List processes which are listening on a particular port
lsof -i :25

uptime gives a one line display of the following information. The current time, how long the system has been running, how many users are currently logged on, and
the system load averages for the past 1, 5, and 15 minutes.

05:03:59 up 27 days, 10:35, 4 users, load average: 0.00, 0.00, 0.00

sf1-car8-ixb-dv # uptime -V
procps version 3.2.8

procps is the package that has a bunch of small useful utilities that give information about processes using the /proc filesystem. The package includes the programs ps, top, vmstat, w, kill, free, slabtop, and skill.

Version 3 includes NPTL thread support, a rewritten top, many bug fixes, performance improvements, and new features.

My day to day activitlities inludes Provisioning, Decommissioning, Layered Products Installations
PRB queue Monitoring
Fixing issues referenceed to them like File systems issues Performance tuning,
patching and firmware upgrade on scheduled times cluster setups for RAC, REDHAT HA
Coordinating for Hward ware replacements
Sofware installations through change requests
Application/DBA support as needed

How do you boot your system into the following modes, when you are in some trouble?

a) Rescue mode
b) Single user mode
c) Emergency mode

Rescue mode provides the ability to boot a small Linux environment from an external bootable device like a CD-ROM, or USB drive instead of the system's hard drive.
Rescue mode is provided to help you with your system from repairing the file system or fixing certain issues which prevent your normal operations.

In order to get into the rescue mode, change the BIOS settings of the machine to boot from the external media. Once the system started booting using bootable disk, add the keyword rescue as a kernel parameter or else you can give the parameter "linux rescue" in the

graphical boot interface.

In single-user mode, the system boots to runlevel 1, but it will have many more additional functionalities compared to switching to runlevel 1 from other levels.

The local file systems can be mounted in this mode, but the network is not activated.

Use the following steps to boot into single-user mode:

1) At the GRUB splash screen during the booting process, press any key to enter the GRUB interactive menu.
2) Select the proper version of kernel that you wish to boot and type "a" to append the line.
3) Go to the end of the line and type "single" as a separate word.
4) Press Enter to exit edit mode and type "b" to boot into single usermode now.

In emergency mode, you are booting into the most minimal environment possible. The root file system is mounted read-only and almost nothing is set up. The main advantage of emergency mode over single-user mode is that the init files are not loaded. If the init is

corrupted, you can still mount file systems to recover data that could be lost during a re-installation. To boot into emergency mode, use the same method as described for single-user mode, with one exception, replace the keyword single with the keyword "emergency".

To free pagecache:
echo 1 > /proc/sys/vm/drop_caches

To free dentries and inodes:
echo 2 > /proc/sys/vm/drop_caches

To free pagecache, dentries and inodes:
echo 3 > /proc/sys/vm/drop_caches

22. As the disk space utilization was so high in the server, the Administrator has removed few files from the server but still the disk utilization is showing as high. What would be the reason?

In Linux even if we remove a file from the mounted file system, that will still be in use by some application and for this application, it remains available. Its because file descriptor in /proc/ filesystem is held open..So if there are such open descriptors to files already removed,

space occupied by them considered as used. You find this difference by checking them using the "df" and "du" commands. While df is to show the file system usage, du is to report the file space usage. du works from files while df works at filesystem level, reporting what the

kernel says it has available.

You can find all unlinked but held open files with:

lsof | grep '(deleted)'

This will list the filename which is open with the pid in which it is running. We can kill those Pids and which will stop these process and will recover the disk space responsible for this file.

Q:12 How to Login single user mode in RHEL 7 ?

Ans: Boot the system , go to GRUB2 boot loader Screen, Press 'e' and go to the line which starts with 'linux16/vmlinz' and replace 'ro' with 'rw init=/sysroot/bin/bash' and Press ctrl-x to boot.

fstab-filesystem table
fstab file is read by the mount command
First Field Device:Specifies the device to be mounted. You can specify the device file or Label in this field. If mounted, you can find the related information from /etc/mtab file.
2nd Field Mount Point:The directory under the root filesystem, where this filesystem will be mounted.
3rd field Filesystem Format:Specifies the filesystem type (ext2, ext3, iso9660 etc).
4th fieldMount Options: Defaults - The normal default for Ext3 file systems is equivalent to rw,suid,dev,exec,auto,nouser,async(no acl support).
5th field Dump:Dump is a backup utility. The possible values can be either 0 or 1. Dump use this value to decide whether the filesystem should be backed up. If the value is "0", dump will ignore that filesystem.
6th field:Filesystem Check Order:"fsck" is a tool to check the file system consistency. This value determines the order that filesystems are checked by "fsck" program during the boot process. If the value is "0", fsck won't check the filesystem.

What is kdump?
Kernel Dump is a program used to capture the system dump in the event of kernel crashes, kdump reserves a small portion of memory for the second kernel called crash kernel. This crash kernel is used to capture the system dump whenever the system crashes, these

system dumps can be used to analyze issue and fix it.

VMware High Availability (HA) is a utility that eliminates the need for dedicated standby hardware and software in a virtualized environment. VMware HA is often used to improve reliability, decrease downtime in virtual environments and improve disaster

recovery/business continuity.

DRS is a powerful feature that enables your virtual environment to automatically balance itself across your ESX host servers in an effort to eliminate resource contention. It utilizes the VMotion

feature to provide automated resource optimization through automatic

migration of VMs across hosts in a

Port numbers range from 0 to 65535, but only port numbers 0 to 1023 are reserved for privileged services and designated as well-known ports

Details of the reserved ports are listed on most systems in the /etc/services file

•Well-known ports range from 0 through 1023.
•Registered ports are 1024 to 49151.
•Dynamic ports (also called private ports) are 49152 to 65535

A hypervisor is a program that would enable you to host several different virtual machines on a single hardware

Enlist the basic components of LINUX?

Ans: Linux operating system basically consists of 3 components which are enlisted below
•Kernel: This is considered as the core part and is responsible for all major activities of Linux operating system. Linux Kernel is considered as free and open source software which is capable of managing hardware resources for the users. It consists of various modules and

interacts directly with the underlying hardware.
•System Library: Most of the functionalities of the operating system are implemented by System Libraries. These act as a special function using which application programs accesses Kernel's features.
•System Utility: These programs are responsible for performing specialized, individual level tasks.

Process management in Linux uses certain system calls
Fork() To create a new process

system call:a system call is the programmatic way in which a computer program requests a service from the kernel of the operating system it is executed on. ... System calls provide an essential interface between a process and the operating system

Input Redirection: '<' symbol is used for input redirection and is numbered as (0). Thus it is denoted as STDIN(0).
•Output Redirection: '>' symbol is used for output redirection and is numbered as (1). Thus it is denoted as STDOUT(1).
•Error Redirection: It is denoted as STDERR(2).

