Secure Shell (SSH) op een access point (AP) inschakelen

Inhoud

Inleiding

Dit document beschrijft hoe u een access point (AP) kunt configureren om op Secure Shell (SSH) gebaseerde toegang mogelijk te maken.

Voorwaarden

Vereisten

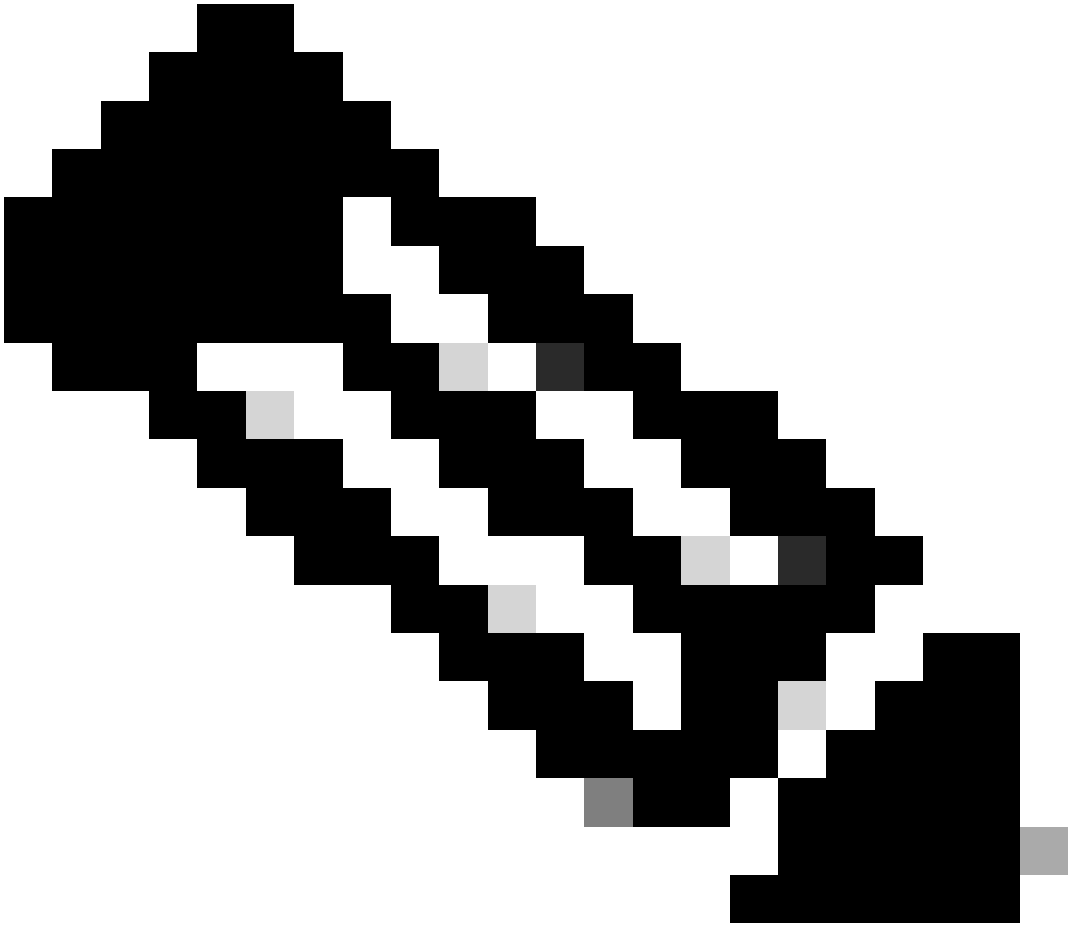
Voordat u deze configuratie uitvoert, moet aan de volgende vereisten worden voldaan:

- Kennis van de configuratie van Cisco Aironet AP's
- Basiskennis van SSH en bijbehorende beveiligingsconcepten

Gebruikte componenten

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

- Aironet 1200 Series access point dat Cisco IOS®-softwarerelease 12.3(8)JEB
- PC of laptop met SSH client utility



Opmerking: dit document gebruikt het SSH-clienthulpprogramma om de configuratie te verifiëren. U kunt een clientprogramma van derden gebruiken om in te loggen op het toegangspunt met behulp van SSH.

