ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFIATION

"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

www.atmicnetworks .com

Warning: Keep connected with our support team for latest updates

Question: 1

What are the differences between hard disk drives and solid state disks? (Choose two correct answers.)

A. Hard disks have a motor and moving parts, solid state disks do not.
B. Hard disks can fail due to physical damage, while solid state disks cannot fail.
C. Solid state disks can store many times as much data as hard disk drives.
D. /dev/sda is a hard disk device while /dev/ssda is a solid state disk.
E. Solid state disks provide faster access to stored data than hard disks.

Answer: AE

Explanation:
The main difference between hard disk drives (HDDs) and solid state drives (SSDs) is the way they store and access data. HDDs use a spinning disk (platter) and a moving head to read and write data, while SSDs use flash memory chips that have no moving parts. This makes SSDs faster, quieter, and more durable than HDDs, but also more expensive and less spacious. HDDs and SSDs are both I/O devices that can be used to boot the system and store data, but they have different advantages and disadvantages depending on the use case.

Reference:
Difference between Hard Disk Drive (HDD) and Solid State Drive (SSD) Hard Disk Drive (HDD) vs. Solid State Drive (SSD): What's the Difference? How to Check Whether Your Disk Is an SSD or HDD on Linux

Question: 2

Reverse DNS assigns hostnames to IP addresses. How is the name of the IP address 198.51.100.165 stored on a DNS server?

A. In the A record for 165.100.51.198.ipv4.arpA.
B. In the PTR record for 165.100.51.198.in-addr.arpA.
C. In the RNAME record for 198-51-100-165.rev.arpA.
D. In the ARPA record for 165.100.51.198.rev.
E. In the REV record for arpA.in-addr.198.51.100.165.

Answer: B

Explanation:

Reverse DNS lookups query DNS servers for a PTR (pointer) record; if the server does not have a PTR record, it

cannot resolve a reverse lookup. PTR records store IP addresses with their segments reversed, and they append ".in-addr.arpa" to that. For example, if a domain has an IP address of 192.0.2.1, the PTR record will store the domain's information under 1.2.0.192.in-addr.arpa. In IPv6, the latest version of the Internet Protocol, PTR records are stored within the ".ip6.arpa" domain instead of ".in-addr.arpa."1 Therefore, the name of the IP address 198.51.100.165 is stored in the PTR record for 165.100.51.198.in-addr.arpa. Reference: 1: Reverse DNS lookup - Wikipedia 1

Question: 3

Which of the following types of bus can connect hard disk drives with the motherboard?

A. The RAM bus
B. The NUMA bus
C. The CPU bus
D. The SATA bus
E. The Auto bus

Answer: D

Explanation:

A bus is a communication system that transfers data between components inside a computer or between computers. There are different types of buses that serve different purposes. The RAM bus connects the CPU with the main memory, the NUMA bus connects multiple processors in a multiprocessor system, the CPU bus connects the CPU with other components on the motherboard, and the Auto bus is a fictional bus that can transform into a robot. The SATA bus is the correct answer because it is a type of bus that can connect hard disk drives with the motherboard. SATA stands for Serial Advanced Technology Attachment and it is a standard interface for connecting storage devices such as hard disk drives, solid state drives, and optical drives. SATA offers faster data transfer rates, lower power consumption, and improved cable management compared to older interfaces such as IDE and SCSI. Reference: : [Bus (computing)] : [Transformers: Robots in Disguise (2015 TV series)] : [Serial ATA]3) : [SATA vs. IDE: What's the Difference?]

Question: 4

Members of a team already have experience using Red Hat Enterprise Linux. For a small hobby project, the team wants to set up a Linux server without paying for a subscription. Which of the following Linux distributions allows the team members to apply as much of their Red Hat Enterprise Linux knowledge as possible?

A. Ubuntu Linux LTS
B. Raspbian
C. Debian GNU/Linux
D. CentOS
E. openSUSE

Answer: D

Explanation:

CentOS is a Linux distribution that is based on the source code of Red Hat Enterprise Linux (RHEL). It is a free and open-source community-supported OS that provides an enterprise-level computing platform. CentOS is fully compatible with RHEL and can run the same applications and packages. Therefore, CentOS allows the team members to apply as much of their Red Hat Enterprise Linux knowledge as possible for their hobby project. Reference:

Linux Essentials Version 1.6 Objectives1, Topic 1.1: Linux Evolution and Popular Operating Systems, Subtopic: Linux Distributions

Linux Essentials Version 1.6 Exam Preparation Guide2, Section 1.1: Linux Evolution and Popular Operating Systems, Page 7

CentOS Website3, About CentOS Linux

Red Hat Enterprise Linux derivatives - Wikipedia4

Question: 5

What information can be displayed by top?

A. Existing files, ordered by their size.
B. Running processes, ordered by CPU or RAM consumption.
C. User accounts, ordered by the number of logins.
D. User groups, ordered by the number of members.
E. User accounts, ordered by the number of files.

Answer: B

Explanation:

The top command is a Linux command that shows the running processes on the system. It provides a dynamic real-time view of the system performance and resource usage. The top command can display various information about the processes, such as their process ID, user, priority, state, CPU and memory usage, command name, and more. The top command can also sort the processes by different criteria, such as CPU or RAM consumption, by using the interactive commands. The top command is useful for monitoring the system load and identifying the processes that are consuming the most resources. Reference:

Linux Essentials Topic 104: The Linux Operating System, section 104.3: Basic features and commands of the Linux standard shells.

Linux Essentials Topic 106: Security and File Permissions, section 106.4: Monitor and manage Linux processes.

Question: 6

Which of the following commands can be used to resolve a DNS name to an IP address?

A. dnsname
B. dns

C. query
D. host
E. iplookup

Answer: D

Explanation:

The host command is used to resolve a DNS name to an IP address or vice versa. It can also perform other DNS queries, such as finding the mail servers for a domain. The host command has the following syntax: host [options] [name] [server]. The name argument can be a hostname, such as www.lpi.org, or an IP address, such as 192.168.0.1. The server argument is optional and specifies the name or IP address of the DNS server to query. If no server is given, the default system resolver is used. Reference:

Linux Essentials Version 1.6 Objectives: 1.4.1. Demonstrate an understanding of the purpose and types of DNS records1

Linux Essentials Version 1.6 Exam Study Resources: Linux Essentials Manual - Chapter 10. Network Fundamentals - 10.3. DNS and Hostname Resolution - 10.3.1. The host Command2

Linux Essentials Version 1.6 Exam Study Resources: Linux Essentials Manual - Appendix A. Answers to the Exercises - Chapter 10. Network Fundamentals - 10.3. DNS and Hostname Resolution - Exercise 10.3.12

Question: 7

Which of the following outputs comes from the command free?

A.
```
21:04:15 up 14 days, 7:43, 3 users, load average: 0.89, 1.00, 0.99
```

B.
```
avg-cpu: %user   %nice    %system %iowait %steal %idle
          34.04    0.03      13.88    1.06    0.00   50.99
```

C
```
Filesystem            Size  Used  Avail  Use%  Mounted on
/dev/mapper/vg_ssd-   25G   20G   3.6G   85%   /
root
```

D
```
1.8M    / tmp
```

E
```
              total        used        free      shared  buff/cache   available
Mem:       16123128    12565680     2011624      412128     1545824     7180416
```

A. Option A B. Option B C. Option C D. Option D E. Option E

Answer: E

Explanation:

Question: 8

What is true about the dmesg command? (Choose two correct answers.)

A. It traces the execution of a command and shows each step the program carries out.
B. It sends messages to the command lines of all current user sessions.
C. It displays the content of the Linux kernel's ring buffer.
D. It immediately outputs all new messages written to the system journal.
E. It might not display older information because it was overwritten by newer information.

Answer: CE

Explanation:

The dmesg command is used to display the messages from the kernel that are stored in a ring buffer. A ring buffer is a fixed-size data structure that overwrites the oldest entries when it is full. Therefore, the dmesg command might not display older information because it was overwritten by newer information. The dmesg command is useful for troubleshooting system issues and checking hardware information. The dmesg command is not used to trace the execution of a command, send messages

to user sessions, or output the system journal. Those functions are performed by other commands such as strace, write, and journalctl respectively. Reference: : [dmesg] : [Ring buffer] : [strace] : [write (Unix)] : [journalctl]4)

Question: 9

Which of the following outputs could stem from the command last?

A. 1 ls
2 cat text.txt
3 logout
B. Password for user last changed at Sat Mar 31 16:38:57 EST 2018
C. Last login: Fri Mar 23 10:56:39 2018 from server.example.com
D. EXT4-fs (dm-7): mounted filesystem with ordered data mode. Opts: (null)
E. root tty2 Wed May 17 21:11 - 21:11 (00:00)

Answer: E

Explanation:

The last command in Linux is used to display the list of all the users logged in and out since the file /var/log/wtmp was created1. The output of the last command shows the username, the terminal, the IP address, the login time and date, and the duration of the session for each record2. The option E is the only one that matches this format. The other options are not related to the last command. Option A shows a list of commands executed by a user. Option B shows the password change information for a user. Option C shows the last login information for a user. Option D shows the mount information for a filesystem. Reference: Linux Essentials Version 1.6 Objectives3, Topic 1.4: Command Line Basics, Subtopic: Basic Shell Commands
Linux last Command Tutorial for Beginners (8 Examples)4

Question: 10

What is the UID of the user root?

A. 1
B. -1
C. 255
D. 65536
E. 0

Answer: E

Explanation:

The UID of the user root is always 0 on Linux systems. This is because the kernel uses the UID 0 to check for the superuser privileges and grant access to all system resources. The name of the user account with UID 0 is usually root, but it can be changed or have aliases. However, some applications may expect the name root and not work properly with a different name. The UID 0 is reserved for the root user and cannot be assigned to any other user. The UID 0 is stored in the /etc/passwd file along with other user information.

Reference:

Linux Essentials Topic 104: The Linux Operating System, section 104.4: Runlevels and Boot Targets. Linux Essentials Topic 106: Security and File Permissions, section 106.1: Basic security and identifying user types. Linux Essentials Topic 106: Security and File Permissions, section 106.2: Creating users and groups.

Question: 11

Which permissions are set on a regular file once the permissions have been modified with the command chmod 654 file.txt?

A. drw-r-xr--
B. d—wxr-x--
C. –wxr-x--x
D. –rwxrw---x
E. -rw-r-xr--

Answer: E

Explanation:

The chmod command is used to change the permissions of files and directories. The permissions are represented by three sets of three characters, indicating the permissions for the owner, the group, and the others. Each character can be either r (read), w (write), x (execute), or - (no permission). The chmod command can use either symbolic or numeric mode to specify the permissions. In this question, the numeric mode is used, which consists of three digits from 0 to 7. Each digit is the sum of the permissions for each set, where r is 4, w is 2, and x is 1. For example, 7 means rwx, 6 means rw-, and 4 means r–. Therefore, the command chmod 654 file.txt sets the permissions as follows: The first digit 6 means rw- for the owner, which means the owner can read and write the file, but not execute it.

The second digit 5 means r-x for the group, which means the group can read and execute the file, but not write it.
The third digit 4 means r-- for the others, which means the others can only read the file, but not write or execute it.
The resulting permissions are -rw-r-xr–, which is the correct answer. The other options are incorrect because they either have the wrong permissions or the wrong file type. A regular file does not have the d (directory) prefix, and a directory cannot have the - (no file type) prefix. Reference: Linux Essentials Version 1.6 Objectives: 4.1. Ownership and Permissions1
Linux Essentials Version 1.6 Exam Study Resources: Linux Essentials Manual - Chapter 8. Security and File Permissions - 8.1. Ownership and Permissions - 8.1.1. The chmod Command2
Linux Essentials Version 1.6 Exam Study Resources: Linux Essentials Manual - Appendix A. Answers to the Exercises - Chapter 8. Security and File Permissions - 8.1. Ownership and Permissions - Exercise 8.1.12

Question: 12

What is true about the owner of a file?

