[Jan 16, 2025 Get New XK0-005 Certification ? Valid Exam Dumps Questions [Q74-Q93

[Jan 16, 2025] Get New XK0-005 Certification – Valid Exam Dumps Questions
100% Passing Guarantee - Brilliant XK0-005 Exam Questions PDF

QUESTION 74

A developer has been unable to remove a particular data folder that a team no longer uses. The developer escalated the issue to the systems administrator. The following output was received:

```
# rmdir data/
rmdir: failed to remove 'data/': Operation not permitted
# rm -rf data/
rm: cannot remove 'data': Operation not permitted
# mv data/ mydata
mv: cannot move 'data/' to 'mydata': Operation not permitted
# cd data/
# cat > test.txt
bash: test.txt: Permission denied
```


Which of the following commands can be used to resolve this issue?
* chgrp -R 755 data/
* chmod -R 777 data/
* chattr -R -i data/
* chown -R data/

Explanation

The command that can be used to resolve the issue of being unable to remove a particular data folder is chattr

-R -i data/. This command will use the chattr utility to change file attributes on a Linux file system. The -R option means that chattr will recursively change attributes of directories and their contents. The -i option means that chattr will remove (unset) the immutable attribute from files or directories. When a file or directory has the immutable attribute set, it cannot be modified, deleted, or renamed.

The other options are not correct commands for resolving this issue. The chgrp -R 755 data/ command will change the group ownership of data/ and its contents recursively to 755, which is not a valid group name. The chgrp command is used to change group ownership of files or directories. The chmod -R 777 data/ command will change the file mode bits of data/ and its contents recursively to 777, which means that everyone can read, write, and execute them. However, this will not remove the immutable attribute, which prevents deletion or modification regardless of permissions. The chmod command is used to change file mode bits of files or directories. The chown -R data/ command is incomplete and will produce an error. The chown command is used to change the user and/or group ownership of files or directories, but it requires at least one argument besides the file name. References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 7:

Managing Disk Storage; chattr(1) – Linux manual page; chgrp(1) – Linux manual page; chmod(1) – Linux manual page; chown(1) – Linux manual page

QUESTION 75

A systems administrator has been tasked with disabling the nginx service from the environment to prevent it from being automatically and manually started. Which of the following commands will accomplish this task?
* systemctl cancel nginx
* systemctl disable nginx
* systemctl mask nginx
* systemctl stop nginx

QUESTION 76

A Linux user reported the following error after trying to connect to the system remotely:

ssh: connect to host 10.0.1.10 port 22: Resource temporarily unavailable The Linux systems administrator executed the following commands in the Linux system while trying to diagnose this issue:

```
# netstat -an | grep 22 | grep LISTEN
tcp      0        0        0.0.0.0:22       0.0.0.0:*        LISTEN

# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: eth0
  sources:
  services: dhcpv6-client
  ports:
  protocols:
  masquerade: no
        forward-ports:
        source-ports:
        icmp-blocks:
        rich rules:
```


Which of the following commands will resolve this issue?
* firewall-cmd –zone=public –permanent –add-service=22
* systemct1 enable firewalld; systemct1 restart firewalld
* firewall-cmd –zone=public –permanent –add-service=ssh
* firewall-cmd –zone=public –permanent –add-port=22/udp

The firewall-cmd –zone=public –permanent –add-service=ssh command will resolve the issue by allowing SSH connections on port 22 in the public zone of the firewalld service. This command will add the ssh service to the permanent configuration of the public zone, which means it will persist after a reboot or a reload of the firewalld service. The firewall-cmd –zone=public –permanent –add-service=22 command is invalid, as 22 is not a valid service name. The systemct1 enable firewalld; systemct1 restart firewalld command will enable and restart the firewalld service, but it will not change the firewall rules. The firewall-cmd –zone=public — permanent –add-port=22/udp command will allow UDP traffic on port 22 in the public zone, but SSH uses TCP, not UDP. References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 18: Securing Linux Systems, page 543.

