CompTIA

Exam Questions XK0-006

CompTIA Linux+ Exam

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
A systems administrator is reconfiguring existing user accounts in a Linux system. Which of the following commands should the administrator use to include "myuser" in the finance group?

A. groupadd finance myuser
B. groupmod finance myuser
C. useradd -g finance myuser
D. usermod -aG finance myuser

Answer: D

Explanation:
Comprehensive and Detailed Explanation: From Exact Extract:
To add an existing user (myuser) to an existing group (finance) without removing them from other groups, the correct command is usermod -aG finance myuser.
The -aG option appends the user to the supplementary group
(s) specified.
Other options:

A. groupadd is for creating new groups, not adding users to groups.

B. groupmod is for modifying group properties, not user membership.

C. useradd creates new users; not applicable to existing users.

Reference:
CompTIA Linux+ Study Guide: Exam XK0-006, Sybex, Chapter 6: "User and Group Management", Section: "Modifying Group Membership"
CompTIA Linux+ XK0-006 Objectives, Domain 1.0: System Management
==========

NEW QUESTION 2
An administrator updates the network configuration on a server but wants to ensure the change will not cause an outage if something goes wrong. Which of the following commands allows the administrator to accomplish this goal?

A. netplan try
B. netplan rebind
C. netplan ip
D. netplan apply

Answer: A

Explanation:
Network configuration changes can cause immediate loss of connectivity if applied incorrectly. Linux+ V8 emphasizes safe configuration practices, particularly when managing remote systems.
The netplan try command applies network configuration changes temporarily and prompts the administrator to confirm them within a timeout period. If the administrator does not confirm, Netplan automatically rolls back to the previous working configuration. This prevents accidental outages caused by misconfigured network settings.
The netplan apply command makes changes permanent immediately and does not provide rollback protection. The other options are not valid Netplan commands.
Linux+ V8 documentation explicitly references netplan try as a safe testing mechanism. Therefore, the correct answer is A.

NEW QUESTION 3
A Linux administrator needs to create and then connect to the app-01-image container. Which of the following commands accomplishes this task?

A. docker run -it app-01-image
B. docker start -td app-01-image
C. docker build -ic app-01-image
D. docker exec -dc app-01-image

Answer: A

Explanation:
Comprehensive and Detailed 250 to 350 words of Explanation: From Linux+ V8 documents:
Container lifecycle management is a core topic within the Automation, Orchestration, and Scripting domain of CompTIA Linux+ V8. Administrators must understand the difference between creating containers, starting containers, and executing commands within running containers.
The correct command is docker run -it app-01-image. The docker run command performs three actions at once: it creates a new container from the specified image, starts the container, and optionally attaches the administrator??s terminal to it. The -i option keeps standard input open, while the -t option allocates a pseudo- terminal (TTY). Together, these options allow the administrator to interactively connect to the container immediately after it is created.
The other options are incorrect for the following reasons. docker start is used only to start an existing stopped container and does not create a new container from an image. Additionally, -t and -d are not valid options for attaching an interactive terminal during container startup. docker build is used to build a Docker image from a Dockerfile and cannot be used to create or connect to a container. docker exec is used to run commands inside an already running container and therefore cannot be used to create a container.
Linux+ V8 documentation emphasizes that docker run is the primary command used when administrators want to instantiate containers from images and interact with them. This command is commonly used during testing, development, and troubleshooting workflows.

NEW QUESTION 4
A systems administrator is preparing a Linux system for application setup. The administrator needs to create an environment variable with a persistent value in one of the user accounts. Which of the following commands should the administrator use for this task?

A. export "VAR=SomeValue" >> ~/.ssh/profile
B. export VAR=value

C. VAR=value
D. echo "export VAR=value" >> ~/.bashrc

Answer: D

Explanation:
Environment variables are widely used in Linux systems to configure application behavior, and Linux+ V8 emphasizes the distinction between temporary and persistent variables. A variable is persistent only if it is defined in a shell initialization file.
The correct approach is echo "export VAR=value" >> ~/.bashrc. This command appends the variable definition to the user??s .bashrc file, ensuring the variable is set automatically every time the user starts a new shell session. This makes the variable persistent for that specific user.
Options B and C only define variables in the current shell session and are lost when the session ends. Option A incorrectly targets the SSH configuration directory and is not appropriate for defining shell environment variables.
Linux+ V8 documentation highlights .bashrc, .bash_profile, and /etc/profile as correct locations for persistent environment variables. Therefore, the correct answer is D.

NEW QUESTION 5
In the echo "profile-$num-$name" line of a shell script, the variable $num seems to not be expanding during execution. Which of the following notations ensures the value is expanded?

A. echo "profile-$(num)-$name"
B. echo 'profile-$num-$name'
C. echo "profile-'$num'-$name"
D. echo "profile-${num}-$name"

Answer: D

Explanation:
Shell variable expansion is a fundamental scripting concept included in Linux+ V8 objectives. In Bash and similar shells, variables are expanded only when they are interpreted within double quotes or unquoted contexts, and sometimes explicit syntax is required to avoid ambiguity.
The correct notation is ${num}, as shown in option D. Using curly braces around the variable name ensures the shell correctly identifies the variable boundary, especially when it is adjacent to other characters. This guarantees proper expansion of the variable's value.
The other options are incorrect. Single quotes prevent variable expansion entirely. The $(...) syntax is used for command substitution, not variable expansion. Quoting the variable name itself also prevents expansion.
Linux+ V8 documentation emphasizes ${VAR} notation as a best practice in shell scripting for clarity and correctness. Therefore, the correct answer is D.

