XK0-005 Q&As

CompTIA Linux+ Certification Exam

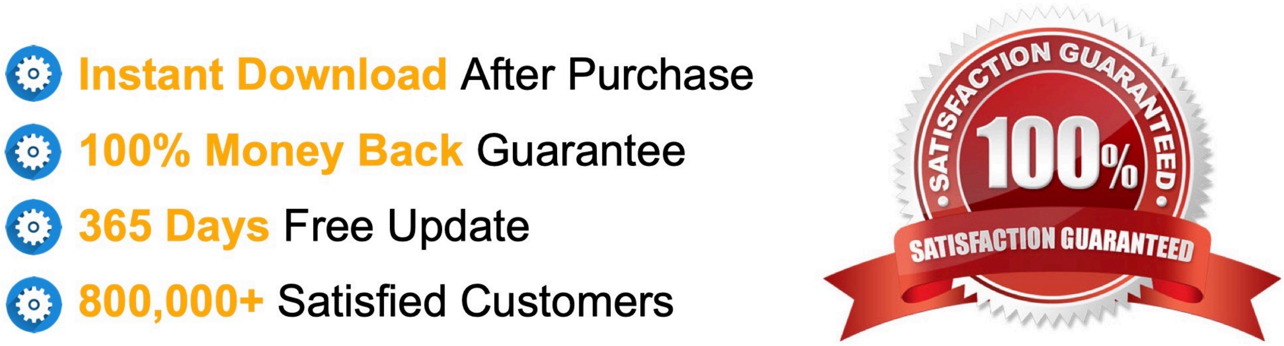
Pass CompTIA XK0-005 Exam with 100% Guarantee

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

https://www.leads4pass.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

An administrator deployed a Linux server that is running a web application on port 6379/tcp.

SELinux is in enforcing mode based on organization policies.

The port is open on the firewall.

Users who are trying to connect to a local instance of the web application receive Error 13, Permission denied.

The administrator ran some commands that resulted in the following output:

```
# semanage port -1 | egrep '(^http_port_t|6379)'
http_port_t tcp 80, 81, 443, 488, 8008, 8009, 8443, 9000

# curl http://1ocalhost/App.php
Cannot connect to App Server.
```

Which of the following commands should be used to resolve the issue?

A. semanage port -d -t http_port_t -p tcp 6379

B. semanage port -a -t http_port_t -p tcp 6379

C. semanage port -a http_port_t -p top 6379

D. semanage port -l -t http_port_tcp 6379

Correct Answer: B

Explanation: The command semanage port -a -t http_port_t -p tcp 6379 adds a new port definition to the SELinux policy and assigns the type http_port_t to the port 6379/tcp. This allows the web application to run on this port and accept connections from users. This is the correct way to resolve the issue. The other options are incorrect because they either delete a port definition (-d), use the wrong protocol (top instead of tcp), or list the existing port definitions (-l). References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 18: Securing Linux Systems, page 535.

QUESTION 2

DRAG DROP

As a Systems Administrator, to reduce disk space, you were tasked to create a shell script that does the following:

