Uname : displays OS name

Uname –r : Kernel version

Uname –i : Architecture

Uname –a : all

Compress : Gzip ,BZip UnCompress : GUnZip,BUnZip

Tar : Tape archive(combine multiple files in to single file)

Tar xvfz(Extracting),tvfz(Table of contents),czvf,cjvf(zip)

Sort : To sort the file content.by default ASC order (sort filename)

Sort –u filename(remove duplicate values)

Sed : serach and replace the string /patterns in the file

# sed “s/Replacing word/Replaced word/gi”

Grep : used to searching a pattern in a given file.

Grep –v root test(Not matching lines)

Grep –n root test(find the line numbers)

Grep –c root test(count the line with root)

Grep ^root test(line start with root)

Grep bash$ test(line with ending bash)

Pipe : logical linking b/n commands

Tee : to write the data in to the new files

Find : searching the resources based on name,size,time,permissions

Find /etc –size +-10mb

Find /etc –mtime +5 (modified for the last 5 days)

Find /etc –ctime /-mtime/-atime

Find /etc –cmin +60/-amin +60 / -amin +60 (minutes only)

Chmod : change mode

Chgrp : change group

Chown : change owner

Link : to give a pointer from the source file

Soft link : short cut

Inode no of source and link files are different ,if source file is deleted cannot accessed it

Can create the across file system

Hard Link : Back up file

Inode no of source and link files are same.can create in same drive only,cannot create for directory.

VI :

^ : beginning of current line

$ : ending of current line

G : cursor move to last line of file

Gg : cursor move to first line of file

5 yy : copy the current line

P : paste the line below cursor line

P : paste the line above cursor line

U : undo changes

Dd : delete lines 5dd,10dd

:se nu : arrange line numbers

:3 : cursor goes to the 3rd line

:3d : delete 3rd line

Cron tab : one job execute 2 or more times

Minutes Hours Dayofmonth Month Dayofweek command

FQDN : Hostname + Domain name

/etc/hostname : make hostname permanently

Manage IP Address :

1. With file /etc/sysconfig/network-scripts/ifcfg-eth0
2. setup

/etc/hosts : Maintain hostname to IP and IP to hostname

Nslookup : particular domain info

Dig : used for Linux only

Ethtool : Lan card is attached or detached ethtool eth0

Netstat : Displays TCP and UDP details .To find out the port no’s

Password Less Login:

---------------------------

1. run ssh-keygen at client location
2. Go to /root/.ssh location
3. Copy public key in to remote location #ssh-copy-id /root/.ssh/id\_rsa.pub root@IP
4. Server has authorized keys created at .ssh location

Command line arg’s / Positional parameters : At the time of execution passing args

Set : to set the positional parameters

Shift : shift to positional parameter

Sh –n sc.sh(show/verify syntax)

Sh –x sc.sh(execution trace)

AWS

-----

IAM : securely control access to aws services and resources for your users.It is global

Policies : it is a document, states that one or more permission ,By default explicit deny overwrites explicit allow

Create custom policy using Policy generator

Role : It is an IAM entity. Defines set of permissions for making aws service requests.

Instance Store block volume : Ephemeral data, data in volumes exists only until the instance is running else if stooped/shutdown it never exists

Elastic block store volume : persistent block storage .HA

Volume types :

--------------------

Standard(Basic) 1GB to 1 TB

SSD(Solid state drive)(transactional work load)

GP2(frequent access)1gb to 16tb

Provisioned iops(4gb to 16tb)

HDD(Harddisk drive)(Streaming work load)

Throughput optimized

Cold hdd

Snapshot : point in time backup for ebs volumes that are stored in s3.Incremental in nature.

Glacier : archive – valut

S3 : object storage with simple web service to store and retrieve data.HA and durability(99.99999999)

Stored in bucket

Standard,standard IA,reduced redundancy,glacier

Suspend versioning

LINUX

======

Partitioning means to divide a single hard drive into many logical drives.

file system in order to make them to store the data. File system is applied on the partition by formatting it with a particular type of file system

Attaching a directory to the file system in order to access the partition and it's file system is known as mounting.