NEW QUESTION 6
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,playbooksare most commonly associated with configuration management tools such asAnsible, which is explicitly referenced in the CompTIA Linux+ V8 objectives. Playbooks are written in YAML and are designed to definea series of tasks, configurations, and desired system statesthat should be applied to one or more Linux systems in a repeatable and automated manner.
A primary use case for playbooks isapplication 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 optionA, 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. OptionBrefers 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. OptionCdescribes container security information, which is typically managed through container runtime configurations, secrets, or security policies rather than playbooks. OptionDrefers 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 isA, as it best describes the practical and documented use case for playbooks in a Linux system.

NEW QUESTION 7
Which of the following commands should a Linux administrator use to determine the version of a kernel module?

A. modprobe bluetooth
B. lsmod bluetooth
C. depmod bluetooth
D. modinfo bluetooth

Answer: D

Explanation:
Kernel module management is an important part of Linux system administration and is covered in the Linux+ V8 objectives. When an administrator needs to determine metadata about a kernel module—such as itsversion, author, description, license, filename, and dependencies—the correct tool is modinfo.
The commandmodinfo bluetoothdisplays detailed information about the specified kernel module, including the module version if it is defined. This makes it the correct and intended command for retrieving version details of kernel modules, whether or not the module is currently loaded.
The other options are incorrect. modprobe bluetooth is used to load or unload kernel modules and does not display version information. lsmod lists loaded modules but does not show version details and does not accept module names as arguments in that manner. depmod is used to generate module dependency information and does not provide module metadata to the administrator.

Linux+ V8 documentation specifically references modinfo as the utility for inspecting kernel module properties. This command is essential for troubleshooting driver issues, verifying compatibility, and auditing kernel components.
Therefore, the correct answer isD. modinfo bluetooth.

NEW QUESTION 8
Which of the following utilities supports the automation of security compliance and vulnerability management?

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

Answer: D

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.OpenSCAPis specifically designed to address these requirements.
OpenSCAP is an open-source framework that implements theSecurity 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 asCIS 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.SELinuxis a mandatory access control system that enforces security policies at runtime but does not perform compliance scanning or vulnerability assessments.Nmapis 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 isD. OpenSCAP.

NEW QUESTION 9
A systems administrator needs to open the DNS TCP port on a Linux system from network 10.0.0.0/24. Which of the following commands should the administrator use for this task?

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 theSecuritydomain of CompTIA Linux+ V8. DNS primarily uses UDP port 53, butTCP port 53is also required for zone transfers, large responses, and certain reliability scenarios. In this case, the administrator explicitly needs to allowDNS over TCPfrom 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 ofleast privilege. Linux+ V8 documentation emphasizes restricting firewall rules by source network whenever possible to minimize attack surfaces.
OptionAis incorrect because UFW service aliases like dns are not always guaranteed to map explicitly to TCP, and the syntax is incomplete. OptionBis invalid because ufw enable is used to enable the firewall globally and does not define rules. OptionDdisables firewall protections and introduces a major security risk.
Linux+ V8 best practices stress precise, minimal firewall rules instead of broad or disabling actions. Therefore,Cis the correct and secure choice.

NEW QUESTION 10
While hardening a system, an administrator runs a port scan with Nmap, which returned the following output:

```
# nmap 104.21.75.76
Starting Nmap 7.80 ( https://nmap.org ) at 2024-07-09 18:09 UTC
Nmap scan report for 104.21.75.76
Host is up (0.00087s latency).
Not shown: 996 closed ports
PORT STATE SERVICE
23/tcp open telnet
80/tcp open http
443/tcp open https
8080/tcp open http-proxy

Nmap done: 1 IP address (1 host up) scanned in 4.93 seconds
```

Which of the following is the best way to address this security issue?

A. Configuring a firewall to block traffic on port 23 on the server
B. Changing the system administrator's password to prevent unauthorized access
C. Closing port 80 on the network switch to block traffic

D. Disabling and removing the Telnet service on the server

Answer: D

Explanation:
This scenario falls under theSecuritydomain of the CompTIA Linux+ V8 objectives and focuses on system hardening and service minimization. The Nmap scan output reveals thatport 23 (Telnet)is open on the system, which represents a significant security risk.
Telnet is an insecure, legacy protocol that transmits authentication credentials and session data inplaintext, making it vulnerable to interception through packet sniffing or man-in-the-middle attacks. Linux+ V8 documentation explicitly emphasizes the principle ofleast functionality, which states that unnecessary or insecure services should be disabled and removed entirely rather than merely restricted.
OptionD, disabling and removing the Telnet service on the server, is the best and most secure solution. This action eliminates the vulnerable service completely, ensuring that it cannot be exploited internally or externally. In secure Linux environments, Telnet should be replaced withSSH, which provides encrypted communication and strong authentication mechanisms.
OptionA, blocking port 23 with a firewall, reduces exposure but does not eliminate the underlying risk. If the firewall rules are misconfigured or bypassed, the Telnet service would still be available. Linux+ V8 best practices recommend removing insecure services rather than relying solely on perimeter controls.
OptionBis unrelated, as changing passwords does not address the risk of plaintext credential transmission. OptionCis incorrect because closing ports at the network switch level is not an appropriate or scalable solution for host-level service hardening and does not address internal access risks.
Linux+ V8 documentation consistently highlights service auditing, port scanning, and removal of insecure protocols as essential system hardening steps.
Therefore, the most effective and secure remediation is to disable and remove the Telnet service.

