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

A systems administrator is investigating a service that is not starting up. Given the following information:

```
root@localhost ~]# systemctl status network
network.service - LSB: Bring up/down networking
Loaded: loaded (/etc/rc.d/init.d/network; bad; vendor preset: disabled)
Active: failed (Result: exit-code) since Jan 2022-01-02 22:55:15 CST;
Docs: man:systemd-sysv-generator(8)
Process: 1083 ExecStart=/etc/rc.d/init.d/network start (code=exited, status=1/FAILURE)
Jan 02 22:55:15 localhost.localdomain network[1083]: Bringing up interface enp0s25: Error: Con...n.
Jan 02 22:55:15 localhost.localdomain network[1083]: [FAILED]
[...]
```

Which of the following systemd commands should the administrator use in order to obtain more details about the failing service?

A. systemct1 analyze network

B. systemct1 info network

C. sysctl -a network

D. journalctl -xu network

Correct Answer: D

The systemd is a system and service manager for Linux systems that provides a standard way to control and monitor system services. The systemd uses various commands and tools to manage and troubleshoot system services, such as

systemct1, sysctl, and journalctl. The systemct1 command is used to start, stop, enable, disable, restart, reload, status, and list system services. The sysctl command is used to configure kernel parameters at runtime. The journalctl command

is used to view and filter the logs of system services.

To investigate a service that is not starting up, the administrator can use the journalctl command with the -xu option. The -x option enables verbose output that includes explanatory text and priority information. The -u option filters the output by

a specific unit name, such as network.service. Therefore, the command journalctl -xu network will show detailed logs of the network service, which can help identify the cause of the failure. The statement D is correct.

The statements A, B, and C are incorrect because they do not provide more details about the failing service. The systemct1 analyze network command does not exist. The systemct1 info network command shows basic information about the

network unit, such as description, load state, active state, sub state, and main PID. The sysctl -a network command shows all kernel parameters related to network settings. References:

[How to Use Systemd to Manage System Services]

QUESTION 2

An administrator recently updated the BIND software package and would like to review the default configuration that shipped with this version. Which of the following files should the administrator review?

A. /etc/named.conf.rpmnew

B. /etc/named.conf.rpmsave

C. /etc/named.conf

D. /etc/bind/bind.conf

Correct Answer: A

Explanation: After installing a new version of a package that includes a configuration file that already exists on the system, such as /etc/httpd/conf/httpd.conf, RPM will create a new file with the .rpmnew extension instead of overwriting the existing file. This allows the administrator to review the default configuration that shipped with this version and compare it with the current configuration before deciding whether to merge or replace the files. The /etc/named.conf.rpmsave file is created by RPM when a package is uninstalled and it contains a configuration file that was modified by the administrator. This allows the administrator to restore the configuration file if needed. The /etc/named.conf file is the main configuration file for the BIND name server, not the httpd web server. The /etc/bind/bind.conf file does not exist by default in Linux systems. References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 19: Managing Packages and Software, page 561.

QUESTION 3

DRAG DROP

You have been asked to parse a log file of logins to determine various information about who is logging in and when.

INSTRUCTIONS

Open and inspect the Login log file.

Drag and drop the correct commands onto the output that was generated from that

command.

Tokens can be used only once and not all will be used.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Select and Place:

Command Ouput

View Login Log

Commands

```
tr "[a-z]" "[A-Z]" < log.txt | grep -i "mar 12"
awk '{ print $1 }' log.txt | uniq
grep -i "mar 12" log.txt | sed 's/[a-z]/[A-Z]/g'
grep "Mar 13" log.txt
grep Mar 13 log.txt
awk '{ print $1 }' log.txt | sort | uniq -c
awk '{ print toupper($0) }' log.txt
awk '{ print $1 }' log.txt | sort | uniq
grep "Mar13" log.txt
grep log.txt "Mar 13"
awk '{ print $2 }' log.txt | sort | uniq
tr "[A-Z]" "[a-z]" < log.txt | grep -i "mar 12"
```

1 2 3

```
[comptia@localhost exercise]$

  ann
  carl
  chris
  comptia
  david
  eric
  joe
  lee
  reboot
```

Correct Answer:

Command Ouput

View Login Log

Commands

```
tr "[a-z]" "[A-Z]" < log.txt | grep -i "mar 12"

grep -i "mar 12" log.txt | sed 's/[a-z]/[A-Z]/g'
grep "Mar 13" log.txt
grep Mar 13 log.txt
awk '{ print $1 }' log.txt | sort | uniq -c
awk '{ print toupper($0) }' log.txt
awk '{ print $1 }' log.txt | sort | uniq
grep "Mar13" log.txt
grep log.txt "Mar 13"
awk '{ print $2 }' log.txt | sort | uniq
tr "[A-Z]" "[a-z]" < log.txt | grep -i "mar 12"
```

1 2 3

```
[comptia@localhost exercise]$ awk '{ print $1 }' log.txt | uniq
  ann
  carl
  chris
  comptia
  david
  eric
  joe
  lee
  reboot
```

QUESTION 4

A Linux administrator was asked to run a container with the httpd server inside. This container should be exposed at port 443 of a Linux host machine while it internally listens on port 8443. Which of the following commands will accomplish this task?

A. podman run -d -p 443:8443 httpd

B. podman run -d -p 8443:443 httpd

C. podman run -d -e 443:8443 httpd

D. podman exec -p 8443:443 httpd

Correct Answer: A

Explanation: The command that will accomplish the task of running a container with the httpd server inside and exposing it at port 443 of the Linux host machine while it internally listens on port 8443 is podman run -d -p 443:8443 httpd. This command uses the podman tool, which is a daemonless container engine that can run and manage containers on Linux systems. The -d option runs the container in detached mode, meaning that it runs in the background without blocking the terminal. The -p option maps a port on the host machine to a port inside the container, using the format host_port:container_port. In this case, port 443 on the host machine is mapped to port 8443 inside the container, allowing external access to the httpd server. The httpd argument specifies the name of the image to run as a container, which in this case is an image that contains the Apache HTTP Server software. The other options are not correct commands for accomplishing the task. Podman run -d -p 8443:443 httpd maps port 8443 on the host machine to port 443 inside the container, which does not match the requirement. Podman run -d -e 443:8443 httpd uses the -e option instead of the -p option, which sets an environment variable inside the container instead of mapping a port. Podman exec -p 8443:443 httpd uses the podman exec command instead of the podman run command, which executes a command inside an existing container instead of creating a new one. References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 18: Automating Tasks

QUESTION 5

A systems administrator requires that all files that are created by the user named web have read-only permissions by the owner. Which of the following commands will satisfy this requirement?

A. chown web:web /home/web

B. chmod -R 400 /home/web

C. echo "umask 377" >> /home/web/.bashrc

D. setfacl read /home/web

Correct Answer: C

Explanation: The command that will satisfy the requirement of having all files that are created by the user named web have read-only permissions by the owner is echo "umask 377" >> /home/web/.bashrc. This command will append the umask 377 command to the end of the .bashrc file in the web user\\'s home directory. The .bashrc file is a shell script that is executed whenever a new interactive shell session is started by the user. The umask command sets the file mode creation mask, which determines the default permissions for newly created files or directories by subtracting from the maximum permissions (666 for files and 777 for directories). The umask 377 command means that the user does not want to give any permissions to the group or others (3 = 000 in binary), and only wants to give read permission to

the owner (7 - 3 = 4 = 100 in binary). Therefore, any new file created by the web user will have read-only permission by the owner

(400) and no permission for anyone else. References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter

8: Managing Users and Groups; Umask Command in Linux | Linuxize