* + top / htop: Real-time CPU usage and processes.
  + top - 
    Tasks: 124 total, 
    kworker/û:ûH-kb lockd 
    3:26, 
    1 user, 
    1 running, 115 
    UBUServer (SERVER -1) [Running] 
    load average: û.ûû, û. 
    ÛÛ, û.ûû 
    sleeping, 
    8 stopped, 
    ê zombie 
    Û.Û hi 
    a.û si, 
    û.û st 
    ZCpu(s) : 
    Mia Mem : 
    MiB SI-Llap: 
    Û.Û us, 
    3966.2 
    Û. 1 Su, 
    total, 
    total, 
    û.û ni, 
    3450.4 
    free, 
    free, 
    322 .û 
    SHR 
    s 
    1 
    8432 s 
    as 
    as 
    1 
    1 
    1 
    1 
    1 
    1 
    1 
    1 
    1 
    as 
    1 
    as 
    as 
    as 
    as 
    as 
    as 
    as 
    1 
    as 
    as 
    as 
    as 
    1 
    as 
    as 
    as 
    as 
    1 
    as 
    1 
    as 
    as 
    as 
    1 
    as 
    as 
    as 
    1 
    used, 
    used. 
    XCPLI 
    PID 
    1778 
    1 
    2 
    3 
    4 
    5 
    6 
    7 
    12 
    13 
    14 
    15 
    16 
    17 
    18 
    IB 
    20 
    21 
    22 
    23 
    24 
    26 
    27 
    28 
    29 
    30 
    32 
    33 
    34 
    35 
    36 
    38 
    3B 
    40 
    44 
    45 
    46 
    47 
    48 
    50 
    51 
    LISER 
    root 
    root 
    root 
    root 
    root 
    root 
    root 
    root 
    root 
    root 
    root 
    root 
    root 
    root 
    root 
    root 
    root 
    root 
    root 
    root 
    root 
    root 
    root 
    root 
    root 
    root 
    root 
    root 
    root 
    root 
    root 
    root 
    root 
    root 
    root 
    root 
    root 
    root 
    root 
    root 
    root 
    root 
    root 
    337.0 
    3644.2 
    XMEM 
    Û. 
    Û. 
    buff/cache 
    avail 
    Mem 
    TIME+ COMMAND 
    kworker/û:a-events 
    sgstemd 
    kthreadd 
    poo lease 
    20 
    20 
    20 
    rt 
    _51 
    -51 
    rt 
    20 
    20 
    -51 
    rt 
    _ 51 
    rt 
    20 
    29 
    20 
    20 
    25 
    NI 
    -a 
    -u 
    -29 
    -29 
    -29 
    -20 
    -20 
    -a 
    -a 
    -a 
    -20 
    -29 
    VIRT 
    21932 
    RES 
    llaaa 
    Û 
    Û 
    Û:ÛI. 
    Û:Ûû. 
    Û:Ûû. 
    Û:Ûû. 
    Û:Ûû. 
    Û:ÛÛ. 
    Û:ÛÛ. 
    Û:Ûû.ûÛ 
    Û:Ûû.ûÛ 
    Û:Ûû. 
    Û:Ûû. 
    Û:Ûû. 
    Û:Ûû. 
    Û:Ûû. 
    Û:aa. 
    Û:Ûû. 
    Û:Ûû. 
    Û:ÛÛ.ÛÛ 
    Û:ÛÛ.17 
    Û:ea.û2 
    Û:Ûû.û2 
    Û:Ûû. 
    Û:Ûû. 
    Û:ÛÛ. 
    Û:Ûû. 
    Û:Ûû. 
    Û:aa. 
    Û:Ûû. 
    Û:ÛÛ. 
    Û:ÛÛ. 
    Û:ÛÛ.ÛI 
    Û:ÛÛ.aa 
    Û:Ûû. 
    Û:Ûû. 
    Û:Ûû. 
    Û:aa. 
    Û:ÛÛ. 
    25 
    11 
    37 
    17 
    IB 
    31 
    47 
    kworker/R-rcu-g 
    kworker/R-rcu_p 
    kworker/R-slub_ 
    kworker/R-netns 
    kworker/R-mm_pe 
    rcu_tasks-kthread 
    rcu_tasks_rude_kthread 
    rcu_tasks_trace_kthread 
    ksoft irqd/û 
    rcu_preernpt 
    migrat ion/û 
    idle_inject/û 
    cpuhp/û 
    cpuhp/l 
    idle_inject/l 
    migrat ion/ 1 
    ksoft irqd/l 
    kworker/l: ûH-kblockd 
    cpuhp/2 
    idle_inject/2 
    migrat ion/2 
    ksoft irqd/2 
    kworker/2 : ûH-events_h ighpri 
    cpuhp/3 
    idle_inject/3 
    migrat ion/3 
    ksoft irqd/3 
    kworker/3 : ûH-kb lockd 
    kdevt mpfs 
    kworker/R- inet_ 
    kauditd 
    khungtaskd 
    oom_reaper 
    kworker/R-write 
    kcompactdû 
    ksmd 
    khugepaged 
    kunrker/R-kinte 

* + mpstat: Detailed CPU performance.
  + Linux 6.8.Ø-48-generic (ubuntuserver. librarg.com) 
    AM CPU 
    AM all 
    %usr ice 
    Ø.ØØ 
    *sys %iowait 
    %irq 
    Ø.ØØ 
    11/13/2024 
    *soft *steal 
    Ø.ØØ 
    _aarch64_ 
    *guest 
    Ø.ØØ 
    (4 
    %gnice 
    Ø.ØØ 
    CPI-I) 
    *idle 
    33.8B 
    vboxuser@ubuntuserver : /$ 

* + sar: Historical CPU performance data.

