Probleemoplossing voor ACI L3Out - rechtstreeks verbonden subnet PCTag1

Inhoud

[Inleiding](#)
[Achtergrondinformatie](#)
[Het scenario](#)
[Topologie en configuratie](#)
[Waargenomen probleem](#)
[Deep-Dive uitgeven](#)
[Oplossing](#)
[Uitleg](#)

Inleiding

Dit document beschrijft een scenario waarin verkeer dat afkomstig is van een direct aangesloten L3Out-subnetwerkknooppunt zonder de juiste configuratie onder de externe EPG kan leiden tot contractdalingen.

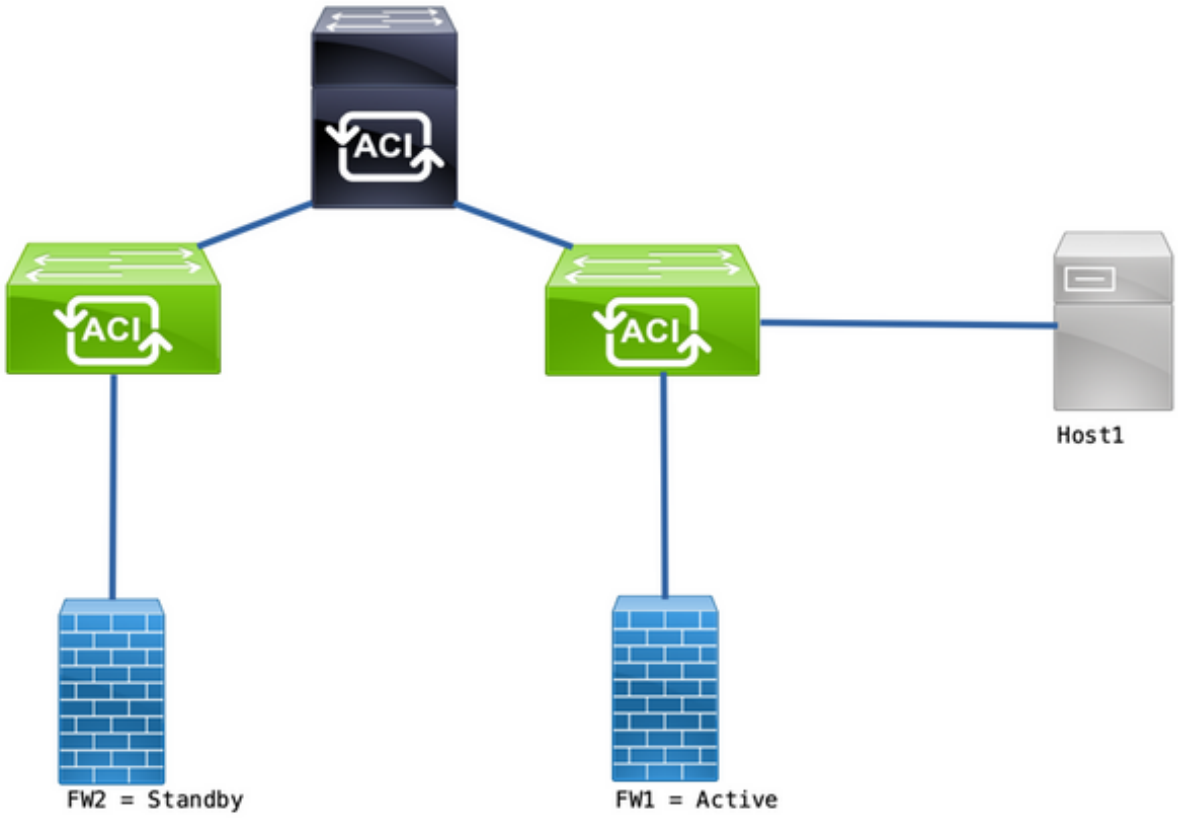
Achtergrondinformatie

De "**Een uitzondering voor een direct verbonden subnetverbinding met 0.0.0.0/0**" sectie van de ACI L3out Whitepaper roept dit gedrag met betrekking tot pcTag 1:

