

APIC voor apparaatbeheer configureren met ISE en TACACS+

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Netwerkdigram](#)

[Verificatieprocedure](#)

[APIC-configuratie](#)

[ISE-configuratie](#)

[Verifiëren](#)

[Problemen oplossen](#)

Inleiding

Dit document beschrijft de procedure om APIC met ISE te integreren voor de verificatie van beheerders met het TACACS+-protocol.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Application Policy Infrastructure Controller-controller (APIC)
- Identity Services Engine (ISE)
- TACACS-protocol

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- APIC versie 4.2(7u)
- ISE-versie 3.2 Patch 1

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.

Configureren

Netwerkdigram



Integratiediagram


Verificatieprocedure

Stap 1. Meld u aan bij de APIC-toepassing met Admin User Credentials.


Stap 2. Het verificatieproces activeert en ISE valideert de referenties lokaal of via Active Directory.

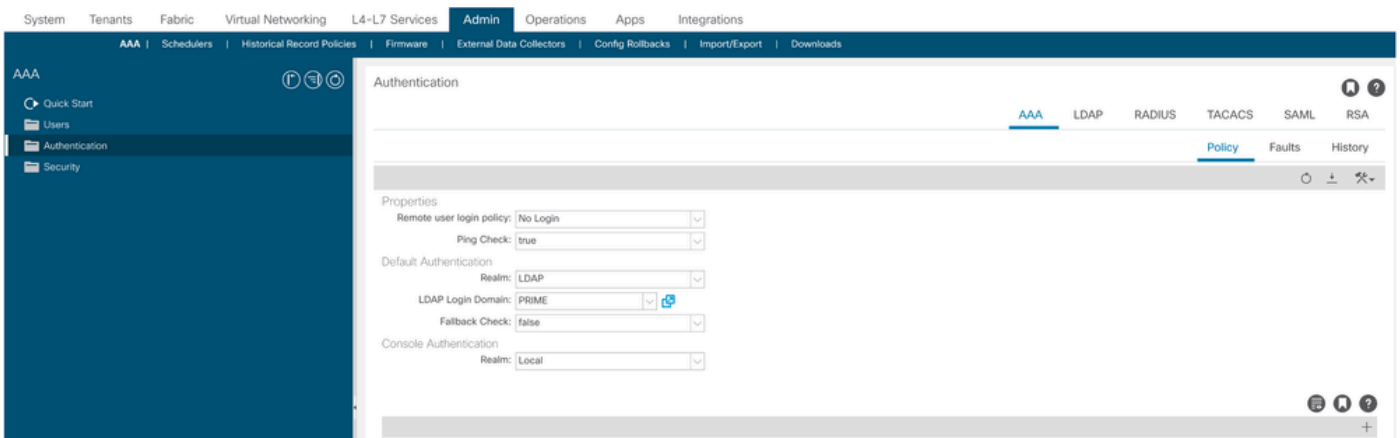
Stap 3. Zodra de verificatie is geslaagd, stuurt ISE een vergunningspakket om de toegang tot de APIC te autoriseren.

Stap 4. ISE toont een succesvol live verificatielogboek.

 **Opmerking:** APIC repliceert de TACACS+-configuratie naar bladeren switches die deel uitmaken van het weefsel.

APIC-configuratie

Stap 1. Navigeer naar **Admin > AAA > Authentication > AAA** en kies  pictogram om een nieuw login domein te maken.



Configuratie van APIC-inlogbeheer

+Stap 2. Bepaal een naam en domein voor het nieuwe Login Domein en klik onder Providers om een nieuwe provider te creëren.

Create Login Domain



Name:

Realm:

Description:

Providers:

Name	Priority	Description
------	----------	-------------

Cancel

Submit

APIC-inlogbeheerder

Providers:

Name	Priority	Description
<input type="text" value="select an option"/>	<input type="text"/>	<input type="text"/>

Create TACACS+ Provider

Update Cancel

APIC TACACS-provider

Stap 3. Definieer het ISE IP-adres of de hostnaam, definieer een gedeeld geheim en kies de Management Endpoint Policy Group (EPG). Klik om de TACACS+ provider toe te voegen aan de inlogbeheerder.

