

Configuratiegids gebruiken voor integratie van DRA's van meerdere leveranciers

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configuratiestappen en best practices](#)

[Stap 1: Bepaal de connectiviteitsmodus van de DRA \(inkomende versus uitgaande peers\)](#)

[Stap 2: Inkomende peer configureren in de beleidsmaker](#)

[Stap 3: Host-IP-adres AVP configureren](#)

[Stap 4: Uitwisseling van peer-mogelijkheden valideren](#)

[Stap 5: Zorg ervoor dat de unieke bronhostnaam voor de diameter wordt gedefinieerd bij elke diameter-peer-node](#)

[Stap 6: Configureer de volgende hoprouteringstabel voor DRA-peers](#)

Inleiding

In dit document worden de configuratiestappen en best practices beschreven voor de integratie van DRA's van meerdere leveranciers in het Cisco Policy Suite (CPS) PCRF-cluster.

Voorwaarden

Vereisten

Cisco beveelt aan dat ingenieurs die met deze oplossing werken, vertrouwd zijn met deze onderwerpen:

- Linux-besturingssysteem
- Cisco Policy Suite (CPS) platform- en clusterarchitectuur
- Functie Beleids- en heffingsregels (PCRF)
- Gebruik van de VI-editor
- Wireshark-netwerkanalysetool

Gebruikte componenten

De informatie in dit document is gebaseerd op CPS 25.1 versie en AlmaLinux release 8.10.

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.

Configuratiestappen en best practices

Stap 1: Bepaal de connectiviteitsmodus van de DRA (inkomende versus uitgaande peers)

- Inkomende peers: De PCRF is geconfigureerd om verbindingsverzoeken van aangewezen diameterpeers te accepteren. De peer node initieert de Diameter Capabilities-Exchange-Request (CER) naar de PCRF.
- Outbound Peers: De PCRF is geconfigureerd om de CER te initiëren naar zijn peers.

Best practice:

Configureer voor de meeste DRA-integraties van meerdere leveranciers de DRA als een inkomende peer, waarbij de DRA de CER naar de PCRF initieert.

Stap 2: Inkomende peer configureren in de beleidsmaker

Configureer binnen de GUI voor beleidsopbouw de inkomende peer name en peer realm, waarbij u naar de tabellen Inbound Peers en Realms verwijst.



Opmerking: Raadpleeg de CPS Mobile Configuration Guide, versie 25.1.0, onder het gedeelte Diameter Stack Configuration voor gedetailleerde parameterbeschrijvingen.

Deze parameters kunnen worden geconfigureerd onder Inbound Peers:

h2>peers-tabel

Parameter	Beschrijving
leeftijdsgenoten	Bepaalt welke peer-namen toestemming hebben om verbindingen met PCRF te initiëren.
Lokale hostnaam	Identificeert de lokale hostnaam van de beleidsdirecteur (load balancer) die identificeert en staat een inkomende verbinding van de Peer toe.
instantienummer	Geeft het toegewezen nummer van het proces voor beleidsserver (QNS) aan dat initieert een verbinding met de uitgaande peer.  Opmerking: de lokale hostnaam en het instantienummer moeten worden opgegeven als het de bedoeling is dat slechts één proces voor beleidsserver (QNS) op de beleidsopbouwfunctie (load balancer) een verbinding met het genoemde peer-else instantienummer mogelijk maakt/initieert, anders kan dit getal als 0 worden behouden. In dat geval moeten alle processen van de beleidsserver (QNS) op de beleidsdirecteur (load balancer) verbinding met de peer proberen/toestaan. De standaardwaarde is 0.
beoordeling	Prioriteit toegewezen aan deze peer voor het indienen van een PCRF-geïnitieerd verzoek. Het Hoe hoger de ratingwaarde, hoe hoger de prioriteit is die aan de peer is toegewezen. De standaardwaarde is 1.
Poortbereik	Moet alleen worden opgegeven als de onderliggende transportverbinding SCTP is en niet vereist wanneer hetzelfde TCP is.

