Free Questions for XK0-005

Shared by Pope on 09-08-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A user is unable to log on to a Linux workstation. The systems administrator executes the following command:

cat /etc/shadow | grep user1

The command results in the following output:

user1 :! 6QERgAsdvojadv4asdvaarC/9dj34GdafGVaregmkdsfa:18875:0:99999:7 :::

Which of the following should the systems administrator execute to fix the issue?

Options:

A- chown -R userl:user1 /home/user1
B- sed -i '/ ::: / :: /g' /etc/shadow
C- chgrp user1:user1 /home/user1
D- passwd -u user1

Answer:

D

Explanation:

The output shows that the user1 account has a locked password, indicated by the exclamation point (!) in the second field of the /etc/shadow file1.To unlock the password and allow the user to log in, the systems administrator should use the passwd command with the -u (unlock) option2.

Question 2

Question Type: MultipleChoice

An administrator is running a web server in a container named web, but none of the error output is not showing. Which of the following should the administrator use to generate the errors on the container?

Options:

A- docker-compose inspect WEB
B- docker logs WEB
C- docker run ---name WEB ---volume/dev/stdout:/var/log/nginx/error.log
D- docker ps WEB -f

Answer:

B

Explanation:

Thedocker logscommand is used to fetch the logs of a container.If the error output is not showing for a running container, thedocker logscommand can be used to view these details56.

Reference:
5(https://www.docker.com/blog/how-to-fix-and-debug-docker-containers-like-a-superhero/)
6(https://stackoverflow.com/questions/33083385/getting-console-output-from-a-docker-container)

Question 3

Question Type: MultipleChoice

A Linux administrator is configuring a new internal web server fleet. The web servers are up and running but can only be reached by users directly via IP address. The administrator is attempting to fix this inconvenience by requesting appropriate records from the DNS team. The details are:

Hostname: devel.comptia.org

IP address: 5.5.5.1, 5.5.5.2, 5.5.5.3, 5.5.5.4

Name server: 5.5.5.254

Additional names: dev.comptia.org, development.comptia.org

Which of the following types of DNS records should the Linux administrator request from the DNS team? (Select three).

Options:

A- MX

B- NS
C- PTR
D- A
E- CNAME
F- RRSIG
G- SOA
H- TXT
I- SRV

Answer:

B, D, E

Explanation:

The Linux administrator should request the following types of DNS records from the DNS team:

A: This record type is used to map a hostname to an IPv4 address. The administrator needs four A records for devel.comptia.org, one for each IP address (5.5.5.1, 5.5.5.2, 5.5.5.3, 5.5.5.4).This will allow users to access the web servers by using the hostname devel.comptia.org instead of the IP addresses1.

CNAME: This record type is used to create an alias for another hostname. The administrator needs two CNAME records, one for dev.comptia.org and one for development.comptia.org, both pointing to devel.comptia.org.This will allow users to access the web servers by using any of these three hostnames interchangeably1.

NS: This record type is used to delegate a domain or a subdomain to another name server.The administrator needs one NS record for comptia.org, pointing to 5.5.5.254, which is the name server that hosts the records for the subdomain devel.comptia.org2.This will allow users to resolve the hostnames under comptia.org by querying the name server 5.5.5.2542.

The other record types are not relevant for the administrator's task:

MX: This record type is used to specify the mail exchange server for a domain or a subdomain1. The administrator does not need this record type because the web servers are not intended to handle email traffic.

PTR: This record type is used to map an IP address to a hostname, which is the reverse of an A record1. The administrator does not need this record type because the web servers are not expected to be accessed by their IP addresses.

RRSIG: This record type is used to provide digital signatures for DNSSEC, which is a security extension for DNS that verifies the authenticity and integrity of DNS responses3. The administrator does not need this record type because it is not mentioned in the task requirements.

SOA: This record type is used to provide information about the authoritative name server and other parameters for a domain or a subdomain1.The administrator does not need this record type because it is usually created automatically by the name server software when a new zone file is created4.

TXT: This record type is used to store arbitrary text data that can be used for various purposes, such as SPF, DKIM, DMARC, etc1. The administrator does not need this record type because it is not related to the web server functionality.

SRV: This record type is used to specify the location and port number of a service that runs on a domain or a subdomain1. The administrator does not need this record type because the web servers use the standard HTTP port 80, which does not require an SRV record.

Question 4

Question Type: MultipleChoice

What is the main objective when using Application Control?

