Exam :   XK0-002
Linux+

Demo Version

To Access Full Version, Please go to

QUESTION 1
On an NIS client, the following is a portion of the output of cat /etc/passwd:
+Joe::::::::
+Sam::::::::
+:*::::::::/bin/false
Which of the following is true for all users other than Joe and Sam?

A. They have full access.
B. They are denied access.
C. They are granted limited access.
D. They gain access after being prompted for a shell.

Answer: B

Explanation: login denied users are displayed with + symbol at the starting of line.

QUESTION 2 How can a user view an X Window from a remote system on their local system?

A. from the local system: export
DISPLAY=local:0.0
B. from the remote system: export
DISPLAY=local:0.0
C. from the local system: export
DISPLAY=remote:0.0
D. from the remote system: export
DISPLAY=remote:0.0

Answer: D
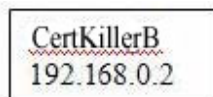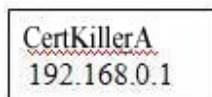
Explanation: First Local host should give the permission to display the X Terminal on local host using xhost command. Then user can export the display from remote host. See the example

Suppose you want to run application on Itexamworld B from Itexamworld A.
Itexamworld B in GUI Terminal:# xhost +192.168.0.1
Itexamworld A in GUI Terminal:# export DISPLAY=192.168.0.2:0
xterm &
Now Terminal of Itexamworld A will display on Itexamworld B

QUESTION 3 Which of the following commands can be used to confirm that the FTP

server is listening?

A. netstat -a ftp
B. netstat | grep ftp
C. netstat -u | grep ftp
D. netstat -a | grep ftp

Answer: D

Explanation: netstat is the multipurpose command, it can list active network connections, routing tables, interface statistics and other vital network information. Syntax: netstat [options] Options are -a à List listening and connected sockets -t à List TCP connection -u à List UDP Connection -p à Show PID and name of the program.

QUESTION 4 When a RAID 5 array is configured with a hot-spare disk under Linux, which of the following is the minimum number of drives required?

A. 2
B. 3
C. 4
D. 5

Answer: C

Explanation: RAID 5 is the most common type of RAID. By distributing parity information across some or all of an array's member disk drives, RAID 5 eliminates the write bottleneck of using one parity disk. The minimum requirements for RAID 5 is 3 disks. According to questions, 3 disks for RAID Level 5 and one spare disk so total 4.

QUESTION 5 A system administrator wants to see if an RPM package is installed on a user workstation. Which of the following commands should be used?

A. rpm -query <filename>
B. rpmfind <name of package>
C. rpm -qa | grep <name of package>
D. find -name rpm | grep <filename>

Answer: C
Explanation: RPM format packages can manage using rpm command. to query the package either installed or not,
rpm -q packagename
To list all installed package:
rpm -qa packagename

QUESTION 6 Which of the following can be used to determine who has scheduled a job?

A. who
B. whodo
C. at -d
D. at -l

Answer: B

QUESTION 7 Which of the following encryption schemes is the LEAST secure?

A. DES
B. MD5
C. AES
D. Blowfish

Answer: A The Data Encryption Standard, a block cipher with 64-bit blocks and a 56-bit key Like MD4, it produces a 128-bit hash. For details see RFC 1321 AES ciphers use a 128-bit block and 128, 192 or 256-bit keys A block cipher using 64-bit blocks and keys of up to 448 bits

QUESTION 8 A Linux machine has a local address of 192.168.1.1 with subnet mask of 255.255.255.0. All services are currently denied. Which of the following lines should be appended to hosts.allow file to permit access to the Web service on the local subnet.

A. httpd: 192.168.1.0/24
B. ALL: 192.168.1.255/24
C. ALL except httpd: 192.168.1.1/24
D. 192.168.1.255/255.255.255.0:httpd

Answer: A

Explanation:
The /etc/hosts.allow and /etc/hosts.deny each have two or more colon-separated fields. The first filed specifies the comma separated list of executable name . The second field

contains a comma-separated list of client specifications, using IP address or host name or network name. httpd: 192.168.1.0/24 à specified the network vsftpd: .example.com à specified the domain.

