

XK0-005^{Q&As}

CompTIA Linux+

Pass CompTIA XK0-005 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.leads4pass.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

An administrator started a long-running process in the foreground that needs to continue without interruption. Which of the following keystrokes should the administrator use to continue running the process in the background?

- A. bg
- B. bg
- C. jobs -1
- D. bg and

Correct Answer: A

A long-running process is a program that takes a long time to complete or runs indefinitely on a Linux system. A foreground process is a process that runs in the current terminal and receives input from the keyboard and output to the screen.

A background process is a process that runs in the background and does not interact with the terminal. A background process can continue running even if the terminal is closed or disconnected. To start a long-running process in the

background, the user can append an ampersand (and) to the command, such as `someapp &`. This will run `someapp` in the background and return control to the terminal immediately.

To move a long-running process from the foreground to the background, the user can use two keystrokes: `Ctrl+Z` and `bg`. The `Ctrl+Z` keystroke will suspend (pause) the foreground process and return control to the terminal. The `bg` keystroke

will resume (continue) the suspended process in the background and detach it from the terminal. The statement B is correct.

The statements A, C, and D are incorrect because they do not perform the desired task. The `bg` keystroke alone will not work unless there is a suspended process to resume. The `Ctrl+B` keystroke will not suspend the foreground process, but

rather move one character backward in some applications. The `jobs` keystroke will list all processes associated with the current terminal. The `bg and` keystroke will cause an error because `bg` does not take any arguments. References: [How to

Run Linux Processes in Background]

QUESTION 2

A Linux administrator is troubleshooting an issue in which an application service failed to start on a Linux server. The administrator runs a few commands and gets the following outputs:

Output 1:

```
Dec 23 23:14:15 root systemd[1] logsearch.service: Failed to start Logsearch.
```

Output 2:

```
logsearch.service - Log Search
Loaded: loaded (/etc/systemd/system/logsearch.service; enabled; vendor preset:enabled)
Active: failed (Result: timeout)
Process: 3267 ExecStart=/usr/share/logsearch/bin/logger ...
Main PID: 3267 (code=killed, signal=KILL)
```

Based on the above outputs, which of the following is the MOST likely action the administrator should take to resolve this issue?

- A. Enable the logsearch.service and restart the service.
- B. Increase the TimeoutStartUsec configuration for the logsearch.service.
- C. Update the OnCalendar configuration to schedule the start of the logsearch.service.
- D. Update the KillSignal configuration for the logsearch.service to use TERM.

Correct Answer: B

Explanation: The administrator should increase the TimeoutStartUsec configuration for the logsearch.service to resolve the issue. The output of `systemctl status logsearch.service` shows that the service failed to start due to a timeout. The output of `cat /etc/systemd/system/logsearch.service` shows that the service has a TimeoutStartUsec configuration of 10 seconds, which might be too short for the service to start. The administrator should increase this value to a higher number, such as 30 seconds or 1 minute, and then restart the service. The other options are incorrect because they are not related to the issue. The service is already enabled, as shown by the output of `systemctl is-enabled logsearch.service`. The service does not use an OnCalendar configuration, as it is not a timer unit. The service does not use a KillSignal configuration, as it is not being killed by a signal. References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 14: Managing Processes and Scheduling Tasks, pages 434-435.

QUESTION 3**CORRECT TEXT**

Junior system administrator had trouble installing and running an Apache web server on a Linux server. You have been tasked with installing the Apache web server on the Linux server and resolving the issue that prevented the junior administrator from running Apache.