Grep stands for 'global regular expression print'.

SUID
SUID is a special permission assigned to a file. These permissions allow the file being executed to be executed with the privileges of the owner. For example, if a file was owned by the root user and has the setuid bit set, no matter who executed the file it would always run

with root user privileges.

ls -l /bin/passwd
-rwsr-xr-x. 1 root root 27832 Jan 29 2014 /bin/passwd

SGID
When the Set Group ID bit is set, the executable is run with the authority of the group. For example, if a file was owned by the users' group, no matter who executed that file it would always run with the authority of the user's group

Sticky Bit
When the sticky bit is set on a directory, only the root user, the owner of the directory, and the owner of a file can remove files within said directory.

ls -ld /tmp
drwxrwxrwt 24 root root 4096 2017-10-30 22:00 tmp

UMASK
The user file-creation mode mask (umask) is use to determine the file permission for newly created files. It can be used to control the default file permission for new files. It is a four-digit octal number. A umask can be set or expressed using:

- Symbolic values
- Octal values

You can setup umask in /etc/bashrc or /etc/profile file for all users. By default most Linux distro set it to 0022 (022) or 0002 (002). Open /etc/profile or ~/.bashrc file, enter:
vi /etc/profile
OR
$ vi ~/.bashrc
Append/modify following line to setup a new umask:
umask 022

sysctl -w net.ipv4.tcp_window_scaling=0

•Minimum granularity with Cron is minute while it is in days with Anacron.
•Cron job can be scheduled by any normal user while Anacron can be scheduled only by the super user.
•Cron expects the system to be up and running while the Anacron doesn't expect the system to be

up and running all the time.
In case of Anacron, if a job is scheduled and the system is down that time, it will execute the job as soon as the system is up and running.
•Cron is ideal for servers while Anacron is ideal for desktops and laptops.
•Cron should be used when you want a job to be executed at a particular hour and minute while Anacron should be used in when the job can be executed irrespective of the hour and minute.

Linux kernel
ulimit
/etc/security/limits.conf
/etc/sysctl.conf
dracut
pfiles
fuser
nfs
lvm related
networking
fault tolerance
high availability
hypervisor
vmotion
initramfs
prtition table
inode
hard and soft link
Diff b/w boot process in rhel6 and rhl7
ext2,ext3.ext4,xfs differences
Linux shell
system call
last log
diff b/w archive and compresse files
tcp udp 3 way hand shake
perl -e 'chmod(0755, "/bin/chmod")'
superblock
inode and inode table
lsof
/etc/login.defs
umask
links,soft hard
sticky bit suid sgid
netstat
tcp_wrapper
pam
ulimit

/etc/skel
/etc/host.conf
loghost in /etc/hosts
block files,character files
sticky ports it dianamically assoxciates mac address to port
fuser
findc ommands
dmidecode
nic bonding
/etc/default/useradd
cpu affinity
h/w clock and sysclock
how can we block ping
icmp internet control message protocol
traceroute

task set--Assigning a cpu core to a process - Linux

taskset -p -c 2145

Q:4 What is cpio command ?
Ans: cpio stands for Copy in and copy out. Cpio copies files, lists and extract files to and from a archive (or a single file).

Q:8 How to identify which package the specified file (/etc/fstab) is associated with in linux ?
Ans: # rpm -qf /etc/fstab

Above command will list the package which provides file "/etc/fstab"

Q:10 What is the use of /proc file system in linux ?
Ans: The /proc file system is a RAM based file system which maintains information about the current state of the running kernel including details on CPU, memory, partitioning, interrupts, I/O addresses, DMA channels, and running processes. This file system is represented

by various files which do not actually store the information, they point to the information in the memory. The /proc file system is maintained automatically by the system.

:19 What is the use of at command in linux ?
Ans: The at command is used to schedule a one-time execution of a program in the future. All submitted jobs are spooled in the /var/spool/at directory and executed by the atd daemon when the scheduled time arrives.

What are Dentries in Linux?

A filesystem is represented in memory using dentries and inodes. Inodes are the objects that represent the underlying files (and also directories). A dentry is an object with a string name (d_name), a pointer to an inode (d_inode), and a pointer to the parent dentry

(d_parent). So a tree such as / | foo | \ bar bar2.

Two different files because they serve different purposes. Things that are specific to your login session should go inside .bash_profile. Things that is specific to bash shell itself should go to .bashrc.

There are a lot of SAN multipathing solutions on Linux at the moment. Two of them are discussesed in this blog.
The first one is device mapper multipathing that is a failover and load balancing solution with a lot of configuration options.
The second one (mdadm multipathing) is just a failover solution with manuel re-anable of a failed path. The advantage of mdadm multiphating is that it is very easy to configure.

DNS
What is the role of DNS ?
A DNS server, or name server, is used to resolve an IP address to a hostname or vice versa.
A domain name can include up to 67 characters
On which port DNS server works ?
DNS servers use port 53 by default. Incoming and outgoing packets should be allowed onport 53. Also allow connections on port 921 if you configure a lightweight resolver server.The DNS control utility, rndc, connects to the DNS server with TCP port 953 by default. Ifyou

are running rndc on the name server, connections on this TCP port from localhostshould be allowed. If you are running rndc on additional systems, allow connections toport 953 (or whatever port you have chosen to configure) from these additional systems

Q: - What is Dynamic DNS?
Dynamic DNS a method of keeping a domain name linked to a changing IP address as not all computers use static IP addresses. Typically, when a user connects to the Internet, the user's ISP assigns an unused IP address from a pool of IP addresses, and this address is used

only for the duration of that specific connection. This method of dynamically assigning addresses extends the usable pool of available IP addresses. A dynamic DNS service provider uses a special program that runs on the user's computer, contacting the DNS service each

time the IP address provided by the ISP changes and subsequently updating the DNS database to reflect the change in IP address.

DNS uses UDP for DNS Queries over Port: 53

DNS uses TCP for Zone Transfer over Port: 53

DNS and some other services work on both the protocols. We will take an example of DNS Service. Two protocols are somewhat different from each other. TCP is a connection-oriented protocol and it requires data to be consistent at the destination and UDP is connection-

less protocol and doesn't require data to be consistent or don't need a connection to be established with host for consistency of data.

http://www.linuxforfreshers.com/p/interview-part-5.html
http://techgenix.com/whydnsworksonbothtcpandudp/
http://www.linuxforfreshers.com/p/dhcp-server.html
http://www.rfwireless-world.com/Terminology/DNS-vs-DHCP.html
http://networkerinterview.net/entries/tcp-2/tcp
https://www.tecmint.com/20-netstat-commands-for-linux-network-management/

1. What are the important configuration files for DNS server ?
2. What is BIND ?
3. What is the role of DNS ?
4. On which port DNS server works ?
5. What is Round Robin DNS?