/etc/fstab entries are:

1 2 3 4 5 6

device name mount point file system type mount options take a backup should run

or not fsck or not

**create different types of partitions**

fdisk -l

fdisk /dev/sdc

(8e LVM,82 swap,83 partiiton)

Partprobe partx (Update partition info in table)

Mkfs.ext2 /dev/sdc

Mkdir mnt/filesys

Mount /dev/sdc /mnt/filesys

/etc/fstab

Mount –a

**Trouble Shoots**

=============

**When trying to unmounting it is not unmounting, how to troubleshoot this one?**

(i) you are in the same directory and trying to unmount it, check with **# pwd**command.

(ii) some users are present or accessing the same directory and using the contents in it, check this with

# fuser -cu <device name> (to check the users who are accessing that partition)

# lsof <device name> (to check the files which are open in that mount point)

# fuser -ck <opened file name with path> (to kill that opened files)

**How to recover if a file system is corrupted or crashed?**

If the normal or not related to O/S file system is corrupted first unmount that file system and run **fsck** command on that file system and if the O/S related file system is corrupted then boot the system with CDROM in single user mode and run the **fsck** command.

If the normal or not related to O/S file system is crashed then restore it from the recent backup and if the O/S related file system is crashed then boot the system with CDROM in single user mode and restore it from the recent backup.

**How will you troubleshoot if one of the eight disks failed in LVM?**

First umount the file system and add the new disk with same size of the failed disk to the volume group. Then move the data from failed physical volume to newly added physical volume and then remove the failed physical volume from the volume group. And finally mount the file system.

**How to inform the client and then troubleshoot if the disk is full?**

First check which files are accessing more disk space by **#du -h |sort - r** command. if any temporary and junk files are present remove them from the disk to make a room for new or updated data. Then inform the actual situation to the client, take the permission from the client to get the lun from storage and extend the file system by adding that lun to the LVM.

**How to recover the root password if missed or deleted?**

**RHEL - 6 :**

(i) Restart the system.

(ii) Select 1st option and press 'e'.

(iii) Select 2nd option and press 'e'.

(iv) At the end give one blank space and type 1 and press Enter key.

(v) Then press 'b' to boot the system in single user mode.

(vi) Then prompt appears and type **# passwd root** command.

New password : XXXXXX

Retype password : XXXXXX

(vii) Exit

(viii) Then system starts as usual.

**How to troubleshoot if the network is not reaching?**

(i) First check the network cable is connected or not by **# ethtool <NIC device name>** command. if connected then check the IP address is assigned or not by **# ifconfig <NIC device name>** command.

(ii) Then check the system uptime by **# uptime** command.

(iii) Then check the network services status by **# service network status** and **# service NetworkManager status** commands.

(iv) Then check the network service at Run Level by **# Chkconfig --list network** command.

(v) Then check whether the source network and destination network are in the same domain or not.

(v) Then finally check the routing table by **# route -n** command.

**How to troubleshoot if the cron job failed?**

(i) See the crontab entries for syntactical errors. If there are any errors then correct them, otherwise it will not execute.

(ii) Check whether the **crond** deamon is working or not. If it is running, then stop the deamon and again start the deamon. Even though the problem occurs, then the crontab entries may be wrong.

(iii) If all the above are ok, then see whether the user who executing cron job has permissions to execute the cron jobs or not ie., check the user entries in **/etc/cron.allow** and **/etc/cron.deny** files.

