

CompTIA

Exam Questions XK0-005

CompTIA Linux+ Certification Exam



NEW QUESTION 1

A Linux administrator intends to start using KVM on a Linux server. Which of the following commands will allow the administrator to load the KVM module as well as any related dependencies?

- A. modprobe kvm
- B. insmod kvm
- C. depmod kvm
- D. hotplug kvm

Answer: A

Explanation:

This command will load the KVM module as well as any related dependencies, such as kvm-intel or kvm-amd, depending on the processor type. The modprobe command is a Linux utility that reads the /etc/modules.conf file and adds or removes modules from the kernel. It also resolves any dependencies between modules, so that they are loaded in the correct order.

The other options are incorrect because:

* B. insmod kvm

This command will only load the KVM module, but not any related dependencies. The insmod command is a low-level Linux utility that inserts a single module into the kernel. It does not resolve any dependencies between modules, so they have to be loaded manually.

* C. depmod kvm

This command will not load the KVM module at all, but only create a list of module dependencies for modprobe to use. The depmod command is a Linux utility that scans the installed modules and generates a file called modules.dep that contains dependency information for each module.

* D. hotplug kvm

This command is invalid and does not exist. The hotplug mechanism is a feature of the Linux kernel that allows devices to be added or removed while the system is running. It does not have anything to do with loading modules.

NEW QUESTION 2

A Linux user is trying to execute commands with sudo but is receiving the following error:

```
$ sudo visudo
```

```
>>> /etc/sudoers: syntax error near line 28 <<< sudo: parse error in /etc/sudoers near line 28 sudo: no valid sudoers sources found, quitting The following output is provided:
```

```
# grep root /etc/shadow root :* LOCK *: 14600 :::::
```

Which of the following actions will resolve this issue?

- A. Log in directly using the root account and comment out line 28 from /etc/sudoers.
- B. Boot the system in single user mode and comment out line 28 from /etc/sudoers.
- C. Comment out line 28 from /etc/sudoers and try to use sudo again.
- D. Log in to the system using the other regular user, switch to root, and comment out line 28 from /etc/sudoers.

Answer: B

NEW QUESTION 3

A Linux administrator wants to find out whether files from the wget package have been altered since they were installed. Which of the following commands will provide the correct information?

- A. rpm -i wget
- B. rpm -qf wget
- C. rpm -F wget
- D. rpm -V wget

Answer: D

Explanation:

The command that will provide the correct information about whether files from the wget package have been altered since they were installed is rpm -V wget. This command will use the rpm utility to verify an installed RPM package by comparing information about the installed files with information from the RPM database.

The verification process can check various attributes of each file, such as size, mode, owner, group, checksum, capabilities, and so on. If any discrepancies are found, rpm will report them using a single letter code for each attribute.

The other options are not correct commands for verifying an installed RPM package. The rpm -i wget command is invalid because -i is used to install a package from a file, not to verify an installed package. The rpm -qf wget command will query which package owns wget as a file name or path name, but it will not verify its attributes. The rpm -F wget command will freshen (upgrade) an already installed package with wget as a file name or path name, but it will not verify its attributes.

References: rpm(8) - Linux manual

page; Using RPM to Verify Installed Packages

NEW QUESTION 4

A Linux administrator is tasked with creating resources using containerization. When deciding how to create this type of deployment, the administrator identifies some key features, including portability, high availability, and scalability in production. Which of the following should the Linux administrator choose for the new design?

- A. Docker
- B. On-premises systems
- C. Cloud-based systems
- D. Kubernetes

Answer: D

Explanation:

The Linux administrator should choose Kubernetes for the new design that requires portability, high availability, and scalability in production using containerization. Kubernetes is an open-source platform that automates the deployment, scaling, and management of containerized applications across clusters of

nodes. Kubernetes provides features such as service discovery, load balancing, storage orchestration, self-healing, secret and configuration management, and batch execution. Kubernetes also supports multiple container runtimes, such as Docker, containerd, and CRI-O, making it portable across different platforms and clouds. References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 18: Automating Tasks; What is Kubernetes? | Kubernetes

NEW QUESTION 5

A Linux administrator has physically added a new RAID adapter to a system. Which of the following commands should the Linux administrator run to confirm that the device has been recognized? (Select TWO).

- A. rmmod
- B. ls -l /etc
- C. lshw —class disk
- D. pvdisplay
- E. rmdir /dev
- F. dmesg

Answer: CF

Explanation:

The following commands can help you confirm that the new RAID adapter has been recognized by the Linux system:

? dmesg: This command displays the kernel messages, which can show the information about the newly detected hardware device. You can use `dmesg | grep -i raid` to filter the output for RAID-related messages.

? lshw -class disk: This command lists the disk devices on the system, including the RAID controller and its model name. You can use `lshw -class disk | grep -i raid` to filter the output for RAID-related information.

The other commands are not relevant for this purpose. For example:

? rmmod: This command removes a module from the Linux kernel, which is not useful for detecting a new device.

? ls -l /etc: This command lists the files and directories in the /etc directory, which is not related to hardware devices.

? pvdisplay: This command displays the attributes of physical volumes, which are part of the logical volume management (LVM) system, not the RAID system.

? rmdir /dev: This command removes an empty directory, which is not helpful for detecting a new device. Moreover, /dev is a special directory that contains device files, and should not be removed.

NEW QUESTION 6

An administrator has source code and needs to rebuild a kernel module. Which of the following command sequences is most commonly used to rebuild this type of module?

- A. ./configure make make install
- B. wget gcc cp
- C. tar xvzf buildcp
- D. build install configure

Answer: A

Explanation:

The best command sequence to rebuild a kernel module from source code is A. `./configure make make install`. This is the standard way to compile and install a Linux kernel module, as explained in the web search result 5. The other commands are either not relevant, not valid, or not sufficient for this task. For example:

? B. `wget gcc cp` will try to download, compile, and copy a file, but it does not specify the source code, the module name, or the destination directory.

? C. `tar xvzf buildcp` will try to extract, build, and copy a compressed file, but it does not specify the file name, the module name, or the destination directory.

? D. `build install configure` will try to run three commands that are not defined or recognized by the Linux shell.

NEW QUESTION 7

A cloud engineer needs to block the IP address 192.168.10.50 from accessing a Linux server. Which of the following commands will achieve this goal?

- A. `iptables -F INPUT -j 192.168.10.50 -m DROP`
- B. `iptables -A INPUT -s 192.168.10.50 -j DROP`
- C. `iptables -i INPUT --ipv4 192.168.10.50 -z DROP`
- D. `iptables -j INPUT 192.168.10.50 -p DROP`

Answer: B

Explanation:

The correct command to block the IP address 192.168.10.50 from accessing a Linux server is `iptables -A INPUT -s 192.168.10.50 -j DROP`. This command appends a rule to the INPUT chain that matches the source address 192.168.10.50 and jumps to the DROP target, which discards the packet. The other commands are incorrect because they either have invalid syntax, wrong parameters, or wrong order of arguments. References:

CompTIA Linux+ Study Guide, Fourth Edition, page 457-458.

NEW 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

Answer: D

Explanation:

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.

NEW QUESTION 9

A Linux administrator is troubleshooting a memory-related issue. Based on the output of the commands:

```
$ vmstat -s --unit M

968 M total memory
331 M used memory
482 M active memory
279 M inactive memory
99 M free memory

$ free -h

             total        used        free      shared  buff/cache   available
Mem:          968M        331M          95M         13M         540M         458M
Swap:           0           0           0

$ ps -aux | grep script.sh
USER  PID   %CPU  %MEM  VSZ   RSS    TTY  STAT  START  TIME  COMMAND
user  8321  2.8   40.5 3224846 371687  7    SN    16:49   2:09  /home/user/script.sh
```

Which of the following commands would address the issue?

- A. top -p 8321
B. kill -9 8321
C. renice -10 8321
D. free 8321

Answer: B

Explanation:

The command that would address the memory-related issue is kill -9 8321. This command will send a SIGKILL signal to the process with the PID 8321, which is the mysqld process that is using 99.7% of the available memory according to the top output. The SIGKILL signal will terminate the process immediately and free up the memory it was using. However, this command should be used with caution as it may cause data loss or corruption if the process was performing some critical operations.

The other options are not correct commands for addressing the memory-related issue. The top -p 8321 command will only display information about the process with the PID 8321, but will not kill it or reduce its memory usage. The renice -10 8321 command will change the priority (niceness) of the process with the PID 8321 to -10, which means it will have a higher scheduling priority, but this will not affect its memory consumption. The free 8321 command is invalid because free does not take a PID as an argument; free only displays information about the total, used, and free memory in the system. References: How to troubleshoot Linux server memory issues; kill(1) - Linux manual page

NEW QUESTION 10

To harden one of the servers, an administrator needs to remove the possibility of remote administrative login via the SSH service. Which of the following should the administrator do?

- A. Add the line DenyUsers root to the /etc/hosts.deny file.
B. Set PermitRootLogin to no in the /etc/ssh/sshd_config file.
C. Add the line account required pam_nologin
D. so to the /etc/pam.d/sshd file.
E. Set PubKeyAuthentication to no in the /etc/ssh/ssh_config file.

Answer: B

Explanation:

The administrator should set PermitRootLogin to no in the /etc/ssh/sshd_config file to remove the possibility of remote administrative login via the SSH service. The PermitRootLogin directive controls whether the root user can log in using SSH. Setting it to no will deny any remote login attempts by the root user. This will harden the server and prevent unauthorized access. The administrator should also restart the sshd service after making the change. The other options are incorrect because they either do not affect the SSH service (/etc/hosts.deny or /etc/pam.d/sshd) or do not prevent remote administrative login (PubKeyAuthentication). References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 13: Managing Network Services, page 413.

NEW QUESTION 10

An administrator needs to make an application change via a script that must be run only in console mode. Which of the following best represents the sequence the administrator should execute to accomplish this task?

- A. `systemctl isolate multi-user.target sh script.sh systemctl isolate graphical.target`
- B. `systemctl isolate graphical.target sh script.sh systemctl isolate multi-user.target`
- C. `sh script.sh systemctl isolate multi-user.target systemctl isolate graphical.target`
- D. `systemctl isolate multi-user.target systemctl isolate graphical.target sh script.sh`

Answer: A

Explanation:

The correct answer is A. `systemctl isolate multi-user.target sh script.sh systemctl isolate graphical.target`

This sequence will allow the administrator to switch from the graphical mode to the console mode, run the script, and then switch back to the graphical mode.

The `systemctl` command is used to control the `systemd` system and service manager, which manages the boot targets and services on Linux systems. The `isolate` subcommand starts the unit specified on the command line and its dependencies and stops all others. The `multi-user.target` is a boot target that provides a text-based console login, while the `graphical.target` is a boot target that provides a graphical user interface. By using `systemctl isolate`, the administrator can change the boot target on the fly without rebooting the system.

