Lab – Monitoring Linux Performance

Overview

In this lab, you will learn to monitor Linux process, memory, and networking. Managing performance on Linux systems can be made easier with a few commands. Managing performance on Linux hosts is often seen as a black art. Many system administrators rarely venture under the hood of their Linux machine, but Linux comes with plenty of built-in monitoring tools to make the job easier.

Most of these tools and commands work with any flavor of Linux.

Requirements

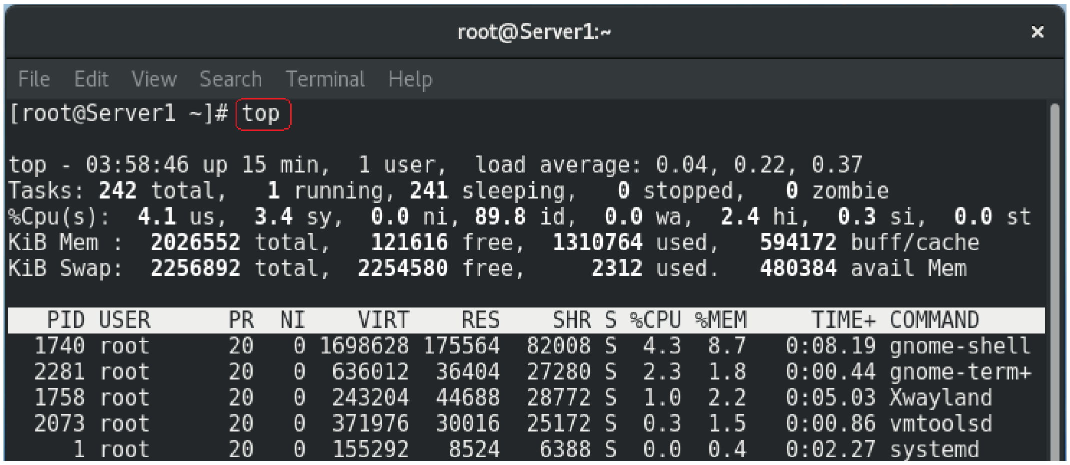
A virtual install of Linux server or workstation.

Start the Lab

Top

The Linux Top command is a performance monitoring program which is frequently used by many system administrators to monitor Linux performance, and it is available under many Linux/Unix like operating systems. The top command used to display all the running and active real-time processes using an ordered list and updates in real time. It displays CPU usage, Memory usage, Swap Memory, Cache Size, Buffer Size, Process PID, User, Commands and much more.

At the terminal type: `top`

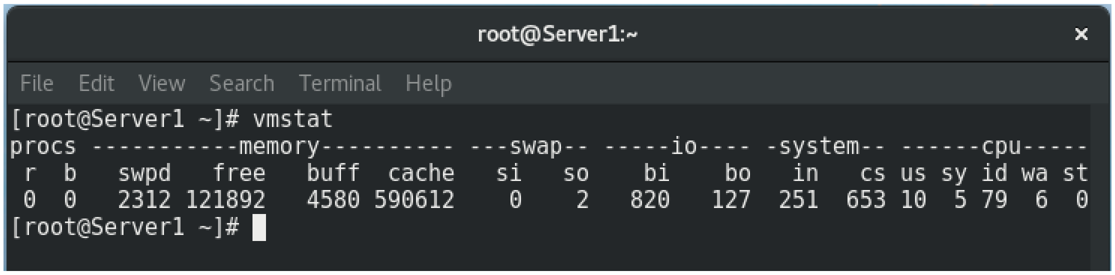


```
[root@Server1 ~]# top

top - 03:58:46 up 15 min,  1 user,  load average: 0.04, 0.22, 0.37
Tasks: 242 total,   1 running, 241 sleeping,   0 stopped,   0 zombie
%Cpu(s):  4.1 us,  3.4 sy,  0.0 ni, 89.8 id,  0.0 wa,  2.4 hi,  0.3 si,  0.0 st
KiB Mem :  2026552 total,   121616 free,  1310764 used,   594172 buff/cache
KiB Swap:  2256892 total,  2254580 free,     2312 used.   480384 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S %CPU %MEM     TIME+ COMMAND
 1740 root      20   0 1698628 175564  82008 S  4.3  8.7   0:08.19 gnome-shell
 2281 root      20   0  636012  36404  27280 S  2.3  1.8   0:00.44 gnome-term+
 1758 root      20   0  243204  44688  28772 S  1.0  2.2   0:05.03 Xwayland
 2073 root      20   0  371976  30016  25172 S  0.3  1.5   0:00.86 vmtoolsd
    1 root      20   0  155292   8524   6388 S  0.0  0.4   0:02.27 systemd
```

VmStat – Virtual Memory Statistics

The Linux VmStat command is used to display statistics of virtual memory, kernel threads, disks, system processes, I/O blocks, interrupts, CPU activity and much more.

