Lecture 8

### **Interview Prep-Performance Monitoring Tools**

**Performance monitoring**

* Interview Question
  + Server is in high utilization.
  + How to monitor it
  + There is one process which is utilization high memory / eating up CPU.
    - What is your daily activity? (Because after taking this course we r not freshers)
    - Ticketing tools
      * + JIRA
        + OTRS
        + Service now
        + BMC Remedy
      * Answer: - at least write 20 lines should be written and memorize

A Linux administrator's daily routine tasks may include:

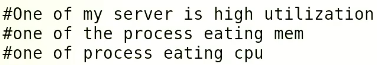
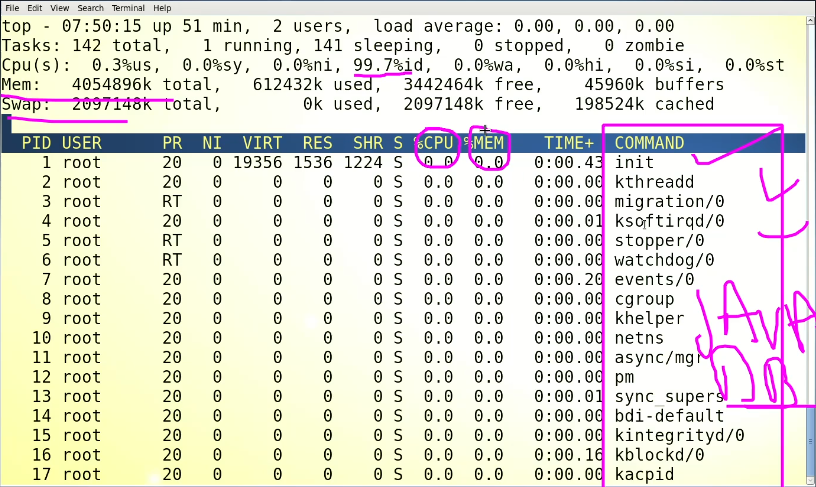
* Monitoring system performance and resource utilization
* Managing user accounts and permissions
* Installing, configuring, and updating software and systems
* Backing up and restoring data
* Troubleshooting and resolving technical issues
* Securing the system by applying patches and updates
* Managing network services, such as DNS and DHCP
* Automating tasks using scripts
* Responding to security incidents and conducting security audits.

A Linux administrator's daily routine tasks may include:

* Monitoring system performance and resource utilization
* Managing user accounts and permissions
* Installing, configuring, and updating software and systems
* Backing up and restoring data
* Troubleshooting and resolving technical issues
* Securing the system by applying patches and updates
* Managing network services, such as DNS and DHCP
* Automating tasks using scripts
* Responding to security incidents and conducting security audits
* Monitoring logs and system events
* Managing storage systems and disk space
* Managing and maintaining system documentation
* Configuring and optimizing system settings
* Deploying new systems and applications
* Providing technical support to end-users
* Upgrading hardware components as needed
* Managing virtualization technologies, such as KVM and VMware
* Ensuring compliance with security and industry regulations
* Collaborating with other IT teams and stakeholders
* Continuously improving processes and procedures to increase efficiency.

1. If server is in high utilization, how to diagnose?
2. What critical issue faced for past 1 month?
   * + - Or trouble shooting in past 1 month?

* **Make written notes of 20 daily activities.** 
  + 2nd Q. Troubleshooting à high load server
    - Scenario à RAM is full in server
    - Connectivity issue from outside
    - Slow machine
    - Application loading slow
  + Its called performance monitoring

1. Scenario
2. 
3. 1st case à TOP command will be used
4. CPU à check à idle value of CPU à if idle value is 0 à too much load
5. In computing, "CPU idle value" refers to the percentage of time that a computer's central processing unit (CPU) is idle, meaning it has no tasks to perform. This value can be measured using performance monitoring tools, such as the Task Manager in Windows or the Activity Monitor in macOS. A high CPU idle value indicates that the CPU is not being utilized to its full capacity, while a low CPU idle value can indicate that the computer is running many processes and the CPU is working at maximum capacity.
6. Memory check à if memory is full à check SWAP à SWAP is full à free -m are other ways to check memory
7. Check last column à check specific process à how much RAM is being utilized
8. 
9. There is a process which is utilization full memory and CPU à (to kill that process is not a solution) à the answer is to engage respective team which is managing that application e.g Java and ask them to diagnose the application.
10. Same question à high load server à but no process is eating up full CPU and RAM à solution à check Hard Disk (df -h) to check if there is any full partition, if there is not full partition $ iostat command to monitor HDD utilization, another command is $ iometer (need to install) à the vendor to be contacted – to check RAID.
11. If there is no issue with HDD then check Network à if there is an application which is broadcasting too much à this can cause high CPU utilization à solution to check network load à commands are,

