通過SSH/Telnet登入時，出現密碼提示前延遲

目錄

簡介

本檔案介紹您透過SSH/Telnet登入時密碼提示出現之前的延遲。

當您嘗試通過SSH或Telnet登入到Nexus 5K/6K上的mgmt0介面時，通常會出現此問題。

輸入使用者ID後，將顯示此文本，並且出現密碼提示之前會有較長的延遲。

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

問題：通過SSH/Telnet登入時，出現密碼提示前延遲

發生此問題的原因是反向DNS查詢。

預設情況下，在Nexus上啟用ip domain-lookup，如果在VRF管理下配置了DNS伺服器清單(ip name-server)，則交換機將在使用者通過SSH或Telnet連線到mgmt0埠時對其源IP地址執行反向DNS查詢。

反向DNS查詢用於安全目的，以驗證源IP地址是否合法並防止IP欺騙。

以下是使用DNS伺服器10.67.84.45的範例

在這種情況下，DNS伺服器沒有客戶端的源IP地址條目，並且它不提供響應。這會導致Nexus交換機執行多個查詢，因為伺服器不返回結果，因此會導致延遲。

```
ip domain-lookup

vrf context management
  ip name-server 10.67.84.45
```

從**show hosts**的輸出中，您可以看到已為VRF管理配置了DNS伺服器，且已啟用IP域查詢。

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

```
Name servers for vrf:management is  10.67.84.45

Host                    Address
```

這些Ethanalzyer捕獲是在輸入使用者名稱後捕獲的，您等待出現密碼提示。

它顯示Nexus交換機對使用者的源IP地址62.84.137.10執行兩次反向DNS查詢

通過SSH連線到N5K mgmt0介面

```
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
:
```

同樣，當您通過Telnet登入時，交換機首先會對使用者的源IP地址執行上述反向DNS查詢，然後顯示登入提示。

Telnet至N5K mgmt0介面

```
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
```

然後會顯示登入提示：

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

解決方案

解決方案1.修改Nexus上配置的DNS伺服器清單，以便在無響應DNS伺服器之前查詢響應的DNS伺服器。

如果Nexus從本地DNS伺服器收到有效的DNS記錄，則不會諮詢清單中的第二個DNS伺服器。這會

減少延遲。

範例：

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

可以使用以下命令驗證本地伺服器在清單中最先出現的DNS伺服器的當前清單：

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

Name servers for vrf:management is  10.67.84.48 10.67.84.45

Host                    Address
```

從這些Ethanalyzer捕獲中，首先執行IP到名稱查詢，然後收到響應。

然後是收到響應的名稱到IP地址查詢。

在這種情況下，通過SSH或Telnet登入時未觀察到明顯的延遲。

```
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
```

解決方案2.從管理VRF中刪除DNS清單。

範例：

vrf內容管理

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

- 禁用IP域查詢

```
no ip domain-lookup
```

附註：有一個增強請求開啟，用於禁用Ssh/Telnet的反向DNS查詢。

CSCur27501禁用SSH/Telnet的r-DNS查詢