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.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Toegang tot de Command-Line Interface (CLI) op Aironet AP

U kunt deze methoden gebruiken om toegang te krijgen tot de opdrachtregelinterface (CLI) op Aironet AP:

- De consolepoort
- Telnet
- SSH

Als het toegangspunt is voorzien van een consolepoort en u fysieke toegang hebt tot het toegangspunt, kunt u de consolepoort gebruiken om in te loggen op het toegangspunt en indien nodig de configuratie te wijzigen. Raadpleeg het gedeelte Verbinding maken met de 1200 Series access points uit het document Het access point voor het eerst configureren voor het gebruik van de consolepoort om in te loggen op het toegangspunt. voor meer informatie over het gebruik van de consolepoort.

Als u het toegangspunt alleen via Ethernet kunt benaderen, gebruikt u het Telnet-protocol of het SSH-protocol om u aan te melden bij het toegangspunt.

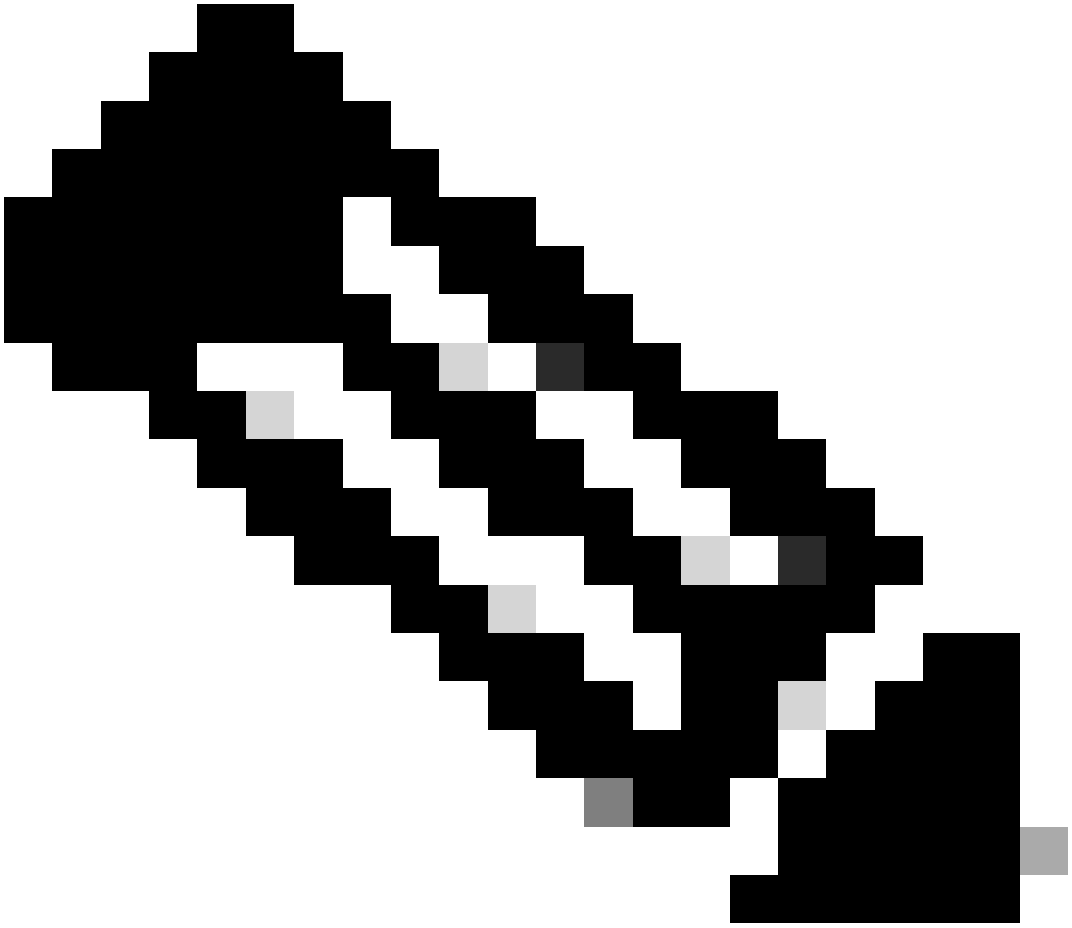
Het Telnet-protocol gebruikt poort 23 voor communicatie. Telnet verzendt en ontvangt gegevens in duidelijke tekst. Omdat de datacommunicatie in duidelijke tekst gebeurt, kan een hacker eenvoudig de wachtwoorden compromitteren en toegang tot de AP. RFC 854 definieert Telnet en breidt Telnet met opties uit door vele andere RFC's.