NEW QUESTION 10
A systems administrator attempts to edit a file as root, but receives the following error:

```
E212: Cannot open file for writing

# ls -l /etc/resolv.conf
-rw-------. 1 root admin 141 May 30 11:00 /etc/resolv.conf

# lsattr /etc/resolv.conf
----i-----------  /etc/resolv.conf
```

Which of the following commands allows the administrator to edit the file?

A. chown root /etc/resolv.conf
B. chattr -i /etc/resolv.conf
C. chmod 750 /etc/resolv.conf
D. chgrp root /etc/resolv.conf

Answer: B

Explanation:
This scenario involves Linux file attributes and falls under theSystem Managementdomain of the CompTIA Linux+ V8 objectives. Although the administrator is operating as the root user, the system prevents the file from being modified. This behavior indicates that standard UNIX permissions are not the root cause of the problem.
The critical clue is provided by the lsattr /etc/resolv.conf output, which shows theimmutable (i) attributeset on the file. When a file is marked immutable, it cannot be modified, deleted, renamed, or written to by any user, including root. This restriction overrides normal file permissions and ownership settings.
The chattr command is used to modify extended file attributes on Linux filesystems such as ext4. The option -i specifically removes the immutable attribute, restoring the file??s ability to be edited. Therefore, running chattr -i /etc/resolv.conf allows the administrator to open and modify the file successfully.
The other options do not resolve the issue. chown root changes file ownership, but the file is already owned by root. chmod 750 modifies permission bits, but permissions are ignored when the immutable attribute is set. chgrp root changes the group ownership, which also has no effect when immutability is enforced.
Linux+ V8 documentation highlights immutable files as a security and stability feature, commonly used to protect critical configuration files from accidental or unauthorized changes. Administrators must explicitly remove this attribute before making modifications.
Therefore, the correct command to allow editing the file isB. chattr -i /etc/resolv.conf.

NEW QUESTION 11
An administrator added a new disk to expand the current storage. Which of the following commands should the administrator run first to add the new disk to the LVM?

A. vgextend
B. lvextend
C. pvcreate
D. pvresize

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
To add a new physical disk to LVM, the disk must first be initialized as a physical volume using the pvcreate command. This prepares the new disk for use by the LVM subsystem. After initializing with pvcreate, you would use vgextend to add the new physical volume to an existing volume group.
Other options:
* A.vgextend adds a physical volume to a volume group, but you must use pvcreate first.
* B.lvextend is used to increase the size of a logical volume, not to add a new disk.
* D.pvresize is used to resize an existing physical volume, not to create one.
[Reference:, CompTIA Linux+ Study Guide: Exam XK0-006, Sybex, Chapter 7: "Managing Storage", Section: "Managing Logical Volumes", CompTIA Linux+ XK0-006 Objectives, Domain 4.0: Storage and Filesystems, ,]

NEW QUESTION 15
An administrator must secure an account for a user who is going on extended leave. Which of the following steps should the administrator take?(Choose two)

A. Set the user's files to immutable.
B. Instruct the user to log in once per week.
C. Delete the user's /home folder.
D. Run the command passwd -l user.
E. Change the date on the /home folder to that of the expected return date.
F. Change the user's shell to /sbin/nologin.

Answer: DF

Explanation:
Comprehensive and Detailed 250 to 350 words of Explanation From Linux+ V8 documents:
Securing dormant or temporarily unused user accounts is a best practice emphasized in theSecuritydomain of CompTIA Linux+ V8. When a user goes on extended leave, the goal is toprevent unauthorized accesswhile preserving the user??s data and account for future use.
The most effective approach is todisable authentication and interactive login accesswithout deleting the account. OptionD, running passwd -l user, locks the user??s password by prepending an invalid character to the encrypted password in /etc/shadow. This prevents password-based authentication while retaining the account, files, and ownership information. Linux+ V8 documentation highlights password locking as a standard method for temporarily disabling accounts.
OptionF, changing the user??s shell to /sbin/nologin, further strengthens account security by preventing interactive shell access entirely. Even if another authentication mechanism were attempted, the user would be denied a login shell. This is a common defense-in-depth measure and is explicitly referenced in Linux+ V8 objectives for access control and account hardening.
The other options are incorrect or inappropriate. OptionA(immutable files) does not prevent account access and may interfere with system operations. OptionBdefeats the purpose of securing an inactive account. OptionCdeletes user data, which is unnecessary and risky. OptionEhas no security effect, as filesystem timestamps do not control access.
Linux+ V8 stresses that secure account management should bereversible, auditable, and minimally disruptive. Locking the password and disabling the login shell meet these criteria and are commonly used together in enterprise environments.

NEW QUESTION 20
An administrator is trying to terminate a process that is not responding. Which of the following commands should the administrator use in order to force the termination of the process?

