Demo Questions

Oracle 1Z0-100 Exam

Oracle Linux 5 and 6 System Administration

Thank you for downloading 1Z0-100 Exam PDF

Question #1*Topic 1*

Which two statements are true concerning the installation and configuration of the bootloader by the Anaconda installer, which is then used to boot Oracle Linux?

- A. The Linux Loader (LILO) bootloader may be chosen for installation.
- B. The bootloader must be password protected and Anaconda prompts for a password in all cases.
- C. The Grand Unified Bootloader (GRUB) is the only bootloader used by Oracle Linux.
- D. If previously installed operating systems are found on disk partitions that were not overwritten, then an attempt is made to configure the bootloader to be able to boot them.
- E. The bootloader is installed by default in the first partition of the disk.

Correct Answer: *AE*
A (not C): Linux boot process from hard drive:
1. PC initializion phase - BIOS, POST.
2. PC starts boot loader - usually grub or lilo.
3. The bootloader locates kernel image on the hard drive.
4. The kernel decompresses and loads itself. Once finished it tries to mount the root filesystem. 5. When the root filesystem is mounted, /sbin/init is executed and continues booting the system using inittab and /etc/rc*.d scripts

Question #2*Topic 1*

You want to display the value of a shell variable called service after assigning a value as shown:

SERVICE =ACCT S -
Which two settings will display the name of the variable and its value?

- A. set | grep service
- B. echo $SERVICE
- C. env | grep SERVICE
- D. env $SERVICE
- E. set $SERVICE

Correct Answer: *BC*
C: env - set the environment for command invocation
If no utility operand is specified, the resulting environment shall be written to the standard output, with one name= value pair per line.

Question #3*Topic 1*

Which statements is true concerning Oracle Linux configuration files for users and groups?

- A. The /etc/passwd file contains hashed passwords for each user.
- B. The /etc/shadow file contains hashed passwords for each user.
- C. The GECOS field in /etc/passwd file may be empty.
- D. The /etc/group file contains the group name and the hashed group password.

Correct Answer: *B*
/etc/shadow file stores actual password in encrypted (one-way hashed) format for user's account with additional properties related to user password i.e. it stores secure user account information

Question #4*Topic 1*

Examine these statements and their output taken right after successful install of Oracle Linux:
[root@FAROUT /] rpm q firstboot
Firstboot -1.110.10-1.0.2.e16.x86_64
[root @FAROUT /] # chkconfig - - list firstboot
Firstboot 0:off 2:off 3:off 4:off 5:off 6;off
[root@FAROUT /] # /etc/sysconfig/firstboot

RUN_FIRSTBOOT=NO -
What is the conclusion?

- A. The option to run firstboot was deselected during Oracle Linux installation.
- B. The system was installed with desktop graphical packages and rebooted and the firstboot utility ran successful.
- C. Firstboot never ran in any run level because the service is turned off for all run levels.
- D. The system was installed without selecting desktop graphical packages, thereby disabling firstboot from running.

Correct Answer: *A*
Firstboot is set to off for all levels.
Example:
The rm command below remove or delate the firstboot file in order to make sure the firstboot program running when we restart or reboot the Fedora machine.
[root@fedora ~]# rm /etc/sysconfig/firstboot
rm: remove regular file `/etc/sysconfig/firstboot'? y
[root@fedora ~]#
Then check and make sure that firstboot program or firstboot service is run when your Fedora startup/boot up.

Check firstboot services -
[root@fedora ~]# chkconfig --list firstboot
firstboot 0:off 1:off 2:off 3:off 4:off 5:off 6:off
[root@fedora ~]#

Question #5*Topic 1*

Which three settings can be controlled by using the chage breemar command as the root user, to modify the parameters in the /etc/shadow file?

- A. The expiration date of the breemar account
- B. The number of days after the breemar account is locked, that it becomes expired
- C. The maximum number of days that must elapse between password changes by the user breemar before the password becomes invalid
- D. The number of days after the breemar account is locked, that it becomes unlocked
- E. The minimum number of days that must elapse between password changes by the user breemar
- F. The maximum number of failed login attempts on the breemar account before the account is locked

Correct Answer: *ACE*
A: chage -E, --expiredate EXPIRE_DATE
Set the date or number of days since January 1, 1970 on which the user's account will no longer be accessible.
CE: You need to use chage command to setup password aging.

The chage command changes the number of days between password changes and the date of the last password change. This information is used by the system to determine when a user must change his/her password.

Question #6*Topic 1*

Examine this extract from the /etc/ssh/sshd_config file:
passwordAuthentication no
What is the effect of this parameter settings on the use of openSSH commands on both the client and server?

- A. Passwords are not required and no ssh-keygen is required either. Only passphrase are required.
- B. Client users whose keys are not in the authorized_keys file on the server are unable to use passwords to authenticate themselves to the server.
- C. The ssh daemon does not ask for a password before starting or stopping the sshd service.
- D. Client users whose keys are not in the authorized_keys file on the client are unable to use passwords to authenticate themselves to the server.

Correct Answer: *B*
If you set PasswordAuthentication to no, you will no longer be able to use a login and password to authenticate and must use a login and public key instead (if
PubkeyAuthentication is set to yes).