Probleemoplossing voor integratie van Hardware Security Modules (HSM) met FND

Inhoud

Inleiding

In dit document worden de Hardware Security Module (HSM), integratie met de FAN-oplossing (Field Area Network) en probleemoplossing voor algemene problemen beschreven.

Hardware security module (HSM)

Hardware Security Modules (HSM) zijn beschikbaar in drie vormen: apparaat, PCI-kaart en cloudaanbod. De meeste implementaties kiezen voor de versie van het apparaat.

Softwarebeveiligingsmodules (SSM)

Software Security Modules (SSM) zijn softwarepakketten die een soortgelijk doel dienen als HSM. Ze worden gebundeld met FND-software en bieden een eenvoudig alternatief in plaats van het apparaat.

Het is belangrijk om op te merken dat zowel HSM als SSM optionele componenten zijn in FND implementaties en niet verplicht zijn.

Functies van de HSM

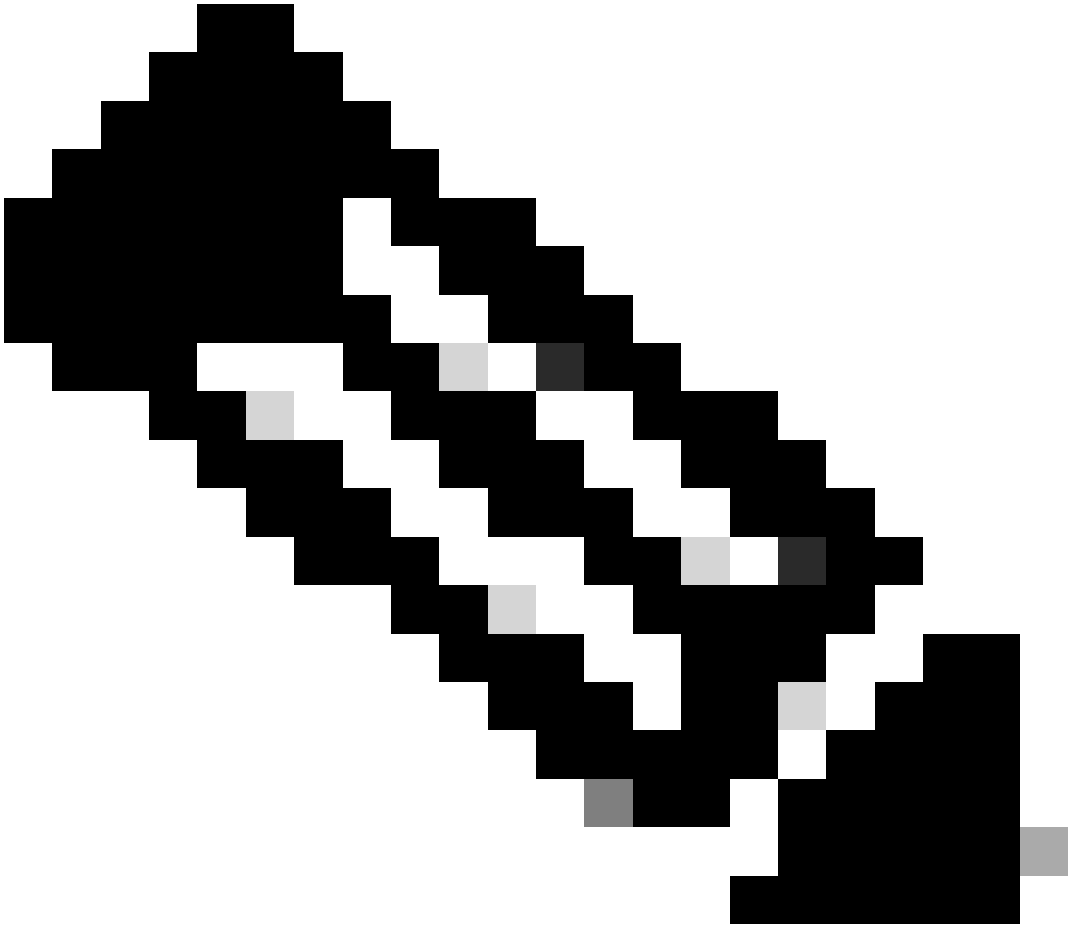
De primaire functie van zowel HSM als SSM in een FND-oplossing is om het PKI-sleutelpaar en het CSMP-certificaat veilig op te slaan, in het bijzonder wanneer CSMP-endpoints zoals meters worden gebruikt.

