

1Z0-100^{Q&As}

Oracle Linux 5 and 6 System Administration

Pass Oracle 1Z0-100 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.pass2lead.com/1z0-100.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Oracle
Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers



QUESTION 1

An Oracle Linux system has not been updated for a while and the currently running kernel is three releases behind the most recent kernel release.

Each released kernel fixed several problems, totaling 11 bug fixes.

You are about to update this kernel using this command:

```
[root@o16 ~]# uptrack-upgrade -all -y
```

How does Ksplice Uptrack apply these updates? (Choose the best answer.)

- A. It downloads three updates, clones the running kernel in memory, applies the updates in one single atomic update, and uses Kexec to activate the updated kernel
- B. It downloads 11 updates and applies them one by one to the running kernel
- C. It downloads 11 updates and applies them in a single transaction to the running kernel
- D. It downloads three updates and applies them in a single transaction to the running kernel

Correct Answer: B

QUESTION 2

Which statement correctly describes the requisite PAM control flag? (Choose the best answer.)

- A. requisite flagged modules are ignored if they fail
- B. requisite flagged modules must be successfully checked for authentication to succeed. If a requisite module checks fails, the user is notified immediately with a message reflecting the first failed required or requisite module
- C. requisite items only play a role when no other modules of that module type have succeeded or failed. In that case, the success or failure of a requisite flagged module determines the overall PAM authentication for that module type
- D. requisite flagged modules must be successfully checked for authentication to succeed. If a requisite module checks fails, the user is not notified until all other modules of the same module's type have been checked

Correct Answer: B

Four types of control flags are defined by the PAM standard: required — the module must be successfully checked in order to allow authentication. If a required module check fails, the user is not notified until all other modules of the same module type have been checked. requisite — the module must be successfully checked in order for the authentication to be successful. However, if a requisite module check fails, the user is notified immediately with a message reflecting the first failed required or requisite module. sufficient — the module checks are ignored if it fails. But, if a sufficient flagged module is successfully checked and no required flagged modules above it have failed, then no other modules of this module type are checked and the user is authenticated. optional — the module checks are ignored if it fails. If the module check is successful, it does not play a role in the overall success or failure for that module type. The only time a module flagged as optional is necessary for successful authentication is when no other modules of that type have succeeded or failed. In this case, an optional module determines the overall PAM authentication for that module type.

Reference: http://www.unix-info.org/RH_Guid.80/rhl-rg-en-8.0/s1-pam-control-flags.html

QUESTION 3

Which two steps should be performed to permit using SSH, SCP, or SFTP commands by the ORACLE account on the host FAROUT to the oracle account on the host WAYOUT without supplying a password?

- A. The oracle account user on host FAROUT must issue an ssh-keygen command to generate public and private key files in the ~ oracle/.ssh directory FAROUT.
- B. The oracle account user on the host WAYOUT must issue an ssh-keygen command to generate public and private key files in the ~/oracle.ssh directory on WAYOUT.
- C. The Oracle account user on host FAROUT must add the contents of ~/oracle/.ssh/id_dsa.pub or ~/oracle/.ssh/is_rsa.pub file to the ~/oracle/.ssh/authorized_keys file on host WAYOUT.
- D. The Oracle account user on host WAYOUT must add the contents of ~/oracle/.ssh/id_dsa or ~/oracle/.ssh/id_rsa.pub file to the ~/oracle/.ssh/authorized_keys file on host FAROUT.
- E. The oracle account user on host WAYOUT must set the permissions on the ~/oracle/.ssh/ authorized_keys file to 644.
- F. The Oracle account user on host FAROUT must set the permissions in ~/oracle/.ssh/authorized_keys file 644.