"...In de standaardinstelling worden direct verbonden subnetten aan pcTag 1 toegewezen, wat een speciale pcTag is om een contract te omzeilen. Dit moet routeprotocolcommunicatie in een hoekscenario impliciet toestaan. Maar... dit kan een veiligheidsprobleem veroorzaken. Vandaar dat dit gedrag in detail wordt uitgelegd via Cisco bug ID CSCuz12913 , die ook een tijdelijke configuratie introduceert:"

Het scenario

Topologie en configuratie



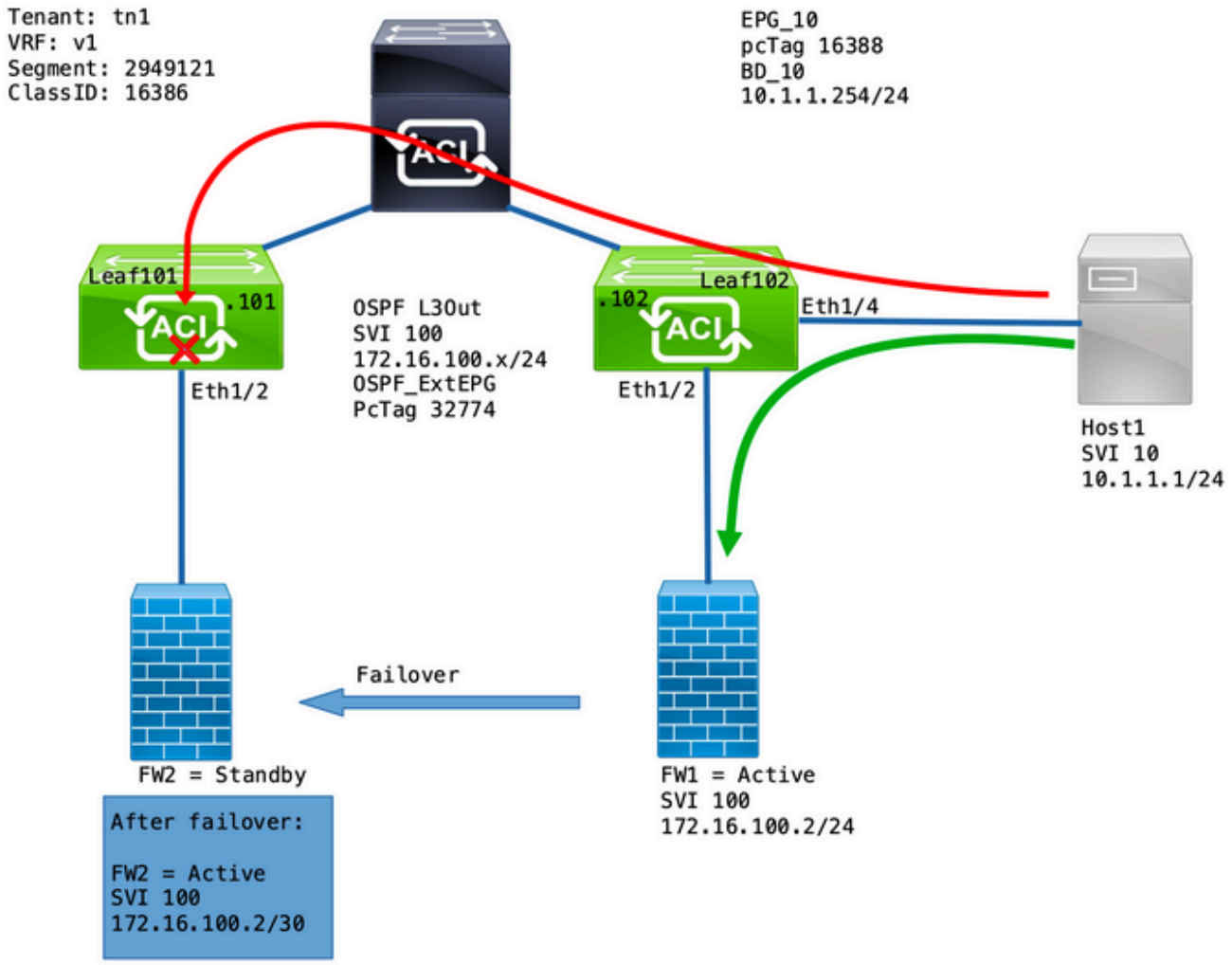
Topologie

- De firewalls (FW) zijn geconfigureerd met Network Address Translation (NAT).
- Al verkeer dat naar de ACI-fabric wordt verzonden, is afkomstig van IP van de FW die de OSPF-nabijheid met ACI vormt.
- De externe EPG heeft een 0.0.0.0/0 netwerk geconfigureerd met **externe subnetten voor de externe EPG**.
- Er is een contract voor communicatie tussen de interne EPG en de externe EPG.

