

Probleemoplossing voor SNMP-peiling en onjuiste interfacegegevens op SNA

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configuraties](#)

[Achtergrondinformatie](#)

[Probleemoplossing](#)

[Onjuiste interfacenamen](#)

[Ontbrekende exporteurs of interfaces](#)

[Connectiviteitsproblemen](#)

[Valideren Manager \(SMC\) mogelijkheid om exporteurs te ondervragen](#)

[Genereert een pakketopname op de SCM met behulp van het IP-adres van een exporteur.](#)

[SNMP-opiniepeilinginstellingen valideren](#)

[Live probleemoplossing bij SNMP-peilingen](#)

[SNMP-opiniepeiling testen vanaf een ander apparaat](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u problemen kunt oplossen met informatie over de interface van ontbrekende exporteurs in Secure Network Analytics

Voorwaarden

- Cisco raadt u aan over eenvoudige SNMP-opiniepeilingen (Simple Network Management Protocol) te beschikken
- Cisco raadt u aan te beschikken over fundamentele kennis van Secure Network Analytics (SNA/StealthWatch)

Vereisten

- SNA Manager in versie 7.4.1 of nieuwer
- SNA Flow Collector in versie 7.4.1 of nieuwer
- Exporteur actief NetFlow naar SNA verzenden

Gebruikte componenten

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.

- SNA Manager in versie 7.4.1 of nieuwer
- SNA Flow Collector in versie 7.4.1 of nieuwer
- SNMPwalk-software
- Software voor Wireshark

Configuraties

- Apparaatconfiguratie: de exporteurs moeten worden geconfigureerd om SNMP-toegang te verlenen. Dit houdt in dat op elk apparaat SNMP-instellingen moeten worden geconfigureerd, waaronder het instellen van SNMP-community-strings, toegangscontrolelijsten (ACL's) en het definiëren van de te gebruiken SNMP-versie
- SNMP Polling Configuration on SNA: Na een succesvolle configuratie van de exporteurs is SNMP-polling standaard ingeschakeld op de SCM met behulp van vooraf ingestelde parameters. Om ervoor te zorgen dat het opiniepeilingsmechanisme optimaal werkt, is het van cruciaal belang dat de noodzakelijke gegevens met betrekking tot de exporteurs, zoals de SNMP-community-strings en de SNMP-versies, worden verstrekt

Achtergrondinformatie

SNA beschikt over de mogelijkheid om uitgebreide rapportage van interfacestatus te bieden, samen met de mogelijkheid om interfacenamen weer te geven voor exporteurs die actief NetFlow-gegevens verzenden naar een Flow Collector. Dit interfacedetail kan worden gezien door naar het menu Investigate -> Interfaces te navigeren vanuit de Manager Web UI.

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

Probleemoplossing

Onjuiste interfacenamen

In het geval dat het gegenereerde rapport een "ifindex-#" weergeeft die niet overeenkomt met uw exporteur interfaces, suggereert het een mogelijk configuratie probleem met SNMP polling of op de SMC of op de exporteur zelf. In dit voorbeeld heb ik een schijnbaar probleem met de SNMP-

polling van een bepaalde exporteur naar voren gebracht.

