PassQueen
a.k.a dumpsqueen.com

CompTIA Linux+ Exam

CompTIA XK0-006

Version Demo

Total Demo Questions: 16

Total Premium Questions: 162

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, System Management	72
Topic 2, Security	32
Topic 3, Scripting, Containers, and Automation	29
Topic 4, Troubleshooting	29
Total	162

QUESTION NO: 1

A systems administrator needs to restore a backup to the /usr/app/data directory. Which of the following commands should the administrator use for this task?

A. tar -xvzf /tmp/backup.tar.gz -C /usr/app/data

B. tar -xvf /tmp/backup.tar.gz /usr/app/data

C. tar -xvzf /usr/app/data /tmp/backup.tar.gz

D. tar -xvzf /tmp/backup.tar.gz > /usr/app/data

ANSWER: A

Explanation:

`tar -xvzf /tmp/backup.tar.gz -C /usr/app/data` is the appropriate command because it extracts a gzip-compressed tar archive directly into the required restore location. The `-x` operation tells `tar` to extract archive members, while `-f /tmp/backup.tar.gz` identifies the archive file to process. The `-z` option applies gzip decompression, which is appropriate for an archive with the `.tar.gz` extension. The `-v` option displays the names of files as they are restored, providing useful confirmation during an administrative recovery operation.

Most importantly, `-C /usr/app/data` changes tar's working directory before extraction. As a result, archive paths are restored relative to `/usr/app/data`, rather than relative to the administrator's current shell directory. The destination directory should exist and the administrator must have sufficient permissions to write there. This use of `-C` is the standard tar mechanism for selecting an extraction destination and avoids requiring a separate directory change command. GNU tar documents extraction as an operation selected with `--extract` and documents `-C`/`--directory` as changing the working directory during processing. See the GNU tar operation summary and the GNU tar documentation for changing directories.

QUESTION NO: 2

An administrator must secure an account for a user who is going on extended leave. Which of the following steps should the administrator take? (Choose two)

A. Set the user's files to immutable.

B. Instruct the user to log in once per week.

C. Delete the user's /home folder.

D. Run the command passwd -l user.

E. Change the date on the /home folder to that of the expected return date.

F. Change the user's shell to /sbin/nologin.

ANSWER: D F

Explanation:

Running `passwd -l user` and changing the user's shell to `/sbin/nologin` are appropriate reversible controls for an account that must be retained during an extended leave. The `passwd -l` command locks the account password by placing a locking character before the password hash in the shadow password entry. This preserves the account, its UID, group memberships, home directory, file ownership, and configuration while preventing password-based authentication. It is therefore suitable when the account may need to be restored when the employee returns.

Setting the login shell to `/sbin/nologin` prevents an interactive login session from being established for the account. Using this shell provides an additional account-access control and can display a configured denial message rather than granting a command prompt. Combining password locking with a non-login shell is a practical defense-in-depth approach: authentication through the password is disabled, and interactive shell access is explicitly denied while the account remains intact for auditing and later reactivation. Before the user returns, the administrator can restore the prior shell and unlock the

password through normal, documented account-management procedures. See the passwd(1) manual page and the nologin(8) manual page.

QUESTION NO: 3

An administrator must allow the user `analyst` to read `/srv/reports/monthly.csv` without changing the file owner, group membership, or access granted to other users. Which of the following commands should the administrator use to grant and verify the required access? (Choose two)

A. setfacl -m u:analyst:r-- /srv/reports/monthly.csv

B. getfacl /srv/reports/monthly.csv

C. chmod 644 /srv/reports/monthly.csv

D. usermod -aG reports analyst

E. setfacl -m g:analyst:r-- /srv/reports/monthly.csv

ANSWER: A B

Explanation:

`setfacl -m u:analyst:r-- /srv/reports/monthly.csv` adds an access control list entry granting the named user read permission on the file. This changes neither the file ownership nor the traditional owner, group, and other permission classes. `getfacl /srv/reports/monthly.csv` displays the resulting ACL entries, including the effective permissions for `analyst`.

Using `chmod 644` could expose the file to every local user. Adding the user to a group changes group membership and may grant access to other resources. An ACL entry for a group does not meet the requirement to grant access specifically to the named user.

QUESTION NO: 4

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:

`wc -l` is the appropriate command because it counts newline-delimited input records. In a pipeline such as `ls -l /opt/application/home/ | wc -l`, the long-format directory listing is sent to `wc`, and `-l` returns the number of lines received. Since `ls -l` normally emits one long-format entry per directory item, this produces a count of the listed items and is the conventional answer for this command combination.

