Q1. Explain the output of vmstat command



Ans: <https://phoenixnap.com/kb/vmstat-command#:~:text=The%20vmstat%20command%20(short%20for,by%20specifying%20a%20sampling%20period>.

<https://www.tecmint.com/linux-process-management/>

Q2. Which HTTP method is commonly used to send the data to the server-

Ans: POST, the reason is POST method send the requested data appending with the body of the HTTP request rather than the page URL and hence there is no restriction in the data length.

GET, always append the data in the URL of the webpage itself and hence there is a length limitation in the URL.

Q3. Which algorithms are being used for SSL certificates?

Ans: AES-128, AES-256

Text

Description automatically generated

Q4. Why is VIRT is higher than RES?

* This field is in the top command

Text

Description automatically generated

* This field is in the ps command **RSS** vs **VSZ**

**RSS:** - resident set size (Current memory using by a process based on the current load at any point in time)

**VSZ:** - virtual memory size (Total virtual memory is being allocated by a greedy process, the process tells OS that I need this much of memory, please allocate this to me)



Shape

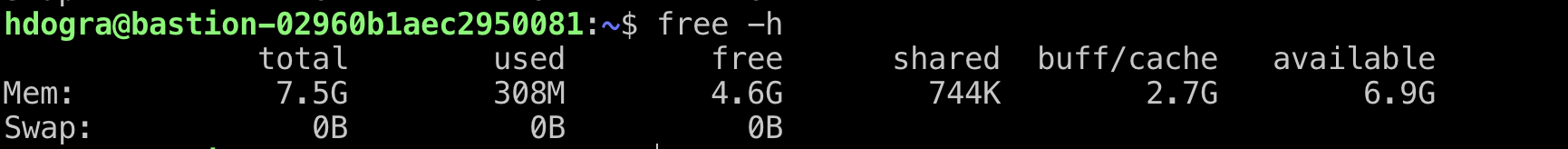
Description automatically generated with low confidence

Ex: Let’s sum up the VSZ which should always be > than the actual physical RAM attached to motherboard of a system

hdogra@bastion-02960b1aec2950081:~$ ps axo vsz | sort | uniq | grep -v "VSZ" | awk '{s+=$1} END {printf "%.0f", s }'

**8405904(KB) ~ 8 GB**

**Actual Ram:**



So total VSZ (8GB) > Physical RAM (7.5GB)

VSZ is never going to increase but RSS can increase depending on the load on the process.

Shape

Description automatically generated

**SHR:** - The shared memory which is being used by multiple processes. So if you calculate the sum if will be much more than VSZ

Q5. How does TLS 3-way handshake work?

<https://www.geeksforgeeks.org/tcp-3-way-handshake-process/?ref=gcse>

Q6. What are the layers of an OSI model?

<https://www.geeksforgeeks.org/layers-of-osi-model/?ref=leftbar-rightbar>

Q7. How does IAM chaining work?

Q8. What are Cgroups in Kubernetes?

Q9. Through the VPC peer, if the DNS name resolution is not happening from a Instance in VPC1 to another Instance in the VPC2 what could be the cause of it?

* The DNS hosted zone is not enabled in the VPC peering configuration and hence that has to be added through the cli as GUI option is not enabled.

Q10. How does traceroute work?

Q11. How does DHCP work?

D -> DHCP Discovery

O -> Offer an IP address

R -> by client gratuitous ARP is performed to avoid IP conflicts and request DHCP to request that IP for assignment

A -> Acknowledgement of the request send by the client from the server.

<https://www.geeksforgeeks.org/dynamic-host-configuration-protocol-dhcp/>

Q12. How does gorilla encoding works?

Q13. Difference b/w ENTRYPOINT and CMD in docker

**ENTRYPOINT** – It could be a script name usually present in the DOCKERFILE.

**CMD** – command line arguments passing in the script.

Q14. On a host machine how to identify which container is consuming more disk space?