At the terminal type: `vmstat`



```
[root@Server1 ~]# vmstat
procs -----------memory---------- ---swap-- -----io---- -system-- ------cpu-----
 r  b   swpd   free   buff  cache   si   so    bi    bo   in   cs us sy id wa st
 0  0   2312 121892   4580 590612    0    2   820   127  251  653 10  5 79  6  0
[root@Server1 ~]#
```

Lsof – List Open Files

The Lsof command is used with Linux/Unix like systems that are used to display a list of all the open files and their processes. The open files included are disk files, network sockets, pipes, devices, and processes. One of the main reason for using this command is when a disk cannot be unmounted and displays the error that files are being used or opened. With this command, you can easily identify which files are in use.

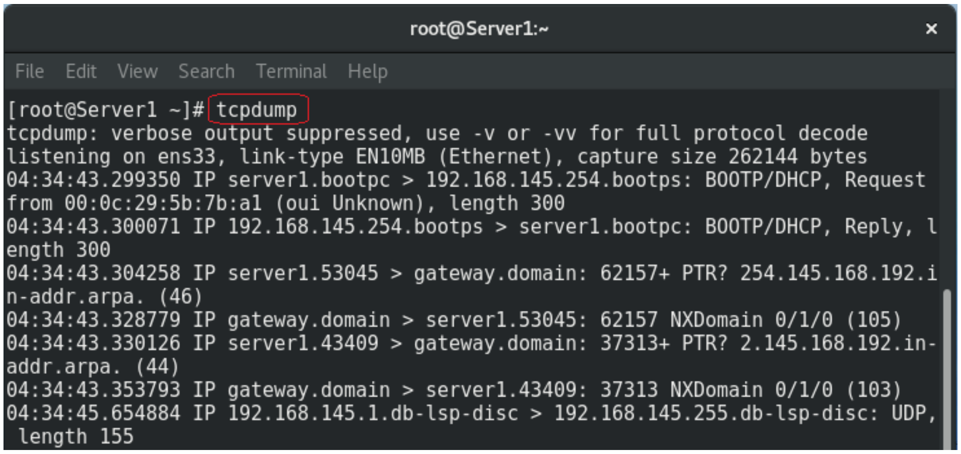
At the terminal type: `lsof` or to help parse through the information much easier. Use the pipe character | along with the more command to list the results one page at a time.

```
lsof | more
```

Tcpdump – Network Packet Analyzer

Tcpdump one of the most widely used command-line network packet analyzer or packets sniffer program used to capture or filter TCP/IP packets received or transferred on a specific interface over a network. Tcpdump is available in nearly all major Linux distributions.

At the terminal type: `tcpdump`



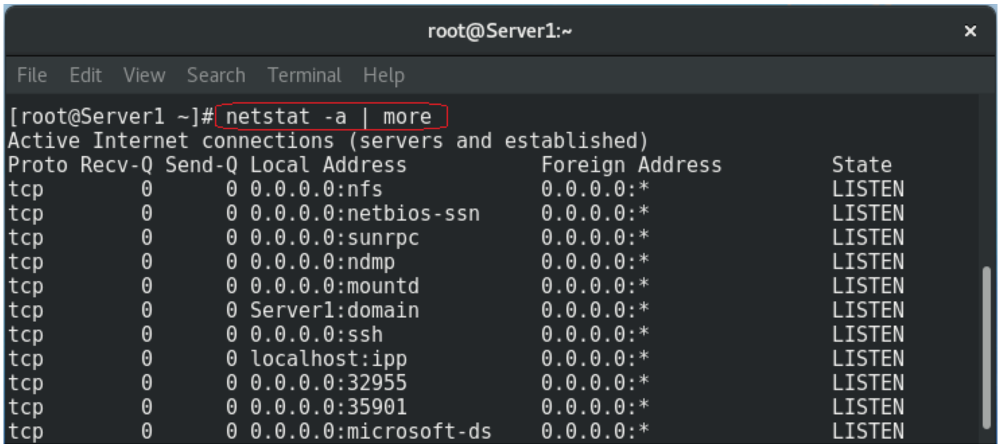
```
[root@Server1 ~]# tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ens33, link-type EN10MB (Ethernet), capture size 262144 bytes
04:34:43.299350 IP server1.bootpc > 192.168.145.254.bootps: BOOTP/DHCP, Request
from 00:0c:29:5b:7b:a1 (oui Unknown), length 300
04:34:43.300071 IP 192.168.145.254.bootps > server1.bootpc: BOOTP/DHCP, Reply, l
ength 300
04:34:43.304258 IP server1.53045 > gateway.domain: 62157+ PTR? 254.145.168.192.i
n-addr.arpa. (46)
04:34:43.328779 IP gateway.domain > server1.53045: 62157 NXDomain 0/1/0 (105)
04:34:43.330126 IP server1.43409 > gateway.domain: 37313+ PTR? 2.145.168.192.in-
addr.arpa. (44)
04:34:43.353793 IP gateway.domain > server1.43409: 37313 NXDomain 0/1/0 (103)
04:34:45.654884 IP 192.168.145.1.db-lsp-disc > 192.168.145.255.db-lsp-disc: UDP,
 length 155
```

