CompTIA

Exam Questions XK0-006

CompTIA Linux+ Exam

NEW QUESTION 1
Which of the following is a protocol for accessing distributed directory services containing a hierarchy of users, groups, machines, and organizational units?

A. SMB
B. TLS
C. LDAP
D. KRB-5

Answer: C

Explanation:
Directory services are a key part of enterprise Linux environments and are covered under the Security domain in Linux+ V8. The Lightweight Directory Access Protocol (LDAP) is specifically designed to access and manage distributed directory information.
LDAP directories store structured, hierarchical data such as users, groups, computers, and organizational units. Linux systems commonly use LDAP for centralized authentication, authorization, and identity management. LDAP is also the foundation for services like Active Directory and FreeIPA.
The other options are incorrect. SMB is a file and printer sharing protocol. TLS is an encryption protocol used to secure communications. Kerberos (KRB-5) is an authentication protocol often used alongside LDAP but does not store directory information itself.
Linux+ V8 documentation highlights LDAP as the primary protocol for directory-based identity services. Therefore, the correct answer is C.

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 creating a backup copy of the /home/ directory. Which of the following commands allows the administrator to archive and compress the directory at the same time?

A. cpio -o /backups/home.tar.xz /home/
B. rsync -z /backups/home.tar.xz /home/
C. tar -cJf /backups/home.tar.xz /home/
D. dd of=/backups/home.tar.xz if=/home/

Answer: C

Explanation:
Creating backups is a core responsibility in Linux system management, and the Linux+ V8 objectives emphasize proper use of archiving and compression tools. The tar utility is the standard Linux tool for creating archive files, and it also supports compression through various options.
The command tar -cJf /backups/home.tar.xz /home/ correctly combines both archiving and compression in a single step. The -c option creates a new archive, -J

specifies XZ compression, and -f allows the administrator to define the output file name. This results in a compressed archive of the entire /home/ directory, which is efficient for storage and transfer.
The other options are incorrect. cpio is an archiving tool but does not perform compression by itself without additional commands or pipelines. rsync -z compresses data during transfer but does not create an archive file. The dd command performs low-level copying of raw data and is not suitable for directory-based backups.
Linux+ V8 documentation highlights tar as the preferred utility for filesystem backups due to its flexibility, reliability, and support for multiple compression algorithms. Therefore, the correct answer is C.

NEW QUESTION 5
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 6
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 7
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 8
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 9
Which of the following is a characteristic of Python 3?

A. It is closed source.
B. It is extensible through modules.
C. It is fully backwards compatible.
D. It is binary compatible with Java.

Answer: B

Explanation:
Python 3 characteristics are part of Linux+ V8 scripting objectives. One of Python??s most important features is itsmodular and extensible architecture. OptionBis correct because Python 3 supports extensibility through modules and packages. Python includes a large standard library and allows developers to extend functionality using third-party modules or custom code. This makes Python highly adaptable for automation, system management, and DevOps tasks.
The other options are incorrect. Python is open source, not closed source. Python 3 is not fully backwards compatible with Python 2, which is a major distinction emphasized in Linux+ V8. Python is also not binary compatible with Java.
Linux+ V8 documentation highlights Python's extensibility as a key reason it is widely used in Linux automation. Therefore, the correct answer isB.

NEW QUESTION 10
A Linux systems administrator is running an important maintenance task that consumes a large amount of CPU, causing other applications to slow. Which of the

following actions should the administrator take to help alleviate the issue?

A. Increase the available CPU time with pidstat.
B. Lower the priority of the maintenance task with renice.
C. Run the maintenance task with nohup.
D. Execute the other applications with the bg utility.