A. Each file is owned by exactly one user and one group.
B. The owner of a file always has full permissions when accessing the file.
C. The user owning a file must be a member of the file's group.
D. When a user is deleted, all files owned by the user disappear.
E. The owner of a file cannot be changed once it is assigned to an owner.

Answer: A

Explanation:

In Linux, every file and directory is associated with an owner and a group. The owner is the user who created the file or directory, and the group is the group to which the owner belongs. Therefore, each file is owned by exactly one user and one group. This is true for option A. The other options are false for the following reasons:
Option B: The owner of a file does not always have full permissions when accessing the file. The permissions are determined by the file mode, which can be changed by the owner or the root user. The file mode specifies the read, write, and execute permissions for the owner, the group, and others. The owner can have different permissions than the group or others.
Option C: The user owning a file does not have to be a member of the file's group. The owner can change the group ownership of the file to any group on the system, regardless of whether the owner belongs to that group or not. However, only the root user or a user with the CAP_CHOWN capability can change the group ownership to a group that the owner is not a member of.
Option D: When a user is deleted, all files owned by the user do not disappear. The files remain on the system, but their owner is changed to an invalid user ID (UID). The files can still be accessed by the group or others, depending on the permissions. The files can also be reclaimed by the root user or a user with the CAP_CHOWN capability, who can change the owner to a valid user.
Option E: The owner of a file can be changed once it is assigned to an owner. The owner can transfer the ownership to another user, or the root user or a user with the CAP_CHOWN capability can change the owner to any user on the system. The command to change the owner of a file is chown. Reference: 1: Chown Command in Linux (File Ownership) | Linuxize 2 3: Linux File Permissions and Ownership Explained with Examples 4 2: 3 Ways to Find File Owner in Linux - howtouselinux 1

Question: 13

Which of the following permissions are set on the /tmp/ directory?

A. rwxrwxrwt
B----- rwX
C. rwSrw-rw-
D. rwxrwS---
E. r-xr-X--t

Answer: A

Explanation:
The correct permissions for the /tmp directory are rwxrwxrwt, which means that the owner, group, and others have read, write, and execute permissions, and that the sticky bit is set. The sticky bit is a special permission that prevents users from deleting or renaming files that they do not own in a shared directory. The /tmp directory is used for storing temporary files that may be created by different users and processes, so it needs to be accessible and writable by all, but also protected from unauthorized deletion or modification of files. The rwxrwxrwt permissions can be set by using the chmod command with either the octal mode 1777 or the symbolic mode a+trwx. Reference: : [File system permissions] : [Sticky bit] : [chmod]

Question: 14

Which command adds the new user tux and creates the user's home directory with default configuration files?

A. defaultuser tux
B. useradd –m tux
C. usercreate tux
D. useradd –o default tux
E. passwd –a tux

Answer: B

Explanation:
The useradd command in Linux is used to create new user accounts on the system1. The -m option tells the command to create the user's home directory as /home/username and copy the files from /etc/skel directory to the user's home directory2. The /etc/skel directory contains the default configuration files for new users3. Therefore, the command useradd -m tux will add the new user tux and create the user's home directory with default configuration files. The other options are either invalid or do not create the user's home directory. Reference:
Linux Essentials Version 1.6 Objectives, Topic 1.4: Command Line Basics, Subtopic: Basic Shell Commands
Linux Essentials Version 1.6 Exam Preparation Guide, Section 1.4: Command Line Basics, Page 16 Linux useradd Command Tutorial for Beginners (15 Examples)

Question: 15

What information is stored in /etc/passwd? (Choose three correct answers.)

A. The user's storage space limit
B. The numerical user ID
C. The username
D. The encrypted password
E. The user\s default shell

Answer: BCE

Explanation:

The /etc/passwd file is a plain text-based database that contains information for all user accounts on the system. It is owned by root and has 644 permissions. The file can only be modified by root or users with sudo privileges and readable by all system users. Each line of the /etc/passwd file contains seven comma-separated fields, representing a user account. The fields are as follows:

Username: The string you type when you log into the system. Each username must be a unique string on the machine. The maximum length of the username is restricted to 32 characters.

Password: In older Linux systems, the user's encrypted password was stored in the /etc/passwd file. On most modern systems, this field is set to x, and the user password is stored in the /etc/shadow file.

User ID (UID): The user identifier is a number assigned to each user by the operating system to refer to a user. It is used by the kernel to check for the user privileges and grant access to system resources. The UID 0 is reserved for the root user and cannot be assigned to any other user.

Group ID (GID): The user's group identifier number, referring to the user's primary group. When a user creates a file, the file's group is set to this group. Typically, the name of the group is the same as the name of the user. User's secondary groups are listed in the /etc/group file.

User ID Info (GECOS): This is a comment field. This field contains a list of comma-separated values with the following information: User's full name or the application name, Room number, Work phone number, Home phone number, Other contact information.

Home directory: The absolute path to the user's home directory. It contains the user's files and configurations. By default, the user home directories are named after the name of the user and created under the /home directory.

Login shell: The absolute path to the user's login shell. This is the shell that is started when the user logs into the system. On most Linux distributions, the default login shell is Bash.

Therefore, the correct answers are B, C, and E. The user's storage space limit (A) is not stored in the /etc/passwd file, but in the /etc/quota file. The encrypted password (D) is not stored in the /etc/passwd file, but in the /etc/shadow file. Reference:

Linux Essentials Topic 104: The Linux Operating System, section 104.4: Runlevels and Boot Targets.

Linux Essentials Topic 106: Security and File Permissions, section 106.1: Basic security and identifying user types.

Linux Essentials Topic 106: Security and File Permissions, section 106.2: Creating users and groups.

Understanding the /etc/passwd File | Linuxize
Understanding the /etc/passwd File - GeeksforGeeks
passwd(5) - Linux manual page - man7.org
Understanding /etc/passwd file in Linux - DEV Community

Question: 16

Which of the following tar options handle compression? (Choose two correct answers.)

A. -bz
B. -z
C. -g
D. -j
E. -z2

Answer: BD

Explanation:

The tar command is used to create or extract compressed archive files that contain multiple files or directories. The tar command has the following syntax: tar [options] [archive-file] [file or directory...]. The options argument specifies how the tar command should operate and what kind of compression should be used. The archive-file argument is the name of the archive file to be created or extracted. The file or directory argument is the name of one or more files or directories to be included in or extracted from the archive file.

The following are some of the common options for the tar command:

- c: create a new archive file.
- x: extract files from an existing archive file.
- t: list the contents of an archive file.
- v: show the progress of the operation.
- f: specify the name of the archive file.
- z: use gzip compression or decompression.
- j: use bzip2 compression or decompression.
- J: use xz compression or decompression.

The options -z and -j are used to handle compression with the tar command. The option -z uses the gzip program to compress or decompress the archive file, which usually has the extension .tar.gz or .tgz. The option -j uses the bzip2 program to compress or decompress the archive file, which usually has the extension .tar.bz2 or .tbz. Both gzip and bzip2 are popular compression programs that reduce the size of files by removing redundant or unnecessary information.

For example, to create a compressed archive file called backup.tar.gz that contains the files and directories in the current directory, the following command can be used:

tar -czvf backup.tar.gz .

To extract the files and directories from the archive file backup.tar.gz to the current directory, the following command can be used: tar -xzvf backup.tar.gz

To create a compressed archive file called backup.tar.bz2 that contains the files and directories in the current directory, the following command can be used: tar -cjvf backup.tar.bz2 .

To extract the files and directories from the archive file backup.tar.bz2 to the current directory, the following command can be used: tar -xjvf backup.tar.bz2

The other options in the question are not related to compression. The option -bz is invalid, as there is no such option for the tar command. The option -g is used to create or update an incremental archive file, which only contains the files that have changed since the last backup. The option -z2 is also invalid, as there is no such option for the tar command. Reference:

Linux Essentials Version 1.6 Objectives: 3.1. Archiving Files on the Command Line1

Linux Essentials Version 1.6 Exam Study Resources: Linux Essentials Manual - Chapter 9. The Power of the Command Line - 9.1. Archiving Files on the Command Line - 9.1.1. The tar Command2 Linux Essentials Version 1.6 Exam Study Resources: Linux Essentials Manual - Appendix A. Answers to the Exercises - Chapter 9. The Power of the Command Line - 9.1. Archiving Files on the Command Line - Exercise 9.1.12

Question: 17

FILL BLANK

What keyword is used in a shell script to begin a loop? (Specify one keyword only, without any additional information.)

Answer: for

Explanation:

The keyword for is used in a shell script to begin a loop that iterates over a list of items or a range of numbers. The syntax of the for loop is as follows: for <var> in <list> do <commands> done

The variable <var> is assigned to each element of the <list> in turn, and the <commands> are executed for each iteration. The <list> can be a sequence of words, numbers, filenames, or other values. If the <list> is omitted, the for loop will iterate over the positional parameters ($1, $2, ...). The do and done keywords mark the beginning and the end of the loop body, respectively. The for loop is one of the three types of loops in shell scripting, along with the while and until loops. Reference: 1: Looping Statements | Shell Script - GeeksforGeeks 1 2: unix - Shell script "for" loop syntax - Stack Overflow 2 3: For Loop Shell Scripting - javatpoint 3

Question: 18

Which of the following commands creates an archive file work.tar from the contents of the directory ./ work/?

A. tar --new work.tar ./work/
B. tar –cf work.tar ./work/
C. tar –create work.tgz –content ./work/
D. tar work.tar < ./work/
E. tar work > work.tar

Answer: B

Explanation:

The correct command to create an archive file work.tar from the contents of the directory ./work/ is tar –cf work.tar ./work/. This command uses the -c option to create a new archive, the -f option to specify the file name, and the ./work/ argument to indicate the source directory. The other commands are incorrect for various reasons:

A . tar --new work.tar ./work/ is incorrect because there is no --new option in the tar command. The correct option for creating a new archive is --create or -c.

C . tar –create work.tgz –content ./work/ is incorrect because the -content option is not valid. The correct option for specifying the source files or directories is --files-from or -T. Also, the work.tgz file name implies compression, but the command does not use any compression option such as -z, -j, or - J.

D . tar work.tar < ./work/ is incorrect because the tar command does not accept input redirection from the standard input. The correct way to use the tar command is to provide the options and arguments after the command name.

E . tar work > work.tar is incorrect because the tar command does not produce output redirection to the standard output. The correct way to use the tar command is to use the -f option to specify the output file name.
Reference: : tar command in Linux with examples - GeeksforGeeks : tar Command in Linux With Examples | phoenixNAP KB

Question: 19

The current directory contains the following file:
-rwxr-xr-x 1 root root 859688 Feb 7 08:15 test.sh
Given that the file is a valid shell script, how can this script be executed? (Choose two correct answers.)

A. run test.sh
B. ${test.sh}
C. cmd ./test.sh
D. ./test.sh
E. bash test.sh

Answer: DE

Explanation:

A shell script is a file that contains a series of commands that can be executed by a shell interpreter. To execute a shell script, there are two main methods:
Method 1: Specify the path to the script file. This method requires that the script file has the execute permission, which can be granted by using the chmod command. The script file also needs to have a shebang line at the beginning, which indicates which interpreter to use for the script. For example, #!/bin/bash means to use the bash interpreter. To execute the script using this method, you can type the absolute path or the relative path to the script file. If you are in the same directory as the script file, you can use the ./ prefix to indicate the current directory. For example, ./test.sh will execute the test.sh script in the current directory.
Method 2: Pass the script file as an argument to the interpreter. This method does not require the execute permission or the shebang line for the script file. You can simply use the name of the interpreter followed by the script file name as an argument. For example, bash test.sh will execute the test.sh script using the bash interpreter.
Therefore, the correct answers are D and E. A. run test.sh is incorrect because run is not a valid command in Linux. B. ${test.sh} is incorrect because this syntax is used for variable expansion, not for executing a script. C. cmd ./test.sh is incorrect because cmd is not a valid command in Linux.
Reference:
Linux Essentials Topic 105: The Power of the Command Line, section 105.3: Basic shell scripting.
How to Run a Shell Script in Linux [Essentials Explained] - It's FOSS
How To Execute a Command with a Shell Script in Linux | DigitalOcean
How To Run the .sh File Shell Script In Linux / UNIX

Question: 20

Which of the following commands sorts the output of the command export-logs?