Netstat – Network Statistics

Netstat is a command line tool for monitoring incoming and outgoing network packets statistics as well as interface statistics. It is a very useful tool for every system administrator to monitor network performance and troubleshoot network related problems.

Listing all ports (both TCP and UDP) using `netstat -a` and parsing through the results one page or one line at a time the `| more` command.

```
netstat -a | more
```



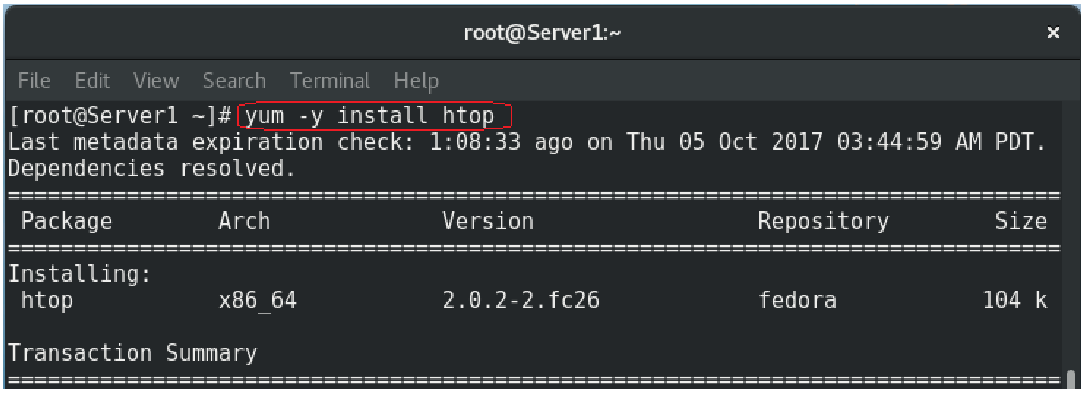
```
[root@Server1 ~]# netstat -a | more
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:nfs             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:netbios-ssn     0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:sunrpc          0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:ndmp            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:mountd          0.0.0.0:*               LISTEN
tcp        0      0 Server1:domain          0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:ssh             0.0.0.0:*               LISTEN
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:32955           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:35901           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:microsoft-ds    0.0.0.0:*               LISTEN
```

Htop – Linux Process Monitoring

Htop is a much advanced interactive and real-time Linux process monitoring tool. This is much similar to Linux top command, but it has some rich features like user-friendly interface to manage the process, shortcut keys, vertical and horizontal view of the processes and much more. Htop is a third party tool and doesn't include in Linux systems; you need to install it using YUM package manager tool. For more information on installation read our article below.