Waargenomen probleem

Met FW1 als actief apparaat, werkt het verkeer zoals verwacht. Er worden geen druppels waargenomen.

Nadat de firewallservices zijn mislukt naar FW2, is de connectiviteit verloren - 10.1.1.1 en 172.16.10.2 kunnen niet meer communiceren.



Deep-Dive uitgeven

Een ELAM-opname op Leaf101 stelt ons in staat te valideren als het verkeer van Host1 naar FW2 wordt gedropt.

Deze ELAM-opties werden gebruikt:

```
leaf101# vsh_lc
module-1# debug platform internal roc elam asic 0
module-1(DBG-elam-insel6)# trigger reset
module-1(DBG-elam)# trigger init in-select 14 out-select 1
module-1(DBG-elam-insel14)# set inner ipv4 src_ip 10.1.1.1 dst_ip 172.16.100.2
module-1(DBG-elam-insel14)# start
module-1(DBG-elam-insel14)# status
```

En als deze functie wordt geactiveerd, kunt u met het e-rapport de zoekresultaten bekijken:

```
<snip>
================================================================================================
================================================
Captured Packet
================================================================================================
================================================
<snip>
```

```
------------------------------------------------------------------------------------------------
------------------------------------------------
Inner L3 Header
------------------------------------------------------------------------------------------------
------------------------------------------------
L3 Type : IPv4
DSCP : 0
Don't Fragment Bit : 0x0
TTL : 254
IP Protocol Number : ICMP
Destination IP                : 172.16.100.2   <<<----
Source IP                     : 10.1.1.1   <<<----
<snip>
================================================================================================
================================================
Contract Lookup ( FPC )
================================================================================================
================================================

------------------------------------------------------------------------------------------------
------------------------------------------------
Contract Lookup Key
------------------------------------------------------------------------------------------------
------------------------------------------------
IP Protocol : ICMP( 0x1 )
L4 Src Port : 2048( 0x800 )
L4 Dst Port : 52579( 0xCD63 )
sclass (src pcTag)                      : 16388( 0x4004 )   <<<----
dclass (dst pcTag)                      : 16386( 0x4002 )   <<<----
<snip>

------------------------------------------------------------------------------------------------
------------------------------------------------
Contract Result
------------------------------------------------------------------------------------------------
------------------------------------------------
Contract Drop                           : yes   <<<----
Contract Logging : yes
Contract Applied : no
Contract Hit : yes
Contract Aclqos Stats Index : 81824
( show sys int aclqos zoning-rules | grep -B 9 "Idx: 81824" )
```

Dit rapport toont aan dat de stroom Contract Dropped samen met deze details is:

- De SCLASS is 16388 wat de pcTag van EPG_10 is.
- De DCLASS is 16386 wat de pcTag van de VRF v1 is.

Daarna, bevestig de zoning regels voor VRF:

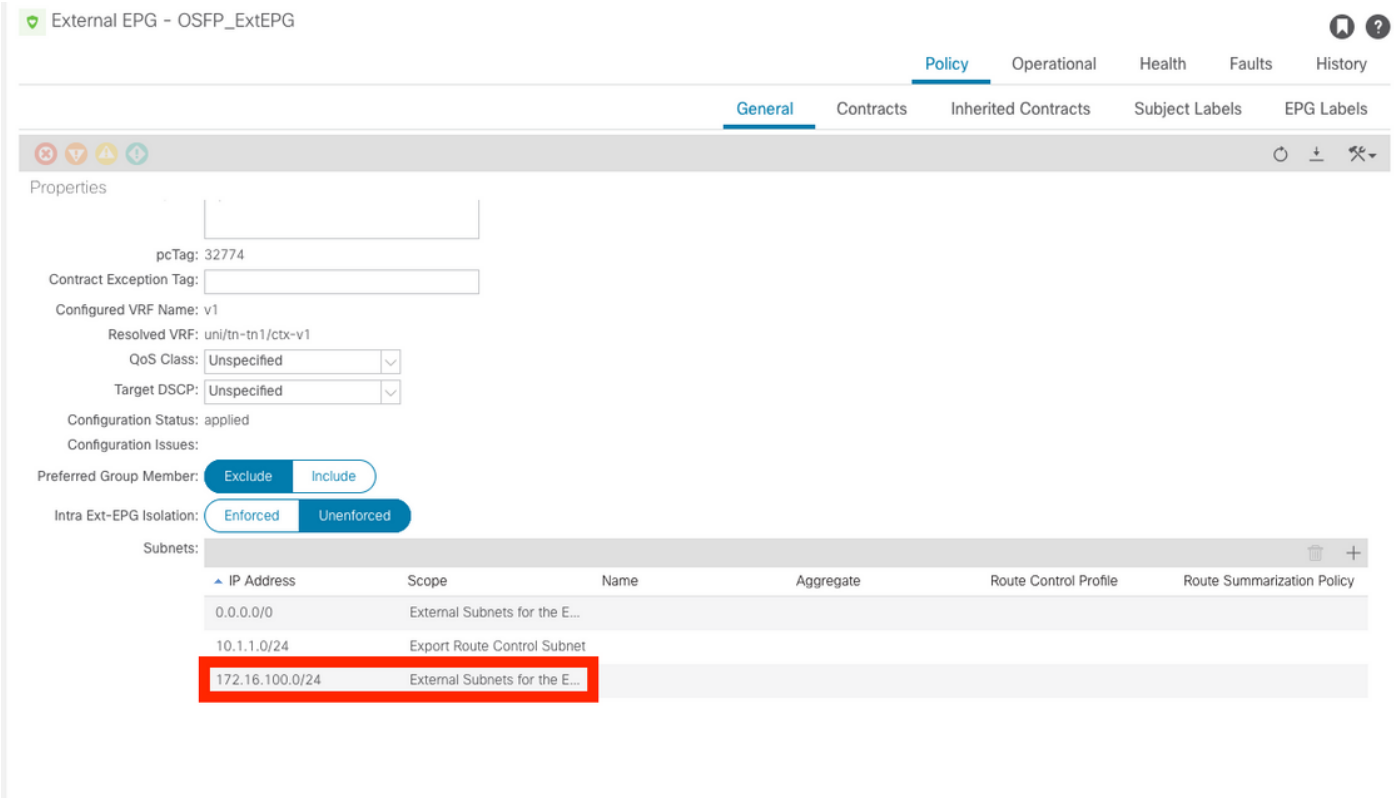
```
leaf102# show zoning-rule scope 2949121
+---------+--------+--------+----------+---------+---------+---------+------------------+-------
---+----------------------+
| Rule ID | SrcEPG | DstEPG | FilterID |   Dir   |  operSt |  Scope  |       Name       |
Action  |       Priority       |
+---------+--------+--------+----------+---------+---------+---------+------------------+-------
---+----------------------+
|   4131  |   0    |   15   | implicit | uni-dir | enabled | 2949121 |                  |
deny,log | any_vrf_any_deny(22) |
|   4130  |   0    |   0    | implarp  | uni-dir | enabled | 2949121 |                  |
permit  |  any_any_filter(17)  |
|   4129  |   0    |   0    | implicit | uni-dir | enabled | 2949121 |                  |
deny,log |   any_any_any(21)    |
```

```
|   4132  |   0    | 49155  | implicit | uni-dir | enabled | 2949121 |                 |
permit  |   any_dest_any(16)   |
|   4112  | 16386  | 16388  | default  | uni-dir | enabled | 2949121 | tn1:EPG-to-L3Out |
permit  |    src_dst_any(9)    |
|   4133  | 16388  |   15   | default  | uni-dir | enabled | 2949121 | tn1:EPG-to-L3Out |
permit  |    src_dst_any(9)    |
+---------+--------+--------+----------+---------+---------+---------+-----------------+-------
---+----------------------+
```

Er is een contract voor communicatie van EPG_10 (16388) naar netwerken achter de OSPF L3Out (0.0.0.0/0 = 15). Echter, het verkeer vanaf 172.16.100.2 is gelabeld onder de VRF v1 pcTag (16386).