For scripting, the administrator should recognize that the result is a count of listing lines, rather than a fully robust count of filesystem objects in every possible filename scenario. Also, on systems where `ls -l` prints a leading `total` line for a directory, that line can affect the displayed count. Nevertheless, when the task explicitly asks which utility to place after `ls -l |` to count the output, `wc -l` directly performs that line-counting function. GNU documentation describes `wc` as printing newline, word, and byte counts, with `-l` selecting newline counts: GNU Coreutils wc invocation. The corresponding `ls` long-listing behavior is documented at GNU Coreutils ls listing information.

QUESTION NO: 5

An administrator uses firewalld and must allow inbound HTTPS traffic permanently. The rule must survive a reboot and become active immediately. Which of the following commands should the administrator use? (Choose two)

A. firewall-cmd --permanent --add-service=https

B. firewall-cmd --reload

C. firewall-cmd --add-service=https

D. firewall-cmd --permanent --remove-service=https

E. systemctl disable firewalld

ANSWER: A B

Explanation:

`firewall-cmd --permanent --add-service=https` adds the HTTPS service to the permanent firewalld configuration. `firewall-cmd --reload` reloads the firewall configuration, applying the permanent rule to the currently active runtime configuration.

A runtime-only `--add-service=https` rule is lost after a reboot. `--remove-service=https` removes access rather than allowing it. Disabling firewalld does not provide a controlled HTTPS exception and removes the host firewall protections.

QUESTION NO: 6

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:

The command `chown -R Ansible:Ansible /opt/Ansible` changes both ownership attributes for the specified directory tree. In `chown` syntax, the name before the colon identifies the new owning user, and the name after the colon identifies the new owning group. Therefore, this command assigns the user `Ansible` as the owner and the group `Ansible` as the group owner of `/opt/Ansible`. The `-R` (recursive) option is essential because the requirement includes not only the directory itself but also every file and subdirectory under it. This is commonly used after deploying application files into an installation directory so that the intended service or administrative account has consistent ownership across the full directory hierarchy. The account and group named `Ansible` must exist before the command is run, and changing ownership generally requires root privileges or the relevant administrative capabilities. The GNU Core Utilities documentation describes `chown` ownership syntax and its recursive behavior: GNU Coreutils: chown invocation. See also the Linux manual page for operational details and recursive traversal behavior: chown(1) manual page.

QUESTION NO: 7

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

A. yum repo-pkgs

B. yum list installed repos

C. yum reposync available

D. yum repolist all

ANSWER: D

Explanation:

The command `yum repolist all` is correct because it displays the complete list of repositories known to YUM, including both enabled and disabled entries. Its output includes each repository's ID, name, and status, allowing an administrator to confirm that the repository referenced in an update error is configured on the system and currently enabled. This is especially useful during troubleshooting because a repository may be present in a `.repo` configuration file but disabled, or it may be enabled but unavailable due to connectivity, metadata, or configuration issues. The default `yum repolist` view focuses on enabled repositories, while adding `all` ensures disabled repositories are visible as well, making it possible to distinguish a missing repository from one that simply needs to be enabled. On current RPM-based systems where DNF has replaced YUM, the equivalent command is generally `dnf repolist --all`; however, YUM-compatible systems support the command stated in the answer. Red Hat documents repository-listing operations in its package management guidance, and the YUM command reference describes repolist as the command for listing configured repositories.

QUESTION NO: 8

A systems administrator is restoring data from a backup. While analyzing the file format, the administrator sees the following output:

data: 7-zip archive data, version 0.4

Which of the following commands should the administrator use to help extract the data?

A. 7za e data

B. tar x --lzip --format=v7 data

C. unzip -p 7 data

D. zcat -S 7 data

ANSWER: A

Explanation:

`7za e data` is the appropriate command because the file-identification output explicitly identifies `data` as a 7-Zip archive. The `7za` utility is a command-line version of 7-Zip for supported archive operations. Its `e` command extracts files from an archive, placing extracted files in the current working directory. This is useful during data restoration when the immediate goal is to recover the archive's contents after determining its format with a tool such as `file`.