QUESTION 77

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?
* /etc/named.conf.rpmnew
* /etc/named.conf.rpmsave
* /etc/named.conf
* /etc/bind/bind.conf

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 78

A Linux administrator needs to obtain a list of all volumes that are part of a volume group. Which of the following commands should the administrator use to accomplish this task?
* vgs
* lvs
* fdisk -1
* pvs

The lvs command can be used to obtain a list of all volumes that are part of a volume group. This command will display information such as the name, size, attributes, and volume group of each logical volume in the system. The vgs command can be used to obtain a list of all volume groups in the system, not the volumes. The fdisk -1 command is invalid, as -1 is not a valid option for fdisk. The pvs command can be used to obtain a list of all physical volumes in the system, not the volumes. Reference: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 14: Managing Disk Storage, page 461.

QUESTION 79

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?
* User1 should be added to the wheel group to manage the service.
* User1 should have “NOPASSWD:” after the “ALL=” in the custom. conf.
* The wheel line in the custom. conf file should be uncommented.
* Webadmin should be listed as a group in the custom. conf file.

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”

QUESTION 80

Which of the following is the best tool for dynamic tuning of kernel parameters?
* tuned
* tune2fs
* tuned-adm
* turbostat

The tuned application is the best tool for dynamic tuning of kernel parameters, as it monitors the system and optimizes the performance under different workloads. It provides a number of predefined profiles for typical use cases, such as power saving, low latency, high throughput, virtual machine performance, and so on. It also allows users to create, modify, and delete profiles, and to switch between them on the fly. The tuned application uses the sysctl command and the configuration files in the /etc/sysctl.d/ directory to adjust the kernel parameters at runtime.

References

* Chapter 2. Getting started with TuneD – Red Hat Customer Portal, paragraph 1

* Kernel tuning with sysctl – Linux.com, paragraph 1

QUESTION 81

A systems administrator receives reports that several virtual machines in a host are responding slower than expected. Upon further investigation, the administrator obtains the following output from one of the affected systems:

16:00:01 PM	CPU	%user	%nice	%system	%iowait	%steal	%idle
16:10:01 PM	all	17.58	0.00	9.36	0.00	54.33	18.73
16:20:01 PM	all	22.34	0.00	11.75	0.00	48.69	17.22
16:30:01 PM	all	20.49	0.00	11.69	0.00	57.85	4.97
16:40:01 PM	all	25.49	0.00	11.69	0.00	53.21	9.61
16:50:01 PM	all	25.49	0.00	11.69	0.00	56.49	6.33

Which of the following best explains the reported issue?
* The physical host is running out of CPU resources, leading to insufficient CPU time being allocated to virtual machines.
* The physical host has enough CPU cores, leading to users running more processes to compensate for the slower response times.
* The virtual machine has enough CPU cycles, leading to the system use percentage being higher than expected.
* The virtual machine is running out of CPU resources, leading to users experiencing longer response times.

Based on the output from one of the affected systems, the best explanation for the reported issue is that the virtual machine is running out of CPU resources, leading to users experiencing longer response times (D). The output shows that the system use

percentage is very high (57.85%), indicating that the virtual machine is using most of its CPU cycles for system processes. This leaves little CPU time for user processes, which results in slower performance. The other explanations are not supported by the output or are contradictory.

References:

* [CompTIA Linux+ Study Guide], Chapter 8: Optimizing Linux Performance, Section: Monitoring CPU Usage

* [How to Interpret CPU Usage Statistics]

QUESTION 82

A Linux administrator cloned an existing Linux server and built a new server from that clone. The administrator encountered the following error after booting the cloned server:

```
Device mismatch detected
```