Answer: B

Explanation:
Process scheduling and resource management are essential Linux administration skills covered in Linux+ V8. When a process consumes excessive CPU resources, it can negatively impact overall system performance.
The correct solution is tolower the priorityof the CPU-intensive task using the renice command. Niceness values influence how much CPU time a process receives relative to others. Increasing the niceness value reduces the process??s priority, allowing other applications to receive CPU resources more fairly.
OptionBdirectly addresses the issue. The other options do not. pidstat monitors processes but does not modify CPU allocation. nohup allows a process to continue running after logout but does not affect scheduling priority. bg resumes a stopped job in the background but does not reduce CPU usage.
Linux+ V8 documentation explicitly references nice and renice for managing CPU contention. Therefore, the correct answer isB.

NEW QUESTION 10
A systems administrator wants to review the amount of time the NetworkManager service took to start. Which of the following commands accomplishes this goal?

A. resolvectl
B. journalctl
C. systemctl daemon-reload
D. systemd-analyze blame

Answer: D

Explanation:
System boot performance analysis is an important system management task included in Linux+ V8. When administrators need to determine how long services take to start during boot,systemd analysis toolsare required.
The correct command issystemd-analyze blame. This command lists all systemd services and shows how long each one took to initialize during the boot process. It is commonly used to identify slow-starting services that may impact system startup performance, including NetworkManager.
The other options are incorrect. resolvectl is used for DNS resolution management and provides no service timing information. journalctl can display logs but does not provide a clear, summarized service startup timing report. systemctl daemon-reload only reloads systemd unit files and does not perform analysis.
Linux+ V8 documentation explicitly references systemd-analyze blame as the correct tool for diagnosing service startup delays. Therefore, the correct answer isD.

NEW QUESTION 12
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 15
A Linux administrator tries to install Ansible in a Linux environment. One of the steps is to change the owner and the group of the directory /opt/Ansible and its contents. Which of the following commands will accomplish this task?

A. groupmod -g Ansible -n /opt/Ansible
B. chown -R Ansible:Ansible /opt/Ansible
C. usermod -aG Ansible /opt/Ansible
D. chmod -c /opt/Ansible

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The chown command is used to change the owner and group of files and directories. The -R (recursive) flag ensures that all contents within the directory are also updated. The correct syntax is chown -R owner:group directory. So, chown -R Ansible:Ansible /opt/Ansible will change the owner and group for /opt/Ansible and

everything inside it to "Ansible".
Other options:
* A.groupmod is used to modify group properties, not ownership of directories or files.
* C.usermod is for modifying user properties or group memberships.
* D.chmod changes permissions, not owner/group.
[Reference:, CompTIA Linux+ Study Guide: Exam XK0-006, Sybex, Chapter 6: "User and Group Management", Section: "Managing File Ownership and Permissions", CompTIA Linux+ XK0-006 Objectives, Domain 1.0: System Management,]

NEW QUESTION 16
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 20
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 24
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 26
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 30
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 31
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 32
Which of the following describes how a user's public key is used during SSH authentication?

A. The user's public key is used to hash the password during SSH authentication.
B. The user's public key is verified against a list of authorized key
C. If it is found, the user is allowed to log in.
D. The user's public key is used instead of a password to allow server access.
E. The user's public key is used to encrypt the communication between the client and the server.

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
During SSH public key authentication, the server checks if the user's public key is present in the ~/.ssh
/authorized_keys file. If the key is found, the server uses it to verify the user's identity by sending a challenge that can only be answered by the corresponding private key. This process does not involve password hashing or using the public key directly for encryption of the communication stream. Instead, the public key is simply used as a reference for authentication.
Reference:
CompTIA Linux+ Study Guide: Exam XK0-006, Sybex, Chapter 11: "Securing Linux", Section: "SSH Key- Based Authentication"
CompTIA Linux+ XK0-006 Objectives, Domain 3.0: Security
==========

