Download CompTIA XK0-006 Exam Dumps Free

Shared by Blair on 17-06-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A systems administrator needs to open the DNS TCP port on a Linux system from network 10.0.0.0/24. Which option best commands should the administrator use for this task?

Options:

A- ufw allow dns/tcp to 10.0.0.0/24
B- ufw enable 53/tcp from 10.0.0.0/24
C- ufw allow 53/tcp from 10.0.0.0/24
D- ufw disable from 10.0.0.0/24

Answer:

C

Explanation:

Firewall configuration is a key topic in the Security domain of CompTIA Linux+ V8. DNS primarily uses UDP port 53, but TCP port 53 is also required for zone transfers, large responses, and certain reliability scenarios. In this case, the administrator explicitly needs to allow DNS over TCP from a specific network.

The correct command is ufw allow 53/tcp from 10.0.0.0/24. This rule allows incoming TCP traffic on port 53 only from the specified subnet, following the principle of least privilege. Linux+ V8 documentation emphasizes restricting firewall rules by source network whenever possible to minimize attack surfaces.

Option A is incorrect because UFW service aliases like dns are not always guaranteed to map explicitly to TCP, and the syntax is incomplete. Option B is invalid because ufw enable is used to enable the firewall globally and does not define rules. Option D disables firewall protections and introduces a major security risk.

Linux+ V8 best practices stress precise, minimal firewall rules instead of broad or disabling actions. Therefore, C is the correct and secure choice.

Question 2

Question Type: MultipleChoice

A Linux administrator is making changes to local files that are part of a Git repository. The administrator needs to retrieve changes from the remote Git repository. Which option best commands should the administrator use to save the local modifications for later review?

Options:

A- git stash
B- git pull
C- git merge
D- git fetch

Answer:

A

Explanation:

In Git-based workflows, especially those used in DevOps environments, it is common for administrators to have uncommitted local changes while needing to retrieve updates from a remote repository. Linux+ V8 emphasizes understanding how to safely manage local modifications during synchronization operations.

The command git stash is specifically designed for this scenario. It temporarily saves (or ''stashes'') local changes in a stack-like structure and reverts the working directory to a clean state that matches the current HEAD. This allows the administrator to perform operations such as git pull without conflicts. Later, the stashed changes can be reapplied using git stash apply or git stash pop.

The other options are incorrect. git pull retrieves and merges remote changes but will fail or cause conflicts if local modifications exist. git merge combines branches and does not save uncommitted changes. git fetch downloads remote references but does not address local working directory changes.

Linux+ V8 documentation highlights git stash as a safe and reversible way to protect local work during repository updates. Therefore, the correct answer is A.

Question 3

Question Type: MultipleChoice

Which of the following can reduce the attack surface area in relation to Linux hardening?

Options:

A- Customizing the log-in banner
B- Reducing the number of directories created
C- Extending the SSH startup timeout period
D- Enforcing password strength and complexity

Answer:

D

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

Reducing the attack surface area in Linux hardening refers to limiting possible points of unauthorized access. According to the CompTIA Linux+ Official Study Guide (Exam XK0-006), enforcing strong password policies is a critical aspect of security hardening. This practice ensures that user accounts are protected by passwords that are difficult to guess or crack, thus minimizing the risk of successful brute-force attacks. Implementing password complexity requirements (such as minimum length, use of uppercase, lowercase, numbers, and special characters) directly addresses one of the primary vectors for unauthorized access.

Other options do not have a direct impact on reducing the attack surface:

A . Customizing the log-in banner serves as a legal notification and does not affect system vulnerabilities.

B . Reducing the number of directories created is not related to hardening or access control.

C . Extending the SSH startup timeout period may give attackers more time to attempt a connection and does not increase security.

CompTIA Linux+ Study Guide: Exam XK0-006, Sybex, Chapter 11: 'Securing the System', Section: 'Implementing Password Policies'

CompTIA Linux+ XK0-006 Exam Objectives, Domain 3.0: Security

Question 4

Question Type: MultipleChoice

A systems administrator wants to review the logs from an Apache 2 error.log file in real time and save the information to another file for later review. Which of the following commands should the

administrator use?

Options:

A- tail -f /var/log/apache2/error.log > logfile.txt
B- tail -f /var/log/apache2/error.log | logfile.txt
C- tail -f /var/log/apache2/error.log >> logfile.txt
D- tail -f /var/log/apache2/error.log | tee logfile.txt

Answer:

D

Explanation:

Log monitoring is a common troubleshooting task in Linux system administration, and Linux+ V8 covers command-line tools for real-time log analysis. The requirement in this scenario is twofold: view log entries as they occur and simultaneously save them to another file.

The command tail -f /var/log/apache2/error.log | tee logfile.txt fulfills both requirements. The tail -f command follows the log file in real time, displaying new entries as they are written. The pipe (|) sends this output to the tee command, which writes the data to logfile.txt while also displaying it on standard output.

The other options are insufficient. Option A redirects output to a file but prevents real-time viewing. Option C appends output but still suppresses terminal display. Option B is syntactically invalid and does not use a proper command for writing output.

Linux+ V8 documentation specifically references tee as a useful utility for duplicating command output streams. This makes option D the correct and most effective solution.

