CompTIA
XK0-006
CompTIA Linux+ V8 Exam

For More Information – Visit link below:

https://www.examsboost.com/

Product Version

✓ **Up to Date products, reliable and verified.**
✓ **Questions and Answers in PDF Format.**

Latest Version: 10.3

Question: 1

A Linux user runs the following command:
nohup ping comptia.com &
Which of the following commands should the user execute to attach the process to the current terminal?

A. renice
B. jobs
C. exec
D. fg

Answer: D

Explanation:
In Linux system management, controlling processes and job execution is a fundamental skill covered extensively in the CompTIA Linux+ V8 objectives. The command shown combines two important concepts: nohup and background execution using &.
The nohup command is used to run a process immune to hangup signals, meaning the process continues running even after the user logs out or the terminal session ends. By default, nohup detaches the process from the controlling terminal and redirects standard output and standard error to a file named nohup.out. When the ampersand (&) is appended, the process is immediately placed into the background, allowing the shell prompt to return without waiting for the command to finish.
Linux provides job control mechanisms that allow users to manage background and foreground processes within a shell session. The fg command is specifically designed to bring a background job into the foreground and reattach it to the current terminal. Once a job is in the foreground, it can receive input from the terminal and display output directly, and it can also be interrupted using signals such as Ctrl+C.
The other answer choices do not fulfill this requirement. The renice command is used to change the scheduling priority of a running process but does not affect terminal attachment. The jobs command only lists background and stopped jobs associated with the current shell and does not modify their execution state. The exec command replaces the current shell process with a new process, which is unrelated to resuming or attaching background jobs.
According to Linux+ V8 documentation and job control best practices, the correct command to attach a background process to the current terminal is fg. Therefore, option D is the correct answer.

Question: 2

Which of the following best describes a use case for playbooks in a Linux system?

A. To provide a set of tasks and configurations to deploy an application

B. To provide the instructions for implementing version control on a repository
C. To provide the security information required for a container
D. To provide the storage volume information required for a pod

| **Answer: A** |

Explanation:
In the context of Linux automation and orchestration, playbooks are most commonly associated with configuration management tools such as Ansible, which is explicitly referenced in the CompTIA Linux+ V8 objectives. Playbooks are written in YAML and are designed to define a series of tasks, configurations, and desired system states that should be applied to one or more Linux systems in a repeatable and automated manner.
A primary use case for playbooks is application deployment and system configuration automation. Playbooks allow administrators to specify tasks such as installing packages, configuring services, managing users, setting permissions, deploying application files, and starting or enabling services. This aligns directly with option A, which accurately describes playbooks as a method to provide a set of tasks and configurations required to deploy an application consistently across environments.
The remaining options are not accurate representations of playbook functionality. Option B refers to version control implementation, which is handled by tools like Git and is not the purpose of playbooks themselves, although playbooks may be stored in version control systems. Option C describes container security information, which is typically managed through container runtime configurations, secrets, or security policies rather than playbooks. Option D refers to storage volume information for a pod, which is specific to Kubernetes manifests and not a general Linux playbook use case.
According to Linux+ V8 documentation, automation tools and playbooks help reduce human error, improve consistency, and support Infrastructure as Code (IaC) practices. Playbooks are a key mechanism for orchestrating multi-step operations across multiple systems, making them essential for modern Linux system administration.
Therefore, the correct answer is A, as it best describes the practical and documented use case for playbooks in a Linux system.

Question: 3

A systems administrator receives reports about connection issues to a secure web server. Given the following firewall and web server outputs:
Firewall output:
Status: active
To Action From
443/tcp DENY Anywhere
443/tcp (v6) DENY Anywhere (v6)
Web server output:
tcp LISTEN 0 4096 *:443 :
Which of the following commands best resolves this issue?

