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

QUESTION 1

One leg of an LVM-mirrored volume failed due to the underlying physical volume, and a systems administrator is troubleshooting the issue. The following output has been provided:

```
Partial mode. Incomplete volume groups will be activated read-only
```

LV	VG	Attr	LSize	Origin	Snap%	Move	Log	Copy%	Devices
linear	vg	-wi-a-	40.00G						unknown device(0)
stripe	vg	-wi-a-	40.00G						unknown device(5120),/dev/sda1(0)

Given this scenario, which of the following should the administrator do to recover this volume?

A. Reboot the server. The volume will automatically go back to linear mode.

B. Replace the failed drive and reconfigure the mirror.

C. Reboot the server. The volume will revert to stripe mode.

D. Recreate the logical volume.

Correct Answer: B

Explanation: The administrator should replace the failed drive and reconfigure the mirror to recover the volume. The LVM (Logical Volume Manager) is a tool for managing disk space on Linux systems. The LVM allows the administrator to create logical volumes that span across multiple physical volumes, such as hard disks or partitions. The LVM also supports different types of logical volumes, such as linear, striped, or mirrored. A mirrored logical volume is a type of logical volume that creates a copy of the data on another physical volume, providing redundancy and fault tolerance. The output shows that the logical volume is mirrored and that one leg of the mirror has failed due to the underlying physical volume. This means that one of the physical volumes that contains the data of the logical volume is damaged or missing. This can cause data loss and performance degradation. The administrator should replace the failed drive and reconfigure the mirror to recover the volume. The administrator should identify the failed physical volume by using commands such as pvdisplay, vgdisplay, or lvdisplay. The administrator should then remove the failed physical volume from the volume group by using the vgreduce command. The administrator should then install a new drive and create a new physical volume by using the pvcreate command. The administrator should then add the new physical volume to the volume group by using the vgextend command. The administrator should then reconfigure the mirror by using the lvconvert command. The administrator should replace the failed drive and reconfigure the mirror to recover the volume. This is the correct answer to the question. The other options are incorrect because they either do not recover the volume (reboot the server. The volume will automatically go back to linear mode or reboot the server. The volume will revert to stripe mode) or do not preserve the data of the volume (recreate the logical volume). References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 10: Managing Storage, pages 333-334.

QUESTION 2

A Linux administrator has defined a systemd script docker-repository.mount to mount a volume for use by the Docker service. The administrator wants to ensure that Docker service does not start until the volume is mounted. Which of the following configurations needs to be added to the Docker service definition to best accomplish this task?

A. After=docker-respository.mount

B. ExecStart=/usr/bin/mount -a

C. Requires=docker-repository.mount

D. RequiresMountsFor=docker-repository.mount

Correct Answer: C

This option declares an explicit dependency between the Docker service and the docker- repository.mount unit. It means that the Docker service will not start unless the docker- repository.mount unit is successfully activated. This ensures that the volume is mounted before the Docker service tries to use it12.

References: 1: systemd.unit - systemd unit configuration 2: How to mount host volumes into docker containers in Dockerfile during build

QUESTION 3

A user created the following script file:

! /bin/bash

FILENAME: /home/user/ script . sh

echo "hello world"

exit 1

However, when the user tried to run the script file using the command "script . sh, an error returned indicating permission was denied. Which of the follow-ing should the user execute in

order for the script to run properly?

A. chmod u+x /home/user/script . sh

B. chmod 600 /home/user/script . sh

C. chmod /home/user/script . sh

D. chmod 0+r /horne/user/script. sh

Correct Answer: A

To run a script file, the user needs to have execute permission on the file. The command chmod u+x /home/user/script.sh (A) will grant execute permission to the owner of the file, which is the user who created it. The other commands will not

give execute permission to the user, and therefore will not allow the script to run properly. References:

[CompTIA Linux+ Study Guide], Chapter 3: Working with Files, Section: Changing File Permissions

[How to Make a Bash Script Executable]

QUESTION 4

A Linux administrator wants to set the SUID of a file named dev_team.text with 744 access rights. Which of the following commands will achieve this goal?

A. chmod 4744 dev_team.txt

B. chmod 744 --setuid dev_team.txt

C. chmod -c 744 dev_team.txt

D. chmod -v 4744 --suid dev_team.txt

Correct Answer: A

Explanation: The command that will set the SUID of a file named dev_team.txt with 744 access rights is chmod 4744 dev_team.txt. This command will use the chmod utility to change the file mode bits of dev_team.txt. The first digit (4) represents the SUID bit, which means that when someone executes dev_team.txt, it will run with the permissions of the file owner. The next three digits (744) represent the read, write, and execute permissions for the owner (7), group (4), and others (4). This means that the owner can read, write, and execute dev_team.txt, while the group and others can only read it. The other options are not correct commands for setting the SUID of a file with 744 access rights. The chmod 744 -setuid dev_team.txt command is invalid because there is no -- setuid option in chmod. The chmod -c 744 dev_team.txt command will change the file mode bits to 744, but it will not set the SUID bit. The -c option only means that chmod will report when a change is made. The chmod -v 4744 --suid dev_team.txt command is also invalid because there is no --suid option in chmod. The -v option only means that chmod will output a diagnostic for every file processed. References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 8: Managing Users and Groups; chmod(1) - Linux manual page

QUESTION 5

An administrator attempts to connect to a remote server by running the following command:

$ nmap 192.168.10.36

Starting Nmap 7.60 (https://nmap.org) at 2022-03-29 20:20 UTC

Nmap scan report for www1 (192.168.10.36)

Host is up (0.000091s latency).

Not shown: 979 closed ports

PORT STATE SERVICE

21/tcp open ftp

22/tcp filtered ssh

631/tcp open ipp

Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds

Which of the following can be said about the remote server?

A. A firewall is blocking access to the SSH server.

B. The SSH server is not running on the remote server.

C. The remote SSH server is using SSH protocol version 1.

D. The SSH host key on the remote server has expired.

Correct Answer: A

This is because the port 22/tcp is shown as filtered by nmap, which means that nmap cannot determine whether the port is open or closed because a firewall or other device is blocking its probes. If the SSH server was not running on the remote server, the port would be shown as closed, which means that nmap received a TCP RST packet in response to its probe. If the remote SSH server was using SSH protocol version 1, the port would be shown as open, which means that nmap received a TCP SYN/ACK packet in response to its probe. If the SSH host key on the remote server had expired, the port would also be shown as open, but the SSH client would display a warning message about the host key verification failure. Therefore, the best explanation for the filtered state of the port 22/tcp is that a firewall is preventing nmap from reaching the SSH server. You can find more information about nmap port states and how to interpret them in the following web search results: Nmap scan what does STATE=filtered mean? How to find ports marked as filtered by nmap Technical Tip: NMAP scan shows ports as filtered