* + %usep 
    ев:ее. 
    • 17 
    t.tt 
    ев: 19. 
    • 17 ЯМ 
    t.tt 
    t.tt 
    t.tt 
    вв. вз 
    ев:ге. 
    • 17 
    t.tt 
    t.tt 
    t.tj 
    ВВ. ВЗ 
    ев:зе. 
    е.екз 
    t.tt 
    t.tt 
    ВВ. ВЗ 
    е.ет 
    е.ее 
    е.ее 
    t.tt 
    ВВ. ВЗ 
    ев:я. 
    t.tt 
    е.ее 
    е.ее 
    е.ее 
    ВВ. ВЗ 
    ев:ее. 
    е.ее 
    е.ее 
    е.ее 
    е.ев 
    ев:1ђ. 
    е.екз 
    е.ее 
    е.ее 
    е.ее 
    ев:ге. 
    е.ее 
    е.ее 
    е.ее 
    е.ее 
    ев:зе. 
    е.ее 
    е.ее 
    е.ее 
    t.tt 
    вв. вз 
    • 17 ЯМ 
    е.ее 
    (3.0 
    t.tt 
    t.tj 
    вв. вз 
    (39:0. 
    (3.0 
    t.tt 
    19:0. 
    е.(ЕЈйЈ 
    вв. вз 
    t.tt 
    t.tt 
    вв. 92 
    -49. 
    • 59:47 
    • 17 
    • 17 
    • 17 
    • 17 
    СРИ 
    а 11 
    а 11 
    а 11 
    а 11 
    а 11 
    а 11 
    а 11 
    а 11 
    all 
    %nice 
    %sgstem 
    %steal 
    %idle 
    vboxuser@ubuntuservep : /$ 
  + uptime: Displays average load over last 1, 5, and 15 minutes.

vboxuser@ubuntuserver:/$ upt ime 
load average: 
up 3:33, 
1 user, 
vboxuser@ubuntuserver : /$ 
0.00, 
0.00, 
0.00 

**Memory Usage**

* + **What to Monitor**: Total memory usage, swap usage, and memory-intensive processes.
  + **Why**: Memory issues can cause slowdowns, application crashes, and even system instability.
  + **Commands/Tools**:
    - free -m: Overview of total memory and swap usage.

vboxuser@ubuntuserver : /$ 
free -m 
used 
322 
0 
free 
3450 
shared 
1 
buff/cache 
337 
available 
3644 
Mem: 
Swap : 
total 
3366 
0 
vboxuser@ubuntuserver : /$ 

* + top / htop: View memory-hungry processes.

* + UBUServer (SERVER -1) [Running] 
    Mem[ll 
    SLIP [ 
    Main 
    PID USER 
    1 
    root 
    310 
    root 
    360 
    root 
    371 
    root 
    372 
    root 
    373 
    root 
    374 
    root 
    375 
    root 
    376 
    root 
    377 
    root 
    SUEtemd-ne 
    524 
    susterrd-re 
    566 
    sust -t i 
    575 
    sust -t i 
    643 
    TIEFS S a E'.'EE--II-I.S 
    654 
    hind 
    660 
    polkitd 
    666 
    683 
    root 
    687 
    root 
    705 
    root 
    714 
    root 
    718 
    root 
    hind 
    721 
    hind 
    722 
    hind 
    723 
    hind 
    724 
    hind 
    725 
    E--lirld 
    726 
    hind 
    727 
    hin-ld 
    723 
    hind 
    730 
    suslog 
    757 
    761 
    root 
    polkitd 
    771 
    polkitd 
    773 
    polkitd 
    774 
    735 
    root 
    sgslog 
    800 
    sgslne 
    801 
    Help 
    Setup 
    20 
    13 
    RT 
    20 
    20 
    RT 
    RT 
    RT 
    RT 
    RT 
    20 
    20 
    20 
    20 
    20 
    20 
    20 
    20 
    20 
    20 
    20 
    20 
    20 
    20 
    20 
    20 
    20 
    20 
    20 
    20 
    20 
    20 
    20 
    20 
    20 
    20 
    20 
    20 
    20 
    Search 
    VIRT 
    0 21332 
    66708 
    -1 
    347M 
    23244 
    347M 
    347M 
    347M 
    347M 
    347M 
    347M 
    18716 
    21436 
    30760 
    30760 
    3372 
    877M 
    375M 
    17836 
    461M 
    461M 
    461M 
    0 
    461M 
    877M 
    877M 
    877M 
    877M 
    877M 
    877M 
    877M 
    877M 
    877M 
    217M 
    107M 
    375M 
    37SM 
    375M 
    217M 
    217M 
    'Filter 
    RES 
    11888 
    16512 
    25384 
    7236 
    25384 
    25384 
    25384 
    25384 
    25384 
    25384 
    8320 
    11776 
    6784 
    6784 
    4480 
    18432 
    8316 
    7680 
    12288 
    12288 
    12288 
    12288 
    18432 
    18432 
    18432 
    18432 
    18432 
    18432 
    18432 
    18432 
    18432 
    4736 
    21624 
    8316 
    8316 
    8316 
    11332 
    4736 
    4736 
    Tree 
    SHR S 
    8432 s 
    15616 
    s 
    7168 
    s 
    4352 s 
    7168 s 
    7168 s 
    7168 
    s 
    7168 s 
    7168 
    s 
    7168 
    s 
    7236 
    s 
    3856 
    s 
    6016 
    s 
    6016 
    s 
    3712 s 
    12800 s 
    6656 s 
    6784 s 
    10368 s 
    10368 s 
    10368 s 
    10368 
    s 
    12800 
    s 
    12800 
    s 
    12800 
    s 
    12800 
    s 
    12800 
    s 
    12800 s 
    12800 s 
    12800 s 
    12800 s 
    3584 s 
    12544 
    s 
    6656 
    s 
    6656 
    s 
    6656 
    s 
    3600 
    s 
    3584 
    s 
    3584 
    s 
    .SortBu 
    TIME+ 
    IB2M/3. 
    OK/OK] 
    Command 
    /sbin/init s 
    Tasks: 33, 35 thr, 88 kthr; 1 running 
    Load average: 0.00 0.00 0.00 
    Uptime: 
    lash no rom t noshell automatic-ubi uitu Vt . handoff=7 
    0. 
    Ø.Ø 
    0. 
    Ø.Ø 
    o. 
    0.6 
    0.6 
    0.6 
    0.6 
    0. 
    o. 
    0.2 
    Ø.Ø 
    o. 
    0.1 
    Ø.Ø 
    o. 
    o. 
    0.3 
    o. 
    o. 
    -f 
    -f 
    -f 
    -f 
    -f 
    Ø.Ø 
    -f 
    Ø.Ø 
    -f 
    Ø.Ø 
    -f 
    -f 
    Ø.Ø 
    o. 
    o. 
    o. 
    o. 
    o. 
    0.1 
    Nice - ;Nice 
    0. 
    0. 
    0. 
    0. 
    0. 
    13. 
    Ø 
    Ø 
    Ø 
    Ø 
    Ø 
    Ø 
    Ø 
    Ø 
    Ø 
    Ø 
    o. 
    o. 
    o. 
    o. 
    o. 
    o. 
    o. 
    o. 
    o. 
    3 
    4 
    6 
    2 
    6 
    6 
    2 
    3 
    2 
    5 
    2 
    2 
    3 
    3 
    3 
    5 
    5 
    s 
    s 
    s 
    5 
    5 
    5 
    I 
    5 
    2 
    2 
    2 
    3 
    I 
    o. 
    o. 
    o. 
    o. 
    o. 
    o. 
    • 01. 
    • 00. 
    0:01. 
    0:00. 
    0:00. 
    0:00. 
    0:00. 
    0:00. 
    0:02. 
    0:00. 
    0:00. 
    0:00. 
    0:00. 
    0:00. 
    0:00. 
    0:00.12 
    Ø:ØØ.Ø9 
    • 00. 
    0:00. 
    0:00. 
    0:00. 
    0:00. 
    0:00. 
    0:00. 
    0:00. 
    0:00. 
    0:00. 
    0:00. 
    Ø:Ø0.Ø3 
    0:00. 
    0:00. 
    0:00. 
    0:00. 
    0:00. 
    0:00. 
    Ø:ØØ. 
    14 
    36 
    16 
    18 
    00 
    00 
    00 
    00 
    20 
    32 
    14 
    14 
    00 
    36 
    05 
    03 
    49 
    02 
    14 
    00 
    00 
    00 
    00 
    00 
    05 
    12 
    01 
    08 
    03 
    00 
    /usr/ lib/syst emd/sgstemd-journa ld 
    /sbin/multipathd -d -s 
    /usr/ lib/syst emd/sgst emd -udevd 
    /sbin/multipathd -d -s 
    /sbin/multipathd -d -s 
    /sbin/multipathd -d -s 
    /sbin/multipathd -d -s 
    /sbin/multipathd -d -s 
    /sbin/multipathd -d -s 
    /usr/ lib/sust emd/sustemd -net workd 
    /usr/ lib/sgst emd/sgst emd -reso Ived 
    /usr/ I ib/sgst emd/sgst emd-t imesgncd 
    /usr/ lib/sgst emd/sgst emd -t imesgncd 
    @dbus-daemon --system --address=sgstemd: --nofork --nopidf i le 
    /usr/sbin/named -f -u bind 
    /usr/lib/polkit-l/polkitd 
    --no-debug 
    /usr/ lib/syst emd/sgst emd- log ind 
    /usr/ libexec/ud isks2/ud isksd 
    /usr/ libexec/udisks2/udisksd 
    /usr/libexec/udisks2/udisksd 
    /usr/ libexec/udisks2/udisksd 
    --sgstemd-activation --syslog-a 
    /usr/sbin/named 
    /usr/sbin/named 
    /usr/sbin/named 
    /usr/sbin/named 
    /usr/sbin/named 
    /usr/sbin/named 
    /usr/sbin/named 
    /usr/sbin/named 
    /usr/sbin/named 
    /usr/sbin/rsuslogd 
    -u 
    -u 
    -u 
    -u 
    -u 
    -u 
    -u 
    -u 
    -u 
    -n 
    bind 
    bind 
    bind 
    bind 
    bind 
    bind 
    bind 
    bind 
    bind 
    - iNONE 
    /usr/bin/puthon3 /usr/share/unattended-upgrades/unattended-upgrade-shutdown 
    /usr/lib/polkit-l/polkitd 
    --no-debug 
    /usr/lib/polkit-l/polkitd 
    --no-debug 
    /usr/lib/polkit-l/polkitd 
    --no-debug 
    /usr/sb in/ModemManager 
    /usr/sbin/rsgslogd -n -iNClNE 
    /usr/sbin/rsqslned -n -iNClNE 
    --wait-for-signal 
    -Kill 
    'Quit 