(iv) If all are ok, again put the job entry in crontab and execute it.

|  |  |
| --- | --- |
| **Telnet** | **SSH** |
| (a) Through telnet we can connect the remote  system, but any network hacker may see the  transferred data. And the telnet port no. is **23.** | (a) Through ssh also we can connect the remote  system, but nobody can see the transferred data.  And the ssh port no. is **22.** |
| (b) Data will be transferred in non-encrypted format. | (b) Data will be transferred in encrypted format. |
| (c) We cannot trust this telnet connection. | (c) We can trust this ssh connection. |
| (d) We cannot give the trusting in telnet. | (d) We can give the trusting in ssh. |
| (e) By snooping or sniffing technologies we can see  the data like system or hostname, login name,  password and other data.  So, there is no security. | (e) By snooping or sniffing technologies we cannot  see the data like system name or hostname, login  name, password and other data.  So, there is a security |
| (f) # telnet<IP address of the remote system>  (provide login name and password) | (f) # ssh<IP address of the remote system>  (provide login name and password) |

# nmap -p 22 <IP address of the remote host> (to see the ssh is running or not on remote system)

**How to reboot the production server?**

(i) In general the production servers will not be rebooted frequently because the end users will suffer if the productions server are in down state. If any changes made to the system like grub, selinux policy, default run level is changed and if kernel patches are applied the system reboot is required.

(ii) If any inconsistency is root ( / ) file system, then take the business approval from higher authorities,make a plan for proper scheduleand also inform to the different teams like application team to stop the application, databaseteam to stop the databases, QC team to stop the testing, monitoring people to ignore the alerts from thisserver and other teams if any and then reboot the system withCDROM in single user mode and then run **#fsck** command on that file system.

(iii) If O/S disk is corrupted or damaged then, reboot the system temporarily with the mirror disk then fix that problem and again boot the system with original disk.

The drivers is Linux system are known as Modules or Kernel Modules.

we can find the kernel modules by **# ls /etc/lib/modules** command.

# modprobe <module name> (to install or re-install the module)

**What is** " **wait** " **and where it is stored?**

(i) If there is not enough memory to run the process, then it will wait for free space in memory. That process is called wait.

(ii) wait is stored in buffer like cache memory.

The process of creating the jobs and make them occur on the system repeatedly hourly, daily, weekly, monthly and yearly is called Job scheduling

scp means secured copy to copy the files or directories from local system to remote system

**rsync** is a very good program for backing up or mirroring a directory tree of files from one machine to another machine and for keeping the two machines " **in sync** ".

If **rsync** is combined with ssh, it makes a great utility to sync the data securely otherwise by sniffing any one can see our data ie., no security for our data.

rpm -qa <package name> (to check whether the package is installed or not)

# rpm -qp --changelog <package name> (displays all the changed logs like lat time, when the package is installed, .....etc.,)

dump is a command used to take a backup of file systems only.

# dump <options><destination file name><source file name>(to take a backup of the file systems)

# restore <options><dump backup file> (to restore the backup contents if that data is lost)

There are mainly three types of backups available.

(i) Full backup (Entire file system backup)

(ii) Incremental backup (backup from the last full backup or incremental backup)

(iii) Cumulative or differential backup (backup from last full backup or cumulative backup)

Backups can be taken in types.

(a) Application Backup (Normally application users will take these types of backups)

(b) File system Backup (O/S backup, System Administrators will take these types of backups)

(c) Database Backup (DBA users will take these types of backups)

A process is a set of instructions which executes in the memory.

# ps -aux

(it displays all the terminals processes information including background processes with user names)

# ps -ef (it displays the total processes information with parent process ID (PPID))

# ps -aux |grep firefox (to check whether the firefox is running or not)

Zombie process (the process which is running without child process and is indicated by " **Z** " ).

Orphan process (the process which is running without parent process and is indicated by " **o "** ).

# nice -n <nice value range from -20 to 19><command> (to set a priority to a process before starting it)

**top** is a command to see the processes states and statuses information continuously until we quit by pressing " **q**

# vmstat is the command to the complete information on virtual memory like no of processes, memory usage, paging memory, block I/O (input /output), traps, disk and CPU activity.