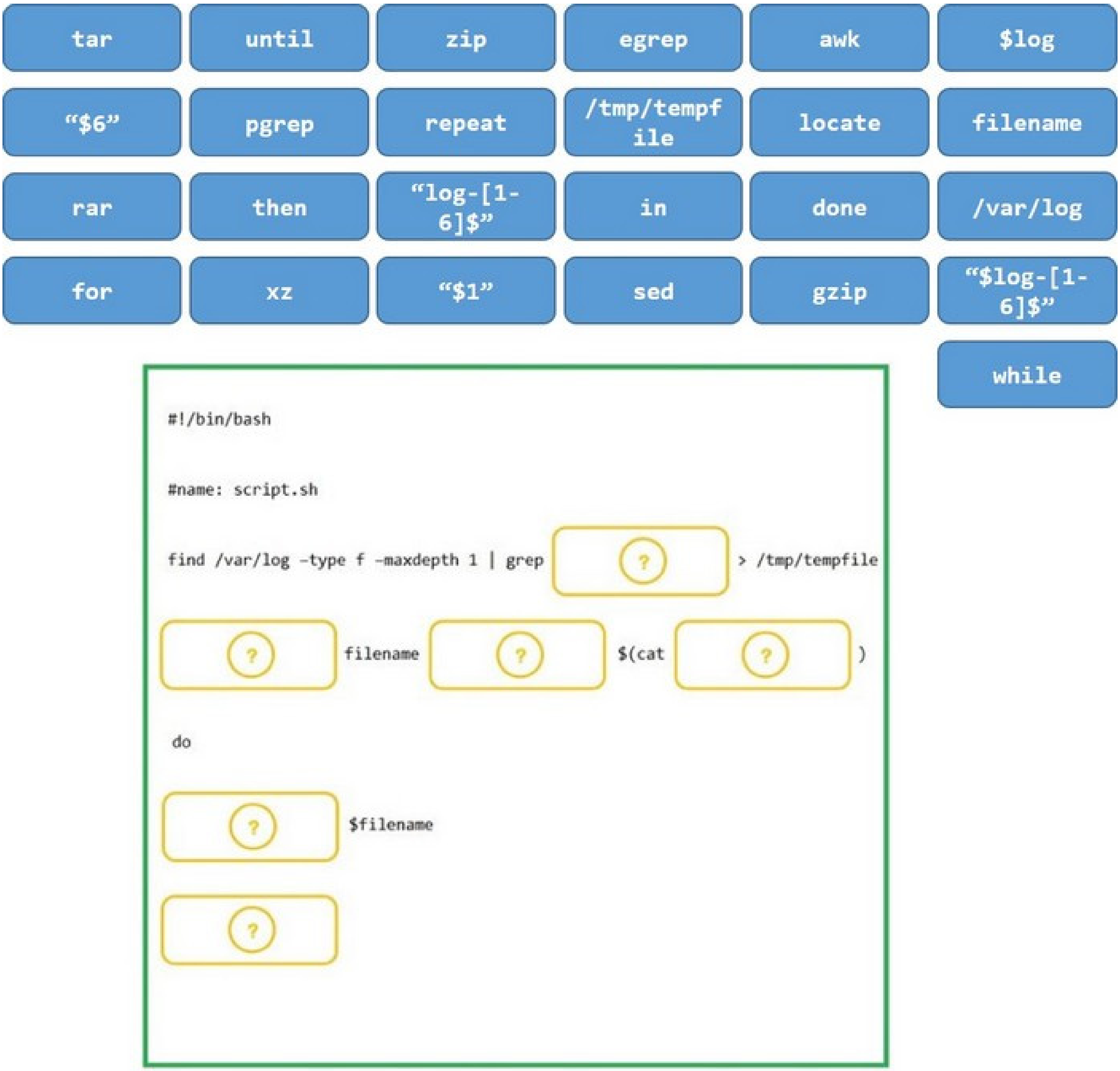
Add relevant content to /tmp/script.sh, so that it finds and compresses rotated files in /var/log without recursion.

