通过SSH/Telnet登录时出现Delay Before Password Prompt（密码提示出现前延迟）

目录

[简介](#)
[问题：通过SSH/Telnet登录时出现Delay before Password Prompt（密码提示出现前的延迟）](#)
[SSH到N5K mgmt0接口](#)
[Telnet至N5K mgmt0接口](#)
[解决方案](#)

简介

本文档介绍在您通过SSH/Telnet登录时出现口令提示前的延迟。

当您尝试通过SSH或Telnet登录Nexus 5K/6K上的mgmt0接口时，通常会发现此问题。

输入用户ID后，此文本将显示，并且在出现密码提示之前，会出现较长的延迟。

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

问题：通过SSH/Telnet登录时出现Delay before Password Prompt（密码提示出现前的延迟）

由于反向DNS查找，因此出现问题。

默认情况下，Nexus上启用ip domain-lookup，如果在VRF Management下配置DNS服务器列表(ip name-server)，则交换机将在用户通过SSH或Telnet连接到mgmt0端口时对其源IP地址执行反向DNS查找。

反向DNS查找旨在确保安全，以验证源IP地址是否合法并防止IP欺骗。

以下是我们使用DNS服务器10.67.84.45的示例

在这种情况下，DNS服务器没有客户端源IP地址的条目，也不提供响应。这会导致Nexus交换机执行多个查询，因为服务器不返回结果，因此这会导致延迟。

```
ip domain-lookup

vrf context management
  ip name-server 10.67.84.45
```

从**show hosts**的此输出中，您可以看到为VRF管理配置了DNS服务器，并且已启用IP域查找。

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

Name servers for vrf:management is  10.67.84.45

Host                    Address
```

这些Ethanalzyer捕获是在输入用户名并等待出现密码提示后捕获的。

它显示Nexus交换机对用户的源IP地址62.84.137.10执行两次反向DNS查找

SSH到N5K mgmt0接口

```
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，当您通过Telnet登录时，交换机首先对用户的源IP地址执行上述反向DNS查找，然后显示登录提示。

Telnet至N5K mgmt0接口

```
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
```

然后显示登录提示：

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

解决方案

解决方案1.修改Nexus上配置的DNS服务器列表，以便在无响应DNS服务器之前咨询响应DNS服务

器。

如果Nexus从本地DNS服务器收到有效的DNS记录，则它不会查询列表中的第二个DNS服务器。这可以减少延迟。

示例：

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

您可以使用以下命令验证当前DNS服务器列表，其中本地服务器首先出现在列表中：

```
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捕获中，首先执行IP到名称查找并收到响应。

随后是收到响应的名称到IP地址查找。

在这种情况下，通过SSH或Telnet登录时未观察到明显延迟。

```
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
```

解决方案2.从管理VRF中删除DNS列表。

示例：

VRF环境管理

```
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：已打开一个增强请求，以禁用SSh/Telnet的反向DNS查找。

CSCur27501禁用SSH/Telnet的r-DNS查找