

迪莱，在密码提示出现前，当您通过SSH/Telnet时登陆

目录

[简介](#)

[问题：迪莱，在密码提示出现前，当您通过SSH/Telnet时登陆](#)

[对N5K mgmt0接口的SSH](#)

[对N5K mgmt0接口的Telnet](#)

[解决方案](#)

简介

本文描述延迟，在密码提示出现前，当您通过SSH/Telnet时登陆。

当您尝试通过SSH登陆或远程登录到在连结5K/6K时的mgmt0接口此问题通常被观察。

在您输入用户ID后，此文本显示，并且有长延迟正如所料，在密码提示出现前。

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

问题：迪莱，在密码提示出现前，当您通过SSH/Telnet时登陆

问题发生由于逆向DNS查找。

默认情况下，ip domain-lookup在连结启用，并且，如果DNS服务器列表(ip name-server)配置在VRF管理下然后交换机将执行用户的源IP地址的逆向DNS查找，每当他们连接到mgmt0端口通过SSH或远程登录。

逆向DNS查找用于安全性目的打算验证源IP地址合法和防止IP伪装。

这是示例我们使用了一个DNS服务器10.67.84.45的地方

DNS服务器在这种情况下没有客户端的源IP地址的一个条目，并且不提供一答复。这导致连结交换机执行的多查询，因为这导致延迟的服务器不返回结果因此。

```
ip domain-lookup

vrf context management
  ip name-server 10.67.84.45
```

从**show hosts**此输出，您能看到有为VRF管理配置的DNS服务器，并且IP域名查找启用。

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

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

```
Host Address
```

这些Ethanalyzer捕获被采取了，在用户名输入后，并且您等待密码提示出现。

它显示连结交换机执行两逆向DNS查找用户的源IP地址，62.84.137.10

对N5K mgmt0接口的SSH

```
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
::
```

同样地，当您通过Telnet时登陆，交换机首先执行在用户的源IP地址的上述逆向DNS查找然后显示登录提示。

对N5K mgmt0接口的Telnet

```
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
登录提示然后显示：

Nexus 5000 Switch
login: admin
Password:
```

解决方案

解决方案1.修改在连结配置的DNS服务器列表，因此响应能力的DNS服务器在无响应的DNS服务器前参见。

如果连结接收从本地DNS服务器的一个有效DNS记录那么不会参见在列表的第二个DNS服务器。这降低延时。

示例：

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

您能使用这些命令验证本地服务器首先在列表出现DNS服务器的当前列表：

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

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

```
Host Address
```

从这些Ethanalyzer捕获，对名称查找的IP首先执行，并且答复接收。

这由答复接收的一个名称到IP地址查找跟随。

在这种情况下，当登陆通过SSH或Telnet时，没有被观察的明显的延迟。

```
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
```

DNS从管理VRF列出的解决方案2.删除。

示例：

vrf context管理

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

- 禁用IP域名查找

```
no ip domain-lookup
```

注意：有增强请求开放为SSH的/Telnet禁用逆向DNS查找。

[CSCur27501](#)禁用SSH/Telnet的r DNS查找