Exam Questions XK0-006

CompTIA Linux+ Exam

https://www.2passeasy.com/dumps/XK0-006/

NEW QUESTION 1
A Linux administrator receives reports about MySQL service availability issues. The administrator observes the following information:

- uptime -p shows the system has been up for only 2 minutes
- journalctl shows messages indicating:mysqld invoked oom-killermysqld cpuset=/ mems_allowed=0 Which of the following explains why the server was offline?

A. The process exhausted server memory.
B. The process was intentionally terminated by a privileged user.
C. The process crashed because of a filesystem error.
D. A network outage caused a service availability issue.

Answer: A

Explanation:
is A. The process exhausted server memory.

NEW QUESTION 2
A systems administrator needs to integrate a new storage array into the company's existing storage pool. The administrator wants to ensure that the server is able to detect the new storage array. Which of the following commands should the administrator use to ensure that the new storage array is presented to the systems?

A. lsscsi
B. lsusb
C. lsipc
D. lshw

Answer: A

Explanation:
Comprehensive and Detailed Explanation: From Exact Extract:
The lsscsi command is used to list information about SCSI devices (including storage arrays) that are attached to the system. This is critical when integrating a new storage array because it allows the administrator to verify that the operating system detects the new device at the SCSI layer, which is the underlying interface for most enterprise storage solutions. lsscsi outputs a list of recognized SCSI devices, their device nodes, and associated information.
Other options:

- B. lsusb: Lists USB devices, not storage arrays on SCSI/SATA/SAS.
- C. lsipc: Displays information on IPC (inter-process communication) facilities, unrelated to hardware detection.
- D. lshw: Lists hardware details and can show storage, but lsscsi is specifically designed for SCSI device detection and is the most direct method for this task.

Reference:
CompTIA Linux+ Study Guide: Exam XK0-006, Sybex, Chapter 7: "Managing Storage", Section: "Identifying and Accessing Storage Devices"
CompTIA Linux+ XK0-006 Objectives: Domain 4.0 – Storage and Filesystems
==========

NEW QUESTION 3
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 4
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 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

An administrator is investigating the reason a Linux workstation is not resolving the website http://www.comptia.org. The administrator executes some commands and receives the following output:

```
$ dig @8.8.8.8 www.comptia.org +short
104.18.16.29

$ nslookup -querytype=A www.comptia.org
...
Name: www.comptia.org
Address: 104.18.16.29

$ nslookup -querytype=AAAA www.comptia.org
...
*** Can't find www.comptia.org: No answer

$ ping -4 www.comptia.org
PING  www.comptia.org (104.18.99.101)
From somehost (192.168.1.192) icmp_seq=3 Destination Host Unreachable
...

$ cat /etc/hosts
127.0.0.1 localhost localhost.localdomain
104.18.99.101    www.comptia.org
```

Which of the following is the most likely cause?

A. The static entry needs to be removed from /etc/hosts.
B. The remote website does not support IPv6, and the workstation requires it.
C. The firewall needs to be modified to allow outbound HTTP and HTTPS.
D. The nameserver in /etc/resolv.conf needs to be updated to 8.8.8.8

Answer: A

Explanation:
When troubleshooting name resolution issues in Linux, /etc/hosts entries take precedence over DNS lookups. The workstation??s /etc/hosts file contains the line:
CopyEdit 104.18.99.101 www.comptia.org
This means any attempt to access www.comptia.org will resolve to 104.18.99.101, regardless of the real DNS response. However, both dig and nslookup show the correct IP as104.18.16.29. Because the local /etc/hosts entry overrides DNS, and the hardcoded IP is either incorrect or unreachable, all network traffic to www.comptia.org will fail or not reach the intended destination, resulting in the observed connectivity issue (Destination Host Unreachable).
Other options:
* B.The lack of IPv6 support is irrelevant since the host is using IPv4 and the DNS queries for IPv4 (A record) are successful.
* C.The firewall would block all HTTP/HTTPS connections, but the error shown is a host unreachable, not a port-specific issue.
* D.The nameserver is working; both dig and nslookup queries succeed and return the correct A record.
[Reference:, CompTIA Linux+ Study Guide: Exam XK0-006, Sybex, Chapter 8: "Networking Fundamentals", Section: "Troubleshooting Name Resolution", CompTIA Linux+ XK0-006 Objectives, Domain 2.0: Networking,]

NEW QUESTION 8
Which of the following is the main reason for setting up password expiry policies?

