Linux User Management Interview Questions

1) Which files stores the user min UID, max UID, password expiration settings, password encryption method being used etc.,?

ANS : /etc/login.defs

2) How do you make a file copied to a new user account automatically upon user account creation?

ANS : Store the file in /etc/skel directory.

3) List the fields in /etc/passwd file.

ANS : UserName | Password | UserID | GroupID | Comments | HomeDir | LoginShell

redhat:x:500:500:Redhat User:/home/redhat:/bin/bash

mssm:x:501:501:another user:/home/mssm:/bin/bash

– “x” in the password column indicates that the encrypted password is stored in /etc/shadow file.

4) How to lock an user account?

Example:-

#usermod -L mango

Once an account gets locked, there would be an exclamation mark before the encrypted password files in “/etc/shadow” as shown below:

mango:!1O5zV5Rj/$XhuRe8Og.AiXMXDGSIsae/:16266:0:99999:7:::

To un-lock an account:-

#usermod -U mango

5) How to disable user login via terminals?

ANS: Add “/sbin/nologin” field instead of “/bin/bash” in “/etc/passwd” file.

Linux Administrator Interview Questions And Answers For Frehsers

6) Which commands are normally recommended to edit “/etc/passwd”, “/etc/shadow”, “/etc/group” and “/etc/gshadow” files?

ANS: vipw > edit the user password file (/etc/passwd)
vigr > edit the user group file(/etc/group)
vipw -s > to edit shadow password file (/etc/shadow)
vigr -s > to edit shadow group file (/etc/gshadow)

These commands would normally lock the file while editing to avoid corruption.

7) Whenever an user **tries to login via terminal,** system **would throw up the error "The account is currently not available", otherwise, via GUI when** user **enters** password**, it looks to be logging in, however, comes back to the login prompt. How could this issue be fixed?**

ANS: This is because of the shell field set as "/sbin/nologin" in "/etc/passwd" file, so change this back to "/bin/bash" and user should be allowed to login.

If the shell field is set as "/bin/false" then whenever an user tries to login there would not be any error or messages, it just comes back to the login prompt and same happens in GUI mode.

(8) How do you make a new user to reset his password upon **his first login?**

{ The prompt should come up like below }

[redhat@localhost ~]$ su – mango
Password:
You are required to change your password immediately (root enforced)
Changing password for mango.
(current) UNIX password:

{ The prompt should come up like above }

ANS: Use 'chage' command and set the expiration date as given below

[root@localhost skel]# chage -d 0 mango

<< To view password aging details >>

[root@localhost skel]# chage -l mango
Last password change : password must be changed
Password expires : password must be changed
Password inactive : password must be changed
Account expires : never
Minimum number of days between password change : 0
Maximum number of days between password change : 99999
Number of days of warning before password expires : 7

(9) Create users home directory in /home1 directory instead of default /home directory. This gets applicable to any new users who gets created i.e the home directory of that user should be /home1/<UserName>/

ANS: – Edit /etc/default/useradd

– Change the line : HOME=/home1

– Save the changes and exit. After this any new users home directory would be under /home1

– You could check the useradd defaults using the command :#useradd -D

OR

#cat /etc/default/useradd

After this you can add users with the command “useradd <UserName>”. This would create the users home directory with the name of the user under the specified HOME directory as defined in /etc/default/useradd.

EXAMPLE:- adding user with “-d”

[root@Redhat5Lvm ~]# useradd -d /root/doctor alldoctors
[root@Redhat5Lvm ~]# grep alldoctors /etc/passwd
alldoctors:x:912:913::/root/doctor:/bin/bash

[root@Redhat5Lvm ~]# ls -ali /root/doctor/
total 28
607780 drwx—— 3 alldoctors alldoctors 4096 Aug 3 00:31 .
543457 drwxr-x— 18 root root 4096 Aug 3 00:31 ..
608253 -rw-r–r– 1 alldoctors alldoctors 33 Aug 3 00:31 .bash_logout
608252 -rw-r–r– 1 alldoctors alldoctors 176 Aug 3 00:31 .bash_profile
608251 -rw-r–r– 1 alldoctors alldoctors 124 Aug 3 00:31 .bashrc
608248 drwxr-xr-x 4 alldoctors alldoctors 4096 Aug 3 00:31 .mozilla

(10) How do you make/grant complete access (rwx) on files created for a user and deny any level of access to others including group?

ANS : – Need to define the umask value for the required user.
– This can be done by editing .bash_profile file.

For example, if we need to define this for a user “mmurthy” then we need to edit this file “/home/mmurthy/.bash_profile” and define umask as given below (assuming that the default home directory location is not changed):

umask 0077

– Save and exit the file.
– Next time this user logs in, files/directories would get exclusive permissions only for this user as masked by umask parameter.
– For root user the umask is defined in “/etc/init.d/functions” file. Otherwise, in /etc/profile (login shell) or /etc/bashrc (non-login shell) file.

Linux System Admin Interview Questions And Answers

(11) How to check if an user **account has been locked?**

ANS:- Run the command “passwd -S <UserName>”, this would show if the password has been locked or not. Otherwise, grep for the username from /etc/shadow file and you could see “!” mark prefixed to the encrypted password field.

[root@server6 ~]# passwd -S smurthy
smurthy LK 1970-01-01 0 99999 7 -1 (Password locked.)

[root@server6 ~]# grep smurthy /etc/shadow
smurthy:!!6jZqvS4ju$k.o6o7OoL7EZ1Bn52uPKeI2gqA76A7qyTl2PM8192jF2mz4ssVTz/u8DfbY2zJ7xCjFymh5FuATWxW5RxFugM1:0:0:99999:7:::

If you notice a double exclamation mark here ("!!") this indicates that the account got locked-up by running the command "passwd -l <UserName>" command (available only for root user). Otherwise, a single exclamation mark indicates that the account got locked with the command "usermod -L <UserName>". Accounts locked with usermod command would record it in /var/log/secure file by default.

To "unlock" an user account, run this command "passwd -u <UserName">. Otherwise, run "usermod -U <UserName" command twice to get rid off double exclamation marks in the encrypted password field.

Otherwise, "usermod -U <UserName" would unlock an account locked by the "usermod -L <UserName>" command.

EXAMPLE:-

[root@server6 ~]# grep smurthy /etc/shadow
smurthy:!!6jZqvS4ju$k.o6o7OoL7EZ1Bn52uPKeI2gqA76A7qyTl2PM8192jF2mz4ssVTz/u8DfbY2zJ7xCjFymh5FuATWxW5RxFugM1:0:0:99999:7:::

[root@server6 ~]# passwd -S smurthy
smurthy LK 1970-01-01 0 99999 7 -1 (Password locked.)