The `sh` command is used to run a shell script, which is a file that contains a series of commands that can be executed by the shell. The `script.sh` is the name of the script that contains the application change that the administrator needs to make. By running `sh script.sh`, the administrator can execute the script in the console mode.

The other options are incorrect because:

* B. `systemctl isolate graphical.target sh script.sh systemctl isolate multi-user.target`

This sequence will switch from the console mode to the graphical mode, run the script, and then switch back to the console mode. This is not what the administrator wants to do, as the script must be run only in console mode.

* C. `sh script.sh systemctl isolate multi-user.target systemctl isolate graphical.target`

This sequence will run the script in the current mode, which may or may not be console mode, and then switch to console mode and back to graphical mode. This is not what the administrator wants to do, as the script must be run only in console mode.

* D. `systemctl isolate multi-user.target systemctl isolate graphical.target sh script.sh`

This sequence will switch from graphical mode to console mode and then back to graphical mode, without running the script at all. This is not what the administrator wants to do, as the script must be run only in console mode.

References:

? `systemctl(1)` - Linux manual page

? How to switch between the CLI and GUI on a Linux server

? How to PROPERLY boot into single user mode in RHEL/CentOS 7/8

? Changing Systemd Boot Target in Linux

? Exit Desktop to Terminal in Ubuntu 19.10

NEW QUESTION 11

A systems administrator frequently connects to a remote host via SSH and a non-standard port. The systems administrator would like to avoid passing the port parameter on the command line every time. Which of the following files can be used to set a different port value for that host?

- A. `/etc/ssh/sshd_config`
- B. `/etc/ssh/moduli`
- C. `~/.ssh/config`
- D. `~/.ssh/authorized_keys`

Answer: C

Explanation:

The `~/.ssh/config` file can be used to set various options for SSH connections, including the port number, for specific hosts or groups of hosts. This file is located in the user's home directory and affects only the current user. The `/etc/ssh/sshd_config` file is used to configure the SSH server daemon, not the client. The `/etc/ssh/moduli` file contains parameters for Diffie-Hellman key exchange, not port settings.

The `~/.ssh/authorized_keys` file contains public keys for authentication, not port settings. References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 12: Secure Shell (SSH), page 414.

NEW QUESTION 12

A systems administrator needs to clone the partition `/dev/sdc1` to `/dev/sdd1`. Which of the following commands will accomplish this task?

- A. `tar -cvzf /dev/sdd1 /dev/sdc1`
- B. `rsync /dev/sdc1 /dev/sdd1`
- C. `dd if=/dev/sdc1 of=/dev/sdd1`
- D. `scp /dev/sdc1 /dev/sdd1`

Answer: C

Explanation:

The command `dd if=/dev/sdc1 of=/dev/sdd1` copies the data from the input file (if) `/dev/sdc1` to the output file (of) `/dev/sdd1`, byte by byte. This is the correct way to clone a partition. The other options are incorrect because they either compress the data (`tar -cvzf`), synchronize the files (`rsync`), or copy the files over a network (`scp`), which are not the same as cloning a partition. References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 10: Managing Storage, page 321.

NEW QUESTION 14

Rugged appliances are small appliances with ruggedized hardware and like Quantum Spark appliance they use which operating system?

- A. CentOS Linux
- B. Gaia embedded
- C. Gaia
- D. Red Hat Enterprise Linux version 5

Answer: B

Explanation:

Rugged appliances are small appliances with ruggedized hardware that use Gaia embedded as their operating system. Gaia embedded is a version of Gaia that is optimized for embedded devices such as Rugged appliances and Quantum Spark appliances. Gaia embedded supports features such as VPN, firewall, identity awareness, application control, URL filtering, and anti-bot. Gaia embedded does not use Centos Linux, Gaia, or Red Hat Enterprise Linux version 5 as their operating system. References: Check Point Rugged Appliance Datasheet, page 1.

NEW QUESTION 17

A Linux administrator wants to prevent the httpd web service from being started both manually and automatically on a server. Which of the following should the administrator use to accomplish this task?

- A. systemctl mask httpd
- B. systemctl disable httpd
- C. systemctl stop httpd
- D. systemctl reload httpd

Answer: A

Explanation:

The best command to use to prevent the httpd web service from being started both manually and automatically on a server is A. systemctl mask httpd. This command will create a symbolic link from the httpd service unit file to /dev/null, which will make the service impossible to start or enable. This is different from systemctl disable httpd, which will only prevent the service from starting automatically on boot, but not manually. The other commands are either not relevant or not sufficient for this task. For example:

? C. systemctl stop httpd will only stop the service if it is currently running, but it will not prevent it from being started again.

? D. systemctl reload httpd will only reload the configuration files of the service, but it will not stop or disable it.

NEW QUESTION 18

Which of the following directories is the mount point in a UEFI system?

- A. /sys/efi
- B. /boot/efi
- C. /efi
- D. /etc/efi

Answer: B

Explanation:

The /boot/efi directory is the mount point in a UEFI system. This directory contains the EFI System Partition (ESP), which stores boot loaders and other files required by UEFI firmware. The /sys/efi directory does not exist by default in Linux systems. The /efi directory does not exist by default in Linux systems. The /etc/efi directory does not exist by default in Linux systems. References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 11: Managing the Linux Boot Process, page 398.

NEW QUESTION 23

A systems administrator wants to be sure the sudo rules just added to /etc/sudoers are valid. Which of the following commands can be used for this task?

- A. visudo -c
- B. test -f /etc/sudoers
- C. sudo vi check
- D. cat /etc/sudoers | tee test

Answer: A

Explanation:

The command visudo -c can be used to check the validity of the sudo rules in the /etc/sudoers file. The visudo command is a tool for editing and validating the /etc/sudoers file, which defines the rules for the sudo command. The -c option checks the syntax and logic of the file and reports any errors or warnings. The command visudo - c will verify the sudo rules and help the administrator avoid any mistakes. This is the correct command to use for this task. The other options are incorrect because they either do not check the validity of the file (test, sudo, or cat) or do not exist (sudo vi check). References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 18: Securing Linux Systems, page 546.

NEW QUESTION 27

A Linux systems administrator is troubleshooting an I/O latency on a single CPU server. The administrator runs a top command and receives the following output: %Cpu(s): 0.2 us, 33.1 sy, 0.0 ni, 0.0 id, 52.4 wa, 0.0 hi, 0.2 si, 0.0 st

Which of the following is correct based on the output received from the exe-cuted command?

- A. The server's CPU is taking too long to process users' requests.
- B. The server's CPU shows a high idle-time value.
- C. The server's CPU is spending too much time waiting for data inputs.
- D. The server's CPU value for the time spent on system processes is low.

Answer: C

Explanation:

The server's CPU is spending too much time waiting for data inputs. This can be inferred from the output of the top command, which shows the percentage of CPU time spent in different states. The wa state stands for wait, and it indicates that the CPU is idle while waiting for an I/O operation to complete. In this case, the wa state is 52.4%, which means that more than half of the CPU time is wasted on waiting for data inputs. This can cause a high I/O latency and affect the performance of the server.

The other options are not correct based on the output received from the executed command. The server's CPU is not taking too long to process users' requests, because the us state, which stands for user, is only 0.2%, which means that the CPU is barely used by user processes. The server's CPU does not show a high idle-time value, because the id state, which stands for idle, is 0.0%, which means that the CPU is not idle at all. The server's CPU value for the time spent on system processes is not low, because the sy state, which stands for system, is 33.1%, which means that the CPU is heavily used by system processes. References: How to Use the Linux top Command (and Understand Its Output); [Understanding Linux CPU Load - when should you be worried?]

NEW QUESTION 31

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`

Answer: C

Explanation:

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]

NEW QUESTION 36

A cloud engineer needs to change the secure remote login port from 22 to 49000. Which of the following files should the engineer modify to change the port number to the desired value?

- A. `/etc/host.conf`
- B. `/etc/hostname`
- C. `/etc/services`
- D. `/etc/ssh/sshd_config`

Answer: D

Explanation:

The file `/etc/ssh/sshd_config` contains the configuration settings for the SSH daemon, which handles the secure remote login. To change the port number, the engineer should edit this file and modify the line that says Port 22 to Port 49000. The other files are not related to the SSH service. References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 13: Managing Network Services, page 411.

NEW QUESTION 39

The group owner of the `/ home/ test` directory would like to preserve all group permissions on files created in the directory. Which of the following commands should the group owner execute?

- A. `chmod g+s /home/test`
- B. `chgrp test /home/test`
- C. `chmod 777 /home/test`
- D. `chown —hR test /home/test`

Answer: A

Explanation:

The correct answer is A. `chmod g+s /home/test`

This command will set the `setgid` bit on the `/home/test` directory, which means that any file or subdirectory created in the directory will inherit the group ownership of the directory. This way, the group permissions on files created in the directory will be preserved. The `chmod` command is used to change the permissions of files and directories. The `g+s` option is used to set the `setgid` bit for the group.

The other options are incorrect because:

* B. `chgrp test /home/test`

This command will change the group ownership of the `/home/test` directory to `test`, but it will not affect the group ownership of files created in the directory. The `chgrp` command is used to change the group of files and directories. The `test /home/test` arguments are used to specify the new group and the target directory.

* C. `chmod 777 /home/test`

This command will give read, write, and execute permissions to everyone (owner, group, and others) on the `/home/test` directory, but it will not affect the group ownership or permissions of files created in the directory. The `chmod` command is used to change the permissions of files and directories. The `777` argument is an octal number that represents the permissions in binary form.

* D. `chown -hR test /home/test`

This command will change the owner and group of the `/home/test` directory and all its contents recursively to `test`, but it will not preserve the original group permissions on files created in the directory. The `chown` command is used to change the owner and group of files and directories. The `-hR` option is used to affect symbolic links and operate on all files and directories recursively. The `test /home/test` arguments are used to specify the new owner and group and the target directory.

References:

? How to Set File Permissions Using `chmod`

? How to Use `Chmod` Command in Linux with Examples

? How to Use `Chown` Command in Linux with Examples

? [How to Use `Chgrp` Command in Linux with Examples]

NEW QUESTION 42

A DevOps engineer needs to download a Git repository from <https://git.company.com/admin/project.git>. Which of the following commands will achieve this goal?

- A. `git clone https://git.company.com/admin/project.git`
- B. `git checkout https://git.company.com/admin/project.git`
- C. `git pull https://git.company.com/admin/project.git`
- D. `git branch https://git.company.com/admin/project.git`

Answer: A

Explanation:

The command `git clone https://git.company.com/admin/project.git` will achieve the goal of downloading a Git repository from the given URL. The `git` command is a tool for managing version control systems. The `clone` option creates a copy of an existing repository. The URL specifies the location of the repository to clone, in this case <https://git.company.com/admin/project.git>. The command `git clone https://git.company.com/admin/project.git` will download the repository and create a directory named `project` in the current working directory. This is the correct command to use to accomplish the goal. The other options are incorrect because they either do not download the repository (`git checkout`, `git pull`, or `git branch`) or do not use the correct syntax (`git checkout https://git.company.com/admin/project.git` instead of `git checkout -b project https://git.company.com/admin/project.git` or `git branch https://git.company.com/admin/project.git` instead of `git branch project https://git.company.com/admin/project.git`). References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 19: Managing Cloud and Virtualization Technologies, page 571.