A. export-logs < sort
B. export-logs > sort
C. export-logs & sort
D. export-logs | sort
E. export-logs <> sort

Answer: D

Explanation:

The sort command is used to sort the lines of a text file or the output of another command in alphabetical, numerical, or other order. The sort command has the following syntax: sort [options] [file...]. The file argument is the name of one or more files to be sorted. If no file is given, the sort command reads from the standard input, which is usually the keyboard or the output of another command.

The | (pipe) symbol is used to connect the output of one command to the input of another command. This allows the creation of pipelines of commands that process data sequentially. The pipe symbol has the following syntax: command1 | command2. The command1 argument is the name of the first command, whose output is sent to the input of the second command. The command2 argument is the name of the second command, which receives the output of the first command as its input.

Therefore, the command export-logs | sort sorts the output of the export-logs command in alphabetical order. The export-logs command is assumed to be a custom command that exports some logs to the standard output. The sort command receives the output of the export-logs command as its input and sorts it according to the default criteria, which is the first character of each line. The sorted output is then displayed on the screen or can be redirected to a file or another command.

The other options in the question are incorrect because they use the wrong symbols to connect the commands. The < (input redirection) symbol is used to read the input of a command from a file instead of the keyboard. The > (output redirection) symbol is used to write the output of a command to a file instead of the screen. The & (background) symbol is used to run a command in the background, which means the command does not wait for user input and allows the user to run other commands simultaneously. The <> (bidirectional redirection) symbol is used to read and write the input and output of a command from and to the same file. None of these symbols can be used to sort the output of the export-logs command.

Reference:

Linux Essentials Version 1.6 Objectives: 3.2. Searching and Extracting Data from Files1

Linux Essentials Version 1.6 Exam Study Resources: Linux Essentials Manual - Chapter 9. The Power of the Command Line - 9.2. Searching and Extracting Data from Files - 9.2.1. The sort Command2 Linux Essentials Version 1.6 Exam Study Resources: Linux Essentials Manual - Chapter 9. The Power of the Command Line - 9.3. Turning Commands into a Script - 9.3.1. Pipes and Redirection2

Linux Essentials Version 1.6 Exam Study Resources: Linux Essentials Manual - Appendix A. Answers to the Exercises - Chapter 9. The Power of the Command Line - 9.2. Searching and Extracting Data from Files - Exercise 9.2.12

Linux Essentials Version 1.6 Exam Study Resources: Linux Essentials Manual - Appendix A. Answers to the Exercises - Chapter 9. The Power of the Command Line - 9.3. Turning Commands into a Script - Exercise 9.3.12

Question: 21

A directory contains the following files:

a .txt

b.txt

c. cav

What would be the output of the following shell script? for file in *.txt

```
do
  echo Sfile
done
```

A. *.txt
B. a b
C. c.cav
D. A.txt
E. A. txt

b. txt

Answer: E

Explanation:

The shell script uses a for loop to iterate over the files that match the pattern *.txt in the current directory. The pattern *.txt means any file name that ends with .txt, regardless of the case. The loop body simply prints the value of the variable file, which holds the name of the current file in each iteration. Therefore, the output of the shell script would be the names of the files that end with .txt, one per line. In this case, the files are A.txt and b.txt, so the output would be: A .txt b.txt

This corresponds to option E. The other options are incorrect for the following reasons:

Option A: *.txt is not the output of the shell script, but the pattern that the loop uses to match the files. The shell expands the pattern to the actual file names before executing the loop.

Option B: a and b are not the names of the files, but the first characters of the file names. The loop prints the whole file name, including the extension.

Option C: c.cav is not a file that matches the pattern *.txt, because it has a different extension. The loop ignores files that do not end with .txt.

Option D: A.txt is only one of the files that matches the pattern *.txt, but not the only one. The loop

prints both A.txt and b.txt.

Reference: 1: 9 Examples of for Loops in Linux Bash Scripts - How-To Geek 2 3: Looping Statements | Shell Script - GeeksforGeeks 1 4: shell - Loop through all the files with .txt extension in bash - Stack Overflow 5

Question: 22

Which of the following commands will search for the file foo.txt under the directory /home?

A. search /home –file foo.txt
B. search /home foo. txt
C. find /home – file foo.txt
D. find /home –name foo.txt
E. find /home foo.txt

Answer: D

Explanation:

The correct command to search for the file foo.txt under the directory /home is find /home –name foo.txt. This command uses the find command, which is used to search for files and directories that match certain criteria. The first argument, /home, specifies the starting point of the search. The second argument, -name, indicates that the search is based on the name of the file or directory. The third argument, foo.txt, is the name of the file to be searched for. The find command will recursively search all the subdirectories under /home and print the path of any file or directory that matches the name foo.txt.

The other commands are incorrect for various reasons:

A . search /home –file foo.txt is incorrect because there is no such command as search in Linux. The correct command for searching files and directories is find.

B . search /home foo.txt is incorrect because, as mentioned above, there is no search command in Linux. Also, this command does not use any option to specify the search criteria, such as -name, - type, -size, etc.

C . find /home – file foo.txt is incorrect because the option -file is not valid. The correct option for specifying the type of file or directory is -type, followed by a letter that indicates the type, such as f for regular file, d for directory, l for symbolic link, etc. For example, find /home -type f -name foo.txt would search for a regular file named foo.txt under /home.

E . find /home foo.txt is incorrect because this command does not use any option to specify the search criteria, such as -name, -type, -size, etc. This command will search for any file or directory that has foo.txt as part of its name, not exactly as its name. For example, this command will also match a file named barfoo.txt or a directory named foo.txt.bak.

Reference: : find command in Linux with examples - GeeksforGeeks : 15 Super Useful Examples of Find Command in Linux

Question: 23

The current directory contains the following file:

-rw-r—r— 1 root exec 24551 Apr 2 12:36 test.sh

The file contains a valid shell script, but executing this file using ./test.sh leads to this error: bash: ./test.sh: Permission denied

What should be done in order to successfully execute the script?

A. The file's extension should be changed from .sh to .bin.
B. The execute bit should be set in the file's permissions.
C. The user executing the script should be added to the exec group.

D. The SetUID bit should be set in the file's permissions
E. The script should be run using #!./test. sh instead of ./test.sh.

Answer: B

Explanation:

The execute bit in Linux is a permission bit that allows the user to run an executable file or enter a directory. For regular files, such as scripts or binaries, the execute bit must be set for the user to run them. For directories, the execute bit allows the user to access the files and subdirectories inside. Therefore, to successfully execute the script test.sh, the execute bit should be set in the file's permissions. This can be done by using the chmod command with the +x option, for example: chmod +x test.sh. The other options are either irrelevant or incorrect. The file's extension does not affect its executability, only its association with a program. The user executing the script does not need to be in the exec group, as long as the user has the execute permission on the file. The SetUID bit is a special permission bit that allows the user to run the file as the file's owner, regardless of the user's identity. This is not necessary for executing the script, and may pose a security risk. The #!./test.sh syntax is invalid, as the #! is used to specify the interpreter for the script, not the script itself. Reference:

Linux Essentials Version 1.6 Objectives1, Topic 1.4: Command Line Basics, Subtopic: Basic Shell Commands
Linux Essentials Version 1.6 Exam Preparation Guide2, Section 1.4: Command Line Basics, Page 16 Execute vs Read bit. How do directory permissions in Linux work?3

Question: 24

What is a Linux distribution?

A. The Linux file system as seen from the root account after mounting all file systems.
B. A bundling of the Linux kernel, system utilities and other software.
C. The set of rules which governs the distribution of Linux kernel source code.
D. An operating system based on Linux but incompatible to the regular Linux kernel.
E. A set of changes to Linux which enable Linux to run on another processor architecture.

Answer: B

Explanation:

A Linux distribution is a collection of software that is based on the Linux kernel and can be installed on a computer or a device to create a functional operating system. A Linux distribution typically includes the Linux kernel, a set of system utilities and libraries, a graphical user interface (GUI), a package manager, and various applications and services. A Linux distribution may also include additional software or features that are specific to the distribution's goals, target audience, or philosophy. For example, some Linux distributions are designed for desktop users, while others are optimized for servers, embedded systems, or security. Some Linux distributions are based on other Linux distributions, while others are developed independently. Some Linux distributions are free and open source, while others are proprietary or commercial. Some Linux distributions are popular and widely used, while others are niche or experimental. Some examples of Linux distributions are Ubuntu, Fedora, Debian, Mint, Arch, and Red Hat. Reference:

Linux Essentials Topic 101: System Architecture, section 101.1: Determine and configure hardware settings.

Linux Essentials Topic 102: Linux Installation and Package Management, section 102.1: Design hard disk layout.
Linux Essentials Topic 103: GNU and Unix Commands, section 103.1: Work on the command line. Linux Essentials Topic 104: The Linux Operating System, section 104.1: Boot the system.
Linux Essentials Topic 105: The Power of the Command Line, section 105.1: Use text streams and filters.
Linux Essentials Topic 106: Security and File Permissions, section 106.3: Modify file and directory permissions.
What is a Linux distribution? - Linux.com
Linux distribution - Wikipedia
Best Linux Distributions For Everyone in 2023 - It's FOSS

Question: 25

Which package management tool is used in Red Hat-based Linux Systems?

A. portage
B. rpm
C. apt-get
D. dpkg
E. packagectl

Answer: B

Explanation:
RPM stands for RPM Package Manager (formerly known as Red Hat Package Manager), which is a powerful, command-line package management tool developed for the Red Hat operating system. It is now used as a core component in many Linux distributions such as CentOS, Fedora, Oracle Linux, openSUSE and Mageia1. RPM can install, uninstall, and query individual software packages, but it cannot manage dependency resolution like YUM2. YUM is another package management tool that is based on RPM and can handle dependencies automatically. YUM is the primary package management tool for installing, updating, removing, and managing software packages in Red Hat Enterprise Linux2. Therefore, the correct answer is B. rpm, as it is the underlying package management tool used in Red Hat-based Linux systems. Reference:
Linux package management with YUM and RPM | Enable Sysadmin
Chapter 13. Package Management Tool Red Hat Enterprise Linux 5 | Red Hat Customer Portal Difference Between YUM and RPM | 2DayGeek

Question: 26

Which of the following programs is a graphical editor for vector graphics?

A. Python
B. NGINX
C. Samba
D. Inkscape
E. MySQL

Answer: D

Explanation:

A vector graphics editor is a software program that allows users to create and edit vector graphics, which are images composed of mathematical curves and shapes. Vector graphics are scalable, meaning they can be resized without losing quality or clarity. Python, NGINX, Samba, and MySQL are not vector graphics editors, but rather other types of software. Python is a programming language, NGINX is a web server, Samba is a file and print server, and MySQL is a database management system. Inkscape is a free and open source vector graphics editor that supports the SVG (Scalable Vector Graphics) format, as well as other formats. Inkscape can be used to create logos, icons, diagrams, illustrations, and other graphics. Inkscape is one of the applications covered in the Linux Essentials certification program from the Linux Professional Institute (LPI). Reference: Linux Essentials - Linux Professional Institute (LPI) Draw Freely | Inkscape

Question: 27

Where is the operating system of a Raspberry Pi stored?

A. On the master device attached to the Raspberry Pi's IDE bus.
B. On a read only partition on the Raspberry Pi's firmware, next to the BIOS.
C. On a removable SD card which is put into the Raspberry Pi.
D. On a Linux extension module connected to the Raspberry Pi's GPIO pins.
E. On rewritable flash storage which is built into the Raspberry Pi.