Deze sleutels en certificaten zijn essentieel voor het versleutelen van communicatie tussen FND

en de CSMP-endpoints.

Wat de implementatie betreft, is HSM een standalone applicatie, terwijl SSM kan worden geïnstalleerd op dezelfde Linux server als FND of op een afzonderlijke Linux server. De configuratie voor SSM wordt gespecificeerd in het bestand cgms.Properties.

Tijdens bootup, FND controleert op HSM clientbibliotheken, ongeacht of HSM-gerelateerde informatie wordt gespecificeerd in cgms.Properties. Logbestanden met betrekking tot ontbrekende HSM-clientbibliotheken tijdens het opstarten kunnen worden genegeerd als HSM niet in de oplossing is opgenomen.



Opmerking: HSM-gerelateerde informatie moet worden gespecificeerd in het cgms.Properties bestand, dat zich in verschillende directory's bevindt, afhankelijk van of FND is geïnstalleerd via OVA of ISO.

HSM-clientinstallatie

De HSM-client moet worden geïnstalleerd op dezelfde Linux-server waar de FND-server zich bevindt. Klanten kunnen de HSM-clientsoftware downloaden van de Thales-website of via een Cisco-ondersteuningscontract.

De FND-softwarerelease documenteert de vereiste software op de HSM-client en HSM-software voor de implementatie. Het wordt vermeld onder de sectie HSM Upgrade Table voor de release notities.

Pad voor HSM-clientinstallatiebestanden, configuratiebestanden en bibliotheken:

De standaardinstallatielocatie is /usr/safenet/lunaclient/bin . De meeste opdrachten, zoals lunacm, vtl, of ckdemo, lopen vanaf dit pad (/usr/safenet/lunaclient/bin).

Het configuratiebestand vindt u op /etc/Chrystoki.conf .

Het pad naar HSM Luna client library files die de FND server nodig heeft op Linux servers is /usr/safenet/lunaclient/jsp/lib/ .

HSM-server

De meeste implementaties gebruiken de HSM-server als apparaat.

De HSM-server moet worden gepartitioneerd en HSM-clients hebben alleen toegang tot de specifieke partitie waaraan ze zijn toegewezen. De HSM-server kan worden beveiligd met verificatie of met een wachtwoord worden geverifieerd.

Bij wachtwoordverificatie volstaan een gebruikersnaam en wachtwoord voor configuratiewijzigingen in de HSM-server.

De met een MPEG-verificatie bevestigde HSM is echter een multifactor-verificatiemethode waarbij, naast een wachtwoord, de persoon die de wijzigingen aanbrengt, toegang nodig heeft tot een MPEG-sleutel.

De SED-toets werkt zoals een dongle en geeft een pincode weer die de gebruiker samen met het wachtwoord moet invoeren om configuratiewijzigingen door te voeren.

Voor bepaalde opdrachten zoals opdrachten tonen en alleen-lezen toegang, is de PD-toets niet nodig. Alleen specifieke configuratiewijzigingen zoals het maken van partities vereisen de SED-toets.

Elke serverpartitie kan meerdere clients toegewezen hebben en alle clients die toegewezen zijn aan een partitie hebben toegang tot de gegevens binnen die partitie.

De HSM-server biedt verschillende gebruikersrollen, waarbij de rollen van admin en Crypto Security Officer bijzonder belangrijk zijn. Bovendien is er de rol van een 'partitie-veiligheidsbeambte'.

Probleemoplossing

FND gebruikt de HSM-client om toegang te krijgen tot de HSM-hardware. Daarom zijn er 2 delen in de integratie.

1. HSM-client naar HSM-servercommunicatie
2. FND naar HSM-clientcommunicatie

Beide onderdelen moeten werken om de HSM-integratie te laten slagen.

HSM-client naar HSM-servercommunicatie

Om te bepalen of de HSM-client met succes de sleutel- en certificaatinformatie kan lezen die in de HSM-partitie is opgeslagen op de HSM-server met behulp van één opdracht, gebruikt u de opdracht /cmu list vanuit de locatie /usr/safenet/lunaclient/bin.