The administrator performed the commands listed below to further troubleshoot and mount the missing filesystem:

```
#ls -al /dev/disk/by-uuid/
total 0
drwxr-xr-x 2 root 220 Jul 08:59 .
drwxr-xr-x 2 root 160 Jul 08:59 ..
lrwxrwxrwx 1 root 26 Jul 11:10 2251a54-6c14-9187-df8629373 -> ../../sdb
lrwxrwxrwx 1 root 26 Jul 11:10 4211c54-2a13-7291-bd8629373 -> ../../sdc
lrwxrwxrwx 1 root 26 Jul 11:10 3451b54-6d10-3561-ad8629373 -> ../../sdd
```


Which of the following should administrator use to resolve the device mismatch issue and mount the disk?
* mount disk by device-id
* fsck -A
* mount disk by-label
* mount disk by-blkid

Explanation

The administrator should use the command mount disk by device-id to resolve the device mismatch issue and mount the disk. The issue is caused by the cloned server having a different device name for the disk than the original server. The output of blkid shows that the disk has the device name /dev/sdb1 on the cloned server, but the output of cat /etc/fstab shows that the disk is expected to have the device name /dev/sda1. The command mount disk by device-id will mount the disk by using its unique identifier (UUID) instead of its device name. The UUID can be obtained from the output of blkid or lsblk -f. The command will mount the disk to the specified mount point (/data) and resolve the issue. The other options are incorrect because they either do not mount the disk (fsck -A), do not use the correct identifier (mount disk by-label or mount disk by-blkid), or do not exist (mount disk by-blkid). References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 10: Managing Storage, pages 318-319.

QUESTION 83

A technician recently installed Linux on a desktop computer.

The desktop has two graphics cards from two different vendors. One of the graphics cards works, but the other does not.

Which of the following commands should the technician use to start troubleshooting this issue?
* Ismod
* Vmstat
* Gdm
* startx

QUESTION 84

A Linux administrator is scheduling a system job that runs a script to check available disk space every hour. The Linux administrator does not want users to be able to start the job.

Given the following:

```
[Unit]
Description=Check available disk space
RefuseManualstart=yes
RefuseManualStop=yes

[Timer]
Persistent=true
OnCalendar=*-*-*-*:00:00
Unit=checkdiskspace.service

[Install]
WantedBy=timers.target
```


The Linux administrator attempts to start the timer service but receives the following error message:

```
Failed to start checkdiskspace.timer: Operation refused ...
```

Which of the following is MOST likely the reason the timer will not start?
* The checkdiskspace.timer unit should be enabled via systemctl.
* The timers.target should be reloaded to get the new configuration.

* The checkdiskspace.timer should be configured to allow manual starts.
* The checkdiskspace.timer should be started using the sudo command.

The most likely reason the timer will not start is that the checkdiskspace.timer should be configured to allow manual starts. By default, systemd timers do not allow manual activation via systemct1 start, unless they have RefuseManualStart=no in their [Unit] section. This option prevents users from accidentally starting timers that are meant to be controlled by other mechanisms, such as calendar events or dependencies. To enable manual starts for checkdiskspace.timer, the administrator should add RefuseManualStart=no to its [Unit] section and reload systemd.

QUESTION 85

A systems administrator creates a public key for authentication. Which of the following tools is most suitable to use when uploading the key to the remote servers?

* scp
* ssh-copy-id
* ssh-agent
* ssh-keyscan

Explanation

The best tool to use when uploading the public key to the remote servers is B. ssh-copy-id. This tool will copy the public key from the local computer to the remote server and append it to the authorized_keys file, which is used for public key authentication. This tool will also create the necessary directories and files on the remote server if they do not exist. The other tools are either not suitable or not relevant for this task. For example:

A: scp is a tool for securely copying files between hosts, but it does not automatically add the public key to the authorized_keys file.

C: ssh-agent is a tool for managing private keys and passphrases, but it does not upload the public key to the remote server.

D: ssh-keyscan is a tool for collecting public keys from remote hosts, but it does not upload the public key to the remote server.

QUESTION 86

A junior Linux administrator is tasked with installing an application. The installation guide states the application should only be installed in a run level 5 environment.

```
$ systemctl get-default
getty.target
```

Which of the following commands would ensure the server is set to runlevel 5?