Correct Answer: BF

QUESTION 4

Examine the output shown:

```
[root@FAROUT fs] # rpm -qa | grep preinstall Oracle-rdbms-server-11gR2-preinstall-1.0-6.e16.x86_64
```

```
[root@FAROUT fs] # rpm -q1 oracle-rdbms-server-11gR2-preinstall-1.0-6.e16.x86_64 /etc/rc.d/init.d/ oracle-rdbms-server-11gR2-preinstall-firstboot /etc/sysconfig/Oracle-rdbms-server-11gR2-preinstall-verify /etc/sysconfig/oracle-rdbms-server-11gR2-preinstall/Oracle-rdbms-server-11gR2-preinstall.param /usr/bin/oracle-rdbms-server-11gR2-preinstall-verify
```

Which three statements are true about oracle-rdbms-server-11gR2-preinstall-1.0-6.e16.x86_64 rpm?

- A. It is a new name for oracle-validated package from Oracle Linux 5 that sets parameters to the same values.
- B. It creates the oracle user if not already created, which owns the Grid Infrastructure software should that get installed.
- C. It creates the grid user if not already created which owns the grid infrastructure software should that get installed.
- D. It modifies kernel parameters in /etc/sysctl.conf.
- E. It runs at the first boot after installing the packages to set a parameter indicating that it has run once.
- F. It modifies parameters in the /etc/sysconfig/network-scripts directly.

G. It creates the osoper group, if not already created.

Correct Answer: CEF

QUESTION 5

What is the purpose of setting USERCTL=yes In an interface configuration file located in /etc/sysconfig/ network-scripts? (Choose the best answer.)

- A. to allow a non-root user to bring a network interface up or down using the ifup and ifdown commands
- B. to allow a non-root user to bring a network interface up or down using the ifconfig command
- C. to allow a non-root user to bring a network interface up or down using the ethtool command
- D. to allow a non-root user to bring a network interface up or down using the ifup, ifdown, and ifconfig commands

Correct Answer: D

QUESTION 6

Which two statements are true regarding the use of the ssh-agent and ssh-add commands?

- A. The ssh-agent is used to hold private keys.
- B. The ssh-add command may ask for a passphrase each time the same key is required by the same user in the same shell.
- C. The ssh-agent is used to hold only public keys.
- D. The ssh-add command asks for the passphrase only the first time a key is required by the same user in the same shell.
- E. The ssh-add command retries the most recently saved passphrase if multiple key files are used.

Correct Answer: AD

A (not C): If you want to omit passphrase and password entry when you are using Solaris Secure Shell, you can use the agent daemon. Use the ssh-agent command at the beginning of the session. Then, store your private keys with the agent by using the ssh-add command.

D: Add your private key to the agent daemon.

The ssh-add command adds your private key to the agent daemon so that subsequent Secure Shell activity does not prompt you for the passphrase.

```
myLocalHost% ssh-add
```

```
Enter passphrase for /home/johndoe/.ssh/id_rsa:
```

Identity added: /home/johndoe/.ssh/id_rsa(/home/johndoe/.ssh/id_rsa) myLocalHost%

QUESTION 7

You must remove the user harhest from your Oracle Linux system because the person has left the company:

User harhest has numerous files, directories, and a crontab.

You issue:

```
Userdel r harhest
```

Which three outcomes result from the execution of this command?

- A. Files in the harhest home directory are removed.
- B. The home directory of harhest is removed.
- C. Files owned by narhest in any directory are removed.
- D. All directories owned by harhest are removed.
- E. The /var/spool/mail/harhest mailbox is removed.
- F. crontab /var/spool/cron/harhest is removed.

Correct Answer: ABE

The userdel command modifies the system account files, deleting all entries that refer to the user name LOGIN. The named user must exist.

parameter r -r, --remove Files in the user's home directory will be removed along with the home directory itself and the user's mail spool. Files located in other file systems will have to be searched for and deleted manually.

QUESTION 8

Which three statements are true about maintaining system parameters in Oracle Linux? (Choose three.)

- A. echo can be used to change values for various system parameters
- B. sysctl -w can be used to change values for various system parameters
- C. Changes made using echo are lost after rebooting the system
- D. Changes made using sysctl -w are preserved after rebooting the system
- E. Changes made to /etc/sysctl.conf take effect immediately after saving the file

Correct Answer: ABD

QUESTION 9

Which two statements correctly describe the type of information and the behavior of files in the proc filesystem on Oracle Linux 6?