* + vmstat:Memory statistics.
  + vboxuser@ubuntuserver:/$ vmstat 
    procs 
    -----------memorg---------- ---swap-- 
    free 
    buff cache 
    io---- -system-- -------cpu------- 
    swpd 
    si 
    so 
    bi 
    26 
    bo 
    in 
    5 
    35 
    cs us su id wa st gu 
    0 100 0 0 
    3523384 22816 324100 
    vboxuser@ubuntuserver : /$ 

**Disk Usage**

* + **What to Monitor**: Disk space usage on each partition, inode usage, and disk read/write speeds.
  + **Why**: Full disks can prevent applications from running properly and can lead to system failures.
  + **Commands/Tools**:
    - df -h: Disk space usage by filesystem.
  + vboxuser@ubuntuserver:/$ df -h 
    Filesgstem 
    t mpfs 
    ,ef ivarfs 
    Vdev/sda2 
    't mpfs 
    t mpfs 
    /dev/sdal 
    tmpfs 
    Size 
    337M 
    256K 
    33G 
    2.ØG 
    5.0M 
    1.1G 
    337M 
    Used Avail 
    1012K 
    3.6K 
    3.3G 
    6.4M 
    12K 
    336M 
    253K 
    :33G 
    2.ØG 
    5.0M 
    1.1G 
    337M 
    I-Ise% 
    1% 
    2% 
    1% 
    1% 
    Mounted on 
    /run 
    /sus/f irmware/ef i/ef ivars 
    /dev/shm 
    /run/ lock 
    /boot/ef i 
    /run/user/1ØOØ 
    vboxuser@ubuntuserver : /$ 

* + du -sh /path: Shows disk usage for specific directories.
  + vboxuser@ubuntuserver : 'et c/dhcp$ 
    /etc/dhcp 
    vboxuser@ubuntuserver : /etc/dhcp$ 
    ,2ûK 
    yboxuser@ubuntuserver : 'et c/dhcp$ 
    ,2ûK 
    vboxuser@ubuntuserver : 'et c/dhcp$ 
    pu-ld 
    sudo du 
    sudo du 
    -sh 
    -sh 


    - iostat:
    - Disk I/O statistics.

* + 'avg-cpu: 
    Device 
    loopØ 
    sda 
    srØ 
    *user 
    ice 
    Ø.ØØ 
    tps 
    Ø.ØØ 
    0.00 
    *system %iowait *steal 
    kB_read/s 
    Ø.ØØ 
    0.00 
    kB_wrtn/s 
    0.00 
    0.00 
    *idle 
    33. aa 
    kB_dscd/s 
    Ø.ØØ 
    0.00 
    0.00 
    kB_read 
    kB_wrtn 
    kB_dscd 

**Network Traffic and Connections**

* + **What to Monitor**: Incoming and outgoing traffic, network bandwidth usage, active connections, and any unusual traffic spikes.
  + **Why**: Monitoring network can help detect potential intrusions, DDoS attacks, and network bottlenecks.
  + **Commands/Tools**:
    - netstat / ss: Active connections and listening ports.