SSH is een toepassing en protocol die een veilige vervanging voor de Berkley r-tools biedt. SSH is een protocol dat een beveiligde, externe verbinding biedt met een Layer 2- of Layer 3-apparaat. Er zijn twee versies van SSH: SSH versie 1 en SSH versie 2. Deze softwarerelease ondersteunt beide SSH-versies. Als u het versienummer niet opgeeft, blijft het toegangspunt standaard bij versie 2.

SSH biedt meer beveiliging voor verbindingen op afstand dan Telnet omdat het een sterke codering biedt wanneer een apparaat wordt geverifieerd. Deze encryptie is een voordeel over een zitting van Telnet, waarin de mededeling in duidelijke tekst gebeurt. Raadpleeg Veelgestelde vragen over Secure Shell (SSH) voor meer informatie over SSH. De SSH-functie heeft een SSH-server en een SSH geïntegreerde client.

De client ondersteunt deze methoden voor gebruikersverificatie:

- RADIUS
- Lokale authenticatie en autorisatie.



Opmerking: de SSH-functie in deze softwarerelease ondersteunt IP-beveiliging (IPSec) niet.

U kunt AP's voor SSH configureren met behulp van de CLI of GUI. Dit document verklaart beide configuratiemethoden.

Configureren

CLI-configuratie

Deze sectie verschaft de informatie over hoe u de functies kunt configureren met behulp van CLI.

Stapsgewijze instructies

Om op SSH gebaseerde toegang op het toegangspunt in te schakelen, moet u eerst het toegangspunt configureren als een SSH-server. Voer deze stappen uit om een SSH-server op het

toegangspunt te configureren vanaf CLI:

1. Configureer een hostnaam en domeinnaam voor het toegangspunt.

   <#root>

   ```
   AP#
   configure terminal

   !--- Enter global configuration mode on the AP.

   AP<config>#
   hostname Test

   !--- This example uses "Test" as the AP host name.

   Test<config>#
   ip domain name domain

   !--- This command configures the AP with the domain name "domain name".
   ```

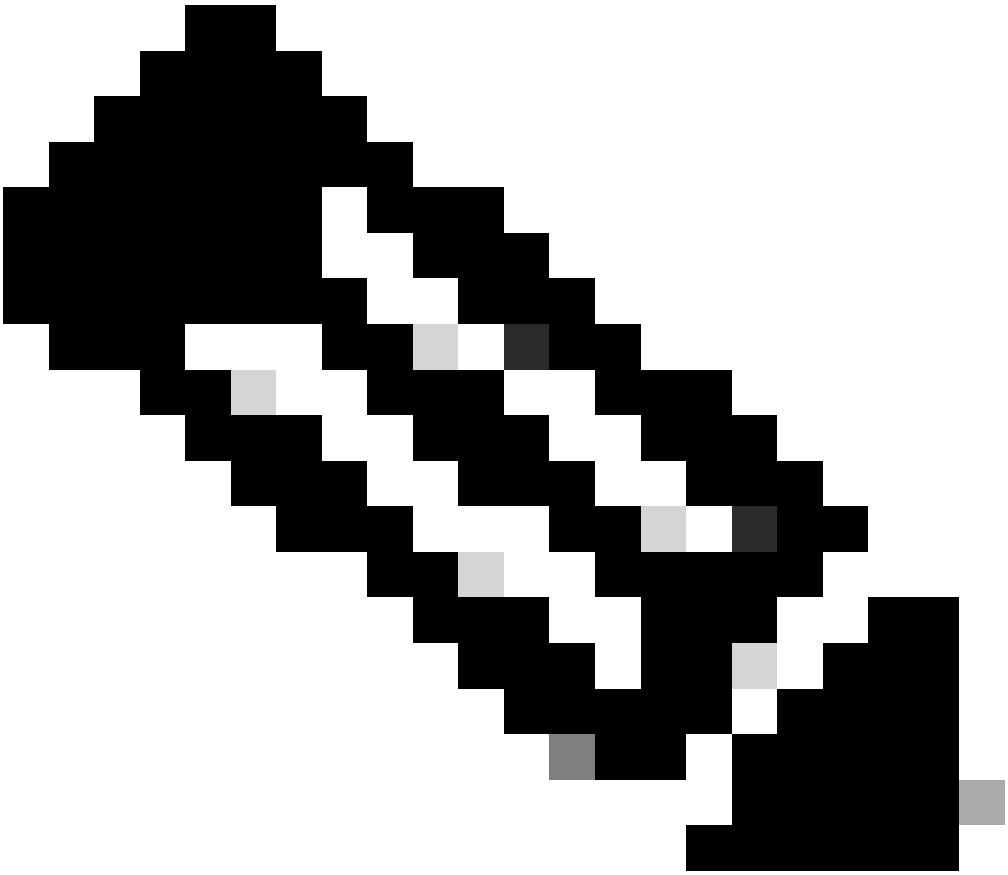
2. Genereer een Rivest, Shamir, en Adelman (RSA) sleutel voor uw AP.