Het uitvoeren van deze opdracht geeft uitvoer die aangeeft of de HSM-client toegang kan krijgen tot de sleutel en het certificaat die zijn opgeslagen in de HSM-partitie.

Let op: deze opdracht vraagt om een wachtwoord, dat hetzelfde moet zijn als het wachtwoord voor de HSM-partitie.

Een succesvolle output lijkt op dit resultaat:

[root@fndblr23 bin]#./cmu-lijst
Certificaatbeheerprogramma (64-bits) v7.3.0-165. Copyright (c) 2018 SafeNet. Alle rechten voorbehouden.

Voer in sleuf 0 het wachtwoord voor een token in: *******

handle=2000001 label=NMS_SOUTHBOUND_KEY
handle=2000002 label=NMS_SOUTHBOUND_KEY—cert0
[root@fndblr23 bin]#

Opmerking:

Als de klant het wachtwoord niet meer weet, decodeert u het wachtwoord dat wordt vermeld in het bestand cgms.Properties zoals hier wordt getoond:

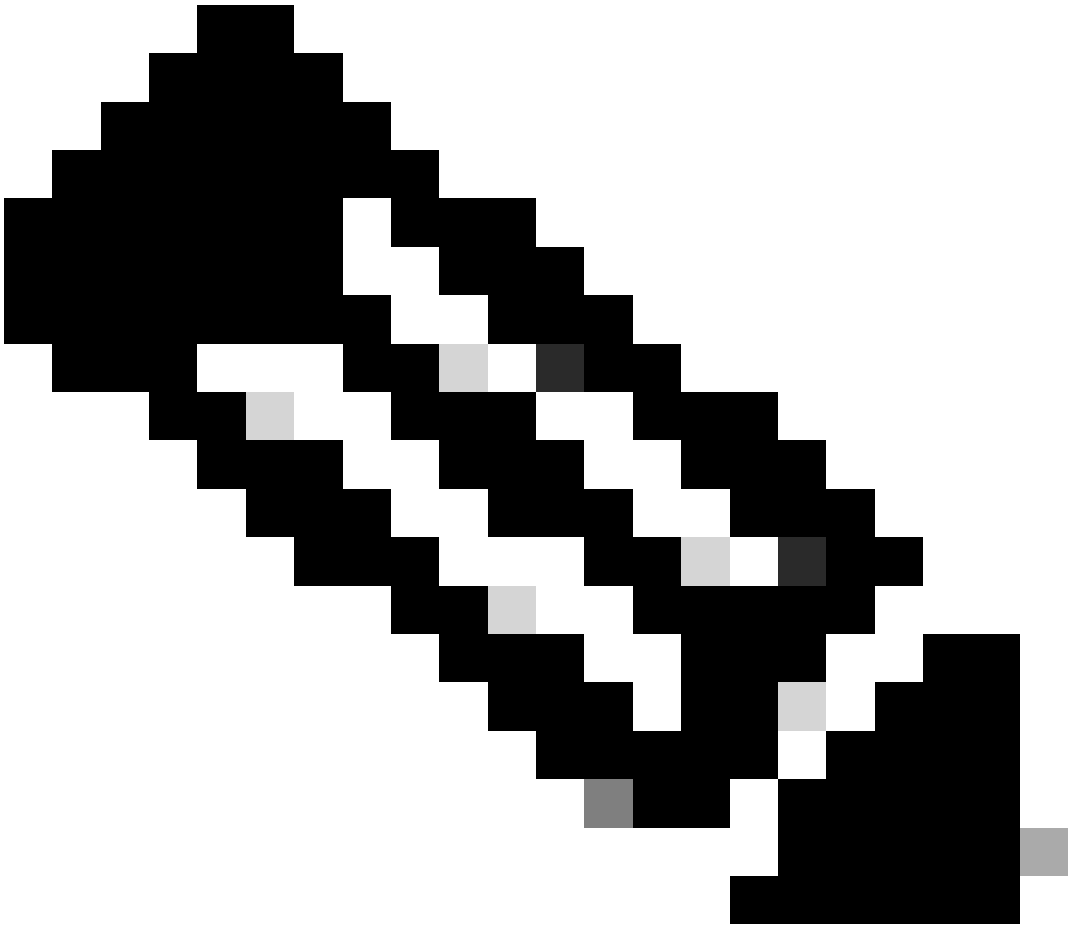
[root@fndblr23 ~]# cat /opt/cgms/server/cgms/conf/cgms.properties | gbr hsm
hsm-keystore-wachtwoord=qnBC7WGvZB5iux4BNNdplTWzcmAxhuISQLmVRXtHBeBWF4=
hsm-keystore-name=TEST2Group
[root@fndblr23 ~]#
[root@fndblr23 ~]# /opt/cgms/bin/encryption_util.sh decrypt
qnBC7WGvZB5iux4BnDPLTWzcmAxhuISQLmVRXtHBeBWF4=
Wachtwoordvoorbeeld
[root@fndblr23 ~]#

