Network Tools for DevOps

Luciano Antonio Borguetti Faustino

Agenda

- netstat and ss
- iptraf
- iftop
- nethogs
- tcpdump
- tcpflow
- ngrep
- ncat
- iperf
- mtr
- traceroute/tcptraceroute

netstat & ss

netstat : print network connections, routing tables, interface statistics, masquerade connections, and multicast memberships

ss : Another utility to investigate sockets

Use case

Display all sockets

```
netstat -na && ss -na
```

Network Statics

```
netstat -s && ss -s
```

Show internal TCP information

```
ss -i
```

Show socket memory usage

```
ss -m
```

Listen tcp sockets

```
netstat -nltp && ss -ntlp
```

iptraf

Interactive Colorful IP LAN Monitor

Use case

```
iptraf-ng
```

iftop

Display bandwidth usage on an interface by host

Use case

```
iftop -n
```

nethogs

Net top tool grouping bandwidth per process

Use case

```
nethogs enp2s0
```

tcpdump

Dump traffic on a network

Use case

Show traffic with filter host and port

```
tcpdump -i any host 192.168.50.10 and port 80
```

Write traffic in output file

```
tcpdump -i enp2s0 -s0 -w /tmp/tcpdump-output.cap
```

tcpflow

Network traffic recorder

Use case

```
tcpflow -s -r file.pcap
```

Or

```
tcpflow -i interface -a -o outdir port 80
```

ngrep

Network grep

Use case

```
ngrep -W byline -t '^(GET|POST) ' 'tcp and dst port 80'
```

Or

```
ngrep -d lo -W byline -t 'USER' 'tcp and dst port 1234'
```

ncat

The nc (or netcat) utility is used for just about anything under the sun involving TCP, UDP, or UNIX-domain sockets.

It can open TCP connections, send UDP packets, listen on arbitrary TCP and UDP ports, do port scanning, etc.

Use case

- Port scanning

```
nc -z -v www.goole.com 80 443
```

- Data Transfer

```
nc -l 1234 > filename.out
nc host.example.com 1234 < filename.in

nc -l 1234 | tar -xpf -
tar -cf - * | nc host.example.com 1234
```

- Remote shell

```
rm -f /tmp/f; mkfifo /tmp/f
cat /tmp/f | /bin/sh -i 2>&1 | nc -l 127.0.0.1 1234 > /tmp/f
```

- Generate huge amounts of useless network data

```
yes AAAAAAAAAAAAAAAAAAAA | nc -v -v -l -p 1234 > /dev/null
yes BBBBBBBBBBBBBBBBBBBB | nc host.example.com 1234 > /dev/null
```

iperf

Perform network throughput tests

Use case

```
iperf -s

iperc -c host.example.com
```

mtr

A network diagnostic tool

Use case

```
mtr www.google.com
```

traceroute/tcptraceroute

print the route packets trace to network host

Use case

```
traceroute www.google.com
```

Or

```
tcptraceroute www.google.com 80
```

BONUS

tcpslice - Extract pieces of and/or merge together tcpdump files
lsof - List open files
vnstat - A console - based network traffic monitor
wireshark - Interactively dump and analyze network traffic
nmap - Network exploration tool and security / port scanner

Others rulez tools :-)

htop - Interactive process viewer
perf - Performance analysis tools for Linux
mpstat - Report processors related statistics.
vmstat - Reports information about processes, memory, paging, block IO, traps, disks and cpu activity.
pmap - The pmap command reports the memory map of a process or processes.
strace - Trace system calls and signals.
iotop - simple top - like I/O monitor
ncdu - NCurses Disk Usage

Thank you

Luciano Antonio Borguetti Faustino
lucianoborguetti@gmail.com (mailto:lucianoborguetti@gmail.com)
https://github.com/lborguetti (https://github.com/lborguetti)
@lborguetti (http://twitter.com/lborguetti)