INSTRUCTIONS

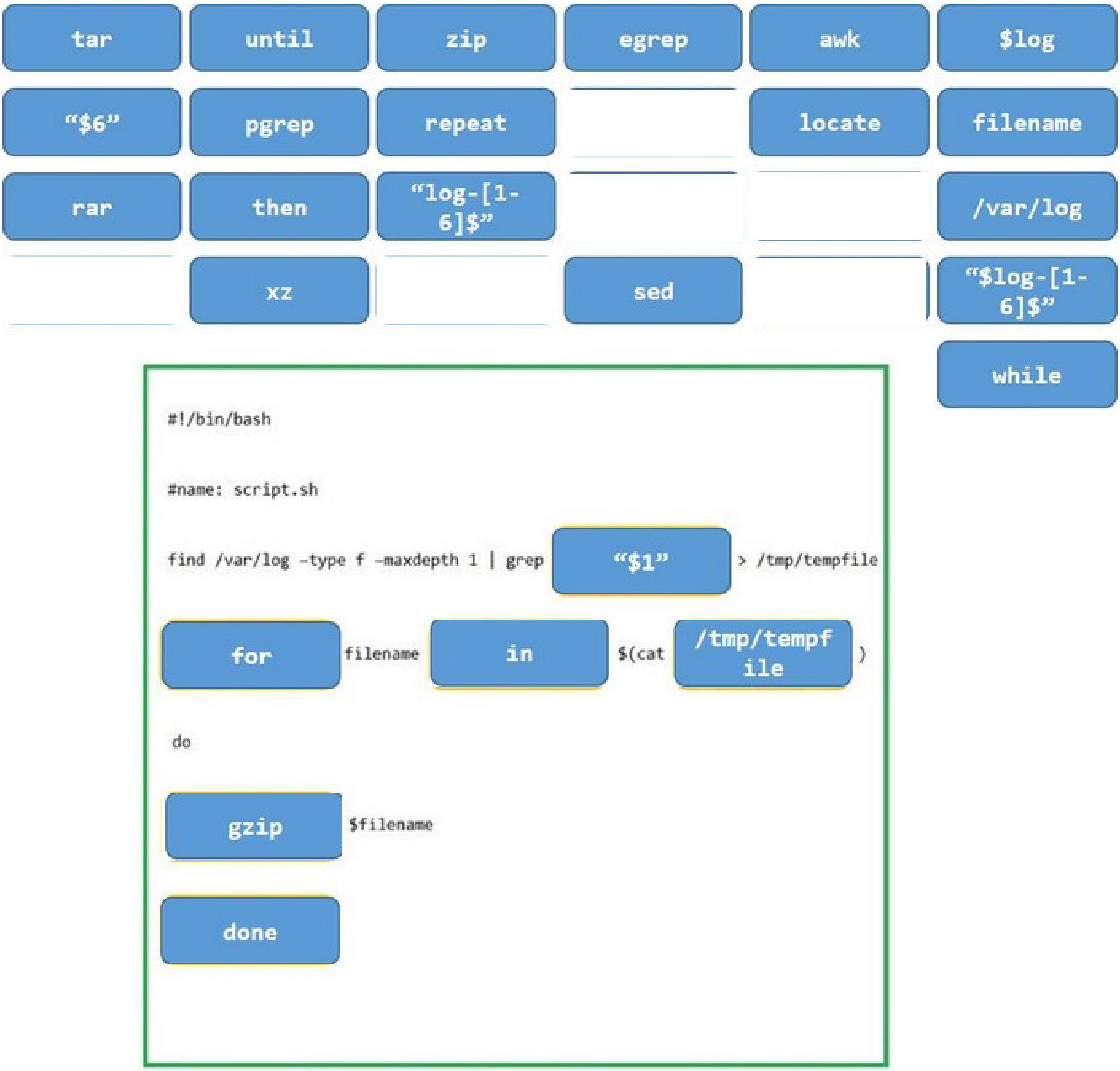
Fill the blanks to build a script that performs the actual compression of rotated log files.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Select and Place:



Correct Answer:



QUESTION 3

Which of the following commands is used to configure the default permissions for new files?

A. setenforce

B. sudo

C. umask

D. chmod

Correct Answer: C

Explanation: The command that is used to configure the default permissions for new files is umask. The umask command is a tool for setting the default permissions for new files and directories on Linux systems. The umask value is a four-digit octal number that represents the permissions that are subtracted from the default permissions. The default permissions for files are 666, which means read and write for owner, group, and others. The default permissions for directories are 777, which means read, write, and execute for owner, group, and others. The umask value consists of four digits: the first digit is for special permissions, such as setuid, setgid, and sticky bit; the second digit is for the owner permissions; the third digit is for the group permissions; and the fourth digit is for the others permissions. The umask value can be calculated by subtracting the desired permissions from the default permissions. For example, if the desired permissions for files are 664, which means read and write for owner and group, and read for others, then the umask value is 002, which is 666 - 664. The command umask 002 will set the umask value to 002, which will ensure that only file owners and group members can modify new files by default. The command that is used to configure the default permissions for new files is umask. This is the correct answer to the question. The other options are incorrect because they either do not set the default permissions for new files (setenforce, sudo, or chmod) or do not exist (kill -HUP or kill -TERM). References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 11: Managing File Permissions and Ownership, page 349.

QUESTION 4

A junior Linux administrator is tasked with installing an application. The installation guide states the application should only be installed in a run level 5 environment.

```
$ systemctl get-default
getty.target
```

Which of the following commands would ensure the server is set to runlevel 5?

