

# T estpassport Q&A



---

*La meilleure qualité le meilleur service*

<http://www.testpassport.fr>

Service de mise à jour gratuit pendant un an

**Exam** : **XK0-005**

**Title** : **CompTIA Linux+ Exam**

**Version** : **DEMO**

1. A Linux system is getting an error indicating the root filesystem is full.

Which of the following commands should be used by the systems administrator to resolve this issue? (Choose three.)

- A. `df -h /`
- B. `fdisk -l /dev/sdb`
- C. `growpart /dev/mapper/rootvg-rootlv`
- D. `pvcreate /dev/sdb`
- E. `lvresize -L +10G -r /dev/mapper/rootvg-rootlv`
- F. `lsblk /dev/sda`
- G. `parted -l /dev/mapper/rootvg-rootlv`
- H. `vgextend /dev/rootvg /dev/sdb`

**Answer:** A C E

**Explanation:**

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

- `df -h /`. This command will show the disk usage of the root filesystem in a human-readable format. The `df` command is a tool for reporting file system disk space usage. The `-h` option displays the sizes in powers of 1024 (e.g., 1K, 234M, 2G). The `/` specifies the root filesystem. The command `df -h /` will show the total size, used space, available space, and percentage of the root filesystem. This command will help the administrator identify the problem and plan the solution.

- `growpart /dev/mapper/rootvg-rootlv`. This command will grow the partition that contains the root filesystem to the maximum size available. The `growpart` command is a tool for resizing partitions on Linux systems. The `/dev/mapper/rootvg-rootlv` is the device name of the partition, which is a logical volume managed by the Logical Volume Manager (LVM). The command `growpart /dev/mapper/rootvg-rootlv` will extend the partition to fill the disk space and increase the size of the root filesystem. This command will help the administrator solve the problem and free up space.

- `lvresize -L +10G -r /dev/mapper/rootvg-rootlv`. This command will resize the logical volume that contains the root filesystem and add 10 GB of space. The `lvresize` command is a tool for resizing logical volumes on Linux systems. The `-L` option specifies the new size of the logical volume, in this case `+10G`, which means 10 GB more than the current size. The `-r` option resizes the underlying file system as well. The `/dev/mapper/rootvg-rootlv` is the device name of the logical volume, which is the same as the partition name. The command `lvresize -L +10G -r /dev/mapper/rootvg-rootlv` will increase the size of the logical volume and the root filesystem by 10 GB and free up space. This command will help the administrator solve the problem and free up space.

The other options are incorrect because they either do not affect the root filesystem (`fdisk -l /dev/sdb`, `pvcreate /dev/sdb`, `lsblk /dev/sda`, or `vgextend /dev/rootvg /dev/sdb`) or do not use the correct syntax (`fdisk -l /dev/sdb` instead of `fdisk -l /dev/sdb` or `parted -l /dev/mapper/rootvg-rootlv` instead of `parted /dev/mapper/rootvg-rootlv print`).

References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 10: Managing Storage, pages 318-319, 331-332.

2. 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 firewalld`) 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.

3.A Linux administrator is tasked with adding users to the system. However, the administrator wants to ensure the users' access will be disabled once the project is over. The expiration date should be 2021-09-30.

Which of the following commands will accomplish this task?

- A. `sudo useradd -e 2021-09-30 Project_user`
- B. `sudo useradd -c 2021-09-30 Project_user`
- C. `sudo modinfo -F 2021-09-30 Project_uses`
- D. `sudo useradd -m -d 2021-09-30 Project_user`

**Answer:** A

**Explanation:**

The command that will accomplish this task is `sudo useradd -e 2021-09-30 Project_user`. This command will create a new user account named `Project_user` with an expiration date of 2021-09-30. The `-e` option of `useradd` specifies the date on which the user account will be disabled in YYYY-MM-DD format. The other options are not correct commands for creating a user account with an expiration date. The

`sudo useradd -c 2021-09-30 Project_user` command will create a new user account named `Project_user` with a comment of `2021-09-30`. The `-c` option of `useradd` specifies a comment or description for the user account, not an expiration date. The `sudo modinfo -F 2021-09-30 Project_user` command is invalid because `modinfo` is not a command for managing user accounts, but a command for displaying information about kernel modules. The `-F` option of `modinfo` specifies a field name to show, not an expiration date. The `sudo useradd -m -d 2021-09-30 Project_user` command will create a new user account named `Project_user` with a home directory of `2021-09-30`. The `-m` option of `useradd` specifies that the home directory should be created if it does not exist, and the `-d` option specifies the home directory name, not an expiration date.

References: `useradd(8)` - Linux manual page; `modinfo(8)` - Linux manual page

4. 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.

5. A cloud engineer is installing packages during VM provisioning.

Which of the following should the engineer use to accomplish this task?

- A. Cloud-init
- B. Bash
- C. Docker
- D. Sidecar

**Answer:** A

**Explanation:**

The cloud engineer should use cloud-init to install packages during VM provisioning. Cloud-init is a tool that allows the customization of cloud instances at boot time. Cloud-init can perform various tasks, such as setting the hostname, creating users, installing packages, configuring network, and running scripts. Cloud-init can work with different cloud platforms and Linux distributions. This is the correct tool to accomplish the task. The other options are incorrect because they are either not suitable for cloud provisioning (Bash or Docker) or not a tool but a design pattern (Sidecar).

References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 19: Managing Cloud and Virtualization Technologies, page 563.