

CompTIA

Exam Questions XK0-006

CompTIA Linux+ Exam



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

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

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

Answer: A

Explanation:

Network configuration changes can cause immediate loss of connectivity if applied incorrectly. Linux+ V8 emphasizes safe configuration practices, particularly when managing remote systems.

The netplan try command applies network configuration changes temporarily and prompts the administrator to confirm them within a timeout period. If the administrator does not confirm, Netplan automatically rolls back to the previous working configuration. This prevents accidental outages caused by misconfigured network settings.

The netplan apply command makes changes permanent immediately and does not provide rollback protection. The other options are not valid Netplan commands. Linux+ V8 documentation explicitly references netplan try as a safe testing mechanism. Therefore, the correct answer is A.

NEW QUESTION 3

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

- A. export "VAR=SomeValue" >> ~/.ssh/profile
- B. export VAR=value
- C. VAR=value
- D. echo "export VAR=value" >> ~/.bashrc

Answer: D

Explanation:

Environment variables are widely used in Linux systems to configure application behavior, and Linux+ V8 emphasizes the distinction between temporary and persistent variables. A variable is persistent only if it is defined in a shell initialization file.

The correct approach is echo "export VAR=value" >> ~/.bashrc. This command appends the variable definition to the user's .bashrc file, ensuring the variable is set automatically every time the user starts a new shell session. This makes the variable persistent for that specific user.

Options B and C only define variables in the current shell session and are lost when the session ends. Option A incorrectly targets the SSH configuration directory and is not appropriate for defining shell environment variables.

Linux+ V8 documentation highlights .bashrc, .bash_profile, and /etc/profile as correct locations for persistent environment variables. Therefore, the correct answer is D.

NEW QUESTION 4

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, aServiceresource 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.

OptionC, 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 isC.

NEW QUESTION 5

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 6

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 7

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 8

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 the Security domain of the CompTIA Linux+ V8 objectives and focuses on system hardening and service minimization. The Nmap scan output reveals that port 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 in plaintext, making it vulnerable to interception through packet sniffing or man-in-the-middle attacks. Linux+ V8 documentation explicitly emphasizes the principle of least functionality, which states that unnecessary or insecure services should be disabled and removed entirely rather than merely restricted.

Option D, 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 with SSH, which provides encrypted communication and strong authentication mechanisms.

Option A, 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.

Option B is unrelated, as changing passwords does not address the risk of plaintext credential transmission. Option C is 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 9

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 10

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

```
E212: Cannot open file for writing

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

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

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

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

Answer: B

Explanation:

This scenario involves Linux file attributes and falls under the System Management domain of the CompTIA Linux+ V8 objectives. Although the administrator is operating as the root user, the system prevents the file from being modified. This behavior indicates that standard UNIX permissions are not the root cause of the problem.

The critical clue is provided by the `lsattr /etc/resolv.conf` output, which shows the immutable (`i`) attribute set on the file. When a file is marked immutable, it cannot be modified, deleted, renamed, or written to by any user, including root. This restriction overrides normal file permissions and ownership settings.

The `chattr` command is used to modify extended file attributes on Linux filesystems such as ext4. The option `-i` specifically removes the immutable attribute, restoring the file's ability to be edited. Therefore, running `chattr -i /etc/resolv.conf` allows the administrator to open and modify the file successfully.

The other options do not resolve the issue. `chown root` changes file ownership, but the file is already owned by root. `chmod 750` modifies permission bits, but permissions are ignored when the immutable attribute is set. `chgrp root` changes the group ownership, which also has no effect when immutability is enforced. Linux+ V8 documentation highlights immutable files as a security and stability feature, commonly used to protect critical configuration files from accidental or unauthorized changes. Administrators must explicitly remove this attribute before making modifications.

Therefore, the correct command to allow editing the file is B. `chattr -i /etc/resolv.conf`.

NEW QUESTION 10

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 14

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

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

Answer: B

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

The `chown` command is used to change the owner and group of files and directories. The `-R` (recursive) flag ensures that all contents within the directory are also updated. The correct syntax is `chown -R owner:group directory`. So, `chown -R Ansible:Ansible /opt/Ansible` will change the owner and group for `/opt/Ansible` and everything inside it to "Ansible".

Other options:

* A. `groupmod` is used to modify group properties, not ownership of directories or files.

* C. `usermod` is for modifying user properties or group memberships.

* D. `chmod` changes permissions, not owner/group.

[Reference:, CompTIA Linux+ Study Guide: Exam XK0-006, Sybex, Chapter 6: "User and Group Management", Section: "Managing File Ownership and

Permissions", CompTIA Linux+ XK0-006 Objectives, Domain 1.0: System Management,]

NEW QUESTION 19

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 21

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

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

Answer: B

Explanation:

Version control rollback operations are a core DevOps skill covered in the Linux+ V8 objectives. When changes in a local Git repository break an application and must be reverted, the administrator must choose a command that directly undoes those changes.

The command `git reset` is the most appropriate option in this scenario. It allows the engineer to move the current branch pointer (HEAD) to a previous commit, effectively discarding or undoing local changes. Depending on the reset mode (`--soft`, `--mixed`, or `--hard`), the engineer can control whether changes are preserved in the staging area or working directory. This flexibility makes `git reset` the primary tool for reverting problematic local changes.

The other options are not suitable. `git pull` fetches and merges changes from a remote repository and does not revert local modifications. `git rebase` rewrites commit history and is used to reapply commits on top of another base, not to undo broken changes. `git stash` temporarily saves uncommitted changes for later use but does not revert the repository to a stable state.

Linux+ V8 documentation emphasizes that `git reset` is commonly used during local development when changes need to be undone quickly before being shared with others. Therefore, the correct answer is B.

NEW QUESTION 25

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 27

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