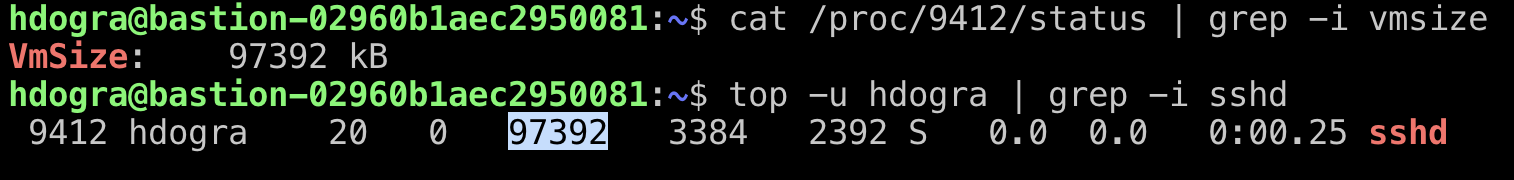
Q15. How will you define the load avg in the Linux machine?

<https://scoutapm.com/blog/understanding-load-averages>

Q16. How does internet work/HTTP protocol/SMTP protocol?

<https://web.stanford.edu/class/msande91si/www-spr04/readings/week1/InternetWhitepaper.htm>

Q17. Speak on /proc for 3 mins.

* It is a live file system storing process status and many more things.
* 
* Here, we see the VIRT, VSZ size stored in the /proc/<pid>/status
* We can add the kernel variables that will drop all ping packets.



Q18. How to filter out processes based on CPU% or mem%

In htop sorting is there by pressing F5

A screenshot of a computer

Description automatically generated with medium confidence

Q19. Total no of Signals available in the linux system?

31

Graphical user interface

Description automatically generated

SIGINT(2) – (ctrl+c) it’s just an interruption send by the user to the process

SIGQUIT(3), SIGTERM(15) does terminate the process by gracefully and generate a core dump for debugging

SIGKILL(9) it is needed when a process is hung then it may not respond any of the above signals and to kill that process we use SIGKILL

<https://www.baeldung.com/linux/sigint-and-other-termination-signals>

Q20. What is the zombie process and how to prevent it?

<https://www.geeksforgeeks.org/zombie-processes-prevention/?ref=gcse>

<https://www.youtube.com/watch?v=taNzTCO-k3U&ab_channel=iFocusInstitute>

Q21. What is the NICE time in the CPU utilization

<https://stackoverflow.com/questions/26154098/understand-what-is-using-up-nice-cpu#:~:text=On%20a%20CPU%20graph%20NICE,will%20show%20up%20as%20NICE>.

Q22. What happens when you enter a command in linux shell?

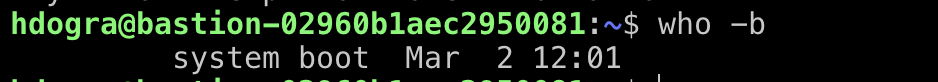
Fork-and-exec process gets executed. Fork() process is to copy the shell itself to another instance and exec() process to execute the actual command passed on.

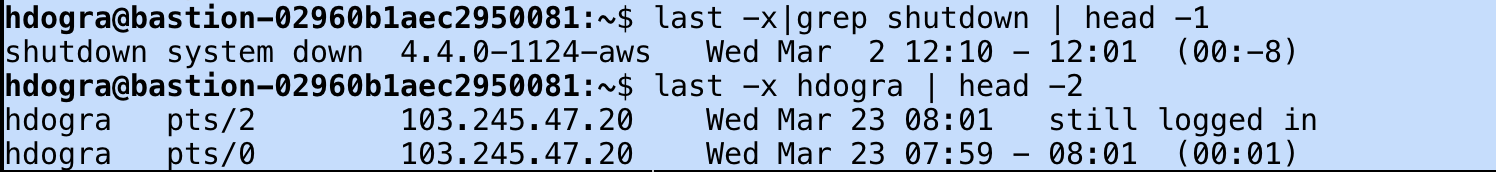
<https://www.makeuseof.com/what-happens-when-you-run-command-linux/#:~:text=When%20you%20enter%20a%20command,token%20in%20the%20command%20line>.

Q23. How to identify the when was the last reboot happened?

last or who commands help







Also file /var/log/wtmp store the last reboot information.

Text

Description automatically generated with medium confidence

/var/log/utmp – tells users logged in at which terminal, logout, system events and uptime(etc)

/var/log/wtmp – gives historic data dump of utmp

/var/log/btmp – failed login attempts

Table

Description automatically generated

Q24. Data structure algorithm & time complexity?

<https://www.educative.io/blog/data-structures-algorithms>

<https://www.geeksforgeeks.org/practice-questions-time-complexity-analysis/>

Q25. How does subnetting work?