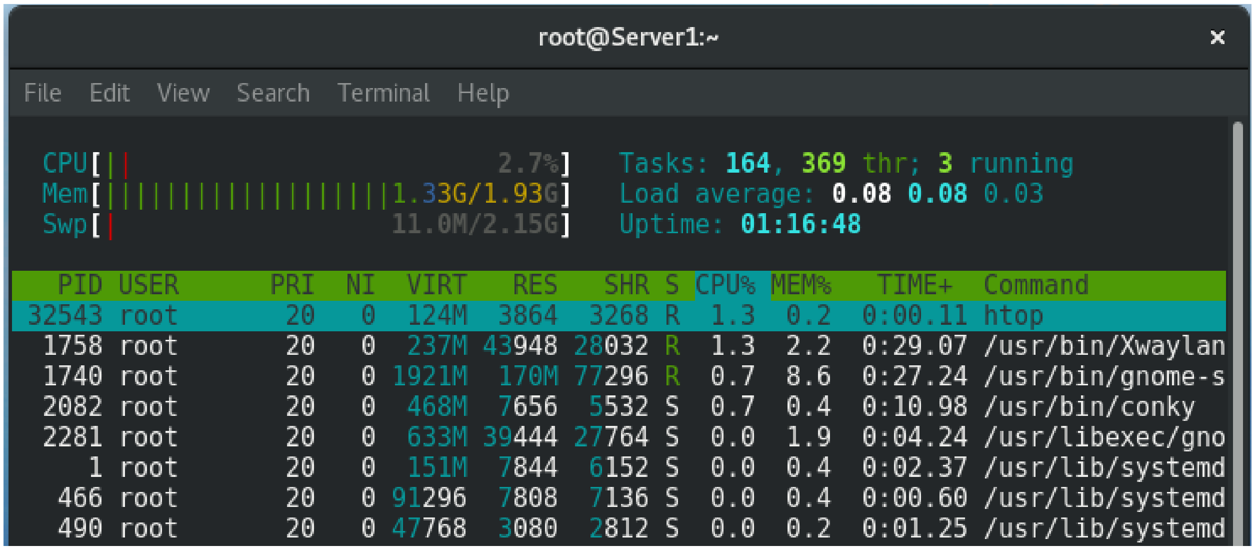
To install htop, use the yum command.

```
yum -y install htop
```



```
[root@Server1 ~]# yum -y install htop
Last metadata expiration check: 1:08:33 ago on Thu 05 Oct 2017 03:44:59 AM PDT.
Dependencies resolved.
================================================================================
 Package          Arch              Version                  Repository    Size
================================================================================
Installing:
 htop             x86_64            2.0.2-2.fc26             fedora       104 k

Transaction Summary
================================================================================
```

Once the package has installed, at the terminal type: `htop`



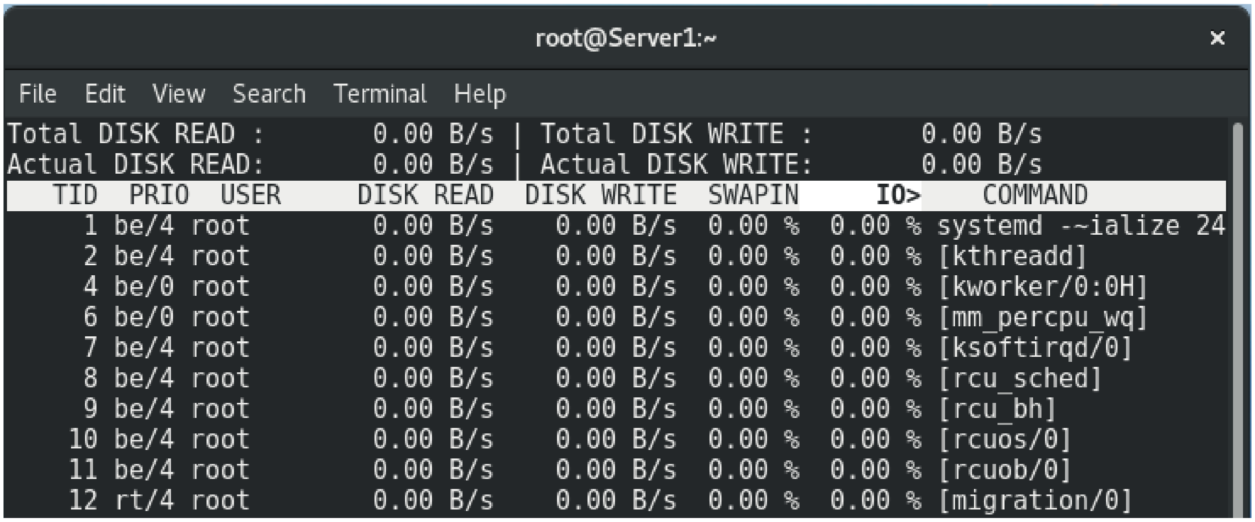
```
  CPU[||                          2.7%]   Tasks: 164, 369 thr; 3 running
  Mem[|||||||||||||||||||1.33G/1.93G]   Load average: 0.08 0.08 0.03
  Swp[|                       11.0M/2.15G]   Uptime: 01:16:48

  PID USER      PRI  NI  VIRT   RES   SHR S CPU% MEM%   TIME+  Command
32543 root       20   0  124M  3864  3268 R  1.3  0.2  0:00.11 htop
 1758 root       20   0  237M 43948 28032 R  1.3  2.2  0:29.07 /usr/bin/Xwaylan
 1740 root       20   0 1921M  170M 77296 R  0.7  8.6  0:27.24 /usr/bin/gnome-s
 2082 root       20   0  468M  7656  5532 S  0.7  0.4  0:10.98 /usr/bin/conky
 2281 root       20   0  633M 39444 27764 S  0.0  1.9  0:04.24 /usr/libexec/gno
    1 root       20   0  151M  7844  6152 S  0.0  0.4  0:02.37 /usr/lib/systemd
  466 root       20   0 91296  7808  7136 S  0.0  0.4  0:00.60 /usr/lib/systemd
  490 root       20   0 47768  3080  2812 S  0.0  0.2  0:01.25 /usr/lib/systemd
```