Options:

A- To filter out specific content.
B- To assist the firewall blade with handling traffic.
C- To see what users are doing.
D- Ensure security and privacy of information.

Answer:

D

Explanation:

The main objective when using Application Control is to ensure the security and privacy of information. Application Control is a security practice that blocks or restricts unauthorized applications from executing in ways that put data at risk.The control functions vary based on the business purpose of the specific application, but the main objective is to help ensure the privacy and security of data used by and transmitted between applications1.Application Control can also prevent malware, untrusted, or unwanted applications from running on the network, reducing the risks and costs associated with data breaches1.Application Control can also improve the overall network stability and performance by eliminating unnecessary or harmful applications1.

Application Control is not mainly used to filter out specific content, although it can be combined

with other technologies such as URL filtering or content filtering to achieve that goal. Application Control is not mainly used to assist the firewall blade with handling traffic, although it can be integrated with firewall policies to enforce granular access rules based on applications. Application Control is not mainly used to see what users are doing, although it can provide visibility and reporting on application usage and activity.

Question 5

Question Type: MultipleChoice

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?

Options:

A- telinit 0
B- systemct1 reboot
C- systemct1 get-default
D- systemct1 emergency

Answer:

B

Explanation:

The systemct1 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 systemct1 get-default command would display the default target, not change it. The systemct1 emergency command would switch the server to emergency.target mode, which is even more restrictive than rescue.target mode.Reference:[CompTIA Linux+ (XK0-005) Certification Study Guide], Chapter 17: System Maintenance and Operation, page 516.

Question 6

Question Type: MultipleChoice

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?

Options:

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. Seelsscsi(8) - Linux man pageandHow to check Disk Interface Types in Linux. Reference 1: https://linux.die.net/man/8/lsscsi 2: https://www.golinuxcloud.com/check-disk-type-linux/

Question 7

Question Type: MultipleChoice

A file called testfile has both uppercase and lowercase letters:

$ cat testfile

ABCDEfgH

lJKLmnoPQ

abcdefgH

ijklLMNopq

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?

Options:

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 file12.

Question 8

Question Type: MultipleChoice

Due to performance issues on a server, a Linux administrator needs to terminate an unresponsive process. Which of the following commands should the administrator use to terminate the process immediately without waiting for a graceful shutdown?

Options:

A- kill -SIGKILL 5545
B- kill -SIGTERM 5545
C- kill -SIGHUP 5545
D- kill -SIGINT 5545

Answer:

A

Explanation:

SIGKILL is used to immediately terminate a process without allowing it to clean up. It does not give the process a chance to gracefully shut down, which is what's needed in the case of an unresponsive process.

Question 9

Question Type: MultipleChoice

A Linux administrator provisioned a new web server with custom administrative permissions for certain users. The administrator receives a report that user1 is unable to restart the Apache web service on this server. The administrator reviews the following output:

[root@server] # id user1

UID=1011 (user1) gid=1011 (USER1) groups=1011 (user1), 101 (www-data), 1120 (webadmin)

[root@server] # cat /etc/sudoers.d/custom.conf

user1 ALL=/usr/sbin/systemctl start httpd, /usr/sbin/systemctl stop httpd

webadmin ALL=NOPASSWD: /etc/init.d.httpd restart, /sbin/service httpd restart, /usr/sbin/apache2ctl restart

#%wheel ALL=(ALL) NOPASSWD: ALL

Which of the following would most likely resolve the issue while maintaining a least privilege security model?

Options:

A- User1 should be added to the wheel group to manage the service.
B- User1 should have 'NOPASSWD:' after the 'ALL=' in the custom. conf.
C- The wheel line in the custom. conf file should be uncommented.
D- Webadmin should be listed as a group in the custom. conf file.

Answer:

D

Explanation:

The custom.conf file grants sudo privileges to user1 and webadmin for managing the Apache web service, but it uses different commands for each of them. User1 is allowed to use systemctl to start and stop the httpd service, while webadmin is allowed to use init.d, service, or apache2ctl to restart the httpd service. However, the user1 is unable to restart the service, only start and stop it. To fix this, user1 should be able to use the same commands as webadmin, which can be achieved by listing webadmin as a group in the custom.conf file, using the syntax %groupname. This way, user1 will inherit the sudo privileges of the webadmin group, and be able to restart the Apache web service without compromising the least privilege security model.

Reference

Sudo and Sudoers Configuration | Servers for Hackers, section ''Groups''

Chapter 12. Managing sudo access - Red Hat Customer Portal, section ''12.1. Configuring sudo access for users and groups''