XK0-005Q&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.pass2lead.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 systems administrator is tasked with setting up key-based SSH authentication. In which of the following locations should the administrator place the public keys for the server?

A. ~/.sshd/authkeys

B. ~/.ssh/keys

C. ~/.ssh/authorized_keys

D. ~/.ssh/keyauth

Correct Answer: C

The location where the systems administrator should place the public keys for the server to set up key-based SSH authentication is option C, ~/.ssh/authorized_keys.

The authorized_keys file is located in the .ssh directory in the home directory of the user account that is being used to log in to the remote server. This file contains a list of public keys that are allowed to authenticate the user when logging in to the server via SSH.

To set up key-based SSH authentication, the systems administrator should copy the public key(s) of the user(s) to the remote server\\'s authorized_keys file using a secure method such as scp. Once the public key(s) have been added to the file, the user(s) should be able to log in to the server using their corresponding private key(s) without being prompted for a password.

QUESTION 2

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

Correct Answer: D

D. setfacl -m g:finance:rw file: This command sets a new ACL (access control list) on the file that grants read and write access to the finance group. This option would allow the finance department to access the file while also maintaining the existing permissions for IT employees. The + in the rw option means to add read and write permissions to the existing permissions. The g: specifies that the permission is being set for a group, and the finance is the name of the group.

QUESTION 3

A Linux administrator modified the SSH configuration file. Which of the following commands should be used to apply the configuration changes?

A. systemctl stop sshd

B. systemctl mask sshd

C. systemctl reload sshd

D. systemctl start sshd

Correct Answer: C

The command that should be used to apply changes to the SSH configuration file is option C, systemctl reload sshd.

The reload command tells the sshd daemon to re-read its configuration file without terminating any existing connections. This makes it possible to apply changes to the SSH configuration file without disrupting any active SSH sessions.

Using the systemctl reload sshd command will cause the SSH service to reload its configuration file and apply any changes that have been made, without requiring the service to be stopped and restarted. This is the preferred method of

applying changes to the SSH configuration file because it allows changes to be made without affecting any currently connected users.

If the systemctl reload sshd command is not available, the systemctl restart sshd command can be used instead. This will stop and start the SSH service, terminating all existing connections and applying the new configuration settings.

However, this approach is less desirable because it will cause any active SSH sessions to be terminated.

QUESTION 4

A junior administrator updated the PostgreSQL service unit file per the database 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 postgresql

D. systemctl mask postgresql

Correct Answer: B

QUESTION 5

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

Correct Answer: A

The correct command is "nslookup." The "nslookup" command allows a user to query a DNS server to determine the IP address of a hostname, or to determine the hostname associated with a particular IP address. It is commonly used to troubleshoot DNS resolution issues. The other options "rsync," "netstat," and "host" are not used for this purpose.