NEW QUESTION 44

While inspecting a recently compromised Linux system, the administrator identified a number of processes that should not have been running:

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
5545	joe	30	-10	5465	56465	8254	R	0.5	1.5	00:35.3	upload.sh
2567	joe	30	-10	6433	75544	9453	R	0.7	1.8	00:25.1	upload_passwd.sh
8634	joe	30	-10	3584	74537	6435	R	0.3	1.1	00:17.6	uploadpw.sh
4846	joe	30	-10	6426	63234	9683	R	0.8	1.9	00:22.2	upload_shadow.sh

Which of the following commands should the administrator use to terminate all of the identified processes?

- A. `pkill -9 -f "upload*.sh"`
- B. `kill -9 "upload*.sh"`
- C. `killall -9 -upload*.sh`
- D. `skill -9 "upload*.sh"`

Answer: A

Explanation:

The `pkill -9 -f "upload*.sh"` command will terminate all of the identified processes. This command will send a SIGKILL signal (-9) to all processes whose full command line matches the pattern "upload*.sh" (-f). This signal will force the processes to terminate immediately without giving them a chance to clean up or save their state. The `kill -9 "upload*.sh"` command is invalid, as `kill` requires a process ID (PID), not a pattern. The `killall -9 "upload*.sh"` command is incorrect, as `killall` requires an exact process name, not a pattern. The `skill -9 "upload*.sh"` command is incorrect, as `skill` requires a username or a session ID (SID), not a pattern. References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 15: Managing Memory and Process Execution, page 470.

NEW QUESTION 45

Users report that connections to a MariaDB service are being closed unexpectedly. A systems administrator troubleshoots the issue and finds the following message in `/var/log/messages`:

```
dbserver kernel: out of Memory: Killed process 1234 (mysqld).
```

Which of the following is causing the connection issue?

- A. The process `mysqld` is using too many semaphores.
- B. The server is running out of file descriptors.
- C. Something is starving the server resources.
- D. The amount of RAM allocated to the server is too high.

Answer: B

Explanation:

The message in `/var/log/messages` indicates that the server is running out of file descriptors. A file descriptor is a non-negative integer identifier for an open file in Linux. Each process has a table of open file descriptors where a new entry is appended upon opening a new file. There is a limit on how many file descriptors a process can open at a time, which depends on the system configuration and the user privileges. If a process tries to open more files than the limit, it will fail with an error message like "Too many open files". This could cause connections to be closed unexpectedly or other problems with the application. The other options are not correct causes for the connection issue. The process `mysqld` is not using too many semaphores, which are synchronization mechanisms for processes that share resources. Semaphores are not related to file descriptors or open files. Something is not starving the server resources, which could mean high CPU usage, memory pressure, disk I/O, network congestion, or other factors that affect performance. These could cause slowdowns or timeouts, but not file descriptor exhaustion. The amount of RAM allocated to the server is not too high, which could cause swapping or paging if it exceeds the physical memory available. This could also affect performance, but not file descriptor availability. References: File Descriptor Requirements (Linux Systems); Limits on the Number of Linux File Descriptors

NEW QUESTION 46

A developer has been unable to remove a particular data folder that a team no longer uses. The developer escalated the issue to the systems administrator. The following output was received:


```
# rmdir data/
rmdir: failed to remove 'data/': Operation not permitted
# rm -rf data/
rm: cannot remove 'data': Operation not permitted
# mv data/ mydata
mv: cannot move 'data/' to 'mydata': Operation not permitted
# cd data/
# cat > test.txt
bash: test.txt: Permission denied
```

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

- A. chgrp -R 755 data/
- B. chmod -R 777 data/
- C. chattr -R -i data/
- D. chown -R data/

Answer: C

Explanation:

The command that can be used to resolve the issue of being unable to remove a particular data folder is `chattr -R -i data/`. This command will use the `chattr` utility to change file attributes on a Linux file system. The `-R` option means that `chattr` will recursively change attributes of directories and their contents. The `-i` option means that `chattr` will remove (unset) the immutable attribute from files or directories. When a file or directory has the immutable attribute set, it cannot be modified, deleted, or renamed.

The other options are not correct commands for resolving this issue. The `chgrp -R 755 data/` command will change the group ownership of `data/` and its contents recursively to 755, which is not a valid group name. The `chgrp` command is used to change group ownership of files or directories. The `chmod -R 777 data/` command will change the file mode bits of `data/` and its contents recursively to 777, which means that everyone can read, write, and execute them. However, this will not remove the immutable attribute, which prevents deletion or modification regardless of permissions. The `chmod` command is used to change file mode bits of files or directories. The `chown -R data/` command is incomplete and will produce an error. The `chown` command is used to change the user and/or group ownership of files or directories, but it requires at least one argument besides the file name. References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 7: Managing Disk Storage; `chattr(1)` - Linux manual page; `chgrp(1)` - Linux manual page; `chmod(1)` - Linux manual page; `chown(1)` - Linux manual page

NEW QUESTION 49

A junior administrator is trying to set up a passwordless SSH connection to one of the servers. The administrator follows the instructions and puts the key in the `authorized_key` file at the server, but the administrator is still asked to provide a password during the connection.

Given the following output:

```
junior@server:~$ ls -lh .ssh/auth*
-rw----- 1 junior junior 566 sep 13 20:56 .ssh/authorized_key
```

Which of the following commands would resolve the issue and allow an SSH connection to be established without a password?

- A. `restorecon -rv .ssh/authorized_key`
- B. `mv .ssh/authorized_key .ssh/authorized_keys`
- C. `systemctl restart sshd.service`
- D. `chmod 600 mv .ssh/authorized_key`

Answer: B

Explanation:

The command `mv .ssh/authorized_key .ssh/authorized_keys` will resolve the issue and allow an SSH connection to be established without a password. The issue is caused by the incorrect file name of the authorized key file on the server. The file should be named `authorized_keys`, not `authorized_key`. The `mv` command will rename the file and fix the issue. The other options are incorrect because they either do not affect the file name (`restorecon` or `chmod`) or do not restart the SSH service (`systemctl`). References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 13: Managing Network Services, page 410.

NEW QUESTION 53

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`

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.

NEW QUESTION 54

Users have been unable to save documents to /home/tmp/temp and have been receiving the following error:

Path not found

A junior technician checks the locations and sees that /home/tmp/tempa was accidentally created instead of /home/tmp/temp. Which of the following commands should the technician use to fix this issue?

- A. cp /home/tmp/tempa /home/tmp/temp
- B. mv /home/tmp/tempa /home/tmp/temp
- C. cd /temp/tmp/tempa
- D. ls /home/tmp/tempa

Answer: B

Explanation:

The mv /home/tmp/tempa /home/tmp/temp command will fix the issue of the misnamed directory. This command will rename the directory /home/tmp/tempa to /home/tmp/temp, which is the expected path for users to save their documents. The cp /home/tmp/tempa /home/tmp/temp command will not fix the issue, as it will copy the contents of /home/tmp/tempa to a new file named /home/tmp/temp, not a directory. The cd /temp/tmp/tempa command will not fix the issue, as it will change the current working directory to /temp/tmp/tempa, which does not exist. The ls /home/tmp/tempa command will not fix the issue, as it will list the contents of /home/tmp/tempa, not rename it. References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 12: Managing Files and Directories, page 413.

NEW QUESTION 58

A Linux administrator needs to create an image named sda.img from the sda disk and store it in the /tmp directory. Which of the following commands should be used to accomplish this task?

- A. dd of=/dev/sda if=/tmp/sda.img
- B. dd if=/dev/sda of=/tmp/sda.img
- C. dd --if=/dev/sda --of=/tmp/sda.img
- D. dd --of=/dev/sda --if=/tmp/sda.img

Answer: B

Explanation:

The command dd if=/dev/sda of=/tmp/sda.img should be used to create an image named sda.img from the sda disk and store it in the /tmp directory. The dd command is a tool for copying and converting data on Linux systems. The if option specifies the input file or device, in this case /dev/sda, which is the disk device. The of option specifies the output file or device, in this case /tmp/sda.img, which is the image file. The command dd if=/dev/sda of=/tmp/sda.img will copy the entire disk data from /dev/sda to /tmp/sda.img and create an image file. This is the correct command to use to accomplish the task. The other options are incorrect because they either use the wrong options (--if or --of instead of if or of) or swap the input and output (dd of=/dev/sda if=/tmp/sda.img or dd --of=/dev/sda --if=/tmp/sda.img). References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 10: Managing Storage, page 323.

NEW QUESTION 60

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

Answer: D

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 61

Users in the human resources department are trying to access files in a newly created directory. Which of the following commands will allow the users access to the files?

- A. `chattr`
- B. `chgrp`
- C. `chage`
- D. `chcon`

Answer: B

Explanation:

The `chgrp` command is used to change the group ownership of files and directories. By using this command, the administrator can assign the files in the newly created directory to the human resources group, which will allow the users in that group to access them. The other commands are not relevant for this task. For example:

? `chattr` is used to change the file attributes, such as making them immutable or append-only¹.

? `chage` is used to change the password expiration information for a user account².

? `chcon` is used to change the security context of files and directories, which is related to SELinux³.

References:

? The CompTIA Linux+ Certification Exam Objectives mention that the candidate should be able to “manage file and directory ownership and permissions” as part of the Hardware and System Configuration domain⁴.

? The web search result 2 explains how to use the `chgrp` command with examples.

? The web search result 3 compares the `chmod` and `chgrp` commands and their effects on file permissions.

NEW QUESTION 63

Which of the following actions are considered good security practices when hardening a Linux server? (Select two).

- A. Renaming the root account to something else
- B. Removing unnecessary packages
- C. Changing the default shell to `/bin/csh`
- D. Disabling public key authentication
- E. Disabling the SSH root login possibility
- F. Changing the permissions on the root filesystem to 600

Answer: BE

Explanation:

Some good security practices when hardening a Linux server are:

? Removing unnecessary packages (B) to reduce the attack surface and eliminate potential vulnerabilities

? Disabling the SSH root login possibility (E) to prevent unauthorized access and brute-force attacks on the root account References:

? [CompTIA Linux+ Study Guide], Chapter 9: Securing Linux, Section: Hardening Linux

? [How to Harden Your Linux Server]

NEW QUESTION 68

A systems administrator is receiving tickets from users who cannot reach the application app that should be listening on port 9443/tcp on a Linux server. To troubleshoot the issue, the systems administrator runs `netstat` and receives the following output:

```
# netstat -anp | grep appd | grep -w LISTEN
tcp 0 0 127.0.0.1:9443 0.0.0.0:* LISTEN 1234/appd
```

Based on the information above, which of the following is causing the issue?