[root@server6 ~]# passwd -u smurthy
Unlocking password for user smurthy.
passwd: Success

[root@server6 ~]# grep smurthy /etc/shadow
smurthy:6jZqvS4ju$k.o6o7OoL7EZ1Bn52uPKeI2gqA76A7qyTl2PM8192jF2mz4ssVTz/u8DfbY2zJ7xCjFymh5FuATWxW5RxFugM1:0:0:99999:7:::

[root@server6 ~]# passwd -S smurthy
smurthy PS 1970-01-01 0 99999 7 -1 (Password set, SHA512 crypt.)

(12) How to find out the shadow password encryption method being used in Linux? How could this be changed (example : from md5 to sha512)?

ANS:- We can find out the password encryption method being used for shadow passwords as shown below:

– Check in /etc/login.defs

[root@server8 ~]# grep -i crypt /etc/login.defs
Use SHA512 to encrypt password.
ENCRYPT_METHOD MD5
MD5_CRYPT_ENAB yes

OR

– Check using “authconfig” command:
[root@server8 ~]# authconfig –test|grep hashing
password hashing algorithm is md5

OR

– Check the password beginning character in the second field of /etc/shadow file:

If it begins with = $6 > indicates sha512
$5 > sha256
$1 > md5
Examples:

ty2:6EyoeIHFK$L2PAXcXRo.Q5Y7zUweYkste8PtiL/CqYJ9Z/
ydBvRIOqvsegpVtOU1hDfkFdUpTcmjEou4kzL/Ej5MF2HdAB7.:16378:3:100:7::16489:
ty3:5Bsv43yG6$/Oa4fhlKF65XW8ROohKnJaSxVIIEhUKFUEdiIcOEfY4:16378:0:99999:7:::
ty5:$1$5J4jzULD$dKGfhSIzXp50Y4mwZxcqB/:16379:0:99999:7:::

To Change Password Encryption Method to sha512:

#authconfig –passalgo=sha512 –update {this would change the password encryption method to sha512}

Verify if it got changed successfully:

[root@server8 ~]# grep -i crypt /etc/login.defs
Use SHA512 to encrypt password.
ENCRYPT_METHOD SHA512
MD5_CRYPT_ENAB no

[root@server8 ~]# authconfig –test|grep hashing

password hashing algorithm is sha512

(13) What are the possible causes when an user **failed to login** into **a Linux system (physical/remote console); despite providing proper credentials?**

ANS:- Here are the possible reasons why an user fails to login into console:

– Account Locked.

When user tries to login via GUI receive an error “authentication failure” after entering password and it goes back to the user list prompt.

In CLI mode, after entering user password, it would fail with an error “incorrect password”. However, if user tries “su” from root account, access would get granted.

– Account Expired.

When account expired, an error notifying about the same would be shown up.

– Shell Disabled

After entering password in GUI, system shows a progress, however, could come back the login prompt. When this user attempts login via CLI, would receive an error “This account is currently not available”. For example, do disable shell of an user “test” : #usermod -s /sbin/nologin test (this only locks only terminal login, however, GUI login would work)

– Only Non-root Users Failed To Login.

If all non-root users are unable to login via GUI/CLI, however, root could login then this could be because of the file “/etc/nologin” presence on the system.

– Only Non-root Users Failed To Login in CLI.

If all non-root users are unable to login via CLI, however, can login via GUI then it would be because of /tmp space limitations. Need to check if /tmp is configured and mounted separately and check free space under /tmp.

– User login failed from GUI or from text console, however, could do su.

If an user fails to login from GUI/Console, however, could login from other user accounts by running ‘su’ then it could be due to pam restrictions. One could use “pam_access” module to restrict login. Need to add :

account required pam _access.so

to files : /etc/pam.d/login & /etc/pam.d/gdm-*

After this add ” – : <UserName> : ALL ” to /etc/security/access.conf file. For example to limit user “test”, we could add below line to access.conf file;

– : test : ALL

{{ there would an error “permission denied” in GUI when user is restricted to login via pam}}

– Only root user login failed from console, however, works in GUI.

This could be because of no terminals available or defined in /etc/securetty file.

If an user failed to login remotely via ssh then the reasons could be different. Here are the reasons:

– User Restricted.

If “AllowUsers” parameter is configured in /etc/ssh/sshd_config then need to add required user to this list to get access.

– Max Logins Set.

If “maxlogins” parameter is set in /etc/security/limits.conf then user would be allowed up to the parameter set and further connections would be denied. There could be “maxsyslogins” configured as well to limit concurrent access to a system.

(14) How to manually add user **without using “**useradd/adduser**” or “**system-config-user**” utilities?**

ANS: Create required directory under /home (default home directory for all local users) and set permissions.

#mkdir /home/user1
#chmod 700 /home/user1

[root@host1 mail]# ls -ld /home/user1
drwx——. 4 user1 user1 4096 Jan 24 07:19 /home/user1

<> Now, edit /etc/passwd file to manually set required parameters for the new user “user1”:

#vipw (this command would block multiple edits of /etc/passwd file)

user1:x:2000:2000:local user:/home/user1:/bin/bash

[root@host1 ~]# grep user1 /etc/passwd

user1:x:2000:2000:local user:/home/user1:/bin/bash

<> Create required group by editing /etc/group file using command ‘vigr’:

#vigr
user1:x:2000:

<> Next step is to create the local profile files for the new user by copying from /etc/skel.

[root@host1 ~]# cp -arv /etc/skel/. /home/user1
`/etc/skel/./.bash_profile’ -> `/home/user1/./.bash_profile’
`/etc/skel/./.bash_logout’ -> `/home/user1/./.bash_logout’
`/etc/skel/./.mozilla’ -> `/home/user1/./.mozilla’
`/etc/skel/./.mozilla/extensions’ -> `/home/user1/./.mozilla/extensions’
`/etc/skel/./.mozilla/plugins’ -> `/home/user1/./.mozilla/plugins’
`/etc/skel/./.gnome2′ -> `/home/user1/./.gnome2′
`/etc/skel/./.bashrc’ -> `/home/user1/./.bashrc’

<> Change permissions of all the files under /home/user1 to be owned by new user:
#chown -R user1:user1 /home/user1

– Try logging in as new user and test.

For user mail requirement, need to create a proper file under /var/spool/mail (default mail box location) with username and permissions:

#cd /var/spool/mail
#touch user1
#chown user1:mail user1

#chmod 660 user1

Linux Administration Interview Questions And Answers

Here you will learn more about **advanced Linux administration interview questions** and answers to succeed in your next Linux interview.

Linux Shell Scripting Interview Questions And Answers

1) How to create simple shell scripts in Linux?

ANS: Make sure that the file begins with “#!/bin/bash” before any command lines. Make it executable : chmod +x <filename>. Executed by running “sh <filename.sh>” OR <./filename.sh>”.

2) Which command to be used to check the shell being used?

ANS: echo $SHELL
echo $0

Like-wise :

#echo $?
…..this shows the exit status of the most previous process command ran in shell.

#echo $$
….this shows current shell ID (when run inside a script this would print the PID assigned to the shell)

#echo $@ OR #echo $*

….this prints the arguments passed when called for execution.

#echo $#
…..this would show up total number of arguments passed.