Create TACACS+ Provider



Host Name (or IP Address):

Description:

Port:

Authorization Protocol: CHAP MS-CHAP PAP

Key:

Confirm Key:

Timeout (sec):

Retries:

Management EPG:

Server Monitoring: Disabled Enabled

Cancel

Submit

Instellingen APIC TACACS-provider

Create Login Domain



Name:

Realm:

Description:

Providers:

Name	Priority	Description
52.13.89	1	


Cancel

Submit

Host Name	Description	Port	Timeout (sec)	Retries
52.13.89		49	5	1

Weergave van TACACS-provider

ISE-configuratie

>Stap 1. Navigeer naar  Beheer > Netwerkbronnen > Netwerkapparaatgroepen. Maak een netwerkapparaatgroep onder Alle apparaattypen.

 **Cisco ISE**

Network Devices **Network Device Groups** Network Device Profiles External

Network Device Groups

All Groups

Choose group 

 **Add** Duplicate Edit  Trash  Show group members  Import  Export 

<input type="checkbox"/> Name	Description
<input type="checkbox"/>  All Device Types	All Device Types
<input type="checkbox"/> APIC	

ISE-netwerkapparaatgroepen

Stap 2. Navigeer naar Administration > Network Resources > Network Devices. Kies **Add** APIC-naam en IP-adres definiëren, kies APIC onder Apparaattypen en aanvinkvakje TACACS+ en definieer het wachtwoord dat wordt gebruikt bij de APIC TACACS+ Provider-configuratie. Klik op de knop **.Submit**

Network Devices

Default Device

Device Security Settings

[Network Devices List](#) > APIC-LAB

Network Devices

Name

Description

IP Address * IP :

Device Profile

Model Name

Software Version

Network Device Group

Location [Set To Default](#)

IPSEC [Set To Default](#)

Device Type [Set To Default](#)

RADIUS Authentication Settings

TACACS Authentication Settings

Shared Secret [Show](#)

[Retire](#)

Herhaal stap 1 en stap 2 voor bladzijdige switches.

Stap 3. Gebruik de instructies op deze link om ISE te integreren met Active Directory;

<https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/217351-ad-integration-for-cisco-ise-gui-and-cli.html>.



Opmerking: Dit document omvat zowel interne gebruikers als AD Administrator-groepen als identiteitsbronnen. De test wordt echter uitgevoerd met de Identity Source van de interne gebruikers. Het resultaat is hetzelfde voor AD-groepen.

Stap 4. (Optioneel) Navigeer naar **☰**>Administration > Identity Management > Groups. Kies **User Identity Groups** en klik **Add**. Maak één groep voor alleen-lezen Admin-gebruikers en Admin-gebruikers.

Identity Groups

EQ

< [List Icon] [Settings Icon]

- > Endpoint Identity Groups
- > **User Identity Groups**

User Identity Groups

Edit Add Delete Import Export

	Name	Description
<input type="checkbox"/>	ALL_ACCOUNTS (default)	Default ALL_
<input type="checkbox"/>	APIC_RO	
<input type="checkbox"/>	APIC_RW	

Identiteitsgroep

Step 5. (Optioneel) Navigeer naar ☰ > Administration > Identity Management > Identity. Klik op **Add** en maak één **Read Only Admin** gebruiker en **Admin** gebruiker aan. Wijs elke gebruiker toe aan elke groep die in Step 4 is gemaakt.

Users

Latest Manual Network Scan Res...

Network Access Users

Edit Add Change Status Import Export Delete Duplicate

	Status	Username	Description	First Name	Last Name	Email Address	User Identity Groups
<input type="checkbox"/>	Enabled	APIC_ROUser					APIC_RO
<input type="checkbox"/>	Enabled	APIC_RWUser					APIC_RW

Step 6. Navigeer naar ☰ > Administration > Identity Management > Identity Source Sequence. Kies **Add**, definieer een naam en kies **AD Join Points** en **Internal Users** Identity Source uit de lijst. Kies **Treat as if the user was not found and proceed to the next store in the sequence** onder **Advanced Search List Settings** en klik **Save**.