iotop – Monitor Linux Disk I/O

Iotop is also much like the top and Htop program, but iotop has an accounting function that monitors and displays real-time Disk I/O and processes. This tool is useful for finding the exact process, and high used disk read/writes of that process.

This program must also be installed using the yum command.

```
yum -y install iotop
```



```
Total DISK READ :       0.00 B/s | Total DISK WRITE :       0.00 B/s
Actual DISK READ:       0.00 B/s | Actual DISK WRITE:       0.00 B/s
   TID  PRIO  USER     DISK READ  DISK WRITE  SWAPIN     IO>    COMMAND
     1 be/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % systemd --~ialize 24
     2 be/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [kthreadd]
     4 be/0 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [kworker/0:0H]
     6 be/0 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [mm_percpu_wq]
     7 be/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [ksoftirqd/0]
     8 be/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [rcu_sched]
     9 be/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [rcu_bh]
    10 be/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [rcuos/0]
    11 be/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [rcuob/0]
    12 rt/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [migration/0]
```

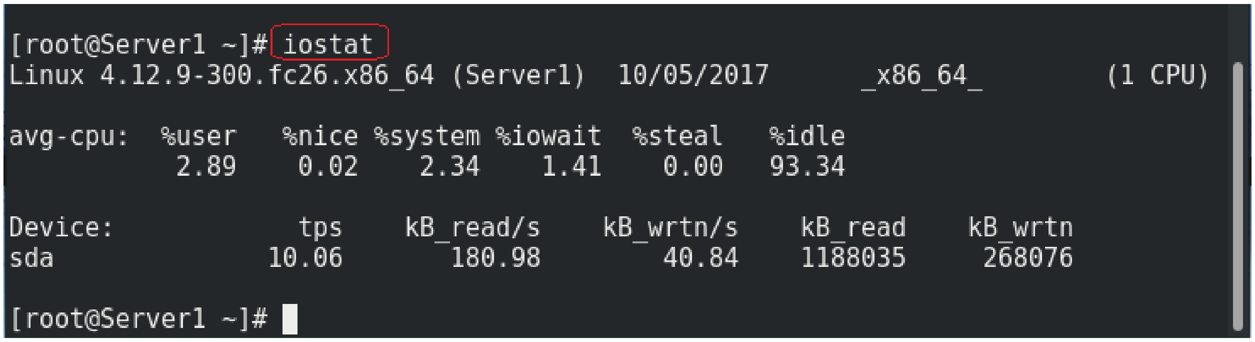
At the terminal type: `iotop`

Iostat – Input/Output Statistics

IoStat is a simple tool that will collect and show system input and output of storage device statistics. This tool is often used to trace storage device performance issues including devices, local disks, and remote disks such as NFS.

At the terminal type: `iostat`

Agree to allow the server to0 install the sysstat program to gain access to the iostat command.



