XK0-005 Reliable Test Cram - XK0-005 Exam Dumps Pdf

BTW, DOWNLOAD part of ExamPrepAway XK0-005 dumps from Cloud Storage: https://drive.google.com/open?id=1EXBUKovDcyjJtR6WsmiGxzrlfEPrtSt6

Nowadays in this talented society XK0-005 professionals are very popular, but the ICompTIA area are also very competitive. So many CompTIA professionals through passing difficult XK0-005 Certification exams to stabilize themselves. ExamPrepAway is websites specifically provide convenience for candidates participating in the XK0-005 certification exams.

Regarding the process of globalization, every fighter who seeks a better life needs to keep pace with its tendency to meet challenges. XK0-005 certification is a stepping stone for you to stand out from the crowd. Nowadays, having knowledge of the XK0-005 study braindumps become widespread, if you grasp solid technological knowledge, you are sure to get a well-paid job and be promoted in a short time. According to our survey, those who have passed the exam with our XK0-005 Test Guide convincingly demonstrate their abilities of high quality, raise their professional profile, expand their network and impress prospective employers.

>> XK0-005 Reliable Test Cram <<

CompTIA XK0-005 Reliable Test Cram: CompTIA Linux+ Certification Exam - ExamPrepAway 10 Years of Excellence

Our worldwide after sale staff will be online for 24/7 and reassure your rows of doubts on our XK0-005 exam questions as well as exclude the difficulties and anxiety with all the customers. Just let us know your puzzles and we will figure out together. You can contact with us at any time and we will give you the most professional and specific suggestions on the XK0-005 Study Materials. What is more, you can free download the demos of the XK0-005 learning guide on our website to check the quality and validity.

CompTIA XK0-005, also known as the CompTIA Linux+ certification exam, is a globally recognized credential for IT professionals seeking to demonstrate their expertise in Linux-based operating systems. CompTIA Linux+ Certification Exam certification is vendor-neutral, which means that it is not tied to any specific Linux distribution, making it a valuable asset for Linux administrators and technicians across various industries.

CompTIA XK0-005 exam is a comprehensive exam that covers various topics related to Linux system administration. XK0-005 exam consists of multiple-choice questions and performance-based questions that test the candidate's practical skills. XK0-005 Exam is designed to test the candidate's knowledge of basic Linux commands, system administration, security, and networking. Candidates who pass XK0-005 exam demonstrate their ability to manage Linux systems in different environments, including cloud, servers, and mobile devices. CompTIA Linux+ Certification Exam certification is valid for three years, and candidates are required to recertify to maintain their certification status.

CompTIA Linux+ Certification Exam Sample Questions (Q65-Q70):

NEW QUESTION # 65
The journald entries have filled a Linux machine's /var volume. Which of the following is the best command for a systems administrator to use to free up the disk space occupied by these entries?

- A. systemctl stop systemd-journald
  systemctl start systemd-journald
- B. journalctl --rotate
  journalctl --vacuum-time=ls
- C. pkill -HUP systemd-journald
  systemctl restart systemd-journald
- D. rm -rf /var/log/journal
  systemctl restart systemd-journald

Answer: B

Explanation:
To safely reduce the size of journald logs, journalctl --rotate forces log rotation, and journalctl -- vacuum-time=ls removes entries older than the specified time. This approach efficiently manages log files without directly deleting files, which could risk corruption.

NEW QUESTION # 66
A Linux administrator created the directory /project/access2all. By creating this directory, the administrator is trying to avoid the deletion or modification of files from non-owners. Which of the following will accomplish this goal?

- A. chmod 2770 /project/access2all
- B. chmod +rws /project/access2all
- C. chmod +t /project/access2all
- D. chmod ugo+rwx /project/access2all

Answer: C

Explanation:
Explanation
The command that will accomplish the goal of avoiding the deletion or modification of files from non-owners is chmod +t /project/access2all. This command will set the sticky bit on the directory /project/access2all, which is a special permission that restricts file deletion or renaming to only the file owner, directory owner, or root user. This way, even if multiple users have write permission to the directory, they cannot delete or modify each other's files.
The other options are not correct commands for accomplishing the goal. The chmod +rws /project/access2all command will set both the SUID and SGID bits on the directory, which are special permissions that allow a program or a directory to run or be accessed with the permissions of its owner or group, respectively.
However, this does not prevent file deletion or modification from non-owners. The chmod 2770 /project/access2all command will set only the SGID bit on the directory, which means that any new files or subdirectories created in it will inherit its group ownership. However, this does not prevent file deletion or modification from non-owners. The chmod ugo+rwx /project/access2all command will grant read, write, and execute permissions to all users (user, group, and others) on the directory, which means that anyone can delete or modify any file in it. References: chmod(1) - Linux manual page; How to Use SUID, SGID, and Sticky Bits on Linux