* + UBUServer (SERVER -1) [Running] 
    u_str 
    u_str 
    u_str 
    *Zenp0sB : ipv6- icmp 
    *Zenp0sB : ipv6- icmp 
    u_dgr 
    u_str 
    Ll_dgr 
    I-I_dgr 
    I-I _dgr 
    u_str 
    u_dgr 
    u_str 
    u_str 
    u_str 
    u_dgr 
    u_str 
    u_dgr 
    u_str 
    u_str 
    u_str 
    u_str 
    u_str 
    u_str 
    u_str 
    u_str 
    u_str 
    u_str 
    u_dgr 
    u_str 
    LI _dgr 
    u_str 
    u-str 
    u_str 
    u_str 
    u_str 
    u_str 
    u_dgr 
    u_str 
    u_str 
    u_str 
    u_str 
    u_str 
    u_str 
    u_str 
    u_str 
    u_str 
    ESTAB 
    ESTAB 
    ESTAB 
    ESTAB 
    ESTAB 
    ESTAB 
    ESTAB 
    ESTAB 
    ESTAB 
    ESTAB 
    ESTAB 
    ESTAB 
    ESTAB 
    ESTAB 
    ESTAB 
    ESTAB 
    ESTAB 
    ESTAB 
    ESTAB 
    ESTAB 
    ESTAB 
    ESTAB 
    ESTAB 
    ESTAB 
    ESTAB 
    ESTAB 
    ESTAB 
    ESTAB 
    ESTAB 
    ESTAB 
    ESTAB 
    ESTAB 
    ESTAB 
    ESTAB 
    ESTAB 
    ESTAB 
    ESTAB 
    ESTAB 
    ESTAB 
    ESTAB 
    ESTAB 
    ESTAB 
    ESTAB 
    ESTAB 
    ESTAB 
    ESTAB 
    LINCONN 
    LINCONN 
    LINCONN 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    0 
    * 3131 
    * 11450 
    /run/syst emd/journal/dev- log 
    6833 
    /run/syst emd/journa l/socket 
    6835 
    * 11557 
    * 9498 
    /run/dbus/sgstem_bus_socket 
    10587 
    11401 
    /run/dbus/sgstem_bus_socket 
    8914 
    * 8313 
    * 11377 
    /run/systemd/journa l/stdout 
    3055 
    * 11278 
    * 8675 
    3846 
    BB 42 
    * 10090 
    /run/syst emd/journa l/stdout 
    9237 
    BB 43 
    BB 44 
    * 2724 
    * 10453 
    /run/syst emd/journa l/stdout 
    3265 
    * 10106 
    /run/systemd/journa l/stdout 
    9941 
    /run/syst emd/journa l/stdout 
    8686 
    10551 
    /run/dbus/sgstem_bus_socket 
    10588 
    BB 45 
    /run/sgstemd/journa l/stdout 
    7113 
    /run/systemd/journa l/stdout 
    6355 
    /run/syst emd/journa l/stdout 
    11054 
    * 10275 
    @bc0746e5eB5aB522/bus/systemd/bus-system 
    11553 
    @d2c77c06e44BB3Bb/bus/sgst emd-t imesgn/bus-ap i -t imesgnc 
    9639 
    @b2232f ac36f 0550f /bus/sgst emd/bus-ap i-sgstem 
    9719 
    1fd675f ddd2Bb47/bus/sgstemd -net work/bus-api-network 
    9645 
    @eaace76e30a35BeB/bus/sgst emd - log ind/sgst em 
    8152 
    @e6ebBbc8d4f5BBcb/bus/sgstemd-resolve/bus-api-resolve 
    8659 
    .. •icmp 
    * 6833 
    * BB3B 
    0 
    0 
    * 11556 
    * 3639 
    * 6833 
    * 8313 
    * 8314 
    * 6835 
    * 11377 
    * 6833 
    9343 
    * 11054 
    * 10275 
    BB 42 
    * 3265 
    BB 45 
    BB 46 
    * 6835 
    * 7113 
    * 6835 
    * 8675 
    9341 
    BB 40 
    * 10551 
    8686 
    8653 
    BB 44 
    * 6833 
    * 778 
    * 2724 
    * 10112 
    * 10587 
    * 8104 
    * 10583 
    * 8822 
    10588 
    icmp6 
    icmp6 
    vboxuser@ubuntuserver : /$ 
  + n
  + iftop: Real-time network bandwidth
  + usage.
  + nload: Graphical view of network traffic.
  + sar -n DEV: Network statistics.
  + tcpdump or wireshark: For capturing and analyzing packets.
  + UBUServer (SERVER - 
    07. 
    .17 AM 
    13.00 
    Ø.ØØ 
    0.00 
    0.00 
    Ø.ØØ 
    13.00 
    Ø.ØØ 
    13.00 
    0.00 
    0.00 
    0.130 
    Ø.ØØ 
    •17 AM 
    0.00 
    0.00 
    0.00 
    0.130 
    0.00 
    0.013 
    0.013 
    Ø.ØØ 
    0.00 
    0.00 
    0.00 
    0.130 
    0.00 
    0.00 
    0.013 
    0.00 
    0.00 
    0.00 
    0.00 
    0.00 
    0.00 
    0.00 
    0.00 
    0.00 
    0.00 
    0.00 
    0.00 
    Ø.ØØ 
    Ø.ØØ 
    o.ØØ 
    0.00 
    o.ØØ 
    0.130 
    Ø.ØØ 
    Ø.ØØ 
    0.00 
    0.130 
    13.130 
    13.00 
    0.013 
    Ø.ØØ 
    Ø.ØØ 
    0.00 
    0.130 
    13.130 
    13.130 
    0.00 
    0.013 
    Ø.ØØ 
    Ø.ØØ 
    0.013 
    Ø.ØØ 
    Ø.ØØ 
    13.130 
    Ø.ØØ 
    Ø.ØØ 
    0.00 
    Ø.ØØ 
    Ø.ØØ 
    0.130 
    Ø.ØØ 
    Ø.ØØ 
    Ø.ØØ 
    Ø.ØØ 
    0.00 
    Ø.ØØ 
    Ø.ØØ 
    13.00 
    0.00 
    Ø.ØØ 
    08. 
    .10 AM 
    Ø.ØØ 
    Ø.ØØ 
    0.00 