- A. The IP address 0.0.0.0 is not valid.
- B. The application is listening on the loopback interface.
- C. The application is listening on port 1234.
- D. The application is not running.

Answer: B

Explanation:

The server is in a "Listen" state on port 9943 using its loopback address. The "1234" is a process-id

The cause of the issue is that the application is listening on the loopback interface. The loopback interface is a virtual network interface that is used for internal communication within the system. The loopback interface has the IP address 127.0.0.1, which is also known as localhost. The `netstat` output shows that the application is listening on port 9443 using the IP address 127.0.0.1. This means that the application can only accept connections from the same system, not from other systems on the network. This can prevent the users from reaching the application and cause the issue. The administrator should configure the application to listen on the IP address 0.0.0.0, which means all available interfaces, or on the specific IP address of the system that is reachable from the network. This will allow the application to accept connections from other systems and resolve the issue. The cause of the issue is that the application is listening on the loopback interface. This is the correct answer to the question. The other options are incorrect because they are not supported by the outputs. The IP address 0.0.0.0 is valid and means all interfaces, the application is not listening on port 1234, and the application is running as shown by the process ID 1234. References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 12: Managing Network Connections, page 383.

NEW QUESTION 71

An administrator is trying to diagnose a performance issue and is reviewing the following output:


```
avg-cpu:  %user  %nice  %system  %iowait  %steal   %idle
           2.00   0.00   3.00    32.00    0.00   63.00
```

Device	tps	kB_read/s	kB_wrtn/s	kB_read	kB_wrtn
sdb	345.00	0.02	0.04	4739073123	23849523
sdb1	345.00	32102.03	12203.01	4739073123	23849523

System Properties: CPU: 4 vCPU

Memory: 40GB

Disk maximum IOPS: 690

Disk maximum throughput: 44Mbps | 44000Kbps

Based on the above output, which of the following BEST describes the root cause?

- A. The system has reached its maximum IOPS, causing the system to be slow.
- B. The system has reached its maximum permitted throughput, therefore iowait is increasing.
- C. The system is mostly idle, therefore the iowait is high.
- D. The system has a partitioned disk, which causes the IOPS to be doubled.

Answer: B

Explanation:

The system has reached its maximum permitted throughput, therefore iowait is increasing. The output of `iostat -x` shows that the device `sda` has an average throughput of 44.01 MB/s, which is equal to the disk maximum throughput of 44 Mbps. The output also shows that the device `sda` has an average iowait of 99.99%, which means that the CPU is waiting for the disk to complete the I/O requests. This indicates that the disk is the bottleneck and the system is slow due to the high iowait. The other options are incorrect because they are not supported by the outputs. The system has not reached its maximum IOPS, as the device `sda` has an average IOPS of 563.50, which is lower than the disk maximum IOPS of 690. The system is not mostly idle, as the output of `top` shows that the CPU is 100% busy. The system does not have a partitioned disk, as the output of `lsblk` shows that the device `sda` has only one partition `sda1`. References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 17: Optimizing Linux Systems, pages 513-514.

NEW QUESTION 75

A systems administrator needs to check if the service `systemd-resolved.service` is running without any errors. Which of the following commands will show this information?

- A. `systemctl status systemd-resolved.service`
- B. `systemctl enable systemd-resolved.service`
- C. `systemctl mask systemd-resolved.service`
- D. `systemctl show systemd-resolved.service`

Answer: A

Explanation:

The command `systemctl status systemd-resolved.service` will show the information about the service `systemd-resolved.service`. The `systemctl` command is a tool for managing system services and units. The `status` option displays the current status of a unit, such as active, inactive, or failed. The output also shows the unit description, loaded configuration, process ID, memory usage, and recent log messages. This command will show if the service `systemd-resolved.service` is running without any errors. This is the correct command to use to accomplish the task. The other options are incorrect because they either perform different actions (enable, mask, or show) or do not show the status of the service (`systemctl show systemd-resolved.service` only shows the properties of the service, not the status). References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 14: Managing Processes and Scheduling Tasks, page 427.

NEW QUESTION 77

A Linux administrator is adding a new configuration file to a Git repository. Which of the following describes the correct order of Git commands to accomplish the task successfully?

- A. `pull -> push -> add -> checkout`
- B. `pull -> add -> commit -> push`
- C. `checkout -> push -> add -> pull`
- D. `pull -> add -> push -> commit`

Answer: B

Explanation:

The correct order of Git commands to add a new configuration file to a Git repository is `pull -> add -> commit -> push`. The `pull` command will fetch and merge the changes from the remote repository to the local repository, ensuring that the local repository is up to date. The `add` command will stage the new configuration file for the next commit, marking it as a new file to be tracked by Git. The `commit` command will create a new snapshot of the project state with the new configuration file and a descriptive message. The `push` command will publish the commit to the remote repository, updating the remote branch with the new configuration file. The `pull -> push -> add -> checkout` order is incorrect, as it will not create a commit for the new configuration file, and it will switch to a different branch without pushing the changes. The `checkout -> push -> add -> pull` order is incorrect, as it will switch to a different branch before adding the new configuration file, and it will overwrite the local changes with the remote changes without creating a commit. The `pull -> add -> push -> commit` order is incorrect, as it will not create a commit before pushing the changes, and it will create a commit that is not synchronized with the remote branch. References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 20: Writing and Executing Bash Shell Scripts, page 579.

NEW QUESTION 80

A systems administrator is adding a Linux-based server and removing a Windows-based server from a cloud-based environment. The changes need to be validated before they are applied to the cloud-based environment. Which of the following tools should be used to meet this requirement?

- A. Ansible
- B. git clone
- C. git pull
- D. terraform plan

Answer: D

Explanation:

Terraform is a tool for building, changing, and managing infrastructure as code in a cloud-based environment. Terraform uses configuration files to describe the desired state of the infrastructure and applies changes accordingly. Terraform supports various cloud providers, such as AWS, Azure, Google Cloud Platform, and more.

To validate changes before they are applied to the cloud-based environment, the administrator can use the terraform plan command. This command will compare the current state of the infrastructure with the desired state defined in the configuration files and show what actions will be performed to achieve the desired state. This command will not make any changes to the infrastructure but only show a plan of changes. The statement D is correct.

The statements A, B, and C are incorrect because they do not validate changes before they are applied to the cloud-based environment. Ansible is another tool for automating infrastructure management, but it does not have a plan command. Git clone and git pull are commands for working with git repositories, which are used for version control of code. References: [How to Use Terraform to Manage Cloud Infrastructure]

NEW QUESTION 82

A Linux administrator needs to transfer a local file named accounts . pdf to a remote / tmp directory of a server with the IP address 10.10.10.80. Which of the following commands needs to be executed to transfer this file?

- A. rsync user@10.10.10.80: /tmp accounts.pdf
- B. scp accounts.pdf user@10.10.10.80:/tmp
- C. cp user@10.10.10. 80: /tmp accounts.pdf
- D. ssh accounts.pdf user@10.10.10.80: /tmp

Answer: B

Explanation:

The best command to use to transfer the local file accounts.pdf to the remote /tmp directory of the server with the IP address 10.10.10.80 is B. scp accounts.pdf user@10.10.10.80:/tmp. This command will use the secure copy protocol (scp) to copy the file from the local machine to the remote server over SSH. The command requires the username and password of the user on the remote server, as well as the full path of the destination directory.

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

? A. rsync user@10.10.10.80:/tmp accounts.pdf will try to use the rsync command to synchronize files between the local and remote machines, but it has the wrong syntax and order of arguments. The source should come before the destination, and a colon (:) should separate the remote host and path.

? C. cp user@10.10.10.80:/tmp accounts.pdf will try to use the cp command to copy files, but it does not work over SSH and it has the wrong syntax and order of arguments. The source should come before the destination, and a colon (:) should separate the remote host and path.

? D. ssh accounts.pdf user@10.10.10.80:/tmp will try to use the ssh command to log into the remote server, but it has the wrong syntax and arguments. The username should come before the remote host, and a file name is not a valid argument for ssh.

NEW QUESTION 83

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 following 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 /home/user/scrip
- E. sh

Answer: A

Explanation:

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]

NEW QUESTION 84

Which of the following will prevent non-root SSH access to a Linux server?

- A. Creating the /etc/nologin file
- B. Creating the /etc/nologin.allow file containing only a single line root
- C. Creating the /etc/nologin/login.deny file containing a single line +all
- D. Ensuring that /etc/pam.d/sshd includes account sufficient pam_nologin.so

Answer: A

Explanation:

This file prevents any non-root user from logging in to the system, regardless of the authentication method. The contents of the file are displayed to the user before the login is terminated. This can be useful for system maintenance or security reasons¹².

References: 1: Creating the /etc/nologin File - Oracle 2: How to Restrict Log In Capabilities of Users on Ubuntu

NEW QUESTION 89

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.

Answer: A

Explanation:

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

NEW QUESTION 94

Due to low disk space, a Linux administrator finding and removing all log files that were modified more than 180 days ago. Which of the following commands will accomplish this task?

- A. `find /var/log -type d -mtime +180 -print -exec rm {} \;`
- B. `find /var/log -type f -modified +180 -rm`
- C. `find /var/log -type f -mtime +180 -exec rm {} \`
- D. `find /var/log -type c -atime +180 -remove`

Answer: C

Explanation:

The command that will accomplish the task of finding and removing all log files that were modified more than 180 days ago is `find /var/log -type f -mtime +180 -exec rm {} ;`. This command will use `find` to search for files (-type f) under /var/log directory that have a modification time (-mtime) older than 180 days (+180). For each matching file, it will execute (-exec) the `rm` command to delete it, passing the file name as an argument ({}). The command will end with a semicolon (;), which is escaped with a backslash to prevent shell interpretation.

The other options are not correct commands for accomplishing the task. The `find /var/log -type d -mtime +180 -print -exec rm {} ;` command will search for directories (-type d) instead of files, and print their names (-print) before deleting them. This is not what the task requires. The `find /var/log -type f -modified +180 -rm` command is invalid because there is no such option as -modified or -rm for find. The correct options are -mtime and -delete, respectively. The `find /var/log -type c -atime +180 -remove` command is also invalid because there is no such option as -remove for find. Moreover, it will search for character special files (-type c) instead of regular files, and use access time (-atime) instead of modification time. References: `find(1)` - Linux manual page; Find and delete files older than n days in Linux

NEW QUESTION 95

Users are unable to create new files on the company's FTP server, and an administrator is troubleshooting the issue. The administrator runs the following commands:

```
# df -h /ftpusers/
```

Filesystem	Size	Used	Avail	Use%	Mounted on
/dev/sda4	150G	40G	109G	26%	/ftpusers

```
# df -i /ftpusers/
```

Filesystem	Inodes	Iused	Ifree	Iuse%	Mounted on
/dev/sda4	34567	34567	0	100%	/ftpusers

Which of the following is the cause of the issue based on the output above?