NEW QUESTION # 67
A Linux administrator is trying to remove the ACL from the file /home/user/data. txt but receives the following error message:

```
setfacl: data.txt: operation not permitted
```

Given the following analysis:

```
/dev/mapper/linux-home on /home type xfs (rw,relatime,seclabel,attr2,inode64,usrquota)

-rw-rw-r--+ 1 user staff 2354 Sep 15 16:33 data.txt
-rw-rw-r--+ user staff unconfined_u:object_r:user_home_t:s0 data.txt

# file: data.txt
# owner: user
# group: staff
user::rw-
user:accounting:rw-
group::r-
mask::rw-
other::r—

Attributes:
-----a-----------
```

Which of the following is causing the error message?

- A. File attributes are preventing file modification.
- B. The administrator is not using a highly privileged account.
- C. The filesystem is mounted with the wrong options.
- D. SELinux file context is denying the ACL changes.

Answer: A

Explanation:

File attributes are preventing file modification, which is causing the error message. The output of lsattr /home
/user/data.txt shows that the file has the immutable attribute (i) set, which means that the file cannot be changed, deleted, or renamed.
The command setfacl -b /home/user/data.txt tries to remove the ACL from the file, but fails because of the immutable attribute. The
administrator needs to remove the immutable attribute first by using the command chattr -i /home/user/data.txt and then try to
remove the ACL again. The other options are incorrect because they are not supported by the outputs. The administrator is using a
highly privileged account, as shown by the # prompt. The filesystem is mounted with the correct options, as shown by the output of
mount | grep /home. SELinux file context is not denying the ACL changes, as shown by the output of ls -Z /home/user/data.txt.
References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 11: Managing Files and Directories, pages 357-358.

NEW QUESTION # 68
When trying to log in remotely to a server, a user receives the following message:

```
Password:
Last failed login: Wed Sep 15 17:23:45 CEST 2021 from 10.0.4.3 on ssh:notty
There were 3 failed login attempts since the last successful login.
Connection to localhost closed
```

The server administrator is investigating the issue on the server and receives the following outputs:
Output 1:

```
user:x:1001:7374::/home/user:/bin/false
```

Output 2:

```
dzwx------. 2 user 62 Sep 15 17:17 /home/user
```

Output 3:

```
Sep 12 14:14:05 server sshd[22958] Failed password for user from 10.0.2.8
Sep 15 17:24:03 server sshd[8460]: Accepted keyboard-interactive/pam for user from 10.0.6.5 port 50928 ssh2
Sep 15 17:24:03 server sshd[8460]: pam_unix(sshd:session): session opened for user testuser
Sep 15 17:24:03 server sshd[8460]: pam_unix(sshd:session): session closed for user testuser
```

Which of the following is causing the issue?

- A. The wrong permissions are on the user's home directory.
- B. The account was locked out due to three failed logins.
- C. The user entered the wrong password.
- D. The user has the wrong shell assigned to the account.

Answer: D

Explanation:
Explanation
The user has the wrong shell assigned to the account, which is causing the issue. The output 1 shows that the user's shell is set to /bin/false, which is not a valid shell and will prevent the user from logging in. The output
2 shows that the user's home directory has the correct permissions (drwxr-xr-x), and the output 3 shows that the user entered the correct password and was accepted by the SSH daemon, but the session was closed immediately due to the invalid shell. The other options are incorrect because they are not supported by the outputs. References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 13: Managing Network Services, page 413.

NEW QUESTION # 69
A company's internal users report that the website is responding slowly, especially when accessing pages that involve static content such as images and scripts. The server's CPU, RAM, and network usage are all within acceptable ranges. Upon investigation, the administrator finds that the antivirus software is actively scanning the web root directory in real time, including every file access request.
Which of the following will MOST likely fix the issue?

- A. Exclude the web root directory from antivirus scanning
- B. Add a second web server and a load balancer
- C. Add more CPUs to the server
- D. Replace the network cable
- E. Add more RAM to the server

Answer: A

Explanation:
When antivirus software is configured to scan files in real time, and it includes the web root directory (e.g., /var/www/html), every time a user requests a page, image, or script, the antivirus scans that file before it's served. This introduces latency, especially on high-traffic servers, even when CPU, RAM, and network usage appear normal.
By excluding the web root from real-time scanning, the server can deliver files faster, improving website performance without adding hardware or changing the infrastructure.

NEW QUESTION # 70
......

You will be cast in light of career acceptance and put individual ability to display. When you apply for a job you could have more opportunities than others. What is more, there is no interminable cover charge for our XK0-005 practice engine priced with reasonable prices for your information. Considering about all benefits mentioned above, you must have huge interest to our XK0-005 Study Materials. You should take the look at our XK0-005 simulating questions right now.