A. systemct1 isolate multi-user.target

B. systemct1 isolate graphical.target

C. systemct1 isolate network.target

D. systemct1 isolate basic.target

Correct Answer: B

Explanation: The command that would ensure the server is set to runlevel 5 is systemct1 isolate graphical.target. This command will change the current target (or runlevel) of systemd to graphical.target, which is equivalent to runlevel 5 in SysV init systems. Graphical.target means that the system will start with a graphical user interface (GUI) and all services required for it. The other options are not correct commands for setting the server to runlevel 5. The systemct1 isolate multi-user.target command will change the current target to multi- user.target, which is equivalent to runlevel 3 in SysV init systems. Multiuser.target means that the system will start with multiple user logins and networking, but without a GUI. The systemct1 isolate network.target command will change the current target to network.target, which is not a real runlevel but a synchronization point for network-related services. Network.target means that network functionality should be available, but does not specify whether it should be started before or after it. The systemct1 isolate basic.target command will change the current target to basic.target, which is also not a real runlevel but a synchronization point for basic system services. Basic.target means that all essential services should be started, but does not specify whether it should be started before or after it. References: systemd System and Service Manager; systemd.special(7) - Linux manual page

QUESTION 5

A Linux administrator is troubleshooting an issue in which users are not able to access https://portal.comptia.org from a specific workstation. The administrator runs a few commands and receives the following output:

```
# cat /etc/hosts
10.10.10.55 portal.comptia.org

# host portal.comptia.org
portal.comptia.org has address 192.168.1.55

#cat /etc/resolv.conf
nameserver 10.10.10.5
```

Which of the following tasks should the administrator perform to resolve this issue?

A. Update the name server in resolv. conf to use an external DNS server.

B. Remove the entry for portal . comptia.org from the local hosts file.

C. Add a network route from the 10.10.10.0/24 to the 192.168.0.0/16.

D. Clear the local DNS cache on the workstation and rerun the host command.

Correct Answer: B

The best task to perform to resolve this issue is B. Remove the entry for portal.comptia.org from the local hosts file. This is because the local hosts file has a wrong entry that maps portal.comptia.org to 10.10.10.55, which is different from the

actual IP address of 192.168.1.55 that is returned by the DNS server. This causes a mismatch and prevents the workstation from accessing the website. By removing or correcting the entry in the hosts file, the workstation will use the DNS

server to resolve the domain name and access the website successfully.

To remove or edit the entry in the hosts file, you need to have root privileges and use a text editor such as vi or nano. For example, you can run the command:

sudo vi /etc/hosts

and delete or modify the line that says:

10.10.10.55 portal.comptia.org Then save and exit the file.

QUESTION 6

A Linux system is failing to start due to issues with several critical system processes. Which of the following options can be used to boot the system into the single user mode? (Choose two.)

A. Execute the following command from the GRUB rescue shell: mount -o remount, ro/sysroot.

B. Interrupt the boot process in the GRUB menu and add systemd.unit=single in the kernel line.

C. Interrupt the boot process in the GRUB menu and add systemd.unit=rescue.target in the kernel line.

D. Interrupt the boot process in the GRUB menu and add single=user in the kernel line.

E. Interrupt the boot process in the GRUB menu and add init=/bin/bash in the kernel line.

F. Interrupt the boot process in the GRUB menu and add systemd.unit=single.target in the kernel line.

Correct Answer: CF

The administrator can use the following two options to boot the system into the single user mode: Interrupt the boot process in the GRUB menu and add systemd.unit=rescue.target in the kernel line. This option will boot the system into the rescue mode, which is a minimal environment that allows the administrator to perform basic tasks such as repairing the system. The GRUB menu is a screen that appears when the system is powered on and allows the administrator to choose which kernel or operating system to boot. The kernel line is a line that specifies the parameters for the kernel, such as the root device, the init system, and the boot options. The administrator can interrupt the boot process by pressing the e key in the GRUB menu and edit the kernel line by adding systemd.unit=rescue.target at the end. This option will tell the system to use the rescue target, which is a unit that defines the state of the system in the rescue mode. The administrator can then press Ctrl+X to boot the system with the modified kernel line. This option will boot the system into the single user mode and allow the administrator to troubleshoot the issues. Interrupt the boot process in the GRUB menu and add systemd.unit=single.target in the kernel line. This option will boot the system into the single user mode, which is a mode that allows the administrator to log in as the root user and perform maintenance tasks. The GRUB menu and the kernel line are the same as the previous option. The administrator can interrupt the boot process by pressing the e key in the GRUB menu and edit the kernel line by adding systemd.unit=single.target at the end. This option will tell the system to use the single target, which is a unit that defines the state of the system in the single user mode. The administrator can then press Ctrl+X to boot the system with the modified kernel line. This option will boot the system into the single user mode and allow the administrator to troubleshoot the issues. The other options are incorrect because they either do not boot the system into the single user mode (execute the following command from the GRUB rescue shell: mount -o remount, ro/sysroot or interrupt the boot process in the GRUB menu and add systemd.unit=single in the kernel line) or do not use the correct syntax (interrupt the boot process in the GRUB menu and add single=user in the kernel line or interrupt the boot process in the GRUB menu and add init=/bin/bash in the kernel line). References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 8: Managing the Linux Boot Process, pages 267-268.