#echo $!
…..this would report PID of previous background process.

To check these, run a small script as shown below :
#!/bin/bash
echo -e “Print Current shell ID (\$$): $$”
echo -e “Arguments passed (\$@): $@”
echo -e “No of arguments passed (\$#): $#”
echo -e “This also prints arguments passed (\$*): $*”
……..example:
[root@ansible-host tmp]# ./test.sh 1 2 3

Print Current shell ID ($$): 107199
Arguments passed ($@): 1 2 3
No of arguments passed ($#): 3
This also prints arguments passed ($*): 1 2 3

Linux Log File Interview Questions And Answers

1) Where are the log files stored usually in Linux**?**

ANS: under /var/log

2) How to check if the syslog **service is running?**

ANS: /etc/init.d/rsyslog status OR service rsyslog status, otherwise, using “systemctl status rsyslog.service (in RHEL7.x).

3) By default log files are set to get rotated on weekly **basis, how to make this gets rotated on** monthly **basis?**

ANS: Edit /etc/logrotate.conf and change below lines

rotate log files monthly
monthly

Save changes and if you want to rotate the log files immediately then run the command:

#logrotate -f /etc/logrotate.conf

4) How do you check the boot messages (kernel ring buffer)?

ANS:- Using “dmesg” or #cat /var/log/dmesg

5) How to increase size of ‘kernel ring buffer’ file (dmesg)?

ANS:- By default the kernel ring buffer size is 512 bytes. So, to increase this space add “log_buf_len=4M” to the kernel stanza in grub.conf file.

Advanced Linux Administration Interview Questions And Answers

6) What does /var/log/wtmp **and /var/log/**btmp **files** indicates **and what do they store?**

ANS:- These files are used to store user login/logout details since from the date of creation.

The user login, logout, terminal type etc are stored in /var/log/wtmp and this is not a user-readable file, so “last” command reads data from this file (or the file designated by the -f flag).

All un-successful(bad) login attempts are recorded in /var/log/btmp which could be displayed using the command “lastb”. All these login/logout events would also get recorded in /var/log/secure file (this file usually stores all authentication/authorization events).

Like-wise, there is /var/log/lastlog which records most previous successful login event of users. In earlier RHEL versions (RHEL 5.x) there used to be a file /var/log/faillog to hold failed login events which had become obsolete since RHEL6.1 and is no longer available.

Linux Package Interview Questions | Linux YUM Interview Questions

1) What does 'ivh' represents in rpm -ivh <PackageName> command?

ANS: i – install
v – verbose mode
h – hash mode where it would print ## characters as the installation progresses

2) What is the difference between rpm -F <PackageName> and rpm -U <PackageName>?

ANS: rpm -F = Basically freshens a package which in turn upgrades an existing package, otherwise doesn't install it if an earlier version not found.
rpm -U = Upgrades an existing package if exists otherwise install it.

3) How to find to **which package the "ls" commands belongs to (to find out package responsible for this command)?**

ANS : #rpm -qf /bin/ls {this would tell about the package to which this command (binary file) belongs to if installed by that package}

4) How to find out the configuration files installed by a package (take into consideration of the "coreutils**" package)?**

ANS : # rpm -qc coreutils

To list out only the document files installed by coreutils package:-
rpm -qd coreutils

To list out all the files installed by this package:-
#rpm -ql coreutils
OR
#rpm -q – -filesbypkg coreutils

To list out dependencies :-
#rpm -qR coreutils

To list out packages which require this package:-
#rpm -q –whatrequires coreutils

To find out more information of this package:-
#rpm -qi coreutils

To find out any scripts executed by this package:-
#rpm -q –scripts coreutils

Similarly, to find details of package which is not yet installed:

List Files In Package:
#rpm -qpl <PathOfPackageNotYetInstalled>

{The list would show up files which would get added to system after installing package}

List Only Config Files:
#rpm -qpc <PathOfPackageNotYetInstalled>

List Only Document Files:
#rpm -qpd <PathOfPackageNotYetInstalled>

List Out Dependancies For This Package:
#rpm -qpR <PathOfPackageNotYetInstalled>

List Details For This Package:
#rpm -qpi <PathOfPackageNotYetInstalled>

5) How do you find out all the packages installed on a RHEL system(server)?

ANS : – /root/install.log > this would only lists packages installed during deployment of the system. Packages installed later would not be listed here.
– Otherwise, run the command #rpm -qa > this would query rpm database and prints out names respectively.

– In RHEL5.x we can check the file : /var/log/rpmpkgs to find out all packages on the system. However, this file is deprecated in RHEL6.

– Note: In Red Hat Enterprise Linux 6, the daily cron file to create /var/log/rpmpkgs is provided by the rpm-cron package, available in the optional repository, not the main ‘rpm’ package. So, if you do not install the package, /var/log/rpmpkgs is not available on Red Hat Enterprise Linux 6. (Ref – https://access.redhat.com/solutions/23743)

Senior Linux Administrator Interview Questions For Experienced

6) How to create a local yum repository which would make use of the mounted linux **ISO image under /**media ?

ANS : Create files ending with .repo extension under /etc/yum.repos.d directory with proper syntax:

[root@localhost yum.repos.d]# cat local.repo
[local]
name=RHEL6.5
baseurl=file:///media
enabled=1
gpgcheck=1
gpgkey=file:///media/RPM-GPG-KEY-redhat-release

7) Different ways that can be used to verify that a package got installed successfully via yum:

ANS : ==Method 1==

– Immediately after running yum command, check exit status, if it shows “0” (numeral) then command executed successfully.

[root@localhost yum.repos.d]# echo $?
0

==Method 2==
– Run rpm -qa and test.

[root@localhost yum.repos.d]# rpm -qa | grep certmonger
certmonger-0.61-3.el6.x86_64

==Method 3==
– Verify with rpm command:

[root@localhost yum.repos.d]# rpm -V certmonger

==Method 4==
– Check the yum log to see the successful log entry about the same package.

[root@localhost yum.repos.d]# grep certmonger /var/log/yum.log
Jul 15 10:33:22 Installed: certmonger-0.61-3.el6.x86_64

8)How to view the installed date of a package (consider the package sg3_utils)?

ANS:- Check in /var/log/yum.log file (provided the package is installed by yum):-

[root@server8 ~]# grep sg3_utils /var/log/yum.log
Oct 22 12:11:38 Installed: sg3_utils-1.28-4.el6.x86_64

OR

Use the command “rpm -q <PackageName> –last”

[root@server8 ~]# rpm -q sg3_utils –last
sg3_utils-1.28-4.el6.x86_64 Wed 22 Oct 2014 12:11:37 PM PDT

OR

Using the “rpm -qi <PackageName> | grep “Install Date” command

[root@server8 ~]# rpm -qi sg3_utils|grep “Install Date”
Install Date: Wed 22 Oct 2014 12:11:37 PM PDT Build Host: x86-004.build.bos.redhat.com

In RHEL 5.x, one could use /var/log/rpmpkgs file to check this. To get a list of all the packages installed date: #rpm -qa –last

9) If for some reasons, a binary file gets corrupted or missing from the system, then how could this be recovered with minimal downtime?