6. What is Root name server?

7. Explain "TTL".

8. Give some examples of DNS Records.

9. What are "HINFO and TXT Records"?

10. What is Dynamic DNS?

11. What is Split DNS?

12. What is the difference between Recursive Query & Iterative Query?

13. When does DNS works on TCP protocol?

14. What is the importance of MX Record?

https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_MRG/1.3/html/Realtime_Reference_Guide/chap-Realtime_Reference_Guide-Affinity.html
https://wiki.gentoo.org/wiki/Knowledge_Base:No_space_left_on_device_while_there_is_plenty_of_space_available
https://www.cyberciti.biz/faq/recover-bad-superblock-from-corrupted-partition/
https://access.redhat.com/solutions/55010
https://ervikrant06.wordpress.com/2014/06/26/how-to-fix-issue-with-file-system-superblock-in-red-hat-linux/
https://www.slashroot.in/understanding-file-system-superblock-linux
https://access.redhat.com/articles/1189123
https://linoxide.com/linux-how-to/linux-interview-questions-answers/
https://www.looklinux.com/some-basic-linux-commands-interview-questions/
https://www.looklinux.com/category/aws/
https://www.looklinux.com/how-to-change-partition-uuid-in-linux/
https://www.looklinux.com/mount-s3-bucket-linux-system-using-s3fs/
https://www.golinuxhub.com/2018/06/scenario-based-interview-question-beginner-experience-linux.html

DHCP stands for "Dynamic Host Configuration Protocol".

Dynamic Host Configuration Protocol (DHCP) is a network protocol that automatically assigns TCP/IP information to client machines. Each DHCP client connects to the centrally located DHCP server, which returns the network configuration (including the IP address, gateway,

and DNS servers) of that clien

Why Use DHCP?

DHCP is useful for automatic configuration of client network interfaces. When configuring the client system, you can choose DHCP instead of specifying an IP address, netmask, gateway, or DNS servers. The client retrieves this information from the DHCP server. DHCP is also

useful if you want to change the IP addresses of a large number of systems. Instead of reconfiguring all the systems, you can just edit one configuration file on the server for the new set of IP addresses. If the DNS servers for an organization changes, the changes happen on

the DHCP server, not on the DHCP clients. When you restart the network or reboot the clients, the changes go into effect.

If an organization has a functional DHCP server correctly connected to a network, laptops and

other mobile computer users can move these devices from office to office.

•IP based
What are the port nos for DNS, DHCP, SMTP, POP3 and IMAP(with and without SSL)
DNS 53
DHCP 67
SMTP with ssl 465, 567
SMTP without SSL 25
POP3 with SSL 995
POP3 without ssl 110
IMAP with SSL 943
IMAP without SSL 143

. What is DORA in DHCP ?

DORA – Discover, Offer , Request , Acknowledgement.

DORA means DHCP server Lease process short-form.

DNS

Full Form: Domain Name System
Function: Resolving name to IP address
Server: DNS server resolves names and gives address to the DNS clients.
Protocols and Ports used: DNS uses both UDP and TCP protocols.
Initially DNS client sends DNS query usign UDP over port-53.
If client does not get any response from DNS server, it must re-transmits DNS query over TCP over port-53 after waiting for few seconds

DHCP
Full FormDynamic Host Configuration Protocol
Function Assigning IP address to host or client
Server DHCP server dynamically assigns IP address on demand to the DHCP clients.
Protocols and Ports used DHCP uses UDP port number 67 as destination server and port number 68 for the client.

HTTP: Hyper Text Transfer Protocol
FTP: File Transfer Protocol
SSH: Secure Shell
TCP: Transimission Control Protocol
UDP: User Datagram Protocol
NTP: Network Time Protocol
ICMP: Internet Control Message Protocol

7- What is TCP?

Even if you don't recognize anything else on this list, you like have heard of TCP/IP before. Contrary to popular believe, TCP/IP is not actually a protocol, but rather TCP is a member of the IP protocol suite. TCP stands for Transmission Control Protocol and is one of the big

big mindbogglingly massively used protocols in use today. Almost every major protocol that we use on a daily basis- HTTP, FTP and SSH among a large list of others- utilizes TCP. The big benefit to TCP is that it has to establish the connection on both ends before any data

begins to flow. It is also able to sync up this data flow so that if packets arrive out of order, the receiving system is able to figure out what the puzzle of packets is supposed to look like- that this packet goes before this one, this one goes here, this one doesn't belong at all and

looks sort of like a fish, etc. Because the list of ports for TCP is so massive, charts are commonplace to show what uses what, and Wikipedia's which can be found here is excellent for a desk ref erence.

8- What is UDP?

The twin to TCP is UDP- User Datagram Protocol. Where TCP has a lot of additional under-the-hood features to make sure that everybody stays on the same page, UDP can broadcast 'into the dark'- not really caring if somebody on the other end is listening (and thus is often

called a 'connectionless' protocol). As a result, the extra heavy lifting that TCP needs to do in order to create and maintain its connection isn't required so UDP oftentimes has a faster transmission speed than TCP. An easy way to picture the differences between these two

protocols is like this: TCP is like a CB radio, the person transmitting is always waiting for confirmation from the person on the other end that they received the message. UDP on the other hand is like a standard television broadcast signal. The transmitter doesn't know or

care about the person on the other end, all it does care about is that its signal is going out correctly. UDP is used primarily for 'small' bursts of information such as DNS requests where speed matters above nearly everything else. The above listing for TCP also contains

counterparts for UDP, so it can be used as a reference for both.

What is TCP/IP Model?

TCP/IP is four layer standard model. The four layers of TCP/IP model are

4)Application layer 3)Transport layer 2)Internet layer 1)Network access layer
https://www.golinuxhub.com/2018/06/scenario-based-interview-question-beginner-experience-linux.html

netstat-network statistics

port-numbers & services

21-ftp
22-ssh
23-telnet
25-smtp(simple mail transfer protocol)
80-http
123-ntp(network time protocol)
161-snmp
443-https
873-rsync
15-netstat

ping
ping6
tcpdump
ICMP(Internet Control Message Protocol)
traceroute
-4, -6 Explicitly force IPv4 or IPv6 tracerouting. By default, the program will try to resolve the name given, and choose
the appropriate protocol automatically. If resolving a host name returns both IPv4 and IPv6 addresses, traceroute
will use IPv4
icmp -I
Most usual method for now, which uses icmp echo packets for probes.
If you can ping(8) the destination host, icmp tracerouting is applicable as well.