    0.00 
    Ø.ØØ 
    0.00 
    0.00 
    Ø.ØØ 
    08. 
    .10 AM 
    Ø.ØØ 
    0.00 
    0.00 
    0.00 
    0.00 
    Ø.ØØ 
    13.00 
    .10 AM 
    08. 
    13.00 
    Ø.ØØ 
    0.00 
    0.00 
    0.00 
    0.00 
    0.00 
    0.00 
    •17 AM 
    0.00 
    0.00 
    0.00 
    0.00 
    0.00 
    0.130 
    0.00 
    0.00 
    0.00 
    0.00 
    0.00 
    0.00 
    0.00 
    0.00 
    0.00 
    0.013 
    0.013 
    0.00 
    0.00 
    13.130 
    0.130 
    o.ØØ 
    0.00 
    0.013 
    0.00 
    0.00 
    Ø.ØØ 
    0.00 
    0.00 
    o.ØØ 
    0.00 
    Ø.ØØ 
    Ø.ØØ 
    0.00 
    o.ØØ 
    0.00 
    0.00 
    Ø.ØØ 
    Ø.ØØ 
    Ø.ØØ 
    0.130 
    13.130 
    0.00 
    0.00 
    0.00 
    Ø.ØØ 
    Ø.ØØ 
    0.013 
    Ø.ØØ 
    Ø.ØØ 
    13.130 
    Ø.ØØ 
    Ø.ØØ 
    Ø.ØØ 
    0.00 
    Ø.ØØ 
    Ø.ØØ 
    (3.130 
    (3.130 
    Ø.ØØ 
    Ø.ØØ 
    Ø.ØØ 
    Ø.ØØ 
    Ø.ØØ 
    Ø.ØØ 
    13.00 
    Ø.ØØ 
    Ø.ØØ 
    Ø.ØØ 
    Ø.ØØ 
    0.00 
    Ø.ØØ 
    Ø.ØØ 
    0.00 
    Ø.ØØ 
    Ø.ØØ 
    .17 AM 
    0.00 
    Ø.ØØ 
    0.00 
    0.00 
    Ø.ØØ 
    13.00 
    0.00 
    0.00 
    Ø.ØØ 
    0.00 
    0.00 
    Ø.ØØ 
    Ø.ØØ 
    •10 AM 
    Ø.ØØ 
    0.00 
    0.00 
    0.00 
    0.013 
    0.130 
    0.00 
    0.00 
    •10 AM 
    0.00 
    0.00 
    0.00 
    0.130 
    0.00 
    0.00 
    0.00 
    Ø.ØØ 
    0.00 
    0.00 
    13.00 
    0.00 
    0.00 
    0.00 
    03. 
    0.00 
    0.00 
    0.00 
    0.00 
    13.130 
    0.00 
    0.00 
    0.00 
    03. 
    Ø.ØØ 
    Ø.ØØ 
    o.ØØ 
    o.ØØ 
    o.ØØ 
    0.00 
    0.00 
    Ø.ØØ 
    03. 
    Ø.ØØ 
    Ø.ØØ 
    o. 00 
    o .00 
    Ø.ØØ 
    0.00 
    Ø.ØØ 
    Ø.ØØ 
    Ø.ØØ 
    0.130 
    13.130 
    13.130 
    13.00 
    Ø.ØØ 
    Ø.ØØ 
    Ø.ØØ 
    13.130 
    Ø.ØØ 
    Ø.ØØ 
    03. 
    Ø.ØØ 
    Ø.ØØ 
    0.00 
    Ø.ØØ 
    Ø.ØØ 
    (3.130 
    13.130 
    Ø.ØØ 
    Ø.ØØ 
    Ø.ØØ 
    0.00 
    Ø.ØØ 
    0.130 
    13.00 
    Ø.ØØ 
    Ø.ØØ 
    .17 AM 
    Ø.ØØ 
    0.00 
    Ø.ØØ 
    o.ØØ 
    0.00 
    Ø.ØØ 
    Ø.ØØ 
    .17 AM 
    Ø.ØØ 
    0.013 
    0.00 
    0.00 
    Ø.ØØ 
    13.00 
    Ø.ØØ 
    Ø.ØØ 
    Ø.ØØ 
    Ø.ØØ 
    0.00 
    0.00 
    0.00 
    0.00 
    Ø.ØØ 
    0.00 
    •17 AM 
    0.00 
    0.00 
    0.00 
    0.130 
    0.00 
    0.00 
    0.00 
    Ø.ØØ 
    0.00 
    0.00 
    0.00 
    0.130 
    0.00 
    0.00 
    0.00 
    Ø.ØØ 
    0.00 
    0.00 
    13.00 
    0.00 
    Ø.ØØ 
    0.00 
    0.00 
    Ø.ØØ 
    0.00 
    0.00 
    o.ØØ 
    0.00 
    Ø.ØØ 
    Ø.ØØ 
    Ø.ØØ 
    0.00 
    o.ØØ 
    0.00 
    0.00 
    Ø.ØØ 
    Ø.ØØ 
    Ø.ØØ 
    0.00 
    0.130 
    0.00 
    13.130 
    0.013 
    Ø.ØØ 
    0.130 
    13.130 
    13.00 
    0.130 
    Ø.ØØ 
    Ø.ØØ 
    Ø.ØØ 
    0.00 
    Ø.ØØ 
    Ø.ØØ 
    13.130 
    Ø.ØØ 
    Ø.ØØ 
    IFACE 
    10 
    enpØs8 
    enpØs3 
    10 
    enp0s8 
    enpØs3 
    10 
    enp0s8 
    enpØs3 
    10 
    enpØs8 
    enpØs3 
    10 
    enpØs8 
    enpØs3 
    10 
    enp0s8 
    enpØs3 
    10 
    enpØs8 
    enp0s3 
    10 
    enpØs8 
    enpØs3 
    10 
    enpØs8 
    enpØs3 
    10 
    enp0s8 
    enp0s3 
    10 
    enpØs8 
    enp0s3 
    10 
    enpØs8 
    enpØs3 
    10 
    enpØs8 
    enpØs3 
    10 
    enp0s8 
    enp0s3 
    10 
    enpØs8 
    enpØs3 
    10 
    enpØs8 
    enpØs3 
    rxpck/s 
    txpck/s 
    rxkB/s 
    txkB/s 
    1) [Running] 
    rxmcst/s 
    •53: 47 AM 
    08:00. 
    •17 
    08:00. 
    08:00. 
    08:10. 
    •17 
    08:10. 
    08:10. 
    08:20. 
    08:20. 
    08:20. 
    08:30. 
    08:30. 
    08:30. 
    08:50. 
    08:50. 
    •17 
    08:50. 
    03:00. 
    03:00. 
    03:00. 
    03:10. 
    03:10. 
    03:10. 
    03:20. 
    03:20. 
    .17 
    03:20. 
    03:30. 
    03:30. 
    03:30. 
    03:50. 
    03:50. 
    10:00. 
    10:00. 
    10:00. 
    .17 
    10:10. 
    10:10. 
    10:10. 
    • 17 
    10:20. 
    10:20. 
    10:20. 
    Average: 
    Average : 
    rxcmp/s 
    txcmp/s 
    Zifutil 
    vboxuser@ubuntuserver : /$ 