QUESTION 7

During a security scan, the password of an SSH key file appeared to be too weak and was cracked. Which of the following commands would allow a user to choose a stronger password and set it on the existing SSH key file?

A. passwd

B. ssh

C. ssh-keygen

D. pwgen

Correct Answer: C

Explanation: The command that would allow a user to choose a stronger password and set it on the existing SSH key file is ssh-keygen -p -f . This command uses the ssh-keygen tool, which is used to generate, manage, and convert authentication keys for SSH. The -p option stands for passphrase, and it allows the user to change or remove the passphrase of an existing private key file. The -f option specifies the filename of the key file. The command will prompt the user for the old passphrase, and then for the new passphrase twice. The other options are not correct commands for changing the password of an SSH key file. The passwd command is used to change the password of a user account on a Linux system, not an SSH key file. The ssh command is used to log in to a remote system using SSH, not to change the password of an SSH key file. The pwgen command is used to generate random passwords, not to change the password of an SSH key file. References: ssh-keygen(1) - Linux manual page; How To: Change Passphrase for SSH Private Key - Unix Tutorial

---

QUESTION 8

The application team has reported latency issues that are causing the application to crash on the Linux server. The Linux administrator starts

troubleshooting and receives the following output:

```
# netstat -s
15762 packets pruned from receive queue because of socket buffer over
690 times the listen queue of a socket overflowed
690 SYNs to LISTEN sockets ignored
2150128 packets collapsed in receive queue due to low socket buffer
TCPBacklogDrop: 844165

# ethtool -S eth0
rx_fw_discards: 4487
```

Which of the following commands will improve the latency issue?

A. # echo \\'net.core.net_backlog = 5000000\\' >> /etc/sysctl.conf # sysctl -p # systemctl daemon-reload

B. # ifdown eth0 # ip link set dev eth0 mtu 800 # ifup eth0

C. # systemctl stop network # ethtool -g eth0 512 # systemctl start network

D. # echo \\'net.core.rmem max = 12500000\\' >> /etc/sysctl.conf # echo \\'net.core.wmem_max = 12500000\\' >> /etc/sysctl.conf # sysctl -p

Correct Answer: D

The best command to use to improve the latency issue is D. # echo `net.core.rmem max = 12500000\\' >> /etc/sysctl.conf # echo `net.core.wmem_max = 12500000\\' >> /etc/sysctl.conf # sysctl -p. This command will increase the size of the

receive and send buffers for the network interface, which can improve the network performance and reduce packet loss. The sysctl command will apply the changes to the kernel parameters without rebooting the system.

The other commands are either incorrect or not suitable for this task. For example:

A. # echo `net.core.net_backlog = 5000000\\' >> /etc/sysctl.conf # sysctl -p # systemctl daemon-reload will try to increase the backlog queue for incoming connections, but this is not relevant for the latency issue. The systemctl daemon- reload command is also unnecessary, as it only reloads the systemd configuration files, not the kernel parameters.

B. # ifdown eth0 # ip link set dev eth0 mtu 800 # ifup eth0 will try to change the maximum transmission unit (MTU) of the network interface to 800 bytes, but this is too low and may cause fragmentation and performance degradation. The default MTU for Ethernet is 1500 bytes, and it should not be changed unless there is a specific reason.

C. # systemctl stop network # ethtool -g eth0 512 # systemctl start network will try to change the ring buffer size of the network interface to 512, but this is too small and may cause packet drops and latency spikes. The default ring buffer size for Ethernet is usually 4096 or higher, and it should be increased if there is a high network traffic.