# vmstat 2 10 (It will give the report for every 2 seconds upto 10 times)

# cat /proc/meminfo (to see the present memory information)

# iostat (to see the Input and Output statistics in the Linux system)

**# cat /proc/cpuinfo** command will show no. of CPUs, no. of cores, no. of threads, no. of sockets and the CPU architecture, ...etc., information.

**# uptime** is the command to check the system load, present time, from how many hours the system is running and load average.

\* The load average shows three fields. The 1st field shows the load average from 1 minute, 2nd field shows the load average from 5 minutes and 3rd field shows the load average from 15 minutes.

**# tcpdump** is the command to capture and analyze the network traffic. By using this command we can also troubleshoot the network problems.

SAR stands for System Activity Report. Using SAR we can check the information of CPU usage, memory, swap, I/O, disk I/O, networking and paging. We can get the information of the present status and post status (history using the data) upto last 7 days because **HISTORY=7** is there in the configuration file.

# sar -p 2 10 (to see the CPU utilization for every 2 seconds upto 10 times)

# sar -r 2 10 (to see the memory utilization for every 2 seconds upto 10 times)

# sar -S 2 10 (to see the swap utilization for every 2 seconds upto 10 times)

# sar -q 2 10 (to see the load average for every 2 seconds upto 10 times)

# sar -d 2 10 (to see the disk usage for every 2 seconds upto 10 times)

# sar -m 2 10 (to see the power management for every 2 seconds upto 10 times)

# sar -b 2 10 (to see the disk input and output statistics for every 2 seconds upto 10 times)

# nproc (to check how many processors (CPUs) are there in the system)

# cat /etc/redhat-release (to see the RHEL version of system)

# dmidecode (to see the complete hardware information of the system)

# dmidecode -t memory (to see the memory information of the system)

# dmidecode -t bios (to see the system's bios information)

# dmidecode -t system (to see the system's information)

# dmidecode -t processor to see the processor's (CPU's) information of the system)

# sleep <seconds>& (to run the sleep processes at background)

# hostname (to see the hostname with fully qualified domain name)

# hostname -i (to see the IP address of the system)

# hostname -d (to check the domain name of the system)

# hostname -s (to check the hostname without domain name)

# netstat -r (to check the default gateway and routing table)

# route (to check the default gateway with routing table)

# netstat -ntulp (to check how many open ports are there in local system)

# ss -ntulp ( " " )

# nmap (to check how many open ports are there in remote system)

# tracepath (it displays the routing information)

# route -n (to check the gateway)

# ls /etc/init.d (is the location of all the services and deamons in RHEL - 6)

# ls /usr/lib/systemd/system (is the location of all the services and deamons in RHEL - 7)

# /etc/rc.local (is the last script to be run when the system is booting)

# netstat -ntulp (to see all the services with port no., status, process ID and all open ports in local system, routing table and NIC device information)

-n -----> port no. (numeric no) -t ----->tcp protocol

-u -----> upd protocol -l -----> port is listening or not

-p -----> display the process ID

# netstat -r (to see all routing table information)

# nmap (to see the network mapping ie., open ports list on remote system)

# nmap -p 80 <remote IP>

(to see the http port is running or not on specified remote system)

SELinux : It is mainly used to protect internal data (not from external data) from system services.

Enforcing means SELinux is on

Profile is a file to enter some settings about users working environment.

Using Access Control list we assign the permissions to some particular users to access the files and directories.