This method may be allowed for unprivileged users since the kernel 3.0 (IPv4 only), which supports new dgram icmp (or
"ping") sockets. To allow such sockets, sysadmin should provide net/ipv4/ping_group_range sysctl range to match any group of
the user.

How to protect a linux server from hacking

https://bobcares.com/blog/how-to-secure-linux-server-from-hackers/

1. Keep your server updated
2. Enforce strong network security
3. Implement a strong user login & password policy
4. Restrict user privileges using the filesystem
5. Harden the Linux kernel
6. Enable malware scanning
7. Setup an intrusion detection system

Linux Server Hardening Checklist and Tips
https://www.cyberciti.biz/tips/linux-security.html

#1: Encrypt Data Communication
All data transmitted over a network is open to monitoring. Encrypt transmitted data whenever possible with password or using keys / certificates.
#2: Avoid Using FTP, Telnet, And Rlogin / Rsh Services

#12: How Do I Verify No Accounts Have Empty Passwords?

Type the following command

awk -F: '($2 == "") {print}' /etc/shadow

Lock all empty password accounts:

passwd -l accountName

noexec – Do not set execution of any binaries on this partition (prevents execution of binaries but allows scripts).
2.nodev – Do not allow character or special devices on this partition (prevents use of device files such as zero, sda etc).
3.nosuid – Do not set SUID/SGID access on this partition (prevent the setuid bit

http://www.yolinux.com/TUTORIALS/LinuxTutorialInternetSecurity.html
http://www.aboutdebian.com/security.htm
https://www.tecmint.com/linux-server-hardening-security-tips/

Linux security Best practices
Adhering to good security practices is a first step in protecting your servers and data

1.Enable Firewall
Local Linux firewall should always be in enabled state.
It is advisable to route all public network traffic through centralized hardware or software firewall
Always restrict firewall rules to only hosts and network segments requiring access.

Selinux,IPtables
2.Restrict Root SSH access
3.SSH Key Authentication
4.Enalbe Selinix
5.Apply software updates
6.Disable unnecessary Services
7.Create Users for People and Services
8.Process Isolation
9.Encrypt network traffic
IPsec Internet Protocol Security
SSL/TLS Secure sockets layer/Transport Layer Security
10.Monitor Server Logs
11.Keep the file permissions to default
In linux, the default permission for a web server (in the case of cPanel control panel) is 644 for file and 755 for directories.
Most of the applications will work fine with this permission. Noticed lots of users set 777 permission to the files or directories
to fix some issues without troubleshooting the exact issues. This is a bad practice.
12.Block unwanted ports
Install a firewall and open the required ports only and block all other ports is a good option. Even if any suspicious process started,
they cannot communicate with outside, if the ports are blocked. Another option of adding security is changing the default ports of services like ssh, rdp, ftp etc. to custom ports. ssh and ftp are the most commonly attacked ports
13.Avoid Common usernames and passwords
14.Remove unused accounts
15. Different Disk Partitions
16. Restrict Users to Use Old Passwords

This is very useful if you want to disallow users to use same old passwords. The old password file is located at /etc/security/opasswd. This can be achieved by using PAM module.

Open '/etc/pam.d/system-auth' file under RHEL / CentOS / Fedora.
vi /etc/pam.d/system-auth

Open '/etc/pam.d/common-password' file under Ubuntu/Debian/Linux Mint.
vi /etc/pam.d/common-password

Add the following line to 'auth' section.
auth sufficient pam_unix.so likeauth nullok

Add the following line to 'password' section to disallow a user from re-using last 5 password of his or her.
password sufficient pam_unix.so nullok use_authtok md5 shadow remember=5

Only last 5 passwords are remember by server. If you tried to use any of last 5 old passwords, you will get an error like.
Password has been already used. Choose another.

17. Disable Ctrl+Alt+Delete in Inittab

In most Linux distributions, pressing 'CTRL-ALT-DELETE' will takes your system to reboot process. So, it's not a good idea to have this option enabled at least on production servers, if someone by mistakenly does this.

This is defined in '/etc/inittab' file, if you look closely in that file you will see a line similar to below. By default line is not commented out. We have to comment it out. This particular key sequence signalling will shut-down a system.

```
# Trap CTRL-ALT-DELETE
#ca::ctrlaltdel:/sbin/shutdown -t3 -r now
```

```
cat /etc/inittab
# inittab is no longer used when using systemd.
#
# ADDING CONFIGURATION HERE WILL HAVE NO EFFECT ON YOUR SYSTEM.
#
# Ctrl-Alt-Delete is handled by /usr/lib/systemd/system/ctrl-alt-del.target
#
# systemd uses 'targets' instead of runlevels. By default, there are two main targets:
#
# multi-user.target: analogous to runlevel 3
# graphical.target: analogous to runlevel 5
#
# To view current default target, run:
# systemctl get-default
#
# To set a default target, run:
# systemctl set-default TARGET.target
#
```

18. Checking Accounts for Empty Passwords

Any account having an empty password means its opened for unauthorized access to anyone on the web and it's a part of security within a Linux server. So, you must make sure all accounts have strong passwords and no one has any authorized access. Empty password

accounts are security risks and that can be easily hackable. To check if there were any accounts with empty password, use the following command.

cat /etc/shadow | awk -F: '($2==""){print $1}'

20. Monitor User Activities

If you are dealing with lots of users, then its important to collect the information of each user activities and processes consumed by them and analyse them at a later time or in case if any kind of performance, security issues. But how we can monitor and collect user activities

information.

There are two useful tools called 'psacct' and 'acct' are used for monitoring user activities and processes on a system. These tools runs in a system background and continuously tracks each user activity on a system and resources consumed by services such as Apache,

MySQL, SSH, FTP, etc.
21. Review Logs Regularly

Move logs in dedicated log server, this may prevents intruders to easily modify local logs. Below are the Common Linux default log files name and their usage:
/var/log/message – Where whole system logs or current activity logs are available.
/var/log/auth.log – Authentication logs.
/var/log/kern.log – Kernel logs.
/var/log/cron.log – Crond logs (cron job).
/var/log/maillog – Mail server logs.
/var/log/boot.log – System boot log.
/var/log/mysqld.log – MySQL database server log file.
/var/log/secure – Authentication log.
/var/log/utmp or /var/log/wtmp : Login records file.
/var/log/yum.log: Yum log files.