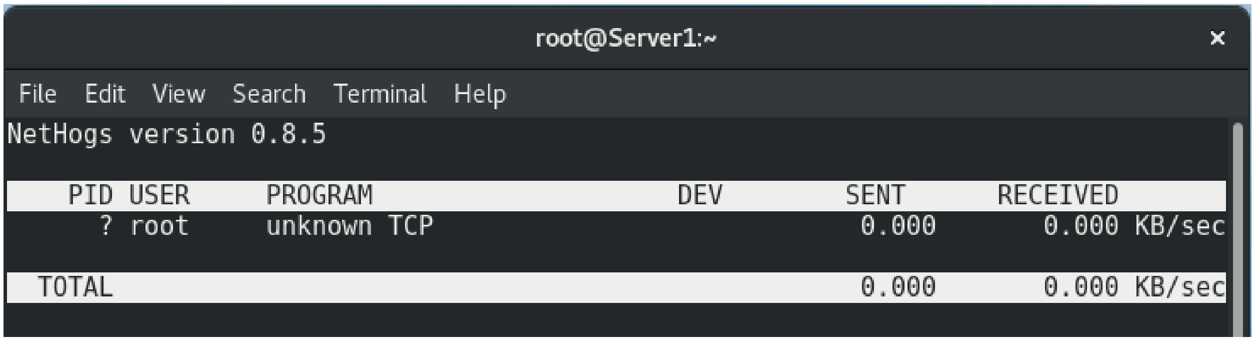
```
[root@Server1 ~]# iostat
Linux 4.12.9-300.fc26.x86_64 (Server1)  10/05/2017      _x86_64_        (1 CPU)

avg-cpu:  %user   %nice %system %iowait  %steal   %idle
           2.89    0.02    2.34    1.41    0.00   93.34

Device:            tps    kB_read/s    kB_wrtn/s    kB_read    kB_wrtn
sda              10.06       180.98        40.84    1188035     268076

[root@Server1 ~]# 
```

NetHogs – Monitor Per Process Network Bandwidth

NetHogs is an open source nice small program (like the Linux top command) that keeps a tab on each process of network activity on your system. It also keeps tracks of network traffic bandwidth usage

At the terminal type in: `nethogs`

Follow the prompts to install the program.



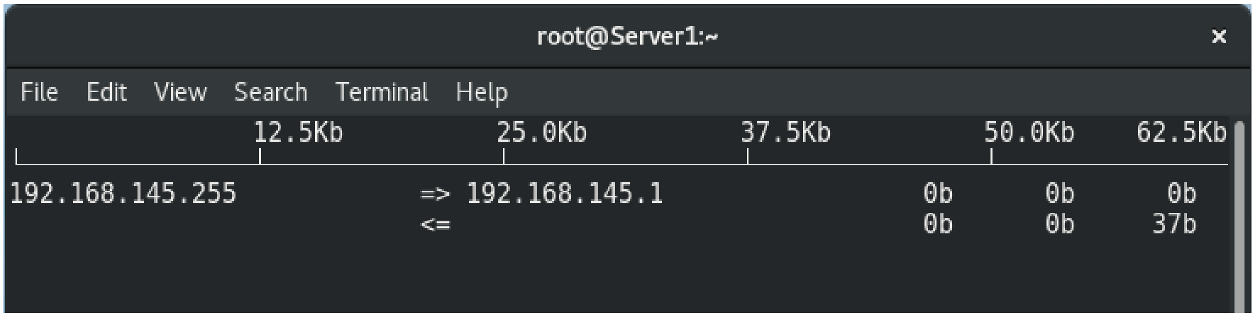
```
NetHogs version 0.8.5

    PID USER     PROGRAM                       DEV         SENT       RECEIVED
      ? root     unknown TCP                                0.000        0.000 KB/sec

  TOTAL                                                     0.000        0.000 KB/sec
```

iftop – Network Bandwidth Monitoring

iftop is another terminal-based free open source system monitoring utility that displays a frequently updated list of network bandwidth utilization (source and destination hosts) that passes through the network interface on your system. iftop does for network usage, what ‘top‘does for CPU usage. iftop is a ‘top ‘family tool that monitors a selected interface and displays a current bandwidth usage between two hosts.

At the terminal type: `iftop`

Follow the prompts to install the program. Allow the program to monitor your network interface, and in just a moment the results of the real-time monitoring will appear.