In this command, `data` is the archive filename and does not require a particular filename extension; 7-Zip can identify the archive format from its contents. The displayed archive version is also consistent with the 7z file format, so selecting a 7-Zip-compatible extraction utility matches the identified format. If preserving the archive's original directory structure is required, an administrator could use the related `x` extraction command instead; however, `e` correctly performs extraction and therefore helps recover the data. The 7-Zip command documentation defines `e` as extracting files without their full stored paths. See the 7-Zip command-line command reference and the 7-Zip command-line switches reference.

QUESTION NO: 9

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:

`export PATH=$PATH:/home/user/scripts` is correct because `PATH` is the shell environment variable that specifies the ordered list of directories searched when a user enters a command without a pathname. Appending `/home/user/scripts` preserves the existing command-search directories and adds the user's script directory, allowing a script there to be started by entering its filename alone. For example, after setting this value, entering `testscript` causes the shell to search the directories in `PATH`, including `/home/user/scripts`, and run `/home/user/scripts/testscript` when found. The script must still be executable, such as after using `chmod +x /home/user/scripts/testscript`, and it should have an appropriate interpreter line, for example `#!/bin/bash`. This `export` command affects the current shell session and processes launched from it. To make the setting persist for future interactive Bash sessions, the user can place the command in an applicable shell startup file such as `~/.bashrc`. Bash documents `PATH` as the search path for commands, while the Linux `path_resolution` manual describes pathname lookup behavior. See the GNU Bash variable documentation and the Linux path_resolution(7) manual page.

QUESTION NO: 10

An administrator maintains an Ansible repository that contains production API credentials. The credentials must not be stored in plaintext in Git, but authorized administrators must be able to use them when running the production playbook. Which of the following actions should the administrator take? (Choose two)

A. Run `ansible-vault encrypt group_vars/production/vault.yml`.

B. Run `ansible-playbook --ask-vault-pass site.yml`.

C. Add the credentials to `ansible.cfg` as plaintext variables.

D. Run `ansible-playbook --check site.yml`.

E. Add the vault file to `.gitignore` and leave the credentials only on one administrator workstation.

ANSWER: A B

Explanation:

`ansible-vault encrypt group_vars/production/vault.yml` encrypts the file containing the sensitive variables before it is committed to version control. The encrypted file can be stored in the repository without exposing its plaintext contents.

`ansible-playbook --ask-vault-pass site.yml` prompts the authorized administrator for the vault secret needed to decrypt protected variables during the playbook run. In managed automation, a protected vault-password file or another approved secret-management integration can be used instead, but the vault secret must be supplied securely.

QUESTION NO: 11

An administrator needs to create a new logical volume from sets of provisioned disks. Which of the following shows the correct order of commands the administrator should execute?

A. 1. pvcreate, 2. vgcreate, 3. lvcreate

B. 1. vgcreate, 2. pvcreate, 3. lvcreate

C. 1. vgcreate, 2. lvcreate, 3. pvcreate

D. 1. lvcreate, 2. pvcreate, 3. vgcreate

ANSWER: A

Explanation:

`1. pvcreate, 2. vgcreate, 3. lvcreate` is the correct LVM provisioning sequence because Logical Volume Manager builds storage in layers. First, `pvcreate` initializes each provisioned disk or disk partition as an LVM physical volume (PV), writing the LVM metadata needed for it to participate in LVM management. After the physical volumes exist, `vgcreate` combines one or more of them into a volume group (VG), which is the pooled storage resource from which capacity can be allocated. Finally, `lvcreate` allocates extents from that volume group to create the requested logical volume (LV). The resulting logical volume is exposed as a block device, typically under `/dev/<volume-group>/<logical-volume>` or `/dev/mapper/`, and can then be formatted with a filesystem and mounted for use. This layered order is fundamental to LVM: physical volumes supply storage to volume groups, and volume groups supply storage to logical volumes. See the pvcreate manual page and the lvcreate manual page for command behavior and LVM object relationships.

QUESTION NO: 12

A Linux administrator wants to use AI to deploy infrastructure as code. Which of the following is a best practice regarding the use of AI for this task?

A. Using copy and paste when possible

B. Generating monolithic code

C. Linting generated code

D. Merging CI/CD pipelines

ANSWER: C

Explanation:

Linting generated code is a best practice because AI-generated infrastructure-as-code must be reviewed and validated before it is allowed to modify an environment. AI can quickly produce Terraform configuration, Ansible playbooks, shell scripts, and similar automation artifacts, but the administrator remains accountable for their correctness, security, maintainability, and alignment with organizational standards. Linting provides an automated early check for issues such as invalid syntax, deprecated constructs, inconsistent formatting, unsafe patterns, and violations of defined coding rules. This makes it appropriate to integrate into a development or CI/CD workflow before infrastructure changes are planned or applied.