Answer: C

Explanation:

The Raspberry Pi uses an SD card (or microSD card for newer models) as its main storage device. This means that the operating system and any other files are stored on the SD card, which can be easily inserted or removed from the Raspberry Pi. The SD card also allows the user to switch between different operating systems by using different cards or partitions. The Raspberry Pi does not have any internal storage, such as a hard disk drive or a solid state drive, nor does it use any external devices, such as an IDE bus, a firmware partition, or a GPIO module, to store the operating system. Reference: Raspberry Pi OS – Raspberry Pi

Choosing Storage for Raspberry Pi - Kingston Technology
Beginner's Guide: How To Install a New OS on Raspberry Pi

Question: 28

What is defined by a Free Software license?

A. Details of the technical documentation each contributor has to provide.
B. The programming languages which may be used to extend the licensed program.
C. A complete list of libraries required to compile the licensed software.
D. Limits on the purposes for which the licensed software may be used.
E. Conditions for modifying and distributing the licensed software.

Answer: E

Explanation:

A free software license is a notice that grants the recipient of a piece of software extensive rights to modify and redistribute that software. These actions are usually prohibited by copyright law, but the rights-holder (usually the author) of a piece of software can remove these restrictions by accompanying the software with a software license which grants the recipient these rights. Software using such a license is free software (or free and open-source software) as conferred by the copyright holder. Free software licenses grant users the freedom to use it for any purpose, study and change the source code and copy and redistribute the software with or without modifications. Free software must come with source code or provide access to it, while the freedom to redistribute includes the right to give away copies gratis as well as sell copies1 Reference: 1: Free-software license - Wikipedia

Question: 29

Why are web browser cookies considered dangerous?

A. Cookies support identification and tracking of users.
B. Cookies are always public and accessible to anyone on the internet.
C. Cookies consume significant amounts of storage and can exhaust disk space.
D. Cookies store critical data which is lost when a cookie is deleted.
E. Cookies can contain and execute viruses and malware.

Answer: A

Explanation:

Web browser cookies are small pieces of data that are stored by a website on a user's browser. They are used to remember information about the user, such as preferences, login details, shopping cart items, etc. Cookies can also be used to identify and track users across different websites, which can have implications for privacy and security. For example, cookies can be used to show targeted ads based on the user's browsing history, or to collect personal information without the user's consent. Cookies are not inherently dangerous, but they can pose some risks if they are misused or compromised by malicious actors. Reference:

Linux Essentials - Linux Professional Institute (LPI), section 1.4.2
1.4 Lesson 1 - Linux Professional Institute Certification Programs, slide 18

Question: 30

Which of the following are typical services offered by public cloud providers? (Choose three correct answers.)

A. Platform as a Service(PaaS)
B. Infrastructure as a Service(IaaS)
C. Internet as a Service(IaaS)
D. Graphics as a Service (GaaS)
E. Software as a Service (SaaS)

Answer: ABE

Explanation:

These are the three most common service models offered by public cloud providers12. They differ in the level of abstraction and control they provide to the customers.

Platform as a Service (PaaS) is a service model where the public cloud provider offers a ready-to-use platform for developing, testing, and deploying applications. The provider manages the underlying infrastructure, such as servers, storage, network, and operating system, while the customer only needs to focus on the application code and configuration. Examples of PaaS include Google App Engine, IBM Cloud Foundry, and Microsoft Azure App Service12.

Infrastructure as a Service (IaaS) is a service model where the public cloud provider offers access to fundamental compute, network, and storage resources on demand over the public Internet or through dedicated connections. The provider manages the physical hardware and virtualization layer, while the customer has full control over the configuration and management of the virtual machines, operating system, and applications. Examples of IaaS include Google Compute Engine, IBM Cloud Virtual Servers, and Microsoft Azure Virtual Machines12.

Software as a Service (SaaS) is a service model where the public cloud provider offers ready-to-use software applications that run on the provider's infrastructure and are accessible through a web browser or a mobile app. The provider manages the entire software stack, including the infrastructure, platform, and application, while the customer only needs to pay for the usage or subscription of the service. Examples of SaaS include Google Workspace, IBM Watson, and Microsoft Office 36512.

Reference:

What is Public Cloud | IBM

What Is a Public Cloud? | Google Cloud

Question: 31

Which of the following characters in a shell prompt indicates the shell is running with root privileges?

A. !

B. #

C. *

D. &

E. $

Answer: B

Explanation:

The shell prompt is a symbol or a string of characters that indicates the shell is ready to accept commands. The shell prompt can be customized by the user or by the system administrator. The default shell prompt for a normal user is usually a dollar sign ($), while the default shell prompt for the root user is usually a hash sign (#). The root user is the superuser or the administrator of the system, who has full access and control over all files, commands, and resources. Running commands as root can be dangerous, as it can cause irreversible damage to the system if done incorrectly. Therefore, it is advisable to use sudo or su to run commands as root only when necessary, and to switch back to a normal user as soon as

possible. The shell prompt indicates the shell is running with root privileges when it ends with a hash sign (#). Reference: Linux Essentials - Linux Professional Institute (LPI)
Running a shell command as root - Unix & Linux Stack Exchange

Question: 32

Which of the following commands are used to get information on the proper use of ls? (Choose two correct answers.)

A. option ls
B. usage ls
C. manual ls
D. man ls
E. info ls

Answer: DE

Explanation:

The commands man ls and info ls are used to get information on the proper use of ls. The man command displays the manual page for a given command, which contains a description, synopsis, options, examples, and other details. The info command displays the info page for a given command, which is similar to the manual page but may have more information and hyperlinks. The option ls, usage ls, and manual ls commands are not valid commands in Linux and will result in an error message. Reference:
Linux Essentials Exam Objectives, Version 1.6, Topic 103.1, Weight 2
Linux Essentials Certification Guide, Chapter 3, Page 51-52
Ls Command in Linux (List Files and Directories) | Linuxize

Question: 33

What is true about a recursive directory listing?

A. It includes the content of sub-directories.
B. It includes the permissions of the directory listed.
C. It includes details of file system internals, such as inodes.
D. It includes ownership information for the files.
E. It includes a preview of content for each file in the directory.

Answer: A

Explanation:

A recursive directory listing is a way of displaying the files and folders in a directory and all its subdirectories. The recursive option can be used with various commands, such as ls, find, or dir, to list the files recursively. For example, the command ls -R will list all the files and folders in the current directory and any sub-directories, showing the hierarchy of the file system123 A recursive directory listing does not include the permissions, ownership, or file system details of the files, unless specified by other options. For example, the

command ls -IR will list the files recursively and also show the permissions, ownership, size, and modification date of each file1 A recursive directory listing also does not include a preview of the content of each file, unless specified by other options. For example, the command ls -R --file-type will list the files recursively and also show the file type indicator, such as / for directories, * for executable files, @ for symbolic links, etc1 Reference: 1: ls (Unix) - Wikipedia 2: Recursively List all directories and files - Stack Overflow 3: Why is ls -R called "recursive" listing? - Ask Ubuntu

Question: 34

Running the command rm Downloads leads to the following error:
rm: cannot remove 'Downloads/': Is a directory
Which of the following commands can be used instead to remove Downloads, assuming Downloads is empty? (Choose two correct answers.)

A. undir Downloads
B. rmdir Downloads
C. dir –r Downloads
D. rem Downloads
E. rm –r Downloads

Answer: BE

Explanation:

To remove a directory, you need to use a command that can delete directories, not just files. The rm command can only remove files by default, unless you use the -r option, which stands for recursive. This option tells rm to delete the directory and all of its contents, including subdirectories and files. The rmdir command can also remove directories, but only if they are empty. If the directory contains

any files or subdirectories, rmdir will fail and display an error message. Therefore, the correct commands to remove Downloads, assuming it is empty, are rmdir Downloads and rm -r Downloads. The other commands are either invalid or do not work on directories. Reference:
Linux Essentials - Linux Professional Institute (LPI), section 2.3.1
LPI Linux Essentials Study Guide: Exam 010 v1.6, 3rd Edition, chapter 4, page 93.

Question: 35

Which of the following directories contains information, documentation and example configuration files for installed software packages?

A. /usr/share/doc/
B. /etc/defaults/
C. /var/info/
D. /doc/
E. /usr/examples/

Answer: A

Explanation:

The /usr/share/doc/ directory is the standard location for documentation files for installed software packages on Linux systems12. It contains subdirectories for each package, which may include README files, manuals, license information, changelogs, examples, and other useful resources12. The /usr/share/doc/ directory is part of the Filesystem Hierarchy Standard (FHS), which defines the structure and layout of files and directories on Linux and other Unix-like operating systems3.

The other options are incorrect because:

/etc/defaults/ is a directory that contains settings for userland applications or services/daemons4.

/var/info/ is not a standard directory on Linux systems. The /var/ directory is used for variable data files, such as logs, caches, spools, and temporary files3.

/doc/ is not a standard directory on Linux systems. The / directory is the root of the filesystem hierarchy and contains essential files and directories for booting, restoring, recovering, and/or repairing the system3.

/usr/examples/ is not a standard directory on Linux systems. The /usr/ directory is used for shareable, read-only data, such as binaries, libraries, documentation, and source code3.

Reference:

Linux configuration: Understanding *.d directories in /etc | Enable Sysadmin

Configuration Files in Linux | Baeldung on Linux

Filesystem Hierarchy Standard - Wikipedia

Which of the Following Directories Contains Information, Documentation ...

Question: 36

Which of the following commands adds the directory /new/dir/ to the PATH environment variable?

A. $PATH=/new/dir: $PATH
B. PATH=/new/dir: PATH
C. export PATH=/new/dir: PATH
D. export $PATH=/new/dir: $PATH
E. export PATH=/new/dir: $PATH

Answer: C

Explanation:

The PATH environment variable is a colon-separated list of directories that the shell searches for commands. To add a new directory to the PATH, you need to append it to the existing value of the variable, using the syntax PATH=new/dir:PATH. However, this only changes the PATH for the current shell session. To make the change permanent, you need to use the export command, which makes the variable available to all child processes of the shell. The export command takes the name of the variable as an argument, without the dollar sign ($). Therefore, the correct command to add /new/dir/ to the PATH and export it is export PATH=/new/dir:PATH.

Reference:

Linux Essentials - Linux Professional Institute (LPI)

How to set the path and environment variables in Windows - Computer Hope

Question: 37

A user is currently in the directory /home/user/Downloads/ and runs the command

ls ../Documents/

Assuming it exists, which directory's content is displayed?

A. /home/user/Documents/
B. /home/user/Documents/Downloads/
C. /home/user/Downloads/Documents/
D. /Documents/
E. /home/Documents

Answer: A

Explanation:
The command ls .../Documents/ lists the contents of the directory /home/user/Documents/. The reason is that the argument .../Documents/ is a relative path that refers to the parent directory of the current directory, which is /home/user/, followed by the subdirectory Documents/. The ls command displays the files and directories in the specified path, or the current directory if no path is given. The command does not change the current directory, so the user remains in /home/user/Downloads/. Reference:
Linux Essentials Exam Objectives, Version 1.6, Topic 103.1, Weight 2
Linux Essentials Certification Guide, Chapter 3, Page 49-50
Ls Command in Linux (List Files and Directories) | Linuxize

Question: 38

A directory contains the following three files:

texts 1.txt
texts 2.txt
texts 3.csv
Which command copies the two files ending in .txt to the /tmp/ directory?

A. cp ??.txt /tmp/
B. cp *.txt /tmp/
C. cp. \.txt /tmp/
D. cp ?.txt /tmp/
E. cp $?.txt /tmp/

Answer: B

Explanation:

The correct command to copy the two files ending in .txt to the /tmp/ directory is cp *.txt /tmp/. This command uses the wildcard character * to match any number of characters before the .txt extension. Therefore, it will copy both texts 1.txt and texts 2.txt to the destination directory /tmp/. The other options are incorrect because they use different wildcard characters or syntax that do not match the desired files. For example, option A uses ?? to match exactly two characters before the .txt extension, but the files have a space and a number, which are not considered as one character. Option C uses a backslash \ to escape the dot . before the .txt extension, but this is unnecessary and will cause the command to fail. Option D uses ? to match exactly one character before the .txt extension, but the files have more than one character. Option E uses $? to match the exit status of the previous command before the .txt extension, but this is not relevant and will cause the command to fail123
Reference: 1: Linux wildcards | How do wildcards work in Linux with examples? - EDUCBA 2: Wildcards in Linux

Question: 39

When typing a long command line at the shell, what single character can be used to split a command across multiple lines?