∨ Identity Source Sequence

* Name

Description

∨ Certificate Based Authentication

Select Certificate Authentication Profile

∨ Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available		Selected
Internal Endpoints		iselab
Guest Users		Internal Users
All_AD_Join_Points		

Navigation buttons: > < >> << (between columns) and ^ > < > (on right side)

∨ Advanced Search List Settings

If a selected identity store cannot be accessed for authentication

- Do not access other stores in the sequence and set the "AuthenticationStatus" attribute to "ProcessError"
- Treat as if the user was not found and proceed to the next store in the sequence

Identity Source Sequence

7. Navigeer naar ☰ > Work Centers > Device Administration > Policy Elements > Results > Allowed Protocols. Selecteer

Add, definieer een naam en uncheck Allow CHAP en sta MS-CHAPv1 toe uit de lijst van verificatieprotocollen. Selecteer Opslaan.

Overview Identities User Identity Groups Ext Id Sources Network Resources

Conditions >

Network Conditions >

Results v

Allowed Protocols

TACACS Command Sets

TACACS Profiles

[Allowed Protocols Services List](#) > TACACS Protocol

Allowed Protocols

Name TACACS Protocol

Description

v Allowed Protocols

Authentication Protocols

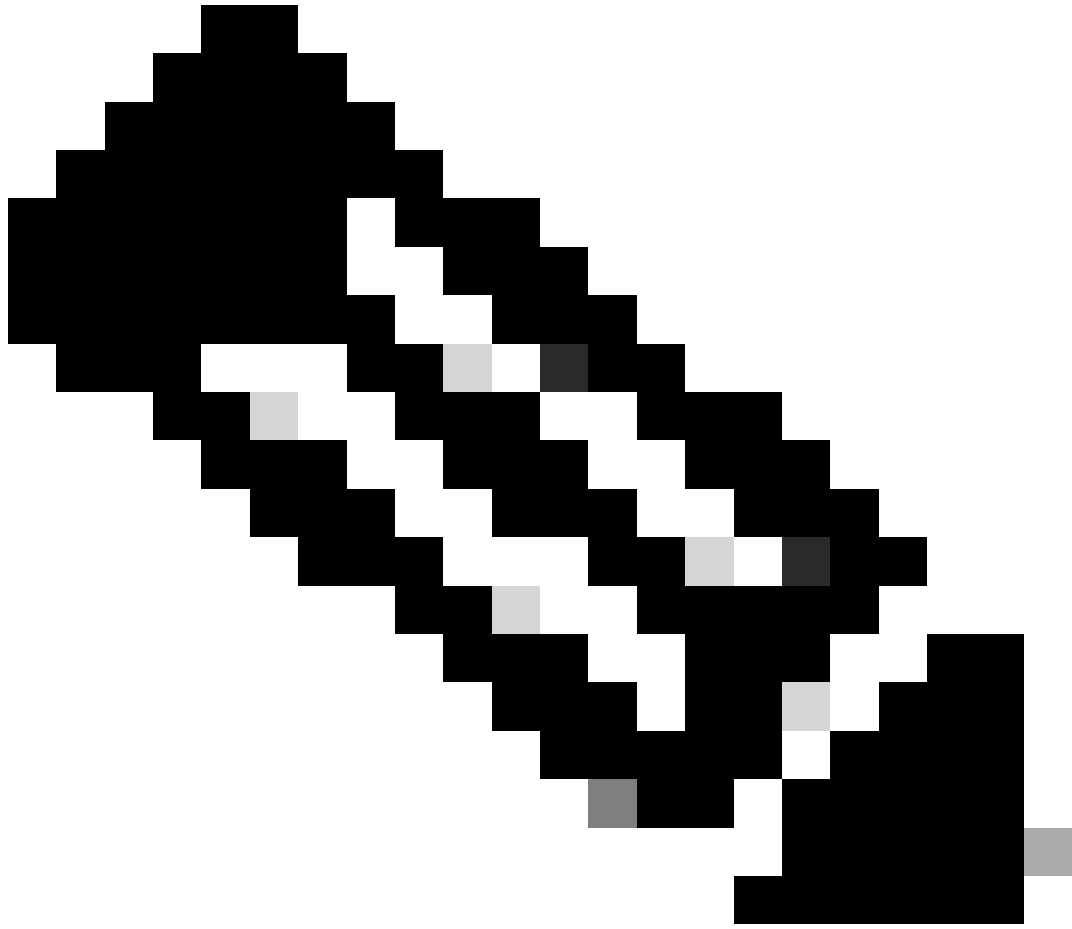
Only Authentication Protocols relevant to TACACS are displayed.

