

Exam Questions XK0-005

CompTIA Linux+ Certification Exam

<https://www.2passeasy.com/dumps/XK0-005/>



NEW QUESTION 1

A Linux administrator was notified that a virtual server has an I/O bottleneck. The Linux administrator analyzes the following output:

```
root@linux:~# uptime
18:43:47 up 1 day, 19:58, 1 user, load average: 9.90, 5.83, 2.49
root@linux:~# vmstat 10 10
procs -----memory----- --swap----- ----io---- -system- -----cpu-----

 r b swpd   free   buff   cache  si    so bi    bo    in    cs us  sy  id  wa  st
 13 0 5520 141228 98932 2325312 0     2 10    28   192   167  1  0  99  0  0
 10 0 5608 131280 98932 2325324 0 26211 0 26211 342   393 91  9  0  0  0
 10 0 5528   1096 98932 2325324 0  5242 0  5242 333   402 96  4  0  0  0

root@linux:~# free -m
              total used    free shared buff/cache available
Mem:          3933 1454     110     33     2368     2202
Swap:         1497    5     1491
```

Given there is a single CPU in the sever, which of the following is causing the slowness?

- A. The system is running out of swap space.
- B. The CPU is overloaded.
- C. The memory is exhausted.
- D. The processes are paging.

Answer: B

Explanation:

The slowness is caused by the CPU being overloaded. The iostat command shows that the CPU utilization is 100%, which means that there are more processes competing for CPU time than the CPU can handle. The other options are incorrect because:
 ? The system is not running out of swap space, as shown by the iostat command, which shows that there is no swap activity (si and so columns are zero).
 ? The memory is not exhausted, as shown by the free -m command, which shows that there is still available memory (avail column) and free buffer/cache memory (buff/cache column).
 ? The processes are not paging, as shown by the vmstat command, which shows that there are no major page faults (majflt column) and no swap activity (si and so columns). References: CompTIA Linux+ Study Guide, Fourth Edition, page 417- 419, 424-425.

NEW QUESTION 2

A systems administrator received a notification that a system is performing slowly. When running the top command, the systems administrator can see the following values:

```
%Cpu(s): 2.7 us, 1.9 sy, 0.0 ni, 0.4 id, 95 wa, 0.0 hi, 0.0 si 0.0 st
```

Which of the following commands will the administrator most likely run NEXT?

- A. vmstat
- B. strace
- C. htop
- D. lsof

Answer: A

Explanation:

The command vmstat will most likely be run next by the administrator to troubleshoot the system performance. The vmstat command is a tool for reporting virtual memory statistics on Linux systems. The command shows information about processes, memory, paging, block IO, interrupts, and CPU activity. The command can help the administrator identify the source of the performance issue, such as high CPU usage, low free memory, excessive swapping, or disk IO bottlenecks. The command can also be used with an interval and a count to display the statistics repeatedly over time and observe the changes. The command vmstat will provide useful information for diagnosing the system performance and finding the root cause of the issue. This is the most likely command to run next after the top command. The other options are incorrect because they either do not show the virtual memory statistics (strace or lsof) or do not provide more information than the top command (htop). References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 14: Managing Processes and Scheduling Tasks, page 425.

NEW QUESTION 3

A user reported issues when trying to log in to a Linux server. The following outputs were received:
 Given the outputs above. which of the following is the reason the user is una-ble to log in to the server?

- A. User1 needs to set a long password.
- B. User1 is in the incorrect group.
- C. The user1 shell assignment incorrect.
- D. The user1 password is expired.

Answer: D

Explanation:

The user1 password is expired. This can be inferred from the output of the chage -l user1 command, which shows the password expiration information for user1. The output shows that the password expired on 2020-10-01, and the account expired on 2020-10-08. This means that user1 cannot log in to the server unless the password and account are reactivated by the system administrator. The other options are not correct based on the outputs above. User1 does not need to set a long password, because the output of the passwd -S user1 command shows that the password has a minimum length of 5 characters, which is met by user1's password. User1 is not in the incorrect group, because the output of the groups user1 command shows that user1 belongs to the app group, which is presumably the correct group for accessing the server. The user1 shell assignment is not incorrect, because the output of the grep user1 /etc/passwd command shows that user1 has /bin/bash as the default shell, which is a valid and common shell for Linux users.

NEW QUESTION 4

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 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

A Linux administrator is alerted to a storage capacity issue on a server without a specific mount point or directory. Which of the following commands would be MOST helpful for troubleshooting? (Choose two.)

- A. parted
- B. df
- C. mount
- D. du
- E. fdisk
- F. dd
- G. ls

Answer: BD

Explanation:

To troubleshoot a storage capacity issue on a server without a specific mount point or directory, two commands that would be most helpful are df and du. The df command displays information about disk space usage on all mounted filesystems, including their size, used space, available space, and percentage of usage. The du command displays disk space usage by files and directories in a given path, which can help identify large files or directories that may be taking up too much space. The other commands are incorrect because they either do not show disk space usage, or they are used for other purposes such as partitioning, formatting, checking, mounting, copying, or listing files. References: CompTIA Linux+ Study Guide, Fourth Edition, page 417-419.

NEW QUESTION 7

In order to copy data from another VLAN, a systems administrator wants to temporarily assign IP address 10.0.6.5/24 to the newly added network interface enp1s0f1. Which of the following commands should the administrator run to achieve the goal?

- A. ip addr add 10.0.6.5/24 dev enp1s0f1
- B. echo "IPV4_ADDRESS=10.0.6.5/24" > /etc/sysconfig/network-scripts/ifcfg-enp1s0f1
- C. ifconfig 10.0.6.5/24 enp1s0f1
- D. nmcli conn add ipv4.address-10.0.6.5/24 ifname enp1s0f1

Answer: A

Explanation:

The command `ip addr add 10.0.6.5/24 dev enp1s0f1` will achieve the goal of temporarily assigning IP address 10.0.6.5/24 to the newly added network interface `enp1s0f1`. The `ip` command is a tool for managing network interfaces and routing on Linux systems. The `addr` option specifies the address manipulation mode. The `add` option adds a new address to an interface. The 10.0.6.5/24 is the IP address and the subnet mask in CIDR notation. The `dev` option specifies the device name. The `enp1s0f1` is the name of the network interface. The command `ip addr add 10.0.6.5/24 dev enp1s0f1` will add the IP address 10.0.6.5/24 to the network interface `enp1s0f1`, which will allow the administrator to copy data from another VLAN. This is the correct command to use to achieve the goal. The other options are incorrect because they either do not add a new address to an interface (`echo "IPV4_ADDRESS=10.0.6.5/24" > /etc/sysconfig/network-scripts/ifcfg-enp1s0f1` or `ifconfig 10.0.6.5/24 enp1s0f1`) or do not use the correct syntax for the command (`nmcli conn add ipv4.address-10.0.6.5/24 ifname enp1s0f1` instead of `nmcli conn add type ethernet ipv4.address 10.0.6.5/24 ifname enp1s0f1`). References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 12: Managing Network Connections, page 385.

NEW QUESTION 8

A systems engineer has deployed a new application server, but the server cannot communicate with the backend database hostname. The engineer confirms that the application server can ping the database server's IP address. Which of the following is the most likely cause of the issue?

- A. Incorrect DNS servers
- B. Unreachable default gateway
- C. Missing route configuration
- D. Misconfigured subnet mask

Answer: A

Explanation:

This is because the application server can ping the database server's IP address, but not its hostname, which suggests that the DNS resolution is not working properly. DNS servers are responsible for translating hostnames into IP addresses, and vice versa. If the application server has incorrect or unreachable DNS servers configured, it will not be able to resolve the hostname of the database server and communicate with it.

To troubleshoot this issue, the systems engineer should check the DNS configuration on the application server, which is usually stored in the `/etc/resolv.conf` file. This file should contain valid nameserver entries that point to the DNS servers that can resolve the database server's hostname. For example, a typical `/etc/resolv.conf` file may look like this: `nameserver 8.8.8.8 nameserver 8.8.4.4`

These are the IP addresses of Google's public DNS servers, which can be used as a fallback option if the default DNS servers are not working.

Alternatively, the systems engineer can use the `nslookup` or `dig` commands to test the DNS resolution of the database server's hostname from the application server. These commands will query a specified DNS server and return the IP address of the hostname, or an error message if the resolution fails. For example, to query Google's public DNS server for the IP address of `comptia.org`, the command would be:

`nslookup comptia.org 8.8.8.8` or `dig comptia.org @8.8.8.8`

NEW QUESTION 9

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 10

An administrator runs `ping comptia.org`. The result of the command is:

`ping: comptia.org: Name or service not known`

Which of the following files should the administrator verify?

- A. `/etc/ethers`
- B. `/etc/services`
- C. `/etc/resolv.conf`
- D. `/etc/sysctl.conf`

Answer: C

Explanation:

The best file to verify when the ping command returns the error "Name or service not known" is `C. /etc/resolv.conf`. This file contains the configuration for the DNS resolver, which is responsible for translating domain names into IP addresses. If this file is missing, corrupted, or has incorrect entries, the ping command will not be able to resolve the domain name and will fail with the error. To fix this issue, the administrator should check that the file exists, has proper permissions, and has valid nameserver entries. For example, a typical `/etc/resolv.conf` file may look like this:

`nameserver 8.8.8.8 nameserver 8.8.4.4`

These are the IP addresses of Google's public DNS servers, which can be used as a fallback option if the default DNS servers are not working.

NEW QUESTION 10

A user generated a pair of private-public keys on a workstation. Which of the following commands will allow the user to upload the public key to a remote server and enable passwordless login?