ANS:- In first attempt, one could try to copy the missing binary (executable) file from a similar working system using scp command.

In next attempt, if the above attempt not possible or doesn't work then we could extract this file from respective package and move it to the system.

Consider the situation wherein the binary command file /sbin/ifconfig is missing or corrupted, hence, unable to run this command. So, we'd need to extract this from package and install it.

Steps
———-

– Identify which package this command belongs to.

– On a working system, run the command 'rpm -qf /sbin/ifconfig'. This would tell which package has installed this executable file:

[root@rh413server sbin]# rpm -qf /sbin/ifconfig
net-tools-1.60-110.el6_2.x86_64

– Mount an iso which holds this package and then run "rpm2cpio" command with "cpio" to extract required file.

– Check if the required file is available in the package before extracting it.

[root@rh413server rpm]# rpm2cpio /media/Packages/net-tools-1.60-110.el6_2.x86_64.rpm |cpio –extract –list –verbose "*ifconfig"
-rwxr-xr-x 1 root root 69440 Apr 26 2012 ./sbin/ifconfig
1542 blocks

– Now, we know that this binary is available with this package, so we'd need to extract this file. Create a directory where to extract.

[root@rh413server package-restore-test]# rpm2cpio /media/Packages/net-tools-1.60-110.el6_2.x86_64.rpm |cpio –extract –make-directories –verbose "*ifconfig"
./sbin/ifconfig
1542 blocks

– The binary would be found under "sbin" directory within current directory.

[root@rh413server package-restore-test]# tree
.
└── sbin
└── ifconfig

1 directory, 1 file

– Later, move this binary file to /sbin folder and make sure proper permissions are set as required.

Linux File System | LVM Interview Questions And Answers

1) How to check what file systems are mounted and their read/write status?

ANS : #cat /etc/mtab
#cat /proc/mounts
#mount
#df -Th > this would not tell the read/write status

2) Where is grub.conf/grub.cfg file stored in RHEL systems?

ANS : In /boot/grub/ OR /etc/grub2 (in case of RHEL7.x) directory.

3) How do you remount a file system read only **on the fly?**

ANS : #mount -o remount,ro <Mountpoint>
– To make a file system gets mounted read only during boot ,need to edit fstab.

4) Command used to convert ext2 file system into ext3.

ANS : tune2fs -j <device or file system name>

5) How to run file system check on a logical volume in rescue mode?

ANS : – Boot into rescue mode (“linux rescue nomount”)
– Don’t mount any file systems, so “Skip” mounting.
– First make the logical volumes available by running these commands:
– lvm pvscan
– lvm vgscan
– lvm lvscan
– lvm lvchange -ay
– Next, run the file system check on the respective lvm.
– #e2fsck -fy /dev/vgname/lvname

6) How to reduce/extend a root lvm**?**

ANS : To Reduce – boot into rescue mode without mounting file system (linux rescue nomount).
– activate the lvms if required as explained in previous answer.
– run file system check on respective lvm.
– reduce file system : #resize2fs /dev/vg1/rootlv 5G
– Next, reduce the corresponding lvm : #lvreduce -L 5G /dev/vg1/rootlv (reducing the LV to 5GB)
– Run fsck again.
– Verify the lvm is reflecting the correct size.

To extend – no need to boot into rescue, this could be done online.
– unmount the respective file system first (this is not absolutely necessary, size can be extended online, but always recommended to unmount respective file system)
– Extend the lv : #lvextend -L +1G /dev/vg1/rootlv (extending the size to 1GB plus)

– Extend the file system : #resize2fs /dev/vg1/rootlv
– Run fsck if necessary.

7) How to verify if a filesystem state is marked as clean?

ANS : [root@redhat Desktop]# dumpe2fs -h /dev/sda1 |grep -i state
dumpe2fs 1.41.12 (17-May-2010)
Filesystem state: clean

OR

[root@server8 Desktop]# tune2fs -l /dev/sda1|grep -i state
Filesystem state: clean

8) How to find out backup superblocks for a logical volume?

ANS : [root@redhat Desktop]# dumpe2fs /dev/vg1/rootlv | grep -i “backup superblock”
dumpe2fs 1.41.12 (17-May-2010)
Backup superblock at 32768, Group descriptors at 32769-32769
Backup superblock at 98304, Group descriptors at 98305-98305
Backup superblock at 163840, Group descriptors at 163841-163841
Backup superblock at 229376, Group descriptors at 229377-229377
Backup superblock at 294912, Group descriptors at 294913-294913
Backup superblock at 819200, Group descriptors at 819201-819201
Backup superblock at 884736, Group descriptors at 884737-884737

OR
If the file system is un-mounted then could use mke2fs : #mke2fs -n /dev/vg1/rootlv | grep -i -A1 “superblock backup”

9) Find out list **of actual devices associated with a logical volume using** lvs **command?**

ANS : [root@redhat Desktop]# lvs -o +segtype,devices

LV VG Attr LSize Pool Origin Data% Move Log Cpy%Sync Convert Type Devices
homelv vg1 -wi-ao—- 1000.00m linear /dev/sda2(0)
rootlv vg1 -wi-ao—- 5.49g linear /dev/sda2(1000)
swaplv vg1 -wi-ao—- 1000.00m linear /dev/sda2(2500)
tmplv vg1 -wi-ao—- 1000.00m linear /dev/sda2(4000)
usrlv vg1 -wi-ao—- 6.37g linear /dev/sda2(2750)
usrlv vg1 -wi-ao—- 6.37g linear /dev/sda2(4250)
varlv vg1 -wi-ao—- 2.93g linear /dev/sda2(250)
testlv vg2 -wi-ao—- 52.00m linear /dev/sdb(0)

OR

– Using vgdisplay : #vgdisplay -v <vgname> {this would list out all the details of the VG including corresponding lvs and pvs within the VG}

— Physical volumes —
PV Name /dev/sdb
PV UUID nFwUZd-F4Cm-tbeq-y75d-OUzX-S2ze-rEeR8x
PV Status allocatable
Total PE / Free PE 25 / 0

PV Name /dev/sdc
PV UUID KWfeHu-cP6u-Qpdz-XzDD-iomY-uSKd-2d6V6G
PV Status allocatable
Total PE / Free PE 25 / 24

OR

– Check the latest lvm archive under /etc/lvm/archive/<archivename>:
[root@redhat Desktop]# grep device /etc/lvm/archive/vg2_00003-697546303.vg
device = "/dev/sdb" # Hint only
device = "/dev/sdc" # Hint only

10) How to set "rw" permissions on file for a user and disable for other users except root user (exclusive permissions)?

ANS : Use "setfacl -m u:<UserName>:<PermissionBits> <File/FolderPath>

#setfacl -m u:redhat:rw /testfile {redhat is an user here}.

