

Exam Questions XK0-006

CompTIA Linux+ Exam

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



NEW QUESTION 1

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. lspic
- 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. lspic: 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 2

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 3

On a Kubernetes cluster, which of the following resources should be created in order to expose a port so it is publicly accessible on the internet?

- A. Deployment
- B. Network
- C. Service
- D. Pod

Answer: C

Explanation:

Container orchestration concepts are part of the Automation and Orchestration domain in Linux+ V8. In Kubernetes, workloads run inside Pods, but Pods are not directly accessible from outside the cluster.

To expose an application externally, a Service resource must be created. Services provide a stable network endpoint and can be configured as NodePort, LoadBalancer, or ClusterIP. Public exposure is typically achieved using NodePort or LoadBalancer types.

Option C, Service, is correct. Deployments manage Pods, but they do not handle networking exposure. Pods represent running containers but lack external accessibility by default. "Network" is not a valid Kubernetes resource type.

Linux+ V8 documentation highlights Services as the mechanism for exposing containerized applications. Therefore, the correct answer is C.

NEW QUESTION 4

Which of the following best describes a use case for playbooks in a Linux system?

- A. To provide a set of tasks and configurations to deploy an application
- B. To provide the instructions for implementing version control on a repository
- C. To provide the security information required for a container
- D. To provide the storage volume information required for a pod

Answer: A

Explanation:

In the context of Linux automation and orchestration, playbooks are most commonly associated with configuration management tools such as Ansible, which is explicitly referenced in the CompTIA Linux+ V8 objectives. Playbooks are written in YAML and are designed to define a series of tasks, configurations, and desired system states that should be applied to one or more Linux systems in a repeatable and automated manner.

A primary use case for playbooks is application deployment and system configuration automation. Playbooks allow administrators to specify tasks such as installing packages, configuring services, managing users, setting permissions, deploying application files, and starting or enabling services. This aligns directly with option A, which accurately describes playbooks as a method to provide a set of tasks and configurations required to deploy an application consistently across environments.

The remaining options are not accurate representations of playbook functionality. Option B refers to version control implementation, which is handled by tools like Git and is not the purpose of playbooks themselves, although playbooks may be stored in version control systems. Option C describes container security information, which is typically managed through container runtime configurations, secrets, or security policies rather than playbooks. Option D refers to storage volume information for a pod, which is specific to Kubernetes manifests and not a general Linux playbook use case.

According to Linux+ V8 documentation, automation tools and playbooks help reduce human error, improve consistency, and support Infrastructure as Code (IaC) practices. Playbooks are a key mechanism for orchestrating multi-step operations across multiple systems, making them essential for modern Linux system administration.

Therefore, the correct answer is A, as it best describes the practical and documented use case for playbooks in a Linux system.

NEW QUESTION 5

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. OpenSCAP is specifically designed to address these requirements.

OpenSCAP is an open-source framework that implements the Security 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 as CIS 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. SELinux is a mandatory access control system that enforces security policies at runtime but does not perform compliance scanning or vulnerability assessments. Nmap is 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 is D. OpenSCAP.

NEW QUESTION 6

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

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

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

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

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 as 104.18.16.29. 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 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 10

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 10

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. firewallld -- 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 firewallld --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 firewallld 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; firewallld 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 firewallld"

CompTIA Linux+ XK0-006 Objectives, Domain 2.0: Networking

=====

NEW QUESTION 14

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 19

Which of the following describes PEP 8?

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

Answer: A

Explanation:

Python scripting is part of Linux automation, and Linux+ V8 includes knowledge of Python development standards. PEP 8 stands for Python Enhancement Proposal 8 and defines the official style guide for Python code.

PEP 8 provides conventions for code layout, indentation, naming, line length, whitespace usage, and commenting. Its purpose is to improve code readability and maintainability, especially in collaborative environments. Linux+ V8 emphasizes that standardized coding practices are critical in automation and DevOps workflows.

The other options are incorrect. Python virtual environments are managed using tools such as venv. Package installation is handled by pip. Octal values are represented using specific syntax and are unrelated to PEP 8.

Therefore, the correct answer is A.

NEW QUESTION 24

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, /proc is the filesystem that contains non-persistent, volatile data.

The /proc filesystem is a virtual filesystem that 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 is C. /proc.