```
$ ss -ltnl
State      Recv-Q Send-Q           LocalAddress:Port PeerAddress:Port Process
LISTEN     0      32      0.0.0.0:53       0.0.0.0:*         nssd
LISTEN     0     128      0.0.0.0:22       0.0.0.0:*         sshd
LISTEN     0    1024      0.0.0.0:443      0.0.0.0:*         httpd
LISTEN     0   4096      0.0.0.0:5355     0.0.0.0:*         ntpd
LISTEN     0     512 7.0.0.1:4711     0.0.0.0:*         ntpd

$ 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 -ltnl 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 32

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

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

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

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

Answer: D

Explanation:

The SSH configuration option PermitRootLogin prohibit-password prevents the root user from logging in with password authentication. This setting means root cannot use a password to log in via SSH; only key- based authentication is permitted for root. The administrator can still log in as root locally, which is not affected by this SSH configuration. To allow SSH access as root, the administrator must use an SSH key instead of a password.

Other options:

- * A. MaxSessions controls the number of simultaneous SSH sessions but is not causing the login denial here.
- * B. PAM (Pluggable Authentication Modules) is disabled, but enabling it is not required for basic SSH authentication.
- * C. Changing the SSH port is unrelated to the authentication method issue.

Reference:

CompTIA Linux+ Study Guide: Exam XK0-006, Sybex, Chapter 11: "Securing Linux", Section: "Securing SSH Access"
CompTIA Linux+ XK0-006 Objectives, Domain 3.0: Security

NEW QUESTION 37

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 38

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 39

An administrator receives reports that a web service is not responding. The administrator reviews the following outputs:

```
$ echo $PWD
/etc/pki/nginx

$ ls -lRt
.:
total 8
drwxr-xr-x. 2 root root 6 Jul 10 10:57 private
-rw-r--r--. 1 root root 895 Jul 10 10:56 server.crt
-rw-----. 1 root root 227 Jul 10 10:56 server.key
./private:
total 0

$ sudo systemctl status nginx
nginx.service - The nginx HTTP and reverse proxy server
   Loaded: loaded (/usr/lib/systemd/system/nginx.service; disabled; preset: disabled)
   Active: failed (Result: exit-code) since Wed 2023-11-01 06:56:51 EDT; 6s ago
     Process: 110551 ExecStartPre=/usr/bin/rm -f /run/nginx.pid (code=exited, status=0/SUCCESS)
     Process: 110552 ExecStartPre=/usr/sbin/nginx -t (code=exited, status=1/FAILURE)
    CPU: 144ms

Nov 01 06:56:51 webserver systemd[1]: Starting nginx.service - The nginx HTTP and reverse proxy server...
Nov 01 06:56:51 webserver nginx[110552]: nginx: [emerg] cannot load certificate key "/etc/pki/nginx/private/server.key": BIO_new_file()
failed (SSL: error:80000002:system library::No such file or directory:calli>
Nov 01 06:56:51 webserver nginx[110552]: nginx: configuration file /etc/nginx/nginx.conf test failed
Nov 01 06:56:51 webserver systemd[1]: nginx.service: Control process exited, code=exited, status=1/FAILURE
Nov 01 06:56:51 webserver systemd[1]: nginx.service: Failed with result 'exit-code'.
Nov 01 06:56:51 webserver systemd[1]: Failed to start nginx.service - The nginx HTTP and reverse proxy server.
```

Which of the following is the reason the web service is not responding?

