Secure Shell (SSH) - FAQ

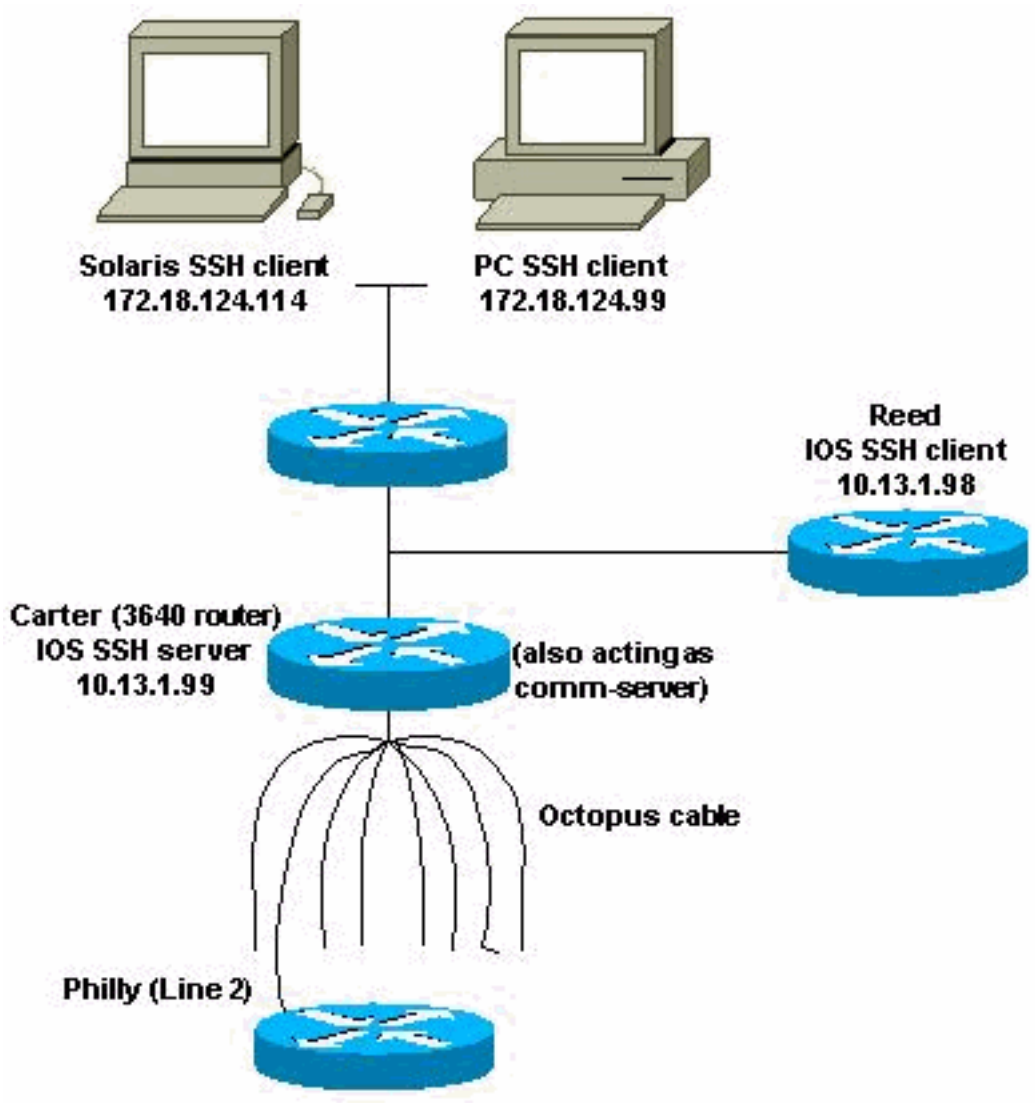
Inhoud

Inleiding

Dit document beantwoordt de meest frequent gestelde vragen (FAQ's) met betrekking tot Secure Shell (SSH). Cisco IOS® SSH-code is de oorspronkelijke Cisco-code.

Hoe vorm ik SSH-terminallijn toegang (ook bekend als reverse-telnet)?

Dit werd eerst geïntroduceerd in sommige platforms van Cisco IOS-softwarerelease 12.2.T.




```
Router(config)#line line-number [ending-line-number]
Router(config-line)#no exec
Router(config-line)#login {local | authentication listname
Router(config-line)#rotary group
Router(config-line)#transport input {all | ssh}
Router(config-line)#exit
Router(config)#ip ssh port portnum rotary group

!--- Line 1 SSH Port Number 2001 line 1 no exec login authentication default rotary 1 transport
input ssh !--- Line 2 SSH Port Number 2002 line 2 no exec login authentication default rotary 2
transport input ssh !--- Line 3 SSH Port Number 2003 line 3 no exec login authentication default
rotary 3 transport input ssh ip ssh port 2001 rotary 1 3
```

Opdrachtreferenties

```
ip ssh port
ip ssh port portnum rotary group
no ip ssh port portnum rotary group
```

- portum - Specificeert de poort waar SSH verbinding mee moet maken, zoals in 2001.
- roterende groep - Specificeert de gedefinieerde rotonde die naar een geldige naam moet zoeken.

