

Vertraging voor wachtwoord verschijnt tijdens inloggen via SSH/telnet

Inhoud

[Inleiding](#)

[Probleem: Vertraging voor Wachtwoord direct weergegeven tijdens inloggen via SSH/telnet SSH naar de N5K0-interface](#)

[Telnet-interface naar N5K0](#)

[Oplossing](#)

Inleiding

Dit document beschrijft de vertraging voordat de wachtwoord wordt gevraagd terwijl u inlogt via SSH/telnet.

Dit probleem wordt vaak waargenomen wanneer u probeert om via SSH of telnet in te loggen op de GMT0-interface op een Nexus 5K/6K.

Nadat u de gebruiker-ID hebt ingevoerd, wordt deze tekst weergegeven en is er een langere vertraging zoals verwacht voordat de wachtwoordmelding wordt weergegeven.

```
login as: admin
<delay for several seconds before below text is appears>
Nexus 5000 Switch
Using keyboard-interactive authentication.
Password:
```

Probleem: Vertraging voor Wachtwoord direct weergegeven tijdens inloggen via SSH/telnet

Het probleem bestaat uit omgekeerde DNS-invoeging.

Standaard wordt ip-domein-lookup ingeschakeld op de Nexus en als een DNS-serverlijst (ip-naam-server) is ingesteld onder VRF-beheer, dan voert de switch een omgekeerde DNS-raadpleging van het IP-adres van de gebruiker uit wanneer ze via SSH of telnet een verbinding maken met de GMT0-poort.

Een omgekeerde DNS raadpleging is bedoeld voor veiligheidsdoeleinden om te controleren of het IP-adres van de bron legitiem is en om IP-spoofing te voorkomen.

Hier is een voorbeeld waar we een DNS-server 10.67.84.45 hebben gebruikt

De DNS-server in dit geval heeft geen ingangssignaal voor het IP-bronadres van de client en geeft geen antwoord. Dit resulteert in de Nexus-schakelaar die meerdere vragen uitvoert, aangezien de server geen resultaat teruggeeft, veroorzaakt dit de vertraging.

```
ip domain-lookup

vrf context management
  ip name-server 10.67.84.45
```

Van deze output van **show hosts**, kunt u zien dat er een DNS-server is die is ingesteld voor VRF-beheer en dat de IP-domeinraadpleging is ingeschakeld.

```
N5548P-2# show hosts
DNS lookup enabled

Name servers for vrf:management is 10.67.84.45

Host                Address
```

Deze Ethanalzyer-opnamen zijn genomen nadat de gebruikersnaam is ingevoerd en u wacht tot de wachtwoordmelding wordt weergegeven.

Het laat zien dat de Nexus-switch twee omgekeerde DNS-lookups uitvoert tegen het IP-adres van de bron van de gebruiker, 62.84.137.10

SSH naar de N5K0-interface

```
Username: admin
<delay for several seconds>

N5548P-2# ethalyzer local interface mgmt display-filter dns
Capturing on eth0
2015-05-09 22:11:44.105674 10.67.84.56 -> 10.67.84.45      DNS Standard query PTR 6
2.84.137.10.in-addr.arpa
2015-05-09 22:11:49.102673 10.67.84.56 -> 10.67.84.45      DNS Standard query PTR 6
2.84.137.10.in-addr.arpa

N5548P-2# 2 packets captured
The password prompt is then displayed for the user
Nexus 5000 Switch
Using keyboard-interactive authentication.
Password
:
```

Op dezelfde manier voert de schakelaar eerst de bovenstaande omgekeerde DNS raadpleging op het bron-IP-adres van de gebruiker uit wanneer u via telnet inlogt en geeft u vervolgens de inlogmelding weer.

Telnet-interface naar N5K0

```
telnet to switch 10.67.84.56
N5548P-2# ethalyzer local interface mgmt display-filter dns
Capturing on eth0
2015-05-09 22:24:56.303878 10.67.84.56 -> 10.67.84.45      DNS Standard query PTR 6
2.84.137.10.in-addr.arpa
2015-05-09 22:25:01.302680 10.67.84.56 -> 10.67.84.45      DNS Standard query PTR 6
2.84.137.10.in-addr.arpa
2 packets captured
```

De loginmelding wordt dan weergegeven:

```
Nexus 5000 Switch
login: admin
Password:
```

Oplossing

Oplossing 1. Wijzig de lijst van DNS-servers die op de Nexus zijn geconfigureerd, zodat de DNS-server wordt geraadpleegd voordat de DNS-server niet reageert.

Als de Nexus een geldige DNS-record van de lokale DNS-server ontvangt, wordt de tweede DNS-server in de lijst niet geraadpleegd. Dit vermindert de vertraging.

Voorbeeld:

```
vrf context management
no ip name-server 10.67.84.45
ip name-server 10.67.84.48 10.67.84.45
```

U kunt deze opdracht gebruiken om de huidige lijst met DNS-servers te controleren wanneer de lokale server als eerste in de lijst verschijnt:

```
N5548P-2# sh hosts
DNS lookup enabled
```

```
Name servers for vrf:management is 10.67.84.48 10.67.84.45
```

```
Host Address
```

Uit deze Ethalyzer-opname wordt eerst het IP om de raadpleging te noemen uitgevoerd en er wordt een reactie ontvangen.

Dit wordt gevolgd door een naam-aan-IP adresraadpleging waar een antwoord wordt ontvangen.

In dit geval werd er geen merkbare vertraging waargenomen bij het inloggen via SSH of telnet.

```
N5548P-2# ethalyzer local interface mgmt display-filter dns
Capturing on eth0
2015-05-09 22:55:46.037079 10.67.84.56 -> 10.67.84.48 DNS Standard query PTR
20.196.104.64.in-addr.arpa
2015-05-09 22:55:46.037444 10.67.84.48 -> 10.67.84.56 DNS Standard query res
ponse PTR no-sense-1.cisco.com
2015-05-09 22:55:46.041907 10.67.84.56 -> 10.67.84.48 DNS Standard query A n
o-sense-1.cisco.com
2015-05-09 22:55:46.042295 10.67.84.48 -> 10.67.84.56 DNS Standard query res
ponse A 64.104.196.20
```

Oplossing 2. Verwijder de DNS-lijst van het beheer VRF.

Voorbeeld:

```
vrf - contextbeheer
```

```
no ip name-server 10.67.84.48 10.67.84.45
```

- Uitschakelen van IP-domein

```
no ip domain-lookup
```

Opmerking: Er is een verbeteringsverzoek geopend voor woekering DNS-raadpleging voor NetH/Telnet uitschakelen.

[CSCur27501](#) raadpleging voor SSH/telnet uitschakelen met r-DNS