CompTIA

Exam Questions XK0-006

CompTIA Linux+ Exam

About Exambible

Your Partner of IT Exam

Found in 1998

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

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

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

NEW QUESTION 1
Which of the following utilities supports the automation of security compliance and vulnerability management?

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

Answer: D

Explanation:
Security compliance and vulnerability management are critical components of Linux system administration, and CompTIA Linux+ V8 places strong emphasis on automated security assessment tools.OpenSCAPis specifically designed to address these requirements.
OpenSCAP is an open-source framework that implements theSecurity Content Automation Protocol (SCAP), a set of standards used for automated vulnerability scanning, configuration compliance checking, and security auditing. It allows administrators to assess Linux systems against established security baselines such asCIS benchmarks, DISA STIGs, and organizational security policies. This makes OpenSCAP the most appropriate tool for automating both compliance and vulnerability management.
The other options serve different security-related purposes but do not fulfill the automation requirement.SELinuxis a mandatory access control system that enforces security policies at runtime but does not perform compliance scanning or vulnerability assessments.Nmapis a network scanning and discovery tool used to identify open ports and services, not compliance automation.AIDE(Advanced Intrusion Detection Environment) is a file integrity monitoring tool that detects unauthorized file changes but does not evaluate overall system compliance.
Linux+ V8 documentation highlights OpenSCAP as a tool used to automate security audits, generate compliance reports, and integrate with configuration management workflows. Its ability to standardize security checks across multiple systems makes it essential in enterprise and regulated environments.
Therefore, the correct answer isD. OpenSCAP.

NEW QUESTION 2
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 3
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?