* Create a partition and format it with ext4 file system.
* Mount the file system with ACL.
* Apply ACL on it.
* **check the ACL permissions?**# getfac
* **to assign ACL permissions?**
* # setfacl <options><argument> : <username>: <permissions><file or directory name>

# faillog -u <user name> (to see the specified users failed login attempts)

# faillog -a (to see failed login attempts of all users)

**How will you lock a user, if he enters wrong password 3 times?**

pam\_tally.so module maintains a count of attempted accesses, can reset count on success, can deny access if too many attempts fail. Edit /etc/pam.d/system-auth file

**auth required pam\_tally.so no\_magic\_root  
account required pam\_tally.so deny=3 no\_magic\_root lock\_time=180**

By configuring the disk quotas we can restrict the user to use unlimited space on the file system

|  |  |
| --- | --- |
| TCP/IP | UDP |
| Transmission Control Protocol | User Datagram Protocol |
| It is connection oriented | It is connection less |
| Reliable | Non-Reliable |
| TCP Acknowledgement will be sent / received | No Acknowledgement |
| Slow communication | Fast communication |
| Protocol No. for TCP is 6 | Protocol No. for UDP is 17 |
| HTTP, FTP, SMTP, ....etc., uses TCP | DNS, DHCP, ....etc., uses UDP |

Every Computer will be assigned an IP address to identify each one to communicate in the network. The IP address sub components are Classes of an IP address, Subnet masks and Gateway.127.0.0.0 and 127.255.255.255 is also reserved for loopback and is used for internal testing on local machines.

A subnet mask allows the users to identify which part of an IP address is reserved for the network and which part is available for host use.

A Gateway is the network point that provides entrance into another network.

**/etc/resolve.conf** is the file which contains DNS server IP and domain name location.

**Bonding or Teaming or Bridging:**

Collection of multiple NIC cards and make them as single connection (virtual) NIC card is called bonding.

(a) Mode 0 -----> Round Robbin

* It provides load balancing and fault tolerance.

(b) Mode 1 -----> Activebackup

* if one NIC card is failed then another NIC card will be activated automatically.No load balancing.

(c) Mode 3 -----> Broadcasting

* the same data will be transferred through two NIC cards.

**command to check all the open ports of your machine?**#nmap localhost

**to check all the open ports of remote machine?**# nmap <IP address or hostname of the remote system>  
**to check all the listening ports and services of your machine?#**netstat –ntulp

**you make a service run automatically after boot?#** chkconfig <service name> on

# find / -mmin 20

(to search for files/directories which are modified within 20 minutes, +20 ----> above 20 minutes and -20 -----> below 20 minutes)

* User names and user id are stored in **/etc/passwd** file.
* User's passwords are stored in  **/etc/shadow** file in an encrypted form.

# id <user name> (It shows the user id group id and user name if that is already created)

locate always looks the locate database and not in a specific location.

# fdisk -l (to see how many disk are attached to the system)

**Journaling:**

It is a dedicated area in the file system where all the changes are tracked when the system crashed.

# tune2fs -l /dev/sdb1 (to check whether the journaling is there or not)

# tune2fs -j /dev/sdb1 (to convert ext2 file system to ext3 file system)

# df -hT (to see device name, file system type, size, used, available size, use% and mount point)

# du -h <filename or directory name> (to see the size of the file or all the file sizes in that directory)

(i) If the size of the RAM is less than or equal to 2GB, then the size of the swap = 2 X RAM size.

(ii) If the size of the RAM is more than 2GB, then the size of the swap = 2GB + RAM size.

# free -m (to see the present swap size)

# swapon -s (to see the swap usage)

# mkswap <device or partition name> (to format the partition with swap file system)

Inode numbers are the objects the Linux O/S uses to record the information about the file.

the **# fsck <device or partition name>**command we can check the integrity of the file system.

# journalctl (It tracks all the log files between two different timings and by default saved in **/run/log** location)

# journalctl -n 5 (to display last five lines of all the log files)

# journalctl -p err (to display all the error messages)

# journalctl -f (to watch journalctl messages continuously)

# journalctl --since<today> or <yesterday> (to see all the journalctl messages since today or yesterday)

# journalctl --since "date" --until "date" (to see the journal messages between the specified two dates)

# sar (sar utility is to watch the system activity report like CPU, memory,...etc.,)

this LVM we can extend or reduce the file systems as per requirement without loss of any data.