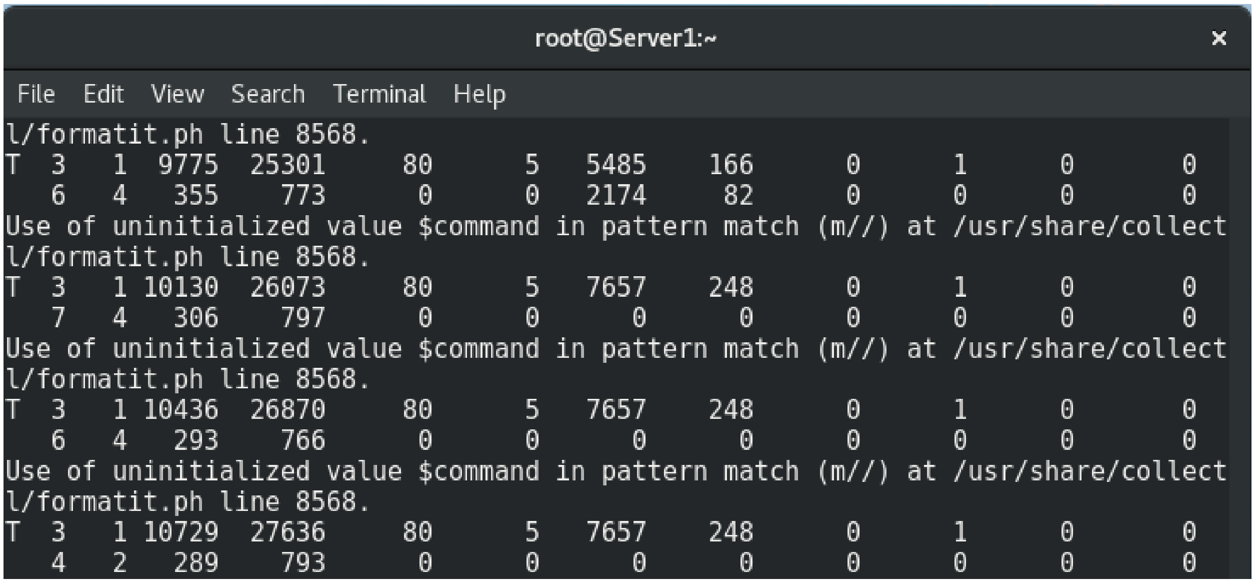
```
                12.5Kb          25.0Kb          37.5Kb          50.0Kb     62.5Kb
└───────────────┴───────────────┴───────────────┴───────────────┴──────────────
192.168.145.255            => 192.168.145.1                   0b       0b       0b
                           <=                                 0b       0b      37b
```

Collectl: All-in-One Performance Monitoring Tool

Collectl is a command line based utility, used to gather information about Linux system resources such as CPU usage, memory, network, processes, nfs, tcp, sockets and much more.

At the terminal type: `colltectl`

Follow the prompt to install.