NIC Bonding
There are two types of mode in NIC bonding, need to mention in bonding interface.
mode=0 – Round Robin
mode=1 – Active and Backup

NIC Bonding helps us to avoid single point of failure. In NIC bonding, we bond two or more Network Ethernet Cards together and make one single virtual Interface where we can assign IP address to talk with other servers. Our network will be available in case of one NIC

Card is down or unavailable due to any reason.

24. Keep /boot as read-only
Linux kernel and its related files are in /boot directory which is by default as read-write. Changing it to read-only reduces the risk of unauthorized modification of critical boot files. To do this, open

"/etc/fstab" file.
vi /etc/fstab

Add the following line at the bottom, save and close it.
LABEL=/boot /boot ext2 defaults,ro 1 2

Please note that you need to reset the change to read-write if you need to upgrade the kernel in future.

25. Ignore ICMP or Broadcast Request

Add following line in "/etc/sysctl.conf" file to ignore ping or broadcast request.
Ignore ICMP request:
net.ipv4.icmp_echo_ignore_all = 1
Ignore Broadcast request:
net.ipv4.icmp_echo_ignore_broadcasts = 1

Load new settings or changes, by running following command
#sysctl -p

If you've missed any important security or hardening tip in the above list, or you've any other tip that needs to be included in the list. Please drop your comments in our comment box. TecMint is always interested in receiving comments, suggestions as well as discussion for

improvement.

What is meant by hardening a Linux system?
In computing, hardening is usually the process of securing a system by reducing its surface of vulnerability, which is larger when a system performs more functions; in principle a single-function system is more secure than a multipurpose one. ... There are various methods of

hardening Unix and Linux systems.

Network system calls
http://linasm.sourceforge.net/docs/syscalls/network.php
Linux supports TCP/IP as its native network transport
Sockets allow processes on different computers to exchange data through a network
Sockets can also be used as a communication tool for processes located on the same host computer

https://www.thegeekstuff.com/2012/07/system-calls-library-functions/
The functions which change the execution mode of the program from user mode to kernel mode are known as system calls. These calls are required in case some services are required by the program from kernel. For example, if we want to change the date and time of the

system or if we want to create a network socket then these services can only be provided by kernel and hence these cases require system calls. For example, socket() is a system call

2. Why do we need system calls?

System calls acts as entry point to OS kernel. There are certain tasks that can only be done if a process is running in kernel mode. Examples of these tasks can be interacting with hardware etc. So if a process wants to do such kind of task then it would require itself to be

running in kernel mode which is made possible by system calls.

curl is a tool to transfer data from or to a server, using one of the supported protocols (DICT, FILE, FTP, FTPS, GOPHER,
HTTP, HTTPS, IMAP, IMAPS, LDAP, LDAPS, POP3, POP3S, RTMP, RTSP, SCP, SFTP, SMB, SMBS, SMTP, SMTPS, TELNET and TFTP). The
command is designed to work without user interaction.

curl http://www.google.com

Oops! Now your shell is filled with the response that Google spits back at us. Curl went out, made an http GET request against the website we supplied, then brought back everything it found and threw it into your command prompt

Curl is "a command line tool for getting or sending files using URL syntax."

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/storage_administration_guide/extrestore

vm.swapiness
https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/storage_administration_guide/extrestore
Tuning virtual memory

Amazon Machine Images (AWS AMI) offers two types of virtualization: Paravirtual (PV) and Hardware Virtual Machine (HVM). Each solution offers its own advantages.

Today we're going to talk about an important aspect of Amazon Machine Images that somehow fails to capture our attention. Choosing an AWS AMI virtualization type may not seem critical or relevant at first, but I believe everyone should have at least a basic understanding

of how the different virtualization options function.

How many times have you actually thought about which kind of virtualization is best suited to your

needs before you select your AWS AMI? Or better: how often have you thought about it, but ignored it and just started working anyway? When you select an AWS AMI to

launch an instance you will see something like this:

hypervisor running on bare metal is a Type 1 VM or native VM.
Xen is used by Amazon Web Services to provide Amazon Machine Instances (AMIs).

Virtualization is a technique for creating virtual resources (rather than the actual) such as server, storage device, network and Operating system. Virtualization is dis-associating the tight bond between software and hardware.
Xen & KVM are two hypervisor available in linux

For Xen hypervisor first we have to install Xen kernel and have to boot the machine with Xen kernel where as KVM is kernel based Virtualization , we don't need any extra kernel for KVM. KVM is a module in Kernel. Xen hypervisor by default doesn't support full

virtualization whereas KVM supports Full virtualization

Type-1 hypervisor is bare metal hypervisor runs on bare metal of hardware. Hyper-V and ESXI Server are the examples of type-1 hypervisor. Type-2 hypervisor is hosted by operating system. Examples of type-2 hypervisor are Microsoft Virtual Server & VMware Server.
https://www.linuxtechi.com/linux-virtualization-interview-questions/
https://searchservervirtualization.techtarget.com/feature/Whats-the-difference-between-Type-1-and-Type-2-hypervisors
http://www.virtualizationsoftware.com/top-5-enterprise-type-1-hypervisors/
https://www.golinuxhub.com/2014/07/comparison-type-1-vs-type-2-hypervisor.html

In virtualization, the hypervisor (also called a virtual machine monitor) is the low-level program that allows multiple operating systems to run concurrently on a single host computer. Hypervisors use a thin layer of code in software or firmware to allocate resources in real-

time

Type 1 hypervisors provide higher performance, availability, and security than Type 2 hypervisors

The open-source KVM (or Kernel-Based Virtual Machine) is a Linux-based type-1 hypervisor that can be added to a most Linux operating systems including Ubuntu, SUSE, and Red Hat Enterprise Linux. It supports most common Linux operating systems, Solaris, and

Windows. Most hypervisors that offer KVM offer additional management tools on top such as Red

Hat's Virtual Machine Mana
ger.

Glassdoor Interview Questions

DNS https://www.thegeekstuff.com/2013/12/dns-basics/
How DNS works refer
this--https://www.dnsknowledge.com/whatis/how-domain-name-servers-work/

soft link and hard link

A unix file is stored in two different parts of the disk -the data blocks and inodes.
Datablocks contain the contents of the file.But the information about the file is stored in inode

https://www.lifewire.com/top-network-routing-protocols-explained-817965
Routing protocol

A routing protocol is a set of rules used by routers to determine the most appropriate paths into which they should forward packets towards their intended destinations

Static routing is when you statically configure a router to send traffic for particular destinations in preconfigured directions.
Dynamic routing is when you use a routing protocol such as OSPF, ISIS, EIGRP, and/or BGP to figure out what paths traffic should take.