Answer: \

Explanation:

The backslash character () is used to escape the meaning of the next character in a command line. This means that the next character is treated as a literal character, not as a special character. For example, if you want to use a space in a file name, you can use a backslash before the space to prevent the shell from interpreting it as a separator. Similarly, if you want to split a long command line across multiple lines, you can use a backslash at the end of each line to tell the shell that the command is not finished yet. The shell will ignore the newline character and continue reading the next line as part of the same command. For example, you can write: ls -l
/home/user/Documents

instead of:
ls -l /home/user/Documents
Both commands will produce the same output, but the first one is easier to read and type. Reference:
Linux Essentials - Linux Professional Institute (LPI), section 2.1.2
2.1 Command Line Basics - Linux Professional Institute Certification Programs, slide 7.

Question: 40

Which of the following DNS record types hold an IP address? (Choose two.)

A. NS
B. AAAA
C. MX
D. A
E. CNAME

Answer: B D

Explanation:
The DNS record types that hold an IP address are the A and AAAA records. These records are used to map a domain name to an IP address of the host, which is necessary for establishing a connection between a client and a server. The A record holds a 32-bit IPv4 address, while the AAAA record holds a 128-bit IPv6 address. For example, the A record for www.example.com could be: www.example.com. IN A 192.0.2.1
This means that the domain name www.example.com resolves to the IPv4 address 192.0.2.1.
Similarly, the AAAA record for www.example.com could be: www.example.com. IN AAAA
2001:db8::1

This means that the domain name www.example.com resolves to the IPv6 address 2001:db8::1.

The other options are incorrect because:

NS records are used to specify the authoritative name servers for a domain. They do not hold an IP address, but a domain name of the name server. For example, the NS record for example.com could be:

example.com. IN NS ns1.example.com.

This means that the name server ns1.example.com is authoritative for the domain example.com.

MX records are used to specify the mail exchange servers for a domain. They do not hold an IP address, but a domain name of the mail server and a preference value. For example, the MX record for example.com could be:

example.com. IN MX 10 mail.example.com.

This means that the mail server mail.example.com has a preference value of 10 for receiving email for the domain example.com.

CNAME records are used to create an alias for a domain name. They do not hold an IP address, but another domain name that the alias points to. For example, the CNAME record for www.example.com could be:

www.example.com. IN CNAME example.com.

This means that the domain name www.example.com is an alias for the domain name example.com.

Reference:

DNS Record Types: Defined and Explained - Site24x7

List of DNS record types - Wikipedia

Question: 41

Which of the following values could be a process ID on Linux?

A. /bin/bash
B. 60b503cd-019e-4300-a7be-922f074ef5ce
C. /sys/pid/9a14
D. fff3
E. 21398

Answer: E

Explanation:

A process ID on Linux is a unique integer value that identifies a running process. The process ID can range from 0 to a maximum limit, which is usually 32768 or higher, depending on the system configuration. The process ID of 0 is reserved for the kernel's idle task, and the process ID of 1 is reserved for the init system, which is the first process launched by the kernel. The process IDs are assigned sequentially to new processes, and are recycled when a process terminates. Therefore, the only valid value for a process ID among the given options is 21398, which is an integer within the possible range. The other values are not valid process IDs because they are either strings, hexadecimal numbers, or file paths, which do not match the format of a process ID on Linux. Reference:

Linux Essentials - Linux Professional Institute (LPI)

How Are Linux PIDs Generated? | Baeldung on Linux

Question: 42

Which of the following is a protocol used for automatic IP address configuration?

A. NFS
B. LDAP
C. SMTP
D. DNS
E. DHCP

Answer: E

Explanation:
DHCP stands for Dynamic Host Configuration Protocol. It is a protocol that provides quick, automatic, and central management for the distribution of IP addresses within a network. It also configures other network information, such as the subnet mask, default gateway, and DNS server information, on the device1. DHCP uses a client/server architecture, where a DHCP server issues unique IP addresses and automatically configures the devices that request them2. DHCP allows devices to move freely from one network to another and receive an IP address automatically, which is helpful with mobile devices1.
The other options are not protocols used for automatic IP address configuration. NFS stands for Network File System, which is a protocol that allows a user to access and modify files over a network as if they were on their own computer. LDAP stands for Lightweight Directory Access Protocol, which is a protocol that provides access to a centralized directory service that stores information about users, groups, computers, and other resources on a network. SMTP stands for Simple Mail Transfer Protocol, which is a protocol that enables the sending and receiving of email messages over a network. DNS stands for Domain Name System, which is a protocol that translates domain names into IP addresses and vice versa. Reference:
Linux Essentials Exam Objectives, Version 1.6, Topic 105.1, Weight 4
What Is DHCP? (Dynamic Host Configuration Protocol) - Lifewire
Dynamic Host Configuration Protocol (DHCP) | Microsoft Learn
Dynamic Host Configuration Protocol - Wikipedia How does AutoIP work? - Barix
[Network File System - Wikipedia]
[Lightweight Directory Access Protocol - Wikipedia] [Simple Mail Transfer Protocol - Wikipedia]
[Domain Name System - Wikipedia]

Question: 43

Which of the following devices represents a hard disk partition?

A. /dev/ttyS0
B. /dev/sata0
C. /dev/part0
D. /dev/sda2
E. /dev/sda/p2

Answer: D

Explanation:

Section: (none)

The correct device name that represents a hard disk partition is /dev/sda2. This device name follows the Linux convention for naming hard disk devices and partitions. According to this convention123:

The first part of the device name indicates the type of the device. For example, /dev/hd* for IDE drives, /dev/sd* for SCSI, SATA, USB, or eSATA drives, /dev/nvme* for NVMe drives, etc.

The second part of the device name indicates the order of the device as detected by the system. For example, /dev/sda is the first serial drive, /dev/sdb is the second serial drive, and so on.

The third part of the device name indicates the number of the partition on the device. For example, /dev/sda1 is the first partition on the first serial drive, /dev/sda2 is the second partition on the first serial drive, and so on.

Therefore, /dev/sda2 means the second partition on the first serial drive, which is a valid hard disk partition. The other options are not valid hard disk partitions, because they do not follow the Linux convention. For example:

/dev/ttyS0 is a serial port device, not a hard disk device4.

/dev/sata0 is not a valid device name, because it does not specify the partition number. It should be something like /dev/sata0p1 or /dev/sata0p2, etc.

/dev/part0 is not a valid device name, because it does not specify the device type or the partition number. It should be something like /dev/sdXp0 or /dev/hdXp0, etc.

/dev/sda/p2 is not a valid device name, because it uses a slash (/) instead of a number to indicate the partition. It should be something like /dev/sda2 or /dev/sda3, etc.

Reference: 1: Hard drive/device partition naming convention in Linux - Unix & Linux Stack Exchange 2: Hard drive partition naming convention in Linux - Ask Ubuntu 3: C.4. Device Names in Linux - Debian 4: What is /dev/ttyS0? - Quora

Explanation

Question: 44

Which of the following statements regarding Linux hardware drivers is correct?

A. Drivers are regular Linux programs which have to be run by the user who wants to use a device. B. Drivers are not used by Linux because the BIOS handles all access to hardware on behalf of Linux.

C. Drivers are stored on their devices and are copied by the Linux kernel when a new device is attached

D. Drivers are downloaded from the vendor's driver repository when a new device is attached.

E. Drivers are either compiled into the Linux kernel or are loaded as kernel modules.

Answer: E

Explanation:

Linux hardware drivers are software components that enable the Linux kernel to communicate with various devices, such as keyboards, mice, printers, scanners, network cards, etc. Drivers are either compiled into the

Linux kernel or are loaded as kernel modules. Kernel modules are pieces of code that can be loaded and unloaded into the kernel on demand. They extend the functionality of the kernel without requiring to rebuild or reboot the system. Drivers that are compiled into the kernel are always available, but they increase the size and complexity of the kernel. Drivers that are loaded as kernel modules are only available when needed, but they require a matching version of the kernel and the module. Linux supports a large number of hardware devices, thanks to the efforts of the open source community and some vendors who provide drivers for their products. However, some devices may not have a driver available for Linux, or may require a proprietary driver that is not included in the Linux distribution. In such cases, the user may need to install the driver manually from the vendor's website or from a third-party repository. Reference:
Linux Essentials - Linux Professional Institute (LPI), section 2.2.1
LPI Linux Essentials Study Guide: Exam 010 v1.6, 3rd Edition, chapter 3, page 67.

Question: 45

What can be found in the /proc/ directory?

A. One directory per installed program.
B. One device file per hardware device.
C. One file per existing user account.
D. One directory per running process.
E. One log file per running service.

Answer: D

Explanation:
The /proc/ directory is a virtual file system that contains information about the system and the processes running on it. It is not a conventional file system that stores files on a disk, but rather a dynamic view of the kernel's data structures. One of the features of the /proc/ directory is that it contains one subdirectory for each process running on the system, which is named after the process ID (PID). For example, the subdirectory /proc/1/ contains information about the process with PID 1, which is usually the init process. The process subdirectories contain various files that provide information about the process, such as its status, memory usage, open files, environment variables, command line arguments, and more. The /proc/ directory also contains a symbolic link called 'self', which points to the process that is accessing the /proc/ file system. Therefore, the correct answer is D. One directory per running process.
The other options are incorrect because:
A . One directory per installed program. This is not true, as the /proc/ directory does not contain information about installed programs, but only about running processes. Installed programs are usually stored in other directories, such as /bin/, /usr/bin/, /opt/, etc.
B . One device file per hardware device. This is not true, as the /proc/ directory does not contain device files, but only virtual files that represent kernel data. Device files are usually stored in the /dev/ directory, which is another special file system that provides access to hardware devices. C . One file per existing user account. This is not true, as the /proc/ directory does not contain information about user accounts, but only about processes. User accounts are usually stored in the /etc/ directory, which contains configuration files, such as /etc/passwd/ and /etc/shadow/, that define the users and their passwords.
E . One log file per running service. This is not true, as the /proc/ directory does not contain log files, but only information files. Log files are usually stored in the /var/log/ directory, which contains various files that record the activities of the system and the services.

Reference:
The /proc Filesystem — The Linux Kernel documentation
A Beginner's Guide to the /proc File System in Linux - Tecmint
Appendix E. The proc File System Red Hat Enterprise Linux 6 | Red Hat ... Chapter 5. The proc File System Red Hat Enterprise Linux 4 | Red Hat ... proc file system in Linux - GeeksforGeeks

Question: 46

A new server needs to be installed to host services for a period of several years. Throughout this time, the server should receive important security updates from its Linux distribution.

Which of the following Linux distributions meet these requirements? (Choose two.)

A. Ubuntu Linux LTS
B. Fedora Linux
C. Debian GNU/Linux Unstable
D. Ubuntu Linux non-LTS
E. Red Hat Enterprise Linux

Answer: AE

Explanation:
Ubuntu Linux LTS and Red Hat Enterprise Linux are two Linux distributions that meet the requirements of hosting services for a period of several years and receiving important security updates from their Linux distribution. LTS stands for Long Term Support, which means that these versions of Ubuntu Linux are supported by Canonical, the company behind Ubuntu, for five years with security patches, bug fixes, and software updates1. Red Hat Enterprise Linux is a commercial Linux distribution that offers a stable and secure platform for enterprise applications, with a 10-year life cycle and regular security updates from Red Hat, the company behind RHEL2. Fedora Linux, Debian GNU/Linux Unstable, and Ubuntu Linux non-LTS are not suitable for the requirements, because they have shorter support cycles and are more focused on providing the latest features and software versions, rather than stability and security. Fedora Linux releases a new version every six months and each version is supported for 13 months3. Debian GNU/Linux Unstable is the development branch of Debian, which is constantly updated with new packages and changes, but is not intended for production use4. Ubuntu Linux non-LTS releases a new version every six months and each version is supported for nine months1. Reference:
Ubuntu release cycle | Ubuntu
Red Hat Enterprise Linux Life Cycle - Red Hat Customer Portal Fedora Release Life Cycle - Fedora Project Wiki
Debian Unstable - Debian Wiki

Question: 47

Which of the following directories must be mounted with read and write access if it resides on its own dedicated file system?