* systemctl isolate multi-user.target
* systemctl isolate graphical.target
* systemctl isolate network.target
* systemctl isolate basic.target

QUESTION 87

A junior developer is unable to access an application server and receives the following output:

```
[root@server1 ~]# ssh dev2@172.16.25.126
dev2@172.16.25.126's password:
Permission denied, please try again.
dev2@172.16.25.126's password:
Permission denied, please try again.
dev2@172.16.25.126's password:
Account locked due to 4 failed logins
Account locked due to 5 failed logins
Last login: Mon Apr 22 21:21:06 2021 from 172.16.16.52
```


The systems administrator investigates the issue and receives the following output:

```
[root@server1 ~]# pam_tally2 --user=dev2
Login Failures Latest failure From
dev2 5 04/22/21 21:22:37 172.16.16.52
```

Which of the following commands will help unlock the account?
* Pam_tally2 –user=dev2 –quiet
* pam_ tally2 –user=dev2
* pam_tally2 –user+dev2 –quiet
* pam_tally2 –user=dev2 –reset

Explanation

To unlock an account that has been locked due to login failures, the administrator can use the command pam_tally2 –user=dev2 –reset (D). This will reset the failure counter for the user “dev2” and allow the user to log in again. The other commands will not unlock the account, but either display or increase the failure count. References:

[CompTIA Linux+ Study Guide], Chapter 4: Managing Users and Groups, Section: Locking Accounts with pam_tally2

[How to Lock and Unlock User Account in Linux]

QUESTION 88

A systems administrator notices several intensive tasks executing from users Joe and Ann.

These processes are impacting server operations but must be allowed to continue running.

Which of the following commands should the systems administrator run to reduce the impact on the server?
* pkill -u joe ann
* renice 11 -u joe ann

* nohup -u joe ann
* strace -u joe ann

https://www.computerhope.com/unix/renice.htm#:~:text=On%20Unix%2Dlike%20operating%20systems,the%20Linux%20version%20of%20renice

QUESTION 89

A Linux administrator copied a Git repository locally, created a feature branch, and committed some changes to the feature branch. Which of the following Git actions should the Linux administrator use to publish the changes to the main branch of the remote repository?

* rebase
* tag
* commit
* push

The push action is used to publish the changes made in a local branch to a remote branch of a Git repository. This action will update the remote branch with the commits made in the local branch and synchronize the two branches. The rebase action is used to reapply commits from one branch onto another branch, creating a linear history of commits. This action does not publish any changes to a remote repository. The tag action is used to create an annotated reference to a specific commit in a Git repository. This action does not publish any changes to a remote repository. The commit action is used to record changes made in the local repository and create a new snapshot of the project state. This action does not publish any changes to a remote repository. Reference: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 20: Writing and Executing Bash Shell Scripts, page 579.

QUESTION 90

A systems administrator configured firewall rules using firewalld. However, after the system is rebooted, the firewall rules are not present:

```
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```


The systems administrator makes additional checks:

```
- dynamic firewall daemon
  Loaded: loaded (/usr/lib/systemd/system/firewalld.service; disabled; vendor preset: enabled)
  Active: inactive (dead)
  Docs: man: firewalld (1)