- A. The private key needs to be renamed from server.crt to server, key so the service can find it.
- B. The private key does not match the public key, and both keys should be replaced.
- C. The private key is not in the correct location and needs to be moved to the correct directory.
- D. The private key has the incorrect permissions and should be changed to 0755 for the service.

Answer: C

Explanation:

This issue falls under the Troubleshooting domain of the CompTIA Linux+ V8 objectives, specifically service startup failures and certificate-related errors. The provided output clearly indicates that the NGINX service fails during startup due to an inability to locate the private key file.

The critical error message is:

cannot load certificate key "/etc/pki/nginx/private/server.key": No such file or directory

This message confirms that NGINX is explicitly configured to look for the private key in the directory /etc/pki/nginx/private/. However, the directory listing shows that the private directory exists but is empty, while the server.key file is located in /etc/pki/nginx/ instead. Because NGINX cannot find the private key at the configured path, the configuration test (nginx -t) fails, and systemd prevents the service from starting.

Option C correctly identifies the root cause: the private key is not in the correct location. Moving server.key into /etc/pki/nginx/private/ (or updating the NGINX configuration to match the current location) would resolve the issue. Linux+ V8 documentation stresses that service failures often result from misaligned configuration paths rather than corrupted files.

The other options are incorrect. Option A incorrectly refers to renaming a certificate file and does not address the path issue. Option B suggests a key mismatch, which would generate a different SSL error rather than a "file not found" error. Option D is also incorrect because private keys should not have executable permissions like 0755; typically, they are restricted (for example, 0600) for security reasons.

Therefore, the web service is not responding because the private key file is not located in the directory expected by the NGINX configuration. The correct answer is C.

NEW QUESTION 43

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

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

Answer: D

Explanation:

Service management using systemd is a core Linux+ V8 system management objective. Administrators frequently need to view the current status of all services to determine which ones are running, stopped, failed, or inactive.

The correct command is systemctl list-units --type=services, which displays all loaded service units along with their current state, including whether they are active, inactive, failed, or running. This provides a comprehensive, real-time view of service statuses on the system and is commonly used during troubleshooting and audits.

Option A, systemctl is-active, is designed to check the status of a single service, not all services. Option B lists socket units, not services. Option C, systemctl is-enabled, checks whether services are enabled at boot, not whether they are currently running.

Linux+ V8 documentation explicitly references systemctl list-units --type=service as the primary command for viewing service runtime states. Therefore, the correct answer is D.

NEW QUESTION 46

An administrator wants to search a file named myFile and look for all occurrences of strings containing at least five characters, where characters two and five are i,

but character 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. `grep a^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 contain at least five characters

Character 2 must be i

Character 3 must not be b

Character 5 must 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`

Option D, `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 is D.

NEW QUESTION 48

A Linux administrator needs to securely erase the contents of a hard disk. Which of the following commands is the best for this task?

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

Answer: B

Explanation:

Secure data destruction is an important security requirement addressed in Linux+ V8 objectives. When data must be permanently erased, standard file deletion commands are insufficient because they do not overwrite the data on disk.

The `shred` command is specifically designed to securely erase files or block devices by overwriting them multiple times with random data. Using `sudo shred /dev/sda1` overwrites the entire partition, making data recovery extremely difficult or impossible. This aligns directly with Linux+ V8 best practices for secure data sanitization.

The other options are incorrect. `rm -rf` removes directory entries but does not overwrite disk data. `parted rm` deletes partition entries but leaves the underlying data intact. `dd if=/dev/null` writes zero bytes and does not overwrite existing data blocks.

Linux+ V8 documentation identifies `shred` as the most appropriate tool for secure erasure when compliance or confidentiality is required. Therefore, the correct answer is B.

NEW QUESTION 52

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 53

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

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

XK0-006 Practice Exam Features:

- * XK0-006 Questions and Answers Updated Frequently
- * XK0-006 Practice Questions Verified by Expert Senior Certified Staff
- * XK0-006 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * XK0-006 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The XK0-006 Practice Test Here](#)