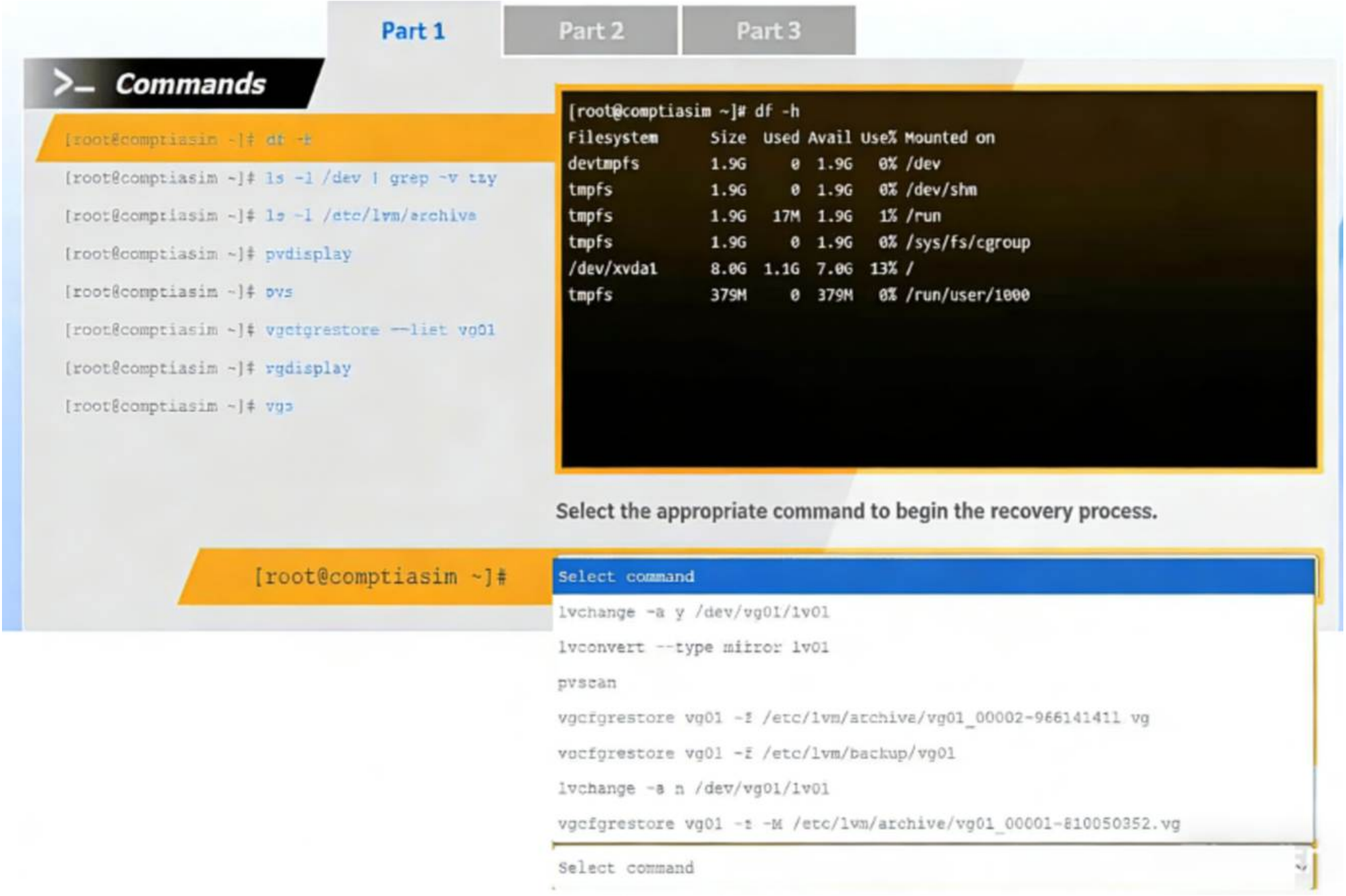
A. less
B. tail -f
C. tr -c

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 4
A junior system administrator removed an LVM volume by mistake.
INSTRUCTIONS
Part 1
Review the output and select the appropriate command to begin the recovery process.
Part 2
Review the output and select the appropriate command to continue the recovery process.
Part 3
Review the output and select the appropriate command to complete the recovery process and access the underlying data.



Part 2 | **Part 2** | Part 2

>_ Commands

```
[root@comptiasim ~]# blkid
[root@comptiasim ~]# dmesg | tail -20
[root@comptiasim ~]# blbik
[root@comptiasim ~]# ls /
[root@comptiasim ~]# lvdisplay
[root@comptiasim ~]# lvs
[root@comptiasim ~]# lvecan
[root@comptiasim ~]# pvs
[root@comptiasim ~]# vgs
```

```
[root@comptiasim ~]# blkid
/dev/xvda1: UUID="388a99ed-9486-4a46-aeb6-06eaf6c47675" TYPE="xfs"
/dev/xvdf: UUID="1uyvyk-Ffd0-8rvF-cYba-lSzC-EHRZ-JM3Uhm" TYPE="LVM2 member"
```

Select the appropriate command to continue the recovery process.

```
[root@comptiasim ~]#
```

Select command

```
pvchange -x y /dev/xvdf
lvextend -L V54 vg01/lv01 /dev/xvdf
lvchange -x y /dev/vg01/lv01
mount /dev/vg01/lv01/ /important data
lvchange -a n /dev/vg01/lv01
```

Select command

Part 1 | Part 2 | **Part 3**

>_ Commands

```
[root@comptiasim ~]# blkid
[root@comptiasim ~]# cat /etc/fstap
[root@comptiasim ~]# ls -l /dev/napper/
[root@comptiasim ~]# ls -l /
[root@comptiasim ~]# lsblk
[root@comptiasim ~]# lvdisplay
[root@comptiasim ~]# lvscan
[root@comptiasim ~]# tail -f /var/log/messages
[root@comptiasim ~]# xfs_repair -n /dev/vg01/lv01
```