- Allow PAP/ASCII
- Allow CHAP
- Allow MS-CHAPv1

Protocol voor TACACS-toestemming

8. Navigeer naar > Work Centers > Device Administration > Policy Elements > Results > TACACS Profile. **Klik** **aan** **maak** twee profielen aan op basis van de kenmerken in de lijst onder Raw View. Klik op de knop .Save

- **Beheerder:** cisco-av-pair=shell:domains=all/admin/
- **Alleen-lezen beheerder gebruiker:** cisco-av-pair=shell:domains=all/read-all



Opmerking: In het geval van spaties of extra tekens mislukt de autorisatiefase.

TACACS Profiles > APIC ReadWrite Profile

TACACS Profile

Name
APIC ReadWrite Profile

Description

Task Attribute View **Raw View**

Profile Attributes

cisco-av-pair=shell:domains=all/admin/

Cancel Save

TACACS-profiel

Overview Identities User Identity Groups Ext Id Sources **Network Resources**

TACACS Profiles

Refresh Add Duplicate Trash Edit

<input type="checkbox"/>	Name	Type	Description
<input type="checkbox"/>	APIC ReadOnly Profile	Shell	
<input type="checkbox"/>	APIC ReadWrite Profile	Shell	

Admin- en Admin-profielen voor TACACS-beheer en alleen-lezen

Stap 9. Navigeer naar > Work Centers > Device Administration > Device Admin Policy Set. Maak een nieuwe beleidsset, definieer een naam en kies het in Stap 1 APICTACACS Protocolgemaakte apparaattype. Kies gemaakt in Stap 7. zoals toegestaan in het Protocol en klikSave.

Policy Sets Reset [Reset Policyset Hitcounts](#) [Save](#)

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
●	APIC		DEVICE-Device Type EQUALS All Device Types#APIC	TACACS Protocol	55		