To read use "getfacl" command: #getfacl /testfile

Linux Troubleshooting Interview Questions And Answers

11) Different fields in /etc/fstab**.**

ANS : – DeviceName MountPoint FilesystemType MountOptions DumpFrequency FsckCheckOrder

12) How do you skip the initial fsck(file system check) on a file system while booting up?

ANS : – Edit /etc/fstab and make the last column of the respective file system as 0 (number). This would skip the file system check process.

13) How to list all the files with SUID (Set User ID) bit set under the top level root directory and ignore any errors/warnings in the process, and list the output in long list format?

ANS:- find / -type f -perm -4000 2>/dev/null | xargs ls -l

14) How to list all the files/folders with SUID/SGID/Sticky Bit (Set Group ID) bit set under the top level root directory and ignore any errors/warnings in the process, and list the output in long list format?

ANS:- find / -type f -perm /7000 2>/dev/null | xargs ls -l

15) How to force file system check to run after random/maximum mount counts?

ANS:- One option is to use “tune2fs” (in Ext file systems) command to set this. There are two options “Maximum mount count:” & “Mount count:” which could be used to control after how-many mounts the file system check should be run. By default the “Maximum mount count:” option would be set “-1” when file system gets created which mask this feature. So, to get a file system check (fsck) on system reboot/reset this has to be set and which in turn depends on “Mount count”. These mount counts would get incremented after each system reset/restart.

Default option:

[root@rh413server yum.repos.d]# tune2fs -l /dev/sda2 |grep -i “mount count”
Mount count: 9
Maximum mount count: -1

So, to force ‘fsck’ on count reach of 10, we can tune-up the file system as shown below:

[root@rh413server yum.repos.d]# tune2fs -c 10 /dev/sda2
tune2fs 1.41.12 (17-May-2010)
Setting maximal mount count to 10
[root@rh413server yum.repos.d]# tune2fs -l /dev/sda2 |grep -i “mount count”
Mount count: 9
Maximum mount count: 10

Now, after the 10th mount of the file system, it would force a file system check and mount counter would be reset to 1.

Otherwise, there is another global option which could be used to make file system check after 180 days or after random number of mounts using “enable_periodic_fsck” in /etc/mk2fs.conf file as shown below:

[root@rh413server yum.repos.d]# grep -i enable_periodic_fsck /etc/mke2fs.conf
enable_periodic_fsck = 1

NOTE: To get this the e2fsprogs package should be at least “e2fsprogs-1.41.12-20.el6”. Hence, need to update older package. This has been added from RHEL 6.6 on-wards.

Ref: https://access.redhat.com/solutions/428583

16) How to search for all files with extension “*.log” in the current working directory and find out total disk space consumed and skip such files under any sub-directories?

ANS : – There are situations wherein an admin would required to find out total disk space consumed by those files such as “*.log” or “*.dat” etc., so one could use this command:

[root@ftp-server data]# find . -maxdepth 1 -name ‘*.log’ | xargs ls -l | awk ‘{ TOTAL += $5} END { print TOTAL }’
3045458

[root@ftp-server data]# find . -maxdepth 1 -name '*.log' -type f -exec du -bc {} + | grep total | cut -f1
3045458

If there are smaller files then running the 'find' command or 'du' command would work, however, if there are bigger files then one may come across error "argument is too long", so need to use "xargs" to parse output to avoid such errors. Ref : https://access.redhat.com/solutions/21118

$ find . -maxdepth 1 -name '*.dat' | xargs ls -l | awk '{ TOTAL += $5} END { print TOTAL }'
20134408530

16) What are the differences between hard & soft links in Linux file system?

ANS : –
Hard Links Soft Links

Gets created using same I-node number with a different name.

Gets created using alias name referring the original file name, but uses different I-node.

Can only be created within same file system.

Can be created across file systems.

Remains even if original file is removed.

Dies after original file is removed, otherwise exists as a dead link.

Can't be created for directories.

Can be used to create links to directories.

Linux Boot Kernel Interview Questions And Answers

1) I've installed the latest kernel on the system successfully, however, my server still boots from the old kernel. How do you make the system to boot from the newly installed kernel?

ANS : – Verify if the new kernel packages are installed successfully.
– Verify if the kernel stanza is added in grub.conf file.
– Make the new kernel as the default kernel to boot in grub.conf file. Either move the kernel stanza to be the first or change "default" entry according to the kernel stanza to boot.

2) There is an error during the boot stating "cannot resolve label for a file system" and system is dropping into single user mode. System would show up Ctrl+D error. How could this be fixed?

ANS : – Make a note of the file system for which the label failed to resolve.
– Boot into single user mode.
– remount root file system in rw mode = #mount -o remount,rw /
– use "blkid" or "e2label" or "findfs" or "lsblk -f" OR "check in /dev/disk/by-uuid/ or /dev/disk/by-label/" to find out the labels/UUIDs assigned to each mounted devices. If the label is not correct in

fstab then edit it.
– Exit and reboot. this would fix the label error.

3) Which command is to be used to create GRUB password to avoid normal user in editing GRUB interface while booting?

ANS :- Using the command “grub-crypt” (in RHEL 6.x). This generates an encrypted password using “sha512” algorithm. You could also use “grub-md5-crypt” which generates “md5” encrypted password.

– paste the generated encrypted password into grub.conf file wherever needed as shown below (only a part of grub.conf file is pasted below):

default=0
timeout=5
splashimage=(hd0,0)/grub/splash.xpm.gz
hiddenmenu
password –encrypted 1EgrNz1$MbdclVToRCCsOF7OuBEgb/
title Red Hat Enterprise Linux (2.6.32-431.el6.x86_64)

So, with the grub password added anyone who wants to pass arguments to kernel while booting has to enter the password by pressing “P” and then proceed. RHEL 5.x, uses “grub-md5-crypt” command by default to generate one and could use “password –md5 <password-hash>” format in grub.conf file.

4) How do you disable the “NetworkManager” service on runlevel 5?

ANS :- [root@redhat Desktop]# chkconfig –level 5 NetworkManager off

[root@redhat Desktop]# chkconfig –list NetworkManager
NetworkManager 0:off 1:off 2:on 3:on 4:on 5:off 6:off

NOTE: In RHEL7.x, NetworkManager is the standard and default daemon for managing network.

5) Which is the parameter that you would add to grub.conf while configuring kdump?

ANS :- crashkernel=128M (for 128MB crash memory) {crashkernel=0M-2G:128M,2G-6G:256M,6G-8G:512M,8G-:768M}

Linux Technical Interview Questions And Answers For Experienced

6) How can I reboot quickly into another kernel (if available) by-passing BIOS process?

