<https://opensource.com/life/16/2/open-source-tools-system-monitoring>

<https://www.tecmint.com/how-to-install-atop-to-monitor-logging-activity-of-linux-system-processes/>

<https://linux.die.net/man/1/atop> (reference used )

**atop** is an interactive monitor to view the load on a Linux system. It shows the occupation of the most critical hardware resources (from a performance point of view) on system level, i.e. cpu, memory, disk and network.

**Processor**

A busy percentage of 90% or higher is considered 'critical'.

**Disk**

A busy percentage of 70% or higher is considered 'critical'.

**Memory**

An occupation percentage of 90% is considered 'critical'.

**Network**

A busy percentage of 90% or higher for the load of an interface is considered 'critical'.

#!/bin/bash

cd /home/ubuntu18/Desktop/dataset\_linux

atop -d >> disk\_1.txt &

atop -s >> process\_1.txt &

atop -m >> memory\_1.txt &

atop -n >> network\_1.txt &

atop -d shows the disks activity on a system level. Disk activity is shown as amount of data that is being transferred by reads/writes.

**Disk activity**

|  |  |  |  |
| --- | --- | --- | --- |
| **Service profile:** Disk activity | | | |
| **ID** | **Feature** | **Type** | **Description** |
| 1 | PID | Number | Process identifier which is active in a Linux kernel |
| 2 | RDDSK | Number | Amount of data read from disk |
| 3 | WRDSK | Number | Amount of data written to disk |
| 4 | WCANCL | Number | Amount of data that was written but has been withdrawn |
| 5 | DSK | Number | Disk occupation percentage |
| 6 | CMD | String | process name which is active in a Linux kernel |
| 7 | label | Number | Tag normal and attack records, where 0 indicates normal and 1 indicates attacks |
| 8 | type | String | Tag attack categories, such as normal, DoS, DDoS and backdoor attacks, and normal records |

atop -s shows shows scheduling information for the main thread of each process. Also indicates how many processes are in state “**running**”.

**Process-scheduling activity**

|  |  |  |  |
| --- | --- | --- | --- |
| **Service profile:** Process-scheduling activity | | | |
| **ID** | **Feature** | **Type** | **Description** |
| 1 | PID | Number | Process identifier which is active in a Linux kernel |
| 2 | TRUN | Number | Number of threads in state 'running' (R) |
| 3 | TSLPI | Number | Number of threads in state 'interruptible sleeping' (S) |
| 4 | TSLPU | Number | Number of threads in state 'uninterruptible sleeping' (D) |
| 5 | POLI | String | Scheduling policy (normal timesharing, realtime round-robin, realtime fifo) |
| 6 | NICE | Number | Nice value which is the more or less static priority that can be given to a proces on a scale from -20 (high priority) to +19 (low priority) |
| 7 | PRI | Number | Priority which is the process' priority ranges from 0 (highest priority) to 139 (lowest priority). Priority 0 to 99 are used for realtime processes (fixed priority independent of their behavior) and priority 100 to 139 for timesharing processes (variable priority depending on their recent CPU consumption and the nice value). |
| 8 | RTPR | Number | Realtime priority which is according the POSIX standard. Value can be 0 for a timesharing process (policy 'norm', 'btch' or 'idle') or ranges from 1 (lowest) till 99 (highest) for a realtime process (policy 'rr' or 'fifo'). |
| 9 | CPUNR | Number | Current processor which is the identification of the CPU the main thread of the process is running on or has recently been running on |
| 10 | Status | Number | Status of a process, where the first position indicates if the process has been started during the last interval (the value N means 'new process'). |
| 11 | EXC | Number | Exit code of a terminated process (second position of column 'ST' is E) or the fatal signal number (second position of column 'ST' is S or C). |
| 12 | State | String | Current state of the main thread of the process: 'R' for running (currently processing or in the runqueue), 'S' for sleeping interruptible (wait for an event to occur), 'D' for sleeping non-interruptible, 'Z' for zombie (waiting to be synchronized with its parent process), 'T' for stopped (suspended or traced), 'W' for swapping, and 'E' (exit) for processes which have finished during the last interval. |
| 13 | CPU | Number | CPU time consumption of this process in system mode (kernel mode), usually due to system call handling. |
| 14 | CMD | String | The name of the process. This name can be surrounded by "less/greater than" signs ('<name>') which means that the process has finished during the last interval. |
| 15 | label | Number | Tag normal and attack records, where 0 indicates normal and 1 indicates attacks |
| 16 | type | String | Tag attack categories, such as normal, DoS, DDoS and backdoor attacks, and normal records |

atop -m shows memory related information about all running processes.

**Memory activity**

|  |  |  |  |
| --- | --- | --- | --- |
| **Service profile:** Memory activity | | | |
| **ID** | **Feature** | **Type** | **Description** |
| 1 | PID | Number | Process identifier which is active in a Linux kernel |
| 2 | MINFLT | Number | The number of page faults issued by this process that have been solved by reclaiming the requested memory page from the free list of pages. |
| 3 | MAJFLT | Number | The number of page faults issued by this process that have been solved by creating/loading the requested memory page. |
| 4 | VSTEXT | Number | The virtual memory size used by the shared text of this process. |
| 5 | VSIZE | Number | The total virtual memory usage consumed by this process (or user). |
| 6 | RSIZE | Number | The total resident memory usage consumed by this process (or user). |
| 7 | VGROW | Number | The amount of virtual memory that the process has grown during the last interval. |
| 8 | RGROW | Number | The amount of resident memory that the process has grown during the last interval. |
| 9 | MEM | Number | Memory occupation percentage |
| 10 | CMD | String | Process name |
| 11 | label | Number | Tag normal and attack records, where 0 indicates normal and 1 indicates attacks |
| 12 | type | String | Tag attack categories, such as normal, DoS, DDoS and backdoor attacks, and normal records |