- A. It is not possible to write to any file in the proc filesystem.
- B. The /proc/cmdline file contains the parameters passed to the kernel.
- C. Each process has a directory named for the process number in the proc filesystem.
- D. The proc filesystem contains the same hardware information that is contained in the sys filesystem for backward compatibility.
- E. Each process thread has a directory named for the process thread number in the proc files/stem.

Correct Answer: AB

B: proc/cmdline This file shows the parameters passed to the kernel at the time it is started. A sample /proc/cmdline file looks like the following: ro root=/dev/VolGroup00/LogVol00 rhgb quiet 3

Note:

/proc is very special in that it is also a virtual filesystem. It's sometimes referred to as a process information pseudo-file system. It doesn't contain 'real' files but runtime system information (e.g. system memory, devices mounted, hardware configuration, etc). For this reason it can be regarded as a control and information centre for the kernel. In fact, quite a lot of system utilities are simply calls to files in this directory.

QUESTION 10

Which two statements are true concerning the configuration and use of cron and anacron?

- A. Anacron jobs are used to make sure cron jobs run if the system had been down when they were meant to run.
- B. All crontabs are held in the /etc/cron.d directory.
- C. Cron jobs may run as frequently as once a minute.
- D. Anacron jobs may run as frequently as once a minute.
- E. The crond daemon looks for jobs only in /etc/crontab.

Correct Answer: CE

Note: Anacron is the cron for desktops and laptops.

Anacron does not expect the system to be running 24 x 7 like a server.

When you want a background job to be executed automatically on a machine that is not running 24 x 7,

you should use anacron.

Incorrect:

not D: /etc/anacrontab file has the anacron jobs mentioned in the following format.

period delay job-identifier command

Field 1 is Recurrence period: This is a numeric value that specifies the number of days.

1 daily

7 weekly

30 monthly

N This can be any numeric value. N indicates number of days

QUESTION 11

Examine these details from the sysctl.conf file and from the proc file system:

```
[root@FAROUT fs]# grep aio-max-nr /etc/sysctl.conf # oracle-rdbms-server-11gR2-preinstall setting for fs.aio-mx-nr is 1048576 fs.aio-max-nr = 1048576
```

```
[root@FAROUT fs] # cat /proc/sys/fs/aio-max-nr 1048576
```

```
[root@FAROUT fs] # rpm -q libaio Libaio-0.0.107-10.e16.x86_64 Libaio-0.3.107-10.e76.i686
```

Which statement is true about the setting created by oracle-rdbms-server-11gR2-preinstall?

- A. It allows a process to request an I/O without waiting for reply.
- B. It allows two or more processes to request I/O simultaneously while running on different CPUs.
- C. It allows a process to request a single I/O without awaiting for a reply. However, if a second I/O is requested, then the process must wait.
- D. It allows two or more processes to request I/Os and then to both be notified when both of them complete.

Correct Answer: B

QUESTION 12

Examine some of the contents of the /boot/grub/grub.com file from an Oracle Linux system:

```
Default=0 Timeout=5 Splashimage=(hd0, 0)/grub/splash.xpm.gz Hiddenmenu Title Oracle Linux Server (2.6.39-100.0.12.16uek.x86_64)
```

```
Root (hd0, 0)
```

```
Kernel /vmlinuz-2.6.39-100.0.12.e16uek.x86_64 ro root=UUID=a4b6049b-9aa1-44b4-87cfaebb17alcdf9 rd_NO_LUKS
re_NO_LVM rd_NO_DM LANG=en_US.UTF-8 SYSFONT=1atarcyreheb-sun16 KEYBOARDTYPE=PC KEYTABLE=us
rhgb quiet numa=off Initrd /initramfs-2.6.39-100.0.12.e16uek.x86_64.img Title Oracle Linux Server
(2.6.32-131.0.15.e16.x86_64)
```