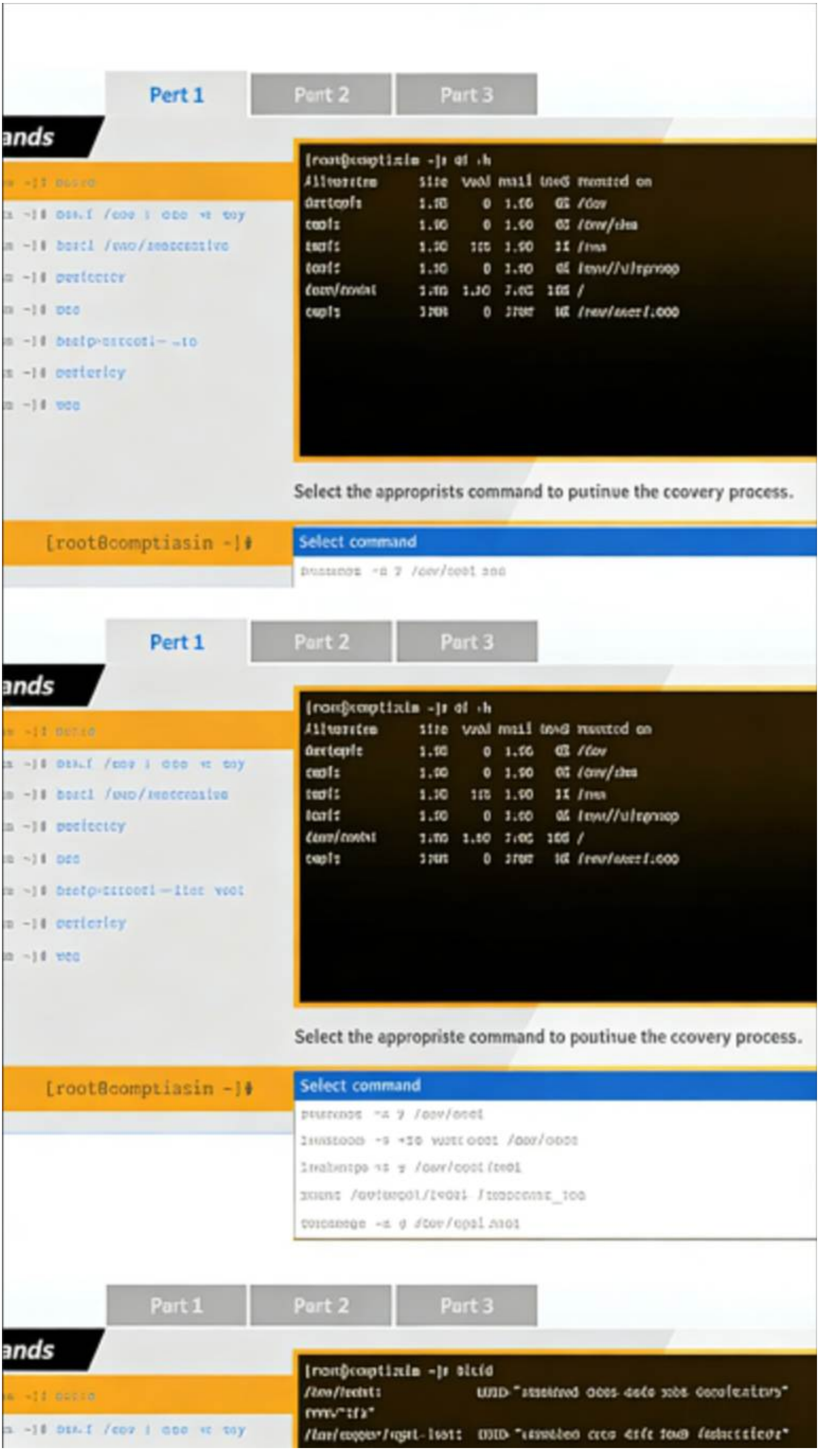
```
[root@comptiasim ~]# blkid
/dev/xvda1:              UUID="388a99ed-9486-4a46-aeb6-06eaf6c47675"
TYPE="xfs"
/dev/mapper/vg01-lv01:   UUID="c63883e9-ceca-45f4-9ad9-f8d8c1814e7e"
TYPE="xfs"
/dev/xvdf:               UUID="1uyvyk-Ffd0-RrYF-CYba-l5zC-EHRZ UM3UHm"
TYPE="LVM2_member"
```

Select command

```
xfs_repait /dev/vg01/lv01
lvscan -a
mount -a
mount /important_data /dev/vg01/lv01
xfs_mdrestore /dev/vg01 /important_data
```

```
[root@comptiasim ~]#
```

Select command


Part 1
Part 2
Part 3
[root@comptiasin ~]#
Select the appropriste command to putinue the ccovery process.
Select command
Select the appropriste command to poutinue the ccovery process.
Select command