firewalld is not running
```

Which of the following is the reason the firewall rules are not active?
* iptables is conflicting with firewalld.
* The wrong system target is activated.
* FIREWALL_ARGS has no value assigned.
* The firewalld service is not enabled.

The reason the firewall rules are not active is that the firewalld service is not enabled. This means that the service will not start automatically at boot time or after a system reload. To enable the firewalld service, the systems administrator needs to use the command sudo systemct1 enable firewalld. This will create a symbolic link from the firewalld service file to the appropriate systemd target, such as multi-user.target. Enabling the service does not start it immediately, so the systems administrator also needs to use the command sudo systemct1 start firewalld or sudo systemct1 reload firewalld to activate the firewall rules.

The other options are not correct reasons for the firewall rules not being active. iptables is not conflicting with firewalld, because firewalld uses iptables as its backend by default. The wrong system target is not activated, because firewalld is independent of the system target and can be enabled for any target. FIREWALL_ARGS has no value assigned, but this is not a problem, because FIREWALL_ARGS is an optional environment variable that can be used to pass additional arguments to the firewalld daemon, such as –debug or –nofork. If FIREWALL_ARGS is empty or not defined, firewalld will use its default arguments.
References: firewalld.

service(8) – Linux manual page; firewall-cmd(1) – Linux manual page; systemct1(1) – Linux manual page

QUESTION 91

A systems administrator is implementing a new service task with systems at startup and needs to execute a script entitled test.sh with the following content:

```
TIMESTAMP=$ (date '+%Y-%m-%d %H:%M:%S')
echo "helpme.service: timestamp $(Timestamp)" | systemd-cat -p info
sleep 60
done
```


The administrator tries to run the script after making it executable with chmod +x; however, the script will not run. Which of the following should the administrator do to address this issue? (Choose two.)
* Add #!/bin/bash to the bottom of the script.
* Create a unit file for the new service in /etc/systemd/system/ with the name helpme.service in the location.
* Add #!//bin/bash to the top of the script.
* Restart the computer to enable the new service.
* Create a unit file for the new service in /etc/init.d with the name helpme.service in the location.
* Shut down the computer to enable the new service.

The administrator should do the following two things to address the issue:

* Add #!/bin/bash to the top of the script. This is called a shebang line and it tells the system which interpreter to use to execute the script. Without this line, the script will not run properly. The shebang line should be the first line of the script and should start with #! followed by the path to the interpreter.

In this case, the interpreter is bash and the path is /bin/bash. The other option (A) is incorrect because the shebang line should be at the top, not the bottom of the script.

* Create a unit file for the new service in /etc/systemd/system/ with the name helpme.service in the location. This is necessary to register the script as a systemd service and enable it to run at startup. A unit file is a configuration file that defines the properties and behavior of a service, such as the description, dependencies, start and stop commands, and environment variables. The unit file should have the extension .service and should be placed in the /etc/systemd/system/ directory. The other option (E) is incorrect because /etc/init.d is the directory for init scripts, not systemd services.

References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 14: Managing Processes and Scheduling Tasks, pages 429-430.

QUESTION 92

A systems administrator wants to be sure the sudo rules just added to /etc/sudoers are valid. Which of the following commands can be used for this task?
* visudo -c
* test -f /etc/sudoers
* sudo vi check
* cat /etc/sudoers | tee test

QUESTION 93

A Linux administrator found many containers in an exited state. Which of the following commands will allow the administrator to clean up the containers in an exited state?
* docker rm –all
* docker rm –state exited
* docker rm $(docker ps -aq)
* docker images prune *

Explanation

The command docker rm $(docker ps -aq) will allow the administrator to clean up the containers in an exited state. The docker command is a tool for managing Docker containers on Linux systems. Docker containers are isolated and lightweight environments that can run applications and services without affecting the host system.

Docker uses images to create containers, which are files that contain the code, libraries, dependencies, and configuration of the applications and services. The rm option removes one or more containers. The $(docker ps -aq) is a command substitution that executes the command inside the parentheses and replaces it with the output. The docker ps -aq command lists all the containers, including the ones in an exited state, and shows only their IDs. The docker rm $(docker ps -aq) command will remove all the containers, including the ones in an exited state, by passing their IDs to the rm option. This will allow the administrator to clean up the containers in an exited state. This is the correct command to use to accomplish the task. The other options are incorrect because they either do not exist (docker rm –all or docker rm –state exited) or do not remove the containers (docker images prune *). References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 19: Managing Cloud and Virtualization Technologies, page 571.

Free XK0-005 braindumps download: https://www.topexamcollection.com/XK0-005-vce-collection.html]