In dit geval is het gedecrypteerde wachtwoord Passwordexample

1. NTSL-communicatiecontrole:

De HSM-client communiceert met de HSM-server met behulp van de bekende poort 1792 voor NTLS-communicatie (Network Transport Layer Security), die zich in de ingestelde staat bevindt.

Om de status van de NTLS-communicatie te controleren op de Linux-server waarop de FND-server draait en waar de HSM-client is geïnstalleerd, gebruikt u deze opdracht:



Opmerking: "netstat" is vervangen door de "ss"-opdracht in Linux

---

opdoffer

Kopieercode

[root@fndblr23 ~]# ss -natp | Vgp 1792

ESTAB 0 0 10.106.13.158:46336 172.27.126.15:1792 gebruikers:("java",pid=11943,fd=317)

Als de verbinding niet in de vastgestelde staat is, wijst het op een probleem met fundamentele communicatie NTLS.

In dergelijke gevallen, adviseer de klant om in te loggen op hun HSM-apparaat en controleer dat de NTLS-service wordt uitgevoerd met behulp van de opdracht "ntls information show".

Bovendien, zorg ervoor dat de interfaces voor NTLS worden toegelaten. U kunt de tellers opnieuw instellen met "ntls information reset" en vervolgens de opdracht "show" opnieuw uitgeven.

Op HSM-applicatie of HSM-server:

jammeren

Kopieercode

[hsmlast] lunash:>ntls informatie tonen

NTLS-informatie:

Operationele status: 1 (omhoog)

Verbonden clients: 1

Verwijzigingen: 1

Succesvolle clientverbindingen: 20095

Mislukte clientverbindingen: 20150

Opdrachtresultaat: 0 (succes)

[laatste] was:>

1. Identificatie client voor Luna Safenet:

De HSM client, ook bekend als Luna Safenet client, kan worden geïdentificeerd door gebruik te maken van de "./lunacm" opdracht vanuit de "/usr/safenet/lunaclient/bin" locatie. Deze opdracht geeft ook een lijst van de HSM-partitie die is toegewezen aan de client en elke geconfigureerde High Availability (HA)-groep.

Kopieercode

[root@fndblr23 bin]# ./lunacm

lunacm (64-bit) v7.3.0-165. Copyright (c) 2018 SafeNet. Alle rechten voorbehouden.

De versie van de geïnstalleerde Luna-client wordt hier aangegeven (in dit voorbeeld, versie 7.3).

De output toont ook informatie over de beschikbare HSMs, met inbegrip van de toegewezen HSM

verdelingen en de configuratie van de Groep HA.

wiskunde

Kopieercode

Sleuf-ID -> 0

Label -> TEST2

Serienummer -> 1358678309716

Model -> LunaSA 7.4.0

Firmware versie -> 7.4.2

Configuratie -> Luna-gebruikerspartitie met POS-toets (SED) Exporteren met kloonmodus

Beschrijving sleuf -> Net Token Slot

Sleuf-ID -> 4

HSM-label -> TEST2Group

HSM-serienummer -> 11358678309716

HSM-model -> LunaVirtual

HSM-firmware versie -> 7.4.2

HSM-configuratie -> DWDM-toetsuitvoer (Luna Virtual HSM) met kloonmodus

HSM-status -> N.v.t. - HA-groep

Controleer dat elke HSM-client is toegewezen aan ten minste één partitie en begrijp de configuraties met betrekking tot HA-groepen voor scenario's met hoge beschikbaarheid.

d. Als u een lijst wilt maken van de HSM-servers die zijn geconfigureerd met de luna-client, gebruikt u de ./vtl listServers op de locatie /usr/safenet/lunaclient/bin

```
[root@fndblr23 bin]# ./vtl listServers
vtl (64-bit) v7.3.0-165. Copyright (c) 2018 SafeNet. All rights reserved.

Server: 172.27.126.15
You have new mail in /var/spool/mail/root
[root@fndblr23 bin]#
```

e. Als we ./vtl typen en vervolgens op enter in de locatie /usr/safenet/lunaclient/bin, toont het de lijst met opties die beschikbaar zijn met vtl commando.

