



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.passapply.com/xk0-005.html>

100% Passing Guarantee
100% Money Back Assurance

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

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



**QUESTION 1**

A Linux administrator needs to connect securely to a remote server in order to install application software. Which of the following commands would allow this connection?

- A. `scp "ABC-key.pem" root@10.0.0.1`
- B. `sftp root@10.0.0.1`
- C. `telnet 10.0.0.1 80`
- D. `ssh -i "ABC-key.pem" root@10.0.0.1`
- E. `sftp "ABC-key.pem" root@10.0.0.1`

Correct Answer: D

Explanation: The command `ssh -i "ABC-key.pem" root@10.0.0.1` would allow the administrator to connect securely to the remote server in order to install application software. The `ssh` command is a tool for establishing secure and encrypted connections between remote systems. The `-i` option specifies the identity file that contains the private key for key-based authentication. The `"ABC-key.pem"` is the name of the identity file that contains the private key. The `root@10.0.0.1` is the username and the IP address of the remote server. The command `ssh -i "ABC-key.pem" root@10.0.0.1` will connect to the remote server using the private key and allow the administrator to install application software. This is the correct command to use to connect securely to the remote server. The other options are incorrect because they either do not use key-based authentication (`sftp root@10.0.0.1` or `telnet 10.0.0.1 80`) or do not use the correct syntax for the command (`scp "ABC-key.pem" root@10.0.0.1` instead of `scp -i "ABC-key.pem" root@10.0.0.1` or `sftp "ABC-key.pem" root@10.0.0.1` instead of `sftp -i "ABC-key.pem" root@10.0.0.1`). References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 17: Implementing Basic Security, page 513.

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 wants to allow the same Kubernetes container configurations to be deployed in development, testing, and production environments. A key requirement is that the containers should be configured so that developers



do not have to statically configure custom, environment-specific locations. Which of the following should the engineer use to meet this requirement?

- A. Custom scheduler
- B. Node affinity
- C. Overlay network
- D. Ambassador container

Correct Answer: D

To allow the same Kubernetes container configurations to be deployed in different environments without statically configuring custom locations, the engineer can use an ambassador container (D). An ambassador container is a proxy container that handles communication between containers and external services. It can dynamically configure locations based on environment variables or other methods. The other options are not related to this requirement. References:

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

Using Ambassador Containers

[How to Use Ambassador Containers]

QUESTION 4

A Linux administrator generated a list of users who have root-level command-line access to the Linux server to meet an audit requirement. The administrator analyzes the following `/etc/passwd` and `/etc/sudoers` files: `$ cat /etc/passwd` root:x:0:0: /home/root: /bin/bash lee: x: 500: 500: /home/lee:/bin/tcsh mallory:x: 501:501: /root:/bin/bash eve:x: 502: 502: /home/eve:/bin/nologin carl:x:0:503: /home/carl:/bin/sh bob:x: 504: 504: : /home/bob:/bin/ksh alice:x: 505:505: /home/alice:/bin/rsh `$ cat /etc/sudoers` Cmnd_Alias SHELLS = /bin/tcsh, /bin/sh, /bin/bash Cmnd_Alias SYSADMIN = /usr/sbin/tcpdump ALL = (ALL) ALL ALL = NOPASSWD: SYSADMIN Which of the following users, in addition to the root user, should be listed in the audit report as having root-level command-line access? (Select two).

- A. Carl
- B. Lee
- C. Mallory
- D. Eve
- E. Bob
- F. Alice

Correct Answer: AC

The users who have root-level command-line access are those who have either the same user ID (UID) as root, which is 0, or the ability to run commands as root using sudo. Based on the `/etc/passwd` and `/etc/sudoers` files, the users who meet these criteria are: Carl: Carl has the same UID as root, which is 0, as shown in the `/etc/passwd` file. This means that Carl can log in as root and execute any command with root privileges. Mallory: Mallory has the ability to run commands as root using sudo, as shown in the `/etc/sudoers` file. The line `ALL = (ALL) ALL` means that any user can run any command as any other user, including root, by using sudo. Mallory can also use the root shell `/bin/bash` as her login



shell, as shown in the /etc/passwd file. Therefore, the correct answer is A and C. Lee, Eve, Bob, and Alice do not have root-level command-line access because they have different UIDs from root and they cannot use sudo to run commands as root. Lee can only use sudo to run the commands listed in the Cmnd_Alias SHELLS, which are /bin/tcsh, /bin/sh, and /bin/bash. Eve cannot log in at all because her login shell is /bin/nologin. Bob and Alice can only use sudo to run the command /usr/sbin/tcpdump without a password, as specified by the Cmnd_Alias SYSADMIN and the line ALL = NOPASSWD: SYSADMIN2

QUESTION 5

The administrator comptia is not able to perform privileged functions on a newly deployed system. Given the following command outputs:

```
[root@newserver ~]# id comptia
uid=1000(comptia) gid=1000(comptia) groups=1000(comptia)

[root@newserver ~]# cat /etc/sudoers.d/admin
%admin ALL= (root) NOPASSWD: EXEC: /usr/bin/ps, /usr/bin/chmod, /usr/bin/yum, /usr/bin/cat, /usr/sbin/lvm,
/usr/sbin/pvs

[root@newserver ~]# grep comptia /etc/passwd
comptia:x:1000:1000:comptia:/home/comptia:/bin/bash

[root@newserver ~]# chage -l comptia
Last password change : never
Password expires : never
Password inactive : never
Account expires : never
Minimum number of days between password change : 0
Maximum number of days between password change : 99999
Number of days of warning before password expires : 7
```

Which of the following is the reason that the administrator is unable to perform the assigned duties?

- A. The administrator needs a password reset.
- B. The administrator is not a part of the correct group.
- C. The administrator did not update the sudo database.
- D. The administrator's credentials need to be more complex.

Correct Answer: B

The reason that the administrator is unable to perform the assigned duties is because the administrator is not a part of the correct group. This is option B. Based on the image that you sent, I can see that the user comptia has a user ID and a

group ID of 1000, and belongs to only one group, which is also comptia. However, the sudoers file, which defines the permissions for users to run commands as root or other users, does not include the comptia group in any of the entries.

Therefore, the user comptia cannot use sudo to perform privileged functions on the system.

The other options are incorrect because:

- A. The administrator needs a password reset.

This is not true, because the password aging information for the user comptia shows that the password was last changed on Oct 24, 2023, and it does not expire until Jan 22, 2024. There is no indication that the password is locked or expired.



C. The administrator did not update the sudo database. This is not necessary, because the sudo database is automatically updated whenever the sudoers file is modified. There is no separate command to update the sudo database. D. The

administrator's credentials need to be more complex. This is not relevant, because the complexity of the credentials does not affect the ability to use sudo. The sudoers file does not specify any password policy for the users or groups that are

allowed to use sudo.

[Latest XK0-005 Dumps](#)

[XK0-005 PDF Dumps](#)

[XK0-005 VCE Dumps](#)