- A. The users do not have the correct permissions to create files on the FTP server.
- B. The ftpusers filesystem does not have enough space.
- C. The inodes is at full capacity and would affect file creation for users.
- D. ftpusers is mounted as read only.

Answer: C

Explanation:

The cause of the issue based on the output above is C. The inodes is at full capacity and would affect file creation for users.

An inode is a data structure that stores information about a file or directory, such as its name, size, permissions, owner, timestamps, and location on the disk. Each file or directory has a unique inode number that identifies it. The number of inodes on a filesystem is fixed when the filesystem is created, and it determines how

many files and directories can be created on that filesystem. If the inodes are exhausted, no new files or directories can be created, even if there is enough disk space available.

The output for the second command shows that the /ftpusers/ filesystem has 0% of inodes available, which means that all the inodes have been used up. This would prevent users from creating new files on the FTP server. The administrator should either delete some unused files or directories to free up some inodes, or resize the filesystem to increase the number of inodes.

The other options are incorrect because:

- * A. The users do not have the correct permissions to create files on the FTP server.
This is not true, because the output for the first command shows that the /ftpusers/ filesystem has 26% of disk space available, which means that there is enough space for users to create files. The permissions of the files and directories are not shown in the output, but they are not relevant to the issue of inode exhaustion.
- * B. The ftpusers filesystem does not have enough space.
This is not true, because the output for the first command shows that the /ftpusers/ filesystem has 26% of disk space available, which means that there is enough space for users to create files. The issue is not related to disk space, but to inode capacity.
- * D. ftpusers is mounted as read only.
This is not true, because the output for the first command does not show any indication that the /ftpusers/ filesystem is mounted as read only. If it was, it would have an (ro) flag next to the mounted on column. A read only filesystem would prevent users from creating or modifying files on the FTP server, but it would not affect the inode usage.

NEW QUESTION 97

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 -l | egrep '(^http_port_t|6379) '
http_port_t tcp 80, 81, 443, 488, 8008, 8009, 8443, 9000

# curl http://localhost/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

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.

NEW QUESTION 99

The development team created a new branch with code changes that a Linux administrator needs to pull from the remote repository. When the administrator looks for the branch in Git, the branch in question is not visible. Which of the following commands should the Linux administrator run to refresh the branch information?

- A. git fetch
- B. git checkout
- C. git clone
- D. git branch

Answer: A

Explanation:

The `git fetch` command downloads commits, files, and refs from a remote repository into the local one. It also updates the remote-tracking branches, which are references to the state of the remote branches. By running `git fetch`, the administrator can see the new branch created by the development team and then use `git checkout` to switch to it. References: 1: Git - git-fetch Documentation 2: Git Fetch | Atlassian Git Tutorial

NEW QUESTION 102

A new Linux systems administrator just generated a pair of SSH keys that should allow connection to the servers. Which of the following commands can be used to copy a key file to remote servers? (Choose two.)

- A. wget
- B. ssh-keygen
- C. ssh-keyscan
- D. ssh-copy-id
- E. ftpd
- F. scp

Answer: DF

Explanation:

The commands `ssh-copy-id` and `scp` can be used to copy a key file to remote servers. The command `ssh-copy-id` copies the public key to the `authorized_keys` file on the remote server, which allows the user to log in without a password. The command `scp` copies files securely over SSH, which can be used to transfer the key file to any location on the remote server. The other options are incorrect because they are not related to copying key files. The command `wget` downloads files from the web, the command `ssh-keygen` generates key pairs, the command `ssh-keyscan` collects public keys from remote hosts, and the command `ftpd` is a FTP

server daemon. References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 13: Managing Network Services, pages 408-410.

NEW QUESTION 106

A Linux administrator needs to redirect all HTTP traffic temporarily to the new proxy server 192.0.2.25 on port 3128. Which of the following commands will accomplish this task?

- A. `iptables -t nat -D PREROUTING -p tcp --sport 80 -j DNAT - -to-destination 192.0.2.25:3128`
- B. `iptables -t nat -A PREROUTING -p top --dport 81 -j DNAT --to-destination 192.0.2.25:3129`
- C. `iptables -t nat -I PREROUTING -p top --sport 80 -j DNAT --to-destination 192.0.2.25:3129`
- D. `iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT --to-destination 192.0.2.25:3128`

Answer: D

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.

NEW QUESTION 111

A systems administrator wants to check for running containers. Which of the following commands can be used to show this information?

- A. `docker pull`
- B. `docker stats`
- C. `docker ps`
- D. `docker list`

Answer: C

Explanation:

The command that can be used to check for running containers is `docker ps`. The `docker ps` command can list all the containers that are currently running on the system. To show all the containers, including those that are stopped, the administrator can use `docker ps -a`

References:

? [CompTIA Linux+ Study Guide], Chapter 11: Working with Containers, Section: Managing Containers with Docker

? [Docker PS Command with Examples]

NEW QUESTION 112

A Linux administrator is creating a primary partition on the replacement hard drive for an application server. Which of the following commands should the administrator issue to verify the device name of this partition?

- A. `sudo fdisk /dev/sda`
- B. `sudo fdisk -s /dev/sda`
- C. `sudo fdisk -l`
- D. `sudo fdisk -h`

Answer: C

Explanation:

The command `sudo fdisk -l` should be issued to verify the device name of the partition. The `sudo` command allows the administrator to run commands as the superuser or another user. The `fdisk` command is a tool for manipulating disk partitions on Linux systems. The `-l` option lists the partitions on all disks or a specific disk. The command `sudo fdisk -l` will show the device names, sizes, types, and other information of the partitions on all disks. The administrator can identify the device name of the partition by looking at the output. This is the correct command to use to accomplish the task. The other options are incorrect because they either do not list the partitions (`sudo fdisk /dev/sda` or `sudo fdisk -h`) or do not exist (`sudo fdisk -s /dev/sda`). References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 10: Managing Storage, page 317.

NEW QUESTION 115

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`

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

NEW QUESTION 118

A Linux administrator found many containers in an exited state. Which of the following commands will allow the administrator to clean up the containers in an exited state?

- A. docker rm --all
- B. docker rm \$(docker ps -aq)
- C. docker images prune *
- D. docker rm --state exited

Answer: B

Explanation:

The command `docker rm $(docker ps -aq)` will allow the administrator to clean up the containers in an exited state. The docker command is a tool for managing Docker containers on Linux systems. Docker containers are isolated and lightweight environments that can run applications and services without affecting the host system. Docker uses images to create containers, which are files that contain the code, libraries, dependencies, and configuration of the applications and services. The rm option removes one or more containers. The `$(docker ps -aq)` is a command substitution that executes the command inside the parentheses and replaces it with the output. The `docker ps -aq` command lists all the containers, including the ones in an exited state, and shows only their IDs. The `docker rm $(docker ps -aq)` command will remove all the containers, including the ones in an exited state, by passing their IDs to the rm option. This will allow the administrator to clean up the containers in an exited state. This is the correct command to use to accomplish the task. The other options are incorrect because they either do not exist (`docker rm --all` or `docker rm --state exited`) or do not remove the containers (`docker images prune *`). References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 19: Managing Cloud and Virtualization Technologies, page 571.

NEW QUESTION 123

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 | xargs grep -ln denied`
- B. `find . -type f -print | xargs grep -nv denied`
- C. `find . -type f -print | xargs grep -wL denied`
- D. `find . -type f -print | xargs grep -li denied`

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.

NEW QUESTION 126

An administrator would like to list all current containers, regardless of their running state. Which of the following commands would allow the administrator to accomplish this task?

- A. `docker ps -a`
- B. `docker list`
- C. `docker image ls`
- D. `docker inspect image`

Answer: A

Explanation:

The best command to use to list all current containers, regardless of their running state, is A. `docker ps -a`. This command will show all containers, both running and stopped, with details such as container ID, image name, status, and ports. The other commands are either invalid or not relevant for this task. For example:

- ? B. `docker list` is not a valid command. There is no subcommand named list in docker.
- ? C. `docker image ls` will list all the images available on the local system, not the containers.
- ? D. `docker inspect image` will show detailed information about a specific image, not all the containers.

NEW QUESTION 131

A Linux administrator recently downloaded a software package that is currently in a compressed file. Which of the following commands will extract the files?

- A. `unzip -v`
- B. `bzip2 -z`

- C. gzip
- D. funzip

Answer: C

Explanation:

The command gzip can extract files that are compressed with the gzip format, which has the extension .gz. This is the correct command to use for the software package. The other options are incorrect because they either compress files (bzip2 -z), unzip files that are compressed with the zip format (unzip -v or funzip), or have the wrong options (-v or -z instead of -d). References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 11: Managing Files and Directories, page 353.

NEW QUESTION 133

An administrator accidentally deleted the /boot/vmlinuz file and must resolve the issue before the server is rebooted. Which of the following commands should the administrator use to identify the correct version of this file?

- A. rpm -qa | grep kernel; uname -a
- B. yum -y update; shutdown -r now
- C. cat /etc/centos-release; rpm -Uvh --nodeps
- D. telinit 1; restorecon -Rv /boot

Answer: A

Explanation:

The command rpm -qa | grep kernel lists all the installed kernel packages, and the command uname -a displays the current kernel version. These commands can help the administrator identify the correct version of the /boot/vmlinuz file, which is the kernel image file. The other options are not relevant or helpful for this task. References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 8: Managing the Linux Boot Process, page 267.

NEW QUESTION 136

A systems administrator needs to remove a disk from a Linux server. The disk size is 500G, and it is the only one that size on that machine. Which of the following commands can the administrator use to find the corresponding device name?

- A. fdisk -V
- B. partprobe -a
- C. lsusb -t
- D. lsscsi -s

Answer: D

Explanation:

The lsscsi command can list the SCSI devices on the system, along with their size and device name. The -s option shows the size of each device. The administrator can look for the device that has a size of 500G and note its device name. See lsscsi(8) - Linux man page and How to check Disk Interface Types in Linux. References1: <https://linux.die.net/man/8/lsscsi>2: <https://www.golinuxcloud.com/check-disk-type-linux/>

NEW QUESTION 139

An administrator needs to get network information from a group of statically assigned workstations before they are reconnected to the network. Which of the following should the administrator use to obtain this information?