NEW QUESTION 34
A Linux administrator just finished setting up passwordless SSH authentication between two nodes. However, upon test validation, the remote host prompts for a password. Given the following logs:

```
-rw-------. 1 root root 588 Apr 3 2022 authorized_keys

avc: denied { read } for pid=xxxx comm="sshd" name="authorized_keys" dev="dm-5" ino=xxxx scontext=system_u:system_r:sshd_t:s0-s0:c0.c1
tcontext=unconfined_u:object_r:home_root_t:s0 tclass=file
[...]

SELinux status: enabled
SELinuxfs mount: /sys/fs/selinux
SELinux root directory: /etc/selinux
Loaded policy name: targeted
Current mode: enforcing
Mode from config file: enforcing
Policy MLS status: enabled
Policy deny_unknown status: allowed
Max kernel policy version: 31
```

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

A. The SELinux policy is incorrectly targeting the unconf ined_u context.
B. The administrator forgot to restart the SSHD after creating the authorizedjceys file.
C. The authorized_keys file has the incorrect root permissions assigned.
D. The authorized_keys file does not have the correct security context to match SELinux policy.

Answer: D

Explanation:
This issue is directly related to SELinux enforcement, which is a key topic in the Security domain of CompTIA Linux+ V8. The logs clearly indicate that SSH key-based authentication is failing due to an SELinux access control violation rather than a traditional file permission or SSH configuration problem.
The most important clue is the AVC denial message, which shows that the sshd process is being denied read access to the authorized_keys file. The security context of the file is listed as unconfined_u:object_r: home_root_t:s0. Under a targeted SELinux policy, SSH is only permitted to read authorized_keys files that are labeled with the correct SELinux type, typically ssh_home_t.
Because SELinux is running in enforcing mode, it actively blocks access that violates policy rules, even if standard UNIX permissions are correct. Although the file permissions (600) are acceptable for an authorized_keys file, SELinux does not rely solely on traditional permissions. The mismatch between the expected SELinux context and the actual context prevents sshd from accessing the file, causing SSH to fall back to password authentication.
Option D correctly identifies the root cause: the authorized_keys file does not have the correct SELinux security context. This is a well-documented Linux+ V8 troubleshooting scenario, commonly resolved by restoring the correct context using commands such as restorecon or by ensuring the file resides in a properly labeled home directory.
The other options are incorrect. Restarting sshd does not fix SELinux labeling issues. The policy itself is functioning as intended, and file ownership alone does not override SELinux access controls.
Linux+ V8 documentation emphasizes that SELinux denials must be addressed by correcting file contexts rather than weakening security controls. Therefore, the correct answer is D.

NEW QUESTION 36
Users cannot access a server after it has been restarted. At the server console, the administrator runs the following commands;

```
$ ss -lnt
State      Recv-Send-Q     LocalAddress:PortPeerAddress:PortProcess
LISTEN     0    32       0.0.0.0:53    0.0.0.0:*
LISTEN     0    128      0.0.0.0:22    0.0.0.0:*
LISTEN     0    1024     0.0.0.0:443   0.0.0.0:*
LISTEN     0    4096     0.0.0.0:5355  0.0.0.0:*
LISTEN     0    5127.0.0.1:4711   0.0.0.0:*

$ sudo firewall-cmd --list-all
FedoraServer (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp3s0
  sources:
  services: cockpit dhcp dhcpv6-client dns dns-over-tls https
  [...]

$ uptime
14:52:35 up 1 day, 3:08, 1 user, load average: 0.05, 0.07, 0.07

$ ping server1 -c 5
PING server1 (192.168.0.2) 56(84) bytes of data.
64 bytes from server1 (192.168.0.2): icmp_seq=1 ttl=64 time=0.436 ms
64 bytes from server1 (192.168.0.2): icmp_seq=2 ttl=64 time=0.644 ms
...
```

Which of the following is the cause of the issue?

A. The DNS entry does not have a valid IP address.
B. The SSH service has not been allowed on the firewall.
C. The server load average is too high.
D. The wrong protocol is being used to connect to the web server.