A. kill PID
B. kill -1 PID
C. kill -9 PID
D. kill -15 PID

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The kill command is used to send signals to processes. The -9 option sends the SIGKILL signal, which immediately terminates the process and cannot be caught or ignored by the process. This is used as a last resort when a process is not responding to the default (SIGTERM, -15) or other signals. The SIGKILL signal guarantees termination.
Other options:
* A.Default kill sends SIGTERM (-15), which requests a graceful shutdown but can be ignored.
* B.-1 sends SIGHUP, used to reload configuration, not terminate.
* D.-15 sends SIGTERM, not guaranteed to kill an unresponsive process.
[Reference:, CompTIA Linux+ Study Guide: Exam XK0-006, Sybex, Chapter 3: "Managing Processes", Section: "Sending Signals to Processes", CompTIA Linux+ XK0-006 Objectives, Domain 1.0: System Management, ,]

NEW QUESTION 22
A Linux administrator receives reports that an application hosted in a system is not completing tasks in the allocated time. The administrator connects to the system and obtains the following details:

```
# uptime
12:47:43 up 22:17, 2 users, load average: 7.75, 5.72, 5.17

# nproc
4

# vmstat -w 1 3
[...]
r b swpd free    buffcachesisobibo in   cs   us syidwa stgu
8 0671563760348103671476 0  0  0  040901386100 0  0  0  0  0
8 0671563760348103671476 0  0  0  040761389100 0  0  0  0  0
8 0671563760348103671476 0  0  0  040761389100 0  0  0  0  0

# free -h
       total  used  free shared buff/cache available
Mem:   3.8Gi 334Mi 3.6Gi   20Mi       70Mi     3.5Gi
Swap:  7.8Gi  65Mi 7.8Gi
```

Which of the following actions can the administrator take to help speed up the jobs?

A. Increase the amount of free memory available to the system.
B. Increase the amount of CPU resources available to the system.
C. Increase the amount of swap space available to the system.
D. Increase the amount of disks available to the system.

Answer: B

Explanation:
This scenario represents a classic CPU-bound performance issue, which is covered under the Troubleshooting domain of CompTIA Linux+ V8. The most important indicator is the load average compared to the number of available CPU cores.
The system has 4 CPU cores, as shown by nproc, but the load averages are consistently above 5, with a peak of 7.75. Load average reflects the number of processes either actively running on the CPU or waiting for CPU time. When the load average exceeds the number of CPU cores for extended periods, it indicates CPU contention. Processes must wait longer to be scheduled, resulting in delayed task completion.
The memory statistics confirm that memory is not the bottleneck. free -h shows over 3.5 GiB of available memory, and swap usage is minimal. Additionally, vmstat shows no significant swap-in or swap-out activity and low I/O wait, ruling out memory pressure and disk bottlenecks.
Increasing swap space would not help because the system is not memory constrained. Adding more disks would not address CPU scheduling delays. Increasing free memory is unnecessary because sufficient memory is already available.
Linux+ V8 documentation emphasizes correlating load average with CPU core count to diagnose CPU saturation. The most effective way to speed up job execution in this case is to increase CPU resources, such as adding more vCPUs, moving the workload to a more powerful system, or distributing the workload across multiple systems.
Therefore, the correct answer is B. Increase the amount of CPU resources available to the system.

NEW QUESTION 27
A user states that an NFS share Is reporting random disconnections. The systems administrator obtains the following information

```
#df -h
Filesystem           Size  Used Avail Use% Mounted on
/dev/mapper/fedora-
root                 15G   15G  204K  100% /
devtmpfs             4.0M  0    4.0M  0%   /dev
tmpfs                2.0G  0    2.0G  0%   /dev/shm
tmpfs                783M  816K 782M  1%   /run
tmpfs                2.0G  0    2.0G  0%   /tmp
/dev/vda2            960M  481M 480M  51%  /boot
10.0.0.1:/nfsdata    4T    3.8T 200G  95%  /share

$ ip -s link show
2: enp1s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mode DEFAULT group default qlen
link/ether 52:5a:00:f7:27:23 brd ff:ff:ff:ff:ff:ff
RX:  bytes      packets   errors   dropped   missed   mcast
     108487310  149198    9584     40721     0        0
TX:  bytes      packets   errors   dropped   carrier  collsns
     3015941    33656     12780    7854      0        0
```

Which of the following best explains the symptoms that are being reported?

A. The mount point is incorrect for the NFS share.
B. The IP address of the NFS share is incorrect.
C. The filesystem is nearly full and is reporting errors.
D. The interface is reporting a high number of errors and dropped packets.

Answer: D

Explanation:
This issue is best analyzed using a layered troubleshooting approach, as recommended in the Troubleshooting domain of CompTIA Linux+ V8. The reported symptom is intermittent or random disconnections from an NFS share, which commonly indicates a network reliability issue rather than a configuration or filesystem problem.
The most critical evidence comes from the output of ip -s link show. The network interface enp1s0 is reporting significant numbers of errors and dropped packets on both the receive (RX) and transmit (TX) paths. High packet loss at the network interface level directly affects protocols like NFS, which rely on stable, continuous TCP/IP communication. When packets are dropped or corrupted, NFS clients may experience timeouts, retransmissions, and apparent disconnections.
Although the df -h output shows that the NFS filesystem is 95% full, this alone does not typically cause random disconnections. A nearly full filesystem may lead to write failures or performance degradation, but it does not explain intermittent connectivity loss. Linux+ V8 documentation notes that filesystem capacity issues usually present as I/O errors, not transport-layer disconnects.
Options A and B can also be ruled out. If the mount point or IP address were incorrect, the NFS share would fail consistently rather than intermittently. The fact that the share is mounted and accessible confirms that the mount configuration and IP addressing are correct.
Linux+ V8 emphasizes that NFS performance and reliability are highly sensitive to network quality. Packet errors, drops, faulty NICs, cabling issues, duplex mismatches, or driver problems commonly result in unstable NFS behavior.
Therefore, the best Explanation for the reported random disconnections is D. The interface is reporting a high number of errors and dropped packets.

