

Retard avant que l'invite du mot de passe apparaisse tandis que vous ouvrez une session par l'intermédiaire de SSH/Telnet

Contenu

[Introduction](#)

[Problème : Retard avant que l'invite du mot de passe apparaisse tandis que vous ouvrez une session par l'intermédiaire de SSH/Telnet](#)

[SSH à l'interface N5K mgmt0](#)

[Telnet à l'interface N5K mgmt0](#)

[Solution](#)

Introduction

Ce document décrit le retard avant que l'invite du mot de passe apparaisse tandis que vous ouvrez une session par l'intermédiaire de SSH/Telnet.

On observe généralement cette question quand vous tentez d'ouvrir une session par l'intermédiaire du SSH ou du telnet à l'interface mgmt0 sur un Nexus 5K/6K.

Après que vous écrivez l'user-id, ce texte est affiché et il y a un plus long retard comme prévu, avant que l'invite du mot de passe apparaisse.

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

Problème : Retard avant que l'invite du mot de passe apparaisse tandis que vous ouvrez une session par l'intermédiaire de SSH/Telnet

Le problème se produit en raison de la consultation inverse de DN.

Par défaut, l'ip domain-lookup est activé sur le Nexus et si une liste de serveur DNS (ip name-server) est configurée sous la Gestion de VRF puis le commutateur exécutera une consultation inverse de DN de l'adresse IP source de l'utilisateur toutes les fois qu'ils se connectent au port mgmt0 par l'intermédiaire du SSH ou du telnet.

Une consultation inverse de DN est destinée pour que des raisons de sécurité vérifient que l'adresse IP source est légitime et d'empêchent l'usurpation d'adresse IP.

Voici un exemple où nous avons utilisé un serveur DNS 10.67.84.45

Le serveur DNS dans ce cas n'a pas une entrée pour l'adresse IP source du client et elle ne fournit pas une réponse. Ceci a comme conséquence le commutateur de Nexus exécutant de plusieurs requêtes, car le serveur ne renvoie pas un résultat par conséquent où ceci entraîne le retard.

```
ip domain-lookup
```

```
vrf context management
```

```
ip name-server 10.67.84.45
```

De cette sortie des **hôtes d'exposition**, vous pouvez voir qu'il y a un serveur DNS configuré pour la Gestion de VRF et que l'ip domain lookup est activé.

```
N5548P-2# show hosts
```

```
DNS lookup enabled
```

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

```
Host Address
```

Ces captures d'Ethanalzyer ont été prises après que le nom d'utilisateur soit écrit et vous attendez l'invite du mot de passe pour apparaître.

Il affiche que le commutateur de Nexus exécute deux consultations inverses de DN contre l'adresse IP source de l'utilisateur, 62.84.137.10

SSH à l'interface N5K mgmt0

```
Username: admin
```

```
<delay for several seconds>
```

```
N5548P-2# ethanalyzer 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
```

```
::
```

De même, quand vous ouvrez une session par l'intermédiaire du telnet, le commutateur exécute d'abord la consultation inverse ci-dessus de DN sur l'adresse IP source de l'utilisateur et affiche ensuite l'invite d'ouverture de connexion.

Telnet à l'interface N5K mgmt0

```
telnet to switch 10.67.84.56
```

```
N5548P-2# ethanalyzer 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

L'invite d'ouverture de connexion est alors affichée :

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

Solution

La solution 1. modifie la liste de serveurs DNS configurés sur le Nexus, de sorte que le serveur DNS sensible soit consulté avant le serveur DNS nonsensible.

Si le Nexus reçoit un enregistrement DNS valide du serveur DNS local puis il ne consultera pas le deuxième serveur DNS dans la liste. Ceci réduit le retard.

Exemple :

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

Vous pouvez utiliser ces dernières commandes de vérifier la liste en cours de serveurs DNS où le serveur local apparaît d'abord dans la liste :

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

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

```
Host Address
```

Des ces la capture d'Ethanalyzer, d'abord l'IP à la recherche de noms est effectuée et une réponse est reçue.

Ceci est suivi par une consultation de l'adresse nom-à-IP où une réponse est reçue.

Dans ce cas, il n'y avait aucun retard apparent observé en ouvrant une session par l'intermédiaire du SSH ou du telnet.

```
N5548P-2# ethanalyzer 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
```

La solution 2. enlève les DN les répertorient du VRF de Gestion.

Exemple :

Gestion de vrf context

```
no ip name-server 10.67.84.48 10.67.84.45
• Ip domain lookup de débranchement
```

```
no ip domain-lookup
```

Remarque: Il y a une demande d'amélioration ouverte pour la consultation de DN d'inverse de débranchement pour le ssh/telnet.

Consultation de r-DN du débranchement [CSCur27501](#) pour SSH/Telnet