* Physical Volume (PV)
* Physical Extent (PE)
* Volume Group (VG)
* Logical Volume (LV)
* Logical Extent (LE)
* Increase the size of the logical volume by **# lvextend or # lvresize** commands.
* Then finally update the file system by **# resize2fs or # xfs\_growfs** commands.

# mount <pen drive name><mount point>

* ( to mount the pen drive on the above created mount point)

# mount -t iso9660 /root/rhel6.iso /iso -o ro, loop (to mount the .iso image files)

RAID : It provides fault tolerance, load balancing using stripping, mirroring and parity concepts.

(i) RAID - 0 ---- Stripping ---- Minimum 2 disks required

(ii) RAID - 1 ---- Mirroring ---- Minimum 2 disks required

(iii) RAID - (1+0) --- Mirroring + Stripping ---- Minimum 4 disks required

(iv) RAID - (0+1) --- Stripping + Mirroring ---- Minimum 4 disks required

(v) RAID - 5 ---- Stripping with parity ---- Minimum 3 disks required

**How to recover if the user deleted by mistake?**

**# pwunconv** (It creates the users according **/etc/passwd** file and deletes the **/etc/shadow** file)

**How to create the duplicate root user?**

# useradd -o -u 0 -g root <user name>

**.bash\_profile :** This is user's login startup program file. It will execute first whenever the user is login. It consists the user's environmental variables.

**.bashrc :** This file is used to create the user's custom commands and to specify the umask values for that user's only.

**How add 45 days to the current system date?**

# date -d "+ 45 days"

# w (this command gives the login user information like how many users currently login and their processes)

# who (to see users who are currently login and on which terminal they login)

# last -x (It shows last shutdown date and time)

# date + %R (to display the time only)

# date + %x (to display the date only)

The user file-creation mode mask (umask) is used to determine the file permissions for newly created files or directories. The umask value for normal user is **0002** and the umask value for root user is **0022.**

**sticky bit?**

It protects the data from other users when all the users having full permissions on one directory.

In Linux systems the booting is done in 6 stages.

* BIOS
* MBR
* GRUB
* Kernel
* Init
* Runlevel
* 0 -----> halt or shutdown the system
* 1 -----> Single user mode
* 2 -----> Multi user without NFS
* 3 -----> Full multi user mode but no GUI and only CLI mode
* 4 -----> Unused
* 5 -----> Full multi user mode with GUI (X11 system)
* 6 -----> reboot the system

DNS stands for Domain Naming System. The **DNS**translates Internet domain and host names to [IP addresses](http://compnetworking.about.com/od/workingwithipaddresses/g/ip-addresses.htm).

A Web server is a system that delivers content or services to end users over the Internet.

Take a backup of the database.

**# mysqldump -u root -p <database name>><file name with full path>**

IP tables is a command-line firewall utility that uses policy chains to allow or block traffic.

# iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT

# iptables -A OUTPUT -p icmp --icmp-type echo-reply -j ACCEPT

# service iptables start (to start the IP tables)

# service iptables stop (to stop the IP tables)

# iptables -A INPUT -i eth0 -p tcp --deport 22 -j ACCEPT (to add the rules to the existing iptables to allow ssh)

where -A ---> Add or append a rule to the INPUT chain for incoming traffic.

# iptables -A INPUT -s 9.9.9.9 -j DROP (to block the 9.9.9.9 input traffic)

# iptables -L (to see the list of the IP tables)

# watch -d -n 5 free (to repeat a free command for every 5 seconds)

**server hardening?**

(i) To checking our system is reaching to standards required by the organization.

**How to troubleshoot if the file system is full?**

(i) First check whether the file system is O/S or other than O/S.

(ii) If it is other than O/S, then inform to that respective teams to house keep the file system (ie., remove the unnecessary files in those file system).

(iii) If not possible to house keep then inform to different teams (raise the CRQ (Change Request)) for increasing the file system.