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Part 1 – Begin the recovery process Answer
vgcfgrestore vg01 -f /etc/lvm/archive/vg01_00001-810050352.vg
Part 2 – Continue the recovery process Answer
lvchange -ay /dev/vg01/lv01
Part 3 – Complete recovery and access data Answer
mount /dev/vg01/lv01 /important_data
This performance-based question tests LVM recovery, a critical System Management skill in CompTIA Linux+ V8. The scenario indicates that a logical volume was removed, but the underlying physical volume and volume group metadata still exist.
Part 1: Restoring Volume Group Metadata
The first screenshot shows that:
* Physical volumes (pvdisplay, pvs) still exist
* The logical volume is missing
* /etc/lvm/archive/ contains archived VG metadata
Linux automatically stores backups of LVM metadata in /etc/lvm/archive whenever changes are made. The correct first step is to restore the volume group metadata using:
vgcfgrestore vg01 -f /etc/lvm/archive/vg01_00001-810050352.vg
This restores the logical volume definitions but does not activate them yet.
This is the only correct starting point in Linux+ V8 recovery workflows.
Part 2: Activating the Logical Volume
After metadata restoration:
* The LV exists but is inactive
* blkid shows the LV as TYPE="LVM2_member"
The logical volume must be activated before it can be mounted: lvchange -ay /dev/vg01/lv01
This makes the LV available under /dev/vg01/lv01. Linux+ explicitly requires LV activation after recovery.
Part 3: Accessing the Data
The final output shows:
* The filesystem type is xfs
* The logical volume is now visible
Since there is no indication of filesystem corruption, no repair is required.
The correct final step is to mount the filesystem: mount /dev/vg01/lv01 /important_data
This restores full access to the underlying data.

NEW QUESTION 5
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     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 6
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 7
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 8
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 9
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 10
Following the completion of monthly server patching, a Linux administrator receives reports that a critical application is not functioning. Which of the following commands should help the administrator determine which packages were installed?

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

Answer: A

Explanation:
Package management troubleshooting is a critical Linux administration skill addressed in CompTIA Linux+ V8. After system patching, identifying which packages were installed, updated, or removed is often the first step in diagnosing application failures.
Thednf historycommand is specifically designed for this purpose. It displays a chronological list of all DNF transactions, including installations, upgrades, downgrades, and removals. Each transaction is assigned an ID and includes timestamps, affected packages, and actions taken. This allows administrators to correlate application failures with recent changes.
OptionAis correct because it provides historical context rather than just current package state. Linux+ V8 documentation highlights dnf history as an essential auditing and rollback tool.
The other options are insufficient. dnf list shows installed or available packages but does not indicate when they were installed. dnf info displays metadata for a specific package but does not show transaction history. dnf search is used to find packages by name or description.
By reviewing recent transactions with dnf history, administrators can quickly identify problematic updates and take corrective action, such as rolling back a package.
Therefore, the correct answer isA.

NEW QUESTION 10
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 14
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 18
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 23
Which of the following is a reason multiple password changes on the same day are not allowed?

A. To avoid brute-forced password attacks by making them too long to perform
B. To increase password complexity and the system's security
C. To stop users from circulating through the password history to return to the originally used password
D. To enforce using multifactor authentication with stronger encryption algorithms instead of passwords

Answer: C

Explanation:
Password policy enforcement is a critical component of system security covered in the CompTIA Linux+ V8 objectives. One common control implemented in Linux systems is restricting how frequently users can change their passwords, often referred to asminimum password ageenforcement.
The primary reason multiple password changes within a short time frame are not allowed is toprevent password cycling attacks. Without this restriction, a user could repeatedly change their password in quick succession to bypass password history controls and eventually reuse a previously compromised or weak password. OptionCaccurately describes this scenario and aligns directly with Linux+ V8 security guidance.
Linux systems enforce this behavior through tools such as chage and PAM (Pluggable Authentication Modules). Administrators can configure minimum password age values to ensure users must wait a defined period before changing passwords again. This ensures that password history requirements are effective and meaningful.
The other options are incorrect. OptionAconfuses password expiration with brute-force mitigation, which is typically addressed through account lockout policies. OptionBrefers to password complexity, which is enforced through character requirements rather than change frequency. OptionDis unrelated, as password expiration policies do not enforce multifactor authentication.
Linux+ V8 documentation emphasizes layered access controls, and preventing password reuse through enforced timing restrictions is a core principle of secure authentication design.
Therefore, the correct answer isC.

NEW QUESTION 26
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 30
A systems administrator is configuring new Linux systems and needs to enable passwordless authentication between two of the servers. Which of the following commands should the administrator use?

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

Answer: A

NEW QUESTION 32
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 34
.....

Relate Links

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

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

Contact us

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

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