- A. ip show
- B. ifcfg —a
- C. ifcfg —s
- D. i fname —s

Answer: B

Explanation:

The ifcfg command is used to configure network interfaces on Linux systems. The -a option displays information about all network interfaces, including their IP addresses, netmasks, gateways, and other parameters. This command can help the administrator obtain the network information from the statically assigned workstations before they are reconnected to the network. References: [Linux Networking: ifcfg Command With Examples]

NEW QUESTION 143

An administrator transferred a key for SSH authentication to a home directory on a remote server. The key file was moved to .ssh/authorized_keys location in order to establish SSH connection without a password. However, the SSH command still asked for the password. Given the following output:

```
[admin@linux ~]$ -ls -lhZ .ssh/auth*  
-rw-r--r--. admin unconfined_u:object_r:user_home_t:s0 .ssh/authorized_keys
```

Which of the following commands would resolve the issue?

- A. restorecon .ssh/authorized_keys
- B. ssh_keygen -t rsa -o .ssh/authorized_keys
- C. chown root:root .ssh/authorized_keys
- D. chmod 600 .ssh/authorized_keys

Answer: D

Explanation:

The command that would resolve the issue is chmod 600 .ssh/authorized_keys. This command will change the permissions of the .ssh/authorized_keys file to 600, which means that only the owner of the file can read and write it. This is necessary for SSH key authentication to work properly, as SSH will refuse to use a

key file that is accessible by other users or groups for security reasons. The output of `ls -l` shows that currently the `.ssh/authorized_keys` file has permissions of 664, which means that both the owner and group can read and write it, and others can read it. The other options are not correct commands for resolving the issue. The `restorecon .ssh/authorized_keys` command will restore the default SELinux security context for the `.ssh/authorized_keys` file, but this will not change its permissions or ownership. The `ssh_keygen -t rsa -o .ssh/authorized_keys` command is invalid because `ssh_keygen` is not a valid command (the correct command is `ssh-keygen`), and the `-o` option is used to specify a new output format for the key file, not the output file name. The `chown root:root .ssh/authorized_keys` command will change the owner and group of the `.ssh/authorized_keys` file to root, but this will not change its permissions or make it accessible by the user who wants to log in with SSH key authentication. References: How to Use Public Key Authentication with SSH; `chmod(1)` - Linux manual page

NEW QUESTION 145

Users have reported that the interactive sessions were lost on a Linux server. A Linux administrator verifies the server was switched to `rescue.target` mode for maintenance. Which of the following commands will restore the server to its usual target?

- A. `telinit 0`
- B. `systemctl reboot`
- C. `systemctl get-default`
- D. `systemctl emergency`

Answer: B

Explanation:

The `systemctl reboot` command will restore the server to its usual target by rebooting it. This will cause the server to load the default target specified in `/etc/systemd/system.conf` or `/etc/systemd/system/default.target` files. The `telinit 0` command would shut down the server, not restore it to its usual target. The `systemctl get-default` command would display the default target, not change it. The `systemctl emergency` command would switch the server to `emergency.target` mode, which is even more restrictive than `rescue.target` mode. References: [CompTIA Linux+ (XK0-005) Certification Study Guide], Chapter 17: System Maintenance and Operation, page 516.

NEW QUESTION 147

Developers have requested implementation of a persistent, static route on the application server. Packets sent over the interface `eth0` to `10.0.213.5/32` should be routed via `10.0.5.1`. Which of the following commands should the administrator run to achieve this goal?

- A. `route -i eth0 -p add 10.0.213.5 10.0.5.1`
- B. `route modify eth0 +ipv4.routes "10.0.213.5/32 10.0.5.1"`
- C. `echo "10.0.213.5 10.0.5.1 eth0" > /proc/net/route`
- D. `ip route add 10.0.213.5/32 via 10.0.5.1 dev eth0`

Answer: D

Explanation:

The command `ip route add 10.0.213.5/32 via 10.0.5.1 dev eth0` adds a static route to the routing table that sends packets destined for `10.0.213.5/32` (a single host) through the gateway `10.0.5.1` on the interface `eth0`. This is the correct way to achieve the goal. The other options are incorrect because they either use the wrong syntax (`route -i eth0 -p add`), the wrong command (`route modify`), or the wrong file (`/proc/net/route`). References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 12: Managing Network Connections, page 379.

NEW QUESTION 149

A systems administrator is implementing a new service task with systems at startup and needs to execute a script entitled `test.sh` with the following content:

```
TIMESTAMP=$(date '+%Y-%m-%d %H:%M:%S')
echo "helpme.service: timestamp $(Timestamp)" | systemd-cat -p info
sleep 60
done
```

The administrator tries to run the script after making it executable with `chmod +x`; however, the script will not run. Which of the following should the administrator do to address this issue? (Choose two.)

- A. Add `#!/bin/bash` to the bottom of the script.
- B. Create a unit file for the new service in `/etc/systemd/system/` with the name `helpme.service` in the location.
- C. Add `#!/bin/bash` to the top of the script.
- D. Restart the computer to enable the new service.
- E. Create a unit file for the new service in `/etc/init.d` with the name `helpme.service` in the location.
- F. Shut down the computer to enable the new service.

Answer: BC

Explanation:

The administrator should do the following two things to address the issue:

? Add `#!/bin/bash` to the top of the script. This is called a shebang line and it tells the system which interpreter to use to execute the script. Without this line, the script will not run properly. The shebang line should be the first line of the script and should start with `#!` followed by the path to the interpreter. In this case, the interpreter is `bash` and the path is `/bin/bash`. The other option (A) is incorrect because the shebang line should be at the top, not the bottom of the script.

? Create a unit file for the new service in `/etc/systemd/system/` with the name `helpme.service` in the location. This is necessary to register the script as a `systemd` service and enable it to run at startup. A unit file is a configuration file that defines the properties and behavior of a service, such as the description, dependencies, start and stop commands, and environment variables. The unit file should have the extension `.service` and should be placed in the `/etc/systemd/system/` directory. The other option (E) is incorrect because `/etc/init.d` is the directory for `init` scripts, not `systemd` services.

References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 14: Managing Processes and Scheduling Tasks, pages 429-430.

NEW QUESTION 154

An administrator would like to mirror the website files on the primary web server, www1, to the backup web server, www2. Which of the following commands should the administrator use to most efficiently accomplish this task?

- A. [www1] rsync -a -e ssh /var/www/html/ user1@www2 : /var/www/html
- B. [www1] scp -r /var/www/html user1@www2 : / var/www/html
- C. [www2] cd /var/www/html; wget -m http: //www1/
- D. [www1] cd /var/www/html && tar cvf —

Answer: A

Explanation:

To mirror the website files on the primary web server, www1, to the backup web server, www2, the administrator can use the command `rsync -a -e ssh /var/www/html/ user1@www2:/var/www/html` (A). This will synchronize all files and directories under /var/www/html/ on www1 to /var/www/html on www2 using ssh as the remote shell. The -a option will preserve all attributes and permissions of the files. The other commands will not mirror the website files, but either copy them once, download them from a web server, or archive them. References:
? [CompTIA Linux+ Study Guide], Chapter 12: Troubleshooting Linux Systems, Section: Synchronizing Files with rsync
? [How to Use rsync Command in Linux]

NEW QUESTION 158

Which of the following specifications is used to perform disk encryption in a Linux system?

- A. LUKS
- B. TLS
- C. SSL
- D. NFS

Answer: A

Explanation:

LUKS stands for Linux Unified Key Setup, which is a specification for disk encryption on Linux systems. LUKS allows users to encrypt partitions or entire disks using a passphrase or a key file. LUKS also supports multiple keys and key slots, which can be used to unlock the encrypted data. LUKS is compatible with various tools and utilities, such as cryptsetup, dm-crypt, and LVM. References: [How to Encrypt Partitions with LUKS on Linux]

NEW QUESTION 162

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

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.

NEW QUESTION 164

A Linux administrator has been tasked with installing the most recent versions of packages on a RPM-based OS. Which of the following commands will accomplish this task?

- A. apt-get upgrade
- B. rpm -a
- C. yum updateinfo
- D. dnf update
- E. yum check-update

Answer: D

Explanation:

The dnf update command will accomplish the task of installing the most recent versions of packages on a RPM-based OS. This command will check for available updates from the enabled repositories and apply them to the system. The apt-get upgrade command is used to install updates on a Debian-based OS, not a RPM-based OS. The rpm -a command is invalid, as -a is not a valid option for rpm. The yum updateinfo command will display information about available updates, but it will not install them. The yum check- update command will check for available updates, but it will not install them. References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 19: Managing Packages and Software, page 559.

NEW QUESTION 166

Which of the following enables administrators to configure and enforce MFA on a Linux system?

- A. Kerberos
- B. SELinux
- C. PAM
- D. PKI

Answer: C

Explanation:

The mechanism that enables administrators to configure and enforce MFA on a Linux system is PAM. PAM stands for Pluggable Authentication Modules, which is a framework for managing authentication and authorization on Linux systems. PAM allows the administrator to define the rules and policies for accessing various system resources and services, such as login, sudo, ssh, or cron. PAM also supports different types of authentication methods, such as passwords, tokens, biometrics, or smart cards. PAM can be used to implement MFA, which stands for Multi-Factor Authentication, which is a security technique that requires the user to provide more than one piece of evidence to prove their identity. MFA can enhance the security of the system and prevent unauthorized access. PAM enables administrators to configure and enforce MFA on a Linux system. This is the correct answer to the question. The other options are incorrect because they either do not manage authentication and authorization on Linux systems (Kerberos or PKI) or do not support MFA (SELinux). References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 17: Implementing Basic Security, page 517.

NEW QUESTION 171

A systems administrator is checking the system logs. The administrator wants to look at the last 20 lines of a log. Which of the following will execute the command?

- A. tail -v 20
- B. tail -n 20
- C. tail -c 20
- D. tail -l 20

Answer: B

Explanation:

The command tail -n 20 will display the last 20 lines of a file. The -n option specifies the number of lines to show. This is the correct command to execute the task. The other options are incorrect because they either use the wrong options (-v, -c, or -l) or have the wrong arguments (20 instead of 20 filename). References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 11: Managing Files and Directories, page 352.

NEW QUESTION 174

A Linux administrator is troubleshooting SSH connection issues from one of the workstations.