(a) First take business approval and raise the CRQ to monitoring team to ignore the alerts from the system, stop the application team to stop the application and database team to stop the database.

(b) Normally team lead or tech lead or manager will do this by initiate the mail thread.

(c) We will do this on weekend to reduce the business impact.

(iv) First take a backup of the file system then unmount the file system.

(v) Remove that partition and again create that file system with increased size, then mount again that file system and restore the backup.

(vi) If the file system belongs to system log files or other log files and not to delete then they requested us to provide one Repository server (only for log files). Normally one script will do automatically redirect the log files to that repository server.

(vii) Sometimes we will delete file contents not the files to reduce the file sizes. For that we execute the command **# cat /dev/null ><file name with path>** ie., nullifying the files.

(ix) If it is root file system or O/S file system,

(a) may be **/opt** full or may be **/var** full or may be **/tmp** full

(b) In **/var/log/secure** or **/var/log/system** or **/var/tmp** files may be full. If those files are important then redirect them to other central repository server or backup those files and nullifying those files.

(c) If **/home** directory is present in root ( **/** ) file system then this file system full will occur. Generally  **/home** will be separated from root file system and created as separate **/home** file system. If **/home** is in root ( **/** ) as a directory then create a separate file system for **/home** and copy those files and directories belongs to **/home** and remove that **/home** directory.

(d) If root ( **/** ) is full then cannot login to the system. So, boot with net or CDROM in single user mode and do the above said.

(x) Normally if file system is other than O/S then we will inform to that respective manager or owner and take the permissions to remove unnecessary files through verbal permission or CRQ .

**23. CPU utilization full, how to troubleshoot it?**

(a) Normally we get these scenarios on weekends because backup team will take heavy backups.

(b) First check which processes are using more CPU utilization by **# top** and take a snap shot of that user processes and send the snap shot and inform to that user to kill the unnecessary process.

(c) If those processes are backups then inform to the backup team to reduce the backups by stopping some backups to reduce the CPU utilization.

(d) Sometimes in peak stages (peak hours means having business hours) CPU utilization will full and get back to the normal position automatically after some time (within seconds). But ticket raised by monitoring team. So, we have to take a snap shot of that peak stage and attach that snap shot to the raised ticket and close that ticket.

(e) Sometimes if heavy applications are running and not to kill (ie., business applications), then if any spare processor is available or other low load CPUs available then move those heavy application processes to those CPUs.

(d) If CPUs are also not available then if the system supports another CPU then inform to the data centre people or CPU vendor to purchase new CPU though Business approval and move some processes to the newly purchased CPUs.

**24. How to troubleshoot when the system is slow?**

(a) System slow means the end users response is slow.

(b) Check the Application file system, CPU utilization, memory utilization and O/S file system utilization.

(c) If all are ok, then check network statistics and interfaces whether the interfaces are running in full duplex mode or half duplex mode and check whether the packets are missing. If all are ok from our side then,

(d) Inform to network team and other respective teams to solve this issue.

**25. How to troubleshoot if the node is down?**

(a) Check pinging the system. If pinging, then check whether the system is in single user mode or not.

(b) If the system is in single user mode then put the system in multi user mode ie., default run level by confirming with our team whether system is under maintenance or not.

(c) Check in which run level the system is running. If it is in init 1 it will not be able to ping. If it is in init s then it will ping.

(d) In this situation also if it is not pinging then try to login through console port. If not possible then inform to data centres people to hard boot the system.

(d) If connected through console port then we may get the console prompt.

**26. How to troubleshoot if the memory utilization full?**

(a) Check how much memory is installed in the system by **# dmidecode -t memory** command.

(b) Check the memory utilization by **# vmstat -v** command.

(c) Normally application or heavy backups utilize more memory. So, inform to application team or backup team or other teams which team is utilizing the more memory to reduce the processes by killing them or pause them.