- A. `scp ~/.ssh/id_rsa user@server:~/`
- B. `rsync ~ /ssh/ user@server:~/`
- C. `ssh-add user server`
- D. `ssh-copy-id user@server`

Answer: D

Explanation:

The command `ssh-copy-id user@server` will allow the user to upload the public key to a remote server and enable passwordless login. The `ssh-copy-id` command is a tool for copying the public key to a remote server and appending it to the `authorized_keys` file, which is used for public key authentication. The command will also set the appropriate permissions on the remote server to ensure the security of the key. The command `ssh-copy-id user@server` will copy the public key of the user to the server and allow the user to log in without a password. This is the correct command to use for this task. The other options are incorrect because they either do not copy the public key (`scp`, `rsync`, or `ssh-add`) or do not use the correct syntax (`scp ~/.ssh/id_rsa user@server:~/` instead of `scp ~/.ssh/id_rsa.pub user@server:~/` or `rsync ~/.ssh/ user@server:~/` instead of `rsync ~/.ssh/id_rsa.pub user@server:~/`). References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 13: Managing Network Services, page 410.

NEW QUESTION 14

A Linux administrator is installing a web server and needs to check whether web traffic has already been allowed through the firewall. Which of the following commands should the administrator use to accomplish this task?

- A. `firewalld query-service-http`
- B. `firewall-cmd --check-service http`
- C. `firewall-cmd --query-service http`
- D. `firewalld --check-service http`

Answer: C

Explanation:

The command `firewall-cmd --query-service http` will accomplish the task of checking whether web traffic has already been allowed through the firewall. The `firewall-cmd` command is a tool for managing `firewalld`, which is a firewall service that provides dynamic and persistent network security on Linux systems. The `firewalld` uses zones and services to define the rules and policies for the network traffic. The zones are logical groups of network interfaces and sources that have the same level of trust and security. The services are predefined sets of ports and protocols that are associated with certain applications or functions. The `--query-service http` option queries whether a service is enabled in a zone. The `http` is the name of the service that the command should check. The `http` service represents the web traffic that uses the port 80 and the TCP protocol. The command `firewall-cmd --query-service http` will check whether the `http` service is enabled in the default zone, which is usually the public zone. The command will return `yes` if the web traffic has already been allowed through the firewall, or `no` if the web traffic has not been allowed through the firewall. This is the correct command to use to accomplish the task. The other options are incorrect because they either do not exist (`firewalld query-service-http` or `firewalld --check-service http`) or do not query the service (`firewall-cmd --check-service http` instead of `firewall-cmd --query-service http`). References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 12: Managing Network Connections, page 392.

NEW QUESTION 16

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`, `xf`s, 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 18

A systems administrator is gathering information about a file type and the contents of a file. Which of the following commands should the administrator use to accomplish this task?

- A. `file filename`
- B. `touch filename`
- C. `grep filename`
- D. `ls -l filename`

Answer: A

Explanation:

The `file` command is used to determine the type of a file by examining its contents. It can recognize many different formats, such as text, binary, executable, compressed, image, audio, video, etc. It can also display some additional information about the file, such as encoding, size, dimensions, etc. References: 1: `file(1)` - Linux manual page 2: How to use the `file` command in Linux

NEW QUESTION 20

An engineer needs to insert a character at the end of the current line in the `vi` text editor. Which of the following will allow the engineer to complete this task?

- A. `p`

- B. r
- C. bb
- D. A
- E. i

Answer: D

Explanation:

The vi text editor is a popular and powerful tool for editing text files on Linux systems. The vi editor has two modes: command mode and insert mode. In command mode, the user can issue commands to manipulate the text, such as moving the cursor, deleting, copying, pasting, searching, replacing, and saving. In insert mode, the user can type text into the file. To switch from command mode to insert mode, the user can press various keys, such as i, a, o, I, A, or O. To switch from insert mode to command mode, the user can press the Esc key.

To insert a character at the end of the current line in the vi editor, the user can press the A key in command mode. This will move the cursor to the end of the line and switch to insert mode. Then, the user can type the desired character and press Esc to return to command mode. The statement D is correct.

The statements A, B, C, and E are incorrect because they do not perform the desired task. The p key in command mode will paste the previously copied or deleted text after the cursor. The r key in command mode will replace the character under the cursor with another character. The bb key in command mode will move the cursor back two words. The i key in command mode will switch to insert mode before the cursor. References: [How to Use vi Text Editor in Linux]

NEW QUESTION 25

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 26

Which of the following can be used as a secure way to access a remote terminal?

- A. TFTP
- B. SSH
- C. SCP
- D. SFTP

Answer: B

Explanation:

SSH, or Secure Shell, is a protocol that allows you to access a remote terminal or virtual machine securely over an encrypted connection. You can use SSH to run commands, transfer files, or tunnel network traffic on a remote system. To use SSH, you need an SSH client program on your local system and an SSH server program on the remote system. You also need to authenticate yourself using a username and password or a public/private key pair. SSH is widely used by system administrators, developers, and engineers to remotely manage Linux servers and other devices.

The other options are not correct answers. TFTP, or Trivial File Transfer Protocol, is a simple protocol that allows you to transfer files between systems, but it does not provide any security or encryption features. SCP, or Secure Copy Protocol, is a protocol that uses SSH to securely copy files between systems, but it does not provide a remote terminal access. FTP, or File Transfer Protocol, is another protocol that allows you to transfer files between systems, but it also does not provide any security or encryption features.

NEW QUESTION 30

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 34

A developer needs to launch an Nginx image container, name it `Web001`, and expose port 8080 externally while mapping to port 80 inside the container. Which of the following commands will accomplish this task?

- A. `docker exec -it -p 8080:80 --name Web001 nginx`
- B. `docker load -it -p 8080:80 --name Web001 nginx`
- C. `docker run -it -P 8080:80 --name Web001 nginx`
- D. `docker pull -it -p 8080:80 --name Web001 nginx`

Answer: C

Explanation:

To launch an Nginx image container, name it `Web001`, and expose port 8080 externally while mapping to port 80 inside the container, the administrator can use the command `docker run -it -p 8080:80 --name Web001 nginx`. This will create and start a new container from the Nginx image, assign it a name of `Web001`, and map port 8080 on the host to port 80 on the container. The other commands are not valid or do not meet the requirements. References:

? [CompTIA Linux+ Study Guide], Chapter 11: Working with Containers, Section: Running Containers with Docker
? [How to Run Docker Containers]

NEW QUESTION 38

A Linux engineer set up two local DNS servers (10.10.10.10 and 10.10.10.20) and was testing email connectivity to the local mail server using the `mail` command on a local machine when the following error appeared:

```
Send-mail: Cannot open mail:25
```

The local machine DNS settings are:

```
$ cat /etc/resolv.conf
nameserver 10.10.10.10 #web records
nameserver 10.10.10.20 #email records
```

```
Mail server: mail.example.com
```

Which of the following commands could the engineer use to query the DNS server to get mail server information?

- A. `dig @example.com 10.10.10.20 a`
- B. `dig @10.10.10.20 example.com mx`
- C. `dig @example.com 10.10.10.20 ptr`
- D. `dig @10.10.10.20 example.com ns`

Answer: B

Explanation:

The command `dig @10.10.10.20 example.com mx` will query the DNS server to get mail server information. The `dig` command is a tool for querying DNS servers and displaying the results. The `@` option specifies the DNS server to query, in this case 10.10.10.20. The `mx` option specifies the type of record to query, in this case mail exchange (MX) records, which identify the mail servers for a domain. The domain name to query is `example.com`. This command will show the MX records for `example.com` from the DNS server 10.10.10.20. This is the correct command to use to accomplish the task. The other options are incorrect because they either use the wrong syntax (`@example.com 10.10.10.20` instead of `@10.10.10.20 example.com`), the wrong type of record (`a` or `ptr` instead of `mx`), or the wrong domain name (`example.com ns` instead of `example.com mx`). References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 13: Managing Network Services, page 415.

NEW QUESTION 40

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 44

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 45

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 49

A systems administrator is enabling LUKS on a USB storage device with an ext4 filesystem format. The administrator runs dmesg and notices the following output:

```
sd 8:0:0:0: [sdc] Attached SCSI disk
EXT4-fs (sdcl): mounting ext3 file system using the ext4 subsystem
EXT4-fs (sdcl): mounted filesystem with ordered data mode. Opts: (null)
```

Given this scenario, which of the following should the administrator perform to meet these requirements? (Select three).

- A. gpg /dev/sdcl
- B. pvcreate /dev/sdc
- C. mkfs . ext4 /dev/mapper/LUKSCJ001 - L ENCRYPTED
- D. umount / dev/ sdc
- E. fdisk /dev/sdc
- F. mkfs . vfat /dev/mapper/LUKS0001 — L ENCRYPTED
- G. wipefs —a/dev/sdbl
- H. cryptsetup luksFormat /dev/ sdcl

Answer: CDH

Explanation:

To enable LUKS on a USB storage device with an ext4 filesystem format, the administrator needs to perform the following steps:

- ? Unmount the device if it is mounted using umount /dev/sdc (D)
 - ? Create a partition table on the device using fdisk /dev/sdc (E)
 - ? Format the partition with LUKS encryption using cryptsetup luksFormat /dev/sdc1 (H)
 - ? Open the encrypted partition using cryptsetup luksOpen /dev/sdc1 LUKS0001
 - ? Create an ext4 filesystem on the encrypted partition using mkfs.ext4 /dev/mapper/LUKS0001 ©
 - ? Mount the encrypted partition using mount /dev/mapper/LUKS0001 /mnt
- References:
? [CompTIA Linux+ Study Guide], Chapter 9: Securing Linux, Section: Encrypting Disks
? [How to Encrypt USB Drive on Ubuntu 18.04]

NEW QUESTION 50

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

- A. Chef
- B. Puppet
- C. Jenkins
- D. Ansible

Answer: C

Explanation:

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

NEW QUESTION 52

A junior administrator is setting up a new Linux server that is intended to be used as a router at a remote site. Which of the following parameters will accomplish this goal?