./vtl verify lijsten van de fysieke HSM-partities die zichtbaar zijn voor de Luna-client.

./vtl listSlots geeft een lijst van alle fysieke en virtuele slots (HA-groep) als HAGroup is geconfigureerd maar uitgeschakeld.

Als HAGroup is geconfigureerd en ingeschakeld, toont het alleen de virtuele groep of de HAGroup-informatie.

```
[root@fndblr23 bin]# ./vtl verify
vtl (64-bit) v7.3.0-165. Copyright (c) 2018 SafeNet. All rights reserved.

The following Luna SA Slots/Partitions were found:
Slot Serial #         Label
==== ================ =====
-    1358678309716    TEST2

[root@fndblr23 bin]#
[root@fndblr23 bin]# ./vtl listSlots
vtl (64-bit) v7.3.0-165. Copyright (c) 2018 SafeNet. All rights reserved.
Number of slots: 1
The following slots were found:

Slot Description          Label                            Serial #              Status
==== ==================== ================================ ================      ============
0    HA Virtual Card Slot TEST2Group                       11358678309716        Present
[root@fndblr23 bin]#
```

f. Om te weten te komen of HAGroup is ingeschakeld of niet, kunnen we de ./vtl listSlots gebruiken. Als het alleen de HAGroup laat zien, en niet de fysieke slots, dan weten we dat HAGroup is ingeschakeld.

Een andere manier om erachter te komen of HAGroup is ingeschakeld, is door de ./lunacm uit /usr/safenet/lunaclient/bin uit te geven en vervolgens de opdracht ha l uit te geven

Het gevraagde wachtwoord is het wachtwoord van de fysieke partitie. In dit bericht dat de enige show HA Slots is ja. Dit betekent dat HA actief is.

Als het neen is, dan is HA ingesteld, maar niet actief.

HA kan worden geactiveerd met de opdracht "ha ha-only enable" in de lunacm-modus.

```
lunacm:>ha l

If you would like to see synchronization data for group TEST2Group,
please enter the password for the group members. Sync info
not available in HA Only mode.

Enter the password: *******

HA auto recovery: disabled
HA recovery mode: activeBasic
```

```
Maximum auto recovery retry: 0
Auto recovery poll interval: 60 seconds
HA logging: disabled
Only Show HA Slots: yes

HA Group Label: TEST2Group
HA Group Number: 11358678309716
HA Group Slot ID: 4
Synchronization: enabled
Group Members: 1358678309716
Needs sync: no
Standby Members: <none>

Slot #       Member S/N               MemberLabel     Status
======       ==========               ============    ======
------       1358678309716            TEST2           alive

Command Result : No Error
```

Klanten hebben toegang tot HSM-servers. Meestal worden HSM-servers gehost in DC en veel van deze worden bediend met PETS.

De PD is als een kleine dongle die security token informatie weergeeft die multi-factor verificatie is voor extra beveiliging, tenzij de gebruiker zowel wachtwoord als token heeft, dan is bepaalde toegang zoals admin of config toegang niet toegestaan.

De enkele opdracht die alle serverinformatie opsomt, is hsm

In deze uitvoer kunnen we zien dat de naam van het hsm-apparaat laatst is. De lunash prompt vertelt ons dat het de HSM server is.

