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.certbus.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 new file was added to a main Git repository. An administrator wants to synchronize a local copy with the contents of the main repository. Which of the following commands should the administrator use for this task?

A. git reflog

B. git pull

C. git status

D. git push

Correct Answer: B

Explanation: The command iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT -- to-destination 192.0.2.25:3128 adds a rule to the nat table that redirects all incoming TCP packets with destination port 80 (HTTP) to the proxy server

192.0.2.25 on port 3128. This is the correct way to achieve the task. The other options are incorrect because they either delete a rule (-D), use the wrong protocol (top instead of tcp), or use the wrong port (81 instead of 80). References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 12: Managing Network Connections, page 381.

QUESTION 2

A Linux administrator is configuring a two-node cluster and needs to be able to connect the nodes to each other using SSH keys from the root account. Which of the following commands will accomplish this task?

A. [root@nodea ssh --i ~/ . ssh/±d rsa root@nodeb

B. [root@nodea scp -i . ssh/id rsa root@nodeb

C. [root@nodea ssh--copy-id --i .ssh/id rsa root@nodeb

D. [root@nodea # ssh add -c ~/ . ssh/id rsa root@nodeb

E. [root@nodea # ssh add -c ~/. ssh/id rsa root@nodeb

Correct Answer: C

The ssh-copy-id command is used to copy a public SSH key from a local machine to a remote server and add it to the authorized_keys file, which allows passwordless authentication between the machines. The administrator can use this command to copy the root user\\'s public key from nodea to nodeb, and vice versa, to enable SSH access between the nodes without entering a password every time. For example: [root@nodea ssh-copy-id -i ~/.ssh/id_rsa root@nodeb]. The ssh command is used to initiate an SSH connection to a remote server, but it does not copy any keys. The scp command is used to copy files securely between machines using SSH, but it does not add any keys to the authorized_keys file. The ssh-add command is used to add private keys to the SSH agent, which manages them for SSH authentication, but it does not copy any keys to a remote server.

QUESTION 3

Which of the following files holds the system configuration for journal when running systemd?

A. /etc/systemd/journald.conf

B. /etc/systemd/systemd-journalctl.conf

C. /usr/lib/systemd/journalctl.conf

D. /etc/systemd/systemd-journald.conf

Correct Answer: A

Explanation: The file that holds the system configuration for journal when running systemd is /etc/systemd/journald.conf. This file contains various settings that control the behavior of the journald daemon, which is responsible for collecting and storing log messages from various sources. The journald.conf file can be edited to change the default values of these settings, such as the storage location, size limits, compression, and forwarding options of the journal files. The file also supports a drop-in directory /etc/systemd/journald.conf.d/ where additional configuration files can be placed to override or extend the main file. References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 18: Automating Tasks; journald.conf(5) - Linux manual page

QUESTION 4

A file called testfile has both uppercase and lowercase letters: $ cat testfile ABCDEfgH IJKLmnoPQ abcdefgH ijklLMNopq A Linux administrator is tasked with converting testfile into all uppercase and writing it to a new file with the name uppercase. Which of the following commands will achieve this task?

A. tr \\'(A-Z}\\' \\'{a-z}\\' uppercase

B. echo testfile | tr "[Z-A]" "[z-a]" uppercase

C. cat testfile | tr \\'{z-a)\\' \\'{Z-A}\\' uppercase

D. tr \\'[a-z]\\' \\'[A-Z]\\' uppercase

Correct Answer: D

This command will use the tr tool to translate all lowercase letters in the testfile to uppercase letters and write the output to the uppercase file. The first argument `[a-z]\\' specifies the set of characters to be replaced, and the second argument ` [A-Z]\\' specifies the set of characters to replace with. The `> /etc/profile