Tcpdump

Ipref

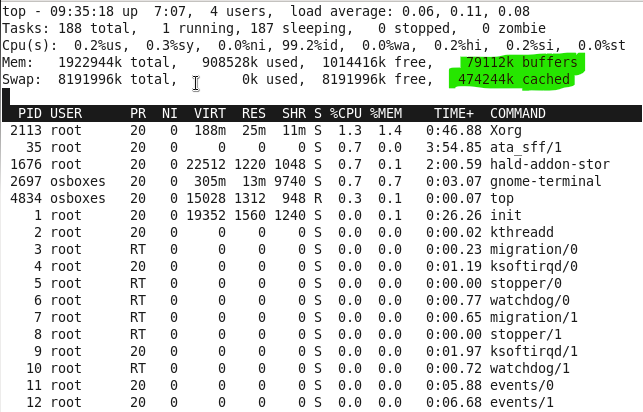
Nmon

Wireshark

**Sar à** great tool ( nw, HDD, Memory and CUP)

1. **Answer of 2nd question à IO** utilization od HDD if its clear à NW utilization will be checked by tools mentioned above.

Same scenario 3rd Question -à high server utilization

* Solution à
  + TOP command à idle value, Mem and SWAP, application (check)
  + The HDD and NW will be checked as mentioned above.
  + $ ps -aux | less à can also be used to monitor the performance as TOP
  + 3rd case à we will check buffer and Cached
  + 
  + Buffer à in RAM à high value means high load à
  + Cache à SWAP (HDD) à high value means high load à
  + What is buffer?
    - 
    - The gray area is “buffer” it is the data written in RAM for smooth viewing of a youtube video. à pre-loaded process in RAM / Memory
    - A buffer is a region of memory used to store temporary data. It acts as a holding area for data being transferred between devices or processing stages. The purpose of a buffer is to smooth out data flow and ensure that data is not lost or corrupted during the transfer.

Buffers are commonly used in computer systems and networks to improve performance and prevent data loss.

There are different types of buffers, including data buffers, input/output buffers, and memory buffers. Data buffers are used to store data temporarily before it is processed, while I/O buffers are used to manage data transfer between the computer and peripheral devices. Memory buffers are used to store data in a temporary location within memory, allowing multiple processing stages to access the data without interfering with each other.

* What is “cache”?
  + Temporary data in HDD. To speedup up the repeated data. It can be cleared à

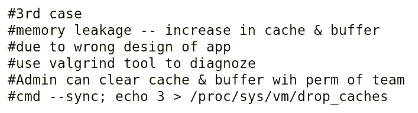
Cache is a type of fast memory that stores frequently accessed data. The purpose of cache is to provide quick access to data that the processor is likely to need next, improving overall system performance by reducing the number of slower disk accesses.

Cache memory is typically located between the CPU and main memory, and it is much smaller and faster than main memory. When the CPU requests data, it first checks the cache to see if the data is stored there. If it is, the data is retrieved from cache, which is much faster than retrieving it from main memory.

There are different types of cache, including L1 cache, L2 cache, and L3 cache, which refer to the levels of cache memory that exist within a computer system. There are also different types of cache in the context of software, such as web browser cache, which stores frequently accessed web pages and resources.

Cache is an important component of computer systems, as it helps improve system performance by storing frequently accessed data in a fast, accessible location.

The reason behind increased buffer and cache à due to memory leakage.

* Wrongly designed application cause memory leakage à the application allocates memory but do not dis-allocate which causes full memory.
* Tool to detect memory leakage à valgrind à mostly used by developers
* As admin Linux Administrator can clear buffer and cache à to cleat à
  + Top command à à before this it is recommended to use $ sync: echo 3 > /proc/sys/vm/drop\_caches
  + 