**File System Integrity and Logs**

* + **What to Monitor**: Integrity of important files, abnormal changes in files, and log files for errors or suspicious activity.
  + **Why**: Unauthorized changes to files or unusual error messages in logs can indicate potential security incidents.
  + **Commands/Tools**:
    - md5sum or sha256sum: Verify file integrity.
    - vboxuser@ubuntuserver:/$ Is 
      bin 
      file. txt 
      lib 
      shin 
      tm _t 
      vboxuser@ubuntuserver:/$ rnd5sum file. txt 
      553cd2Ø436a2b1f387Ø313ØaØ0613ed3 file. txt 
      vboxuser@ubuntuserver:/$ sha256sum file. txt 
      4bd8144876c8adef a3d62613 7f 13ac87Ø6ca4f 44 Isa 11b763aaf2 
      vboxuser@ubuntuserver : /$ 
      file. txt 
    - auditd: Linux Auditing System to monitor changes in criti
    - cal files.
    - journalctl: View system logs.
  + Nov 
    10:13. 
    Nov 
    Nov 
    Nov 
    *Nov 
    Nov 
    bNov 
    10:13. 
    'Nov 
    10:13. 
    tNov 
    10:13. 
    Olov 
    10:13. 
    Nov 
    10:13. 
    Nov 
    10:13. 
    Nov 
    10:13. 
    Nov 
    10:13. 
    Nov 
    Nov 
    10:13. 
    gNov 
    10:13. 
    Nov 
    Nov 
    10:13. 
    Nov 
    10:13. 
    Nov 
    10:13. 
    Nov 
    10:13. 
    PNov 
    10:13. 
    Nov 
    10:13. 
    Nov 
    10:13. 
    Nov 
    10:13. 
    Nov 
    Nov 
    Nov 
    Nov 
    Nov 
    Nov 
    10:13. 
    'Nov 
    10:13. 
    Nov 
    10:13. 
    Nov 
    10:13. 
    Nov 
    10:13. 
    Nov 
    10:13. 
    Nov 
    10:13. 
    Nov 
    10:13. 
    Nov 
    10:13. 
    Nov 
    10:13. 
    Nov 
    Nov 
    Nov 
    10:13. 
    Nov 
    10:13. 
    Nov 
    10:13. 
    Nov 
    10:13. 
    Nov 
    10:13. 
    Nov 
    10:13. 
    04 
    04 
    04 
    04 
    04 
    04 
    04 
    04 
    04 
    04 
    04 
    04 
    04 
    04 
    04 
    04 
    04 
    04 
    04 
    04 
    04 
    04 
    04 
    04 
    04 
    04 
    04 
    04 
    04 
    04 
    04 
    04 
    04 
    04 
    04 
    04 
    04 
    04 
    04 
    04 
    04 
    04 
    04 
    04 
    04 
    04 
    04 
    04 
    04 
    ines 71-113 
    •23 
    •23 
    •23 
    •23 
    •23 
    •23 
    •23 
    •23 
    •23 
    •23 
    •23 
    •23 
    •23 
    •23 
    •23 
    •23 
    •23 
    •23 
    •23 
    •23 
    •23 
    •23 
    •23 
    •23 
    •23 
    •23 
    •23 
    •23 
    •23 
    •23 
    •23 
    •23 
    •23 
    •23 
    •23 
    LIBIJServer 
    LIBIJServer 
    LIBIJServer 
    LIBIJServer 
    LIBLlServer 
    LIBLlServer 
    LIBIJServer 
    LIBIJServer 
    LIBIJServer 
    LIBIJServer 
    LIBIJServer 
    LIBLIServer 
    LIBLIServer 
    LIBLIServer 
    LIBIJServer 
    LIBLlServer 
    LIBIJServer 
    LIBLIServer 
    LIBIJServer 
    LIBLIServer 
    LIBIJServer 
    LIBIJServer 
    LIBIJServer 
    LIBLIServer 
    LIBLIServer 
    LIBLIServer 
    LIBLlServer 
    LIBIJServer 
    LIBIJServer 
    LIBIJServer 
    LIBLlServer 
    LIBLIServer 
    LIBLIServer 
    LIBIJServer 
    LIBIJServer 
    LIBIJServer 
    LIBLIServer 
    LIBLIServer 
    LIBIJServer 
    LIBIJServer 
    LIBIJServer 
    LIBIJServer 
    LIBLlServer 
    LIBLlServer 
    LIBLIServer 
    LIBIJServer 
    LIBIJServer 
    LIBIJServer 
    LIBIJServer 
    kernel: 
    kernel: 
    kernel: 
    kernel: 
    kernel: 
    kernel: 
    kernel: 
    kernel: 
    kernel: 
    kernel: 
    kernel: 
    kernel: 
    kernel: 
    kernel: 
    kernel: 
    kernel: 
    kernel: 
    kernel: 
    kernel: 
    kernel: 
    kernel: 
    kernel: 
    kernel: 
    kernel: 
    kernel: 
    kernel: 
    kernel: 
    kernel: 
    kernel: 
    kernel: 
    kernel: 
    kernel: 
    kernel: 
    kernel: 
    kernel: 
    kernel: 
    kernel: 
    kernel: 
    kernel: 
    kernel: 
    kernel: 
    kernel: 
    kernel: 
    kernel: 
    kernel: 
    kernel: 
    kernel: 
    kernel: 
    kernel: 
    rcu: srcu_init: Setting srcu_struct sizes based on contention. 
    arch_timer: cp15 timer(s) running at 24.00MHz (virt) . 
    clocksource: arch_sgs_counter: mask: Oxffffffffffffff max_cgcles: Ox588fe3dcØ, max_idle_ns: 440735202532 ns 
    sched_clock: 56 bits at 24MHz, resolut ion 41ns, wraps everg 4338046511Ø37ns 
    Console: colour dummy device 8Øx25 
    printk: legacy console [ttgØ] enabled 
    Calibrating delay loop (skipped), value calculated using timer frequency.. 
    48.00 BogoMIPS (Ipj=24ØOØ) 
    pid_max: default: 32768 minimum: 301 
    LSM: initializing Ism-lockdown, capability, integrity 
    landlock: Up and running. 
    Yama: becoming mindful. 
    AppArmor: AppArmor initialized 
    Mount-cache hash table entries: 16384 (order: 5, 131072 bytes, linear) 
    Mountpoint-cache hash table entries: 16384 (order: 5, 131072 bytes, linear) 
    cacheinfo: Unable to detect cache hierarchy for CPU 0 
    RCLI Tasks: Setting shift to 2 and lim to 1 rcu_task_cb_adjust=l. 
    RCLI Tasks Rude: Setting shift to 2 and lim to 1 rcu_task_cb_adjust=l. 
    RCLI Tasks Trace: Setting shift to 2 and lim to 1 
    rcu: Hierarchical SRCLI implementat ion. 
    Max phase no-delay instances is 400. 
    rcu: 
    Remapping and enabling EFI services. 
    smp: Bringing up secondary CPUs . 
    Detected PIPT I-cache on CPI-Il 
    GICv3: CPI-Il: found redistributor 
    CPI-Il: Booted secondary processor 
    Detected PIPT I-cache on CPI-IZ 
    GICv3: CPI-12: found redistributor 
    CPI-12: Booted secondary processor 
    Detected PIPT I-cache on CPI-IS 
    GICv3: CPI-13: found redistributor 
    CPI-13: Booted secondary processor 
    1 region o:ox0000ØOØ144a2ØOØ0 
    oxoooooooool [Ox610fOOOO] 
    2 region o:oxØOØOØOØ144a4ØOØ0 
    [Ox610fOOOO] 
    3 region O:ØxØOØOØOØ144a6ØOØO 
    [Ox610fOØØØ] 
    smp : 
    SMP: 
    CPU: 
    CPU 
    CPU 
    CPI-I 
    CPU 
    CPI-I 
    CPU 
    CPU 
    CPU 
    CPU 
    CPU 
    CPI-I 
    CPI-I 
    CPU 
    CPU 
    CPI-I 
    Brought up 1 node, 4 CPI-Is 
    Total of 4 processors activated. 
    All CPU(s) started 
    features: 
    features: 
    features: 
    features: 
    features: 
    features: 
    features: 
    features: 
    features: 
    features: 
    features: 
    features: 
    features: 
    features: 
    features: 
    detected: 
    detected: 
    detected: 
    detected: 
    detected: 
    detected: 
    detected: 
    detected: 
    detected: 
    detected: 
    detected: 
    detected: 
    detected: 
    detected: 
    detected: 
    at ELI 
    ARMv8.4 Translation Table Level 
    Data cache clean to the POI-I not required for I/D coherence 
    Common not Private translations 
    CRC32 instruct ions 
    Data cache clean to Point of Deep Persistence 
    Data cache clean to Point of Persistence 
    Data independent timing control (DI T) 
    EOPD 
    Generic authentication (IMP DEF algorithm) 
    RCpc load-acquire (LDAPR) 
    LSE atomic instructions 
    Privileged Access Never 
    RAS Extension Support 
    Speculation barrier (SB) 
    TLB range maintenance instructions 
    - /var/log/: Default directory for log files, e.g., /var/log/syslog, /v
    - ar/log/auth.log.