ANS :- This is possible provided kexec-tools package is installed. Say for example there are two kernel images installed:
(kernel-2.6.32-642.4.2.el6.x86_64 & kernel-2.6.32-642.el6.x86_64), and running kernel is “2.6.32-642.4.2.el6.x86_64″, and to boot quickly boot into older kernel by-passing BIOS process, need to run the below commands:

#kexec -l /boot/vmlinuz-2.6.32-642.el6.x86_64 –initrd=/boot/initramfs-2.6.32-642.el6.x86_64.img –command-line=”$(cat /proc/cmdline)”

So, what the above command does is:

> kexec -l /boot/vmlinuz-2.6.32-642.el6.x86_64 <<< this specifies the which kernel image to load

> –initrd=/boot/initramfs-2.6.32-642.el6.x86_64.img <<< which initird image to load

> –command-line=”$(cat /proc/cmdline)” <<<< shows command-line parameters

Once the above command is executed successfully, run the command “kexec -e” to reboot quickly into older kernel.

Linux System Hardware Interview Questions And Answers

1) Commands:

– To check memory availability #free -m Or #cat /proc/meminfo OR top or #vmstat
– To check CPU details #cat /proc/cpuinfo Or lscpu (RHEL6) or check in dmesg
– To check the loaded modules #lsmod
– To load a module #modprobe
– To check all (active/inactive) network interfaces #ifconfig -a Or ip a Or #cat /proc/net/dev
– To scan bus so that all newly added devices/luns would come up: #rescan-scsi-bus.sh or #echo “- – -” > /sys/class/scsi_host/host<ID>/scan {to get the rescan-scsi-bus.sh command, need to install sg3_utils package}
– To check most recent system reboot :#last reboot | head -1 {last command reads from /var/log/wtmp, lastb reads from /var/log/btmp}

[root@redhat Desktop]# last reboot|head -1
reboot system boot 2.6.32-431.el6.x Thu Jul 17 15:43 – 17:09 (01:25)

– To check the most recent system shutdown time :#last -x|grep shutdown|head -1

[root@redhat Desktop]# last -x | grep shutdown|head -1
shutdown system down 2.6.32-431.el6.x Thu Jul 17 15:43 – 15:43 (00:00)

– To check processor statistics : #mpstat or #iostat {these commands belongs to sysstat package}

2) Common Standard Ports Used :

ANS: =
= 21/20 ftp
= 22 ssh
= 23 telnet
= 25 smtp
= 53 DNS (tcp/udp)
= 68 DHCP
= 69 TFTP
= 80/443 http/https (tcp)
= 88/464 Kerberos (tcp/udp)

= 110 pop3
= 123 NTP(udp)
= 137 nmbd
= 138,139,445 smbd
= 143 IMAP
= 161 SNMP
= 389/636 LDAP/LDAPS (tcp)
= 514 (udp) syslogd
= 2049 NFS

3) How to find out the system hardware details such as “manufacture, product name” etc,.?

ANS: Using “dmidecode”

#dmidecode –type system |egrep -i “Manufacturer|Product Name|Serial Number|Family”
OR
#dmidecode –type system |grep “System Information” -A 8

– To find out BIOS details :
#dmidecode –type bios |grep “BIOS Information” -A 6

Please visit my recent blog post for more details and easier way to get the information:

View System Hardware Info

4) The option “Open in Terminal” is missing when user right clicks on terminal in GUI. How to fix this?

ANS : This is basically because of missing package “nautilus-open-terminal”. Once this is installed, the right click option would show up.

5) How to change the default display manager or desktop from Gnome Display Manager (gdm) to kde?

ANS: You would need to install the KDE related packages first. Run command “yum groupinstall “KDE Desktop” to get all the KDE related packages to be installed (provided yum is configured). Once this is done, create the file “/etc/sysconfig/desktop” and add the below lines:

DISPLAYMANAGER=”KDE”
DESKTOP=”KDE”

After this change, restart the X window session.

In RHEL 5.x, you could use “switchdesk” command to switch to different display managers. So, to switch to KDE, you could use the command “switchdesk kde”. This may prompt to install “KDE Software Development” group if not installed.

Advanced Linux Administration Interview Questions And Answers

6) How to run ‘free’ command to print output of 2 instances with 2 seconds interval and store that output in a file (skipping any errors/warnings), and run this in background?

ANS:

```
[root@localhost ~]# free -s 2 -c 2 1> /tmp/free.out 2> /dev/null &
[1] 4836
[root@localhost ~]# cat /tmp/free.out
total used free shared buffers cached
Mem: 461456 349112 112344 0 12768 47780
-/+ buffers/cache: 288564 172892
Swap: 2031608 26712 2004896

total used free shared buffers cached
Mem: 461456 349120 112336 0 12768 47780
-/+ buffers/cache: 288572 172884
Swap: 2031608 26712 2004896

[1]+ Done free -s 2 -c 2 > /tmp/free.out 2> /dev/null
```

7) How to find out when was the last time a service got restarted?

ANS:- One way is to check in respective configured logs, otherwise, we could find the process start time using “ps” command.

For example, if you wish to find out the restart occurrence of “sshd” then check in /var/log/secure, you would see something similar to below lines:

```
Jun 18 05:29:18 nagios sshd[5413]: Received signal 15; terminating.
Jun 18 05:29:18 nagios sshd[5612]: Server listening on 0.0.0.0 port 22.
Jun 18 05:29:18 nagios sshd[5612]: Server listening on :: port 22.
```

Using ps command:

```
[root@nagios Desktop]# ps -p $(ps -C sshd -o pid=) -o lstart
STARTED
Thu Jun 18 05:29:18 2015
```

OR

```
[root@nagios Desktop]# ps -p $(pgrep sshd) -o lstart
STARTED
Thu Jun 18 05:29:18 2015
```

Replace the service name with respective service you wish to check far. To find out the most recent ‘httpd’ service restart time :

[root@nagios Desktop]# ps -p $(ps -C httpd -o pid=|head -1) -o lstart
STARTED
Thu Jun 18 05:34:35 2015

Otherwise, check in httpd log files, you would similar lines like below:

[Thu Jun 18 05:34:35 2015] [notice] caught SIGTERM, shutting down
[Thu Jun 18 05:34:36 2015] [notice] Apache/2.2.15 (Unix) DAV/2 PHP/5.3.3 configured — resuming normal operations

8) What is an elevator (disk elevator) or IO scheduler?

ANS:- It is an algorithm that is used by storage sub-system which takes care of how data gets re-arranged when called in for read/write and merges the requests in a way which would be efficient to the system.

To find out the elevator being used on a disk : # cat /sys/block/<DEVICE>/queue/scheduler

[root@ansible-host ~]# cat /sys/block/sda/queue/scheduler
noop anticipatory deadline [cfq]

To change an elevator on the fly:

[root@ansible-host ~]# echo deadline > /sys/block/sda/queue/scheduler
[root@ansible-host ~]# cat /sys/block/sda/queue/scheduler
noop anticipatory [deadline] cfq

To make changes permanent, add the elevator parameter (elevator=deadline) to grub configuration file into default kernel line.

Different elevator methods being used:

–“– Noop –“—

As the name implies this does nothing of data re-order or queuing, it just manages data as First-In-First-Out basis and would ideal when there is a separate storage based controller which does better data re-ordering and understanding of disk layout so that the kernel workload would gets reduced. This would be an ideal option when SSD drives are used.