For example, `ansible-lint` analyzes playbooks, roles, and collections against rules intended to identify problematic automation practices. Its documentation describes using the tool to check Ansible content and enforce consistent quality controls. Terraform also provides validation capabilities that check whether configuration is syntactically valid and internally consistent. These checks do not replace testing, peer review, least-privilege design, or a controlled deployment process, but they are an important safeguard when code has been generated or assisted by AI. See the ansible-lint documentation and HashiCorp's Terraform validate command documentation.

QUESTION NO: 13

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: A B G

Explanation:

Temporarily routing IPv4 traffic through a Linux VM requires enabling kernel packet forwarding, permitting the forwarded traffic through the firewall, and translating source addresses when the routed subnet needs to reach networks beyond the VM. `echo " 1 " > /proc/sys/net/ipv4/ip_forward` sets the kernel's `ip_forward` control to enabled at runtime. This allows the host to forward received IPv4 packets between its network interfaces; because it is written directly to `/proc`, the setting is not persistent across a reboot unless separately configured.

`iptables -A FORWARD -j ACCEPT` appends an accepting rule to the filter table's FORWARD chain. Packets traversing the VM between interfaces are evaluated by this chain, so allowing them is necessary when firewall policy or existing rules could otherwise block forwarding. Finally, `iptables -t nat -s 10.10.204.0/24 -A POSTROUTING -j MASQUERADE` applies source NAT to traffic originating from the specified subnet as it leaves the VM. MASQUERADE is appropriate for an egress interface whose address may be dynamic, and it enables return traffic to be associated with the translated connection. Together, these runtime changes provide forwarding, firewall passage, and outbound NAT for the 10.10.204.0/24 segment. See the Linux kernel IP sysctl documentation and the iptables manual page.

QUESTION NO: 14

A database stores its data on the logical volume `/dev/vgdata/db`. The administrator must create a block-level backup while ensuring the backup represents a consistent database state. The volume group has sufficient free extents for a snapshot. Which of the following actions should the administrator take? (Choose two)

A. Stop the database service before creating the snapshot.

B. Create an LVM snapshot of /dev/vgdata/db.

C. Copy /dev/vgdata/db directly while the database remains active.

D. Extend /dev/vgdata/db before starting the backup.

E. Run pvcreate on the disk containing /dev/vgdata/db.

ANSWER: A B

Explanation:

The administrator should stop the database service before taking the snapshot so pending writes are completed and the data is in a consistent state. The administrator can then create an LVM snapshot of the logical volume and perform the backup from the snapshot device. Once the snapshot exists, the database service can resume while the backup process reads the point-in-time copy.

Copying the active logical volume directly can capture data while it is changing. Extending the logical volume adds capacity but does not create a consistent backup point. Recreating the physical volume would destroy the LVM metadata and data on that device.

QUESTION NO: 15

A shared project directory at `/srv/project` is owned by `root:root`. Members of the `developers` group must be able to create and modify files there, and newly created files must automatically grant the same group access. Which of the following commands should the administrator use? (Choose two)

A. setfacl -m g:developers:rwx /srv/project

B. setfacl -d -m g:developers:rwx /srv/project

C. chmod 700 /srv/project

D. chown developers:developers /srv/project

E. umask 007 /srv/project

ANSWER: A B

Explanation:

`setfacl -m g:developers:rwx /srv/project` grants the named `developers` group read, write, and execute access to the existing directory. Execute permission on a directory permits traversal, while write permission permits creating and removing entries.

`setfacl -d -m g:developers:rwx /srv/project` creates a default ACL entry. Default ACLs on a directory are inherited by newly created files and subdirectories, subject to the creating process's requested mode and ACL mask. A regular ACL alone does not ensure that new content receives the required group access.

QUESTION NO: 16 - (SIMULATION)

Joe, a user, has taken a position previously held by Ann. As a systems administrator, you

need to archive all the files from Ann ' s home directory and extract them into Joe ' s home

directory.

INSTRUCTIONS

Within each tab, click on an object to form the appropriate commands. Command objects may only be used once, but the spacebar _ object may be used multiple times. Not all objects will be used.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

ANSWER: See the explanation for the answer

Explanation:

Use the following object sequences in the two tabs:

Archive tab

Extract tab