ifIndex.8 = INTEGER: 8
IF-MIB::ifIndex.9 = INTEGER: 9
IF-MIB::ifIndex.10 = INTEGER: 10
IF-MIB::ifDescr.1 = STRING: GigabitEthernet1
IF-MIB::ifDescr.2 = STRING: GigabitEthernet2
IF-MIB::ifDescr.3 = STRING: GigabitEthernet3
IF-MIB::ifDescr.4 = STRING: GigabitEthernet4
IF-MIB::ifDescr.5 = STRING: GigabitEthernet5
IF-MIB::ifDescr.6 = STRING: VoIP-Null0
IF-MIB::ifDescr.7 = STRING: Null0
IF-MIB::ifDescr.8 = STRING: GigabitEthernet6
IF-MIB::ifDescr.9 = STRING: GigabitEthernet7
IF-MIB::ifDescr.10 = STRING: Tunnel1
IF-MIB::ifType.1 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.2 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.3 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.4 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.5 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.6 = INTEGER: other(1)

```

- Überprüfen Sie, ob der Exporteur mit SNMP-Daten antwortet.

Zugehörige Informationen

- Weitere Unterstützung erhalten Sie vom Technical Assistance Center (TAC). Ein gültiger Supportvertrag ist erforderlich: [Weltweiter Kontakt zum Cisco Support](#).
- Sie können auch die Cisco Security Analytics-Community [hier](#) besuchen.
- [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.