–“– Anticipatory –“–

In this disk elevator algorithm, each read/write requests would wait a short time before after a request to see if another read/write request for nearby sector is coming up. So, each such requests would have “antic_expire” parameter set measured in milliseconds. If so it will wait for another antic_expire for another. However, each requests whether read/write would also have “read/write expire” parameter set which would serve the requests after the timeout count goes 0 (zero). This is ideal in case of contiguous reads such as FTP servers but not good for database servers.

–“– Deadline –“–

Just like how anticipatory elevator works, the deadline also maintains read/write expiry time outs, however, doesn't wait for a nearby request before moving requests into queue. Requests in queue would get served in batches based on FIFO. This best suited for servers which does heavy read/write operations such as database servers.

–"– CFQ (Completely Fair Queuing) –"–

This is designed for systems which does a lot of small disk read/writes and multiple processes would be generating disk IOs. This is default elevator being used in RHEL 6. This would normally be used in Desktop system or Usenet servers.

"deadline" is now the default IO scheduler in RHEL 7.x (except SATA drives) which was earlier "cfq" by default.

Linux Networking Interview Questions And Answers

1) How do you change the network speed of an interface to 100Mbps with auto-negotiation off and duplex in full mode(example for interface eth0)?

ANS : – #ethtool -s eth0 speed 100 autoneg off duplex full {changing the speed on the fly}
– To make this changes persistent need to add the below line to /etc/sysconfig/network-scripts/ifcfg-eth0 file:
ETHTOOL_OPTS="speed 100 autoneg off duplex full"

2) Every time the system reboots the network interface doesn't come up. However, if you restart network service or execute "ifup eth0" command which would bring up the network fine? How could this be fixed?

ANS : Make sure that "ONBOOT=Yes" is set in the respective configuration file (example in ifcfg-eth0 for eth0). In this case the "ONBOOT" parameter would be set to "NO".

– If the above step doesn't help then check /etc/sysconfig/network file and make sure "NETWORKING" is set to "Yes". {These are the most likely reasons in this case}

3) How do you check the network routing table using commands?

ANS : – #route -n
OR
#netstat -nr

4) After changing the network card on a system the network interface name got changed from eth0 to eth1. This shows when you run the command "ifconfig -a". Running "service network restart", shows this error "Device eth0 doesn't seem to be present". But when you run the command "ifconfig -a" you would notice eth1 is listed there instead of eth0. So, running "ifup eth1" shows error as "configuration for eth1 not found". How to make sure that the network interface becomes eth0 here and up along with the server?

ANS : – Make a note of the HW/MAC address of the second network interface here. {ifconfig eth1}
– Enter this MAC into the field “HWADDR” in ifcfg-eth0 file.
– Now, edit “/etc/udev/rules.d/70-persistent-net.rules file.
– You comment out the line of eth0 here and change the name of eth1 to eth0. Save and exit.
– Reboot the system. {this should fix the issue, tested on RHEL6.5 system}.

* This file has been deprecated in RHEL7.x [https://access.redhat.com/solutions/1554703]

—OR—

If the environment doesn’t permit of restart of the system then one could use “udevadm trigger” command to get the changes done without restart.

– First make sure the respective interface config file is present, if not then need to create one manually. In the question here, the interface name was changed from eth0 to eth1, hence, need to look out for ifcfg-eth0 interface file under “/etc/sysconfig/network-scripts” directory and change “HWADDR” and other fields as necessary (these options such as “Hwaddr”, “UUID” are not mandatory, if you wish then you could drop them or remove them if not required).

– Stop the network service. (#service network stop, assuming NetworkManager is not being used).

– Now, navigate to “/etc/udev/rules.d/” directory and edit “70-persistent-net.rules” file. Make sure the hardware address recorded here is correct and change the “NAME” attribute value to match your needs, save it and exit from vi mode.

– Trigger the udevadm to re-read network device rules.

#udevadm control –reload-rules
#udevadm trigger –verbose –subsystem-match=net

– Now, check out the currently available network interfaces (#ip addr show). This should show up modified one as “eth0” instead of “eth1”.

– Start the network service (#service network start).

– If for some reason the interface name don’t change, then unload network module and re-load it (this would drop off current connection, please be aware). If there is no direct access to systems then run a simple “at” command with required time stamp to load network modules, after which connections would work.

Linux Technical Interview Questions And Answers

5) How to fix/troubleshoot “no network” or “network down” or “unable to ping remote host” or “localhost doesn’t ping” problems?

ANS :- When network is down or unable to ping remote (another) host system, we’d need to start checking the following things sequentially:

<> Check if local network interface is working properly.

– Ping localhost to confirm that local network interface is up and required network modules are loaded. If unable to ping localhost check for following things:

<> Check if “lo” (loop-back) interface is up (ifconfig lo)

– You should see “UP LOOPBACK RUNNING” line in the output. If not then bring up the loopback interface : #ifup lo

<>Check if 127.0.0.1 address is mapped with localhost in /etc/hosts file. If there is no such entry then pinging 0 (numeral) would work, however, pining localhost would fail. So, add the entry as:

= 127.0.0.1 localhost

<> Check if at least one network interface is up on system.

#ifconfig eth0 (it could be any interface)

– This should show up a valid IP address and also would indicate if network is active (UP). If network is down then bring it up:

#ifup eth0

– If unable to get a valid IP address here, then need to check how is IP address being provisioned, it could be static or dynamic. If static then check in /etc/sysconfig/network-scripts/ifcfg-eth0 (i’ve taken eth0 as an example here) and look for valid entries as shown below:

DEVICE=”eth0″
BOOTPROTO=”static”
HWADDR=”00:0C:29:98:64:4C”
ONBOOT=”yes”
TYPE=”Ethernet”
UUID=”99b3f47f-5a68-4ffd-992a-aaa24ad12139″
IPADDR=”192.168.1.211″
NETMASK=”255.255.255.0″

– Bring up the interface if it is down :#ifup eth0
– Still unable to bring up network interface then restart the network service :
#service network restart
OR
#service NetworkManager restart

– If it is dynamic mode of IP address then check if there is any problem on the DHCP server. Try to set a test (static) IP address and check if that works.

<> Next step is to ping the hostname to confirm that name resolution works good.

#ping `hostname` OR ping <IPAddressOfeth0>

– If the above ping fails then ping the ipaddress directly and test if that works then problem with name resolution (DNS), so it should be either addressed at DNS level or fixing /etc/hosts file.

<> Ping another host/node OR Gateway address.

– Now, ping another host/node on the same network group. If ping success then we'd say routing is working, otherwise, check if gateway is configured properly. Ping the gateway address and check.

– Unable to ping another remote host then problem could be at the router end or routing problem. So, run traceroute at this stage and check where network is dropping connections.

<> Unable to ping anything either localhost or remote host or loopback address.