INTERFACE	EXPORTER	CURRENT UTILIZATION	CURRENT TRAFFIC	MAXIMUM UTILIZATION	MAX TRAFFIC	DIRECTION	SPEED
ifindex-5		90.93%	909.27 Mbps	162.76%	1.63 Gbps	INBOUND	1 Gbps
ifindex-8		85.71%	857.08 Mbps	85.71%	857.08 Mbps	OUTBOUND	1 Gbps
ifindex-26		85.71%	857.08 Mbps	85.71%	857.08 Mbps	INBOUND	1 Gbps
ifindex-3		80.46%	804.6 Mbps	82.07%	820.69 Mbps	INBOUND	1 Gbps
ifindex-25		79.06%	790.63 Mbps	80.29%	802.94 Mbps	OUTBOUND	1 Gbps
ifindex-16		79.06%	790.63 Mbps	80.29%	802.94 Mbps	INBOUND	1 Gbps
ifindex-13		53.29%	532.87 Mbps	94.85%	948.5 Mbps	OUTBOUND	1 Gbps
ifindex-24		53.29%	532.87 Mbps	94.85%	948.5 Mbps	INBOUND	1 Gbps
ifindex-0		0.43%	4.29 Mbps	2.58%	25.84 Mbps	OUTBOUND	1 Gbps
TenGigabitEthernet1/0/38		0.32%	3.17 Mbps	0.98%	9.77 Mbps	INBOUND	1 Gbps
ifindex-0		0.13%	1.28 Mbps	0.37%	3.66 Mbps	OUTBOUND	1 Gbps
ifindex-0		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

Ontbrekende exporteurs of interfaces

Sjabloonverificatie is van groot belang in de context van NetFlow-gegevensverwerking. Het zorgt er met name voor dat de NetFlow-sjabloon die van de exporteur wordt ontvangen alle vereiste velden bevat voor succesvolle decodering en verwerking door de Flow Collector. Het niet tegenkomen van een geldig sjabloon leidt tot het uitsluiten van de bijbehorende reeks stromen van decodering, waardoor ze ontbreken in de lijst van interfaces.

Als de verwachte exporteur/interfaces niet in de lijst met interfaces staan, moet u de inkomende netwerkgegevens en de sjabloon verifiëren. Om het NetFlow-sjabloon te verifiëren kan een pakketopname worden gemaakt aan de kant van Flow Collector, door het IP te specificeren van de exporteur waar we NetFlow van krijgen door "x.x.x.x" te veranderen:

- Log in op de Flow Collector via SSH of console met root referenties.
- Voer een pakketopname uit vanuit de betreffende exporteur-IP- en netflow-poort:

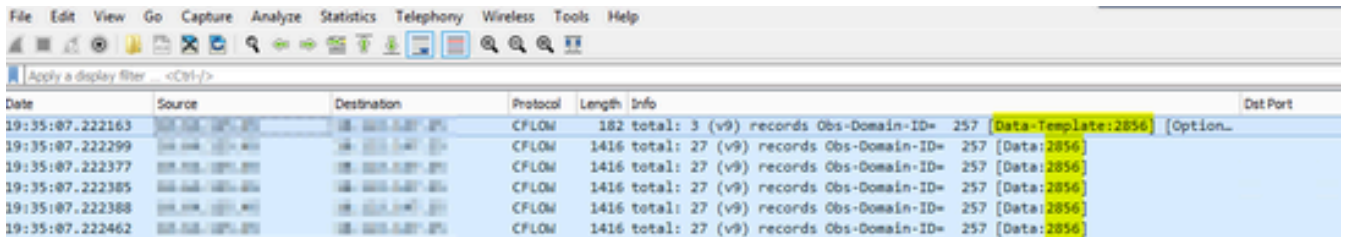
```
tcpdump -s0 -v -nnn -i eth0 host x.x.x.x and port 2055 -w /lancope/var/admin/tmp/
```

.pcap

- Kopieer de pakketopname van het apparaat naar een werkstation waarin de Wireshark-

toepassing is geïnstalleerd, gebruik de voorkeursmethode (bijvoorbeeld: SCP, SFTP).