A. /opt B. /lib C. /etc D. /var

E. /usr

Answer: D

Explanation:

The /var directory must be mounted with read and write access if it resides on its own dedicated file system. The reason is that the /var directory contains files and directories that are expected to change in size and content as the normal operation of the system progresses, such as logs, spool files, and temporary files1. Therefore, the /var directory needs to have enough space and permission to accommodate these changes. If the /var directory is mounted as read-only, some system services and applications may fail to start or function properly2.

The other options are not directories that must be mounted with read and write access if they reside on their own dedicated file system. The /opt directory contains optional or third-party software packages that are not part of the default installation1. The /lib directory contains libraries and kernel modules that are essential for the binaries in /bin and /sbin directories1. The /etc directory contains configuration files for the system and applications1. The /usr directory contains user-related programs, libraries, documentation, and data1. These directories are usually mounted as read-only to prevent accidental or malicious modification of their contents3.

Reference: Linux Essentials Exam Objectives, Version 1.6, Topic 102.1, Weight 3

Linux Essentials Certification Guide, Chapter 2, Page 34-35

Linux Filesystem Hierarchy, Chapter 3, Page 17-18

Question: 48

The ownership of the file doku.odt should be changed. The new owner is named tux. Which command accomplishes this change?

A. chmod u=tux doku.odt
B. newuser doku.odt tux
C. chown tux doku.odt
D. transfer tux: doku.odt
E. passwd doku.odt:tux

Answer: C

Explanation:

The correct command to change the ownership of the file doku.odt to a new owner named tux is chown tux doku.odt. This command uses the chown command, which stands for change owner, followed by the name of the new owner and the name of the file as arguments. The chown command allows you to change the user and/or group ownership of a given file, directory, or symbolic link12. The other options are incorrect because they use different commands or syntax that do not change the ownership of the file. For example:

Option A uses the chmod command, which stands for change mode, and is used to change the permissions of files and directories, not the ownership3.

Option B uses the newuser command, which is used to create a new user account, not to change the ownership of a file4.
Option D uses the transfer command, which is not a valid Linux command.
Option E uses the passwd command, which is used to change the password of a user account, not the ownership of a file5.
Reference: 1: Chown Command in Linux (File Ownership) | Linuxize 2: chown command in Linux with Examples - GeeksforGeeks 3: Chmod Command in Linux (File Permissions) | Linuxize 4: newusers(8) - Linux man page 5: passwd(1) - Linux man page

Question: 49

What happens to a file residing outside the home directory when the file owner's account is deleted? (Choose two.)

A. During a file system check, the file is moved to /lost +found.
B. The file is removed from the file system.
C. The UID of the former owner is shown when listing the file's details.
D. The user root is set as the new owner of the file.
E. Ownership and permissions of the file remain unchanged.

Answer: CE

Explanation:
When a user account is deleted, the files owned by that user are not automatically deleted from the file system, unless they are in the user's home directory. The files residing outside the home directory will remain unchanged, but they will have an invalid owner. The owner of a file is identified by a numeric user ID (UID), which is mapped to a user name by the /etc/passwd file. When a user is deleted, the corresponding entry in the /etc/passwd file is removed, but the UID of the file is not changed. Therefore, when listing the file's details, the UID of the former owner is shown instead of the user name. For example, if the user alice with UID 1001 is deleted, and she owns a file named report.txt in the /tmp directory, the output of ls -l /tmp/report.txt will look something like this: -rw-r–r-- 1 1001 users 1024 Nov 20 14:11 /tmp/report.txt
The user root is not set as the new owner of the file, nor is the file moved to /lost+found or removed from the file system. The /lost+found directory is used to store files that are recovered from a corrupted file system after running the fsck command, not from deleted user accounts. The file system check does not affect the ownership or permissions of the files, unless there is a serious inconsistency that needs to be fixed. Reference:
Linux Essentials - Linux Professional Institute (LPI), section 5.2.1
5.2 Lesson 1 - Linux Professional Institute Certification Programs, slide 6.

Question: 50

Which statements about the directory /etc/skel are correct? (Choose two.)
A. The personal user settings of root are stored in this directory.
B. The files from the directory are copied to the home directory of the new user when starting the system.
C. The files from the directory are copied to the home directory of a new user when the account is created.
D. The directory contains a default set of configuration files used by the useradd command.
E. The directory contains the global settings for the Linux system.

Answer: CD

Explanation:

The /etc/skel directory is a skeleton directory that contains the default files and directories that are automatically copied to the home directory of a new user when the account is created by the useradd command12. The purpose of this directory is to provide a consistent and uniform environment for all new users and to save the system administrator's time and effort in configuring the user settings12. The /etc/skel directory can be customized by adding or removing files and directories as needed, depending on the desired default settings for the new users12.

The other options are incorrect because:

A . The personal user settings of root are stored in this directory. This is not true, as the personal user settings of root are stored in the /root directory, which is the home directory of the root user3. The /etc/skel directory does not affect the root user's settings, but only the settings of the new users created by the useradd command12.

B . The files from the directory are copied to the home directory of the new user when starting the system. This is not true, as the files from the directory are copied to the home directory of the new user when the account is created, not when starting the system12. The copying process only happens once, when the useradd command is executed, and not every time the system is started12.

E . The directory contains the global settings for the Linux system. This is not true, as the directory contains the default settings for the new users, not the global settings for the Linux system12. The global settings for the Linux system are usually stored in other directories under /etc, such as /etc/default, /etc/sysconfig, /etc/init.d, etc4.

Reference:

Understanding the /etc/skel directory in Linux – The Geek Diary
/etc/skel directory in Linux - techPiezo
Linux File System Hierarchy - /root directory - LinuxConfig.org
Linux configuration: Understanding *.d directories in /etc | Enable Sysadmin

Question: 51

What is true about links in a Linux file system?

A. A symbolic link can only point to a file and not to a directory.
B. A hard link can only point to a directory and never to a file.
C. When the target of the symbolic link is moved, the link is automatically updated.
D. A symbolic link can point to a file on another file system.
E. Only the root user can create hard links.

Answer: D

Explanation:

A symbolic link, also known as a symlink or soft link, is a special type of file that points to another file or directory by its name. A symbolic link can point to a file or directory on the same or different file system, as long as the target is accessible. For example, you can create a symbolic link to a file on a USB drive or a network share, as long as the device is mounted or the connection is established. However, if the target of the symbolic link is moved, renamed, or deleted, the link becomes broken and does not work. To create a symbolic link, you can use the ln command with the -s or --symbolic option, followed by the target name and the link name. For example, ln -s /mnt/usb/file.txt link.txt creates a symbolic link named

link.txt that points to the file.txt on the USB drive mounted at /mnt/usb.

The other options are not true about links in a Linux file system. A symbolic link can point to a directory as well as a file. A hard link, which is a direct reference to the same data as another file, can only point to a file and not a directory. A hard link cannot span across different file systems, because it depends on the inode number, which is unique within a file system. When the target of the symbolic link is moved, the link is not automatically updated, but becomes broken. Any user can create hard links, as long as they have the permission to read and write the target file and the link directory.

Reference:

Linux Essentials - Linux Professional Institute (LPI)

Ln Command in Linux (Create Symbolic Links) | Linuxize

Question: 52

Which files are the source of the information in the following output? (Choose two.) uid=1000 (bob) gid=1000 (bob) groups=1000 (bob), 10 (wheel), 150 (docker), 1001 (libvirt) (wireshark), 989

A. /etc/id
B. /etc/passwd
C. /etc/group
D. /home/index
E. /var/db/users

Answer: BC

Explanation:

The files /etc/passwd and /etc/group are the source of the information in the following output: uid=1000 (bob) gid=1000 (bob) groups=1000 (bob), 10 (wheel), 150 (docker), 1001 (libvirt) (wireshark), 989

The /etc/passwd file contains information about user accounts, such as the username, password, user ID (UID), group ID (GID), full name, home directory, and login shell1. The /etc/group file contains information about groups, such as the group name, password, group ID (GID), and members2.

The output shows the UID, GID, and group membership of the user bob. The UID and GID of bob are 1000, which can be found in the /etc/passwd file. The groups that bob belongs to are bob, wheel, docker, libvirt, wireshark, and 989, which can be found in the /etc/group file. The group names are shown in parentheses after the GID, except for the last group, which has no name.

The other options are not files that store user and group information in Linux. The /etc/id file does not exist by default. The /home/index file is not a standard file and has no relation to user and group information. The /var/db/users file is not a standard file and has no relation to user and group information. Reference:

Linux Essentials Exam Objectives, Version 1.6, Topic 103.1, Weight 2

Linux Essentials Certification Guide, Chapter 3, Page 51-52

Linux Filesystem Hierarchy, Chapter 3, Page 17-18

Linux Users and Groups, Chapter 2, Page 9-10

Question: 53

Which of the following tasks can the command passwd accomplish? (Choose two.)

A. Change a user's username.
B. Change a user's password.
C. Create a new user account.
D. Create a new user group.
E. Lock a user account.

Answer: BE

Explanation:
The passwd command in Linux is used to change the password of a user account. A normal user can run passwd to change their own password, and a system administrator (the superuser) can use passwd to change another user's password, or define how that account's password can be used or changed1. The passwd command can also be used to lock or unlock a user account. Locking a user account means disabling the user's ability to log in to the system, while unlocking a user account means restoring the user's ability to log in. To lock a user account, the passwd command can be used with the -l option, followed by the username. To unlock a user account, the passwd command can be used with the -u option, followed by the username12. The passwd command cannot be used to change a user's username, create a new user account, or create a new user group. These tasks require different commands, such as usermod, useradd, or groupadd345. Reference: 1: Linux Passwd Command Help and Examples 2: Passwd command in Linux: 8 Practical Examples 3: usermod(8) - Linux man page 4: useradd(8) - Linux man page 5: groupadd(8) - Linux man page

Question: 54

What is true about the su command?

A. It is the default shell of the root account.
B. It can only be used by the user root.
C. It runs a shell or command as another user.
D. It changes the name of the main administrator account.
E. It locks the root account in specific time frames.

Answer: C

Explanation:
The su command stands for substitute user or switch user. It allows you to run a shell or a command as another user, usually the superuser or root. To use the su command, you need to know the password of the target user. For example, if you want to switch to the root user, you can type su - and enter the root password. This will give you a root shell, where you can execute commands with administrative privileges. To exit the root shell, you can type exit or press Ctrl-D. The su command is not the default shell of the root account, nor can it only be used by the root user. It can be used by any user who knows the password of another user. The su command does not change the name of the main administrator account, which is always root on Linux systems. The su command also does not lock the root account in specific time frames, although there are other ways to do that, such as using the pam_time module. Reference:
Linux Essentials - Linux Professional Institute (LPI), section 5.1.1
LPI Linux Essentials Study Guide: Exam 010 v1.6, 3rd Edition, chapter 9, page 219.

Question: 55

What parameter of ls prints a recursive listing of a directory's content? (Specify ONLY the option name without any values or parameters.)

Answer: ls -R

Explanation:

The -R parameter of the ls command prints a recursive listing of a directory's content, meaning that it will list not only the files and directories in the current directory, but also the files and directories in all the subdirectories12. For example, if you have a directory structure like this:

/home/user/ p— dirl | p— filel | [1]— file2 [L]— dir2 p— file3 [L]— file4

You can use the command ls -R /home/user/ to list all the files and directories recursively, and the output will look like this:

/home/user/: dir1 dir2
/home/user/dir1: file1 file2
/home/user/dir2: file3 file4

The -R parameter is also known as the --recursive option, which is the long form of the same parameter12. You can use either -R or --recursive to achieve the same result.

Reference:

Use ls Command Recursively - Linux Handbook
How to List Files Recursively in Linux command line

Question: 56

Most commands on Linux can display information on their usage. How can this information typically be displayed?