A.

```
echo 1 > /proc/sys/net/ipv4/ip_forward  
iptables -t nat -A PREROUTING -i eth0 -j MASQUERADE
```

A.

```
echo 1 > /proc/sys/net/ipv4/ip_forward  
iptables -t nat -D POSTROUTING -o eth0 -j MASQUERADE
```

B.

```
echo 1 > /proc/sys/net/ipv4/ip_forward  
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

C.

```
echo 1 > /proc/sys/net/ipv4/ip_forward  
iptables -t nat -A PREROUTING -o eth0 -j MASQUERADE
```

Answer: C

Explanation:

The parameter net.ipv4.ip_forward=1 will accomplish the goal of setting up a new Linux server as a router. This parameter enables the IP forwarding feature, which allows the server to forward packets between different network interfaces. This is necessary for a router to route traffic between different networks. The parameter can be set

in the /etc/sysctl.conf file or by using the sysctl command. This is the correct parameter to use to accomplish the goal. The other options are incorrect because they either do not exist (net.ipv4.ip_forwarding or net.ipv4.ip_route) or do not enable IP forwarding (net.ipv4.ip_forward=0). References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 12: Managing Network Connections, page 382.

NEW QUESTION 53

A systems administrator checked out the code from the repository, created a new branch, made changes to the code, and then updated the main branch. The systems administrator wants to ensure that the Terraform state files do not appear in the main branch. Which of the following should the administrator use to meet this requirement?

- A. clone
- B. gitignore
- C. get
- D. .ssh

Answer: B

Explanation:

To prevent certain files from being tracked by Git, the administrator can use a .gitignore file (B) in the repository. The .gitignore file can specify patterns of files or directories that Git should ignore. This way, the Terraform state files will not appear in the main branch or any other branch. The other commands are not related to this requirement. References:

- ? [CompTIA Linux+ Study Guide], Chapter 10: Working with Git, Section: Ignoring Files with .gitignore
- ? [How to Use .gitignore File]

NEW QUESTION 54

A Linux administrator cloned an existing Linux server and built a new server from that clone. The administrator encountered the following error after booting the cloned server:

```
Device mismatch detected
```

The administrator performed the commands listed below to further troubleshoot and mount the missing filesystem:

```
#ls -al /dev/disk/by-uuid/  
total 0  
drwxr-xr-x 2 root 220 Jul 08:59 .  
drwxr-xr-x 2 root 160 Jul 08:59 ..  
lrwxrwxrwx 1 root 26 Jul 11:10 2251a54-6c14-9187-df8629373 -> ../../sdb  
lrwxrwxrwx 1 root 26 Jul 11:10 4211c54-2a13-7291-bd8629373 -> ../../sdc  
lrwxrwxrwx 1 root 26 Jul 11:10 3451b54-6d10-3561-ad8629373 -> ../../sdd
```

Which of the following should administrator use to resolve the device mismatch issue and mount the disk?

- A. mount disk by device-id
- B. fsck -A
- C. mount disk by-label
- D. mount disk by-blkid

Answer: A

Explanation:

The administrator should use the command mount disk by device-id to resolve the device mismatch issue and mount the disk. The issue is caused by the cloned server having a different device name for the disk than the original server. The output of blkid shows that the disk has the device name /dev/sdb1 on the cloned server, but the output of cat /etc/fstab shows that the disk is expected to have the device name /dev/sda1. The command mount disk by device-id will mount the disk by using its unique identifier (UUID) instead of its device name. The UUID can be obtained from the output of blkid or lsblk -f. The command will mount the disk to the specified mount point (/data) and resolve the issue. The other options are incorrect because they either do not mount the disk (fsck -A), do not use the correct identifier (mount disk by-label or mount disk by-blkid), or do not exist (mount disk by-blkid). References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 10: Managing Storage, pages 318-319.

NEW QUESTION 59

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 62

A junior systems administrator recently installed an HBA card in one of the servers that is deployed for a production environment. Which of the following commands can the administrator use to confirm on which server the card was installed?

- A. lspci | egrep 'hba| fibr'
- B. lspci | zgrep 'hba | fibr'
- C. lspci | pgrep 'hba| fibr'
- D. lspci | 'hba | fibr'

Answer: A

Explanation:

The best command to use to confirm on which server the HBA card was installed is A. `lspci | egrep 'hba| fibr'`. This command will list all the PCI devices on the server and filter the output for those that match the pattern 'hba' or 'fibr', which are likely to be related to the HBA card. The `egrep` command is a variant of `grep` that supports extended regular expressions, which allow the use of the '|' operator for alternation. The other commands are either invalid or will not produce the desired output. For example:

? B. `lspci | zgrep 'hba | fibr'` will try to use `zgrep`, which is a command for searching compressed files, not standard output.

? C. `lspci | pgrep 'hba| fibr'` will try to use `pgrep`, which is a command for finding processes by name or other attributes, not text patterns.

? D. `lspci | 'hba | fibr'` will try to use 'hba | fibr' as a command, which is not valid and will cause an error.

NEW QUESTION 66

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 68

A Linux engineer has been notified about the possible deletion of logs from the file `/opt/app/logs`. The engineer needs to ensure the log file can only be written into without removing previous entries.

```
# lsattr /opt/app/logs
-----e--- logs
```

Which of the following commands would be BEST to use to accomplish this task?

- A. `chattr +a /opt/app/logs`
- B. `chattr +d /opt/app/logs`
- C. `chattr +i /opt/app/logs`
- D. `chattr +c /opt/app/logs`

Answer: A

Explanation:

The command `chattr +a /opt/app/logs` will ensure the log file can only be written into without removing previous entries. The `chattr` command is a tool for changing file attributes on Linux file systems. The `+a` option sets the append-only attribute, which means that the file can only be opened in append mode for writing. This prevents the file from being modified, deleted, or renamed. This is the best command to use to accomplish the task. The other options are incorrect because they either set the wrong attributes

(`+d`, `+i`, or `+c`) or do not affect the file at all (`-a`). References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 11: Managing Files and Directories, page 357.

NEW QUESTION 69

A Linux administrator needs to determine whether a hostname is in the DNS. Which of the following would supply the information that is needed?

- A. `nslookup`
- B. `rsyn`
- C. `netstat`
- D. `host`

Answer: A

Explanation:

The commands nslookup or host can be used to determine whether a hostname is in the DNS. The DNS is the domain name system, which is a service that translates domain names into IP addresses and vice versa. The nslookup command is a tool for querying the DNS and obtaining information about a domain name or an IP address. The host command is a similar tool that performs DNS lookups. Both commands can be used to check if a hostname is in the DNS by providing the hostname as an argument and seeing if the command returns a valid IP address or an error message. For example, the command nslookup www.google.com or host www.google.com will return the IP address of the Google website, while the command nslookup www.nosuchdomain.com or host www.nosuchdomain.com will return an error message indicating that the hostname does not exist. These commands will supply the information that is needed to determine whether a hostname is in the DNS. These are the correct commands to use for this task. The other options are incorrect because they do not query the DNS or obtain information about a hostname (rsync or netstat). References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 12: Managing Network Connections, page 378.

NEW QUESTION 70

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

- A. Kill the process with PID 1.
- B. Kill the PID of the processes.
- C. Kill the parent PID of the processes.
- D. Reboot the server.

Answer: C

Explanation:

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

References

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

NEW QUESTION 75

A systems administrator is encountering performance issues. The administrator runs 3 commands with the following output