- Open de pakketopname met Wireshark en controleer de sjabloon en de gegevens die de exporteur naar de Flow Collector verzendt



Date	Source	Destination	Protocol	Length	Info	Dest Port
19:35:07.222163	10.10.10.10	10.10.10.10	CFLOW	182	total: 3 (v9) records Obs-Domain-ID= 257 [Data-Template:2856]	
19:35:07.222299	10.10.10.10	10.10.10.10	CFLOW	1416	total: 27 (v9) records Obs-Domain-ID= 257 [Data:2856]	
19:35:07.222377	10.10.10.10	10.10.10.10	CFLOW	1416	total: 27 (v9) records Obs-Domain-ID= 257 [Data:2856]	
19:35:07.222385	10.10.10.10	10.10.10.10	CFLOW	1416	total: 27 (v9) records Obs-Domain-ID= 257 [Data:2856]	
19:35:07.222388	10.10.10.10	10.10.10.10	CFLOW	1416	total: 27 (v9) records Obs-Domain-ID= 257 [Data:2856]	
19:35:07.222462	10.10.10.10	10.10.10.10	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) on interface 0
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: 10.10.10.10, Dst: 10.10.10.10
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
```

Controleer of de NetFlow-sjabloon de 9 vereiste velden gebruikt, de exacte naam van deze sjabloonvelden kan variëren afhankelijk van het uitvoertype, dus zorg ervoor dat u de documentatie raadpleegt voor het specifieke uitvoertype dat u configureert:

- IP-bronadres
- IP-adres van bestemming
- Bronpoort
- Doelpoort
- Layer 4-protocol
- Aantal bytes
- PacketCount
- Stroombegintijd
- Flow End-tijd


Voeg ook toe om interfaces correct weer te geven:


- interface-uitgang
- interface-ingang


Hier is een voorbeeldsjabloon voor pakketopname van een bepaald exporteur-apparaat

- Rode pijlen: vereiste NetFlow-velden
- Groene pijlen: SNMP-velden

```
> 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 ←
```

 Opmerking: de poort in de voorbeeldopdracht kan variëren afhankelijk van de configuratie van uw exporteur. De standaardwaarde is 2055

 Opmerking: houd de pakketopname van 5-10 minuten lopen, afhankelijk van de exporteur

 kan de sjabloon worden verzonden elke N minuten en u moet die sjabloon te vangen zodat de NetFlow correct gedecodeerd wordt, als sjabloon niet wordt weergegeven, herhaal de pakketopname voor een langere periode

Connectiviteitsproblemen

Controleer Connectiviteit: zorg ervoor dat er connectiviteit is tussen SNA Manager apparaat en de exporteurs. Controleer of de exporteurs bereikbaar zijn via de Stealthwatch-beheerconsole door hun IP-adressen te pingen. Als er problemen zijn met de netwerkconnectiviteit, kunt u problemen oplossen en ze dienovereenkomstig oplossen.

Valideren Manager (SMC) mogelijkheid om exporteurs te ondervragen

- Verbinding maken met SNA-beheerder via SSH en inloggen met root-referenties
- Analyseer het `/lancope/var/smc/log/smc-configuration.log` bestand en zoek naar de logboeken van het type `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
```

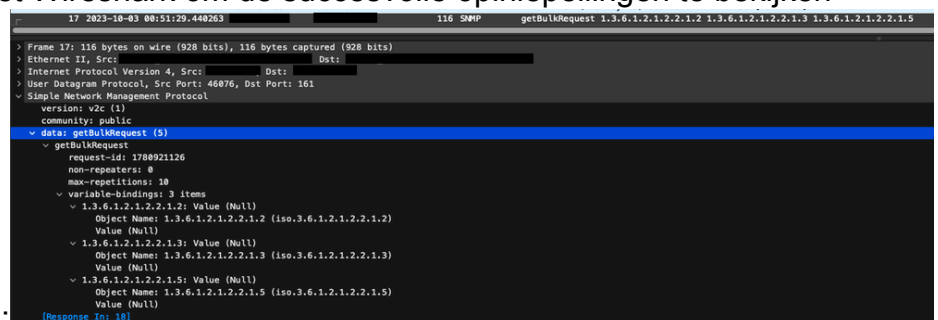
- In dit opinieonderzoek werden voor exporteur 10.1.0.253 geen fouten ontdekt. Echter, exporteur 10.1.0.254 ervoer aanvankelijk een time-out foutmelding, maar slaagde er vervolgens in om de enquête succesvol uit te voeren na een vertraging van 20 seconden.