NEW QUESTION 30
An administrator needs to remove the directory /home/user1/data and all of its contents. Which of the following commands should the administrator use?

A. rmdir -p /home/user1/data
B. ln -d /home/user1/data
C. rm -r /home/user1/data
D. cut -d /home/user1/data

Answer: C

Explanation:
File and directory management is a core system administration skill addressed in Linux+ V8. When an administrator needs to delete a directory that contains files or subdirectories, a recursive deletion is required.
The correct command is rm -r /home/user1/data. The rm command removes files, and the -r (recursive) option allows it to delete directories and all of their contents, including nested files and subdirectories. This is the standard and correct method for removing non-empty directories.
The other options are incorrect. rmdir -p only removes empty directories and will fail if the directory contains files. ln -d is used to create directory hard links, not remove directories. cut -d is a text-processing command unrelated to filesystem operations.
Linux+ V8 documentation stresses caution when using rm -r, as it permanently deletes data without recovery unless backups exist. Therefore, the correct answer is C.

NEW QUESTION 32
A systems administrator is writing a script to analyze the number of files in the directory /opt/application
/home/. Which of the following commands should the administrator use in conjunction with ls -l | to count the files?

A. less
B. tail -f
C. tr -c
D. wc -l

Answer: D

Explanation:
Explanation
Comprehensive and Detailed Explanation From Exact Extract:
wc -l counts the number of lines of input provided to it, which is commonly used to count the number of files when used with ls -l (excluding the header line). For example, ls -l /opt/application/home/ | wc -l gives the total count of lines, which corresponds to the number of files and directories (including the total line at the top).
Other options:
* A. less is a pager utility.
* B. tail -f shows the end of a file in real time.
* C. tr -c translates or deletes characters, not for counting lines.
Reference:
CompTIA Linux+ Study Guide: Exam XK0-006, Sybex, Chapter 4: "Working with the Command Line", Section: "Text Processing Commands"
CompTIA Linux+ XK0-006 Objectives, Domain 1.0: System Management

NEW QUESTION 33
A Linux user needs to download the latest Debian image from a Docker repository. Which of the following commands makes this task possible?

A. docker image init debian
B. docker image pull debian
C. docker image import debian
D. docker image save debian

Answer: B

Explanation:
Container management and image handling are part of modern Linux automation practices covered in CompTIA Linux+ V8. Docker images are stored in container registries such as Docker Hub, and administrators commonly need to download images to deploy containers.

The correct command for downloading an image from a Docker repository is docker image pull. This command retrieves the specified image from a configured container registry and stores it locally. When no tag is specified, Docker automatically pulls the latest available version of the image. Therefore, docker image pull debian downloads the most recent Debian image from Docker Hub.
The other options are incorrect. docker image init is not a valid Docker command and does not exist in Docker??s CLI. docker image import is used to create a Docker image from a tarball file, not to download an image from a repository. docker image save exports an existing local image into a tar archive and does not retrieve images from a remote registry.
Linux+ V8 documentation emphasizes understanding container image lifecycles, including pulling, tagging, and running images. Pulling images is a foundational step before container execution and automation workflows.
Therefore, the correct answer is B. docker image pull debian.

NEW QUESTION 37
A DevOps engineer made some changes to files in a local repository. The engineer realizes that the changes broke the application and the changes need to be reverted back. Which of the following commands is the best way to accomplish this task?

A. git pull
B. git reset
C. git rebase
D. git stash

Answer: B

Explanation:
Version control rollback operations are a core DevOps skill covered in the Linux+ V8 objectives. When changes in a local Git repository break an application and must be reverted, the administrator must choose a command that directly undoes those changes.
The command git reset is the most appropriate option in this scenario. It allows the engineer to move the current branch pointer (HEAD) to a previous commit, effectively discarding or undoing local changes. Depending on the reset mode (--soft, --mixed, or --hard), the engineer can control whether changes are preserved in the staging area or working directory. This flexibility makes git reset the primary tool for reverting problematic local changes.
The other options are not suitable. git pull fetches and merges changes from a remote repository and does not revert local modifications. git rebase rewrites commit history and is used to reapply commits on top of another base, not to undo broken changes. git stash temporarily saves uncommitted changes for later use but does not revert the repository to a stable state.
Linux+ V8 documentation emphasizes that git reset is commonly used during local development when changes need to be undone quickly before being shared with others. Therefore, the correct answer is B.

NEW QUESTION 39
A Linux user frequently tests shell scripts located in the /home/user/scripts directory. Which of the following commands allows the user to run the program by invoking only the script name?

A. export SHELL=$SHELL=/home/user/scripts
B. export TERM=$TERM=/home/user/scripts
C. export PATH=$PATH:/home/user/scripts
D. export alias /home/user/scripts='/bin'

Answer: C

Explanation:
In Linux, the ability to execute a program by typing only its name depends on whether the directory containing the executable is included in the user??s PATH environment variable. The PATH variable defines a colon-separated list of directories that the shell searches when a command is entered.
Option C, export PATH=$PATH:/home/user/scripts, correctly appends the /home/user/scripts directory to the existing PATH variable. Once this command is executed, any executable script located in that directory can be run simply by typing its filename, provided the script has execute permissions. This behavior is explicitly covered in the Linux+ V8 objectives related to environment variables and shell configuration.
The other options are incorrect. Option A incorrectly attempts to redefine the SHELL variable and uses invalid syntax. Option B modifies the TERM variable, which controls terminal type and has nothing to do with command execution. Option D attempts to create an alias using invalid syntax and would not affect command lookup behavior.
Linux+ V8 documentation emphasizes modifying the PATH variable as the standard and recommended method for simplifying script execution. This approach is commonly used by developers and administrators who frequently run custom scripts.
Therefore, the correct answer is C.