4th case / scenario

Server is in high load,

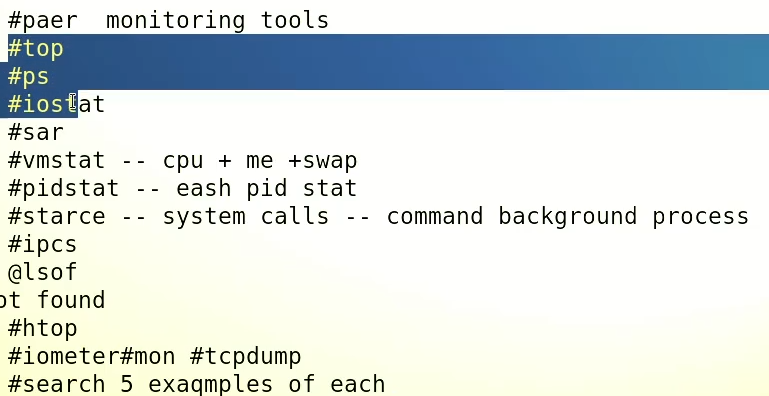
TOP and ps -aux à CPU idle à load à mem utilization à SWAp utilization à applications process (if utilization is high)

à $ iostat à $tcpdump (for NW utilization) à sar command

à buffer and cache à $ sync: echo 3 > /proc/sys/vm/drop\_caches

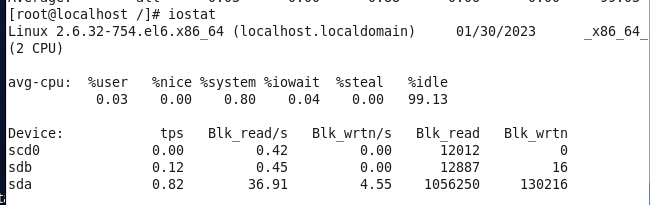
If server is still slow,

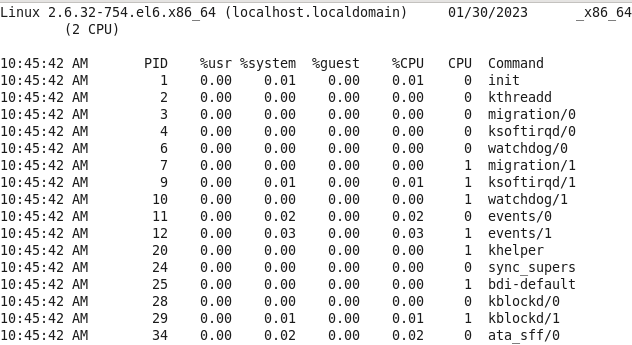
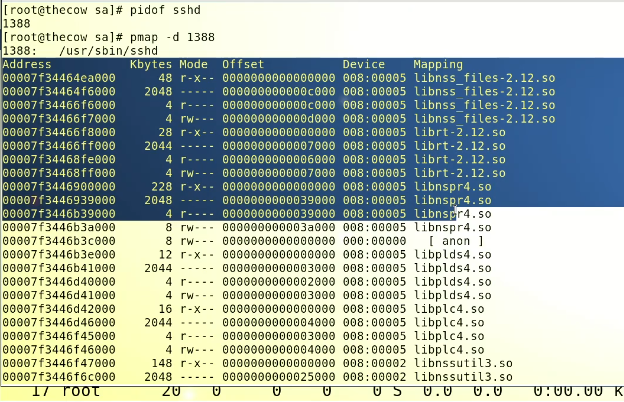
* Faulty hardware à Management console
* RAM à $ memtest
* CPU over clocking ?
* To check faulty HW à tool i7z
* CPU temperature tool



**5th case à high server utilization**

**$ iostat à** The "iostat" command in Linux is used to monitor system I/O (input/output) activity.

* ****
* Flags $ iostat -x -d -p
* Table

  Description automatically generated with medium confidence
* $ iostat -x -d -p 2 3 à displays 3 outputs after every 2 sec
* Further à the process which is utilization a specific partition can be monitored.
* Tip:- to take output in a file
* **$ iostat -x -d -p 2 > /opt/31012023\_iostat\_output.txt**
* At leat 5 examples of ps command à
* $ pidstat à live performance monitoring à PID statistics
* 
* $ mpstat à CPU monitoring
* $ vmstat à cache, buffer, swap, CPU monitoring
* $ sar à NW, CPU, HDD System statistics utility à **generates report in backend à where the report is saved à /var/log/sa (interview question)**
* Check sar command utilization in geeksforgeeks.com
* # pmap à process ID details
* 
* $ strace à system calls and signals
* strace is a Linux utility that is used to trace system calls and signals of a given command. It provides information about the interactions between a process and the Linux kernel, including system calls, signals, and other inputs/outputs. Strace can be used to debug and monitor the behavior of a program, troubleshoot system errors, and examine the performance of a system.
* What is happening behind every command. Strace is the answer.