Answer: B

Explanation:
This issue is a classic example of post-reboot connectivity troubleshooting, which falls under the Troubleshooting domain of CompTIA Linux+ V8. The administrator has correctly gathered evidence using multiple diagnostic tools, allowing the root cause to be identified through correlation.
The ss -lnt output confirms that the SSH daemon is running and listening on TCP port 22. This eliminates the possibility that the SSH service failed to start after reboot. Additionally, the uptime output shows a very
low load average, indicating that system performance is not a limiting factor. The successful ping test confirms that the server is reachable at the network layer and that DNS resolution and basic connectivity are functioning correctly.
The critical clue comes from the firewall configuration. The output of firewall-cmd --list-all shows that only specific services are allowed through the firewall, such as https, dns, and cockpit. The SSH service is notably absent. On systems using firewalld, services must be explicitly allowed, even if the daemon itself is running and listening on the correct port.
As a result, incoming SSH connection attempts are being blocked by the firewall, preventing users from accessing the server remotely after reboot. This aligns precisely with option B.
The other options are incorrect. DNS is functioning, as shown by successful ping responses. System load is low and not contributing to the issue. There is no indication that users are attempting to access the web server using an incorrect protocol.
Linux+ V8 documentation emphasizes that administrators must verify both service status and firewall rules when diagnosing access issues. In this case, allowing SSH with a command such as firewall-cmd --add- service=ssh --permanent followed by a reload would resolve the problem.

NEW QUESTION 41
An administrator attempts to install updates on a Linux system but receives error messages regarding a specific repository. Which of the following commands should the administrator use to verify that the repository is installed and enabled?

A. yum repo-pkgs
B. yum list installed repos
C. yum reposync available
D. yum repolist all

Answer: D

Explanation:

Package management troubleshooting is an important skill in Linux+ V8, especially on RPM-based distributions that use yum or dnf. When update errors reference a repository, the administrator must verify whether the repository exists and whether it is enabled.
The command yum repolist all displays all configured repositories, including those that are enabled, disabled, or temporarily unavailable. This makes it the most effective command for diagnosing repository-related issues. It allows administrators to quickly confirm the repository??s status and take corrective action, such as enabling it or fixing configuration errors.
The other options are incorrect. yum repo-pkgs manages packages within a repository but does not list repository status. yum list installed repos is not a valid yum command. yum reposync is used to mirror repositories locally and is not intended for verification.
Linux+ V8 documentation highlights yum repolist all as the standard command for repository inspection and troubleshooting.
Therefore, the correct answer is D. yum repolist all.

NEW QUESTION 44
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 45
A Linux administrator is testing a web application on a laboratory service and needs to temporarily allow DNS and HTTP/HTTPS traffic from the internal network. Which of the following commands will accomplish this task?

A. firewalld -- add-service=dns, http,https -- zone=internal
B. iptables -- enable-service='dns|http|https' -- zone=internal
C. firewall-cmd --add-service={dns, http, https} --zone=internal
D. systemctl mask firewalld --for={dns, http, https} --zone=internal

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The correct way to temporarily allow specific services in a particular zone with firewalld is to use firewall- cmd --add-service=service --zone=zone. Multiple services can be specified in curly braces and separated by commas. The correct syntax is:
bash CopyEdit
firewall-cmd --add-service={dns,http,https} --zone=internal
This command will allow DNS (port 53), HTTP (port 80), and HTTPS (port 443) through the firewall for the "internal" zone temporarily (for the current runtime session).
Other options:
* A. The command syntax is incorrect; firewalld is a service, not a command-line tool.
* B. iptables does not use the --enable-service flag, nor does it have zones in this way.
* D. systemctl mask disables services, and the rest of the command is invalid.
Reference:
CompTIA Linux+ Study Guide: Exam XK0-006, Sybex, Chapter 9: "Networking", Section: "Managing Firewalls with firewalld"
CompTIA Linux+ XK0-006 Objectives, Domain 2.0: Networking
==========

NEW QUESTION 46
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?

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.