A. By running the command with the option /? or /??.
B. By running the command with the option ?! or ?=!.
C. By running the command with the option /doc or /documentation.
D. By running the command with the option -h or --help.
E. By running the command with the option -m or --manpage.

Answer: D

Explanation:

Most commands on Linux can display information on their usage by running the command with the option -h or --help. This option shows a brief summary of the command syntax, options, arguments, and examples. For example, running ls -h or ls --help will display the usage information for the ls command, which lists files and directories. The -h or --help option is a standard convention for most Linux commands, and it is useful for learning how to use a command or checking its available options. However, some commands may not support this option, or may use a different option to display usage information. In that case, you can use the man command to access the manual page for the command, which provides more detailed information on the command usage, description, options, arguments, examples, and references. For example, running man ls will display the manual page for the ls command. The man command is one of the applications

covered in the Linux Essentials certification program from the Linux Professional Institute (LPI). Reference:
Linux Essentials - Linux Professional Institute (LPI)
Linux Commands Cheat Sheet: Beginner to Advanced - GeeksforGeeks

Question: 57

Which of the following commands shows the absolute path to the current working directory?

A. who
B. cd ..
C. pwd
D. ls -l
E. cd ~/home

Answer: C

Explanation:
The command pwd stands for “print working directory”. It will print the absolute path of the current working directory to the terminal. For example, if we are currently in the /home/user/directory, it will print out that exact path1. The pwd command is useful for finding out where we are in the file system hierarchy and for verifying the location of files and directories2.
The other options are not commands that show the absolute path to the current working directory. The who command shows the users who are currently logged in to the system3. The cd .. command changes the current working directory to the parent directory of the current one2. The ls -l command lists the files and directories in the current working directory in a long format, which shows the permissions, ownership, size, date, and name of each file and directory2. The cd ~/home command changes the current working directory to the /home directory under the user’s home directory, which may or may not exist2. Reference:
Linux Essentials Exam Objectives, Version 1.6, Topic 103.1, Weight 2
Linux Essentials Certification Guide, Chapter 3, Page 51-52
How to Get the current directory in Linux - howtouselinux
How To Find The Absolute Path Of A File Or Directory In Linux - systranbox

Question: 58

Which of the following commands output the content of the file Texts 2.txt? (Choose two.)

A. cat 'Texts 2.txt’
B. cat -- Texts 2.txt
C. cat |Texts 2.txt|
D. cat 'Texts\ 2.txt’
E. cat Texts\ 2.txt

Answer: AE

Explanation:

The correct commands to output the content of the file Texts 2.txt are A and E. These commands use the cat command, which stands for concatenate, to display the content of one or more files. The cat command can take one or more filenames as arguments and print their content to the standard output (usually the terminal screen)12. The commands A and E use different ways to deal with the space character in the filename. The space character is a special character in Linux that separates words and commands. To prevent the shell from interpreting the space as a word separator, the commands A and E use either of the following methods34:

Option A uses single quotes (') around the filename to preserve the literal value of the space character. This tells the shell to treat the filename as a single argument and pass it to the cat command. For example: cat 'Texts 2.txt'

Option E uses a backslash () before the space character to escape its special meaning. This tells the shell to ignore the space as a word separator and treat it as part of the filename. For example: cat Texts\ 2.txt

The other options are incorrect because they use different syntax that do not output the content of the file. For example:

Option B uses a double dash (–) before the filename to indicate the end of options. This is usually used to prevent the shell from interpreting a filename that starts with a dash (-) as an option. However, in this case, the filename does not start with a dash, so the double dash is unnecessary and will cause the command to fail. For example: cat – Texts 2.txt

Option C uses vertical bars (|) around the filename to indicate a pipe. A pipe is a way of connecting the output of one command to the input of another command. However, in this case, there is no command before or after the pipe, so the pipe is meaningless and will cause the command to fail. For example: cat |Texts 2.txt|

Option D uses single quotes (') and a backslash () together around the filename. This is redundant and will cause the command to fail. The single quotes already preserve the literal value of the space character, so the backslash is not needed. Moreover, the backslash inside the single quotes will be treated as part of the filename, not as an escape character. For example: cat 'Texts\ 2.txt' Reference: 1: How to Use Linux Cat Command (With Examples) - phoenixNAP 2: Cat command in Linux with examples - GeeksforGeeks 3: How to escape spaces in path during scp copy in Linux? - Stack Overflow 4: How to handle spaces in file names when using xargs on find results? - Ask Ubuntu

Question: 59

Which command displays file names only and no additional information?

A. ls -a
B. ls -lh
C. ls -l
D. ls -alh
E. ls -nl

Answer: A

Explanation:

: The ls command is used to list the files and directories in a given path. By default, the ls

command displays only the file names, without any additional information. However, the ls command can also take various options to modify its output. For example, the -l option tells ls to display the long format, which includes the file permissions, owner, group, size, date, and name. The -h option tells ls to display the file sizes in a human-readable format, such as KB, MB, GB, etc. The -a option tells ls to display all files, including the hidden ones that start with a dot (.). The -n option tells ls to display the numeric user ID and group ID instead of the user name and group name. Therefore, the only option that does not add any additional information to the file names is the -a option. The command ls -a will display all the file names in the current directory, including the hidden ones, but nothing else. Reference:

Linux Essentials - Linux Professional Institute (LPI), section 2.1.1

2.1 Lesson 1 - Linux Professional Institute Certification Programs, slide 6.

Question: 60

What is the purpose of the PATH environment variable?

A. It allows the execution of commands without the need to know the location of the executable.
B. It increases security by preventing commands from running in certain locations.
C. It specifies the location of a user's home directory.
D. It indicates the location of the default shell to be used when a user logs in.
E. It contains the absolute path to the current directory.

Answer: A

Explanation:

The PATH environment variable is a special variable that contains a list of directories that the system searches when looking for a command to execute12. The purpose of the PATH variable is to make it easier and faster for users to run commands without having to type the full path to the executable file. For example, if you want to run the ls command, which is located in the /bin directory, you don't have to type /bin/ls every time. You can just type ls, and the system will find the executable file in the /bin directory, which is one of the directories in the PATH variable. The PATH variable can be viewed with the echo command12:

$ echo $PATH

The PATH variable can also be modified by adding or removing directories, either temporarily or permanently, depending on the user's needs12. For example, if you have a custom script or program in your home directory, and you want to run it from anywhere, you can add your home directory to the PATH variable with the export command12:

$ export PATH=$PATH:~/myprogram

This will append your home directory to the end of the PATH variable, and the system will search it last when looking for a command. To make this change permanent, you need to edit a configuration file, such as ~/.bashrc or ~/.profile, and add the export command there12.

Reference:

How To View and Update the Linux PATH Environment Variable | DigitalOcean Linux path environment variable - Linux command line - LinuxConfig.org

Question: 61

Which of the following commands sets the variable USERNAME to the value bob?

A. set USERNAME bob
B. $USERNAME==bob
C. var USERNAME=bob D. USERNAME<=bob
E. USERNAME=bob

Answer: E

Explanation:
The correct command to set the variable USERNAME to the value bob is USERNAME=bob. This command assigns the string bob to the variable name USERNAME, using the equal sign (=) as the assignment operator. There is no space around the equal sign, and the variable name and value are

case-sensitive. This command sets a shell variable, which is only valid in the current shell session. To make the variable an environment variable, which can be inherited by child processes and subshells, you need to use the export command, such as export USERNAME=bob. The other commands are not valid for setting variables in Linux. The set command is used to set or unset shell options and positional parameters, not variables. The $ sign is used to reference the value of a variable, not to assign it. The == sign is used for comparison, not assignment. The var keyword is not used in Linux, but in some other programming languages. The <= sign is used for redirection, not assignment. Reference:
Linux Essentials - Linux Professional Institute (LPI)
How to Set and List Environment Variables in Linux | Linuxize

Question: 62

What command displays manual pages? (Specify ONLY the command without any path or parameters.)

Answer: man

Explanation:

The command that displays manual pages for Linux commands is the man command. The man command is used to display the manual pages for a given command or topic. For example, to view the manual page for the ls command, you can type: man ls
This will open the manual page for the ls command in a pager, which allows you to scroll and search through the text. You can also specify the section number of the manual page if there are multiple pages with the same name. For example, to view the manual page for the passwd command in section 1, you can type: man 1 passwd
The man command is one of the most useful and important commands for learning and using Linux. It provides detailed information about the syntax, options, arguments, examples, and other aspects of a command or topic. You can also use the --help option to get a brief summary of the usage and options of a command. For example, to get a quick help for the man command, you can type: man --help
To learn more about the man command and how to use it effectively, you can refer to the following

resources:

Linux Essentials Exam Objectives, Version 1.6, Topic 103.1, Weight 2

Linux Essentials Certification Guide, Chapter 3, Page 51-52

How to Access Manual Pages for Linux Commands - Linux Tutorials - Learn Linux Configuration

How to Easily Read a Linux Man Page - Make Tech Easier

Question: 63

Which command copies the contents of the directory /etc/, including all sub-directories, to /root/?

A. copy /etc /root
B. cp -r /etc/* /root
C. cp -v /etc/* /root
D. rcp /etc/* /root
E. cp -R /etc/*.* /root

Answer: B

Explanation:

The correct command to copy the contents of the directory /etc/, including all sub-directories, to /root/ is cp -r /etc/* /root. This command uses the cp command, which stands for copy, and is used to copy files and directories on Linux and Unix systems. The command also uses the following options and arguments123:

The -r option, which stands for recursive, and tells cp to copy all files and sub-directories of the source directory. Alternatively, the -R option can be used, which has the same effect as -r.

The /etc/* argument, which specifies the source directory and all its contents. The asterisk (*) is a wildcard character that matches any file or directory name. This argument tells cp to copy everything inside the /etc/ directory, but not the directory itself.

The /root argument, which specifies the destination directory. This argument tells cp to copy the source files and sub-directories to the /root/ directory.

The other options are incorrect because they use different commands or syntax that do not copy the contents of the directory /etc/, including all sub-directories, to /root/. For example:

Option A uses the copy command, which is not a valid Linux command. The correct command is cp. Option C uses the -v option, which stands for verbose, and tells cp to print verbose output. This option does not affect the copying process, but only the output. It also does not include the -r or -R option, which is necessary to copy the sub-directories.

Option D uses the rcp command, which stands for remote copy, and is used to copy files between different hosts on a network. This command is not relevant for copying files on the same host. Option E uses the -R option, which is correct, but also uses the . argument, which is incorrect. The dot (.) is a special character that matches any single character. This argument tells cp to copy only the files and directories that have a dot in their name, which may exclude some files and directories that do not have a dot.

Reference: 1: Cp Command in Linux (Copy Files) | Linuxize 2: cp command in Linux with examples - GeeksforGeeks 3: How to Copy Files and Directories in the Linux Terminal

Question: 64

Which of the following commands puts the lines of the file data.csv into alphabetical order?

A. a..z data.csv
B. sort data.csv
C. abc data.csv
D. wc -s data.csv
E. grep --sort data.csv

Answer: B

Explanation:
The sort command is used to sort the lines of a file or a stream of input according to a specified criterion, such as alphabetical order, numerical order, reverse order, etc. By default, the sort command sorts the lines in ascending alphabetical order, using the first character of each line as the key. For example, the command sort data.csv will sort the lines of the file data.csv in alphabetical order and display the output on the screen. If you want to save the sorted output to a new file, you can use the redirection operator (>) to specify the output file name. For example, the command sort data.csv > sorted_data.csv will sort the lines of the file data.csv in alphabetical order and save the output to a new file named sorted_data.csv. The other commands are either invalid or do not perform the sorting operation. The a...z command does not exist, the abc command is a text editor, the wc command counts the number of words, lines, and bytes in a file, and the grep command searches for a pattern in a file or a stream of input. Therefore, the correct answer is B. Reference: Linux Essentials - Linux Professional Institute (LPI), section 2.3.2
LPI Linux Essentials Study Guide: Exam 010 v1.6, 3rd Edition, chapter 4, page 95.