Root (hd0, 0)

```
Kernel /vmlinuz-2.6.32-131.0.15.e16.x86_64 ro root=UUID=a4b6049b-9aa1-44b4-87cf-aebb17a1cdf9 rd_NO_LUKS
rd_NO_LVM rd_NO_LVM re_NO_MD rd_NO_DM LANG=en_UD.UTF-8 SYSFONT=lataarcyheb-sun16
KEYBOARDTYPE=PC KEYTABLE=us Crashkernel=auto rhgp quiet numa = off
```

Initrd /initramfs-2.6.32-131.0.15.e16.x86_64.img

Which three statements are true about the behavior and configuration of GRUB on this system?

- A. (hd0, 0) represents the first partition on device /dev/hd0.
- B. The hiddenmenu directive hides the GRUB menu only for 5 seconds after which it becomes visible again.
- C. The root directive specifies an initial root filesystem, allowing access to block device modules to mount the real root filesystem on disk.
- D. (hd0, 0) represents the first partition on the first drive detected by the BIOS.
- E. The initrd directive specifies the initamfs, an initial root filesystem in RAM, allowing access to block device modules to mount the real root filesystem.
- F. Each kernel must have an initramfs that matches the version of the kernel.
- G. Because there is an Unbreakable Enterprise Kernel installed, it must be the default kernel listed as shown by the default=0 directive.

Correct Answer: ACE

QUESTION 13

Which three statements are true configuration files and the behavior of module parameters specified in those files, in the /etc/modprobe.d directory?

- A. The files may contain options to be passed to a module only when it is a dependency of a module being inserted.
- B. The file may contain shell commands to be run instead of inserting a particular module in the kernel.
- C. The files may contain options to be passed to a module, only when it is inserted using a modprobe command.
- D. The files may contain alias names for modules.
- E. The file may contain instructions to ignore certain modules.
- F. The files may contain options to be passed to a module only when it is Inserted using an insmod command.

Correct Answer: ACD

modprobe.d - Configuration directory for modprobe Because the modprobe command can add or remove more than one module, due to modules having dependencies, we need a method of specifying what options are to be used with those modules (A). All files underneath the /etc/modprobe.d directory which end with the .conf extension specify those options as required. They can also be used to create convenient aliases (D): alternate names for a module, or they can override the normal modprobe behavior altogether for those with special requirements (such as inserting more than one module).

C: options modulename option...

This command allows you to add options to the module modulename (which might be an alias) every time

it is inserted into the kernel: whether directly (using modprobemodulename or because the module being

inserted depends on this module.

QUESTION 14

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 15

Examine this MDAM output: Which two aspects can be determined from this output?

mdam - - detail /dev/md0

```
/dev/md0
Version           : 1.2
Creation Time     : Fri Apr 12 16:53:38 2013
Raid Level        : raid5
Array Size        : 207872 (203.03 MiB 212.86 MB)
Used Dev size     : 103936 (101.52 MiB 106.43 MB)
Raid Devices      : 3
Total Devices     : 3
Persistence      : Superblock is persistent
Update Time      : Fri Apr 12 16:57:59 2013
State             : clean, degraded, recovering
Active Devices    : 2
Working Devices   : 3
Failed Devices    : 0
Spare Devices     : 1
Layout            : Left Symmetric
Chunk Size        : 512k
Rebuild Status    : 60% complete
Name              : o16.example.com:0 (local to host o16.example.com)
UUID              : 70f8d2f:0505d92d:750a781e:c24508d
Events           : 66
```

Number	Major	Minor	RaidDevice	State
0	8	49	0	active sync /dev/sadd1
1	8	65	1	active sync /dev/sde1
3	8	81	2	spare rebuilding /dev/sdf1

- A. A RAID device failed and has been replaced with the hot spare.
- B. A new RAID device was just added to replace a failed one.
- C. Read and write performance is currently not optimal on this RAID set.
- D. Only write performance is currently not optimal on this raid set.
- E. An extra device was added to this RAID set to increase its size.

Correct Answer: AE