When users attempt to log in from the workstation to a server with the IP address 104.21.75.76, they receive the following message:

```
ssh: connect to host 104.21.75.76 port 22: Connection refused
```

The administrator reviews the information below:

Workstation output 1:

```
eth0: <BROADCAST,MULTICAST, UP, LOWER_UP> mtu 1500 qdisc mq state UP group default
link/ether 00:15:5d:e9:e9:fb brd 5.189.153.255 scope global eth0
inet 5.189.153.89/24 brd 5.189.153.255 scope global eth0
```

Workstation output 2:

```
default via 5.189.153.1 dev eth0
5.189.153.0/24 dev eth0 proto kernel scope link src 5.189.153.89
```

Server output 1:

target	prot	opt	source	destination
REJECT	tcp	--	101.68.78.194	0.0.0.0/0
REJECT	tcp	--	222.186.180.130	0.0.0.0/0
REJECT	tcp	--	104.131.1.39	0.0.0.0/0
REJECT	tcp	--	68.183.196.11	0.0.0.0/0
REJECT	tcp	--	5.189.153.89	0.0.0.0/0
REJECT	tcp	--	41.93.32.148	0.0.0.0/0

```
tcp dpt:22 ctstate NEW, UNTRACKED
reject-with icmp-port-unreachable
tcp dpt:22 ctstate NEW, UNTRACKED
reject-with icmp-port-unreachable
tcp dpt:22 ctstate NEW, UNTRACKED
reject-with icmp-port-unreachable
tcp dpt:22 ctstate NEW, UNTRACKED
reject-with icmp-port-unreachable
tcp dpt:22 ctstate NEW, UNTRACKED
reject-with icmp-port-unreachable
```

Server output 2:

```
sshd.service - OpenSSH server daemon
Loaded: loaded (/usr/lib/systemd/system/sshd.service; disabled; vendor preset: enabled)
Active: active (running) since Thu 2021-08-26 18:50:19 CEST; 2 weeks 5 days ago
```

Server output 3:

```
eth0: <BROADCAST, MULTICAST, UP, LOWER_UP> mtu 1500 qdisc mq state UP group default
link/ether 52:52:00:2a:bb:98 brd 104.21.75.255 scope global eth0
inet 104.21.75.76/24 brd 104.21.75.255 scope global eth0
```

Server output 4:

```
default via 104.21.75.254 dev eth0
104.21.75.0/24 dev eth0 proto kernel scope link src 104.21.75.76
```

Which of the following is causing the connectivity issue?

- A. The workstation has the wrong IP settings.
- B. The sshd service is disabled.
- C. The server's firewall is preventing connections from being made.
- D. The server has an incorrect default gateway configuration.

Answer: C

Explanation:

The server's firewall is preventing connections from being made, which is causing the connectivity issue. The output of `iptables -L -n` shows that the firewall is blocking all incoming traffic on port 22, which is the default port for SSH. The output of `ssh -v user@104.21.75.76` shows that the connection is refused by the server. To resolve the issue, the administrator needs to allow port 22 on the firewall. The other options are incorrect because they are not supported by the outputs. The workstation has the correct IP settings, as shown by the output of `ip addr show`. The sshd service is enabled and running, as shown by the output of `systemctl status sshd`. The server has the correct default gateway configuration, as shown by the output of `ip route show`. References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 13: Managing Network Services, pages 406-407.

NEW QUESTION 178

After installing some RPM packages, a systems administrator discovers the last package that was installed was not needed. Which of the following commands can be used to remove the package?

- A. `dnf remove packagename`
- B. `apt-get remove packagename`
- C. `rpm -i packagename`
- D. `apt remove packagename`

Answer: A

Explanation:

The command that can be used to remove an RPM package that was installed by mistake is `dnf remove packagename`. This command will use the DNF package manager to uninstall an RPM package and its dependencies from a Linux system that uses RPM-based distributions, such as Red Hat Enterprise Linux or CentOS. The DNF package manager handles dependency resolution and metadata searching for RPM packages. The other options are not correct commands for removing an RPM package from a Linux system. The `apt-get remove packagename` and `apt remove packagename` commands are used to remove Debian packages from a Linux system that uses Debian-based distributions, such as Ubuntu or Debian. They are not compatible with RPM packages. The `rpm -i packagename` command is used to install an RPM package, not to remove it. References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 9: Managing Software Packages; How to install/remove/query/update RPM packages in Linux (Cheat Sheet ...

NEW QUESTION 183

The applications team is reporting issues when trying to access the web service hosted in a Linux system. The Linux systems administrator is reviewing the following outputs:

Output 1:

* httpd.service = The Apache HTTPD Server

Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled) Active: inactive (dead)

Docs: man:httpd(8) man:apachectl(8) Output 2:

16:51:16 up 28 min, 1 user, load average: 0.00, 0.00, 0.07

Which of the following statements best describe the root cause? (Select two).

- A. The httpd service is currently started.
- B. The httpd service is enabled to auto start at boot time, but it failed to start.
- C. The httpd service was manually stopped.
- D. The httpd service is not enabled to auto start at boot time.
- E. The httpd service runs without problems.
- F. The httpd service did not start during the last server reboot.

Answer: CD

Explanation:

The httpd.service is the Apache HTTPD Server, which is a web service that runs on Linux systems. The output 1 shows that the httpd.service is inactive (dead), which means that it is not running. The output 1 also shows that the httpd.service is disabled, which means that it is not enabled to auto start at boot time. Therefore, the statements C and D best describe the root cause of the issue. The statements A, B, E, and F are incorrect because they do not match the output 1. References: [How to Manage Systemd Services on a Linux System]

NEW QUESTION 188

A Linux administrator needs to ensure that Java 7 and Java 8 are both locally available for developers to use when deploying containers. Currently only Java 8 is available. Which of the following commands should the administrator run to ensure both versions are available?

- A. `docker image load java:7`
- B. `docker image pull java:7`
- C. `docker image import java:7`
- D. `docker image build java:7`

Answer: B

Explanation:

The command that the administrator should run to ensure that both Java 7 and Java 8 are locally available for developers to use when deploying containers is `docker image pull java:7`. This command will use the `docker image pull` subcommand to download the `java:7` image from Docker Hub, which is the default registry for Docker images. The `java:7` image contains Java 7 installed on a Debian-based Linux system. The administrator can also specify a different registry by using the syntax `registry/repository:tag`. The other options are not correct commands for ensuring that both Java 7 and Java 8 are locally available for developers to use when deploying containers. The `docker image load java:7` command will load an image from a tar archive or STDIN, not from a registry. The `docker image import java:7` command will create a new filesystem image from the contents of a tarball, not from a registry. The `docker image build java:7` command will build an image from a Dockerfile, not from a

registry. References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 18: Automating Tasks; docker image pull | Docker Docs

NEW QUESTION 189

A systems administrator is configuring a Linux system so the network traffic from the internal network 172.17.0.0/16 going out through the eth0 interface would appear as if it was sent directly from this interface. Which of the following commands will accomplish this task?

- A. `iptables -A POSTROUTING -s 172.17.0.0/16 -o eth0 -j MASQUERADE`
- B. `firewalld -A OUTPUT -s 172.17.0.0/16 -o eth0 -j DIRECT`
- C. `nmcli masq-traffic eth0 -s 172.17.0.0/16 -j MASQUERADE`
- D. `ifconfig -- nat eth0 -s 172.17.0.0/16 -j DIRECT`

Answer: A

Explanation:

This command will use the iptables tool to append a rule to the POSTROUTING chain of the nat table, which will match any packet with a source address of 172.17.0.0/16 and an output interface of eth0, and apply the MASQUERADE target to it. This means that the packet will have its source address changed to the address of the eth0 interface, effectively hiding the internal network behind a NAT12.

References: 1: Iptables NAT and Masquerade rules - what do they do? 2: Routing from docker containers using a different physical network interface and default gateway

NEW QUESTION 192

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:

```
[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
```

Which of the following remediation steps will prevent the web service from running as a privileged user?

- A. Removing the ExecStarWusr/sbin/webserver -D SOPTIONS from the service file
- B. Updating the Environment File line in the [Service] section to/home/websevice/config
- C. Adding the User=websevice to the [Service] section of the service file
- D. Changing the:multi-user.target in the [Install] section to basic.target

Answer: C

Explanation:

The remediation step that will prevent the web service from running as a privileged user is adding the User=websevice 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 websevice is the name of the user that the administrator wants to run the web service as. The administrator should add the User=websevice 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/websevice/config) or do not affect the user that the service runs as (changing the multi-user.target in the [Install] section to basic.target). References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 15: Managing System Services, page 458.

NEW QUESTION 197

A Linux administrator needs to resolve a service that has failed to start. The administrator runs the following command:

```
ls -l startup file
```

The following output is returned

```
-----. root root 81k Sep 13 19:01 startupfile
```

Which of the following is MOST likely the issue?

- A. The service does not have permissions to read write the startupfile.
- B. The service startupfile size cannot be 81k.
- C. The service startupfile cannot be owned by root.
- D. The service startupfile should not be owned by the root group.

Answer: A

Explanation:

The most likely issue is that the service does not have permissions to read or write the startupfile. The output of `systemctl status startup.service` shows that the service has failed to start and the error message is "Permission denied". The output of `ls -l /etc/startupfile` shows that the file has the permissions `-rw-r--r--`, which means that only the owner (root) can read and write the file, while the group (root) and others can only read the file. The service may not run as root and may need write access to the file. The administrator should change the permissions of the file by using the `chmod` command and grant write access to the group or others, or change the owner or group of the file by using the `chown` command and assign it to the user or group that runs the service. The other options are incorrect because they are not supported by the outputs. The file size, owner, and group are not the causes of the issue. References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 11: Managing Files and Directories, pages 345-346.

NEW QUESTION 202

A systems administrator wants to list all local accounts in which the UID is greater than 500. Which of the following commands will give the correct output?

- A. `find /etc/passwd -size +500`
- B. `cut -d: f1 / etc/ passwd > 500`
- C. `awk -F: '$3 > 500 {print $1}' /etc/passwd`
- D. `sed '/UID/' /etc/passwd < 500`

Answer: C

Explanation:

The correct command to list all local accounts in which the UID is greater than 500 is:

`awk -F: '$3 > 500 {print $1}' /etc/passwd`

This command uses `awk` to process the `/etc/passwd` file, which contains information about the local users on the system. The `-F:` option specifies that the fields are separated by colons. The `$3` refers to the third field, which is the UID. The condition `$3 > 500` filters out the users whose UID is greater than 500. The action `{print $1}` prints the first field, which is the username.

The other commands are incorrect because:

? `find /etc/passwd -size +500` will search for files that are larger than 500 blocks in size, not users with UID greater than 500.

? `cut -d: f1 / etc/ passwd > 500` will cut the first field of the `/etc/passwd` file using colon as the delimiter, but it will not filter by UID or print only the usernames. The `> 500` part will redirect the output to a file named 500, not compare with the UID.

? `sed '/UID/' /etc/passwd < 500` will use `sed` to edit the `/etc/passwd` file and replace any line that contains UID with 500, not list the users with UID greater than 500.

The `< 500` part will redirect the input from a file named 500, not compare with the UID.

References:

? Linux List All Users In The System Command - nixCraft, section "List all users in Linux using `/etc/passwd` file".

? Unix script getting users with UID bigger than 500 - Stack Overflow, section "Using `awk`".

NEW QUESTION 206

An application developer received a file with the following content:

##This is a sample Image ## FROM ubuntu:18.04

MAINTAINER demohut@gmail.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 .`

Answer: A

Explanation:

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`.

NEW QUESTION 207

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`

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.

NEW QUESTION 209

A new application container was built with an incorrect version number. Which of the following commands should be used to rename the image to match the correct version 2.1.2?