Question 5

Question Type: MultipleChoice

An administrator receives reports that a web service is not responding. The administrator reviews the following outputs:

```
$ echo $PWD
/etc/pki/nginx

$ ls -lRt
.:
total 8
drwxr-xr-x. 2 root root 6 Jul 10 10:57 private
-rw-r--r--. 1 root root 895 Jul 10 10:56 server.crt
-rw-------. 1 root root 227 Jul 10 10:56 server.key
./private:
total 0

$ sudo systemctl status nginx
  nginx.service - The nginx HTTP and reverse proxy server
       Loaded: loaded (/usr/lib/systemd/system/nginx.service; disabled; preset: disabled)
       Active: failed (Result: exit-code) since Wed 2023-11-01 06:56:51 EDT; 6s ago
    Process: 110551 ExecStartPre=/usr/bin/rm -f /run/nginx.pid (code=exited, status=0/SUCCESS)
    Process: 110552 ExecStartPre=/usr/sbin/nginx -t (code=exited, status=1/FAILURE)
       CPU: 144ms

Nov 01 06:56:51 webserver systemd[1]: Starting nginx.service - The nginx HTTP and reverse proxy server...
Nov 01 06:56:51 webserver nginx[110552]: nginx: [emerg] cannot load certificate key "/etc/pki/nginx/private/server.key": BIO_new_file()
failed (SSL: error:80000002:system library::No such file or directory:calli>
Nov 01 06:56:51 webserver nginx[110552]: nginx: configuration file /etc/nginx/nginx.conf test failed
Nov 01 06:56:51 webserver systemd[1]: nginx.service: Control process exited, code=exited, status=1/FAILURE
Nov 01 06:56:51 webserver systemd[1]: nginx.service: Failed with result 'exit-code'.
Nov 01 06:56:51 webserver systemd[1]: Failed to start nginx.service - The nginx HTTP and reverse proxy server.
```

Which of the following is the reason the web service is not responding?

Options:

A- The private key needs to be renamed from server.crt to server, key so the service can find it.
B- The private key does not match the public key, and both keys should be replaced.
C- The private key is not in the correct location and needs to be moved to the correct directory.
D- The private key has the incorrect permissions and should be changed to 0755 for the service.

Answer:

C

Explanation:

This issue falls under the Troubleshooting domain of the CompTIA Linux+ V8 objectives, specifically service startup failures and certificate-related errors. The provided output clearly indicates that the NGINX service fails during startup due to an inability to locate the private key file.

The critical error message is:

cannot load certificate key '/etc/pki/nginx/private/server.key': No such file or directory

This message confirms that NGINX is explicitly configured to look for the private key in the directory /etc/pki/nginx/private/. However, the directory listing shows that the private directory exists but is empty, while the server.key file is located in /etc/pki/nginx/ instead. Because NGINX cannot find the private key at the configured path, the configuration test (nginx -t) fails, and systemd prevents the service from starting.

Option C correctly identifies the root cause: the private key is not in the correct location. Moving server.key into /etc/pki/nginx/private/ (or updating the NGINX configuration to match the current

location) would resolve the issue. Linux+ V8 documentation stresses that service failures often result from misaligned configuration paths rather than corrupted files.

The other options are incorrect. Option A incorrectly refers to renaming a certificate file and does not address the path issue. Option B suggests a key mismatch, which would generate a different SSL error rather than a ''file not found'' error. Option D is also incorrect because private keys should not have executable permissions like 0755; typically, they are restricted (for example, 0600) for security reasons.

Therefore, the web service is not responding because the private key file is not located in the directory expected by the NGINX configuration. The correct answer is C.

Question 6

Question Type: MultipleChoice

Users cannot access an application that is running inside containers. The administrator wants to validate whether the containers are running. Which of the following commands should the administrator use?

Options:

A- docker start
B- docker ps
C- docker run
D- docker images

Answer:

B

Explanation:

Container troubleshooting is a key competency within the Automation, Orchestration, and Scripting domain of CompTIA Linux+ V8. When users report that an application running inside containers is not accessible, one of the first validation steps is to confirm whether the containers are currently running.

The docker ps command is specifically designed to list running containers on the system. By default, it displays container IDs, image names, command executed, uptime, port mappings, and container names. This allows administrators to quickly determine whether the application container is active and whether it is exposing the expected ports. This aligns directly with Linux+

V8 guidance on container lifecycle management and operational validation.

The other options are not suitable for this purpose. docker start is used to start one or more stopped containers but does not display container status. docker run creates and starts a new container, which is not appropriate when the goal is only to check the status of existing containers. docker images lists locally available container images but provides no information about running or stopped containers.

Linux+ V8 documentation emphasizes the importance of using the correct Docker subcommands when diagnosing containerized applications. Verifying container runtime state using docker ps is a foundational troubleshooting step before investigating networking, firewall rules, or application-level errors.

Therefore, the correct command to validate whether containers are running is docker ps, making Answer B correct.

Question 7

Question Type: MultipleChoice

Following the completion of monthly server patching, a Linux administrator receives reports that a critical application is not functioning. Which option best commands should help the administrator determine which packages were installed?

Options:

A- dnf history
B- dnf list
C- dnf info
D- dnf search

Answer:

A

Explanation:

Package management troubleshooting is a critical Linux administration skill addressed in CompTIA Linux+ V8. After system patching, identifying which packages were installed, updated, or removed is often the first step in diagnosing application failures.

The dnf history command is specifically designed for this purpose. It displays a chronological list

of all DNF transactions, including installations, upgrades, downgrades, and removals. Each transaction is assigned an ID and includes timestamps, affected packages, and actions taken. This allows administrators to correlate application failures with recent changes.

Option A is correct because it provides historical context rather than just current package state. Linux+ V8 documentation highlights dnf history as an essential auditing and rollback tool.

The other options are insufficient. dnf list shows installed or available packages but does not indicate when they were installed. dnf info displays metadata for a specific package but does not show transaction history. dnf search is used to find packages by name or description.

By reviewing recent transactions with dnf history, administrators can quickly identify problematic updates and take corrective action, such as rolling back a package.

Therefore, the correct answer is A.

P2P exams