QUESTION 9

A cloud engineer needs to remove all dangling images and delete all the images that do not have an associated container. Which of the following commands will help to accomplish this task?

A. docker images prune -a

B. docker push images -a

C. docker rmi -a images

D. docker images rmi --all

Correct Answer: A

Explanation: The command docker images prune -a will help to remove all dangling images and delete all the images that do not have an associated container. The docker command is a tool for managing Docker containers and images. The images subcommand operates on images. The prune option removes unused images. The -a option removes all images, not just dangling ones. A dangling image is an image that is not tagged and is not referenced by any container. This command will accomplish the task of cleaning up the unused images. The other options are incorrect because they either do not exist (docker push images -a or docker images rmi --all) or do not remove images (docker rmi -a images only removes images that match the name or ID of "images"). References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 19: Managing Cloud and Virtualization Technologies, page 567.

QUESTION 10

An application developer received a file with the following content:

##This is a sample Image ##

FROM ubuntu:18.04

MAINTAINER demohut@gtmail.com.hac

COPY . /app

RUN make /app CMD python /app/app.py

RUN apt-get update

RUN apt-get install -y nginx

CMD ["echo","Image created"]

The developer must use this information to create a test bed environment and identify the image (myimage) as the first version for testing a new

application before moving it to production. Which of the following commands will accomplish this task?

A. docker build -t myimage:1.0 .

B. docker build -t myimage: .

C. docker build -t myimage-1.0 .

D. docker build -i myimage:1.0 .

Correct Answer: A

The docker build command is used to build an image from a Dockerfile and a context1. The Dockerfile is a text file that contains the instructions for creating the image, and the context is a set of files that can be used in the image creation

process1. The file that the developer received is an example of a Dockerfile.

The -t option is used to specify a name and an optional tag for the image1. The name and tag are separated by a colon (:), and the tag is usually used to indicate the version of the image2. For example, -t myimage:1.0 means that the image

will be named myimage and tagged as 1.0.

The last argument of the docker build command is the path to the context, which can be a local directory or a URL1. The dot (.) means that the current working directory is the context2. Therefore, docker build -t myimage:1.0 . means that the

image will be built from the Dockerfile and the files in the current working directory, and it will be named myimage and tagged as 1.0.

QUESTION 11

Users are reporting that writes on a system configured with SSD drives have been taking longer than expected, but reads do not seem to be affected. A Linux systems administrator is investigating this issue and working on a solution. Which of the following should the administrator do to help solve the issue?

A. Run the corresponding command to trim the SSD drives.

B. Use fsck on the filesystem hosted on the SSD drives.

C. Migrate to high-density SSD drives for increased performance.

D. Reduce the amount of files on the SSD drives.

Correct Answer: A

TRIM is a feature that allows the operating system to inform the SSD which blocks of data are no longer in use and can be wiped internally. This helps to maintain the SSD\\'s performance and endurance by preventing unnecessary write operations and reducing write amplification12. Running the corresponding command to trim the SSD drives, such as fstrim or blkdiscard on Linux, can help to solve the issue of slow writes by freeing up space and optimizing the SSD\\'s internal garbage collection34. References: 1: What is SSD TRIM, why is it useful, and how to check whether it is turned on 2: How to Trim SSD in Windows 10 3: How to run fsck on an external drive with OS X? 4: How to Use the fsck Command on Linux

---

QUESTION 12

The development team wants to prevent a file from being modified by all users in a Linux system, including the root account. Which of the following commands can be used to accomplish this objective?

A. chmod / app/conf/file

B. setenforce / app/ conf/ file

C. chattr +i /app/conf/file

D. chmod 0000 /app/conf/file

Correct Answer: C

The chattr command is used to change file attributes on Linux systems that support extended attributes, such as ext2, ext3, ext4, btrfs, xfs, and others. File attributes are flags that modify the behavior of files and directories.

To prevent a file from being modified by all users in a Linux system, including the root account, the development team can use the chattr +i /app/conf/file command. This command will set the immutable attribute (+i) on the file /app/conf/file,

which means that the file cannot be deleted, renamed, linked, appended, or written to by any user or process. To remove the immutable attribute, the development team can use the chattr -i /app/conf/file command. The statement C is correct.