INSTRUCTIONS

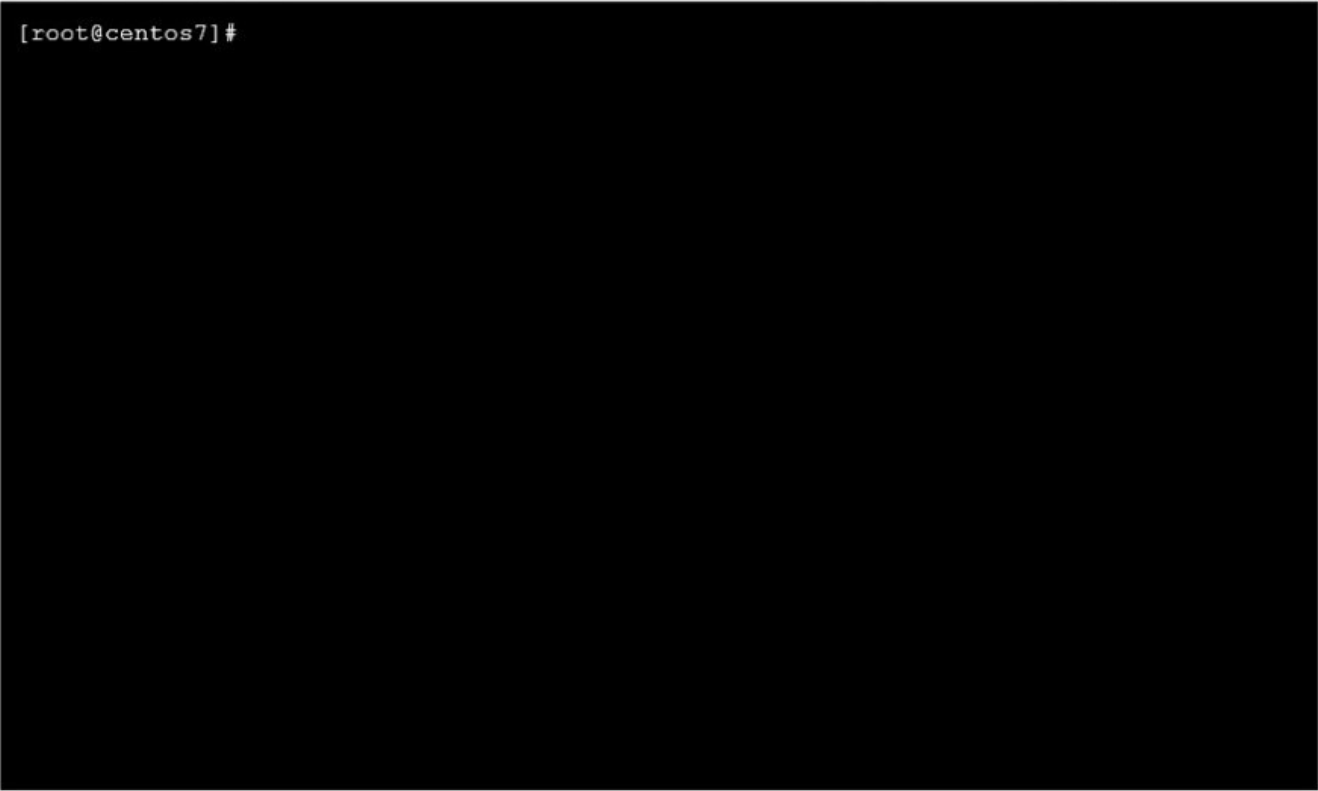
Install Apache and start the service. Verify that the Apache service is running with the defaults.

Typing "help" in the terminal will show a list of relevant event commands.

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

CentOS Command Prompt

```
[root@centos7] #
```



A. See the explanation below.

B. Placeholder

C. Placeholder

D. Placeholder

Correct Answer: A

```
yum install httpd systemctl --now enable httpd systemctl status httpd netstat -tunlp | grep 80 pkill systemctl restart httpd  
systemctl status httpd
```

QUESTION 4

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 :!$6$QERgAsdvojadv4asdvaarC/9dj34GdafGVaregmkdsfa:18875:0:99999:7 :::
```

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

A. `chown -R user:user1 /home/user1`

B. `sed -i \\\ / :: / :: /g\\ /etc/shadow`

C. `chgrp user1:user1 /home/user1`

D. `passwd -u user1`

Correct Answer: D

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. References: 1: Understanding the /etc/shadow File 2: How To Use The Passwd Command In Linux

QUESTION 5

Users are unable to create new files on the company's FTP server, and an administrator is troubleshooting the issue. The administrator runs the following commands:

```
# df -h /ftpusers/
```

Filesystem	Size	Used	Avail	Use%	Mounted on
/dev/sda4	150G	40G	109G	26%	/ftpusers

```
# df -i /ftpusers/
```

Filesystem	Inodes	Iused	Ifree	Iuse%	Mounted on
/dev/sda4	34567	34567	0	100%	/ftpusers

Which of the following is the cause of the issue based on the output above?

A. The users do not have the correct permissions to create files on the FTP server.

B. The ftpusers filesystem does not have enough space.

C. The inodes is at full capacity and would affect file creation for users.

D. ftpusers is mounted as read only.

Correct Answer: C

The cause of the issue based on the output above is C. The inodes is at full capacity and would affect file creation for users.

An inode is a data structure that stores information about a file or directory, such as its name, size, permissions, owner, timestamps, and location on the disk. Each file or directory has a unique inode number that identifies it. The number of

inodes on a filesystem is fixed when the filesystem is created, and it determines how many files and directories can be

created on that filesystem. If the inodes are exhausted, no new files or directories can be created, even if there is enough

disk space available. The output for the second command shows that the `/ftpusers/` filesystem has 0% of inodes available, which means that all the inodes have been used up. This would prevent users from creating new files on the FTP

server. The administrator should either delete some unused files or directories to free up some inodes, or resize the filesystem to increase the number of inodes.

The other options are incorrect because:

A. The users do not have the correct permissions to create files on the FTP server. This is not true, because the output for the first command shows that the `/ftpusers/` filesystem has 26% of disk space available, which means that there is

enough space for users to create files. The permissions of the files and directories are not shown in the output, but they are not relevant to the issue of inode exhaustion. B. The `ftpusers` filesystem does not have enough space. This is not true,

because the output for the first command shows that the `/ftpusers/` filesystem has 26% of disk space available, which means that there is enough space for users to create files. The issue is not related to disk space, but to inode capacity.

D. `ftpusers` is mounted as read only.

This is not true, because the output for the first command does not show any indication that the `/ftpusers/` filesystem is mounted as read only. If it was, it would have an `(ro)` flag next to the mounted on column. A read only filesystem would

prevent users from creating or modifying files on the FTP server, but it would not affect the inode usage.

QUESTION 6

A systems administrator frequently connects to a remote host via SSH and a non-standard port. The systems administrator would like to avoid passing the port parameter on the command line every time. Which of the following files can be used to set a different port value for that host?

A. `/etc/ssh/sshd_config`

B. `/etc/ssh/moduli`

C. `~/.ssh/config`

D. `~/.ssh/authorized_keys`

Correct Answer: C

Explanation: The `~/.ssh/config` file can be used to set various options for SSH connections, including the port number, for specific hosts or groups of hosts. This file is located in the user's home directory and affects only the current user. The /

`etc/ssh/sshd_config` file is used to configure the SSH server daemon, not the client. The `/etc/ssh/moduli` file contains parameters for Diffie-Hellman key exchange, not port settings. The `~/.ssh/authorized_keys` file contains public keys for

authentication, not port settings. References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 12:

Secure Shell (SSH), page 414.

QUESTION 7

A Linux administrator booted up the server and was presented with a non-GUI terminal. The administrator ran the command `systemctl isolate graphical.target` and rebooted the system by running `systemctl reboot`, which fixed the issue. However, the next day the administrator was presented again with a non-GUI terminal. Which of the following is the issue?

- A. The administrator did not reboot the server properly.
- B. The administrator did not set the default target to `basic.target`.
- C. The administrator did not set the default target to `graphical.target`.
- D. The administrator did not shut down the server properly.

Correct Answer: C

Explanation: The issue is that the administrator did not set the default target to `graphical.target`. A target is a unit of `systemd` that groups together other units by a common purpose or state. The `graphical.target` is a target that starts the graphical user interface (GUI) along with other services. The administrator used the command `systemctl isolate graphical.target` to switch to this target temporarily, but this does not change the default target that is activated at boot time. To make this change permanent, the administrator should have used the command `systemctl set-default graphical.target`, which creates a symbolic link from `/etc/systemd/system/default.target` to `/usr/lib/systemd/system/graphical.target`. The other options are not correct explanations for the issue. The administrator did reboot the server properly by using `systemctl reboot`, which shuts down and restarts the system cleanly. The administrator did not need to set the default target to `basic.target`, which is a minimal target that only starts essential services. The administrator did not shut down the server improperly, which could have caused file system corruption or data loss, but not affect the default target. References: `systemctl(1)` - Linux manual page; How to Change Runlevels (targets) in SystemD

QUESTION 8

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?

- A. `Pam_tally2 --user=dev2 ---quiet`
- B. `pam_tally2 --user=dev2`
- C. `pam_tally2 --user+dev2 ---quiet`
- D. `pam_tally2 --user=dev2 ---reset`

Correct Answer: D

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 9

A Linux administrator wants to find out whether files from the `wget` package have been altered since they were installed. Which of the following commands will provide the correct information?

- A. `rpm -i wget`
- B. `rpm -qf wget`
- C. `rpm -F wget`
- D. `rpm -V wget`

Correct Answer: D

Explanation: The command that will provide the correct information about whether files from the `wget` package have been altered since they were installed is `rpm -V wget`. This command will use the `rpm` utility to verify an installed RPM package by comparing information about the installed files with information from the RPM database. The verification process can check various attributes of each file, such as size, mode, owner, group, checksum, capabilities, and so on. If any discrepancies are found, `rpm` will report them using a single letter code for each attribute. The other options are not correct commands for verifying an installed RPM package. The `rpm -i wget` command is invalid because `-i` is used to install a package from a file, not to verify an installed package. The `rpm -qf wget` command will query which package owns `wget` as a file name or path name, but it will not verify its attributes. The `rpm -F wget` command will freshen

(upgrade) an already installed package with `wget` as a file name or path name, but it will not verify its attributes. References: `rpm(8)` - Linux manual page; Using RPM to Verify Installed Packages

QUESTION 10

At what point is the Internal Certificate Authority (ICA) created?

- A. During the primary Security Management Server installation process.
- B. Upon creation of a certificate.
- C. When an administrator decides to create one.
- D. When an administrator initially logs into SmartConsole.

Correct Answer: A

Explanation: The Internal Certificate Authority (ICA) is created during the primary Security Management Server installation process. The ICA is a component of Check Point's Public Key Infrastructure (PKI) that issues and manages certificates for Security Gateways and administrators. The ICA is automatically installed and initialized when the primary Security Management Server is installed. The ICA is not created upon creation of a certificate, when an administrator decides to create one, or when an administrator initially logs into SmartConsole. References: Check Point Certified Security Administrator (CCSA) R80.x Study Guide, Chapter 3: Check Point Security Management Architecture, page 32.

QUESTION 11

After starting an Apache web server, the administrator receives the following error:

```
Apr 23 localhost.localdomain httpd[4618] : (98) Address already in use: AH00072: make_sock: could not bind to address [::]80
```

Which of the following commands should the administrator use to further troubleshoot this issue?

- A. `ss`
- B. `ip`
- C. `dig`
- D. `nc`

Correct Answer: A

The `ss` command is used to display information about socket connections, such as the port number, state, and process ID. The error message indicates that the port 80 is already in use by another process, which prevents the Apache web server from binding to it. By using the `ss` command with the `-l` and `-n` options, the administrator can list all the listening sockets and their port numbers in numeric form, and identify which process is using the port 80. For example: `ss -ln | grep :80`. The `ip`, `dig`, and `nc` commands are not relevant for this issue, as they are used for different purposes, such as configuring network interfaces, querying DNS records, and testing network connectivity.

QUESTION 12

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?

- A. vgs
- B. lvs
- C. fdisk -l
- D. pvs

Correct Answer: B

Explanation: 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 -l command is invalid, as -l 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. References: CompTIA Linux+ (XK0- 005) Certification Study Guide, Chapter 14: Managing Disk Storage, page 461.

QUESTION 13

Based on an organization's new cybersecurity policies, an administrator has been instructed to ensure that, by default, all new users and groups that are created fall within the specified values below.