```
09:10:18 up 457 days, 32min, 5 users, load average: 4.22 6.63 5.98
```

The Linux server has the following system properties CPU: 4 vCPU

Memory: 50GB

Which of the following accurately describes this situation?

- A. The system is under CPU pressure and will require additional vCPUs
- B. The system has been running for over a year and requires a reboot.
- C. Too many users are currently logged in to the system
- D. The system requires more memory

Answer: A

Explanation:

Based on the output of the image sent by the user, the system is under CPU pressure and will require additional vCPUs. The output shows that there are four processes running upload.sh scripts that are consuming a high percentage of CPU time (99.7%, 99.6%, 99.5%, and 99.4%). The output also shows that the system has only 4 vCPUs, which means that each process is using almost one entire vCPU. This indicates that the system is struggling to handle the CPU load and may experience performance issues or slowdowns. Adding more vCPUs to the system would help to alleviate the CPU pressure and improve the system performance. The system has not been running for over a year, as the uptime command shows that it has been up for only 1 day, 2 hours, and 13 minutes. The number of users logged in to the system is not relevant to the performance issue, as they are not consuming significant CPU resources. The system does not require more memory, as the free command shows that it has plenty of available memory (49 GB total, 48 GB free). References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 15: Managing Memory and Process Execution, pages 468-469.

NEW QUESTION 78

A Linux administrator has set up a new DNS forwarder and is configuring all internal servers to use the new forwarder to look up external DNS requests. The administrator needs to modify the firewall on the server for the DNS forwarder to allow the internal servers to communicate to it and make the changes persistent between server reboots. Which of the following commands should be run on the DNS forwarder server to accomplish this task?

- A. ufw allow out dns
- B. systemctl reload firewalld
- C. iptables -A OUTPUT -p udp -ra udp -dport 53 -j ACCEPT
- D. firewall-cmd --zone=public --add-port=53/udp --permanent

Answer: D

Explanation:

The command that should be run on the DNS forwarder server to accomplish the task is firewall-cmd --zone=public --add-port=53/udp --permanent.

The firewall-cmd command is a tool for managing firewalld, which is a firewall service that provides dynamic and persistent network security on Linux systems. The firewalld uses zones and services to define the rules and policies for the network traffic. The zones are logical groups of network interfaces and sources that have the same level of trust and security. The services are predefined sets of ports and protocols that are associated with certain applications or functions. The --zone=public option specifies the zone name that the rule applies to. The public zone is the default zone that represents the untrusted network, such as the internet. The --add-port=53/udp option adds a port and protocol to the zone. The 53 is the port number that is used by the DNS service. The udp is the protocol that is used by the DNS service. The --permanent option makes the change persistent across reboots. The command firewall-cmd --zone=public --add-port=53/udp --permanent will modify the firewall on the server for the DNS forwarder to allow the internal servers to communicate to it and make the changes persistent

between server reboots. This is the correct command to use to accomplish the task. The other options are incorrect because they either do not modify the firewall on the server for the DNS forwarder (ufw allow out dns or systemctl reload firewall) or do not use the correct syntax for the command (iptables -A OUTPUT -p udp -ra udp -dport 53 -j ACCEPT instead of iptables -A OUTPUT - p udp -ra udp --dport 53 -j ACCEPT). References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 12: Managing Network Connections, page 392.

NEW QUESTION 81

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 86

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 87

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

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

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

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

- A. Reboot the serve
- B. The volume will automatically go back to linear mode.
- C. Replace the failed drive and reconfigure the mirror.
- D. Reboot the serve
- E. The volume will revert to stripe mode.
- F. Recreate the logical volume.

Answer: B

Explanation:

The administrator should replace the failed drive and reconfigure the mirror to recover the volume. The LVM (Logical Volume Manager) is a tool for managing disk

space on Linux systems. The LVM allows the administrator to create logical volumes that span across multiple physical volumes, such as hard disks or partitions. The LVM also supports different types of logical volumes, such as linear, striped, or mirrored. A mirrored logical volume is a type of logical volume that creates a copy of the data on another physical volume, providing redundancy and fault tolerance. The output shows that the logical volume is mirrored and that one leg of the mirror has failed due to the underlying physical volume. This means that one of the physical volumes that contains the data of the logical volume is damaged or missing. This can cause data loss and performance degradation. The administrator should replace the failed drive and reconfigure the mirror to recover the volume. The administrator should identify the failed physical volume by using commands such as `pvdisplay`, `vgdisplay`, or `lvdisplay`. The administrator should then remove the failed physical volume from the volume group by using the `vgreduce` command.

The administrator should then install a new drive and create a new physical volume by using the `pvcreate` command. The administrator should then add the new physical volume to the volume group by using the `vgextend` command. The administrator should then reconfigure the mirror by using the `lvconvert` command. The administrator should replace the failed drive and reconfigure the mirror to recover the volume. This is the correct answer to the question. The other options are incorrect because they either do not recover the volume (reboot the server. The volume will automatically go back to linear mode or reboot the server. The volume will revert to stripe mode) or do not preserve the data of the volume (recreate the logical volume). References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 10: Managing Storage, pages 333-334.

NEW QUESTION 90

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 91

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 94

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 98

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/lsscsi2>: <https://www.golinuxcloud.com/check-disk-type-linux/>

NEW QUESTION 101

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 103

A junior systems administrator has just generated public and private authentication keys for passwordless login. Which of the following files will be moved to the remote servers?

- A. id_dsa.pem
- B. id_rsa
- C. id_ecdsa
- D. id_rsa.pub

Answer: D

Explanation:

The file id_rsa.pub will be moved to the remote servers for passwordless login. The id_rsa.pub file is the public authentication key that is generated by the ssh-keygen command. The public key can be copied to the remote servers by using the ssh-copy-id command or manually. The remote servers will use the public key to authenticate the user who has the corresponding private key (id_rsa). This will allow the user to log in without entering a password. The other options are incorrect because they are either private keys (id_rsa, id_dsa.pem, or id_ecdsa) or non-existent files (id_dsa.pem or id_ecdsa). References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 13: Managing Network Services, page 410.

NEW QUESTION 108

A Linux administrator needs to create a new cloud.cpio archive containing all the files from the current directory. Which of the following commands can help to accomplish this task?

- A. ls | cpio -iv > cloud.cpio
- B. ls | cpio -iv < cloud.cpio
- C. ls | cpio -ov > cloud.cpio
- D. ls cpio -ov < cloud.cpio

Answer: C

Explanation:

The command ls | cpio -ov > cloud.cpio can help to create a new cloud.cpio archive containing all the files from the current directory. The ls command lists the files in the current directory and outputs them to the standard output. The | operator pipes the output to the next command. The cpio command is a tool for creating and extracting compressed archives. The -o option creates a new archive and the -v option shows the verbose output. The > operator redirects the output to the cloud.cpio file. This command will create a new cloud.cpio archive with all the files from the current directory. The other options are incorrect because they either use the wrong options (-i instead of -o), the wrong arguments (cloud.epio instead of cloud.cpio), or the wrong syntax (< instead of > or missing |). References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 11: Managing Files and Directories, page 351.

NEW QUESTION 110

Employees in the finance department are having trouble accessing the file /opt/work/file. All IT employees can read and write the file. Systems administrator reviews the following output:

```
admin@server:/opt/work$ ls -al file
-rw-rw----+ 1 root it 4 Sep 5 17:29 file
```

Which of the following commands would permanently fix the access issue while limiting access to IT and finance department employees?

- A. chattr +i file
- B. chown it:finance file
- C. chmod 666 file
- D. setfacl -m g:finance:rw file

Answer: D

Explanation:

The command setfacl -m g:finance:rw file will permanently fix the access issue while limiting access to IT and finance department employees. The setfacl

command is a tool for modifying the access control lists (ACLs) of files and directories on Linux systems. The ACLs are a mechanism that allows more fine-grained control over the permissions of files and directories than the traditional owner-group-others model. The `-m` option specifies the modification to the ACL. The `g:finance:rw` means that the group named finance will have read and write permissions on the file. The file is the name of the file to modify, in this case `/opt/work/file`. The command `setfacl -m g:finance:rw file` will add an entry to the ACL of the file that will grant read and write access to the finance group. This will fix the access issue and allow the finance employees to access the file. The command will also preserve the existing permissions of the file, which means that the IT employees will still have read and write access to the file. This will limit the access to IT and finance department employees and prevent unauthorized access from other users.

This is the correct command to use to accomplish the task. The other options are incorrect because they either do not fix the access issue (`chattr +i file` or `chown it:finance file`) or do not limit the access to IT and finance department employees (`chmod 666 file`). References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 11: Managing File Permissions and Ownership, page 352.

NEW QUESTION 112

After listing the properties of a system account, a systems administrator wants to remove the expiration date of a user account. Which of the following commands will accomplish this task?

- A. `chgrp system accountname`
- B. `passwd -s accountname`
- C. `chmod -G system account name`
- D. `chage -E -1 accountname`

Answer: D

Explanation:

The command `chage -E -1 accountname` will accomplish the task of removing the expiration date of a user account. The `chage` command is a tool for changing user password aging information on Linux systems. The `-E` option sets the expiration date of the user account, and the `-1` value means that the account will never expire. The command `chage -E -1 accountname` will remove the expiration date of the user account named `accountname`. This is the correct command to use to accomplish the task. The

other options are incorrect because they either do not affect the expiration date (`chgrp`, `passwd`, or `chmod`) or do not exist (`chmod -G`). References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 15: Managing Users and Groups, page 467.

NEW QUESTION 117

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 121

A senior Linux administrator has created several scripts that will be used to install common system applications. These scripts are published to a repository to share with the systems team. A junior Linux administrator needs to retrieve the scripts and make them available on a local workstation. Which of the following Git commands should the junior Linux administrator use to accomplish this task?

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

Answer: C

Explanation:

To retrieve the scripts from a repository and make them available on a local workstation, the junior Linux administrator can use the command `git clone @`. This will create a copy of the repository on the local machine, including all the scripts and history. The other commands will not clone the repository, but either `fetch`, `checkout`, or `branch` from an existing repository. References:

? [CompTIA Linux+ Study Guide], Chapter 10: Working with Git, Section: Cloning Repositories with Git

? [How to Clone a Git Repository]

NEW QUESTION 125

A Linux system is failing to boot. The following error is displayed in the serial console: `[[1;33mDEPEND[Om] Dependency failed for /data. [[1;33mDEPEND[Om] Dependency failed for Local File Systems`

...

Welcome to emergency mode! After logging in, type `"journalctl -xb"` to view system logs, `"systemctl reboot"` to reboot, `"systemctl default"` to try again to boot into default mode. Give root password for maintenance (or type Control-D to continue)

Which of the following files will need to be modified for this server to be able to boot again?

- A. `/etc/mtab`
- B. `/dev/sda`
- C. `/etc/fstab`
- D. `/etc/grub.conf`

Answer: C

Explanation:

The file that will need to be modified for the server to be able to boot again is `/etc/fstab`. The `/etc/fstab` file is a file that contains the information about the file systems that are mounted at boot time on Linux systems. The file specifies the device name, mount point, file system type, mount options, dump frequency, and pass number for each file system. The error message indicates that the dependency failed for `/data`, which is a mount point for a file system. This means that the system could not mount the `/data` file system at boot time, which caused the system to enter the emergency mode. The emergency mode is a mode that allows the administrator to log in as the root user and perform basic tasks such as repairing the system. The administrator should modify the `/etc/fstab` file and check the entry for the `/data` file system. The administrator should look for any errors or inconsistencies in the device name, file system type, or mount options, and correct them. The administrator should also verify that the device and the file system are intact and functional by using commands such as `blkid`, `fdisk`, `fsck`, or `mount`. The administrator should then reboot the system and see if the issue is resolved. The file that will need to be modified for the server to be able to boot again is `/etc/fstab`. This is the correct answer to the question. The other options are incorrect because they are not related to the file systems that are mounted at boot time (`/etc/mtab`, `/dev/sda`, or `/etc/grub.conf`). References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 10: Managing Storage, page 321.

NEW QUESTION 126

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

- A. `[root@nodea ssh -i ~/ . ssh/±d rsa root@nodeb`
- B. `[root@nodea scp -i . ssh/id rsa root@nodeb`
- C. `[root@nodea ssh-copy-id -i .ssh/id rsa root@nodeb`
- D. `[root@nodea # ssh add -c ~/ . ssh/id rsa root@nodeb`
- E. `[root@nodea # ssh add -c ~/ . ssh/id rsa root@nodeb`

Answer: C

Explanation:

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

NEW QUESTION 129

Which of the following technologies can be used as a central repository of Linux users and groups?

- A. LDAP
- B. MFA
- C. SSO
- D. PAM

Answer: A

Explanation:

LDAP stands for Lightweight Directory Access Protocol, which is a protocol for accessing and managing a central directory of users and groups. LDAP can be used as a central repository of Linux users and groups, allowing for centralized authentication and authorization across multiple Linux systems. MFA, SSO, and PAM are not technologies that can be used as a central repository of Linux users and groups. MFA stands for Multi-Factor Authentication, which is a method of verifying a user's identity using more than one factor, such as a password, a token, or a biometric. SSO stands for Single Sign-On, which is a feature that allows a user to log in once and access multiple applications or systems without having to re-enter credentials. PAM stands for Pluggable Authentication Modules, which is a framework that allows Linux to use different authentication methods, such as passwords, tokens, or biometrics. References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 8: Managing Users and Groups

NEW QUESTION 132

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    tcp dpt:22 ctstate NEW, UNTRACKED
           reject-with icmp-port-unreachable
REJECT    tcp    --    222.186.180.130  0.0.0.0/0    tcp dpt:22 ctstate NEW, UNTRACKED
           reject-with icmp-port-unreachable
REJECT    tcp    --    104.131.1.39    0.0.0.0/0    tcp dpt:22 ctstate NEW, UNTRACKED
           reject-with icmp-port-unreachable
REJECT    tcp    --    68.183.196.11  0.0.0.0/0    tcp dpt:22 ctstate NEW, UNTRACKED
           reject-with icmp-port-unreachable
REJECT    tcp    --    5.189.153.89   0.0.0.0/0    tcp dpt:22 ctstate NEW, UNTRACKED
           reject-with icmp-port-unreachable
REJECT    tcp    --    41.93.32.148   0.0.0.0/0    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 mg 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 134

A user is asking the systems administrator for assistance with writing a script to verify whether a file exists. Given the following:

```
#!/bin/bash
filename=$1
<CONDITIONAL>
echo "File exists"
else
echo "File does not exist"
fi
```

Which of the following commands should replace the <CONDITIONAL> string?

- A. `if [-f "$filename"]; then`
- B. `if [-d "$filename"]; then`
- C. `if [-f "$filename"] then`
- D. `if [-f "$filename"]; while`

Answer: A

Explanation:

The command `if [-f "$filename"]; then` checks if the variable `$filename` refers to a regular file that exists. The `-f` option is used to test for files. If the condition is true, the commands after then are executed. This is the correct way to replace the <CONDITIONAL> string. The other options are incorrect because they either

use the wrong option (-d tests for directories), the wrong syntax (missing a semicolon after the condition), or the wrong keyword (while is used for loops, not conditions). References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 16: Writing and Executing Bash Shell Scripts, page 493.

NEW QUESTION 137

At what point is the Internal Certificate Authority (ICA) created?

- A. During the primary Security Management Server installation process.
- B. Upon creation of a certificate.
- C. When an administrator decides to create one.
- D. When an administrator initially logs into SmartConsole.

Answer: A

Explanation:

The Internal Certificate Authority (ICA) is created during the primary Security Management Server installation process. The ICA is a component of Check Point's Public Key Infrastructure (PKI) that issues and manages certificates for Security Gateways and administrators. The ICA is automatically installed and initialized when the primary Security Management Server is installed. The ICA is not created upon creation of a certificate, when an administrator decides to create one, or when an administrator initially logs into SmartConsole. References: Check Point Certified Security Administrator (CCSA) R80.x Study Guide, Chapter 3: Check Point Security Management Architecture, page 32.

NEW QUESTION 141

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 142

A Linux administrator rebooted a server. Users then reported some of their files were missing. After doing some troubleshooting, the administrator found one of the filesystems was missing. The filesystem was not listed in /etc/fstab and might have been mounted manually by someone prior to reboot. Which of the following would prevent this issue from reoccurring in the future?

- A. Sync the mount units.
- B. Mount the filesystem manually.
- C. Create a mount unit and enable it to be started at boot.
- D. Remount all the missing filesystems

Answer: C

Explanation:

The best way to prevent this issue from reoccurring in the future is to create a mount unit and enable it to be started at boot. A mount unit is a systemd unit that defines how and where a filesystem should be mounted. By creating a mount unit for the missing filesystem and enabling it with `systemctl enable`, the administrator can ensure that the filesystem will be automatically mounted at boot time, regardless of whether it is listed in /etc/fstab or not. Syncing the mount units will not prevent the issue, as it will only synchronize the state of existing mount units with /etc/fstab, not create new ones. Mounting the filesystem manually will not prevent the issue, as it will only mount the filesystem temporarily, not permanently. Remounting all the missing filesystems will not prevent the issue, as it will only mount the filesystems until the next reboot, not after. References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 14: Managing Disk Storage, page 457.

NEW QUESTION 143

A systems administrator has been tasked with disabling the nginx service from the environment to prevent it from being automatically and manually started. Which of the following commands will accomplish this task?

- A. `systemctl cancel nginx`
- B. `systemctl disable nginx`
- C. `systemctl mask nginx`
- D. `systemctl stop nginx`

Answer: C

Explanation:

The command `systemctl mask nginx` disables the nginx service from the environment and prevents it from being automatically and manually started. This command creates a symbolic link from the service unit file to `/dev/null`, which makes the service impossible to start. This is the correct way to accomplish the task. The other options are incorrect because they either do not exist (`systemctl cancel nginx`), do not prevent manual start (`systemctl disable nginx`), or do not prevent automatic start (`systemctl stop nginx`). References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 14: Managing Processes and Scheduling Tasks, page 429.

NEW QUESTION 146

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 `ExecStart=/usr/sbin/webserver -D $OPTIONS` from the service file
- B. Updating the Environment File line in the `[Service]` section to `/home/webserver/config`
- C. Adding the `User=webserver` to the `[Service]` section of the service file
- D. Changing the `WantedBy=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=webserver` 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 `webserver` is the name of the user that the administrator wants to run the web service as. The administrator should add the `User=webserver` 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 Environment File line in the `[Service]` section to `/home/webserver/config`) or do not affect the user that the service runs as (changing the `WantedBy=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 148

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 153

A Linux administrator needs to create a symlink for `/usr/local/bin/app-a`, which was installed in `/usr/local/share/app-a`. Which of the following commands should the

administrator use?

- A. `ln -s /usr/local/bin/app-a /usr/local/share/app-a`
- B. `mv -f /usr/local/share/app-a /usr/local/bin/app-a`
- C. `cp -f /usr/local/share/app-a /usr/local/bin/app-a`
- D. `rsync -a /usr/local/share/app-a /usr/local/bin/app-a`

Answer: A

Explanation:

To create a symlink for `/usr/local/bin/app-a`, which was installed in `/usr/local/share/app-a`, the administrator can use the command `ln -s /usr/local/share/app-a /usr/local/bin/app-a` (A). This will create a symbolic link named `/usr/local/bin/app-a` that points to the original file `/usr/local/share/app-a`. The other commands will not create a symlink, but either move, copy, or synchronize the file. References:

? [CompTIA Linux+ Study Guide], Chapter 3: Working with Files, Section: Creating Links

? [How to Create Symbolic Links in Linux]

NEW QUESTION 156

A systems administrator is troubleshooting connectivity issues and trying to find out why a Linux server is not able to reach other servers on the same subnet it is connected to. When listing link parameters, the following is presented:

```
# ip link list dev eth0
2: eth0: <NO-CARRIER, BROADCAST, MULTICAST, UP> mtu 1500, qdisc
fq_codel state DOWN mode DEFAULT group default qlen 1000
link/ether ac:00:11:22:33:cd brd ff:ff:ff:ff:ff:ff
```

Based on the output above, which of following is the MOST probable cause of the issue?

- A. The address `ac:00:11:22:33:cd` is not a valid Ethernet address.
- B. The Ethernet broadcast address should be `ac:00:11:22:33:ff` instead.
- C. The network interface `eth0` is using an old kernel module.
- D. The network interface cable is not connected to a switch.

Answer: D

Explanation:

The most probable cause of the connectivity issue is that the network interface cable is not connected to a switch. This can be inferred from the output of the `ip link list dev eth0` command, which shows that the network interface `eth0` has the `NO-CARRIER` flag set. This flag indicates that there is no physical link detected on the interface, meaning that the cable is either unplugged or faulty. The other options are not valid causes of the issue. The address `ac:00:11:22:33:cd` is a valid Ethernet address, as it follows the format of six hexadecimal octets separated by colons. The Ethernet broadcast address should be `ff:ff:ff:ff:ff:ff`, which is the default value for all interfaces. The network interface `eth0` is not using an old kernel module, as it shows the `UP` flag, which indicates that the interface is enabled and ready to transmit data. References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 14: Managing Networking

NEW QUESTION 157

A Linux administrator booted up the server and was presented with a non-GUI terminal. The administrator ran the command `systemctl isolate graphical.target` and rebooted the system by running `systemctl reboot`, which fixed the issue. However, the next day the administrator was presented again with a non-GUI terminal. Which of the following is the issue?

- A. The administrator did not reboot the server properly.
- B. The administrator did not set the default target to `basic.target`.
- C. The administrator did not set the default target to `graphical.target`.
- D. The administrator did not shut down the server properly.

Answer: C

Explanation:

The issue is that the administrator did not set the default target to `graphical.target`. A target is a unit of `systemd` that groups together other units by a common purpose or state. The `graphical.target` is a target that starts the graphical user interface (GUI) along with other services. The administrator used the command `systemctl isolate graphical.target` to switch to this target temporarily, but this does not change the default target that is activated at boot time. To make this change permanent, the administrator should have used the command `systemctl set-default graphical.target`, which creates a symbolic link from `/etc/systemd/system/default.target` to `/usr/lib/systemd/system/graphical.target`.

The other options are not correct explanations for the issue. The administrator did reboot the server properly by using `systemctl reboot`, which shuts down and restarts the system cleanly. The administrator did not need to set the default target to `basic.target`, which is a minimal target that only starts essential services. The administrator did not shut down the server improperly, which could have caused file system corruption or data loss, but not affect the default target. References: `systemctl(1)` - Linux manual page; How to Change Runlevels (targets) in SystemD

NEW QUESTION 160

A Linux administrator is providing a new Nginx image from the registry to local cache. Which of the following commands would allow this to happen?

- A. `docker pull nginx`
- B. `docker attach nginx`
- C. `docker commit nginx`
- D. `docker import nginx`

Answer: A

Explanation:

The command that would allow this to happen is `docker pull nginx`. Docker is a software platform that allows the administrator to create, run, and manage containers on Linux systems. 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. Docker uses a registry to store and distribute images, which is a service that hosts and serves images. Docker Hub is the default public registry that provides a large number of official and community images. Nginx is a popular web server and reverse proxy that can run as a container. The command `docker pull nginx` will download the latest version of the Nginx image from the Docker Hub registry to the local cache, which is the storage location for the images on the host system. This will allow the administrator to provide a new Nginx image from the registry to the local cache. This is the correct command to use to accomplish the task. The other options are incorrect because they either do not download an image from the registry (`docker attach nginx` or `docker commit nginx`) or do not exist (`docker import nginx`). References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 19: Managing Cloud and Virtualization Technologies, page 571.

NEW QUESTION 164

As part of the requirements for installing a new application, the `swappiness` parameter needs to be changed to 0. This change needs to persist across re-boots and be applied immediately. A Linux systems administrator is performing this change. Which of the following steps should the administrator complete to accomplish this task?

- A. `echo "v`
- B. `swappiness—()" >> /etc/sysctl . conf && sysctl —p`
- C. `echo "vr`
- D. `>> / proc/meminfo && sysctl —a`
- E. `sysctl —v >> / proc/meminfo & & echo "v`
- F. `swappiness=0"`
- G. `sysctl —h "v`
- H. `swappiness—O" && echo / etc/vmswappiness`

Answer: A

Explanation:

To change the `swappiness` parameter to 0 and make it persistent across reboots and applied immediately, the administrator can perform the following steps:

? Append the line `vm.swappiness=0` to the file `/etc/sysctl.conf` using `echo`

`"vm.swappiness=0" >> /etc/sysctl.conf` (A). This will set the `swappiness` parameter to 0 for future boots.

? Reload the `sysctl` configuration using `sysctl -p` (A). This will apply the changes to the current system without rebooting. The other commands will not achieve this task, but either write to a wrong file, use a wrong option, or have a syntax error. References:

? [CompTIA Linux+ Study Guide], Chapter 8: Optimizing Linux Performance, Section: Tuning Kernel Parameters with `sysctl`

? [How to Change Swappiness in Linux]

NEW QUESTION 165

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 166

A Linux administrator needs to create a new user named `user02`. However, `user02` must be in a different home directory, which is under `/comptia/projects`. Which of the following commands will accomplish this task?

- A. `useradd -d /comptia/projects user02`
- B. `useradd -m /comptia/projects user02`
- C. `useradd -b /comptia/projects user02`
- D. `useradd -s /comptia/projects user02`

Answer: A

Explanation:

The command `useradd -d /comptia/projects user02` will accomplish the task of creating a new user named `user02` with a different home directory.

The `useradd` command is a tool for creating new user accounts on Linux systems. The `-d` option specifies the home directory for the new user, which is the directory where the user's personal files and settings are stored. The `/comptia/projects` is the path of the home directory for the new user, which is different from the default location of `/home/user02`.

The `user02` is the name of the new user. The command `useradd -d /comptia/projects user02` will create a new user named `user02` with a home directory under `/comptia/projects`. This is the correct command to use to accomplish the task. The other options are incorrect because they either do not specify the home directory for the new user (`useradd -m /comptia/projects user02` or `useradd -s /comptia/projects user02`) or do not use the correct option for the home directory (`useradd -b /comptia/projects user02` instead of `useradd -d /comptia/projects user02`). References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 13: Managing Users and Groups, page 403.

NEW QUESTION 167

Ann, a security administrator, is performing home directory audits on a Linux server. Ann issues the `su Joe` command and then issues the `ls` command. The output displays files that reside in Ann's home directory instead of Joe's. Which of the following represents the command Ann should have issued in order to list Joe's files?

- A. `su - Joe`
- B. `sudo Joe`
- C. `visudo Joe`
- D. `pkexec joe`

Answer: A

Explanation:

The `su` command is used to switch to another user account on Linux systems. The `-` option makes the shell a login shell, which means that it will read the profile and environment variables of the target user. Without this option, the shell will retain the environment variables of the original user. This can cause confusion when issuing commands that depend on these variables, such as `ls`, which uses the `$HOME` variable to determine the home directory. Therefore, Ann should have issued `su - Joe` to list Joe's files instead of her own. References: [How to Use `su` Command in Linux with Examples]

NEW QUESTION 171

A file called `testfile` has both uppercase and lowercase letters:

```
$ cat testfile ABCDEfgH
```

```
IJKLmnoPQ abcdefgh ijklMNopq
```

A Linux administrator is tasked with converting `testfile` into all uppercase and writing it to a new file with the name `uppercase`. Which of the following commands will achieve this task?

- A. `tr '(A-Z)' '{a-z}' < testfile > uppercase`
- B. `echo testfile | tr "[Z-A]" "[z-a]" < testfile > uppercase`
- C. `cat testfile | tr '{z-a}' '{Z-A}' < testfile > uppercase`
- D. `tr '[a-z]' '[A-Z]' < testfile > uppercase`

Answer: D

Explanation:

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

References: 1: Linux Tr Command - javatpoint 2: Linux tr Command with Examples - phoenixNAP

NEW QUESTION 172

Which of the following tools is BEST suited to orchestrate a large number of containers across many different servers?

- A. Kubernetes
- B. Ansible
- C. Podman
- D. Terraform

Answer: A

Explanation:

The tool that is best suited to orchestrate a large number of containers across many different servers is Kubernetes. Kubernetes is an open-source platform for managing containerized applications and services. Kubernetes allows the administrator to deploy, scale, and update containers across a cluster of servers, as well as to automate the configuration and coordination of the containers. Kubernetes also provides features such as service discovery, load balancing, storage management, security, monitoring, and logging. Kubernetes can handle complex and dynamic workloads and ensure high availability and performance of the containers. Kubernetes is the tool that is best suited to orchestrate a large number of containers across many different servers. This is the correct answer to the question. The other options are incorrect because they either do not orchestrate containers (Ansible or Terraform) or do not operate across many different servers (Podman). References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 19: Managing Cloud and Virtualization Technologies, page 573.

NEW QUESTION 176

A Linux administrator was tasked with deleting all files and directories with names that are contained in the `sobelete.txt` file. Which of the following commands will accomplish this task?

- A. `xargs -f cat toDelete.txt -rm`
- B. `rm -d -r -f toDelete.txt`
- C. `cat toDelete.txt | rm -frd`
- D. `cat toDelete.txt | xargs rm -rf`

Answer: D

Explanation:

The command `cat toDelete.txt | xargs rm -rf` will delete all files and directories with names that are contained in the `toDelete.txt` file. The `cat` command reads the file and outputs its contents to the standard output. The `|` operator pipes the output to the next command. The `xargs` command converts the output into arguments for the next command. The `rm -rf` command removes the files and directories recursively and forcefully. This is the correct way to accomplish the task. The other options are incorrect because they either use the wrong options (`-f` instead of `-a` for `xargs`), the wrong arguments (`toDelete.txt` instead of `toDelete.txt` filename for `rm`), or the wrong commands (`rm` instead of `xargs`). References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 11: Managing Files and Directories, pages 349-350.

NEW QUESTION 181

A systems administrator detected corruption in the `/data` filesystem. Given the following output:

```
root@localhost ~]# lsblk -f
```

NAME	FSTYPE	LABEL/UUID	MOUNTPOINT
sda			
└─sda1	vfat	4E7D-9539	/boot/efi
└─sda2	xfs	98442caf-473d-448e-ae5-561a82297314	/boot
└─sda3	swap	19f064e4-7c51-4b02-8219-99362a3c45ec	[SWAP]
└─sda4	xfs	25d96ada-4289-4def-9202-6ab11affbed3	/
└─sda5	xfs	61435ee9-855d-4de9-9c67-39aeb7f3edb5	/home
sdc			
└─sdcl	ext4	92435ff9-745e-4fg9-9c67-39aeb7f3exf5	/data

Which of the following commands can the administrator use to best address this issue?

- A. umount /data mkfs . xfs /dev/sdcl mount /data
- B. umount /data xfs repair /dev/ sdcl mount /data
- C. umount /data fsck /dev/ sdcl mount / data
- D. umount /data pvs /dev/sdcl mount /data

Answer: B

Explanation:

The xfs repair command is used to check and repair an XFS filesystem, which is the type of filesystem used for the /data partition, as shown in the output. The administrator needs to unmount the /data partition before running the xfs repair command on it, and then mount it back after the repair is done. For example: umount /data; xfs_repair /dev/sdcl; mount /data. The mkfs.xfs command is used to create a new XFS filesystem, which would erase all the data on the partition. The fsck command is used to check and repair other types of filesystems, such as ext4, but not XFS. The pvs command is used to display information about physical volumes in a logical volume manager (LVM) setup, which is not relevant for this issue.

NEW QUESTION 185

A systems administrator is notified that the mysqld process stopped unexpectedly. The systems administrator issues the following command: sudo grep -i -r 'out of memory' /var/log

The output of the command shows the following:

kernel: Out of memory: Kill process 9112 (mysqld) score 511 or sacrifice child.

Which of the following commands should the systems administrator execute NEXT to troubleshoot this issue? (Select two).

- A. free -h
- B. nc -v 127.0.0.1 3306
- C. renice -15 \$(pidof mysql)
- D. lsblk
- E. killall -15
- F. vmstat -a 1 4

Answer: AF

Explanation:

The free -h command can be used to check the amount of free and used memory in the system in a human-readable format. This can help to troubleshoot the issue of mysqld being killed due to out of memory. The vmstat -a 1 4 command can be used to monitor the system's virtual memory statistics, such as swap usage, paging activity, and memory faults, every one second for four times. This can help to identify any memory pressure or performance issues that may cause out of memory errors. The nc -v 127.0.0.1 3306 command would attempt to connect to the MySQL server on port 3306 and display any diagnostic messages, but this would not help to troubleshoot the memory issue. The renice -15 \$(pidof mysql) command would change the priority of the mysql process to -15, but this would not prevent it from being killed due to out of memory. The lsblk command would display information about block devices, not memory usage. The killall -15 command would send a SIGTERM signal to all processes with a matching name, but this would not help to troubleshoot the memory issue. References: [CompTIA Linux+ (XK0-005) Certification Study Guide], Chapter 15: Managing Memory and Process Execution, pages 468-469.

NEW QUESTION 187

A Linux administrator has logged in to a server for the first time and needs to know which services are allowed through the firewall. Which of the following options will return the results for which the administrator is looking?

- A. firewall-cmd --get-services
- B. firewall-cmd --check-config
- C. firewall-cmd --list-services
- D. systemctl status firewalld

Answer: C

Explanation:

The firewall-cmd --list-services command will return the results for which the administrator is looking. This command will list all services that are allowed through the firewall in the default zone or a specified zone. A service is a predefined set of ports and protocols that can be enabled or disabled by firewalld. The firewall-cmd --get-services command will list all available services that are supported by firewalld, not only those that are allowed through the firewall. The firewall-cmd --check-config command will check if firewalld configuration files are valid, not list services. The systemctl status firewalld command will display information about the firewalld service unit, such as its state, PID, memory usage, and logs, not list services. References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 18: Securing Linux Systems, page 543.

NEW QUESTION 188

A Linux administrator would like to use systemd to schedule a job to run every two hours. The administrator creates timer and service definitions and restarts the server to load these new configurations. After the restart, the administrator checks the log file and notices that the job is only running daily. Which of the following is MOST likely causing the issue?

- A. The checkdiskspace.service is not running.
- B. The checkdiskspace.service needs to be enabled.
- C. The OnCalendar schedule is incorrect in the timer definition.
- D. The system-daemon services need to be reloaded.

Answer: C

Explanation:

The OnCalendar schedule is incorrect in the timer definition, which is causing the issue. The OnCalendar schedule defines when the timer should trigger the service. The format of the schedule is OnCalendar=<year>-<month>-<day> <hour>:<minute>:<second>. If any of the fields are omitted, they are assumed to be *, which means any value. Therefore, the schedule OnCalendar=*-*-* 00:00:00 means every day at midnight, which is why the job is running daily. To make the job run every two hours, the schedule should be OnCalendar=*-*-* *:00:00/2, which means every hour divisible by 2 at the start of the minute. The other options are incorrect because they are not related to the schedule. The checkdiskspace.service is running, as shown by the output of systemctl status checkdiskspace.service. The checkdiskspace.service is enabled, as shown by the output of systemctl is-enabled checkdiskspace.service. The system-daemon services do not need to be reloaded, as the timer and service definitions are already loaded by the restart. References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 14: Managing Processes and Scheduling Tasks, page 437.

NEW QUESTION 190

An administrator attempts to rename a file on a server but receives the following error.

```
mv: cannot move 'files/readme.txt' to 'files/readme.txt.orig': Operation not permitted.
```

The administrator then runs a few commands and obtains the following output:

```
$ ls -ld files/
drwxrwxrwt.1  users  users  20   Sep 10
              15:15  files/

$ ls -a files/
drwxrwxrwt.1  users  users  20   Sep 10
              15:15  -
drwxr-xr-x.1  users  users  32   Sep 10
              15:15  ..
-rw-rw-r--.1  users  users   4   Sep 12
              10:34  readme.txt
```

Which of the following commands should the administrator run NEXT to allow the file to be renamed by any user?

- A. chgrp reet files
- B. chacl -R 644 files
- C. chown users files
- D. chmod -t files

Answer: D

Explanation:

The command that the administrator should run NEXT to allow the file to be renamed by any user is chmod -t files. This command uses the chmod tool, which is used to change file permissions and access modes. The -t option removes (or sets) the sticky bit on a directory, which restricts deletion or renaming of files within that directory to only their owners or root. In this case, since files is a directory with sticky bit set (indicated by t in drwxrwxrwt), removing it will allow any user to rename or delete files within that directory. The other options are not correct commands for allowing any user to rename files within files directory. The chgrp reet files command will change the group ownership of files directory to reet, but it will not affect its permissions or access modes. The chacl -R 644 files command is invalid, as chacl is used to change file access control lists (ACLs), not permissions or access modes. The chown users files command will change the user ownership of files directory to users, but it will not affect its permissions or access modes. References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 8: Managing Users and Groups; chmod(1) - Linux manual page

NEW QUESTION 193

A server is experiencing intermittent connection issues. Some connections to the Internet work as intended, but some fail as if there is no connectivity. The systems administrator inspects the server configuration:

Routing table:

```
default via 89.107.157.129 dev ens3 proto static metric 100
default via 10.0.5.1 dev ens11 proto dhcp metric 101
10.0.0.0/16 dev sn11 proto kernel scope link src 10.0.6.225 metric 101
89.107.157.128/26 via 89.107.157.129 dev ens3 proto static metric 100
89.107.157.129 dev ens3 proto static scope link metric 100
89.107.157.160/29 dev ens3 proto kernel scope link src 89.107.157.161 metric 100
```

IP configuration:

```
ens3:
  inet 89.107.157.161/29 brd 89.107.157.167 scope global noprefixroute ens3
ens11:
  inet 10.0.6.225/16 brd 10.0.255.255 scope global noprefixroute dynamic ens11
```

ARP table:

Address	Hwtype	Hwaddress	Flags	Mask	Iface
10.0.5.1	ether	64:d1:54:c4:75:cb	C		ens11
89.107.157.129	ether	5c:5e:ab:01:85:cf	C		ens3
89.107.157.162	ether	52:54:00:e1:44:0a	C		ens3
10.0.255.1	ether	00:50:7f:e3:aa:1c	C		ens11