Genereert een pakketopname op de SCM met behulp van het IP-adres van een exporteur.

- Log in op het Manager knooppunt via SSH of console met root referenties
- Voer uit:

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

- Exporteer de pakketopname van het apparaat met de voorkeursmethode (Voorbeeld: SCP, SFTP)
- Open de pakketopname met Wireshark om de succesvolle opiniepeilingen te bekijken



```
17 2023-10-03 00:51:29.440263 116 SNMP getBulkRequest 1.3.6.1.2.1.2.2.1.2 1.3.6.1.2.1.2.2.1.3 1.3.6.1.2.1.2.2.1.5
> Frame 17: 116 bytes on wire (928 bits), 116 bytes captured (928 bits) on interface
> Ethernet II, Src: [redacted], Dst: [redacted]
> Internet Protocol Version 4, Src: [redacted], Dst: [redacted]
> User Datagram Protocol, Src Port: 46076, Dst Port: 161
> Simple Network Management Protocol
  version: v2c (1)
  community: public
  data: getBulkRequest (5)
    getBulkRequest
      request-id: 1708921126
      non-repeters: 0
      max-repetitions: 10
      variable-bindings: 3 items
        1.3.6.1.2.1.2.2.1.2: Value (Null)
          Object Name: 1.3.6.1.2.1.2.2.1.2 (iso.3.6.1.2.1.2.2.1.2)
          Value (Null)
        1.3.6.1.2.1.2.2.1.3: Value (Null)
          Object Name: 1.3.6.1.2.1.2.2.1.3 (iso.3.6.1.2.1.2.2.1.3)
          Value (Null)
        1.3.6.1.2.1.2.2.1.5: Value (Null)
          Object Name: 1.3.6.1.2.1.2.2.1.5 (iso.3.6.1.2.1.2.2.1.5)
          Value (Null)
    [Response (0)]
```

- Verzoek van de SMC:

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), Version (Version 3), Port (161), User Name (admin), and Authentication Protocol (HMAC_MD5).

- Log in op de SCM via SSH of console met root referenties.
- Naar deze map navigeren:

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

- Voer uit:

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

- Voor SNMPv3 zou een veelvoorkomende foutmelding zijn:

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

- Controleer of het verificatiewachtwoord in het SNMP-profiel is ingesteld op 8 tekens of meer.
- Als het live oplossen van problemen is voltooid, retourneert u de Polling (minuten)-configuratie voor de exporteur of de configuratiesjabloon naar de vorige waarde.

SNMP-opiniepeiling testen vanaf een ander apparaat

Test SNMP Polling: Start handmatig een SNMP poll van een lokale machine naar een specifiek netwerkapparaat en controleer of het een antwoord ontvangt. Dit kan worden gedaan met behulp van SNMP-opiniepeilingtools of hulpprogramma's zoals SNMPwalk. Controleer of het netwerkapparaat met de gevraagde SNMP-gegevens reageert. Als er geen reactie is, wijst het op een probleem met de configuratie of de connectiviteit van SNMP.

- Vervang op uw lokale machine met SNMPwalk-software "x.x.x.x" voor de exporteur IP en start op CLI:

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

- -v2c: specificeert de te gebruiken SNMP-versie
- -c: stelt de community-string in

```
% 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)
```

- Controleer of de exporteur met SNMP-gegevens reageert

Gerelateerde informatie

- Voor extra assistentie kunt u contact opnemen met het Technical Assistance Center (TAC). Een geldig ondersteuningscontract is vereist: [Cisco's wereldwijde contactgegevens voor ondersteuning](#).
- U kunt [hier](#) ook de Cisco Security Analytics [Community](#) bezoeken.
- [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.