**2. Monitoring Memory-Intensive Processes**

* + **Commands**:
    - ps aux --sort=-%mem: Lists processes sorted by memory usage.
  + A screenshot of a computer program

    Description automatically generated
    - top / htop: Interactive tools to display processes with real-time memory usage.

These commands help identify if a particular application or process is consuming an unusually large amount of memory.

A screenshot of a computer

Description automatically generated

**3. Understanding Log Files**

* + **What Are Log Files**: Log files record system events, errors, and user activities, providing a record for troubleshooting and monitoring.
  + **Locations**:
    - /var/log/syslog: General system log.
    - /var/log/auth.log: Authentication logs, including login attempts.
    - /var/log/kern.log: Kernel logs.
    - /var/log/dmesg: Boot and hardware-related messages.
  + **Commands to View Logs**:
    - cat, less, or tail -f (e.g., tail -f /var/log/syslog): To view log entries in real-time.
    - journalctl: For systems using systemd, view logs with various filters (e.g., journalctl -u sshd.service for SSH logs).

**4. Monitoring User Activity and Sessions**

* + **Commands**:
    - who: Shows currently logged-in users.
    - last: Displays the last logins of users and their source IPs.
    - lastb: Displays failed login attempts (useful for detecting brute-force attempts).
    - ausearch -c '<command>': For auditing commands executed by users (requires auditd to be enabled).
    - history: Shows command history for the current user (if accessible).

Monitoring user activity is essential for security, as it can help detect unauthorized access or malicious actions.

**5. Health and Performance Metrics**

* + **Important Metrics**:
    - **CPU Load**: Average over 1, 5, and 15 minutes.
    - **Memory Usage**: Percentage of used memory and swap.
    - **Disk Space**: Percentage of used disk on each filesystem.
    - **Network Usage**: Current network throughput, error rates, and dropped packets.
    - **System Temperature** (if applicable): Check CPU and GPU temperatures to prevent overheating.
  + **Commands**:
    - top, htop, free -m, df -h, iostat, sar, netstat, uptime, and tools like sensors (from lm-sensors package) to check temperature.

**6. System Uptime**

* + **Command**:
    - uptime: Shows how long the system has been running, along with average load.
    - **Why**: Checking uptime can indicate if unexpected reboots occurred, which could be related to crashes, power issues, or intrusions.

This sounds like a great foundational challenge for developing system administration and security operations skills. To get you started, here's a structured approach and some key information you could include in your research and report files for Linux system monitoring.

**Task 1: Research and Documentation**

For your research file, consider structuring the document to cover each area of monitoring in separate sections, discussing what to monitor, why it's important, and specific Linux commands/tools to use.

