XK0-005 Q&As

CompTIA Linux+ Certification Exam

Pass CompTIA XK0-005 Exam with 100% Guarantee

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

https://www.pass4itsure.com/xk0-005.html

100% Passing Guarantee
100% Money Back Assurance

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

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

QUESTION 1

A Linux system fails to start and delivers the following error message:

```
Checking all file systems.
/dev/sda1 contains a file system with errors, check forced.
/dev/sda1: Inodes that were part of a corrupted orphan linked list found.
/dev/sda1: UNEXPECTED INCONSISTENCY;
```

Which of the following commands can be used to address this issue?

A. fsck.ext4 /dev/sda1

B. partprobe /dev/sda1

C. fdisk /dev/sda1

D. mkfs.ext4 /dev/sda1

Correct Answer: A

Explanation: The command fsck.ext4 /dev/sda1 can be used to address the issue. The issue is caused by a corrupted filesystem on the /dev/sda1 partition. The error message shows that the filesystem type is ext4 and the superblock is invalid. The command fsck.ext4 is a tool for checking and repairing ext4 filesystems. The command will scan the partition for errors and attempt to fix them. This command can resolve the issue and allow the system to start. The other options are incorrect because they either do not fix the filesystem (partprobe or fdisk) or destroy the data on the partition (mkfs.ext4). References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter

10: Managing Storage, page 325.

QUESTION 2

A systems administrator receives reports that several virtual machines in a host are responding slower than expected. Upon further investigation, the administrator obtains the following output from one of the affected systems:

16:00:01	PM	CPU	%user	%nice	%system	%iowait	%steal	%idle
16:10:01	PM	all	17.58	0.00	9.36	0.00	54.33	18.73
16:20:01	PM	all	22.34	0.00	11.75	0.00	48.69	17.22
16:30:01	PM	all	25.49	0.00	11.69	0.00	57.85	4.97
16:40:01	PM	all	25.49	0.00	11.69	0.00	53.21	9.61
16:50:01	PM	all	25.49	0.00	11.69	0.00	56.49	6.33

Which of the following best explains the reported issue?

A. The physical host is running out of CPU resources, leading to insufficient CPU time being allocated to virtual machines.

B. The physical host has enough CPU cores, leading to users running more processes to compensate for the slower

response times.

C. The virtual machine has enough CPU cycles, leading to the system use percentage being higher than expected.

D. The virtual machine is running out of CPU resources, leading to users experiencing longer response times.

Correct Answer: D

Explanation: Based on the output from one of the affected systems, the best explanation for the reported issue is that the virtual machine is running out of CPU resources, leading to users experiencing longer response times (D). The output shows that the system use percentage is very high (57.85%), indicating that the virtual machine is using most of its CPU cycles for system processes. This leaves little CPU time for user processes, which results in slower performance. The other explanations are not supported by the output or are contradictory. References: [CompTIA Linux+ Study Guide], Chapter 8: Optimizing Linux Performance, Section: Monitoring CPU Usage [How to Interpret CPU Usage Statistics]

QUESTION 3

A database administrator requested the installation of a custom database on one of the servers. Which of the following should the Linux administrator configure so the requested packages can be installed?

A. /etc/yum.conf

B. /etc/ssh/sshd.conf

C. /etc/yum.repos.d/db.repo

D. /etc/resolv.conf

Correct Answer: C

Explanation: The Linux administrator should configure /etc/yum.repos.d/db.repo so that the requested packages can be installed. This file defines a custom repository for yum, which is a package manager for RPM-based systems. The file should contain information such as the name, baseurl, gpgcheck, and enabled options for the repository. By creating this file and enabling the repository, the administrator can use yum to install packages from the custom repository. The /etc/ yum.conf file is the main configuration file for yum, but it does not define repositories. The /etc/ssh/sshd.conf file is the configuration file for sshd, which is a daemon that provides secure shell access to remote systems. The /etc/resolv.conf file is the configuration file for DNS resolution, which maps domain names to IP addresses. References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 19: Managing Packages and Software, page 559.

QUESTION 4

A Linux system is failing to boot. The following error is displayed in the serial console:

[[1;33mDEPEND[Om] Dependency failed for /data.

[[1;33mDEPEND[Om] Dependency failed for Local File Systems

...

Welcome to emergency mode! After logging in, type "journalctl -xb" to viewsystem logs, "systemct1 reboot" to reboot, "systemct1 default" to try again to boot into default mode.

Give root password for maintenance

(or type Control-D to continue}

Which of the following files will need to be modified for this server to be able to boot again?

A. /etc/mtab

B. /dev/sda

C. /etc/fstab

D. /ete/grub.conf

Correct Answer: C

Explanation: The file that will need to be modified for the server to be able to boot again is /etc/fstab. The /etc/fstab file is a file that contains the information about the file systems that are mounted at boot time on Linux systems. The file specifies the device name, mount point, file system type, mount options, dump frequency, and pass number for each file system. The error message indicates that the dependency failed for /data, which is a mount point for a file system. This means that the system could not mount the /data file system at boot time, which caused the system to enter the emergency mode. The emergency mode is a mode that allows the administrator to log in as the root user and perform basic tasks such as repairing the system. The administrator should modify the /etc/fstab file and check the entry for the /data file system. The administrator should look for any errors or inconsistencies in the device name, file system type, or mount options, and correct them. The administrator should also verify that the device and the file system are intact and functional by using commands such as blkid, fdisk, fsck, or mount. The administrator should then reboot the system and see if the issue is resolved. The file that will need to be modified for the server to be able to boot again is /etc/fstab. This is the correct answer to the question. The other options are incorrect because they are not related to the file systems that are mounted at boot time (/etc/mtab, /dev/sda, or /etc/grub.conf). References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 10: Managing Storage, page 321.

QUESTION 5

A Linux administrator reviews a set of log output files and needs to identify files that contain any occurrence of the word denied. All log files containing entries in uppercase or lowercase letters should be included in the list. Which of the following commands should the administrator use to accomplish this task?

A. find . -type f -print | xrags grep -ln denied

B. find . -type f -print | xrags grep -nv denied

C. find . -type f -print | xrags grep -wL denied

D. find . -type f -print | xrags grep -li denied

Correct Answer: D

Explanation: The command find . -type f -print | xargs grep -li denied will accomplish the task of identifying files that contain any occurrence of the word denied. The find command is a tool for searching for files and directories on Linux systems. The . is the starting point of the search, which means the current directory. The -type f option specifies the type of the file, which means regular file. The -print option prints the full file name on the standard output. The | is a pipe symbol that redirects the output of one command to the input of another command. The xargs command is a tool for building and executing commands from standard input. The grep command is a tool for searching for patterns in files or input. The -li option specifies the flags that the grep command should apply. The -l flag shows only the file names that match the pattern, instead of the matching lines. The -i flag ignores the case of the pattern, which means it matches

both uppercase and lowercase letters. The denied is the pattern that the grep command should search for. The command find . - type f -print | xargs grep -li denied will find all the regular files in the current directory and its subdirectories, and then search for any occurrence of the word denied in those files, ignoring the case, and print only the file names that match the pattern. This will allow the administrator to identify files that contain any occurrence of the word denied. This is the correct command to use to accomplish the task. The other options are incorrect because they either do not ignore the case of the pattern (find . -type f -print | xargs grep -ln denied or find . -type f -print | xargs grep -wL denied) or do not show the file names that match the pattern (find . -type f -print | xargs grep -nv denied). References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 16: Managing Logging and Monitoring, page 489.