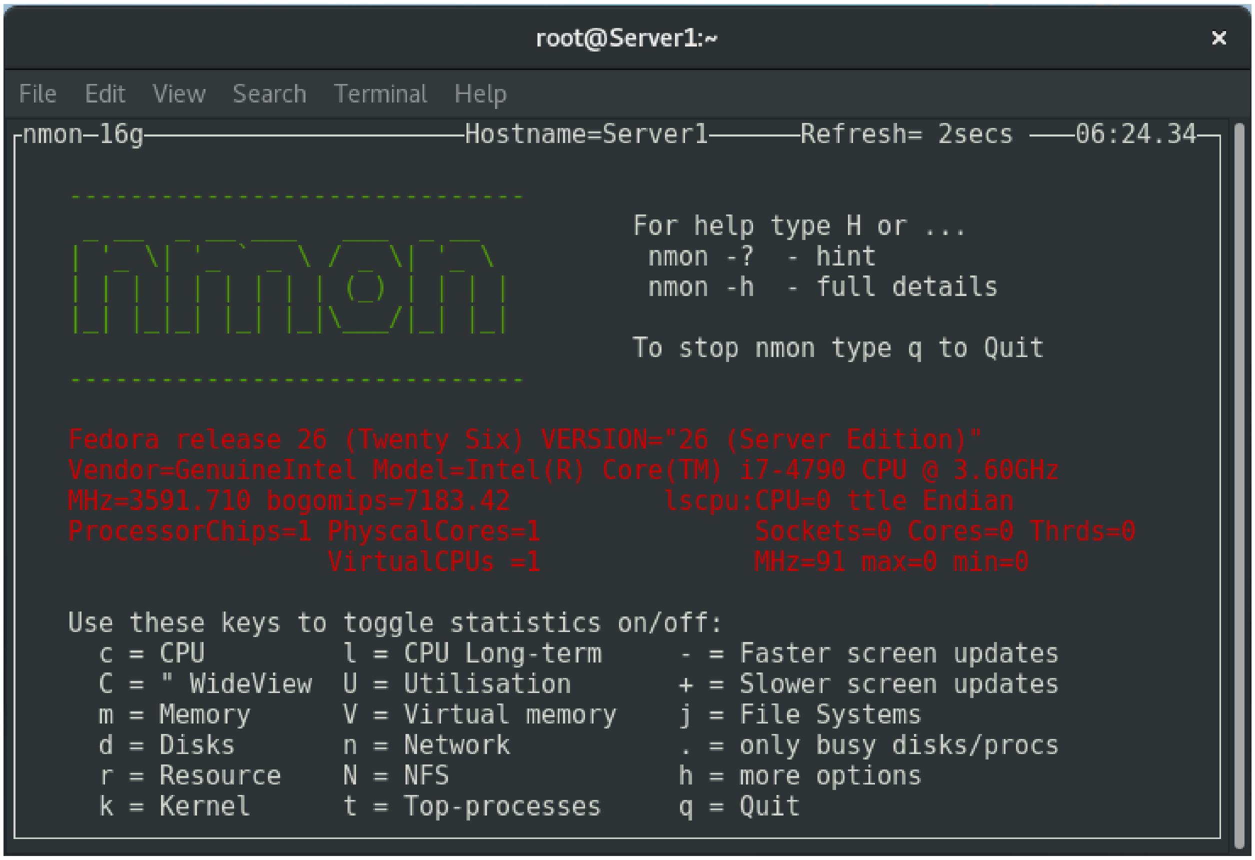


```
l/formatit.ph line 8568.
T  3   1  9775  25301     80      5   5485    166      0      1      0       0
   6   4   355    773      0      0   2174     82      0      0      0       0
Use of uninitialized value $command in pattern match (m//) at /usr/share/collect
l/formatit.ph line 8568.
T  3   1 10130  26073     80      5   7657    248      0      1      0       0
   7   4   306    797      0      0      0      0      0      0      0       0
Use of uninitialized value $command in pattern match (m//) at /usr/share/collect
l/formatit.ph line 8568.
T  3   1 10436  26870     80      5   7657    248      0      1      0       0
   6   4   293    766      0      0      0      0      0      0      0       0
Use of uninitialized value $command in pattern match (m//) at /usr/share/collect
l/formatit.ph line 8568.
T  3   1 10729  27636     80      5   7657    248      0      1      0       0
   4   2   289    793      0      0      0      0      0      0      0       0
```

Nmon: Monitor Linux Performance

Nmon (stands for Nigel's Performance Monitor) is used to monitor all Linux resources such as CPU, Memory, Disk Usage, Network, Top processes, NFS, Kernel and much more. This tool comes in two modes: Online Mode and Capture Mode.

The Online Mode is used for real-time monitoring and Capture Mode, is used to store the output to a CSV format for later processing.



```
┌nmon─16g───────────────────────Hostname=Server1──────Refresh= 2secs ───06:24.34─┐
│                                                                                   │
│   ------------------------------                                                  │
│    _ __  _ __ ___   ___  _ __          For help type H or ...                     │
│   | '_ \| '_ ` _ \ / _ \| '_ \          nmon -?  - hint                           │
│   | | | | | | | | | (_) | | | |         nmon -h  - full details                   │
│   |_| |_|_| |_| |_|\___/|_| |_|                                                   │
│                                        To stop nmon type q to Quit                │
│   ------------------------------                                                  │
│                                                                                   │
│   Fedora release 26 (Twenty Six) VERSION="26 (Server Edition)"                    │
│   Vendor=GenuineIntel Model=Intel(R) Core(TM) i7-4790 CPU @ 3.60GHz               │
│   MHz=3591.710 bogomips=7183.42          lscpu:CPU=0 ttle Endian                  │
│   ProcessorChips=1 PhyscalCores=1              Sockets=0 Cores=0 Thrds=0          │
│                    VirtualCPUs =1              MHz=91 max=0 min=0                 │
│                                                                                   │
│   Use these keys to toggle statistics on/off:                                     │
│     c = CPU         l = CPU Long-term     - = Faster screen updates               │
│     C = " WideView  U = Utilisation       + = Slower screen updates               │
│     m = Memory      V = Virtual memory    j = File Systems                        │
│     d = Disks       n = Network           . = only busy disks/procs               │
│     r = Resource    N = NFS               h = more options                        │
│     k = Kernel      t = Top-processes     q = Quit                                │
└───────────────────────────────────────────────────────────────────────────────────┘
```

End of the lab!