Performance Troubleshooting

For Linux Operating System

TOP Command

Command on Server ➔ top

```
top - 11:24:32 up 5 min,  2 users,  load average: 0.09, 0.26, 0.14
Tasks: 217 total,   2 running, 215 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0.7 us,  0.3 sy,  0.0 ni, 99.0 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
KiB Mem :  3861496 total,  1637788 free,   754820 used,  1468888 buff/cache
KiB Swap:  4063228 total,  4063228 free,        0 used.  2789240 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S  %CPU %MEM     TIME+ COMMAND
 2605 sunil     20   0 3558700 239548  57204 R   1.6  6.2   0:13.07 gnome-shell
    9 root      20   0       0      0      0 S   0.3  0.0   0:01.07 rcu_sched
```

CPU Load Average:

Zombie Process:

%wa (imp): I/O status. Make sure this is close to zero. Higher the number critical will be the health.

%hi: H/W interrupts for CPU happening on server

%si: S/W interrupts for CPU happening on server

%st: This amount of stolen CPU from server to perform operation on shared virtual server to perform some operation.

SWAP Memory: It starts when Physical memory is full. Then Swapping will start moving unused memory blocks to SWAP Memory.

VMSTAT

Command on server → vmstat (e.g. vmstat 10 or vmstat 10 5)

```
[sunil@localhost ~]$ vmstat 5
procs -----------memory---------- ---swap-- -----io---- -system-- ------cpu-----
 r  b   swpd   free   buff  cache   si   so    bi    bo   in   cs us sy id wa st
 2  0      0 1617116   2152 1466612    0    0   218   207  193  208  2  2 95  0  0
 0  0      0 1617852   2152 1466608    0    0     0     0  204  318  3  1 96  0  0
 0  0      0 1617916   2152 1466608    0    0     0     0  196  325  3  1 96  0  0
 0  0      0 1617868   2152 1466608    0    0     0     0  122  202  2  0 98  0  0
 0  0      0 1617824   2152 1466608    0    0     0    30  230  361  3  1 95  0  0
 0  0      0 1615852   2152 1466644    0    0     0     2  609 1081  7  2 91  0  0
```

r: how many processes are waiting for CPU time. Higher the value of r , bad the server is behaving. It means issue with CPU

b: wait queue, higher the number of b , it means the issue with disk .

swapd: SWAP memory stats.

free: Free physical memory

buff: before I/O operation

Cache: Mapped by Kernel

si: Swap IN, once swap is started. Disk to Physical

so: Physical to SWAP

bi: Disk I/O, Blocks received from Disk to RAM

bo: Disk I/O , Blocks written to Disk

in: Number of interrupts per sec

cs: Context switches, CPU move from one process to other. Higher means issue with CPU.

IOSTAT

Command on Server → iostat

This provides information related to CPU, Disk

```
[sunil@localhost ~]$ iostat
Linux 3.10.0-957.27.2.el7.x86_64 (localhost.localdomain)        01/01/2020      _x86_64_        (2 CPU)

avg-cpu:  %user   %nice %system %iowait  %steal   %idle
           1.09    0.52    1.69    0.13    0.00   96.56

Device:            tps    kB_read/s    kB_wrtn/s    kB_read    kB_wrtn
scd0              0.01         0.44         0.00       1050          0
sda               8.58       302.07       287.49     720810     686030
dm-0              8.25       288.41       286.62     688211     683943
dm-1              0.04         1.03         0.00       2460          0
```

```
[sunil@localhost ~]$ iostat -x 2 5
Linux 3.10.0-957.27.2.el7.x86_64 (localhost.localdomain)        01/01/2020      _x86_64_        (2 CPU)

avg-cpu:  %user   %nice %system %iowait  %steal   %idle
           1.02    0.47    1.55    0.12    0.00   96.83

Device:         rrqm/s   wrqm/s     r/s     w/s    rkB/s    wkB/s avgrq-sz avgqu-sz   await r_await w_await  svctm  %util
scd0              0.00     0.00    0.01    0.00     0.40     0.00    72.41     0.00    2.21    2.21    0.00   1.86   0.00
sda               0.00     0.22    6.43    1.31   271.41   258.62   136.83     0.01    1.52    1.26    2.83   0.80   0.62
dm-0              0.00     0.00    5.92    1.53   259.13   257.83   138.73     0.01    1.75    1.34    3.32   0.82   0.61
dm-1              0.00     0.00    0.03    0.00     0.93     0.00    54.67     0.00    0.18    0.18    0.00   0.14   0.00
```

%iowait is important here

Gives details about disk read and write per sec.