Oplossing

Voeg het direct-verbonden subnet van L3Out onder OSPF Ext_EPG toe.



Deze toevoeging heeft 2 effecten:

1. Het verkeer vanaf het direct verbonden subnetnetwerk is gelabeld onder de OSPF_ExtEPG pcTag (32774)
2. Er worden regels toegevoegd om de stroom van en naar EPG_10 en OSPF_ExtEPG mogelijk te maken

```
leaf102# show zoning-rule scope 2949121
+---------+--------+--------+----------+----------------+---------+---------+-----------------
+----------+----------------------+ | Rule ID | SrcEPG | DstEPG | FilterID | Dir | operSt |
Scope | Name | Action | Priority | +---------+--------+--------+----------+----------------+----
-----+---------+------------------+----------+----------------------+ | 4131 | 0 | 15 | implicit
| uni-dir | enabled | 2949121 | | deny,log | any_vrf_any_deny(22) | | 4130 | 0 | 0 | implarp |
uni-dir | enabled | 2949121 | | permit | any_any_filter(17) | | 4129 | 0 | 0 | implicit | uni-
dir | enabled | 2949121 | | deny,log | any_any_any(21) | | 4132 | 0 | 49155 | implicit | uni-dir
| enabled | 2949121 | | permit | any_dest_any(16) | | 4112 | 16386 | 16388 | default | uni-dir |
```

```
enabled | 2949121 | tn1:EPG-to-L3Out | permit | src_dst_any(9) | | 4133 | 16388 | 15 | default |
uni-dir | enabled | 2949121 | tn1:EPG-to-L3Out | permit | src_dst_any(9) | |   4134  | 16388  |
32774  | default  |     bi-dir     | enabled | 2949121 | tn1:EPG-to-L3Out |  permit  |
src_dst_any(9)    |  <<<----
|   4135  | 32774  | 16388  | default  | uni-dir-ignore | enabled | 2949121 | tn1:EPG-to-L3Out |
permit  |    src_dst_any(9)    |  <<<----
+---------+--------+--------+----------+----------------+---------+---------+-----------------
+----------+----------------------+
```

Uitleg

De reden waarom dit werkt wanneer de FW en Host zijn verbonden met hetzelfde blad (zonder de L3Out subnettoevoeging) is omdat direct verbonden subnetten een speciale pcTag van 1 gebruiken die alle contracten omzeilt. Dit moet routeprotocolcommunicatie in een hoekscenario impliciet toestaan.

Met deze triggers kunnen we een verkeersstroom vangen van 172.16.100.2 naar 10.1.1.1 terwijl op Leaf102:

```
leaf102# vsh_lc
module-1# debug platform internal roc elam asic 0
module-1(DBG-elam)# trigger reset
module-1(DBG-elam)# trigger init in-select 6 out-select 1
module-1(DBG-elam-insel6)# set outer ipv4 src_ip 172.16.100.2 dst_ip 10.1.1.1
module-1(DBG-elam-insel6)# start
module-1(DBG-elam-insel6)# status
 ELAM STATUS
===========
Asic 0 Slice 0 Status Triggered
```