- A. docker tag comptia/app:2.1.1 comptia/app:2.1.2
- B. docker push comptia/app:2.1.1 comptia/app:2.1.2
- C. docker rmi comptia/app:2.1.1 comptia/app:2.1.2
- D. docker update comptia/app:2.1.1 comptia/app:2.1.2

Answer: A

Explanation:

The best command to use to rename the image to match the correct version 2.1.2 is A. docker tag comptia/app:2.1.1 comptia/app:2.1.2. This command will create a new tag for the existing image with the new version number, without changing the image content or ID. The other commands are either incorrect or not suitable for this task. For example:

? B. docker push comptia/app:2.1.1 comptia/app:2.1.2 will try to push two images to a remote repository, but it does not rename the image locally.

? C. docker rmi comptia/app:2.1.1 comptia/app:2.1.2 will try to remove two images from the local system, but it does not rename the image.

? D. docker update comptia/app:2.1.1 comptia/app:2.1.2 will try to update the configuration of a running container, but it does not rename the image.

NEW QUESTION 212

A cloud engineer wants to delete all unused networks that are not referenced by any container. Which of the following commands will achieve this goal?

- A. docker network erase
- B. docker network clear
- C. docker network prune
- D. docker network rm

Answer: C

Explanation:

The docker command is used to manage Docker containers, images, networks, volumes, and other resources on a Linux system. Docker is a platform that allows users to run applications in isolated environments called containers. Docker also provides networking features that allow users to create and manage networks for containers.

To delete all unused networks that are not referenced by any container, the cloud engineer can use the docker network prune command. This command will remove all networks that have no containers connected to them. The statement C is correct.

The statements A, B, and D are incorrect because they do not delete all unused networks.

The docker network erase and docker network clear commands do not exist. The docker network rm command deletes a specific network by name or ID, but not all unused networks. References: [How to Manage Docker Networks]

NEW QUESTION 215

A Linux administrator needs to correct the permissions of a log file on the server. Which of the following commands should be used to set filename.log permissions to -rwxr--r--. ?

- A. chmod 755 filename.log
- B. chmod 640 filename.log
- C. chmod 740 filename.log
- D. chmod 744 filename.log

Answer: A

Explanation:

The command chmod 755 filename.log should be used to set filename.log permissions to -rwxr--r--. The chmod command is a tool for changing file permissions on Linux file systems. The permissions can be specified in octal notation, where each digit represents the permissions for the owner, group, and others respectively. The permissions are encoded as follows:

? 0: no permission

? 1: execute permission

? 2: write permission

? 4: read permission

? 5: read and execute permissions (4 + 1)

? 6: read and write permissions (4 + 2)

? 7: read, write, and execute permissions (4 + 2 + 1)

The command chmod 755 filename.log will set the permissions to -rwxr--r--, 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). This is the correct command to use to accomplish the task. The other options are incorrect because they either set the wrong permissions (chmod 640, chmod 740, or chmod 744) or do not exist (chmod -G). References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 11: Managing Files and Directories, page 345.

NEW QUESTION 219

A systems administrator is working on a security report from the Linux servers. Which of the following commands can the administrator use to display all the firewall rules applied to the Linux servers? (Select two).

- A. ufw limit
- B. iptables —F
- C. systemctl status firewalld
- D. firewall—cmd —1ist—a11
- E. ufw status

F. iptables —A

Answer: DE

Explanation:

These commands can display all the firewall rules applied to the Linux servers, depending on which firewall service is being used.

? The firewall-cmd command is a utility for managing firewalld, which is a dynamic firewall service that supports zones and services. The --list-all option will show all the settings and rules for the default zone, or for a specific zone if specified. For example, firewall-cmd --list-all --zone=public will show the rules for the public zone1.

? The ufw command is a frontend for iptables, which is a low-level tool for manipulating netfilter, the Linux kernel's packet filtering framework. The status option will show the status of ufw and the active rules, or the numbered rules if verbose is specified. For example, ufw status verbose will show the numbered rules and other information2.

The other options are incorrect because:

* A. ufw limit

This command will limit the connection attempts to a service or port using iptables' recent module. It does not display any firewall rules2.

* B. iptables -F

This command will flush (delete) all the rules in the selected chain, or all chains if none is given. It does not display any firewall rules3.

* C. systemctl status firewalld

This command will show the status of the firewalld service, including whether it is active or not, but it does not show the firewall rules4.

* F. iptables -A

This command will append one or more rules to the end of the selected chain. It does not display any firewall rules3.

NEW QUESTION 224

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

A. setenforce

B. sudo

C. umask

D. chmod

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.

NEW QUESTION 229

An administrator thinks that a package was installed using a snap. Which of the following commands can the administrator use to verify this information?

A. snap list

B. snap find

C. snap install

D. snap try

Answer: A

Explanation:

The snap list command is used to display the installed snaps on the system1. Snaps are self-contained software packages that can be installed and updated across different Linux distributions2. The snap list command shows the name, version, revision, developer and notes of each snap1.

The snap find command is used to search for snaps in the Snap Store, which is an online repository of snaps2. The snap install command is used to install snaps from the Snap Store or from a local file2. The snap try command is used to test a snap without installing it, by mounting a directory that contains the snap files2.

These commands are not useful for verifying if a package was installed using a snap.

NEW QUESTION 233

Users are experiencing high latency when accessing a web application served by a Linux machine. A systems administrator checks the network interface counters and sees the following:

```
# ip -s link list dev enp0s25

2: enp0s25: <BROADCAST,MULTICAST,LOWER_UP,UP> mtu 1500 qdisc fq_codel state DOWN mode DEFAULT group default qlen 1000 link/ether
ac:12:34:56:78:cd brd ff:ff:ff:ff:ff:ff

RX: bytes  packets  errors  dropped missed  mcast
2011664755 3579033 2394390 508      0        0

TX: bytes  packets  errors  dropped carrier collsns
309541780 1705408 0       0       12340    0
```

Which of the following is the most probable cause of the observed latency?

A. The network interface is disconnected.

B. A connection problem exists on the network interface.

C. No IP address is assigned to the interface.

D. The gateway is unreachable.

Answer: B

Explanation:

The high number of errors and dropped packets in the output of the network interface counters indicate a connection problem on the network interface.

References:

? CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 10: Managing Networking, Section: Troubleshooting Network Issues, Page 359.

? Linux+ (Plus) Certification, Exam Objectives: 4.3 Given a scenario, troubleshoot and resolve basic network configuration and connectivity issues.

NEW QUESTION 235

A Linux engineer finds multiple failed login entries in the security log file for application users. The Linux engineer performs a security audit and discovers a security issue. Given the following:

```
# grep -iE '*www*[db]' /etc/passwd
```

```
www-data:x:502:502:www-data:/var/www:/bin/bash db:x: 505:505:db: /opt/db:/bin/bash
```

Which of the following commands would resolve the security issue?

- A. `usermod -d /srv/www-data www-data && usermod -d /var/lib/db db`
- B. `passwd -u www-data && passwd -u db`
- C. `renice -n 1002 -u 502 && renice -n 1005 -u 505`
- D. `chsh -s /bin/false www-data && chsh -s /bin/false db`

Answer: D

Explanation:

This command will use the chsh tool to change the login shell of the users www-data and db to /bin/false, which means they will not be able to log in to the system1. This will prevent unauthorized access attempts and improve security.

References: 1: Replacing /bin/bash with /bin/false in /etc/passwd file

NEW QUESTION 239

A Linux administrator needs to analyze a failing application that is running inside a container. Which of the following commands allows the Linux administrator to enter the running container and analyze the logs that are stored inside?

- A. `docker run -ti app /bin/sh`
- B. `podman exec -ti app /bin/sh`
- C. `podman run -d app /bin/bash`
- D. `docker exec -d app /bin/bash`

Answer: B

Explanation:

Podman `exec -ti app /bin/sh` allows the Linux administrator to enter the running container and analyze the logs that are stored inside. This command uses the podman tool, which is a daemonless container engine that can run and manage containers on Linux systems. The `exec` option executes a command inside an existing container, in this case `app`, which is the name of the container that runs the failing application. The `-ti` option allocates a pseudo-TTY and keeps STDIN open, allowing for interactive shell access to the container. The `/bin/sh` argument specifies the shell command to run inside the container, which can be used to view and manipulate the log files.

The other options are not correct commands for entering a running container and analyzing the logs. `Docker run -ti app /bin/sh` creates a new container from the `app` image and runs the `/bin/sh` command inside it, but does not enter the existing container that runs the failing application. `Podman run -d app /bin/bash` also creates a new container from the `app` image and runs the `/bin/bash` command inside it, but does so in detached mode, meaning that it runs in the background without interactive shell access. `Docker exec -d app /bin/bash` executes the `/bin/bash` command inside the existing `app` container, but also does so in detached mode, without interactive shell access.

References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 18: Automating Tasks; View container logs | Docker Docs; How to see the logs of a docker container - Stack Overflow

NEW QUESTION 244

A user is unable to log on to a Linux workstation. The systems administrator executes the following command:

```
cat /etc/shadow | grep user1
```

The command results in the following output:

```
user1 :! $6$QERgAsdvojadv4asdvaarC/9dj34GdafGVaregmksdfa:18875:0:99999:7 :::
```

Which of the following should the systems administrator execute to fix the issue?

- A. `chown -R user1:user1 /home/user1`
- B. `sed -i ' / :: / :: /g' /etc/shadow`
- C. `chgrp user1:user1 /home/user1`
- D. `passwd -u user1`

Answer: D

Explanation:

The output shows that the user1 account has a locked password, indicated by the exclamation point (!) in the second field of the /etc/shadow file1. To unlock the password and allow the user to log in, the systems administrator should use the passwd command with the -u (unlock) option2.

References: 1: Understanding the /etc/shadow File 2: How To Use The Passwd Command In Linux

NEW QUESTION 246

A Linux systems administrator receives a notification that one of the server's filesystems is full. Which of the following commands would help the administrator to identify this filesystem?

- A. `lsblk`
- B. `fdisk`
- C. `df -h`
- D. `du -ah`

Answer: C

Explanation:

The `df -h` command can be used to identify the filesystem that is full. This command displays the disk usage of each mounted filesystem in a human-readable format, showing the total size, used space, available space, and percentage of each filesystem. The `lsblk` command displays information about block devices, not filesystems. The `fdisk` command can be used to manipulate partition tables, not check disk usage. The `du -ah` command displays the disk usage of each file and directory in a human-readable format, not the filesystems. References: [CompTIA Linux+ (XK0-005) Certification Study Guide], Chapter 14: Managing Disk Storage, page 454.

NEW QUESTION 251

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

XK0-005 Practice Exam Features:

- * XK0-005 Questions and Answers Updated Frequently
- * XK0-005 Practice Questions Verified by Expert Senior Certified Staff
- * XK0-005 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * XK0-005 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The XK0-005 Practice Test Here](#)