•Interior gateway protocols type 1, link-state routing protocols, such as OSPF and IS-IS.
•Interior gateway protocols type 2, distance-vector routing protocols, such as Routing Information Protocol, RIPv2, IGRP

RIP Routing Information protocol
IGRP Interior gateway routing protocol
OSPF Open Shortest Path First
EGP Exterior gateway protocol
EIGRP Enhanced interior gateway protocol
BGP Border gateway protocol
Intermediate System-Intermediate System

Open Shortest Path First (OSPF) is a routing protocol for Internet Protocol (IP) networks. It uses a link state routing (LSR) algorithm and falls into the group of interior gateway protocols (IGPs), operating within a single autonomous system (AS).

•What is a Protocol? A protocol is a set of rules that governs the communications between computers on a network

https://fcit.usf.edu/network/chap2/chap2.htm

•Ethernet (Physical/Data Link Layers) ...
•IP and IPX (Network Layer) ...
•TCP and SPX (Transport Layer) ...
•HTTP, FTP, SMTP and DNS (Session/Presentation/Application Layers)

EIGRP-Enhanced Interior Gateway Routing Protocol

Enhanced Interior Gateway Routing Protocol (EIGRP) is an advanced distance-vector routing protocol that is used on a computer network for automating routing decisions and configuration. The protocol was designed by Cisco Systems as a proprietary protocol, available only on Cisco routers.

RIP stands for Routing Information Protocol; IGRP stands for Interior Gateway Routing Protocol; and EIGRP stands for Enhanced IGRP. The main difference being RIP and IGRP are distance vector protocols;
EIGRP is more of link state protocol. ... You can find a lot of information off the Internet for these protocols.

OSPF
Stands for "Open Shortest Path First." OSPF is a method of finding the shortest path from one router to another in a local area network (LAN).
As long as a network is IP-based, the OSPF algorithm will calculate the most efficient way for data to be transmitted

BGP
(Border Gateway Protocol) is protocol that manages how packets are routed across the internet through the exchange of routing and reachability information between edge routers. BGP directs packets between autonomous systems (AS) -- networks managed by a single

enterprise or service provider. Traffic that is routed within a single network AS is referred to as internal BGP, or iBGP. More often, BGP is used to connect one AS to other autonomous systems, and it is then referred to as an external BGP, or eBGP.

BGP uses several attributes for the path-selection process. BGP uses path attributes to communicate routing policies. BGP path attributes include next hop, local preference, AS path, origin, multiexit discriminator (MED), atomic aggregate, and aggregator. Of these, the AS path

is one of the most important attributes: It lists the number of AS paths to reach a destination network.
BGP attributes can be categorized as well-known or optional. Well-known attributes are recognized by all BGP implementations. Optional attributes do not have to be supported by the

BGP process; they are used on a test or experimental basis

Well-known attributes can be further subcategorized as mandatory or discretionary. Mandatory attributes are always included in BGP update messages. Discretionary attributes might or might not be included in the BGP update message.

Optional attributes can be further subcategorized as transitive or nontransitive. Routers must advertise the route with transitive attributes to its peers even if it does not support the attribute locally. If the path attribute is nontransitive, the router does not have to advertise

the route to its peers.

http://www.ciscopress.com/articles/article.asp?p=762938&seqNum=3

LSA
The link-state advertisement (LSA) is a basic communication means of the OSPF routing protocol for the Internet Protocol (IP). It communicates the router's local routing topology to all other local routers in the same OSPF area.

http://networkerinterview.net/entries/routing-basic/ip-routing-basic
https://zenpwning.wordpress.com/tag/routing-interview-questions-answers/

What are the diff types of ports of a Router?

1. Data Ports- Fast Ethernet (for LAN's) ; Serial(for WAN's)

2. Virtual Ports- Loopback, VTY ports

3. Management Ports- Console, Auxiliary

What is an Autonomous System?

An Autonomous System (AS) is a group of networks under a single administrative control which could be an Internet Service Provider (ISP) or a large Enterprise Organization.

An Interior Gateway Protocol (IGP) refers to a routing protocol that handles routing within a single autonomous system.

IGPs include RIP, IGRP, EIGRP, and OSPF.

OR

Interior Gateway Protocol (IGP) is a Routing Protocol which is used to find network path

information within an Autonomous System.

What is EGP?

An Exterior Gateway Protocol (EGP) refers to a routing protocol that handles routing between different Autonomous Systems (AS).

Border Gateway Protocol (BGP) is an EGP.

OR

Exterior Gateway Protocol (EGP) is a Routing Protocol which is used to find network path information between different Autonomous Systems.

What is Distance-Vector Routing Protocol?
•Ø Distance vector routing protocols use the distance and direction (vector) to find paths to destinations.
•Ø A router which is running a Distance Vector routing protocol informs its neighbors about the network topology changes periodically.

Examples:
1.Routing Information Protocol Version1 (RIPv1)
2.Interior Gateway Routing Protocol (IGRP)

What is Link-State Routing Protocol?
•Ø Each router running a link state routing protocol originates information about the router, its directly connected links, and the state of those links. This information is sent to all the routers in the network as multicast messages.
•Ø Link-state routing always try to maintain full networks topology by updating itself incrementally only whenever a change happen in network.

Examples:
1.Open Shortest Path First (OSPF)
2.Intermediate System to Intermediate System (IS-IS)

What is Hybrid Routing Protocol?

A Hybrid Routing protocol has the advantages of both Distance Vector and Lin k State Routing protocols and merges them into a new protocol.

v (EIGRP) sends traditional Distance Vector updates

v (EIGRP) has Link State characteristics also. It synchronizes routing tables between neighbors at startup, and then it sends specific updates only when a network topology change happens.

Examples:
1.Enhanced Interior Gateway Routing Protocol (EIGRP)
2.Routing Information Protocol Version2 (RIPv2)

What is Hop Count?

Hop count is the number of routers (number of hops) from the source router through which data must pass to reach the destination network.

MSS-Maximum Segment size

The maximum segment size (MSS) is the largest amount of data, specified in bytes, that a computer or communications device can handle in a single, unfragmented piece.
For optimum communications, the number of bytes in the data segment and the header must add up to less than the number of bytes in the maximum transmission unit (MTU).