**1. Main Areas of Concern in System Monitoring**

* + **CPU Load and Utilization**
    - **What to Monitor: Monitor average CPU load, individual CPU utilization, and whether any processes are overloading the CPU.**
    - **Why: High CPU load affects overall system performance and could indicate a runaway process, inefficient software, or an attack.**
    - **Commands/Tools:**
      * **top / htop: Real-time CPU usage and processes.**
      * **mpstat: Detailed CPU performance.**
      * **sar: Historical CPU performance data.**
      * **uptime: Displays average load over last 1, 5, and 15 minutes.**
  + **Memory Usage**
    - **What to Monitor: Total memory usage, swap usage, and memory-intensive processes.**
    - **Why: Memory issues can cause slowdowns, application crashes, and even system instability.**
    - **Commands/Tools:**
      * **free -m: Overview of total memory and swap usage.**
      * **top / htop: View memory-hungry processes.**
      * **vmstat: Memory statistics.**
  + **Disk Usage**
    - **What to Monitor: Disk space usage on each partition, inode usage, and disk read/write speeds.**
    - **Why: Full disks can prevent applications from running properly and can lead to system failures.**
    - **Commands/Tools:**
      * **df -h: Disk space usage by filesystem.**
      * **du -sh /path: Shows disk usage for specific directories.**
      * **iostat: Disk I/O statistics.**
  + **Network Traffic and Connections**
    - **What to Monitor: Incoming and outgoing traffic, network bandwidth usage, active connections, and any unusual traffic spikes.**
    - **Why: Monitoring network can help detect potential intrusions, DDoS attacks, and network bottlenecks.**
    - **Commands/Tools:**
      * **netstat / ss: Active connections and listening ports.**
      * **iftop: Real-time network bandwidth usage.**
      * **nload: Graphical view of network traffic.**
      * **tcpdump or wireshark: For capturing and analyzing packets.**
      * **sar -n DEV: Network statistics.**
  + **File System Integrity and Logs**
    - **What to Monitor: Integrity of important files, abnormal changes in files, and log files for errors or suspicious activity.**
    - **Why: Unauthorized changes to files or unusual error messages in logs can indicate potential security incidents.**
    - **Commands/Tools:**
      * **md5sum or sha256sum: Verify file integrity.**
      * **auditd: Linux Auditing System to monitor changes in critical files.**
      * **journalctl: View system logs.**
      * **/var/log/: Default directory for log files, e.g., /var/log/syslog, /var/log/auth.log.**

**2. Monitoring Memory-Intensive Processes**

* + **Commands**:
    - ps aux --sort=-%mem: Lists processes sorted by memory usage.
    - top / htop: Interactive tools to display processes with real-time memory usage.

These commands help identify if a particular application or process is consuming an unusually large amount of memory.

**3. Understanding Log Files**

* + **What Are Log Files**: Log files record system events, errors, and user activities, providing a record for troubleshooting and monitoring.
  + **Locations**:
    - /var/log/syslog: General system log.
    - /var/log/auth.log: Authentication logs, including login attempts.
    - /var/log/kern.log: Kernel logs.
    - /var/log/dmesg: Boot and hardware-related messages.
  + **Commands to View Logs**:
    - cat, less, or tail -f (e.g., tail -f /var/log/syslog): To view log entries in real-time.
    - journalctl: For systems using systemd, view logs with various filters (e.g., journalctl -u sshd.service for SSH logs).

**4. Monitoring User Activity and Sessions**

* + **Commands**:
    - who: Shows currently logged-in users.
    - last: Displays the last logins of users and their source IPs.
    - lastb: Displays failed login attempts (useful for detecting brute-force attempts).
    - ausearch -c '<command>': For auditing commands executed by users (requires auditd to be enabled).
    - history: Shows command history for the current user (if accessible).

Monitoring user activity is essential for security, as it can help detect unauthorized access or malicious actions.

**5. Health and Performance Metrics**

* + **Important Metrics**:
    - **CPU Load**: Average over 1, 5, and 15 minutes.
    - **Memory Usage**: Percentage of used memory and swap.
    - **Disk Space**: Percentage of used disk on each filesystem.
    - **Network Usage**: Current network throughput, error rates, and dropped packets.
    - **System Temperature** (if applicable): Check CPU and GPU temperatures to prevent overheating.
  + **Commands**:
    - top, htop, free -m, df -h, iostat, sar, netstat, uptime, and tools like sensors (from lm-sensors package) to check temperature.

**6. System Uptime**

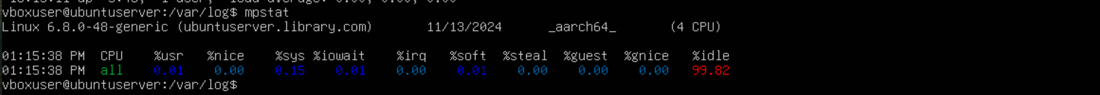
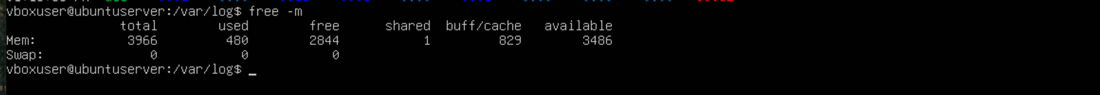
* + **Command**:
    - uptime: Shows how long the system has been running, along with average load.
    - **Why**: Checking uptime can indicate if unexpected reboots occurred, which could be related to crashes, power issues, or intrusions.

**7. Assessing Network Traffic**

* + **Commands/Tools**:
    - iftop: Real-time view of bandwidth usage by IP and port.
    - nload: Graphical display of incoming and outgoing network traffic.
    - tcpdump or wireshark: Packet capture and analysis.
    - netstat or ss: To list network connections and listening ports.

lolasl

**System Monitoring Report for [Machine Name or IP Address]**

* + **System Overview**
    - **Uptime: [Include uptime output]**
    - **CPU and Memory Usage:**
      * **Average Load: 0.0**
      * **CPU Utilization: [Output from mpstat or top]**
      * ****
      * **Memory Usage: [Output from free -m or vmstat]**
      * ****

* + **Filesystem Overview**: [Output of df -h]
    - A black background with a white object in the middle

      Description automatically generated

* + **Disk Usage**
    - **Disk I/O Performance: [Output from iostat]**
    - **A screenshot of a computer

      Description automatically generated**
  + **Network Traffic and Connections**
    - **Active Connections: [Output from netstat or ss]**
    - **A screenshot of a computer

      Description automatically generated**
    - **laBandwidth Usage: [Output from iftop or nload]**
  + **User Activity**
    - **Last Logins: [Output of last]**
    - ****

* + **Failed Login Attempts**: [Output of lastb]
  + A screen shot of a computer

    Description automatically generated
  + **Command History** (if applicable): [Sample from history]
  + **Log Analysis**
    - **Summary of recent messages from /var/log/syslog, /var/log/auth.log, etc., to highlight any critical messages, errors, or unusual activity.**
  + **Temperature (If Relevant)**
    - **System Temperatures: [Output from sensors if available]**