NEW QUESTION 44
Users report that a Linux system is unresponsive and simple commands take too long to complete. The Linux administrator logs in to the system and sees the following:
Output 1:
10:06:29 up 235 day, 19:23, 2 users, load average: 8.71, 8.24, 7.71
Output 2:

Linux 6.8.0-31-generic (host) 05/10/2024 _x86_64_ (4 CPU)

10:07:42	AM	CPU	%usr	%nice	%sys	%iowait	%irq	%soft	%steal	%guest	%gnice	%idle
10:07:42	AM	all	65.88	0	20.54	5.65	0	7.93	0	0	0	0

Which of the following is the system experiencing?

A. High latency
B. High uptime
C. High CPU load
D. High I/O wait times

Answer: C

Explanation:

This scenario is a classic performance troubleshooting case covered under the Troubleshooting domain of the CompTIA Linux+ V8 objectives. The key indicators to analyze are the load average values and the CPU utilization statistics.
The uptime command shows load averages of 8.71, 8.24, and 7.71 over the 1-, 5-, and 15-minute intervals. Load average represents the average number of processes that are either running on the CPU or waiting to run. On a system with 4 CPU cores, a healthy load average would typically be close to or below 4. Load averages consistently near or above 8 indicate that there are significantly more runnable processes than available CPU resources, causing processes to wait and resulting in poor system responsiveness.
The CPU output further confirms this condition. The %idle value is 0, meaning the CPU has no idle time available. The majority of CPU time is spent in user space (65.88%) and system/kernel space (20.54%), indicating heavy computational and kernel activity. While %iowait is present at 5.65%, it is not high enough to suggest that disk I/O is the primary bottleneck.
Option C, high CPU load, best explains the symptoms. High CPU load causes commands to execute slowly because processes are competing for limited CPU time. This directly matches the observed behavior of the system being unresponsive.
The other options are incorrect. High uptime simply indicates how long the system has been running and does not cause performance issues by itself. High latency is a general term and not a specific diagnosis shown by the metrics provided. High I/O wait times would require a significantly higher %iowait value.
According to Linux+ V8 documentation, correlating load averages with CPU core count and utilization is essential for accurate performance diagnosis. Therefore, the correct answer is C. High CPU load.

NEW QUESTION 49
A Linux administrator attempts to log in to a server over SSH as root and receives the following error message: Permission denied, please try again. The administrator is able to log in to the console of the server directly with root and confirms the password is correct. The administrator reviews the configuration of the SSH service and gets the following output:

```
Port 22
PermitRootLogin prohibit-password
PasswordAuthentication yes
PermitEmptyPassword no
Use PAM no
MaxSessions 1
MaxAuthTries 3
```

Based on the above output, which of the following will most likely allow the administrator to log in over SSH to the server?

A. Log out other user sessions because only one is allowed at a time.
B. Enable PAM and configure the SSH module.
C. Modify the SSH port to use 2222.
D. Use a key to log in as root over SSH.

Answer: D

Explanation:
The SSH configuration option PermitRootLogin prohibit-password prevents the root user from logging in with password authentication. This setting means root cannot use a password to log in via SSH; only key- based authentication is permitted for root. The administrator can still log in as root locally, which is not affected by this SSH configuration. To allow SSH access as root, the administrator must use an SSH key instead of a password.
Other options:
* A. MaxSessions controls the number of simultaneous SSH sessions but is not causing the login denial here.
* B. PAM (Pluggable Authentication Modules) is disabled, but enabling it is not required for basic SSH authentication.
* C. Changing the SSH port is unrelated to the authentication method issue.
Reference:
CompTIA Linux+ Study Guide: Exam XK0-006, Sybex, Chapter 11: "Securing Linux", Section: "Securing SSH Access"
CompTIA Linux+ XK0-006 Objectives, Domain 3.0: Security

NEW QUESTION 54
Which of the following describes PEP 8?

A. The style guide for Python code
B. Python virtual environments
C. A package installer for Python
D. A Python variable holding octal values

Answer: A

Explanation:
Python scripting is part of Linux automation, and Linux+ V8 includes knowledge of Python development standards. PEP 8 stands for Python Enhancement Proposal 8 and defines the official style guide for Python code.
PEP 8 provides conventions for code layout, indentation, naming, line length, whitespace usage, and commenting. Its purpose is to improve code readability and maintainability, especially in collaborative environments. Linux+ V8 emphasizes that standardized coding practices are critical in automation and DevOps workflows.
The other options are incorrect. Python virtual environments are managed using tools such as venv. Package installation is handled by pip. Octal values are represented using specific syntax and are unrelated to PEP 8.
Therefore, the correct answer is A.

NEW QUESTION 59
Which of the following passwords is the most complex?

