

ESET Tech Center

Kennisbank > ESET Security Management Center > Using tcpdump on a Virtual Appliance

Using tcpdump on a Virtual Appliance

Steeff | ESET Nederland - 2019-08-21 - Comments (0) - ESET Security Management Center

When troubleshooting network related issues on an ESMC virtual appliance, tcpdump is the linux equivalent of wireshark.

To install tcpdump:

Enter the following command in the terminal of the appliance to install tcpdump:

```
yum install tcpdump
```

Confirm the installation with "y"

```
=====
Installing:
tcpdump          x86_64          14:4.9.2-3.e17          base          421 k
Transaction Summary
=====
Install 1 Package

Total download size: 421 k
Installed size: 1.0 M
Is this ok [y/d/N]: y
Downloading packages:
tcpdump-4.9.2-3.e17.x86_64.rpm          | 421 kB    00:10
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : 14:tcpdump-4.9.2-3.e17.x86_64          1/1
  Verifying  : 14:tcpdump-4.9.2-3.e17.x86_64          1/1

Installed:
tcpdump.x86_64 14:4.9.2-3.e17

Complete!
```

Use the following command to capture and save the packets in a file:

```
tcpdump -vv -w ESMCVAany.pcap -i any
```

Reproduce the issue, so it is captured in the tcpdump log.

To cancel the capture press:

```
Ctrl + c
```

To compress the output file:

```
tar -cvzf ESMCVAany.tar.gz ESMCVAany.pcap
```

Please send the compressed output file ESMCVAany.tar.gz to ESET Support.

Gerelateerde inhoud

- [How do I use ESET Log Collector?](#)
- [How do I use ESET Log Collector for macOS?](#)
- [Run the Info_get.command on a Linux machine and send the logs to ESET Technical Support](#)
- [How to create a Wireshark log](#)
- [How do I generate a memory dump manually?](#)
- [How to create a Process Dump / Memory Dump](#)