– This could be a problem either with firewall (iptables rules are set), otherwise, with sysctl settings configured on the system. Check if
"net.ipv4.icmp_echo_ignore_all" has been set in /etc/sysctl.con file, if so, please un-set this.

– If firewall problem, then make sure "icmp" protocol and "lo" interface is allowed for communication.

= iptables -A INPUT -i lo -j ACCEPT {A – Append OR I -Insert}

iptables -A INPUT -p icmp -j ACCEPT

6) What are the alternative steps that could be used to test a remote server alive status when ping check fails (if blocked by iptables)?

ANS :

–> Ping failure doesn't necessarily mean that remote host is down. In such cases it could be possible that ICMP replies would have been disabled (via sysctl) or blocked by firewall rules via iptables.

–> In this case, one could try to check if connectivity works via ssh. Try running ssh in verbose mode (ssh -v username@RemoteHostAddress). If this fails then this would indicate either ssh service is down or user-restricted or blocked by firewall on remote host.

–> At this stage we are still un-sure if remote host is up when both ping & SSH fails to get an acknowledgement. At this juncture, one may use an un-secure telnet (might require to install telnet package) to test if remote host is listening on a port. This would also not respond if port is blocked by firewall.

#telnet <RemoteHostIP> <PortNumber>

–> Next step when telnet also doesn't show up successful connection is to use nmap (belongs to nmap package)command which would scan the remote host and provides details about host live status along with ports which are filter/un-filtered.

#nmap -sn <RemoteHostIP>

–> This command would performs only host discovery without port scanning. This would fetch quick discovery of hosts alive status. Use "nmap -sn <RemoteHostIP> -n" to ignore name resolution. If the

nmap command returns “0 hosts up” or “Host seems to be down” then it would indicate a problem with remote system or network.

–> Optionally, there is “tcping” package available from EPEL which can be used to test remote host alive status using port ping.

#tcping <RemoteHostAddress> <PortNumber>

–> Also there is “netcat” utility (need to install this package) available which is another handy network tool which does a lot of functions including port scanning, so this could be used to test if a port on a remote host is allowed or blocked via firewall.

#nc -z <RemoteHostAddress> <PortNumber>

[root@server1 Desktop]# nc -z 192.168.1.100 22
Connection to 192.168.1.100 22 port [tcp/ssh] succeeded!

Linux Security Interview Questions And Answers

1) How do you backup and restore iptables (configurations)?

ANS : #iptables-save > /tmp/iptables.out
#iptables-restore < /tmp/iptables.out

2) What does the character “S” or “s” in the execute bit location of user permission indicates?

ANS : # “S” indicates that the SUID has been set, however, execute permission is not set. “s” indicates SUID has been set with execute permission.

3) How do you provide an user exclusive permissions to shutdown or reboot a system?

ANS : # Make the user sudo with appropriate permissions on the commands required.
– Edit the file /etc/sudoers using the command “visudo”.
– Add the below lines to /etc/sudoers file: (example to make user “raj” to execute shutdown/reboot commands)

{format
<username> <host>=<commands> }

raj ALL=/sbin/shutdown,/sbin/reboot,/sbin/poweroff

– The next user logins and executes the command “sudo /sbin/shutdown” the user would be prompted to enter password and upon successful authentication the command gets executed.

4) How to disable password-less login for root user in single user mode?

ANS:- Change the line that reads “SINGLE=/sbin/sushell” to “SINGLE=/sbin/sulogin” in “/etc/sysconfig/init” file.

This prompts for user (root) to enter a valid password to authenticate. However, if “init=/bin/sh” is passed as grub parameter then system would boot without prompting for password.

5) How to temporarily disable all user log-in except root user (either via SSH or terminal or in GUI)?

ANS:- This could be achieved by creating /etc/nologin file (as root user). If this file exists then any user who tries to log-in would gets rejected and only root user would be allowed (the root user may not be allowed to login via ssh if “PermitRootLogin” is set to “no” in /etc/ssh/sshd_config).

Linux Admin Interview Questions And Answers For Experienced

6) How to disable “Restart” & “Shut Down” buttons on the GUI Login screen?

ANS: In RHEL 6.x, you would need to use gconftool-2 or gconf-editor commands for this purpose.

Using gconftool-2 command:

To disable “Restart” & “Shut Down” buttons on the GUI log-in screen, run the below command as root user:

#gconftool-2 –direct –config-source xml:readwrite:/etc/gconf/gconf.xml.defaults –type bool –set /apps/gdm/simple-greeter/disable_restart_buttons true

These are defined as schemas in “/etc/gconf/schemas/gdm-simple-greeter.schemas” file.

Same way, if you wish to disable user list, run the below command as root user:

#gconftool-2 –direct –config-source xml:readwrite:/etc/gconf/gconf.xml.defautls –type bool –set /apps/gdm/simple-greeter/disable_user_list true

Using gconf-editor command:

Run “gconf-editor” command, expand “apps” and then “gdm”, click on “simple-greeter” and then check “disable_restart_buttons”, then right click on “disable_restart_buttons” and choose “Set as Default”.

In RHEL 5.x

The simplest way to achieve this in RHEL 5.x is to run the command “gdmsetup” in GUI as root user, un-check “Show Actions Menu” under “Menu Bar” in “local” tab. This would remove “Restart” & “Shut Down” buttons on the GUI log-in screen.

In RHEL 7.x

Edit (as root user) “/etc/dconf/db/gdm.d/01-custom-gdm-settings” file and the following lines:

[org/gnome/login-screen]
disable-user-list=true

Then update “dconf” database using the command “dconf update”, finally restart gdm service “systemctl restart gdm”

7) What does the umask value of 0022 indicates for a root user?

ANS:Before understanding this, one must understand the numerical values being used to represent permission bits in Unix environment. It is as shown below:

r – “read” permission – numerical equivalent value “4”
w – “write” permission – numerical equivalent value “2”
x – “execute” permission – numerical equivalent value “1”
s – “special” permission bit – numerical equivalent “4” for SUID (SetUserID), “2” for SGID(SetGroupID “1” for Sticky-bit.

u – “user”
g – “group”
o – “others”

Set/Unset Permissions: Using chmod command. Say for example you wish to set only “read & write (rw)” permission for owner, no permissions for group and others then this could be done like below:

$chmod 600 <filename> OR $chmod u+rw,go-rwx <filename>

Now, lets check what does 0022 umask value indicates:

0 – Indicates special character bit, not masked.
0 – Indicates mask nothing, all permission bits are set for “Owner”.
2 – Indicates mask 2 for “Group” (for files it is “x4x” meaning both read & write bits are set likewise for directories it is “x5x” meaning both read & execute bits are set)
2 – Indicates mask 2 for others (as explained above)

Saying so, when a root user creates a file/directory this umask bit would be used to set the effective permissions. For a file it would be (666-022=644), rw-,r–,r– (read&write,read,read) respectively for user, group and others (ugo). However, when a directory is created it would be (777-022=755) rwx,r-x,r-x for ugo. Same way the default umask value for other users is 0002.