<https://www.auvik.com/franklyit/blog/subnetting-primer/#:~:text=A%20subnet%20is%20just%20a,has%20only%20one%20IP%20address>.

Q26. Why DNS uses UDP over TCP?

<https://www.geeksforgeeks.org/why-does-dns-use-udp-and-not-tcp/>

Q27. HTTPS working, tcp and SSL handshake?

<https://community.spiceworks.com/topic/2304867-difference-between-tcp-3-way-handshake-vs-ssl-handshake>

<https://www.mysoftkey.com/security/4-phases-of-ssl-protocol/>

Q28. HTTP status code?

<https://www.geeksforgeeks.org/servlet-http-status-codes/>

Q29. Why do we need LB in front of our application servers?

* Fundamentally, the application servers Ips keep on changing as if they containers then keep on crashing or using DHCP servers etc. but LB have static IP and hostname which helps internet users to reach out to that and they will forward the request internally.
* ALB can perform SSL termination which NLB can’t.

Q30. Difference b/w ALB and NLB?

<https://medium.com/awesome-cloud/aws-difference-between-application-load-balancer-and-network-load-balancer-cb8b6cd296a4#:~:text=NLB%20just%20forward%20requests%20whereas,assure%20availability%20of%20the%20application>.

Q31. Difference b/w session/cookies in HTTP?

Session: - Stores at the server side in an $\_session array until client closes the browser connection.

* Before storing the user information locally at webserver, session\_start() method has to be executed.
* This also has session\_destroy() method to erase all the saved user’s information.

Cookies: - Stores at client side browser with max of 4 KB file.

* Contains the personalized information of the user such as session ID, user preferences etc.
* This helps web services to show the advertisements/personalized contents of the user’s choices.
* Since http is stateless, cookies helps to keep a track the state of application.

<https://www.guru99.com/difference-between-cookie-session.html>

<https://www.bitspedia.com/2012/05/how-session-works-in-web-applications.html>

**IMPORTANT:**

HTTP/1.0 – Needs a new connection for each request/response.

HTTP/1.1 – Can server multiple requests in a single TCP connection. (Persistent connection/pipeline connections)

<https://stackoverflow.com/questions/246859/http-1-0-vs-1-1>

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Connection_management_in_HTTP_1.x>

<https://www.tutorialspoint.com/http/http_overview.htm>

Q32. How to perform the n/w latency troubleshooting?

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated with medium confidence

<https://www.geeksforgeeks.org/ping-command-in-linux-with-examples/>

* Prefer to use application delivery controllers (ADC) which also providing Load Balancing. This acts as a gateway with the use of specialized hardware to accelerate SSL encryption & SSL decryption. As an outcome ADC reduces the processing loads on the web servers.

<https://www.a10networks.com/glossary/what-is-ssl-offloading/#:~:text=The%20SSL%20Offloading%20Advantage&text=Because%20application%20delivery%20controllers%20are,it%20also%20decreases%20network%20latency>.

* The latency can cause due to the physical distance from client <-> server, hence better to use CDN instead of just origin server.

Q33. What is garbage collection, how to take heapdumps?

Q34. How does MTR work?

* It is a combination of both ping and traceroute.
* First, it probes the n/w connections b/w local machine and remote host you specified in the command.
* Then it establishes the address of each hop (routers, gateways, bridges etc.)
* Then pings (sends a sequence ICMP ECHO requests to) to each one to determine the quality of link to each machine.

<https://www.tecmint.com/mtr-a-network-diagnostic-tool-for-linux/>

Q35. Shared based troubleshooting

<https://opster.com/analysis/elasticsearch-failed-to-start-shard/>

<https://www.guru99.com/elasticsearch-interview-questions.html>

Q36. What is cross site scripting and how to prevent it?

Prevention: - <https://portswigger.net/web-security/cross-site-scripting/content-security-policy>

* use content security policy response header with defining the directives like script-src; media-src; img-src
* script-src could use nonce and hash directives to enable security.
* Nonce is a random number value, which is used by the tag that loads the script, which is being generated a new value every time a new page load.
* Hash checks if there is any modification in the script if yes then it doesn’t load that script.

Graphical user interface, text, application, email

Description automatically generated

Definition and Types: - <https://portswigger.net/web-security/cross-site-scripting>

Q37. Linux Memory Management?

<https://www.geeksforgeeks.org/memory-management-in-operating-system/>