NEW QUESTION 50
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 52
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 53
A Linux administrator wants to add a user to the Docker group without changing the user??s primary group. Which of the following commands should the administrator use to complete this task?

A. sudo groupmod docker user

B. sudo usermod -g docker user
C. sudo usermod -aG docker user
D. sudo groupmod -G docker user

Answer: C

Explanation:
User and group management is a core System Management topic in CompTIA Linux+ V8. When adding a user to an additional group—such as the docker group—care must be taken not to alter the user's primary group.
The correct command issudo usermod -aG docker user. The -G option specifies a supplementary group, and the -a (append) option ensures the user is added to the groupwithout removing existing group memberships. This is especially important because omitting -a would overwrite the user's supplementary groups.
OptionB, usermod -g docker user, changes the user'sprimary group, which is not desired. OptionsAandDmisuse groupmod, which is intended for modifying group properties, not user membership.
Linux+ V8 documentation explicitly warns that failing to use -a with -G can unintentionally remove a user from all other supplementary groups, potentially causing access issues.
Therefore, the correct and safe command isC. sudo usermod -aG docker user.

NEW QUESTION 57
Which of the following can reduce the attack surface area in relation to Linux hardening?

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 bannerserves as a legal notification and does not affect system vulnerabilities.
* B. Reducing the number of directories createdis not related to hardening or access control.
* C. Extending the SSH startup timeout periodmay give attackers more time to attempt a connection and does not increase security.
[Reference:, 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, , ,]

NEW QUESTION 59
Which of the following commands should an administrator use to convert a KVM disk file to a different format?

A. qemu-kvm
B. qemu-ng
C. qemu-io
D. qemu-img

Answer: D

Explanation:
Virtualization management is part of Linux system administration and is included in Linux+ V8 objectives. KVM virtual machines commonly use disk image formats such as qcow2, raw, or vmdk. Converting between these formats is a routine administrative task.
The correct tool for disk image conversion isqemu-img. This utility allows administrators to create, convert, resize, and inspect virtual disk images. For example, converting a qcow2 image to raw format can be accomplished using qemu-img convert. This capability is explicitly referenced in Linux+ V8 documentation related to virtualization tooling.
The other options are incorrect. qemu-kvm refers to the hypervisor component, not disk manipulation. qemu-ng is not a valid QEMU utility. qemu-io is used for low-level I/O testing and debugging, not image format conversion.
Therefore, the correct answer isD. qemu-img.

NEW QUESTION 64
A systems administrator needs to set the IP address of a new DNS server. Which of the following files should the administrator modify to complete this task?

A. /etc/whois.conf
B. /etc/resolv.conf
C. /etc/nsswitch.conf
D. /etc/dnsmasq.conf

Answer: B

Explanation:
DNS client configuration is a foundational Linux networking task covered in Linux+ V8 system management objectives. When an administrator needs to specify the IP address of a DNS server that the system should use for name resolution, the correct file to modify is/etc/resolv.conf.
The /etc/resolv.conf file defines DNS resolver settings, including one or more nameserver entries that specify the IP addresses of DNS servers. Applications and system services rely on this file to resolve hostnames to IP addresses.
The other options are incorrect. /etc/whois.conf configures WHOIS queries. /etc/nsswitch.conf controls the order of name resolution sources but does not define DNS server IP addresses. /etc/dnsmasq.conf configures a local DNS caching service, not the system-wide resolver directly.
Linux+ V8 documentation highlights /etc/resolv.conf as the authoritative DNS client configuration file, though it may be dynamically managed by tools such as NetworkManager or systemd-resolved.
Therefore, the correct answer isB. /etc/resolv.conf.