QUESTION 9 A Linux administrator is about to install a Linux server. The server has 256MB of RAM. Which of the following sizes of the swap partition is generally recommended?

A. 128MB
B. 256MB
C. 512MB
D. 1024MB

Answer: C

Explanation: Swap space in Linux is used when the amount of physical memory (RAM) is full. If the system needs more memory resources and the RAM is full, inactive pages in memory are moved to the swap space. While swap space can help machines with a small amount of RAM, it should not be considered a replacement for more RAM. Swap space is located on hard drives, which have a slower access time than physical memory. Swap space can be a dedicated swap partition (recommended), a swap file, or a combination of swap partitions and swap files. The size of your swap should be equal to twice your computer's physical RAM for up to 2 GB of physical RAM. For physical RAM above 2 GB, the size of your swap should be equal to the amount of physical RAM above 2 GB. The size of your swap should never less than 32 MB. Using this basic formula, a system with 2 GB of physical RAM would have 4 GB of swap, while one with 3 GB of physical RAM would have 5 GB of swap.

QUESTION 10 Which driver, if any, is required to support L3 cache on the system processor?

A. msr.o
B. mtrr.o
C. cache.o
D. No driver is required.

Answer: D

Explanation: To Support L3 cache on the system processor, no any driver is required.

QUESTION 11 A user wants to remotely connect to a Linux system to transfer files from an oversea IP address. Which of the following programs allows the user to do this securely?

A. rcp
B. ftp
C. sftp
D. telnet

Answer: C

Explanation:

ssh is the service, which provides the secure communication. Other services like telnet, ftp, rlogin are unsecured services. scp, sftp etc are services provides the secure communiation provided by openssh packages.

QUESTION 12 When the command mke2fs -j is run, what type of system is created?

A. ext2
B. ext3
C. jfs
D. xfs

Answer: B

Explanation: By default mke2fs command creates the ext2 file system, To create the file system on ext3 file system Use mke2fs -j device Or mkfs -t ext3 device What are the advantages of ext3?Why do you want to migrate from ext2 to ext3? Four main reasons: availability, data integrity, speed, and easy transition. Availability After an unclean system shutdown (unexpected power failure, system crash), each ext2 file system cannot be mounted until its consistency has been checked by the e2fsck program. The amount of time that the e2fsck program takes is determined primarily by the size of the file system, and for today's relatively large (many tens of gigabytes) file systems, this takes a long time. Also, the more files you have on the file system, the longer the consistency check takes. File systems that are several hundreds of gigabytes in size may take an hour or more to check. This severely limits availability. By contrast, ext3 does not require a file system check, even after an unclean system shutdown, except for certain rare hardware failure cases (e.g. hard drive failures). This is because the data is written to disk in such a way that the file system is always consistent. The time to recover an ext3 file system after an unclean system shutdown does not depend on the size of the file system or the number of files; rather, it depends on the size of the "journal" used to maintain consistency. The default journal size takes about a second to recover (depending on the speed of the hardware). Data Integrity Using the ext3 file system can provide stronger guarantees about data integrity in case of an unclean system shutdown. You choose the type and level of protection that your data receives. You can choose to keep the file system consistent, but allow for damage to data on the file system in the case of unclean system shutdown; this can give a modest speed up under some but not all circumstances. Alternatively, you can choose to ensure that the data is consistent with the state of the file system; this means that you will; never see garbage data in recently-written files after a crash. The safe choice, keeping the data consistent with the state of the file system, is the default. Speed Despite writing some data more than once, ext3 is often faster (higher throughput) than ext2 because ext3's journaling optimizes hard drive head motion. You can choose from three journaling modes to optimize speed, optionally choosing to trade off some data integrity.
1.   1. One mode, data=writeback, limits the data integrity guarantees, allowing old data to show up in files after a crash, for a potential increase in speed under some circumstances. (This mode, which is the default journaling mode for most journaling file

systems, essentially provides the more limited data integrity guarantees of the ext2 file system and merely avoids the long file system check at boot time.)