Time-out voor respons	Cisco raadt aan deze parameter niet te gebruiken.
naampatroon	Origin-Host Een VP-waarde in CER moet in om de verbinding tot stand te brengen. Als dat niet gebeurt, zal de CER wordt stilletjes verwijderd en de TCP-verbinding wordt gereset door PCRF. Naampatrooncontrole vindt niet plaats als de optie Ongedefinieerde peer accepteren is ingeschakeld beschreven in Diameter Stack Configuration. Het naampatroon moet de standaard Java-expressie zijn syntaxis hier beschreven.

Realms-tabel

Parameter	Beschrijving
rijken	Definieert welke peer-rijken verbindingen mogen initiëren naar PCRF.
peertype	Niet gebruikt met inbound realms.
verwerkingsprotocol	Toewijzing tussen de realmnaam en de specifieke PCRF-logica die worden toegepast voor het bericht, voor meer informatie over het verwerkingsprotocol. Wanneer een diameterstapel met een diametergebied zonder protocol wordt geïmporteerd toegewezen, neemt het de standaardwaarde als GX_TGPP .
beoordeling	Prioriteit toegewezen aan dit rijk voor het leveren van een PCRF geïnitieerd verzoek. Dit wordt alleen gebruikt met het SY_PRIME-verwerkingsprotocol.

	De standaardwaarde is 0. Hoe lager de ratingwaarde, hoe hoger de prioriteit is die aan het rijk is toegewezen. Een rijk met Rating=10 wordt bijvoorbeeld gebruikt nadat een rijk Beoordeling=1.
statusalias	Wat de statistieken die worden gegenereerd voor de respectieve rijk krijgt de naam die is geconfigureerd in statusalias die aan die statistieken is toegevoegd. Dit is alleen van toepassing op de statistieken van com.broadhop.message.
naampatroon	Origin-Realm Een VP-waarde in CER moet in om het binnenkomende bericht te verwerken. Als dat niet gebeurt, het bericht wordt in stilte verwijderd en de TCP-verbinding wordt gereset door PCRF. Het naampatroon moet de standaard Java-expressie zijn syntaxis hier beschreven.

Best practice:

Configureer voor meer granulaire besturing specifieke peer- en realm-vermeldingen volgens de vereiste, ook om peer creation alleen van specifieke peers toe te staan, schakel de Accept Undefined Peer uit.

Voorbeeld:

Afbeelding 1: Inbound Peers-tabel

REFERENCE DATA

File Tools

Systems

- Summary
- system-1
 - Plugin Configurations
 - cluster-1
 - Plugin Configurations
 - Diameter Configuration
 - Lab-PCRF
 - USuM Configuration

- Account Balance Templates
- Custom Reference Data Tables
- Diameter Agents
- Diameter Clients
- Diameter Defaults
- Fault List
- Notifications
- Policy Enforcement Points
- Rule Retry Profiles
- Subscriber Data Sources
- Tariff Times

Diameter Stack

*Name

Lab-PCRF

*Realm

pcrf.mnc[REDACTED].mcc[REDACTED].3gppnetwork[REDACTED]

☐ Accept Undefined Peer

Settings

Inbound Peers

Peers

Local Host Name	Instance Number	*Rating	Port Range	*Response Timeout	*Name Pattern
	0	1		[REDACTED]	*[REDACTED]*

Add Remove

Realms

Peer Type	*Processing Protocol	Rating	Stats Alias	*Name Pattern
	GX_TGPP	0		.*
	RX_TGPP	0		.*

Afbeelding 1: Inbound Peers-tabel

Stap 3: Host-IP-adres AVP configureren

De Diameter Host-IP-Address AVP communiceert het IP-adres van de node tijdens CER/CEA-uitwisselingen (RFC 3588) voor op SCTP gebaseerde verbindingen. In Cisco CPS PCRF is dit adres standaard de interne interface-IP, die verschilt van de verwachte diameterservice-IP voor bepaalde DRA-leveranciers.

In Cisco CPS PCRF kunt u de Load Balancer Virtual IP (LbVIP) of de fysieke IP van de load-balancer VM's gebruiken als het diameter-bron-eindpunt IP.

Standaard wordt de interne interface-IP gecommuniceerd als het Host-IP-adres in Diameter CER/CEA-berichten, zoals weergegeven in de afbeelding, waarbij het Bron-IP-adres in de opname verschilt van het IP-adres dat wordt gezien in de Host-IP-adres-AVP.