A. H3sa1dt01d
B. he$@ID$heTold
C. H3s@1dSh3t0|d
D. HeSaidShetold

Answer: C

Explanation:
Comprehensive and Detailed 250 to 350 words of Explanation From Linux+ V8 documents:
Password complexity is a fundamental concept within theSecuritydomain of CompTIA Linux+ V8. Complex passwords significantly reduce the risk of successful brute-force, dictionary, and credential-stuffing attacks. Linux+ emphasizes evaluating passwords based onlength, character variety, unpredictability, and resistance to common word patterns.
OptionC, H3s@1dSh3t0|d, is the most complex password among the choices. It demonstrates strong security characteristics by incorporating:
Uppercase letters (H, S)
Lowercase letters (s, d, t)
Numbers (3, 1, 0)
Multiple special characters (@, |)
A longer overall length compared to some other options
Additionally, optionCusescharacter substitution (leet-style)in a way that breaks up recognizable words more effectively than the other choices. This significantly increases entropy and makes the password harder to guess using rule-based or hybrid cracking techniques.
OptionAincludes uppercase letters and numbers but lacks special characters and is relatively short. OptionBincludes special characters and mixed case, but it still closely resembles readable words, making it more susceptible to dictionary-based attacks. OptionDuses only alphabetic characters and clear word patterns, making it the weakest choice.
Linux+ V8 documentation highlights that thestrongest passwords combine length with diverse character classes and minimal predictability. PasswordCbest meets all of these criteria and would score highest against common password-cracking strategies.
Therefore, the correct answer isC. H3s@1dSh3t0|d.

NEW QUESTION 64
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,/procis the filesystem that contains non-persistent, volatile data.
The /proc filesystem is avirtual filesystemthat 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 isC. /proc.

NEW QUESTION 66
Following the completion of monthly server patching, a Linux administrator receives reports that a critical application is not functioning. Which of the following commands should help the administrator determine which packages were installed?

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.
Thednf historycommand 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.
OptionAis 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 isA.

NEW QUESTION 71
A systems administrator needs to check the statuses of all the services on a Linux server. Which of the following commands accomplishes this task?

A. systemctl is-active --services

B. systemctl list-sockets --type=services
C. systemctl is-enabled --services
D. systemctl list-units --type=services

Answer: D

Explanation:
Service management usingsystemdis a core Linux+ V8 system management objective. Administrators frequently need to view the current status of all services to determine which ones are running, stopped, failed, or inactive.
The correct command issystemctl list-units --type=services, which displays all loaded service units along with their current state, including whether they are active, inactive, failed, or running. This provides a comprehensive, real-time view of service statuses on the system and is commonly used during troubleshooting and audits.
OptionA, systemctl is-active, is designed to check the status of a single service, not all services. OptionBlists socket units, not services. OptionC, systemctl is-enabled, checks whether services are enabled at boot, not whether they are currently running.
Linux+ V8 documentation explicitly references systemctl list-units --type=service as the primary command for viewing service runtime states. Therefore, the correct answer isD.

NEW QUESTION 75
An administrator logs in to a Linux server and notices the clock is 37 minutes fast. Which of the following commands will fix the issue?

A. hwclock
B. ntpdate
C. timedatectl
D. ntpd -q

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The ntpdate command synchronizes the system clock with a remote NTP server immediately, correcting any significant time drift. This is ideal for one-time corrections.
For example:
bash
CopyEdit
ntpdate pool.ntp.org
Other options:
* A.hwclock reads or sets the hardware clock, but does not sync with network time.
* C.timedatectl can set the time manually or manage time settings, but does not immediately sync with a remote NTP server.
* D.ntpd -q can also sync the clock once, but ntpdate is designed specifically for immediate synchronization and is more straightforward for one-time corrections.
[Reference:, CompTIA Linux+ Study Guide: Exam XK0-006, Sybex, Chapter 5: "System Management", Section: "Time Synchronization", CompTIA Linux+ XK0-006 Objectives, Domain 1.0: System Management, ==========]

NEW QUESTION 79
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

Answer: C

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.

NEW QUESTION 81
A Linux software developer wants to use AI to optimize source code used in a commercial product. Which of the following steps should the developer take first?

A. Research which available AI chatbots are best at optimizing source code.
B. Verify that the company has a policy governing the use of AI in software development.
C. Install a private LLM to use on the internal network for source code optimization.
D. Use open-source LLMs that undergo regular security reviews by the community.

Answer: B

Explanation:
Linux+ V8 emphasizessecurity, compliance, and governancewhen introducing new automation technologies, including AI. Before using AI tools to optimize commercial source code, the developer must ensure that such usage complies with organizational policies.
OptionBis correct because verifying company policy is the first and most critical step. AI tools may introduce risks such as intellectual property leakage, licensing conflicts, or regulatory violations. Many organizations restrict how source code can be shared with external systems, including AI services.
The other options are premature. Selecting tools or deploying models should only occur after policy approval. Linux+ V8 highlights governance-first approaches when adopting automation technologies.
Therefore, the correct answer isB.

NEW QUESTION 85
A systems administrator receives reports from users who are having issues while trying to modify newly created files in a shared directory. The administrator sees the following outputs:

```
[student3@hostname share]$ ls -ld /share
drwxrwxr-x. 5 userdata users 56 Jul 9 16:31 /share
[student3@hostname share]$ ls -l
total 4
drwxrwxr-x. 2 student users 6 Jul 9 16:28 originaldata
drwxrwxr-x. 2 student users 6 Jul 9 16:28 originalfile
-rw-rw-r--. 1 student2 student2 0 Jul 9 16:31 newfile2
drwxrwxr-x. 2 student2 student2 6 Jul 9 16:31 mynewdir
-rw-rw-r--. 1 student3 student3 0 Jul 9 16:33 newfile

[student3@hostname share]$ echo "content" >> newfile2
bash: newfile2: Permission denied

[student3@hostname share]$ touch mynewdir/file
touch: cannot touch 'mynewdir/file': Permission denied
```

Which of the following provides the best resolution to this issue?