2.   2. The second mode, data=ordered (the default mode), guarantees that the data is consistent with the file system; recently-written files will never show up with garbage contents after a crash.

3.   3. The last mode, data=journal, requires a larger journal for reasonable speed in most cases and therefore takes longer to recover in case of unclean shutdown, but is sometimes faster for certain database operations. The default mode is recommended for general-purpose computing needs. To change the mode, add the data=something option to the mount options for that file system in the /etc/fstab file, as documented in the mount man page (man mount). Easy Transition It is easy to change from ext2 to ext3 and gain the benefits of a robust journaling file system, without reformatting. That's right, there is no need to do a long, tedious, and error-prone backup-reformat-restore operation in order to experience the advantages of ext3. There are two ways to perform the transition:

1. The Red Hat Linux installation program offers to transition your file systems when you upgrade your system. All you have to do is select one checkbox per file system. The tune2fs program can add a journal to an existing ext2 file system. If the file system is already mounted while it is being transitioned, the journal will be visible as the file .journal in the root directory of the file system. If the file system is not mounted, the journal will be hidden and will not appear in the file system. Just run tune2fs -j /dev/hda1 (or whatever device holds the file system you are transitioning) and change ext2 to ext3 on the matching lines in /etc/fstab. If you are transitioning your root file system, you will have to use an initrd to boot. Run the mkinitrd program as described in the manual and make sure that your LILO or GRUB configuration loads the initrd. (If you fail to make that change, the system will still boot, but the root file system will be mounted as ext2 instead of ext3 - you can tell this by looking at the output of the command cat /proc/mounts.) More information on tune2fs can be found in the tune2fs man page (man tune2fs).

QUESTION 13 In addition to selected packages and partition maps, which of the following should also be documented during a Linux server installation?

A. System hardware and user passwords
B. Root password and performance baseline
C. Daemon configuration and performance baseline
D. System hardware and daemon configuration

Answer: C

Explanation: During Server Installation, you should think, which services are required. You should select the respective packages.

QUESTION 14 Which of the following commands can be run to determine which package owns /etc/exports?

A. rpm -qf /etc/exports

B. rpm -ql /etc/exports
C. rpm --file /etc/exports
D. rpm --verify /etc/exports

Answer: A

Explanation: To determine the package owns the specified file, rpm -qf filename where -q means query and -f means filename.

QUESTION 15 The root user types 'echo $PATH' and sees the following output: .:/bin:/usr/bin:/sbin:/usr/X11R6/bin:/usr/src Which of the following parts of this path is considered to be a security risk?

A. .
B. /sbin
C. /usr/src
D. /usr/X11R6/bin

Answer: A A common mistake in the past (?) was to keep '.' in the root's path. Malicious hacker makes program 'ls' in his home directory. If root makes # cd ~hacker # ls he executes ls command of hacker's.
QUESTION 16 Which of the following commands can be used to mount a Samba share?

A. smbmount //servername/sharename /mountdirectory -o username=mywindowsusername, password=mywindowspassword
B. mount -t samba /servername/sharename /mountdirectory -o username=mywindowsusername, password=mywindowspassword
C. mount -t smbf \\servername\sharename /mountdirectory -o username=mywindowsusername, password=mywindowspassword
D. smbmount -t smbfs //servername/sharename /mountdirectory -o username=mywindowsusername, password=mywindowspassword

Answer: A

Explanation: We can mount the samba share using mount, smbmount command. smbmount command automatically apply the smbfs filesystem. But to mount samba share using mount command, we should specify the smbfs filesystem.
Syntax for mount:
mount -t smbfs //server/sharename /mountpoint -o username=server's username, password=user's password
Syntax for msbmount
smbmount //server/sharename /mountpoint -o username=server's username, password=user's password
Always netbios name specified using //.