

Délai avant l'invite de mot de passe apparaît lorsque vous vous connectez via SSH/Telnet

Contenu

[Introduction](#)

[Problème : Délai avant que l'invite de mot de passe ne s'affiche lorsque vous vous connectez via SSH/Telnet](#)

[SSH à l'interface de gestion N5K](#)

[Établissez une connexion Telnet avec l'interface N5K mgmt0](#)

[Solution](#)

Introduction

Ce document décrit le délai avant l'affichage de l'invite de mot de passe pendant que vous vous connectez via SSH/Telnet.

Ce problème est généralement observé lorsque vous essayez de vous connecter via SSH ou Telnet à l'interface mgmt0 sur un Nexus 5K/6K.

Après avoir saisi l'ID utilisateur, ce texte s'affiche et le délai est plus long que prévu, avant que l'invite de mot de passe ne s'affiche.

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

Problème : Délai avant que l'invite de mot de passe ne s'affiche lorsque vous vous connectez via SSH/Telnet

Le problème se produit en raison de la recherche DNS inverse.

Par défaut, la recherche de domaine IP est activée sur le Nexus et si une liste de serveurs DNS (ip name-server) est configurée sous Gestion VRF, le commutateur effectue une recherche DNS inverse de l'adresse IP source de l'utilisateur chaque fois qu'il se connecte au port mgmt0 via SSH ou Telnet.

Une recherche DNS inversée est destinée à des fins de sécurité pour vérifier que l'adresse IP source est légitime et pour empêcher l'usurpation d'adresse IP.

Voici un exemple où nous avons utilisé un serveur DNS 10.67.84.45

Dans ce cas, le serveur DNS n'a pas d'entrée pour l'adresse IP source du client et ne fournit pas de réponse. Le commutateur Nexus exécute donc plusieurs requêtes, car le serveur ne retourne pas de résultat, ce qui entraîne le retard.

```
ip domain-lookup

vrf context management
  ip name-server 10.67.84.45
```

À partir de cette sortie de **show hosts**, vous pouvez voir qu'il y a un serveur DNS configuré pour la gestion VRF et que la recherche de domaine IP est activée.

```
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 la saisie du nom d'utilisateur et vous attendez l'affichage de l'invite du mot de passe.

Il indique que le commutateur Nexus effectue deux recherches DNS inversées par rapport à l'adresse IP source de l'utilisateur, 62.84.137.10

SSH à l'interface de gestion N5K

```
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
::
```

De même, lorsque vous vous connectez via Telnet, le commutateur effectue d'abord la recherche DNS inverse ci-dessus sur l'adresse IP source de l'utilisateur, puis affiche l'invite de connexion.

Établissez une connexion Telnet avec l'interface N5K mgmt0

```
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
```

L'invite de connexion s'affiche ensuite :

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

Solution

Solution 1. Modifiez la liste des serveurs DNS configurés sur le Nexus, de sorte que le serveur DNS réactif soit consulté avant le serveur DNS non réactif.

Si le Nexus reçoit un enregistrement DNS valide du serveur DNS local, il ne consultera pas le deuxième serveur DNS de la liste. Cela réduit le délai.

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 cette commande pour vérifier la liste actuelle des serveurs DNS où le serveur local apparaît en premier 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
```

À partir de cette capture Ethalyzer, la recherche du nom IP est effectuée et une réponse est reçue.

Cette opération est suivie d'une recherche d'adresse nom-adresse IP où une réponse est reçue.

Dans ce cas, aucun retard notable n'a été observé lors de la connexion via SSH ou 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
```

Solution 2. Supprimez la liste DNS du VRF de gestion.

Exemple :

gestion du contexte vrf

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

- Désactiver la recherche de domaine IP

```
no ip domain-lookup
```

Note: Une demande d'amélioration est ouverte pour désactiver la recherche DNS inversée pour SSH/Telnet.

[CSCur27501](#) Désactiver la recherche r-DNS pour SSH/Telnet