B. echo \\'export PATH=/opt/operations1/bin\\' >> /etc/profile

C. echo \\'export PATH=$PATH/opt/operations1/bin\\' >> /etc/profile

D. echo \\'export $PATH:/opt/operations1/bin\\' >> /etc/profile

Correct Answer: A

Explanation: The command echo \\'export PATH=$PATH:/opt/operations1/bin\\' >> /etc/profile should be used to resolve the issue of users not being able to access the application without using the full path. The echo command prints the given string to the standard output. The export command sets an environment variable and makes it available to all child processes. The PATH variable contains a list of directories where the shell looks for executable files. The $PATH expands to the current value of the PATH variable. The : separates the directories in the list. The /opt/operations1/bin is the directory where the application is installed. The >> operator appends the output to the end of the file. The /etc/profile file is a configuration file that is executed when a user logs in. The command echo \\'export PATH=$PATH:/opt/operations1/bin\\' >> /etc/profile will add the /opt/operations1/bin directory to the PATH variable for all users and allow them to access the application without using the full path. This is the correct command to use to

resolve the issue. The other options are incorrect because they either overwrite the PATH variable (echo \\'export PATH=/opt/operations1/bin\\' >> /etc/profile) or do not use the correct syntax (echo \\'export PATH=$PATH/opt/operations1/bin\\' >> /etc/profile or echo \\'export $PATH:/opt/operations1/bin\\' >> /etc/profile). References: CompTIA Linux+ (XK0- 005) Certification Study Guide, Chapter 9: Working with the Linux Shell, page 295.

QUESTION 9

A Linux administrator was asked to run a container with the httpd server inside. This container should be exposed at port 443 of a Linux host machine while it internally listens on port 8443. Which of the following commands will accomplish this task?

A. podman run -d -p 443:8443 httpd

B. podman run -d -p 8443:443 httpd

C. podman run -d -e 443:8443 httpd

D. podman exec -p 8443:443 httpd

Correct Answer: A

Explanation: The command that will accomplish the task of running a container with the httpd server inside and exposing it at port 443 of the Linux host machine while it internally listens on port 8443 is podman run -d -p 443:8443 httpd. This command uses the podman tool, which is a daemonless container engine that can run and manage containers on Linux systems. The -d option runs the container in detached mode, meaning that it runs in the background without blocking the terminal. The -p option maps a port on the host machine to a port inside the container, using the format host_port:container_port. In this case, port 443 on the host machine is mapped to port 8443 inside the container, allowing external access to the httpd server. The httpd argument specifies the name of the image to run as a container, which in this case is an image that contains the Apache HTTP Server software. The other options are not correct commands for accomplishing the task. Podman run -d -p 8443:443 httpd maps port 8443 on the host machine to port 443 inside the container, which does not match the requirement. Podman run -d -e 443:8443 httpd uses the -e option instead of the -p option, which sets an environment variable inside the container instead of mapping a port. Podman exec -p 8443:443 httpd uses the podman exec command instead of the podman run command, which executes a command inside an existing container instead of creating a new one. References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 18: Automating Tasks

QUESTION 10

A Linux engineer is setting the sticky bit on a directory called devops with 755 file permission. Which of the following commands will accomplish this task?

A. chown -s 755 devops

B. chown 1755 devops

C. chmod -s 755 devops

D. chmod 1755 devops

Correct Answer: D

Explanation: The command that will set the sticky bit on a directory called devops with 755 file permission is chmod 1755 devops. This command will use chmod to change the mode of the directory devops to 1755, which means that the

owner has read, write, and execute permissions (7), the group has read and execute permissions (5), and others have read and execute permissions (5). The first digit 1 indicates that the sticky bit is set on the directory, which is a special permission that prevents users from deleting or renaming files in the directory that they do not own. The other options are not correct commands for setting the sticky bit on a directory. The chown -s 755 devops command is invalid because chown is used to change the owner and group of files or directories, not their permissions. The -s option for chown is used to remove a symbolic link, not to set the sticky bit. The chown 1755 devops command is also invalid because chown does not accept numeric arguments for changing permissions. The chmod -s 755 devops command will remove the sticky bit from the directory devops, not set it. References: chmod(1) - Linux manual page; How to Use SUID, SGID, and Sticky Bits on Linux

QUESTION 11

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

QUESTION 12

A systems administrator notices the process list on a mission-critical server has a large number of processes that are in state "Z" and marked as "defunct." Which of the following should the administrator do in an attempt to safely remove these entries from the process list?

A. Kill the process with PID 1.

B. Kill the PID of the processes.

C. Kill the parent PID of the processes.

D. Reboot the server.

Correct Answer: C

Explanation: As the web search results show, processes in state Z are defunct or zombie processes, which means they have terminated but their parent process has not reaped them properly. They do not consume any resources, but they occupy a slot in the process table. To remove them from the process list, the administrator needs to kill the parent process of the zombies, which will cause them to be reaped by the init process (PID 1). Killing the zombies themselves or the init process will not have any effect, as they are already dead. Rebooting the server may work, but it is not a safe or efficient option, as it may cause unnecessary downtime or data loss for a mission-critical server.