A. ufw disable
B. ufw allow 80/tcp

C. ufw delete deny https/tcp
D. ufw allow 4096/tcp

<div align="right">

Answer: C

</div>

Explanation:
This scenario involves firewall configuration and service accessibility, which falls under the Security domain of the CompTIA Linux+ V8 objectives. The key to resolving this issue is interpreting both the firewall output and the web server status correctly.
The web server output shows that the service is actively listening on TCP port 443, which is the standard port for HTTPS (secure web traffic). The line tcp LISTEN 0 4096 *:443 *:* confirms that the web server is running properly and is ready to accept incoming connections on port 443 from any interface. This indicates that the problem is not with the web server configuration itself.
However, the firewall output clearly shows that incoming connections to port 443 are being blocked. The rules 443/tcp DENY Anywhere and 443/tcp (v6) DENY Anywhere (v6) indicate that the Uncomplicated Firewall (UFW) is explicitly denying HTTPS traffic for both IPv4 and IPv6. As a result, external clients cannot establish a secure connection to the server, even though the service is running correctly.
To resolve this issue securely and correctly, the administrator must remove the firewall rule that denies HTTPS traffic. Option C, ufw delete deny https/tcp, directly removes the blocking rule while preserving the rest of the firewall configuration. This aligns with Linux+ best practices, which emphasize making precise firewall changes rather than disabling security controls entirely.
The other options are incorrect. Option A, ufw disable, would completely turn off the firewall, creating a significant security risk. Option B, ufw allow 80/tcp, only opens HTTP traffic on port 80 and does not resolve HTTPS connectivity issues. Option D, ufw allow 4096/tcp, incorrectly attempts to open an internal socket backlog value rather than a valid service port.
Therefore, the correct and most secure solution is C.

Question: 4

Which of the following utilities supports the automation of security compliance and vulnerability management?

A. SELinux
B. Nmap
C. AIDE
D. OpenSCAP

<div align="right">

Answer: D

</div>

Explanation:
Security compliance and vulnerability management are critical components of Linux system administration, and CompTIA Linux+ V8 places strong emphasis on automated security assessment tools. OpenSCAP is specifically designed to address these requirements.
OpenSCAP is an open-source framework that implements the Security Content Automation Protocol

(SCAP), a set of standards used for automated vulnerability scanning, configuration compliance checking, and security auditing. It allows administrators to assess Linux systems against established security baselines such as CIS benchmarks, DISA STIGs, and organizational security policies. This makes OpenSCAP the most appropriate tool for automating both compliance and vulnerability management.

The other options serve different security-related purposes but do not fulfill the automation requirement. SELinux is a mandatory access control system that enforces security policies at runtime but does not perform compliance scanning or vulnerability assessments. Nmap is a network scanning and discovery tool used to identify open ports and services, not compliance automation. AIDE (Advanced Intrusion Detection Environment) is a file integrity monitoring tool that detects unauthorized file changes but does not evaluate overall system compliance.

Linux+ V8 documentation highlights OpenSCAP as a tool used to automate security audits, generate compliance reports, and integrate with configuration management workflows. Its ability to standardize security checks across multiple systems makes it essential in enterprise and regulated environments.

Therefore, the correct answer is D. OpenSCAP.

Question: 5

Which of the following filesystems contains non-persistent or volatile data?

A. /boot
B. /usr
C. /proc
D. /var

Answer: C

Explanation:
Understanding Linux filesystems and their purposes is a fundamental system management skill outlined in the Linux+ V8 objectives. Among the listed options, /proc is the filesystem that contains non-persistent, volatile data.

The /proc filesystem is a virtual filesystem that exists entirely in memory and is dynamically generated by the Linux kernel. It does not store data on disk and does not persist across system reboots. Instead, /proc provides real-time information about running processes, kernel parameters, system memory, CPU statistics, and hardware state. Files within /proc represent kernel data structures and change constantly as the system operates.

The other filesystems contain persistent data stored on disk. /boot stores bootloader files and kernel images, which are critical for system startup. /usr contains user applications, libraries, and documentation, all of which are persistent. /var holds variable data such as logs, spool files, and caches, which may change frequently but are still stored persistently on disk.

Linux+ V8 documentation emphasizes that /proc is used primarily for system monitoring and tuning. Administrators often interact with /proc to inspect process details or modify kernel parameters using tools like sysctl. Because its contents are generated at runtime and cleared on reboot, /proc is classified as non-persistent or volatile.

Therefore, the correct answer is C. /proc.

Thank You for Trying Our Product

For More Information – **Visit link below:**

https://www.examsboost.com/

15 USD Discount Coupon Code:

G74JA8UF

FEATURES

- ✓ **90 Days Free Updates**

- ✓ **Money Back Pass Guarantee**

- ✓ **Instant Download or Email Attachment**

- ✓ **24/7 Live Chat Support**

- ✓ **PDF file could be used at any Platform**

- ✓ **50,000 Happy Customer**