A. To avoid using the same passwords repeatedly
B. To mitigate the use of exposed passwords
C. To force usage of passwordless authentication
D. To increase password strength and complexity

Answer: B

Explanation:
Password management is a core topic in the Security domain of CompTIA Linux+ V8. Password expiry policies are implemented to reduce the risk associated with long-lived credentials.
The primary reason for enforcing password expiration is to mitigate the risk of exposed or compromised passwords. If a password is leaked through phishing, malware, keylogging, or data breaches, limiting its lifespan reduces the window of opportunity for attackers to exploit it. Requiring periodic password changes ensures that compromised credentials eventually become invalid.
Option B correctly captures this security objective. Linux+ V8 documentation emphasizes minimizing credential exposure as a key principle of access control.
The other options are secondary or incorrect. Avoiding password reuse and increasing complexity are addressed through password history and complexity policies, not expiration alone. Password expiry does not force passwordless authentication, making option C incorrect.
Therefore, the correct answer is B. To mitigate the use of exposed passwords.

NEW QUESTION 9
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, ,]

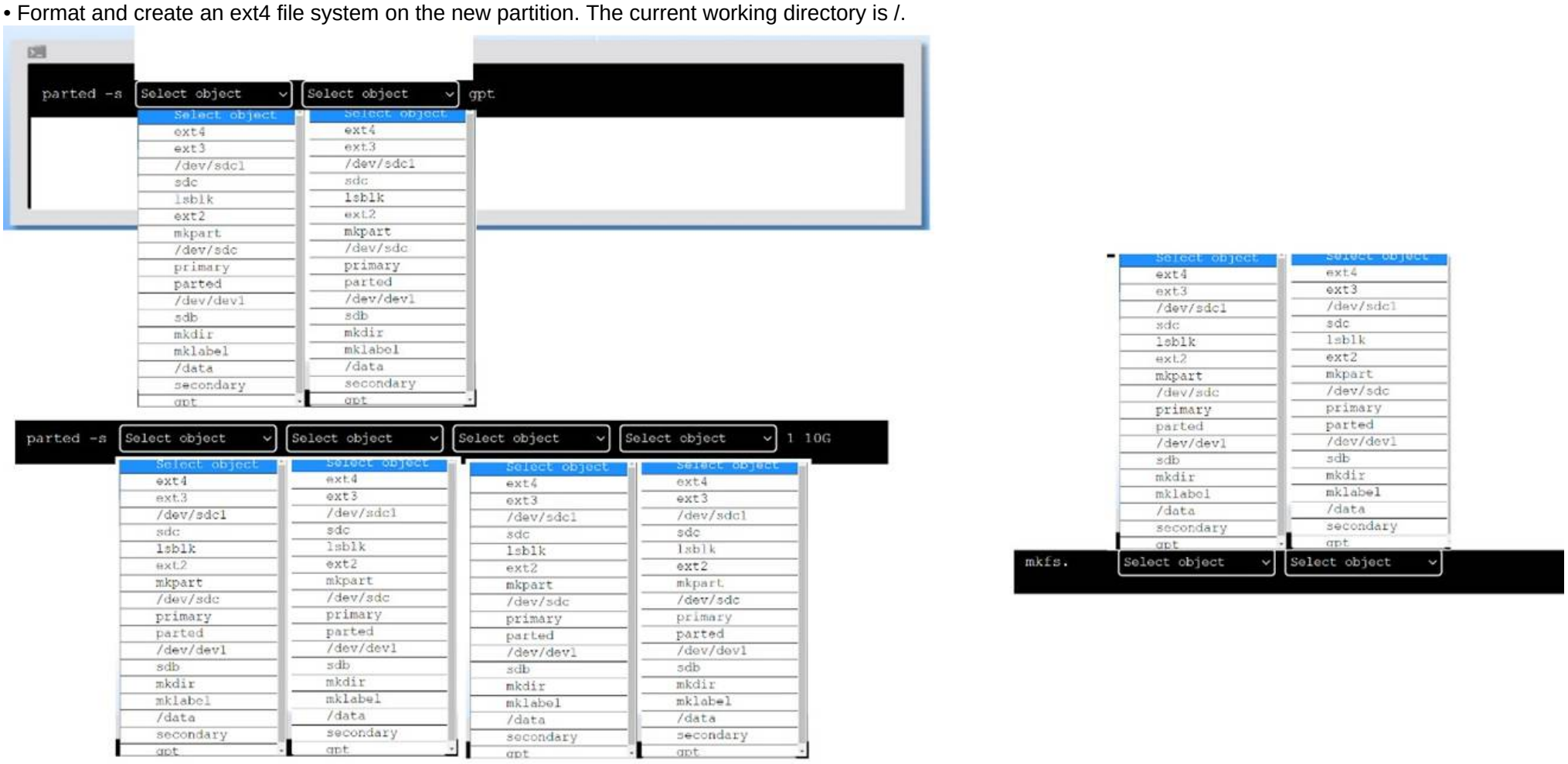
NEW QUESTION 10
A systems administrator wants to review the amount of time the NetworkManager service took to start. Which of the following commands accomplishes this goal?