References Processes in a Zombie (Z) or Defunct State | Support | SUSE, paragraph 3 linux - Zombie vs Defunct processes? - Stack Overflow, answer by admirableadmin How To Kill Zombie Processes on Linux | Linux Journal, paragraph 4

QUESTION 13

A systems administrator made some unapproved changes prior to leaving the company. The newly hired administrator has been tasked with revealing the system to a compliant state. Which of the following commands will list and remove the correspondent packages?

A. dnf list and dnf remove last

B. dnf remove and dnf check

C. dnf info and dnf upgrade

D. dnf history and dnf history undo last

Correct Answer: D

Explanation: The commands that will list and remove the corresponding packages are dnf history and dnf history undo last. The dnf history command will display a list of all transactions performed by dnf, such as installing, updating, or removing packages. Each transaction has a unique ID, a date and time, an action, and a number of altered packages. The dnf history undo last command will undo the last transaction performed by dnf, meaning that it will reverse all package changes made by that transaction. For example, if the last transaction installed some packages, dnf history undo last will remove them. The other options are not correct commands for listing and removing corresponding packages. The dnf list command will display a list of available packages in enabled repositories, but not the packages installed by dnf transactions. The dnf remove command will remove specified packages from the system, but not all

packages from a specific transaction. The dnf info command will display detailed information about specified packages, but not about dnf transactions. The dnf upgrade command will upgrade all installed packages to their latest versions, but not undo any package changes. References: Handling package management history; dnf(8) - Linux manual page

QUESTION 14

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 15

A Linux system is getting an error indicating the root filesystem is full. Which of the following commands should be used by the systems administrator to resolve this issue? (Choose three.)

A. df -h /

B. fdisk -1 /dev/sdb

C. growpart /dev/mapper/rootvg-rootlv

D. pvcreate /dev/sdb

E. lvresize -L +10G -r /dev/mapper/rootvg-rootlv

F. lsblk /dev/sda

G. parted -l /dev/mapper/rootvg-rootlv

H. vgextend /dev/rootvg /dev/sdb

Correct Answer: ACE

The administrator should use the following three commands to resolve the issue of the root filesystem being full:

df -h /. This command will show the disk usage of the root filesystem in a human- readable format. The df command is a tool for reporting file system disk space usage. The -h option displays the sizes in powers of 1024 (e.g., 1K, 234M, 2G).

The / specifies the root filesystem. The command df -h / will show the total size, used space, available space, and percentage of the root filesystem. This command will help the administrator identify the problem and plan the solution.

growpart /dev/mapper/rootvg-rootlv. This command will grow the partition that contains the root filesystem to the maximum size available. The growpart command is a tool for resizing partitions on Linux systems. The /dev/mapper/rootvg-rootlv

is the device name of the partition, which is a logical volume managed by the Logical Volume Manager (LVM). The command growpart /dev/mapper/rootvg-rootlv will extend the partition to fill the disk space and increase the size of the root

filesystem. This command will help the administrator solve the problem and free up space.

lvresize -L +10G -r /dev/mapper/rootvg-rootlv. This command will resize the logical volume that contains the root filesystem and add 10 GB of space. The lvresize command is a tool for resizing logical volumes on Linux systems. The -L option

specifies the new size of the logical volume, in this case +10G, which means 10 GB more than the current size. The -r option resizes the underlying file system as well. The /dev/mapper/rootvg-rootlv is the device name of the logical volume,

which is the same as the partition name. The command lvresize -L +10G -r /dev/mapper/rootvg-rootlv will increase the size of the logical volume and the root filesystem by 10 GB and free up space. This command will help the administrator

solve the problem and free up space. The other options are incorrect because they either do not affect the root filesystem (fdisk - 1 /dev/sdb, pvcreate /dev/sdb, lsblk /dev/sda, or vgextend /dev/rootvg /dev/sdb) or do not use the correct syntax

(fdisk -1 /dev/sdb instead of fdisk -l /dev/sdb or parted -l /dev/mapper/rootvg-rootlv instead of parted /dev/mapper/rootvg-rootlv print). References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 10:

Managing Storage, pages 318-319, 331-332.