Afbeelding 2: CEA-bericht met intern IP als host-IP-adres

No.	Time	Source	Destination	Protocol	Length	Info
28	11.542641	DRA IP	PCRF Service IP	DIAME...	264	cmd=Capabilities-Exchange Request(257) flags=R--- appl=Diameter Common Message
30	11.794483	PCRF Service IP	DRA IP	DIAME...	592	cmd=Capabilities-Exchange Answer(257) flags=----- appl=Diameter Common Messages

Frame 30: 592 bytes on wire (4736 bits), 592 bytes captured (4736 bits)

> Linux cooked capture v1

> Internet Protocol Version 4, Src: PCRF Service IP (10.130.130.130), Dst: DRA IP (10.18.18.18)

> Transmission Control Protocol, Src Port: 3868, Dst Port: 49151, Seq: 1, Ack: 197, Len: 524

> Diameter Protocol

Version: 0x01

Length: 524

Flags: 0x00

Command Code: Capabilities-Exchange (257)

ApplicationId: Diameter Common Messages (0)

Hop-by-Hop Identifier: 0x5992d592

End-to-End Identifier: 0x071fbd73

[Request In: 28]

[Response Time: 0.251842000 seconds]

> AVP: Origin-Host(264) l=63 f=M- val=pcrf.mnc.mcc.3gppnetwork.org

> AVP: Origin-Realm(296) l=42 f=M- val=pcrf.mnc046.mcc404.3gppnetwork.org

> AVP: Host-IP-Address(257) l=14 f=M- val=192.12 (192.12)

> AVP: Vendor-Id(266) l=12 f=M- val=26878

> AVP: Supported-Vendor-Id(265) l=12 f=M- val=10415

> AVP: Vendor-Specific-Application-Id(260) l=32 f=M-

> AVP: Auth-Application-Id(258) l=12 f=M- val=3GPP Gx (16777238)

> AVP: Supported-Vendor-Id(265) l=12 f=M- val=8164

> AVP: Vendor-Specific-Application-Id(260) l=32 f=M-

> AVP: Supported-Vendor-Id(265) l=12 f=M- val=9

> AVP: Vendor-Specific-Application-Id(260) l=32 f=M-

> AVP: Supported-Vendor-Id(265) l=12 f=M- val=7898

> AVP: Vendor-Specific-Application-Id(260) l=32 f=M-

> AVP: Supported-Vendor-Id(265) l=12 f=M- val=5535

> AVP: Vendor-Specific-Application-Id(260) l=32 f=M-

> AVP: Vendor-Specific-Application-Id(260) l=32 f=M-

> AVP: Auth-Application-Id(258) l=12 f=M- val=3GPP Rx (16777236)

> AVP: Supported-Vendor-Id(265) l=12 f=M- val=13019

> AVP: Vendor-Specific-Application-Id(260) l=32 f=M-

> AVP: Product-Name(269) l=21 f= val=Cisco Quantum

> AVP: Result-Code(268) l=12 f=M- val=DIAMETER_SUCCESS (2001)

Afbeelding 2: CEA-bericht met intern IP als host-IP-adres

Hoewel deze AVP niet verplicht is wanneer TCP wordt gebruikt als het transportprotocol (zie RFC 3588), verwijzen sommige DRA-leveranciers naar deze AVP terwijl ze een diameterverbinding tot stand brengen en verwachten ze de IP-diameterservice van PCRF in plaats van interne IP. Als aan deze verwachting niet wordt voldaan, zouden de peers er niet in slagen om vast te stellen.

Best practice:

Als u reclame wilt maken voor het IP-adres van de diameterservice in het Host-IP-Address AVP van PCRF, werkt u het bestand /etc/hosts bij met een item dat de PCRF-bron FQDN (zoals gedefinieerd in de Diameter Stack Local End Points) toewijst aan het gewenste IP-adres.



Opmerking: Raadpleeg de tabellen met lokale eindpunten in de CPS Mobile Configuration Guide, versie 25.1.0, onder het gedeelte Diameter Stack Configuration voor meer informatie.

Extra hosts-items bijwerken in CPS PCRF op basis van Openstack:

- Controleer of het CPS-cluster zich in een geïmplementeerde toestand bevindt.

curl -X GET [installer API-systeem](#).