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 10
A new drive was recently added to a Linux system. Using the environment and tokens provided, complete the following tasks:
• Create an appropriate device label.
• Format and create an ext4 file system on the new partition. The current working directory is /.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
To create an appropriate device label, format and create an ext4 file system on the new partition, you can use the following commands:

To create a GPT (GUID Partition Table) label on the new drive /dev/sdc, you can use the parted command with the -s option (for script mode), the device name (/dev/sdc), the mklabel command, and the label type (gpt). The command is:
parted -s /dev/sdc mklabel gpt
To create a primary partition of 10 GB on the new drive /dev/sdc, you can use the parted command with the -s option, the device name (/dev/sdc), the mkpart command, the partition type (primary), the file system type (ext4), and the start and end points of the partition (1 and 10G). The command is:
parted -s /dev/sdc mkpart primary ext4 1 10G
To format and create an ext4 file system on the new partition /dev/sdc1, you can use the mkfs command with the file system type (ext4) and the device name (/dev/sdc1). The command is:
mkfs.ext4 /dev/sdc1
You can verify that the new partition and file system have been created by using the lsblk command, which will list all block devices and their properties.

NEW QUESTION 12
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 13
A Linux administrator updates the DNS record for the company using:
cat /etc/bind/db.abc.com
The revised partial zone file is as follows:
ns1 IN A 192.168.40.251
ns2 IN A 192.168.40.252
www IN A 192.168.30.30
When the administrator attempts to resolve www.abc.com to its IP address, the domain name still points to its old IP mapping:
nslookup www.abc.com

Server: 192.168.40.251
Address: 192.168.40.251#53
Non-authoritative answer
Name: www.abc.com
Address: 199.168.20.81
Which of the following should the administrator execute to retrieve the updated IP mapping?

A. systemd-resolve query www.abc.com
B. systemd-resolve status
C. service nslcd reload
D. resolvectl flush-caches

Answer: D

Explanation:
This scenario represents a classic DNS troubleshooting situation covered in the Troubleshooting domain of the CompTIA Linux+ V8 objectives. Although the DNS zone file has been updated correctly on the BIND server, the system continues to resolve the domain name to an outdated IP address. This behavior strongly indicates DNS caching rather than a configuration error in the zone file itself.
Modern Linux systems that use systemd-resolved cache DNS responses locally to improve performance and reduce external queries. Even after a DNS record is updated on the authoritative server, cached results may persist until the cache expires or is manually cleared. The nslookup output showing a non-authoritative answer further confirms that the response is being served from a cache rather than directly from the updated zone data.
The correct solution is to flush the local DNS cache so the system can retrieve the updated record from the DNS server. The command resolvectl flush-caches clears all cached DNS entries maintained by systemd- resolved, forcing fresh queries to authoritative name servers. This aligns directly with Linux+ V8 documentation for resolving name resolution inconsistencies caused by stale cache entries.
The other options are incorrect for the following reasons. systemd-resolve query www.abc.com performs a DNS lookup but does not clear cached entries. systemd-resolve status only displays resolver configuration and statistics. service nslcd reload reloads the Name Service LDAP daemon and is unrelated to DNS resolution or caching.
Linux+ V8 emphasizes identifying whether issues originate from services, configuration, or cached data. In this case, flushing the DNS cache is the correct and least disruptive corrective action.
Therefore, the correct answer is D. resolvectl flush-caches.

NEW QUESTION 16
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 17
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 18

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 22
Which of the following Ansible components contains a list of hosts and host groups?

A. Fact
B. Inventory
C. Playbook
D. Collection

Answer: B

Explanation:
Ansible architecture and core components are part of the Automation, Orchestration, and Scripting domain in CompTIA Linux+ V8. Among these components, the inventory plays a foundational role in defining the infrastructure Ansible manages.
An Ansible inventory is a file (or set of files) that contains a list of managed hosts and optionally organizes them into logical groups. These hosts can be defined by IP address, fully qualified domain name (FQDN), or hostname. Inventories may be written in INI, YAML, or dynamically generated formats. Grouping hosts allows administrators to apply configurations, roles, and tasks to multiple systems simultaneously.
Option B, Inventory, is correct because it explicitly defines which systems Ansible will target. Without an inventory, Ansible does not know where to execute tasks. Linux+ V8 documentation emphasizes inventories as the starting point for all Ansible operations.
The other options are incorrect. Facts are system variables automatically collected by Ansible about managed hosts, such as OS version or IP address. Playbooks define what actions to perform but rely on the inventory to know where to perform them. Collections are distribution units that package roles, modules, and plugins, not host definitions.
Therefore, the correct answer is B. Inventory.