NEW QUESTION 29

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 banner serves as a legal notification and does not affect system vulnerabilities.

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

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

[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 32

A Linux systems administrator needs to extract the contents of a file named /home/dev/web.bkp to the /var/www/html/ directory. Which of the following commands should the administrator use?

- A. `cd /var/www/html/ && gzip -c /home/dev/web.bkp | tar xf -`
- B. `pushd /var/www/html/ && cpio -idv < /home/dev/web.bkp && popd`
- C. `tar -c -f /home/dev/web.bkp /var/www/html/`
- D. `unzip -c /home/dev/web.bkp /var/www/html/`

Answer: B

Explanation:

Comprehensive and Detailed 250 to 350 words of Explanation From Linux+ V8 documents:

File extraction and backup restoration are fundamental System Management tasks covered in CompTIA Linux+ V8. In this scenario, the administrator must extract the contents of an existing backup file into a target directory.

The correct command is option B, which uses `cpio` in extract mode. The command changes into the destination directory (/var/www/html/) using `pushd`, extracts the archive contents with `cpio -idv`, and then returns to the original directory with `popd`. This ensures that files are restored into the correct location without modifying paths inside the archive.

The `cpio` utility is commonly used for backups created with `cpio -o` and supports reading archive data from standard input. Linux+ V8 documentation includes `cpio` as a valid and supported archive format for backup and restore operations.

The other options are incorrect. Option A incorrectly assumes the backup is a gzip-compressed tar archive. Option C creates a new archive instead of extracting one. Option D assumes the file is a ZIP archive, which is not indicated by the .bkp extension.

Linux+ V8 emphasizes using the correct tool based on the archive format and restoring files into the intended directory. Therefore, the correct answer is B.

NEW QUESTION 35

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 under System Management in the CompTIA Linux+ V8 objectives, particularly in the areas of virtualization and resource management.

For a live migration to succeed, the CPU architecture must match between 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, option D is required.

Additionally, the destination host must have sufficient available memory to 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 option E mandatory.

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 are D and E.

NEW QUESTION 37

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 is `lsof | 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 is D.

NEW QUESTION 42

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 44

A technician wants to temporarily use a Linux virtual machine as a router for the network segment 10.10.204.0/24. Which of the following commands should the technician issue? (Select three).

A. echo "1" > /proc/sys/net/ipv4/ip_forward

B. iptables -A FORWARD -j ACCEPT

C. iptables -A PREROUTING -j ACCEPT

D. iptables -t nat -s 10.10.204.0/24 -p tcp -A PREROUTING -j MASQUERADE

E. echo "0" > /proc/sys/net/ipv4/ip_forward

F. echo "1" > /proc/net/tcp

G. iptables -t nat -s 10.10.204.0/24 -A POSTROUTING -j MASQUERADE

Answer: ABG

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

To temporarily configure a Linux virtual machine as a router, the technician must enable IP forwarding and set up iptables rules to allow and masquerade traffic:

* A. echo "1">/proc/sys/net/ipv4/ip_forward: Enables IPv4 forwarding in the Linux kernel, allowing the VM to forward packets between interfaces.

* B. iptables -A FORWARD -j ACCEPT: Adds a rule to the iptables firewall to accept all forwarded packets (allows traffic to be routed).

* G. iptables -t nat -s 10.10.204.0/24 -A POSTROUTING -j MASQUERADE: Sets up network address translation (NAT) for outgoing packets from the 10.10.204.0/24 subnet, masquerading them as if they are coming from the VM's external IP.

Other options:

* C.andH.are not relevant for routing/NAT in this context (PREROUTING is generally used for DNAT, not for standard source NAT).

* D.is syntactically incorrect and mixes PREROUTING with MASQUERADE, which is not the proper combination for SNAT.

* E.disables forwarding.

* F.is not related to IP forwarding.

[Reference:, CompTIA Linux+ Study Guide: Exam XK0-006, Sybex, Chapter 9: "Networking", Section: "Configuring Linux as a Router", CompTIA Linux+ XK0-006 Objectives: Domain 2.0 – Networking, Official CompTIA Linux+ Cert Guide, Chapter 12: "Firewall and NAT configuration",]

NEW QUESTION 49

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 emphasizes security, compliance, and governance when 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.

Option B is 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 is B.

NEW QUESTION 52

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 56

.....

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