A. Adding a setuid bit to the user in the shared folder
B. Manually changing the group of the newly created files
C. Changing all directory contents to be writable and readable for everyone
D. Adding a setgid bit to the group in the shared folder

Answer: D

Explanation:
This scenario involvesshared directory collaboration, which is a common system management task covered in the CompTIA Linux+ V8 objectives. The key issue is that users can create files in the shared directory, but other users in the same group cannot modify those files. This behavior is directly related togroup ownership inheritance.
By default, when a user creates a file or directory, it is owned by the user and assigned the user??sprimary group, not necessarily the group of the parent directory. As shown in the output, files inside /share are owned by different groups (student, student2, student3), which prevents other group members from modifying them, even though the parent directory is group-writable.
The correct solution is toset the setgid (set group ID) bit on the shared directory, making optionDcorrect. When the setgid bit is applied to a directory, all newly created files and subdirectories inherit thegroup ownership of the parent directory, rather than the creator??s primary group. This ensures consistent group ownership and allows all members of the shared group to collaborate effectively.
The other options are incorrect or poor practice. OptionA(setuid) is intended for executables, not directories. OptionBrequires constant manual intervention and does not scale. OptionCweakens security by granting write access to all users, violating the principle of least privilege.
Linux+ V8 documentation explicitly recommends using thesetgid bit on shared directoriesto manage collaborative access securely and efficiently.

NEW QUESTION 89
A systems administrator is having issues with a third-party API endpoint. The administrator receives the following output:

```
# curl https://comptia.com/endpoint
curl: (6) Could not resolve host: comptia.com


# dig comptia.com
; <<>> <<>> comptia.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 14031
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;comptia.com. IN A
;; AUTHORITY SECTION:
com. 900 IN SOA a.gtld-servers.net. nstld.verisign-grs.com. 1720473015 1800 900 604800 86400
;; Query time: 159 msec
;; SERVER: 10.255.255.254#53(10.255.255.254) (UDP)
;; WHEN: Mon Jul 08 15:10:45 CST 2024
;; MSG SIZE rcvd: 117
```

Which of the following actions should the administrator take to resolve the issue?

A. Open a secure port in the server's firewall.
B. Request a new API endpoint from a third party.
C. Review and fix the DNS client configuration file.
D. Enable internet connectivity on the host.

Answer: C

NEW QUESTION 92
Which of the following best describes journald?

A. A system service that collects and stores logging data
B. A feature that creates crash dumps in case of kernel failure
C. A service responsible for keeping the filesystem journal
D. A service responsible for writing audit records to a disk

Answer: A

NEW QUESTION 96
A systems administrator is configuring new Linux systems and needs to enable passwordless authentication between two of the servers. Which of the following commands should the administrator use?

A. ssh-keygen -t rsa && ssh-copy-id -i ~/.ssh/id_rsa.pub john@server2
B. ssh-keyscan -t rsa && ssh-copy-id john@server2 -i ~/.ssh/key
C. ssh-agent -i rsa && ssh-copy-id ~/.ssh/key john@server2
D. ssh-add -t rsa && scp -rp ~/.ssh john@server2

Answer: A

NEW QUESTION 101
An administrator set up a new user account called "test". However, the user is unable to change their password. Given the following output:

```
[test@localhost ~]$ passwd
Changing password for user test.
Current password:
passwd: Authentication token manipulation error

[test@localhost ~]$ ls -l /bin/passwd
-rwxr-xr-x. 1 root root 33424 Feb 7 2022 /bin/passwd

[test@localhost ~]$ chage -l test
Last password change : Oct 19, 2023
Password expires : never
Password inactive : never
Account expires : never
Minimum number of days between password change : 0
Maximum number of days between password change : 99999
Number of days of warning before password expires : 7

[root@localhost bin]# passwd test
Changing password for user test.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

Which of the following is the most likely cause of this issue?

A. The SUID bit is missing on the /bin/passwd file.
B. The password provided by the user "test" does not meet complexity requirements.
C. The user "test" already changed the password today.
D. The password has been disabled for user "test".

Answer: A

Explanation:
For normal users to change their own password, /bin/passwd must have the SUID bit set (permissions should be -rwsr-xr-x). The SUID bit allows users to run the program with the permissions of the file owner (root), which is required to update /etc/shadow. The provided output shows /bin/passwd does not have the SUID bit (no 's' in the owner's execute field). As a result, user "test" receives an "Authentication token manipulation error". The password can be changed as root, which confirms it's a permissions/SUID issue.
Other options:
* B. If the password didn??t meet requirements, a different error would appear.
* C. There is no minimum day limit preventing password change (see chage -l output).
* D. The account and password are active (not disabled).
Reference:
CompTIA Linux+ Study Guide: Exam XK0-006, Sybex, Chapter 6: "User and Group Management", Section: "Managing User Passwords and Policies"
CompTIA Linux+ XK0-006 Objectives, Domain 1.0: System Management

NEW QUESTION 103
.....

Relate Links

100% Pass Your XK0-006 Exam with Exambible Prep Materials

https://www.exambible.com/XK0-006-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/