Wordt SSH ondersteund op Catalyst 2900?

Nee, dat is het niet.

Hoe kan ik bepalen welke platforms en versies van code SSH ondersteunen?

Zie de Functie Navigator (alleen geregistreerde klanten) en specificeer de **SSH** optie.

Wanneer ik bepaalde SSH-opdrachten uit mijn router probeer te verwijderen, blijft het me vragen om RSA-toetsen te maken om SSH in te schakelen. Waarom is dit?

Hier wordt een voorbeeld van dit probleem gegeven:

```
804#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
804(config)#no ip ssh time-out 120
Please create RSA keys to enable SSH.
804(config)#no ip ssh authen
Please create RSA keys to enable SSH.
804(config)
```

U hebt Cisco bug-id CSCdv70159 aangetroffen (alleen geregistreerde klanten).

Ondersteuning van Cisco IOS SSH versie 2 voor Digital Signature Standard (DSS)?

Cisco IOS SSH versie 2 ondersteunt DSS niet.

Steunt de Cisco IOS SSH server agent die door:sturen?

Cisco IOS SSH ondersteunt het doorsturen van agents niet. Het interopereert met alle commerciële SSH-implementaties.

Welke mechanismen voor clientverificatie worden ondersteund op de Cisco IOS SSH-server?

Cisco IOS SSH versie 2 (SSHv2) ondersteunt toetsenbord-interactieve en op wachtwoord gebaseerde verificatiemethoden. Naast deze authenticatiemethoden ondersteunt de SSHv2-verbeteringen voor RSA-sleutels (beschikbaar in Cisco IOS-softwarerelease 15.0(1)M en later) op RSA gebaseerde openbare verificatie voor de client en server. Raadpleeg voor extra informatie over de verificatiemechanismen die worden ondersteund door de Cisco IOS SSH-server de ondersteuning Secure Shell (versie 2).

Wat doet de fout `lokaal: Corrupte check bytes op invoergemiddelde`?

Corrupte checkbytes betekent dat het ontvangen SSH-pakket niet is gecontroleerd op de integriteit van het programma. Dit komt meestal door onjuiste decryptie. Dit komt ook doordat er een verkeerde toets is gebruikt. De onjuiste sleutel wordt veroorzaakt door het laten vallen van een gecodeerd SSH-pakket. U hebt een versleuteld pakje laten vallen dat verzonden of laten vallen, een gecodeerd pakje dat gedecrypteerd had moeten worden.

Ondersteunt Cisco IOS SSH met het Blowfish-algoritme?

Cisco IOS ondersteunt SSH niet met Blowfish algoritme. Wanneer een SSH-client een dergelijk niet-ondersteund algoritme verstuurt, geeft de router debug-berichten die in SSH-client zijn vermeld, weer door niet-ondersteunde (zwarte) client.

Wanneer ik RSA toetsen voor SSH-toegang op een router probeer te genereren met behulp van de crypto-toets die rsa-opdracht in de configuratie-modus genereren, ontvang ik deze fout: `% Ongeldige invoer gedetecteerd bij '^' marker.`. Het laat de router de toetsen RSA niet genereren om SSH-toegang voor de router mogelijk te maken. Hoe is deze fout opgelost?

Deze fout verschijnt wanneer het beeld dat op de router wordt gebruikt, niet de **crypto-toets ondersteunt die rsa** opdracht **genereren**. Deze opdracht wordt alleen ondersteund in beveiligingsafbeeldingen. Om deze fout op te lossen gebruikt u het beveiligingsbeeld van de juiste serie van de Cisco IOS-router die gebruikt wordt.

Ondersteunt Crypto-beelden een sterk algoritme om SSH met ciphers zoals 3DES of AES te gebruiken?

Ja. Alleen encryptie-afbeeldingen ondersteunen een sterk algoritme. Om SSH met cifen zoals 3DES of AES te kunnen gebruiken moet u Crypto beelden op uw apparaat van Cisco hebben.

Deze berichten worden gezien in de logs wanneer ik SSH op een router probeer te configureren: `SSH2 13: RSA_teken: private sleutel niet gevonden` en `SSH2 13: Het aanmaken van de handtekening is mislukt, status -1`. Hoe wordt dit opgelost?

Deze logberichten worden gezien door Cisco bug-ID's CSCsa83601 (alleen geregistreerde klanten) en CSCtc4114 (alleen geregistreerde klanten). Raadpleeg deze insecten voor meer informatie.

Gerelateerde informatie

- SSH-ondersteuningspagina
- Technische ondersteuning en documentatie – Cisco Systems