XK0-005 Q&As

CompTIA Linux+ Certification Exam

Pass CompTIA XK0-005 Exam with 100% Guarantee

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

https://www.geekcert.com/xk0-005.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

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

```
# df -h /ftpusers/

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

# df -i /ftpusers/

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

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

A. The users do not have the correct permissions to create files on the FTP server.

B. The ftpusers filesystem does not have enough space.

C. The inodes is at full capacity and would affect file creation for users.

D. ftpusers is mounted as read only.

Correct Answer: C

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

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

inodes on a filesystem is fixed when the filesystem is created, and it determines how many files and directories can be created on that filesystem. If the inodes are exhausted, no new files or directories can be created, even if there is enough

disk space available. The output for the second command shows that the /ftpusers/ filesystem has 0% of inodes available, which means that all the inodes have been used up. This would prevent users from creating new files on the FTP

server. The administrator should either delete some unused files or directories to free up some inodes, or resize the filesystem to increase the number of inodes.

The other options are incorrect because:

A. The users do not have the correct permissions to create files on the FTP server. This is not true, because the output for the first command shows that the /ftpusers/ filesystem has 26% of disk space available, which means that there is

enough space for users to create files. The permissions of the files and directories are not shown in the output, but they are not relevant to the issue of inode exhaustion. B. The ftpusers filesystem does not have enough space. This is not true,

because the output for the first command shows that the /ftpusers/ filesystem has 26% of disk space available, which means that there is enough space for users to create files. The issue is not related to disk space, but to inode capacity.

D. ftpusers is mounted as read only.

This is not true, because the output for the first command does not show any indication that the /ftpusers/ filesystem is mounted as read only. If it was, it would have an (ro) flag next to the mounted on column. A read only filesystem would

prevent users from creating or modifying files on the FTP server, but it would not affect the inode usage.

QUESTION 2

Which of the following data structures is written in JSON?

○ A.
```
---
name: user1
position: DevOps
floor: 3
```

○ B.
```
<table>
<tbody><tr>
<td>user1</td>
<td>DevOps</td>
<td>3</td>
</tr>
</tbody></table>
```

○ C.
```
<root>
   <floor>3</floor>
   <name>user1</name>
   <position>DevOps</position>
</root>
```

○ D.
```
{
   "name": "user1",
   "job": "DevOps",
   "floor": 3
}
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: C

Explanation: Option C is the only data structure that is written in JSON format. JSON stands for JavaScript Object Notation, and it is a lightweight and human-readable data interchange format. JSON uses curly braces to enclose objects, which consist of key-value pairs separated by commas. JSON uses square brackets to enclose arrays, which consist of values separated by commas. JSON supports six data types: strings, numbers, booleans, null, objects, and arrays. Option C follows these rules and syntax of JSON, while the other options do not. Option A is written in XML format, which uses tags to enclose elements and attributes. Option B is written in YAML format, which uses indentation and colons to define key-value pairs. Option D is written in INI format, which uses sections and equal signs to define key-value pairs. References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 21: Automating Tasks with Ansible, page 591.

QUESTION 3

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

Correct 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.

QUESTION 4

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

A. docker network erase

B. docker network clear

C. docker network prune

D. docker network rm

Correct Answer: C

The docker command is used to manage Docker containers, images, networks, volumes, and other resources on a Linux system. Docker is a platform that allows users to run applications in isolated environments called containers. Docker also provides networking features that allow users to create and manage networks for containers. To delete all unused networks that are not referenced by any container, the cloud engineer can use the docker network prune command. This command will remove all networks that have no containers connected to them. The statement C is correct. The statements A, B, and D are incorrect because they do not delete all unused networks. The docker network erase and docker network clear commands do not exist. The docker network rm command deletes a specific network by name or ID, but not all unused networks. References: [How to Manage Docker Networks]

QUESTION 5

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

A. Renaming the root account to something else

B. Removing unnecessary packages

C. Changing the default shell to /bin/csh

D. Disabling public key authentication

E. Disabling the SSH root login possibility

F. Changing the permissions on the root filesystem to 600

Correct Answer: BE

Some good security practices when hardening a Linux server are:

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

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

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

[How to Harden Your Linux Server]