```
/etc/resolv.conf:
Generated by NetworkManager
search company.com
nameserver 10.0.5.1
```

Which of the following is MOST likely the cause of the issue?

- A. An internal-only DNS server is configured.
- B. The IP netmask is wrong for ens3.
- C. Two default routes are configured.
- D. The ARP table contains incorrect entries.

Answer: C

Explanation:

The most likely cause of the issue is that two default routes are configured on the server. The default route is the route that is used when no other route matches the destination of a packet. The default route is usually the gateway that connects the local network to the Internet. The server configuration shows that there are two default routes in the routing table, one with the gateway 192.168.1.1 and the other with the gateway 10.0.0.1. This can cause a conflict and confusion for the server when deciding which gateway to use for the outgoing packets. Some packets may be sent to the wrong gateway and fail to reach the Internet, while some packets may be sent to the correct gateway and work as intended. This can result in intermittent connection issues and inconsistent behavior. The administrator should remove one of the default routes and keep only the correct one for the network. This can be done by using the `ip route del` command or by editing the network configuration files. This will resolve the issue and restore the connectivity. The other options are incorrect because they are not supported by the outputs. The DNS server, the IP netmask, and the ARP table are not the causes of the issue. References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 12: Managing Network Connections, pages 381-382.

NEW QUESTION 198

A junior administrator updated the PostgreSQL service unit file per the data-base administrator's recommendation. The service has been restarted, but changes have not been applied. Which of the following should the administrator run for the changes to take effect?

- A. `systemctl get—default`
- B. `systemctl daemon—reload`
- C. `systemctl enable postgresq1`
- D. `systemctl mask postgresq1`

Answer: B

Explanation:

To apply changes to a systemd service unit file, the administrator needs to reload the systemd daemon using the command `systemctl daemon-reload` (B). This will make systemd aware of the new or changed unit files. The other commands will not reload the systemd daemon or apply the changes. References: ? [CompTIA Linux+ Study Guide], Chapter 7: Managing System Services, Section: Modifying Systemd Services ? [How to Reload Systemd Services]

NEW QUESTION 199

A Linux administrator created a new file system. Which of the following files must be updated to ensure the filesystem mounts at boot time?

- A. `/etc/sysctl`
- B. `/etc/filesystems`
- C. `/etc/fstab`
- D. `/etc/nfsmount.conf`

Answer: C

Explanation:

The file that must be updated to ensure the filesystem mounts at boot time is `/etc/fstab`. This file contains information about the filesystems that are mounted

automatically by the `mount -a` command, which is usually invoked during the system startup. The `/etc/fstab` file has six fields for each filesystem: device name, mount point, filesystem type, mount options, dump frequency, and pass number. To add a new filesystem to the `/etc/fstab` file, you need to specify these fields correctly and make sure the mount point directory exists.

The other options are not correct files for controlling persistent mount points of filesystems. The `/etc/sysctl` file is used to configure kernel parameters at runtime. The `/etc/filesystems` file is used to specify the order of filesystem types used by `mount` when no filesystem type is given. The `/etc/nfsmount.conf` file is used to set options for mounting NFS

filesystems. References: Persistently mounting file systems; `fstab(5)` - Linux manual page

NEW QUESTION 204

When trying to log in remotely to a server, a user receives the following message:

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

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

Output 1:

```
user:xr1001:7374::/home/user:/bin/false
```

Output 2:

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

Output 3:

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

Which of the following is causing the issue?

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

Answer: D

Explanation:

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

NEW QUESTION 209

A systems administrator created a web server for the company and is required to add a tag for the API so end users can connect. Which of the following would the administrator do to complete this requirement?

- A. `hostnamectl status --no-ask-password`
- B. `hostnamectl set-hostname "$(perl -le "print" "A" x 86)"`
- C. `hostnamectl set-hostname Comptia-WebNode -H root@192.168.2.14`
- D. `hostnamectl set-hostname Comptia-WebNode --transient`

Answer: C

Explanation:

The command `hostnamectl set-hostname Comptia-WebNode -H root@192.168.2.14` sets the hostname of the web server to `Comptia-WebNode` and connects to the server using the SSH protocol and the root user. This is the correct way to complete the requirement. The other options are incorrect because they either display the current hostname status (`hostnamectl status`), set an invalid hostname (`hostnamectl set-hostname "$(perl -le "print" "A" x 86)"`), or set a transient hostname that is not persistent (`hostnamectl set-hostname Comptia-WebNode --transient`). References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 9: Managing System Components, page 291.

NEW QUESTION 210

Which of the following commands will display the operating system?

- A. `uname -n`
- B. `uname -s`
- C. `uname -o`
- D. `uname -m`

Answer: C

Explanation:

The command that will display the operating system is `uname -o`. This command uses the `uname` tool, which is used to print system information such as the kernel name, version, release, machine, and processor. The `-o` option stands for operating system, and prints the name of the operating system implementation (usually GNU/Linux). The other options are not correct commands for displaying the operating system. The `uname -n` command will display the network node hostname of the system. The `uname -s` command will display the kernel name of the system. The `uname -m` command will display the machine hardware name of the system. References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 1: Exploring Linux Command-Line Tools; `uname(1)` - Linux manual page

NEW QUESTION 211

A systems administrator has been unable to terminate a process. Which of the following should the administrator use to forcibly stop the process?

- A. kill -1
- B. kill -3
- C. kill -15
- D. kill -HUP
- E. kill -TERM

Answer: E

Explanation:

The administrator should use the command kill -TERM to forcibly stop the process. The kill command is a tool for sending signals to processes on Linux systems. Signals are messages that inform the processes about certain events and actions. The processes can react to the signals by performing predefined or user-defined actions, such as terminating, suspending, resuming, or ignoring. The -TERM option specifies the signal name or number that the kill command should send. The TERM signal, which stands for terminate, is the default signal that the kill command sends if no option is specified. The TERM signal requests the process to terminate gracefully, by closing any open files, releasing any resources, and performing any cleanup tasks. However, if the process does not respond to the TERM signal, the kill command can send a stronger signal, such as the KILL signal, which forces the process to terminate immediately, without any cleanup. The administrator should use the command kill -TERM to forcibly stop the process. This is the correct answer to the question. The other options are incorrect because they either do not terminate the process (kill -1 or kill -3) or do not terminate the process forcibly (kill -15 or kill -HUP). References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 14: Managing Processes, page 431.

NEW QUESTION 216

Based on an organization's new cybersecurity policies, an administrator has been instructed to ensure that, by default, all new users and groups that are created fall within the specified values below.

```
# Min/max values for automatic uid selection in useradd
#
UID_MIN 1000
UID_MAX 60000
# Min/max values for automatic gid selection in groupadd
#
GID_MIN 1000
GID_MAX 60000
```

To which of the following configuration files will the required changes need to be made?

- A. /etc/login.defs
- B. /etc/security/limits.conf
- C. /etc/default/useradd
- D. /etc/profile

Answer: A

Explanation:

The required changes need to be made to the /etc/login.defs configuration file. The /etc/login.defs file defines the default values for user and group IDs, passwords, shells, and other parameters for user and group creation. The file contains the directives UID_MIN, UID_MAX, GID_MIN, and GID_MAX, which set the minimum and maximum values for automatic user and group ID selection. The administrator can edit this file and change the values to match the organization's new cybersecurity policies. This is the correct file to modify to accomplish the task. The other options are incorrect because they either do not affect the user and group IDs (/etc/security/limits.conf or /etc/profile) or do not set the default values (/etc/default/useradd). References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 15: Managing Users and Groups, page 463.

NEW QUESTION 221

A developer reported an incident involving the application configuration file /etc/httpd/conf/httpd.conf that is missing from the server. Which of the following identifies the RPM package that installed the configuration file?

- A. rpm -qf /etc/httpd/conf/httpd.conf
- B. rpm -ql /etc/httpd/conf/httpd.conf
- C. rpm --query /etc/httpd/conf/httpd.conf
- D. rpm -q /etc/httpd/conf/httpd.conf

Answer: A

Explanation:

The rpm -qf /etc/httpd/conf/httpd.conf command will identify the RPM package that installed the configuration file. This command will query the database of installed packages and display the name of the package that owns the specified file. The rpm -ql /etc/httpd/conf/httpd.conf command is invalid, as -ql is not a valid option for rpm. The rpm --query /etc/httpd/conf/httpd.conf command is incorrect, as --query requires a package name, not a file name. The rpm -q /etc/httpd/conf/httpd.conf command is incorrect, as -q requires a package name, not a file name. References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 19: Managing Packages and Software, page 560.

NEW QUESTION 222

A systems administrator is investigating why one of the servers has stopped connecting to the internet.

```
#curl http://google.com
curl: (6) Could not resolve host: google.com

#cat /etc/resolv.conf
search user.company.com company.com
#nameserver 10.10.10.10

#ip route
0.0.0.0/0 via 10.0.5.1 dev eth0 proto static metric 100
10.0.0.0/16 dev eth0 proto kernel scope link src 10.0.3.60 metric 101

#nmcli connection show
NAME                UUID                                TYPE      DEVICE
eth0                 ba4a3d30-efdc-4fa5-83d3-3721fd4aff75  ethernet  eth0
Wired connection 1  8d569d5a-22a2-356d-8532-9a2638f11b5a5  ethernet  --
```

Which of the following is causing the issue?

- A. The DNS address has been commented out in the configuration file.
- B. The search entry in the /etc/resolv.conf file is incorrect.
- C. Wired connection 1 is offline.
- D. No default route is defined.

Answer: D

Explanation:

The issue is caused by the lack of a default route defined in the /etc/sysconfig/network-scripts/ifcfg-enp0s3 file. A default route is a special route that specifies where to send packets that do not match any other routes in the routing table. Without a default route, the server will not be able to communicate with hosts outside its local network. The default route is usually configured with the GATEWAY option in the network interface configuration file. For example, to set the default gateway to 192.168.1.1, the file should contain:
GATEWAY=192.168.1.1

The other options are not causing the issue. The DNS address is not commented out in the configuration file, it is specified with the DNS1 option. The search entry in the /etc/resolv.conf file is correct, it specifies the domain name to append to unqualified hostnames. Wired connection 1 is online, as indicated by the ONBOOT=yes option and the output of ip link show enp0s3 command. References: Configuring IP Networking with nmcli; Configuring IP Networking with ifcfg Files

NEW QUESTION 223

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual XK0-005 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the XK0-005 Product From:

<https://www.2passeasy.com/dumps/XK0-005/>

Money Back Guarantee

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