NEW QUESTION 25
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 27
A Linux administrator wants to make the enable_auth variable set to 1 and available to the environment of subsequently executed commands. Which of the following should the administrator use for this task?

A. let ENABLE_AUTH=1
B. ENABLE_AUTH=1
C. ENABLE_AUTH=$(echo $ENABLE_AUTH)
D. export ENABLE_AUTH=1

Answer: D

Explanation:
Environment variables in Linux can exist either locally within a shell or be exported to child processes. CompTIA Linux+ V8 emphasizes the distinction betweenshell variablesandenvironment variables, as this affects how applications inherit configuration values.
OptionD, export ENABLE_AUTH=1, is the correct choice because it both assigns the variable and marks it for export to the environment. Once exported, the variable becomes available to all subsequently executed commands and child processes spawned from the current shell. This behavior is required when applications or scripts rely on environment variables for configuration.
OptionB, ENABLE_AUTH=1, only sets a shell-local variable. While it is accessible within the current shell session, it is not inherited by child processes unless explicitly exported. OptionA, let ENABLE_AUTH=1, performs arithmetic evaluation and does not export the variable. OptionCincorrectly assigns the output of a command substitution and does not set the desired value.
Linux+ V8 documentation highlights export as the correct mechanism for making variables available system-wide within a user session. Therefore, the correct answer isD.

NEW QUESTION 32
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 34
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 37
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 40
Which of the following describes the method of consolidating system events to a single location?

A. Log aggregation
B. Health checks
C. Webhooks
D. Threshold monitoring

Answer: A

Explanation:
Comprehensive and Detailed 250 to 350 words of Explanation From Linux+ V8 documents:
Consolidating system events from multiple sources into a single, centralized location is a key concept in Linux system administration and is explicitly covered underlogging and monitoringtopics in the CompTIA Linux+ V8 objectives. This method is known aslog aggregation, making optionAthe correct answer.
Log aggregation refers to the practice of collecting logs generated by operating systems, services, applications, and network devices and storing them in a centralized repository. In Linux environments, logs may originate from systemd-journald, syslog, application-specific log files, containers, and cloud-based workloads. Aggregating these logs allows administrators to analyze events more efficiently, correlate issues across systems, and improve troubleshooting, auditing, and security monitoring.
Linux+ V8 documentation emphasizes centralized logging as a best practice in environments with multiple servers. Without log aggregation, administrators would need to log in to each system individually to inspect logs, which is inefficient and error-prone. Centralized solutions such as syslog servers, ELK/EFK stacks, and SIEM platforms enable real-time analysis, long-term retention, and alerting based on log data.
The other options do not describe log consolidation.Health checksare used to verify whether services or systems are operational but do not collect or store event data.Webhooksare HTTP-based callbacks used for event-driven automation and notifications, not for storing logs.Threshold monitoringinvolves generating alerts when metrics exceed defined limits, such as CPU or memory usage, but it does not centralize system event records.
Linux+ V8 stresses that effective log aggregation improves incident response, supports compliance requirements, and enhances system visibility. It is especially important for detecting security incidents, diagnosing failures, and performing root-cause analysis across distributed systems.

NEW QUESTION 44
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 46
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 47
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 48
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 51
An administrator wants to search a file named myFile and look for all occurrences of strings containingat least five characters, wherecharacters two and five are i, butcharacter three is not b. Which of the following commands should the administrator execute to get the intended result?

A. grep .a*^b-.a myFile
B. grep .a., [a] myFile
C. grepa^b*a myFile
D. grep .i[^b].i myFile

Answer: D

Explanation:
Pattern matching using regular expressions is a key troubleshooting and text-processing skill covered in CompTIA Linux+ V8. The grep command, combined with regular expressions, allows administrators to search for complex string patterns within files.
The requirement specifies:
The string must containat least five characters
Character 2must be i
Character 3mustnotbe b
Character 5must be i
To meet these conditions, the correct regular expression structure is:
. ?? any character (position 1)
i ?? literal i (position 2)
[^b] ?? any character except b (position 3)
. ?? any character (position 4)
i ?? literal i (position 5)
This results in the expression:
i[^b].i
OptionD, grep .i[^b].i myFile, correctly implements this logic. It ensures positional matching and excludes unwanted characters using a negated character class ([^b]), which is explicitly covered in Linux+ V8 regular expression objectives.
The other options contain invalid or malformed regular expressions and do not meet the positional or exclusion requirements. Linux+ V8 emphasizes understanding anchors, character classes, and position-based matching when troubleshooting log files or configuration data.
Therefore, the correct answer isD.

NEW QUESTION 55
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 60
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 61
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual XK0-006 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the XK0-006 Product From:

https://www.2passeasy.com/dumps/XK0-006/

Money Back Guarantee

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