(d) Try to kill or disable or stop the unnecessary services.

(e) If all the ways are not possible then inform to team lead or tech lead or manager to increase the memory (swap space). If it is also not possible then taking higher authority's permissions to increase the physical memory. For those we contact the server vendor and co-ordinate with them through data centre people to increase the RAM size.

**A record :**

* It is the Address records also known as host records
* Points to the IP address reflecting the domain
* Used for forward lookup of any domain name

**CNAME Record :**

* It is short abbreviation for Canonical Name
* Provides an alias name for same hostname
* Helps create subdomains

DNS:

----

Host file : provides resolution of hostnames

Add name and ip address.used /etc/hosts file

Zone : contains storage db.2 types of zone records as forward(host-ip) ,reverse(ip-host) lookup zones

Start Of Authority(SOA) ; holds general admiistraive and control info

NameServer : contains ip address or cname of the name server

A(address) : maps hostname to ip address

PTR (pointer): maps ip address to hostname

CNAMe(canonical) : used as alias

Httpd conf file : /etc/httpd/conf/httpd.conf

Apache troubleshoot using logfiles

/var/log/httpd/access\_log,error\_log

Cut : divides a string or output

Cut(delimeters,fileds,character) filename

SED:

----

Sed “ s/root//g” sample delete word from a file

Sed -n “2p” sample print 2nd row

Sed -n “3,5p” sample print3,4,5 rows

Sed -n “1p

>$p” sample print 1st and last row

Sed “3d” sample delete 3rd row

Sed “2,5d” sample delete 2 to 5 lines

Sed “ 2,5w file” sample copies 2nd to 5th rows from sample file to file

Sed “=” sample get line numbers

DevOps

====

Customers --. Requirements 🡪 Dev/testers 🡪 Gaps 🡪 IT Ops

Devops is a sw development method, that stresses communication,coloboration and integration bn software developers and IT professionals.

Uses ; successful releases,consistent releases process,predicitibility,integration,completeness,quality

1, Automated release mgmt.

2,reusability and automation

3,functional,non functional ,business and operational readiness

CI

===

*Integrate the code changes remains the main branch should be up to date*

*It refers integrating,building,testing code with in dev environment.*

*CI pipeline should be run for every commit*

*CD*

*===*

*Took CI build and run through deployment procedures on prod,non prod servers*

*Operations*

*--------------*

* 1. *Infrastructure automation*
  2. *Configuration Management*
  3. *Deployment automation*
  4. *Log management*
  5. *Performance management*
  6. *Monitoring*

*Pipeline:*

*=====*

1. *Pushing to the code repo :*

*CI server monitors repository,and if any new commit happened then code is checked out and pipeline has been run.pipeline is automated tasks*

1. *Static analysis : coding errors,check style,findbugs*
2. *Pre-deployment testing : unit testing and functional testing*
3. *Packaging,deployment,to the test environemt*
4. *Post deployment testing*

*Once deployed test env,execute remaining tests with out executing the deployed application*

*Includes functional,integration and performance tests*

*Once this step has been completed ci pipeline has been done,waiting for the manual verifications*

*POM file : includes versioning,configuration,dependencies,application,testing resources,*

*Saves in root directory of project*

*Group id,artifact id,version id*

*Elemets : name,url,packaging,dependencies,repositories,build,reports,plugin repositories*

*Build life cycle phases : clean,compile,test compile,test,package,install,deploy*

*Profile : build project in different ways*

*Dev,test,dep profiles,*

1. *Per project(pom) 2. Per user (settings) 3. Global(settings)*

*Life cycle : 1. Default 2. Clean 3. Site*

*Settings file : configure setting can access across pom maven files*

*Home dir/.m2/settings.xml, maven installation /m2\_home/settings.xml*

*Profile activation :*

1. *Default variable 2 maven settings 3 os settings 4 command console*

*Dependency scope:*

*Compile,runtime,provided,test,system*