- Ophalen en bijwerken van de additionele-hosts.yaml via REST API.

```
curl -X GET http://<Cluster Manager IP>:8458/api/system/config/additional-hosts >> additional-hosts.yaml
```

- Breng wijzigingen aan met curl-opdrachten zoals beschreven in de productdocumentatie.

```
curl -X PUT API systeem extra hosts -H "Content-Type: application/yaml" --data-binary @additional-hosts.yaml
```

Wanneer deze API-aanroep is voltooid, wordt Clusterbeheer geconfigureerd met het nieuwe /etc/hostsbestand en worden alle andere geïmplementeerde VM's asynchroon bijgewerkt.



Opmerking: Raadpleeg de sectie Orchestration API van de CPS Installation Guide for OpenStack voor gedetailleerde instructies.

Extra hosts-items bijwerken in CPS PCRF op VMware:

- Voeg de vermelding toe in het bestand AdditionalHosts.csv op pad
/var/qps/config/deploy/csv/
- U kunt als volgt wijzigingen importeren in de VM van Clusterbeheer:

```
/var/qps/install/current/scripts/import/import_deploy.sh
```

- Wijzigingen toepassen vanuit Clusterbeheer:

```
/var/qps/install/current/scripts/build_all.sh
```

```
/var/qps/install/current/scripts/upgrade/reinit.sh
```



Opmerking: Raadpleeg voor gedetailleerde instructies de sectie CPS-installatiehandleiding voor VMware, Aanvullende hostconfiguratie.

Voorbeeld:

Afbeelding 3: lokale eindpunten van de GUI-diameterstapel

***Local End Points**

*Local Host Name	Instance Number	*Advertised Diameter F Q D N	*Listening Port	Local Bind Ip	*Transport Protocol	Multi Homing Hosts
HOSTNAME-lb01	0	HOSTNAME.pcrf.mncXXX.mccYYY.3gppnetwork.org	3868		TCP	
HOSTNAME-lb02	0	HOSTNAME.pcrf.mncXXX.mccYYY.3gppnetwork.org	3868		TCP	

Add Remove ↕ ↕

Afbeelding 3: lokale eindpunten van de GUI-diameterstapel

Voorbeeld /etc/hosts Entry:

<#root>

10.x.x.130HOSTNAME.pcrf.mncXXX.mccYYY.3gppnetwork.orgHOSTNAME.pcrf.mncXXX.mccYYY.3gppnetwork.org

```
192.x.x.16 HOSTNAME-cluman installer
#END_QPS_OTHER_HOSTS
[root@Hostname-cluman ~]#
```

Stap 4: Uitwisseling van peer-mogelijkheden valideren

De DRA moet expliciet reclame maken voor ondersteuning voor diametertoepassingen zoals Gx (16777238) en Rx (16777236) in berichten over Capabilities-Exchange-Request (CER) en Capabilities-Exchange-Answer (CEA).

De Relay-toepassing, met Application Identifier 0xffffffff, wordt niet ondersteund door Cisco PCRF. Als alleen de Relay-toepassing (4294967295) wordt uitgewisseld en niet Gx/Rx, wordt de peer-verbinding tot stand gebracht als alleen-relaismodus en reageert PCRF niet op CCR-I-berichten.

Raadpleeg het gedeelte Volgende hoproutering in de CPS Mobile Configuration Guide voor meer informatie.

Best practice:

Leg tijdens de installatiefase van de peer-verbinding altijd de pcap op PCRF vast om ervoor te zorgen dat DRA een bericht stuurt met een diameter Capabilities-Exchange-Request (CER) met een AVP Auth-Application-ID-waardeset Diametertoepassingen zoals Gx (16777238) of Rx (16777236) of beide en PCRF reageert met vergelijkbare waarden in het bericht Capabilities-Exchange-Answer (CEA).