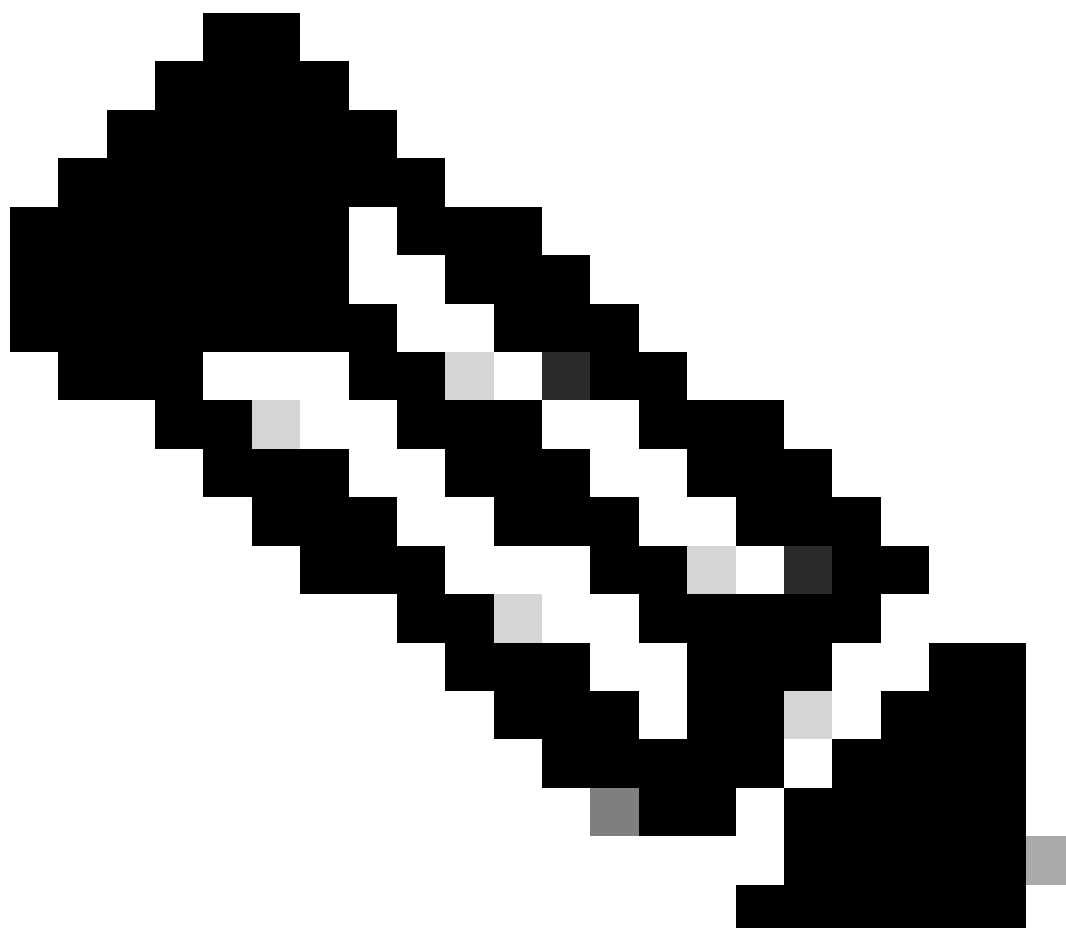
TACACS-beleidsset

Stap 10. Klik onder nieuw Policy Set op het pijltje rechts en voer een verificatiebeleid in. Definieer een naam en kies het IP-adres van het apparaat als voorwaarde. Kies vervolgens de Identity Source Sequence die in Stap 6 is gemaakt.

Authentication Policy (2)

Status	Rule Name	Conditions	Use	Hits	Actions
●	APIC Authentication Policy	Network Access Device IP Address EQUALS 188.21	APIC_ISS	55	Options

Verificatiebeleid



Opmerking: Locatie of andere kenmerken kunnen als verificatievoorwaarde worden gebruikt.

Stap 1. Maak een autorisatieprofiel voor elk Admin-gebruikerstype, definieer een naam en kies een interne gebruiker en/of AD-gebruikersgroep als voorwaarde. Aanvullende voorwaarden zoals APIC kunnen worden gebruikt. Kies het juiste shell-profiel op elk autorisatiebeleid en klik op Save.

Authorization Policy (3)

Status	Rule Name	Conditions	Results		
			Command Sets	Shell Profiles	Hits
ON	APIC Admin RO	AND Network Access Device IP Address EQUALS :188.21 IdentityGroup-Name EQUALS User Identity Groups:APIC_RO		APIC ReadOnly Profile	34
ON	APIC Admin User	AND Network Access Device IP Address EQUALS :188.21 OR IdentityGroup-Name EQUALS User Identity Groups:APIC_RW Iselab-ExternalGroups EQUALS cisco:lab/Bullin/Administrators		APIC ReadWrite Profile	16
ON	Default		DenyAllCommands	Deny All Shell Profile	0

Autorisatieprofiel TACACS

Verifiëren

Stap 1. Meld u aan bij de APIC UI met gebruikersbeheerder referenties. Kies de optie TACACS uit de lijst.

APIC
Version 4.2(7u)
CISCO

User ID
APIC_ROUser

Password
.....

Domain
S_TACACS

Login

APIC-aanmelding

Stap 2. Controleer de toegang op de APIC UI en het juiste beleid wordt toegepast op de TACACS Live logs.

