Prime Infrastructure パケット キャプチャ手順

内容

概要

このドキュメントでは、tcpdump CLI コマンドを使用して Cisco Prime Infrastructure (PI) サーバから目的のパケットをキャプチャする方法を説明します。

tcpdump コマンドの使用

ここでは、tcpdump コマンドの使用例を説明します。

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

show interface コマンドの出力に、現在使用中のインターフェイスの名前と番号に関する正確な情報が示されます。

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

> **注**：上記のコマンドでは、特定のパッケージの数を表示できます。特定のパッケージの数を表示しない場合、無制限の連続キャプチャが実行されます。

```
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
```

> **注**：これは、ファイルを保存して確認するための最も簡単な方法です。この例では、サーバ

はディレクトリ構造のルートにファイルを保存します。ファイルを表示するには、**dir コマンドを入力します。**

キャプチャされたファイルの外部ロケーションへのコピー

キャプチャしたファイルをサーバ外部のロケーションにコピーする例を 2 つ示します。

- 以下の例では、キャプチャ ファイルは IP アドレス **1.2.3.4** が割り当てられた FTP サーバにコピーされます。

  ```
  copy disk:/test-capture.pcap ftp://1.2.3.4/
  ```
- 以下の例では、キャプチャ ファイルは IP アドレス 5.6.7.8 が割り当てられた TFTP サーバにコピーされます。

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

ルート ユーザとしてのパケットのキャプチャ

キャプチャの粒度を細かくする必要がある場合は、*管理者 ユーザとしてログインした後、ルート ユーザとして CLI にログインします。*

```
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~]#
```

ルート ユーザによるキャプチャの例

ここでは、ルート ユーザが行うキャプチャの例を 3 つ示します。

- 以下の例では、PI サーバ上のポート **162 宛てのすべてのパケットをキャプチャします。**

  ```
  [root@nms-pi~]# tcpdump -i eth0 -s0 -n dst port 162
  ```
- 次の例では、ポート**9991宛てのすべてのパケットがキャプチャさ**れ、test.pcapというファイルに書き込まれ、**/localdisk/ftp/ディレクトリに格納されます。**

  ```
  [root@nms-pi~]# tcpdump -w /localdisk/ftp/test.pcap -s0 -n dst port 9991
  ```
- 以下の例では、送信元 IP アドレスが **1.1.1.1 のパケットをキャプチャします。**

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