SAR

Command on Server → sar

For current and historical details. Linux Package name - sysstat

Collective CPU usage

Memory, SWAP stats

I/O details on server

N/W stats

SAR (historical) on specific time with 10 min of range

SAR version → sar -V

sar 1 2 → output for every 1 sec for two times

sar -f /var/log/sa/sa10 → CPU stats of 10th (day or date) of the month .

sar -P ALL → Report of all cpu as well as all individual cores

sar -r → memory stats

sar -b → I/O activity (tps → transitions per sec, breads/sec → bytes read per sec)

sar -p -d → I/O Report of all individual disks

sar -w → CPU content (switch to different process)

sar -q → CPU load avg

sar -n → Network stats

sar -n DEV → Enough details for N/W devices for troubleshooting

```
[sunil@localhost ~]$ sar -n DEV
Linux 3.10.0-957.27.2.el7.x86_64 (localhost.localdomain)        01/01/2020      _x86_64_        (2 CPU)

11:19:12 AM       LINUX RESTART

11:20:01 AM     IFACE   rxpck/s   txpck/s    rxkB/s    txkB/s   rxcmp/s   txcmp/s  rxmcst/s
11:30:01 AM        lo      0.00      0.00      0.00      0.00      0.00      0.00      0.00
11:30:01 AM virbr0-nic      0.00      0.00      0.00      0.00      0.00      0.00      0.00
11:30:01 AM    virbr0      0.00      0.00      0.00      0.00      0.00      0.00      0.00
11:30:01 AM     ens33    738.26    279.72   1052.82     16.57      0.00      0.00      0.00
11:40:01 AM        lo      0.00      0.00      0.00      0.00      0.00      0.00      0.00
```

sar -f /var/log/sa/sa1 -s 00:11:00 -e 00:45:00 → Output of only with start and end time

LSOF

Command on Server → lsof

lsof +D /data → Number of processes opened for directory /data

lsof /var/log/messages → List the files used by any process

lsof -c ssh → Listing the files associated with process (such as sshd process)

lsof /data/ → processes running in specific mount point

lsof -u <user name> → Any specific user

lsof -p <pid> → For any specific process

FUSER

Command on server → fuser

This displays all the files used by a particular user

fuser -cu /data → This will show user accessing the file-system.

fuser -ck /data → Kill the users accessing the file-system

TCPDUMP

Command on Server → tcpdump

tcpdump -i eth0 → It will capture all the packets on the N/W interface until interrupted (ctrl +c).

tcpdump -c 10 -i eth0 → It will capture 10 packets

tcpdump -w <filename>.pcap -i eth0 → Write in file

tcpdump -r <filename>.pcap → Read from file

tcpdump -n -i eth0 → Output will be more readable format

tcpdump -n -i eth0 tcp → Captures only tcp packets

tcpdump -n -i eth0 port 80 → Captures specific to port

tcpdump -i eth0 -s 0 host <destination server IP> → This will capture packet between my server and destination server. So basically it captures packet communication between two servers.

Top Running process by CPU and Memory

High Memory processes:

ps -eo pid,ppid,cmd,%mem,%cpu –sort=-%mem | head

ps -eo pmem,pcpu,pidargs | tail -n +2 | sort -rnk 1 | head

ps -eo pmem,pcpu,vsize,pid,cmd | sort -k 1 -nr | head -10

ps axo ruser,%mem,comm,pid,euser | sor -nr | head -n 10

top -b -o +%MEM | head -n 50

-b output top in batch mode

-o for sorting process

-n number of lines (processes)

High CPU processes:

ps -eo pmem,pcpu,pidargs | tail -n +2 | sort -rnk 2 | head