   Door een RSA-toets te genereren kan SSH op het toegangspunt worden ingeschakeld. Geef deze opdracht in globale configuratiemodus uit:

   <#root>

   ```
   Test<config>#
   crypto key generate rsa rsa_key_size

   !--- This generates an RSA key and enables the SSH server.
   ```



Opmerking: de aanbevolen minimale grootte van de RSA-sleutel is 1024.

3. Configureer de gebruikersverificatie op het toegangspunt.

   Op het toegangspunt kunt u gebruikersverificatie configureren door gebruik te maken van de lokale lijst of van een externe verificatie-, autorisatie- en accounting (AAA) server. In dit voorbeeld wordt een lokaal gegenereerde lijst gebruikt om de gebruikers te verifiëren:

   <#root>

   ```
   Test<config>#
   aaa new-model

   !--- Enable AAA authentication.

   Test<config>#
   aaa authentication login default local none
   ```

```
!--- Use the local database in order to authenticate users.

Test<config>#

username Test password Test123

!--- Configure a user with the name "Test".

Test<config>#

username ABC password xyz123

!--- Configure a second user with the name "Domain".
```

Met deze configuratie wordt het toegangspunt geconfigureerd voor het uitvoeren van gebruikersgebaseerde verificatie met behulp van een lokale database die op het toegangspunt is geconfigureerd. In het voorbeeld worden twee gebruikers in de lokale database geconfigureerd, "Test" en "ABC".