```
# Min/max values for automatic uid selection in useradd
#
UID_MIN 1000
UID_MAX 60000
# Min/max values for automatic gid selection in groupadd
#
GID_MIN 1000
GID_MAX 60000
```

To which of the following configuration files will the required changes need to be made?

- A. /etc/login.defs
- B. /etc/security/limits.conf
- C. /etc/default/useradd
- D. /etc/profile

Correct Answer: A

Explanation: The required changes need to be made to the /etc/login.defs configuration file. The /etc/login.defs file

defines the default values for user and group IDs, passwords, shells, and other parameters for user and group creation. The file contains the directives `UID_MIN`, `UID_MAX`, `GID_MIN`, and `GID_MAX`, which set the minimum and maximum values for automatic user and group ID selection. The administrator can edit this file and change the values to match the organization's new cybersecurity policies. This is the correct file to modify to accomplish the task. The other options are incorrect because they either do not affect the user and group IDs (`/etc/security/limits.conf` or `/etc/profile`) or do not set the default values (`/etc/default/useradd`). References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 15: Managing Users and Groups, page 463.

QUESTION 14

Which of the following enables administrators to configure and enforce MFA on a Linux system?

- A. Kerberos
- B. SELinux
- C. PAM
- D. PKI

Correct Answer: C

Explanation: The mechanism that enables administrators to configure and enforce MFA on a Linux system is PAM. PAM stands for Pluggable Authentication Modules, which is a framework for managing authentication and authorization on Linux systems. PAM allows the administrator to define the rules and policies for accessing various system resources and services, such as login, sudo, ssh, or cron. PAM also supports different types of authentication methods, such as passwords, tokens, biometrics, or smart cards. PAM can be used to implement MFA, which stands for Multi-Factor Authentication, which is a security technique that requires the user to provide more than one piece of evidence to prove their identity. MFA can enhance the security of the system and prevent unauthorized access. PAM enables administrators to configure and enforce MFA on a Linux system. This is the correct answer to the question. The other options are incorrect because they either do not manage authentication and authorization on Linux systems (Kerberos or PKI) or do not support MFA (SELinux). References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 17: Implementing Basic Security, page 517.

QUESTION 15

The development team wants to prevent a file from being modified by all users in a Linux system, including the root account. Which of the following commands can be used to accomplish this objective?

- A. `chmod / app/conf/file`
- B. `setenforce / app/ conf/ file`
- C. `chattr +i /app/conf/file`
- D. `chmod 0000 /app/conf/file`

Correct Answer: C

The `chattr` command is used to change file attributes on Linux systems that support extended attributes, such as `ext2`, `ext3`, `ext4`, `btrfs`, `xfs`, and others. File attributes are flags that modify the behavior of files and directories.

To prevent a file from being modified by all users in a Linux system, including the root account, the development team

can use the `chattr +i /app/conf/file` command. This command will set the immutable attribute (+i) on the file `/app/conf/file`,

which means that the file cannot be deleted, renamed, linked, appended, or written to by any user or process. To remove the immutable attribute, the development team can use the `chattr -i /app/conf/file` command. The statement C is correct.

The statements A, B, and D are incorrect because they do not prevent the file from being modified by all users. The `chmod /app/conf/file` command does not work because it requires an argument to specify the permissions to change. The

`setenforce /app/conf/file` command does not work because it is used to change the SELinux mode, not file attributes. The `chmod 0000 /app/conf/file` command will remove all permissions from the file, but it can still be modified by the root

account. References: [How to Use chattr Command in Linux]

[Latest XK0-005 Dumps](#)

[XK0-005 VCE Dumps](#)

[XK0-005 Study Guide](#)