NEW QUESTION 68
To perform a live migration, which of the following must match on both host servers?(Choose two)

A. USB ports
B. Network speed
C. Available swap
D. CPU architecture
E. Available memory
F. Disk storage path

Answer: DE

Explanation:
Comprehensive and Detailed 250 to 350 words of Explanation From Linux+ V8 documents:
Live migration is a virtualization feature that allows a running virtual machine to be moved from one host to another with minimal or no downtime. This topic falls underSystem Managementin the CompTIA Linux+ V8 objectives, particularly in the areas of virtualization and resource management.
For a live migration to succeed, theCPU architecture must matchbetween the source and destination hosts. This is critical because the running virtual machine??s CPU state, instruction set, and registers must be compatible with the destination system. Migrating between different CPU architectures (for example, x86_64 to ARM) is not supported and would cause the virtual machine to fail. Therefore, optionDis required.
Additionally, the destination host must havesufficient available memoryto accommodate the virtual machine being migrated. During live migration, the memory contents of the running VM are copied from the source host to the destination host while the VM continues to run. If enough memory is not available, the migration cannot complete successfully. This makes optionEmandatory.
The other options are not strict requirements. USB ports do not need to match for live migration. Network speed may affect migration performance but does not need to be identical. Available swap space is not directly required for migration. Disk storage paths do not need to match as long as shared storage or compatible storage access is available.
Linux+ V8 documentation emphasizes CPU compatibility and memory availability as core prerequisites for live migration. Therefore, the correct answers areD and E.

NEW QUESTION 71
An administrator receives the following output while attempting to unmount a filesystem:
umount /data1: target is busy.
Which of the following commands should the administrator run next to determine why the filesystem is busy?

A. ps -f /data1
B. du -sh /data1
C. top -d /data1
D. lsof | grep /data1

Answer: D

Explanation:
Filesystem unmount failures are common troubleshooting scenarios covered in Linux+ V8. When the error"target is busy"appears, it means one or more processes are actively using files or directories within the mount point.
The correct diagnostic command islsof | grep /data1. The lsof (list open files) utility displays all open files and the processes using them. Filtering the output with grep /data1 identifies exactly which processes are holding file descriptors on the filesystem, preventing it from being unmounted.
The other options are incorrect. ps -f displays process information but does not show open file usage. du -sh calculates disk usage and does not identify active processes. top monitors system performance but cannot pinpoint filesystem locks.
Linux+ V8 documentation emphasizes using lsof or fuser to identify resource locks before unmounting filesystems. Therefore, the correct answer isD.

NEW QUESTION 73
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 74
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 77
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 78
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 80
A Linux administrator needs to securely erase the contents of a hard disk. Which of the following commands is the best for this task?

A. sudo rm -rf /dev/sda1
B. sudo shred /dev/sda1
C. sudo parted rm /dev/sda1
D. sudo dd if=/dev/null of=/dev/sda1

Answer: B

Explanation:
Secure data destruction is an important security requirement addressed in Linux+ V8 objectives. When data must be permanently erased, standard file deletion commands are insufficient because they do not overwrite the data on disk.
The shred command is specifically designed to securely erase files or block devices by overwriting them multiple times with random data. Using sudo shred /dev/sda1 overwrites the entire partition, making data recovery extremely difficult or impossible. This aligns directly with Linux+ V8 best practices for secure data sanitization.
The other options are incorrect. rm -rf removes directory entries but does not overwrite disk data. parted rm deletes partition entries but leaves the underlying data intact. dd if=/dev/null writes zero bytes and does not overwrite existing data blocks.
Linux+ V8 documentation identifies shred as the most appropriate tool for secure erasure when compliance or confidentiality is required. Therefore, the correct answer isB.

NEW QUESTION 81
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 82
Which of the following best describes the role of initrd?

A. It is required to connect to the system via SSH.
B. It contains basic kernel modules and drivers required to start the system.
C. It contains trusted certificates and secret keys of the system.
D. It is required to initialize a random device within a Linux system.

Answer: B

NEW QUESTION 86
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

XK0-006 Practice Exam Features:

* XK0-006 Questions and Answers Updated Frequently

* XK0-006 Practice Questions Verified by Expert Senior Certified Staff

* XK0-006 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* XK0-006 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year