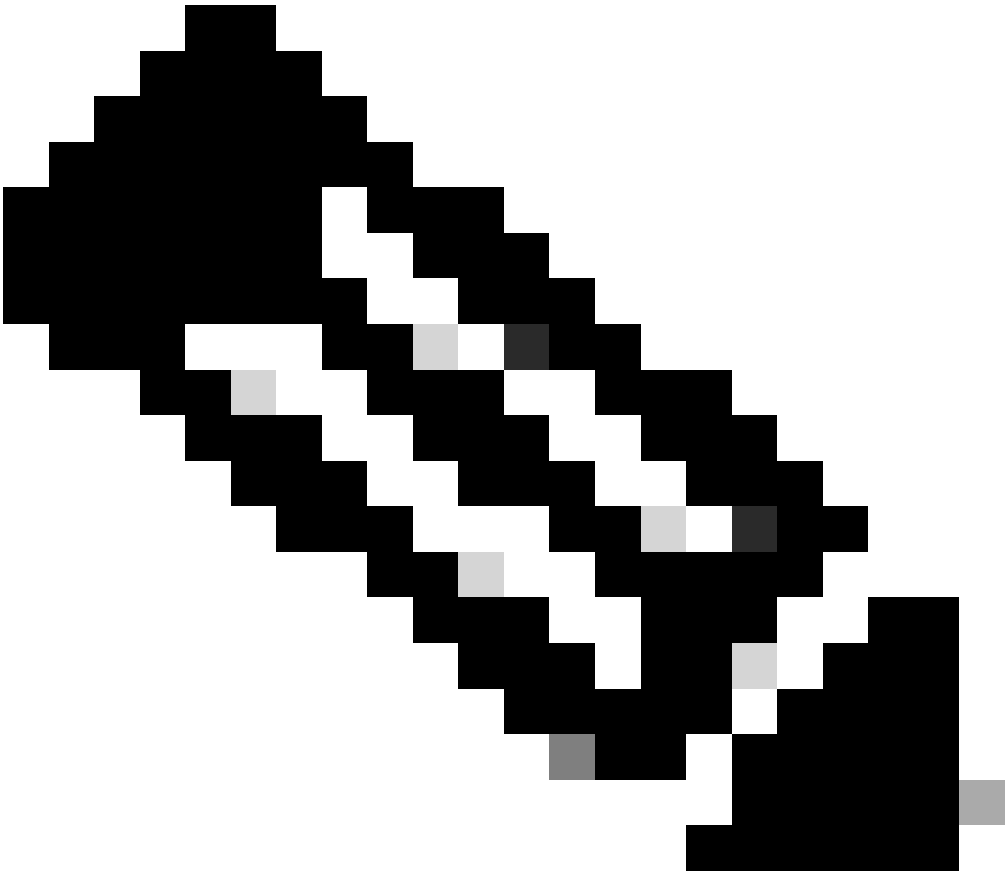
4. Configureer de SSH-parameters.

<#root>

```
Test<config>#

ip ssh {[timeout seconds] | [authentication-retries integer]}

!--- Configure the SSH control variables on the AP.
```



Opmerking: u kunt de timeout in seconden instellen, maar u mag de 120 seconden niet overschrijden. De standaardwaarde is 120. Dit is de specificatie die van toepassing is op de SSH-onderhandelingsfase. U kunt ook opgeven hoeveel verificatiepogingen moeten worden uitgevoerd, maar het aantal verificatiepogingen mag niet groter zijn dan vijf. De standaardinstelling is drie.

Configuratie GUI

U kunt ook de GUI gebruiken om op SSH gebaseerde toegang tot het toegangspunt in te schakelen.

Stapsgewijze instructies

Voer de volgende stappen uit:

1. Log in op het toegangspunt via de browser.

   Het venster Samenvatting van de status verschijnt.

2. Klik op Services in het menu links.

   Het venster Serviceoverzicht wordt weergegeven.

3. Klik op Telnet/SSH om de Telnet/SSH-parameters in te schakelen en te configureren.

   Het venster Services: Telnet/SSH wordt weergegeven. Blader naar beneden naar het configuratiegebied van Secure Shell. Klik op Inschakelen naast Secure Shell en voer de SSH-parameters in zoals dit voorbeeld toont:

   In dit voorbeeld worden deze parameters gebruikt:

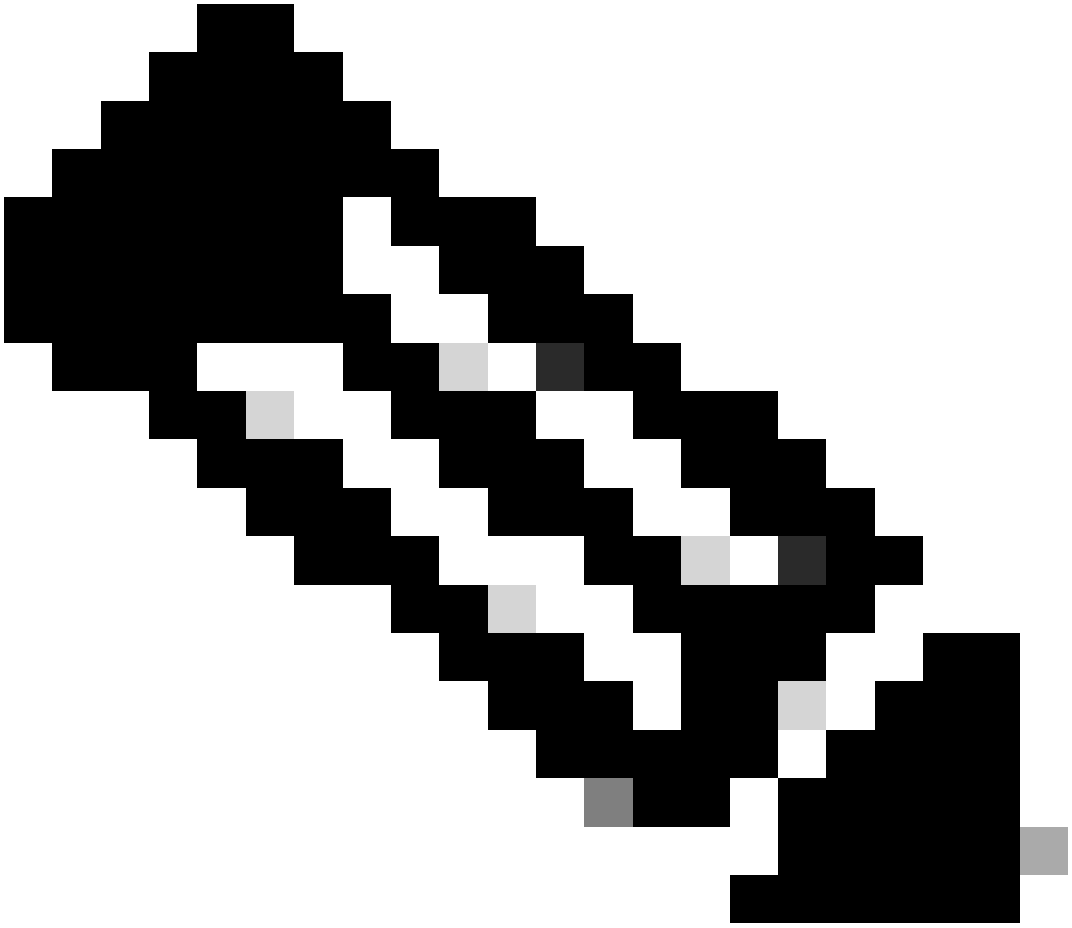
   - Systeemnaam: Test
   - Domeinnaam:
   - RSA-sleutelgrootte: 1024
   - Time-out verificatie: 120
   - Verificatiepogingen: 3

4. Klik op Toepassen om de wijzigingen op te slaan.

Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

De Output Interpreter Tool (OIT) ondersteunt bepaalde show opdrachten. Gebruik de OIT om een analyse te bekijken van de output van de opdracht show.



Opmerking: alleen geregistreerde Cisco-gebruikers kunnen toegang krijgen tot interne Cisco-tools en -informatie.

- toon ip sh-Verificeert als SSH op het AP is ingeschakeld en u in staat stelt om de versie van SSH te controleren die op het AP wordt uitgevoerd. Deze output geeft een voorbeeld:
- toon ssh-laat u toe om de status van uw SSH serververbindingen te bekijken. Deze output geeft een voorbeeld:

Start nu een verbinding via een pc die SSH-software van derden uitvoert en probeer vervolgens in te loggen op het toegangspunt. Bij deze verificatie wordt het IP-adres van het toegangspunt gebruikt, 10.0.0.2. Omdat u de Test van de gebruikersnaam hebt gevormd, gebruik deze naam om tot AP door SSH toegang te hebben:

Problemen oplossen

Deze sectie bevat informatie om uw configuratie te troubleshooten.

Als uw SSH-configuratieopdrachten worden afgewezen als illegale opdrachten, hebt u geen RSA-sleutelpaar gegenereerd voor uw AP.

SSH uitschakelen

Om SSH op een AP uit te schakelen, moet u het RSA-paar verwijderen dat op het AP gegenereerd is. Als u het RSA-paar wilt verwijderen, moet u de opdracht RSA in globale configuratiemodus op de crypto-toets zeroize uitgeven. Wanneer u het RSA-sleutelpaar verwijdert, schakelt u automatisch de SSH-server uit. Deze output geeft een voorbeeld:

Gerelateerde informatie

- Ondersteuning van Secure Shell (SSH)
- Cisco Technical Support en downloads

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.