How to make tcpdump captures

Applies to VoipNow Professional, VoipNow 3, and VoipNow 3.5!

Every time you have to debug a call in order to identify the causes of abnormal behaviors, you need to make a traffic capture.

For this, you need tcpdump. Tcpdump is not installed by default. To install it, execute the following command on the server:

```
yum -y install tcpdump
```

Step-by-step guide

Possible solutions

In case the replication scenario is known, follow the steps below:

1. Start a capture using the following command.

   ```
   tcpdump -nni any -s 0 udp port 5050 or port 5060 -w /usr/local/voipnow/admin/htdocs/out.pcap
   ```

2. Place the call and, once you notice the problem, hang up.
3. Press CTRL+C.
4. Download out.pcap capture from you server, open it in Wireshark and try to identify the issues.

Rotate captures with a timestamp and a number limit

Tcpdump is able to rotate captures after a certain period of time. Assuming that you want to create an unlimited number of captures, in fact they are limited by the disk space, here is how things should unfold.

1. Execute the following command.

   ```
   tcpdump -Z root -i any -s65535 -G 3600 -vnn udp port 5050 or port 5060 -w /usr/local/voipnow/admin/htdocs
   /'output_%Y-%m-%d_%H:%M:%S.pcap'
   ```

2. The output of the above command will be a file named: output_2015-02-25_07:37:18.pcap.
3. The capture is automatically rotated according to the values specified in -G parameter. In this example, a new file is created every 3600 seconds; the only limit is the disk space available.
4. To limit the number of captures produced, insert the -W parameter where the number of the captures can be specified.

   ```
   tcpdump -Z root -i any -s65535 -G 3600 -vnn udp port 5050 or port 5060 -W 10 -w /usr/local/voipnow/admin
   /htdocs/'output_%Y-%m-%d_%H:%M:%S.pcap'
   ```

5. The command above produces 10 captures, as specified by the -W parameter. A new capture is created every 3600 seconds (the -G parameter). After 10 captures, the command will be automatically stopped.

Rotate capture by size and limit the number of captures

Tcpdump is also able to rotate captures by size. Assuming that you want to make a capture of 100MB max, here is how things should unfold:

1. Execute the following command.

   ```
   tcpdump -Z root -i any -s65535 -vnn udp port 5050 or port 5060 -C 100 -w /usr/local/voipnow/admin/htdocs
   /output
   ```

2. The output of the command will be a file called output. When this capture has reached the size limit specified by the -C parameter (100MB), a new file will be created (*output1*, *output2, output3, etc*). The only limit of this command is the disk space available.
3. To limit the number of captures produced, insert the -W parameter where the number of the captures can be specified.

   ```
   tcpdump -Z root -i any -s65535 -vnn udp port 5050 or port 5060 -C 100 -W 10 -w /usr/local/voipnow/admin
   /htdocs/output
   ```

4. In this case, only 10 files are created. Each file is 100MB large. After 10 captures, the command will be automatically stopped.

Related articles

- Troubleshooting fax issues
- How to decode SIP over TLS with Wireshark
- How to make tcpdump captures
- How to use Homer capture agents with VoipNow
- How to monitor VoipNow with Homer