Prime基礎架構封包擷取程式

目錄

簡介

本檔案將說明如何使用**tcpdump** CLI命令從Cisco Prime Infrastructure(PI)伺服器擷取所需的封包。

使用tcpdump命令

本節提供的範例將說明使用**tcpdump**命令的方式。

```
nms-pi/admin# tech dumptcp ?
<0-3> Gigabit Ethernet interface number
```

show interface命令的輸出提供了有關當前使用的介面名稱和編號的準確資訊。

```
nms-pi/admin# tech dumptcp 0 ?
count Specify a max package count, default is continuous (no limit)
<cr> Carriage return.
```

> **附註**：您可以在上一命令中指定特定軟體包計數。如果沒有指定特定的軟體包計數，則無限制地運行連續捕獲。

```
nms-pi/admin# tech dumptcp 0 | ?
Output modifier commands:
begin Begin with line that matches
count Count the number of lines in the output
end End with line that matches
exclude Exclude lines that match
include Include lines that match
last Display last few lines of the output

nms-pi/admin# tech dumptcp 0 > test-capture.pcap
```

> **附註**：先儲存檔案，然後檢視檔案最為輕鬆。在此示例中，伺服器將檔案儲存在目錄結構的根目錄中。若要檢視檔案，請輸入**dir**指令。

將捕獲的檔案複製到外部位置

以下兩個範例說明將擷取檔案複製到伺服器以外的位置的方式：

- 在本範例中，擷取檔案被複製到IP位址為1.**2.3.4的FTP伺服器**：

```
copy disk:/test-capture.pcap ftp://1.2.3.4/
```

- 在本範例中，擷取檔案被複製到IP位址為**5.6.7.8的TFTP伺服器**：

```
copy disk:/test-capture.pcap tftp://5.6.7.8/
```

以根使用者身份捕獲資料包

如果您需要更精細的捕獲，請在以*admin*使用者身份登入後，以*root*使用者身份登入CLI。

```
test$ ssh admin@12.13.14.15
Password:
nms-pi/admin#
nms-pi/admin# root
Enter root password :
Starting root bash shell ...
ade # su -
[root@nms-pi~]#
```

根使用者捕獲示例

以下是根使用者捕獲的三個示例：

- 在本範例中，所有目的地為PI伺服器上連線埠**162**的封包都會擷取：

```
[root@nms-pi~]# tcpdump -i eth0 -s0 -n dst port 162
```

- 在此範例中，所有目的地為連線埠**9991**的封包都會擷取並寫入**/localdisk/ftp/**目錄中名為**test.pcap**的檔案：

```
[root@nms-pi~]# tcpdump -w /localdisk/ftp/test.pcap -s0 -n dst port 9991
```

- 在此範例中，擷取來源IP位址為**1.1.1.1的所有**封包：

```
[root@nms-pi~]# tcpdump -n src host 1.1.1.1
```