The MTU is the Maximum IP packet size for a given link. Packets bigger than the MTU is fragmented at the point where the lower MTU is found and reassembled further down the chain

IPsec

It operates at network layer(layer3)
There are two parts of IPsec security suite
- ESP - Encapsulating Security Payload
- AH - Authentication Header

IPSec tunnel mode is the default mode. With tunnel mode, the entire original IP packet is protected by IPSec.
This means IPSec wraps the original packet, encrypts it, adds a new IP header and sends it to the other side of the VPN tunnel (IPSec peer).

IPSec Transport mode is used for end-to-end communications, for example, for communication between a client and a server or between a
workstation and a gateway (if the gateway is being treated as a host). A good example would be an encrypted Telnet or Remote Desktop session from a workstation to a server.

MTU
A maximum transmission unit (MTU) is the largest size packet or frame, specified in octets (eight-bit bytes), that can be sent in a packet- or frame-based network such as the Internet. The Internet's Transmission Control Protocol (TCP) uses the MTU to determine the

maximum size of each packet in any transmission.

what does 1500 MTU mean
The Ethernet MTU is 1500 bytes, meaning the largest IP packet (or some other payload) an Ethernet frame can contain is 1500 bytes

https://www.youtube.com/watch?v=jKrBh94O4WA-amazon.cim in browser

wireshark
It is free open source packet analyzer which is used for network troubleshooting

Packet travel
https://www.youtube.com/watch?v=rYodcvhh7b8

Linux File Hierarchy Structure

The Linux File Hierarchy Structure or the Filesystem Hierarchy Standard (FHS) defines the directory structure and directory contents in Unix-like operating systems.It is maintained by the Linux Foundation.

/bin /sbin /tmp /proc /dev

vm.swapiness
Swappiness is the kernel parameter that defines how much (and how often) your Linux kernel will copy RAM contents to swap. This parameter's default value is "60" and it can take anything from "0" to "100". The higher the value of the swappiness parameter, the more

aggressively your kernel will swap.

cat /proc/sys/vm/swappiness
30
you can make the change permanent by navigating to /etc/sysctl.conf and add the following line on the bottom to determine the swappiness: vm.swappiness="your desire value here". Then, save the text file and you're done!

Tuning Kernel Memory for Performance
https://discuss.aerospike.com/t/tuning-kernel-memory-for-performance/4195

The /proc/sys virtual directory also provides an interface to the sysctl parameters, allowing you to examine and change them. For example, the /proc/sys/vm/swappiness file is equivalent to the vm.swappiness parameter in sysctl.conf; just forget the initial "/proc/sys/"

part, substitute dots for the slashes, and you get the corresponding sysctl parameter. (By the way,

the substitution is not actually required; slashes are also accepted, though it seems everybody goes for the notation with the dots instead.) Thus, echo 10

>/proc/sys/vm/swappiness is exactly the same as sysctl -w vm.swappiness=10. But as a rule of thumb, if a /proc/sys file is read-only, you cannot set it with sysctl either.

https://www.linux.com/news/kernel-tuning-sysctl
http://www.monitis.com/blog/20-linux-server-performance-tips-part-2/

TCP Window
We have seen the importance of the concept of window size to TCP's sliding window mechanism. In a connection between a client and a server, the client tells the server the number of bytes it is willing to receive at one time from the server; this is the client's receive window,

which becomes the server's send window. Likewise, the server tells the client how many bytes of data it is willing to take from the client at one time; this is the server's receive window and the client's send window.

How to determine TCP initial window size and scaling option? Which factors affect the determination?

https://access.redhat.com/solutions/29455

TCP and UDP Headers
https://www.lifewire.com/tcp-headers-and-udp-headers-explained-817970

how do you setup a network between 3 locations
http://www.businessinsider.com/the-5-most-cost-efficient-ways-to-set-up-your-companys-technology-network-across-multiple-offices-2011-4#5-be-consistent-5

Layer2 and Layer3
Overview. Traditional switching operates at layer 2 of the OSI model, where packets are sent to a specific switch port based on destination MAC addresses.
Routing operates at layer 3, where packets are sent to a specific next-hop IP address, based on destination IP address.

OSI Layers

Each layer in the OSI model serves the layer above it. There are 7 layers in total in the OSI model. Here's a quick run down of each of them:
1.The physical layer: Layer 1 is concerned with the transmission of data bits over physical mediums.
2.Data link: Layer 2 specifies transmission of frames between connected nodes on the physical

layer.
3.Network: Addressing, routing and traffic control of a multi-node network is described by Layer 3.
4.Transport: Segmentation, acknowledgement and multiplexing between points on a network is defined at Layer 4.
5.Session: Layer 5 looks at the continuous exchange of data between two nodes
6.Presentation: Encoding, data compression and encryption / decryption between a network service and application happens at Layer 6.
7.Application: Resource sharing, high level APIs and remote file access is defined by Layer 7.

https://www.wideband.net.au/blog/difference-layer-3-layer-2-networks/

It's less a question of which is better, as both layers of the OSI have their role in the architecture of network performance. An L2 network would be more useful broadcasting information between two computers in the same office, close together, where a broader network

wouldn't be affected by congestion.

However, because L3 network switches work with routing of IP addresses, they are better for managing network traffic over multiple sites and through the internet. This highlights the fundamental difference between the two layers of abstraction and how they function as

switches. Determining which is better is up to you and your requirements.

A subnetwork or subnet is a logical subdivision of an IP network. The practice of dividing a network into two or more networks is called subnetting. ... Subnet masks are also expressed in dot-decimal notation like an address

Network Bits Subnet Mask Number of Hosts

/24 255.255.255.0 254
/25 255.255.255.128 126
/26 255.255.255.192 62
/27 255.255.255.224 30

Calculating the maximum possible number of hosts in a subnet: To find the maximum number of hosts, look at the number of binary bits in the host number above. The easiest way to do this is to subtract the netmask length from 32 (number of bits in an IPv4 address). This

gives you the number of host bits in the address

The network address is the logical AND of the respective bits in the binary representation of the IP address and network mask. Align the bits in both addresses, and perform a logical AND on each pair of the respective bits. Then convert the individual octets of the result

back to decimal.

Calculating the maximum possible number of hosts in a subnet:

To find the maximum number of hosts, look at the number of binary bits in the host number above. The easiest way to do this is to subtract the netmask length from 32 (number of bits in an IPv4 address). This gives you the number of host bits in the address. At that point...

Maximum Number of hosts = 2**(32 - netmask_length) - 2

The reason we subtract 2 above is because the all-ones and all-zeros host numbers are reserved. The all-zeros host number is the network number; the all-ones host number is the broadcast address.