Afbeelding 4: CER-bericht met verkeerde waarde in Auth-Application-Id als relais

```
√ Diameter Protocol
  Version: 0x01
  Length: 196
  > Flags: 0x80, Request
  Command Code: Capabilities-Exchange (257)
  ApplicationId: Diameter Common Messages (0)
  Hop-by-Hop Identifier: 0x5b2c55d3
  End-to-End Identifier: 0x171b0936
  [Answer In: 409]
  > AVP: Origin-Host(264) l=59 f=-M- val=[REDACTED]01ors.mnc[REDACTED].mcc[REDACTED].3gppnetwork.org
  > AVP: Origin-Realm(296) l=41 f=-M- val=epc.mnc084.mcc404.3gppnetwork.org
  > AVP: Host-IP-Address(257) l=14 f=-M- val=10.[REDACTED].[REDACTED].146
  > AVP: Vendor-Id(266) l=12 f=-M- val=323
  > AVP: Product-Name(269) l=20 f=--- val=Eagle XG DSR
  √ AVP: Auth-Application-Id(258) l=12 f=-M- val=Relay (4294967295)
    AVP Code: 258 Auth-Application-Id
    > AVP Flags: 0x40, Mandatory: Set
    AVP Length: 12
    Auth-Application-Id: Relay (4294967295)
  > AVP: Firmware-Revision(267) l=12 f=--- val=6491648
```

Afbeelding 4: CER-bericht met verkeerde waarde in Auth-Application-Id als relais

Afbeelding 5: CER-bericht met correcte waarden in Auth-Application-Id: Gx en Rx

Command Code: Capabilities-Exchange (257)

ApplicationId: Diameter Common Messages (0)

Hop-by-Hop Identifier: 0x38370427

End-to-End Identifier: 0x0d3fbc01

[Answer In: 30]

```
> AVP: Origin-Host(264) l=60 f=-M- val=[redacted]drax016[redacted].mnc084.mcc404.3gppnetwork.org
> AVP: Origin-Realm(296) l=41 f=-M- val=epc.mnc084.mcc404.3gppnetwork.org
> AVP: Host-IP-Address(257) l=14 f=-M- val=10.[redacted].[redacted].151
> AVP: Vendor-Id(266) l=12 f=-M- val=323
> AVP: Product-Name(269) l=20 f=--- val=Eagle XG DSR
✓ AVP: Vendor-Specific-Application-Id(260) l=32 f=-M-
  AVP Code: 260 Vendor-Specific-Application-Id
  > AVP Flags: 0x40, Mandatory: Set
  AVP Length: 32
  ✓ Vendor-Specific-Application-Id: 0000010a4000000c000028af000001024000000c01000014
    > AVP: Vendor-Id(266) l=12 f=-M- val=10415
    ✓ AVP: Auth-Application-Id(258) l=12 f=-M- val=3GPP Rx (16777236)
      AVP Code: 258 Auth-Application-Id
      > AVP Flags: 0x40, Mandatory: Set
      AVP Length: 12
      Auth-Application-Id: 3GPP Rx (16777236)
  ✓ AVP: Vendor-Specific-Application-Id(260) l=32 f=-M-
    AVP Code: 260 Vendor-Specific-Application-Id
    > AVP Flags: 0x40, Mandatory: Set
    AVP Length: 32
    ✓ Vendor-Specific-Application-Id: 0000010a4000000c000028af000001024000000c01000016
      > AVP: Vendor-Id(266) l=12 f=-M- val=10415
      > AVP: Auth-Application-Id(258) l=12 f=-M- val=3GPP Gx (16777238)
> AVP: Firmware-Revision(267) l=12 f=--- val=6557952
```

Afbeelding 5: CER-bericht met de juiste waarden in Auth-Application-Id: Gx en Rx

Stap 5: Zorg ervoor dat de unieke bronhostnaam voor de diameter wordt gedefinieerd bij elke diameter-peer-node

Cisco CPS PCRF ondersteunt een omgeving waarin voor elk van de aangesloten peer nodes een unieke bronhostnaam met diameter vereist is.

Als de migratie moet worden uitgevoerd voor peer-diameterverbindingen van bestaande directe Gx- of Rx-connectiviteit naar DRA-gemedieerde koppelingen, moet de DRA-koppeling voor elke diameterinterface (Gx of Rx) tussen PCEF of P-CSCF en DRA idealiter een unieke bronhostnaam gebruiken voor diametertoepassing (de waarde van de AVP Origin-Host) die anders zou zijn dan die gebruikt voor directe PCRF-connectiviteit met dezelfde peer node.