Dit rapport toont de zoekresultaten:

```
module-1(DBG-elam-insel6)# ereport
Python available. Continue ELAM decode with LC Pkg
 ELAM REPORT
================================================================================================================
=====================================================
                                                                    Captured Packet
================================================================================================================
=====================================================

----------------------------------------------------------------------------------------------------------------
-----------------------------------------------------
Outer L3 Header
----------------------------------------------------------------------------------------------------------------
-----------------------------------------------------
L3 Type                      : IPv4
IP Version                   : 4
DSCP                         : 0
IP Packet Length             : 84 ( = IP header(28 bytes) + IP payload )
Don't Fragment Bit           : not set
TTL                          : 255
IP Protocol Number           : ICMP
IP CheckSum                  : 32320( 0x7E40 )
Destination IP               : 10.1.1.1      <<<----
```

```
Source IP                     : 172.16.100.2  <<<----

================================================================================================================
================================================
                                                                        Contract Lookup ( FPC )
================================================================================================================
================================================

----------------------------------------------------------------------------------------------------------------
------------------------------------------------
Contract Lookup Key
----------------------------------------------------------------------------------------------------------------
------------------------------------------------
IP Protocol                           : ICMP( 0x1 )
L4 Src Port                           : 0( 0x0 )
L4 Dst Port                           : 19821( 0x4D6D )
sclass (src pcTag)                    : 1( 0x1 )           <<<----
dclass (dst pcTag)                    : 16388( 0x4004 )    <<<----
src pcTag is from local table         : yes
derived from a local table on this node by the lookup of src IP or MAC
Unknown Unicast / Flood Packet        : no
If yes, Contract is not applied here because it is flooded

----------------------------------------------------------------------------------------------------------------
------------------------------------------------
Contract Result
----------------------------------------------------------------------------------------------------------------
------------------------------------------------
Contract Drop                         : no  <<<----
Contract Logging                      : no
Contract Applied                      : no  <<<----
Contract Hit                          : yes
Contract Aclqos Stats Index           : 81903
```

Zo valideert u de retourstroom:

```
module-1(DBG-elam-insel6)# trigger reset
module-1(DBG-elam)# trigger init in-select 6 out-select 1
module-1(DBG-elam-insel6)# set outer ipv4 src_ip 10.1.1.1 dst_ip 172.16.100.2
module-1(DBG-elam-insel6)# start
module-1(DBG-elam-insel6)# status
 ELAM STATUS
===========
Asic 0 Slice 0 Status Triggered
```

De zoekresultaten van de retourstroom:

```
module-1(DBG-elam-insel6)# ereport
Python available. Continue ELAM decode with LC Pkg
 ELAM REPORT
================================================================================================================
================================================
                                                                      Captured Packet
================================================================================================================
================================================
----------------------------------------------------------------------------------------------------------------
------------------------------------------------
Outer L3 Header
----------------------------------------------------------------------------------------------------------------
------------------------------------------------
```

```
L3 Type                      : IPv4
IP Version                   : 4
DSCP                         : 0
IP Packet Length             : 84 ( = IP header(28 bytes) + IP payload )
Don't Fragment Bit           : not set
TTL                          : 255
IP Protocol Number           : ICMP
IP CheckSum                  : 32198( 0x7DC6 )
Destination IP               : 172.16.100.2  <<<----
Source IP                    : 10.1.1.1      <<<----

================================================================================================
=================================================
                                                                  Contract Lookup ( FPC )
================================================================================================
=================================================

------------------------------------------------------------------------------------------------
-------------------------------------------------
Contract Lookup Key
------------------------------------------------------------------------------------------------
-------------------------------------------------
IP Protocol                          : ICMP( 0x1 )
L4 Src Port                          : 2048( 0x800 )
L4 Dst Port                          : 18134( 0x46D6 )
sclass (src pcTag)                   : 16388( 0x4004 ) <<<----
dclass (dst pcTag)                   : 1( 0x1 )        <<<----
src pcTag is from local table        : yes
derived from a local table on this node by the lookup of src IP or MAC
Unknown Unicast / Flood Packet       : no
If yes, Contract is not applied here because it is flooded

------------------------------------------------------------------------------------------------
-------------------------------------------------
Contract Result
------------------------------------------------------------------------------------------------
-------------------------------------------------
Contract Drop                        : no    <<<----
Contract Logging                     : no
Contract Applied                     : no    <<<----
Contract Hit                         : yes
Contract Aclqos Stats Index          : 81903
```

In deze tabel wordt een overzicht gegeven van de te verwachten gedragingen bij Gen2-switches:

scenario	directionaliteit	Contractdaling	Geen contractva
Op hetzelfde blad VRF-beleidshandhaving: Beide	X naar L3Out		X
	L3Out naar X		X
Over 2 bladknooppunten VRF-beleidshandhaving: Ingress	X naar L3Out	X	
	L3Out naar X		X
Over 2 bladknooppunten VRF-beleidshandhaving: uitgang	X naar L3Out		X
	L3Out naar X		X

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.