We zien de HSM-softwareversie die 7.4.0-226 is. We kunnen andere informatie zien, zoals serienummer van het apparaat, en wat de verificatiemethode is, of het nu een PAD of een wachtwoord is, en we kunnen het totale aantal partities op die HSM zien. Merk op zoals we eerder zagen dat HSM-clients worden geassocieerd met partities in het apparaat.

```
[hsmlatest] lunash:>
[hsmlatest] lunash:>hsm show

Appliance Details:
==================
Software Version: 7.4.0-226

HSM Details:
============
HSM Label: HSMLatest
Serial #: 583548
Firmware: 7.4.2
HSM Model: Luna K7
HSM Part Number: 808-000066-001
Authentication Method: PED keys
HSM Admin login status: Not Logged In
```

```
HSM Admin login attempts left: 3 before HSM zeroization!
RPV Initialized: No
Audit Role Initialized: No
Remote Login Initialized: No
Manually Zeroized: No
Secure Transport Mode: No
HSM Tamper State: No tamper(s)

Partitions created on HSM:
==============================
Partition: 1358678309715, Name: Test1
Partition: 1358678309716, Name: TEST2

Number of partitions allowed: 5
Number of partitions created: 2

FIPS 140-2 Operation:
=====================
The HSM is NOT in FIPS 140-2 approved operation mode.

HSM Storage Information:
========================
Maximum HSM Storage Space (Bytes): 16252928
Space In Use (Bytes): 6501170
Free Space Left (Bytes): 9751758

Environmental Information on HSM:
=================================
Battery Voltage: 3.115 V
Battery Warning Threshold Voltage: 2.750 V
System Temp: 39 deg. C
System Temp Warning Threshold: 75 deg. C

Functionality Module HW: Non-FM
=======================
Command Result : 0 (Success)
[hsmlatest] lunash:>
```

Andere nuttige opdrachten op de HSM-server omvatten partitie tonen opdracht.

De velden die we moeten noemen zijn de partitienaam, het serienummer, het aantal partitieobjecten. Het aantal partitieobjecten is hier 2.

Dat wil zeggen dat één object dat in de parititon is opgeslagen het sleutelpaar is voor CSMP-berichtversleuteling en een ander object dat is opgeslagen het CSMP-certificaat is.

opdracht clientlijst:

De client die we controleren, wordt vermeld in de lijst met geregistreerde clients in de opdracht clientlijst.

client show -c <client name> geeft alleen die client informatie, de hostnaam, IP-adres en de partitie waaraan deze client is toegewezen. Succesvolle outputs zien er zo uit.

Hier kunnen we kijken naar de partitienaam, het serienummer en ook de Partitie-objecten. In dit geval is het partitieobject = 2, waarbij de twee objecten de privésleutel en het CSMP-certificaat

zijn.

```
[hsmlatest] lunash:>partition show

Partition Name: Test1
Partition SN: 1358678309715
Partition Label: Test1
Partition SO PIN To Be Changed: no
Partition SO Challenge To Be Changed: no
Partition SO Zeroized: no
Partition SO Login Attempts Left: 10
Crypto Officer PIN To Be Changed: no
Crypto Officer Challenge To Be Changed: no
Crypto Officer Locked Out: no
Crypto Officer Login Attempts Left: 10
Crypto Officer is activated: yes
Crypto User is not initialized.
Legacy Domain Has Been Set: no
Partition Storage Information (Bytes): Total=3240937, Used=1036, Free=3239901
Partition Object Count: 2


Partition Name: TEST2
Partition SN: 1358678309716
Partition Label: TEST2
Partition SO PIN To Be Changed: no
Partition SO Challenge To Be Changed: no
Partition SO Zeroized: no
Partition SO Login Attempts Left: 10
Crypto Officer PIN To Be Changed: no
Crypto Officer Challenge To Be Changed: no
Crypto Officer Locked Out: no
Crypto Officer Login Attempts Left: 10
Crypto Officer is activated: yes
Crypto User is not initialized.
Legacy Domain Has Been Set: no
Partition Storage Information (Bytes): Total=3240937, Used=1036, Free=3239901
Partition Object Count: 2

Command Result : 0 (Success)
[hsmlatest] lunash:>
[hsmlatest] lunash:>client list

registered client 1: ELKSrv.cisco.com
registered client 2: 172.27.171.16
registered client 3: 10.104.188.188
registered client 4: 10.104.188.195
registered client 5: 172.27.126.209
registered client 6: fndblr23

Command Result : 0 (Success)
[hsmlatest] lunash:>
[hsmlatest] lunash:>client show -c fndblr23

ClientID: fndblr23
IPAddress: 10.106.13.158
Partitions: "TEST2"

Command Result : 0 (Success)
[hsmlatest] lunash:>
```

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.