Dit zorgt ervoor dat verzoeken van peer nodes worden gerouteerd via de juiste DRA peer link en niet worden gedropt als oude directe link down vermeldingen aanwezig zijn in de PCRF show_peers.py lijst.

Best practice:

Als het niet mogelijk is om de hostnaam voor DRA-koppelingen op de peer te wijzigen, voert u een volledige herstart van alle vier de QNS-services sequentieel uit op elke VM met taakverdeling nadat u directe peer-koppelingen hebt verwijderd.

Dit zou ervoor zorgen dat oude verouderde (Origin: host) vermeldingen van peers die eerder werden gebruikt voor directe diameter interface (Gx/Rx) tussen PCEF/P-CSCF en PCRF niet meer aanwezig zijn in de PCRF diameter peer connection list, en show_peers.py output zou alleen DRA peer connections hebben en dus een goede routing van diameter applicatie berichten (bijvoorbeeld: Gx_CCA-I, Gx_CCA-T) van nieuw gecreëerde diameter links tussen DRA en PCRF.



Opmerking: het opnieuw starten van QNS-services op LB VM's heeft gevolgen voor het verkeer en stelt alle diameterpeer-verbindingen op die QNS-instanties opnieuw in. Voer deze stap uit tijdens een gepland onderhoudsvenster.

Stap 6: Configureer de volgende hoproutingstabel voor DRA-peers

Deze functie maakt het mogelijk om te werken met een DRA die zich niet in de topologie verbergen modus. Wanneer een DRA een verbinding tot stand brengt, adverteert het zijn eigen Origin-Host- en Realm-waarden. Diameter-toepassingsberichten gebruiken echter de Origin-Host en Realm (bijvoorbeeld PCEF, TDF, AF) van de werkelijke toepassingshost, dus PCRF moet bepalen welke DRA-verbinding moet worden gebruikt voor het verzenden van berichten naar de juiste host.



Opmerking: de tabel Volgende hoproutes wordt alleen gebruikt voor PCRF-geïnitieerde aanvragen. Reacties op inkomende verzoeken worden altijd verzonden via dezelfde verbinding waarop ze zijn ontvangen, om asymmetrische routing te voorkomen.

Deze parameters kunnen worden geconfigureerd onder Next Hop Routing tabel:

Parameter	Beschrijving
Volgende Hop Realm	Naam van het DRA-gebied zoals ontvangen in Origin-Realm AVP in CER of CEA Bericht.

	 Opmerking: Alle volgende hopgebieden (Next Hop Realm) moeten overeenkomen met de Origin-Realm A VP-waarde in het inkomende CER/CEA-bericht.
Volgende hophosts	DRA-hostnamen zoals ontvangen in Origin-Host AVP in CER of CEA Bericht.
	 Opmerking: Alle volgende hophostnamen (Next Hop Hosts) moeten overeenkomen met de Origin-Host A VP-waarde in het inkomende CER/CEA-bericht.
Toepassings-ID	Diameter applicatie-ID geadverteerd als ondersteund door de DRA. IT Bevat informatie die de specifieke service identificeert die de service De sessie is van.
bestemmingsrijken-patroon	Feitelijk bestemmingsrijk naampatroon zoals ontvangen in Origin-Realm AVP in AAR-bericht. Het patroon moet de standaard Java regular zijn expressiesyntaxis.
bestemmingshostpatroon	Feitelijk bestemmingshostnaampatroon zoals ontvangen in Origin-Host in AVP AAR-bericht. Het patroon moet standaard Java-patroon zijn conventies. Het patroon moet de standaard Java regular zijn expressiesyntaxis.

Best practice:

Probeer altijd het juiste regex-patroon te gebruiken (jokermatching) terwijl u vermeldingen maakt in de kolom Destination Realms Pattern en Destination Host Pattern in

Volgende Hop Routing-tabel om configuratievermeldingen voor Gx- en Rx-peers meerdere

verbindingen te minimaliseren en configuratiefouten te voorkomen.



Opmerking: Raadpleeg de CPS Mobile Configuration Guide, versie 25.1.0, onder de sectie Next Hop Routing voor gedetailleerde configuratierichtlijnen.

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.