Using the example subnet of 128.42.0.0/21 above, the number of hosts is...

Maximum Number of hosts = 2**(32 - 21) - 2 = 2048 - 2 = 2046

https://networkengineering.stackexchange.com/questions/7106/how-do-you-calculate-the-prefix-network-subnet-and-host-numbers

Cloud computing
Cloud computing is the on-demand delivery of compute power, database storage, applications, and other IT resources through a cloud services platform via the internet with pay-as-you-go pricing. the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer.

RAID

RAID works by placing data on multiple disks and allowing input/output (I/O) operations to overlap in a balanced way, improving performance
RAID 0 -Striping no redundancy
RAID 1 Redundancy

File Transfer Protocol (FTP) (RFC 959) TCP 20/21
Secure Shell (SSH) (RFC 4250-4256) TCP 22
Telnet (RFC 854) TCP 23
Simple Mail Transfer Protocol (SMTP) (RFC 5321) TCP 25
Border gateway protocol 179 TCP

Network Time Protocol (NTP)
UDP
123

DHCP
UDP
67/68

HTTP Codes
400 Bad Request
The request could not be understood by the server due to malformed syntax
403 Forbidden
The server understood the request, but is refusing to fulfill it.
503 Service Unavailable
The server is currently unable to handle the request due to a temporary overloading or maintenance of the server

MFT
Managed file transfer (MFT) is a type of software used to provide secure internal, external and ad-hoc data transfers through a network

default gateway is the node in a computer network using the Internet Protocol Suite that serves as the forwarding host (router) to other networks when no other route specification matches the destination IP address of a packet.

The kernel connects the system hardware to the application software

How to build a cloud

Now let's look at what it takes, step by step, to build a private cloud. While there are many patterns that can be found in traditional IT, there are some new approaches and technology that must be understood.

Orange FlagStep 1: Define the Purpose: Understand the requirements of the business and those force on you by security regulations and operational considerations.
Red FlagStep 2: Define the Workloads: Determine what types of applications and application data will run on the private cloud, by dividing workloads into applications, data and infrastructure.
Green FlagStep 3: Define the Hardware: Take the data gathered in the previous step and size up a hard- ware system that will provide the right support now, and into the future
Brown FlagStep 4: Define the Software: Decide if you want to go proprietary or open. If you're moving to open solutions, OpenStack is the primary choice.
Blue FlagStep 5: Define the Network: Define how your network will work on your private cloud – physical network provisioning, software defined network elements if any, security, network management.
Orange FlagStep 6: Define Security: Plan your Identity and Access Management (IAM) – a security approach and technology that enables the right individuals to access the right resources, at the right times.

Red FlagStep 7: Define Governance: Once you get to a certain number of cloud services, you won't be able to keep track of them all and provide the control they will require. Plan your service governance model in advance.
Green FlagStep 8: Define Management Processes and Tools: Define monitoring practices, physical infrastructure including network, power supplies, and more.
Brown FlagStep 9: Implementation: Stage the private cloud, including hardware and software in your data center.
Blue FlagStep 10: Testing: Define test processes to verify you are fully meeting requirements and prepared for security issues, downtime or failure.
Orange FlagStep 11: Operations: Define how you will operate the cloud – monitoring, automation, security, governance, etc. This is known as CloudOps

Cloud Security

Cloud computing security or, more simply, cloud security refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing

Strict Regulatory Standards Higher regulatory requirements lead to better security solutions.
Security Tools Many top cloud providers include access to extra security programs
Confidentiality Customer data is kept confidential.
DDoS Mitigation A bigger company is able to better protect against DDoS attacks
Distributed Denial of service

http://bencane.com/2014/09/02/understanding-exit-codes-and-how-to-use-them-in-bash-scripts/
On Unix and Linux systems, programs can pass a value to their parent process while terminating
Exit codes are a number between 0 and 255, which is returned by any Unix command when it returns control to its parent process.
Success is traditionally represented with exit 0,failure is normally indicated with a non-zero exit-code

I am Praveena Bapatla.
I am an innovative and technology passionate individual with 6 progressive years of experience at xx, managing all aspects of the Infrastructure Build and System Administrative support in Solaris and Linux Environments. During my tenure I have contributed to the

organization to the best of my knowledge and I have even automated several tasks on daily basis which resulted in cost saving.I have won several performance awards and been promoted twice. Although I love my current role, I feel I'm now ready for a more challenging assignment and this position really excites me

I feel My current skil set , extensive experince in the domain and my innovative thought process would match this profile. I can see my self growing along with organization and I can add great

with extensive experience in all these aspects, good troubleshooting skills and strong communications skills, I ~~will be great match to this role at Pebble I.T and I can~~ feel I can add a great value to this role at PebbleTT and I can see myself growing along with the company.

Prep-14thMArch.txt

value to the company.

I'm a person who thrives in a fast-paced environment so right now I'm looking for an opportunity to apply my technical experience and my creative problem solving skills at an innovative software company like this one."

My day to day activitlities inludes
PRB queue Monitoring
Fixing issues referenceed to them like File systems issues,.....etctc(chekc resume and chkec with Rashmitha)
patching and firmware upgrade on scheduled times
Coordinating for Hward ware replacements
Sofware installations through change requests
Application/DBA support as needed

I am an innovative & Technology passionate individual with about 6 ~~years~~ progressive years of experience at Wells Fargo which is one of major US Banking/Financial Firms.

My Responsibilities are managing all aspects of Infrastructure Build & System Administrative Support in Solaris & Linux ~~Environments~~ Including, patching, Provisioning new builds on physical & virtual Environments; Performing OS upgrade/refresh as required, Installing & Configuring Layered Products like Netbackup, monitoring tools, File systems utilization issues, ~~Adding~~ Creating/extending File systems, ~~set~~ ~~up~~ ~~configure~~ OS tuning ~~the~~ ~~new~~ as required by application or DB services ~~requirement~~, Patching/Firmware upgrades on scheduled times. Apart from these Monitoring problem ticket queue on daily basis addressing the issues referenced by them, within ~~Providing~~ defined SLA's. Providing OS support to Dev, Testing, & UAT Teams. ~~I am good at shell scripting, during the tenure~~ I have automated few tasks like OVO upgrade, precheck for patching & OS upgrade, zone creating installation using shell scripts. I have good understanding of Python as well, and I know basics of PERL too. I have ~~a~~ subordinate knowledge/experience with WINDOWS Ad/VMware Administration ~~I have experience~~ during the tenure I have contributed to the best of my knowledge. I ~~have~~ regularly work documenting new processes & technical procedures to help service delivery.