The statements A, B, and D are incorrect because they do not prevent the file from being modified by all users. The chmod /app/conf/file command does not work because it requires an argument to specify the permissions to change. The

setenforce /app/conf/file command does not work because it is used to change the SELinux mode, not file attributes. The chmod 0000 /app/conf/file command will remove all permissions from the file, but it can still be modified by the root

account. References: [How to Use chattr Command in Linux]

QUESTION 13

Which of the following tools is commonly used for creating CI/CD pipelines?

A. Chef

B. Puppet

C. Jenkins

D. Ansible

Correct Answer: C

Explanation: The tool that is commonly used for creating CI/CD pipelines is Jenkins. Jenkins is an open-source automation server that enables continuous integration and continuous delivery (CI/CD) of software projects. Jenkins allows developers to build, test, and deploy code changes automatically and frequently using various plugins and integrations. Jenkins also supports distributed builds, parallel execution, pipelines as code, and real-time feedback. References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 19: Managing Source Code; Jenkins

QUESTION 14

A systems administrator received a request to change a user\\'s credentials. Which of the following commands will grant the request?

A. sudo passwd

B. sudo userde 1

C. sudo chage

D. sudo usermod

Correct Answer: A

Explanation: This command will allow the systems administrator to change the password of another user account in the system. The sudo prefix will grant the administrator the necessary privileges to perform this action, and the passwd

command will prompt for the new password for the specified user. For example, if the administrator wants to change the password of a user named tom, the command will look like this:

sudo passwd tom

The other options are incorrect because:

B. sudo userdel

This command will delete a user account from the system, not change its credentials. The userdel command removes the user\\'s entry from the /etc/passwd and /etc/shadow files, as well as deletes the user\\'s home directory and mail spool.

This is not what the request asked for.

C. sudo chage

This command will change the password expiration and aging information for a user account, not its credentials. The chage command can be used to set or modify various parameters related to password aging, such as the minimum and

maximum number of days between password changes, the number of days before password expiration to issue a warning, and so on. This is not what the request asked for.

D. sudo usermod

This command will modify various attributes of a user account, such as its login name, home directory, default shell, primary group, and so on. However, it cannot change the user\\'s password directly. To do that, the usermod command

requires the -p option followed by an encrypted password string, which is not easy to generate manually. Therefore, this is not a practical way to change a user\\'s credentials.

References:

How to Change Account Passwords on Linux

How to Change a Password in Linux for Root and Other Users CompTIA Linux+ Certification Exam Objectives

QUESTION 15

The security team has identified a web service that is running with elevated privileges A Linux administrator is working to change the systemd service file to meet security compliance standards. Given the following output: Which of the following remediation steps will prevent the web service from running as a privileged user?

```
[Unit]
Description=CompTIA server daemon
Documentation=man:webserver(8) man:webserver_config(5)
After=network.target

[Service]
Type=notify
EnvironmentFile=/etc/webserver/config
ExecStart=/usr/sbin/webserver -D $OPTIONS
ExecReload=/bin/kill -HUP $MAINPID
KillMode=process
Restart=on-failure
RestartSec=42s

[Install]
WantedBy=multi-user.target
```

A. Removing the ExecStarWusr/sbin/webserver -D SOPTIONS from the service file

B. Updating the Environment File line in the [Service] section to/home/webservice/config

C. Adding the User-webservice to the [Service] section of the service file

D. Changing the:nulti-user.target in the [Install] section to basic.target

Correct Answer: C

Explanation: The remediation step that will prevent the web service from running as a privileged user is adding the User=webservice to the [Service] section of the service file. The service file is a configuration file that defines the properties and behavior of a systemd service. The systemd is a system and service manager that controls the startup and operation of Linux systems. The service file contains various sections and options that specify how the service should be started, stopped, and managed. The [Service] section defines how the service should be executed and what commands should be run. The User option specifies the user name or ID that the service should run as. The webservice is the name of the user that the administrator wants to run the web service as. The administrator should add the User=webservice to the [Service] section of the service file, which will prevent the web service from running as a privileged user, such as root, and improve the security of the system. This is the correct remediation step to use to prevent the web service from running as a privileged user. The other options are incorrect because they either do not change the user that the service runs as (removing the ExecStart=/usr/sbin/webserver -D OPTIONS from the service file or updating the EnvironmentFile line in the [Service] section to /home/webservice/config) or do not affect the user that the service runs as (changing the multiuser.target in the [Install] section to basic.target). References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 15: Managing System Services, page 458.