

# Probleemoplossing voor fouten in SSH-hostsleutelverificatie

## Inhoud

---

## Inleiding

Dit document beschrijft het proces om het mislukte probleem van de SSH-hosttoetsverificatie op te lossen.

## Achtergrond

Deze fout treedt op wanneer een gebruiker probeert om SSH naar DNACenter's grapevine nadat DNACenter afbeelding is bijgewerkt. Tot nu toe is dit probleem alleen gezien bij macOS-gebruikers.

## Beschrijving

Nadat DNACenter is geüpgraded naar een nieuwe afbeelding, behoudt het SSH-sleutelregisterbestand van de lokale gebruiker de SSH-toets die wordt gebruikt om verbinding te maken met de druivenvoorzet van de vorige DNACenter. Dit is de fout:

```
MPAVLOVI-M-902T:~ mpavlovi$ ssh grapevine@172.16.21.86 -p 2222
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!    @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that a host key has just been changed.
The fingerprint for the ECDSA key sent by the remote host is
SHA256:+dnn+NRIXTDMmgpUNbeqjdDQscabBBWmC35F01ZFnlS.
Please contact your system administrator.
Add correct host key in /Users/mpavlovi/.ssh/known_hosts to get rid of this message.
Offending ECDSA key in /Users/mpavlovi/.ssh/known_hosts:16
ECDSA host key for [172.16.21.86]:2222 has changed and you have requested strict checking.
Host key verification failed.
MPAVLOVI-M-902T:~ mpavlovi$
```

## Oplossing

Om dit probleem op te lossen, moet de vorige grapevine SSH-toets worden verwijderd uit het registratiebestand `known_host` in de lokale directory `~/.ssh/`.

Als u de vorige SSH-toetsen wilt verwijderen, gaat u naar terminal en gebruikt u de teksteditor naar keuze om het bestand te openen:

```
MPAVLOVI-M-902T:~ mpavlovi$ vim ~/.ssh/known_hosts
```

Schrap de regel die het DNACenter IP-adres bevat

```
[10.197.218.12]:2222 ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBKkToWAUhe  
[172.16.21.86]:2222 ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBKz4ObQLQE7
```



Opmerking: Het wijzigen van andere toetsen kan van invloed zijn op uw SSH-toegang tot andere apparaten/sites. Alleen de benodigde SSH-toets(en) verwijderen.

---

```
[10.197.218.12]:2222 ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBKkToWAUHe
```

Sla de wijzigingen in de teksteditor op en probeer opnieuw naar SSH om DNACenter grapevine. Typ het woord "ja" wanneer hierom wordt gevraagd.

```
MPAVLOVI-M-902T:~ mpavlovi$ ssh grapevine@172.16.21.86 -p 2222
The authenticity of host '[172.16.21.86]:2222 ([172.16.21.86]:2222)' can't be established.
ECDSA key fingerprint is SHA256:+dnn+NRIXTDMmgrpUNbeqjdjDQscabBBWmC35F01ZFnlS.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[172.16.21.86]:2222' (ECDSA) to the list of known hosts.
```

Gebruik het wachtwoord voor de referenties van de wijnstok.

grapevine@172.16.21.86's password:

Welcome to the Cisco APIC-EM Appliance - Powered by Grapevine

System information as of Wed Jul 19 22:20:17 UTC 2017

System load:	1.02	Users logged in:	1
Usage of /:	11.7% of 365.80GB	IP address for eth0:	12.99.1.2
Memory usage:	41%	IP address for eth1:	172.16.21.86
Swap usage:	0%	IP address for grape-br0:	169.254.0.1
Processes:	695		

APIC-EM Version: 2.0.0.3757

Grapevine Version: 2.0.0.3757.dev1065-ge50d0c2

Last login: Wed Jul 19 21:45:22 2017 from 10.41.49.41

(grapevine)

[Wed Jul 19 22:20:18 UTC] grapevine@12.99.1.2 (grapevine-root-1) ~

\$

## 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.