Welcome to APIC

What's new in version 4.2(7u)



New Features

- Floating L3out
 - Docker EE (Kubernetes) container integration
 - L4-L7 Services support in vPod
 - Backup PBR destination
 - Support for 64 Remote Leaf pairs
- UI Enhancements:
 - User-defined UI banner
 - First Time Setup wizard
 - Simplified L3Out creation
 - EPG to leafs deployment view

[View Release Notes](#)

Getting Started

[What's New in v4.2\(7u\)](#)

[Online Videos \(YouTube™\)](#)

[View All Tutorial Videos](#)

Explore

[Configuration Guides](#)

[Knowledge Base Articles](#)

[APIC Communities](#)

Support

[Online Help](#)

[Troubleshooting](#)

[Documentation](#)

Do not show on login

[Review First Time Setup](#)

[Get Started](#)

APIC welkomstboodschap

Herhaal stap 1 en 2 voor gebruikers van Alleen-lezen beheerder.

☰ Cisco ISE

Operations · TACACS

Live Logs

🔄 Export To

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	Network Devic...
×	▼		Identity	▼	Authentication Policy	Authorization Policy	Ise Node	Network Device N...
Apr 20, 2023 10:14:42.4...	✓	🔒	APIC_ROUser	Authorizat...		APIC >> APIC Admin RO	PAN32	APIC-LAB
Apr 20, 2023 10:14:42.2...	✓	🔒	APIC_ROUser	Authentic...	APIC >> APIC Authentication Po...		PAN32	APIC-LAB

Last Updated: Fri Apr 21 2023 00:14:53 GMT+0200 (Central European Summer Time)

Levende logbestanden voor TACACS+

Problemen oplossen

Stap 1. Navigeer naar ☰ > Operations > Troubleshoot > Debug Wizard. Kies TACACS en klik Debug Nodes.

Debug Profile Configuration

Debug Wizard contains predefined debug templates with the help of which you can troubleshoot issues on ISI

 [Add](#)  [Edit](#)  [Remove](#)  [Debug Nodes](#)

<input type="checkbox"/>	Name	Description	Status
<input type="checkbox"/>	802.1X/MAB	802.1X/MAB	DISABLED
<input type="checkbox"/>	Active Directory	Active Directory	DISABLED
<input type="checkbox"/>	Application Server Issues	Application Server Issues	DISABLED
<input type="checkbox"/>	BYOD portal/Onboarding	BYOD portal/Onboarding	DISABLED
<input type="checkbox"/>	Context Visibility	Context Visibility	DISABLED
<input type="checkbox"/>	Guest portal	Guest portal	DISABLED
<input type="checkbox"/>	Licensing	Licensing	DISABLED
<input type="checkbox"/>	MnT	MnT	DISABLED
<input type="checkbox"/>	Posture	Posture	DISABLED
<input type="checkbox"/>	Profiling	Profiling	DISABLED
<input type="checkbox"/>	Replication	Replication	DISABLED
<input checked="" type="checkbox"/>	TACACS	TACACS	DISABLED

Configuratie debug-profiel

Stap 2. Kies het knooppunt dat het verkeer ontvangt en klik [Save](#).

Diagnostic Tools Download Logs **Debug Wizard**




Debug Profile Configuration
Debug Log Configuration

Debug Profile Configuration > Debug Nodes

Debug Nodes

Selected profile TACACS

Choose on which ISE nodes you want to enable this profile.

 Filter  

<input type="checkbox"/>	Host Name	Persona	Role
<input checked="" type="checkbox"/>	PAN32.ciscoise.lab	Administration, Monitoring, Policy Service	PRI(A), PRI(M)
<input type="checkbox"/>	SPAN32.ciscoise.lab	Administration, Monitoring, Policy Service, ...	SEC(A), SEC(M)

[Cancel](#) [Save](#)

Selectie van debugknooppunten

Stap 3. Voer een nieuwe test uit en download de logbestanden onder Operations > Troubleshoot > Download logs zoals getoond:

```
AcsLogs,2023-04-20 22:17:16,866,DEBUG,0x7f93cab7700,cntx=0004699242,sesn=PAN32/469596415/70,CPMSession
```

Als debugs geen authenticatie- en autorisatie-informatie tonen, valideert u dit:

1. De service Apparaatbeheer is ingeschakeld voor de ISE-knooppunt.
2. Het juiste ISE IP-adres is toegevoegd aan de APIC-configuratie.
3. Als een firewall in het midden zit, controleer dan of poort 49 (TACACS) is toegestaan.

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.