Question: 65

Which of the following examples shows the general structure of a for loop in a shell script?

A. for *.txt as file => echo $file
B. for *.txt (echo $i)
C. for file in *.txt do
echo $i done
D. for ls *.txt exec {} \;
E. foreach @{file} { echo $i
}

Answer: C

Explanation:
The general structure of a for loop in a shell script is as follows12: for variable in list do commands done
The variable is the name of a loop counter or iterator that takes on the values of the items in the list. The list can be a sequence of words, numbers, filenames, or the output of a command. The commands are the body of the loop that are executed for each value of the variable. The do and done keywords mark the beginning and the end of the loop body.

The option C. for file in *.txt do echo $i done follows this structure, with the variable being file, the list being *.txt (which matches all the files with the .txt extension in the current directory), and the command being echo $i (which prints the value of the variable i, which is presumably set somewhere else in the script).

The other options are incorrect because:

A . for *.txt as file => echo $file uses an invalid syntax for a for loop. The as keyword is not part of the shell script syntax, and the => symbol is not a valid operator. The correct way to write this loop would be:

for file in *.txt do echo $file done

B . for *.txt (echo $i) uses an invalid syntax for a for loop. The parentheses are not part of the shell script syntax, and the loop body is missing the do and done keywords. The correct way to write this loop would be:

for i in *.txt do echo $i done

D . for ls *.txt exec {} ; uses an invalid syntax for a for loop. The ls command is not a valid variable name, and the exec {} ; is not a valid command. This looks like a mix of a for loop and a find command. The correct way to write this loop would be: for file in *.txt do exec $file done

E . foreach @{file} { echo $i } uses an invalid syntax for a for loop. The foreach keyword is not part of the shell script syntax, and the @{file} and { echo $i } are not valid expressions. This looks like a mix of a for loop and a Perl syntax. The correct way to write this loop would be: for file in * do echo $file done

Reference:

Looping Statements | Shell Script - GeeksforGeeks

How do I write a 'for' loop in Bash? - Stack Overflow

Question: 66

Which operator in a regular expression matches the preceding character either zero or one time?

A. ?
B. *
C. +
D. %
E. $

Answer: A

Explanation:

The operator that matches the preceding character either zero or one time in a regular expression is the question mark (?). This operator is also known as the optional quantifier, because it makes the preceding character or group of characters optional. For example, the regular expression colou?r matches both color and colour, because the u is optional. The question mark can also be used to modify other quantifiers, such as * (zero or more), + (one or more), or {m,n} (between m and n times), to make them non-greedy, meaning they will match the shortest possible string instead of the longest. For example, the regular expression .*? matches any character zero or more times, but as few as possible. The question mark is one of the basic regular expression operators covered in the Linux Essentials certification program from the Linux Professional Institute (LPI). Reference: Linux Essentials - Linux Professional Institute (LPI)

Regular Expressions:Difference between 'optional occurrence' and 'zero ...

Question: 67

The file script.sh in the current directory contains the following content:

#!/bin/bash echo $MYVAR

The following commands are used to execute this script:

MYVAR=value
./script.sh

The result is an empty line instead of the content of the variable MYVAR. How should MYVAR be set in order to make script.sh display the content of MYVAR?

A. !MYVAR=value
B. env MYVAR=value
C. MYVAR=value
D. $MYVAR=value
E. export MYVAR=value

Answer: E

Explanation:

The reason why the script.sh does not display the content of the variable MYVAR is that the variable is not exported to the environment of the script. When a script is executed, it runs in a separate process that inherits the environment variables from the parent process, but not the shell variables. A shell variable is a variable that is defined and visible only in the current shell session, while an environment variable is a variable that is exported to the environment and visible to all processes that run in that environment1.

To make a shell variable an environment variable, we need to use the export command. The export command takes a shell variable name and adds it to the environment of the current shell and any subshells or processes that are created from it2. For example, to export the variable MYVAR with the value value, we can use:

export MYVAR=value

This will make the variable MYVAR available to the script.sh when it is executed, and the script will print the value of MYVAR as expected. Alternatively, we can also use the export command with the -n option to remove a variable from the environment, or with the -p option to list all the environment variables2.

The other options are not valid ways to set MYVAR as an environment variable. The !MYVAR=value option is not a valid syntax for setting a variable in bash. The env MYVAR=value option will run the env command with the MYVAR=value argument, which will print the environment variables with the addition of MYVAR=value, but it will not affect the current shell or the script.sh3. The MYVAR=value option will set MYVAR as a shell variable, but not as an environment variable, so it will not be visible to the script.sh1. The $MYVAR=value option will try to set the variable whose name is the value of MYVAR to the value value, which is not what we want4. Reference: Linux Essentials Exam Objectives, Version 1.6, Topic 103.1, Weight 2 Linux Essentials Certification Guide, Chapter 3, Page 51-52 env(1) - Linux manual page

Bash Variables - LinuxConfig.org

Question: 68

What is the return value of a shell script after successful execution?

A. 1
B. 0
C. -1
D. -255
E. 255

Answer: B

Explanation:
The return value of a shell script after successful execution is 0. This is a convention followed by most UNIX and Linux commands, programs, and utilities. A return value of 0 indicates that the command or script completed successfully, without any errors. A return value of non-zero (1-255) indicates that the command or script failed, and the value can be interpreted as an error code. The return value of a command or script is stored in the special variable $? and can be used to test the outcome of a command or script123. For example, the following script will print a message based on the return value of the ls command: #!/bin/bash ls if [$? -eq 0]; then echo “ls command executed successfully” else echo “ls command failed” fi Reference: 1: Exit and Exit Status - Linux Documentation Project 2: Linux Passwd Command Help and Examples 3: bash - Which is the best way to check return result? - Unix & Linux Stack Exchange

Question: 69

Which of the following commands creates the ZIP archive poems.zip containing all files in the current directory whose names end in .txt?

A. zip *.txt > poems.zip
B. zcat *.txt poems.zip
C. zip poems.zip *.txt
D. zip cfz poems.zip *.txt
E. cat *.txt | zip poems.zip

Answer: C

Explanation:
The zip command is used to create compressed archive files that can contain one or more files or directories. The zip command takes the name of the archive file as the first argument, followed by

the names of the files or directories to be included in the archive. You can also use wildcards to match multiple files or directories with a common pattern. For example, the command zip poems.zip *.txt will create the ZIP archive poems.zip containing all files in the current directory whose names end in .txt. The other commands are either invalid or do not perform the desired operation. The command zip *.txt > poems.zip will try to create an

archive for each file ending in .txt and redirect the output to poems.zip, which is not a valid archive file. The command zcat *.txt poems.zip will try to decompress and concatenate the contents of the files ending in .txt and poems.zip, which is not a valid ZIP file. The command zip cfz poems.zip *.txt will fail because the options c, f, and z are not valid for the zip command. The command cat *.txt | zip poems.zip will try to read the contents of the files ending in .txt from the standard input and create an archive named poems.zip, but this will not preserve the file names or attributes of the original files. Reference: Linux Essentials - Linux Professional Institute (LPI), section 3.1.1
3.1 Archiving Files on the Command Line - Linux Professional Institute Certification Programs, slide

Question: 70

Which of the following statements are true regarding a typical shell script? (Choose two.)

A. It has the executable permission bit set.
B. It starts with the two character sequence #!.
C. It is located in /usr/local/scripts/.
D. It is located in /etc/bash/scripts/.
E. It is compiled into a binary file compatible with the current machine architecture.

Answer: AB

Explanation:
A typical shell script is a text file that contains a series of commands or instructions that can be executed by a shell interpreter. A shell script usually has the executable permission bit set, which means that it can be run as a program by the user or another program. A shell script also starts with the two character sequence #!, which is called a shebang or a hashbang. This sequence tells the operating system which shell interpreter to use to run the script. For example, #!/bin/bash indicates that the script should be run by the bash shell.
Reference:
Linux Essentials - Linux Professional Institute (LPI) 1
Linux Essentials - Linux Professional Institute Certification Programs 2

Question: 71

Which of the following commands extracts the contents of the compressed archive file1.tar.gz?

A. tar -czf file1.tar.gz
B. ztar file1.tar.gz
C. tar -xzf file1.tar.gz
D. tar --extract file1.tar.gz
E. detar file1.tar.gz

Answer: C

Explanation:

The correct command to extract the contents of the compressed archive file1.tar.gz is tar -xzf file1.tar.gz. This command uses the following options:

- x means extract files from an archive.
- z means filter the archive through gzip, which is a compression program that reduces the size of files.
- f means use the following archive file name, which is file1.tar.gz in this case.

The other commands are incorrect for the following reasons:

tar -czf file1.tar.gz creates a compressed archive file1.tar.gz from the files specified after the command, not extract it.

ztar file1.tar.gz is not a valid command, as ztar is not a standard program or option for tar.

tar --extract file1.tar.gz is missing the -z option to handle the gzip compression, and also the -f option to specify the file name.

detar file1.tar.gz is not a valid command, as detar is not a standard program or option for tar.

Reference:

Linux Essentials - Topic 106: The Linux Operating System, section 106.2 Use single shell commands and one line command sequences to perform basic tasks on the command line.

LPI Linux Essentials Study Guide: Exam 010 v1.6, 3rd Edition, Chapter 5: Working with Files and Directories, section Compressing and Archiving Files.

Question: 72

Which of the following commands finds all lines in the file operating-systems.txt which contain the term linux, regardless of the case?

A. igrep linux operating-systems.txt
B. less -i linux operating-systems.txt
C. grep -i linux operating-systems.txt
D. cut linux operating-systems.txt
E. cut [Ll] [Ii] [Nn] [Uu] [Xx] operating-systems.txt

Answer: C

Explanation:

The grep command is used to search for a pattern in a file or input. The -i option makes the search case-insensitive, meaning that it will match both uppercase and lowercase letters. The grep command takes the pattern as the first argument and the file name as the second argument.

Therefore, the command grep -i linux operating-systems.txt will find all lines in the file operating- systems.txt which contain the term linux, regardless of the case. Reference: Linux Essentials - Topic 103: Finding Linux Documentation and Linux Essentials - Topic 104: Command Line Basics

Question: 73

Which one of the following statements concerning Linux passwords is true?

A. All passwords can be decrypted using the system administrator's master password.
B. Passwords may never start with a non-letter.
C. Users cannot change their password once it has been set.
D. Passwords are only stored in hashed form.
E. Passwords may be at most six characters long.

Answer: D

Explanation:
Linux passwords are not stored in plain text, but in a scrambled or encrypted form known as a hash. A hash is a one-way function that transforms a string of characters into a fixed-length value. The same input always produces the same hash, but it is impossible to reverse the process and recover the original input from the hash. This way, the system can verify the user's password without exposing it to anyone who can read the file where the hashes are stored. The file that contains the password hashes is /etc/shadow, which is only readable by the root user or members of the shadow group. The passwd utility is used to change the user's password, which updates the hash in the /etc/shadow file. Reference: Linux Essentials 1.6 Topic 105: Security and File Permissions, How to Change Account Passwords on Linux, Where is my password stored on Linux?

Question: 74

Which of the following programs are web servers? (Choose two.)

A. Apache HTTPD
B. Postfix
C. Curl
D. Dovecot
E. NGINX

Answer: AE

Explanation:
A web server is a program that listens for requests from web browsers and serves web pages, images, or other resources. Apache HTTPD and NGINX are two popular web servers that can run on Linux systems. They can handle multiple protocols, such as HTTP, HTTPS, FTP, and SMTP. Postfix, Curl,

and Dovecot are not web servers, but they are related to web or network services. Postfix is a mail transfer agent (MTA) that can send and receive emails. Curl is a command-line tool that can transfer data from or to a web server. Dovecot is a mail delivery agent (MDA) that can store and retrieve emails from a local mailbox.

Reference:
Linux Essentials - Linux Professional Institute (LPI), section 1.2 Major Open Source Applications
LPI Linux Essentials 010-160 - Testprep Training Tutorials, section 4.4 Your Computer on the Network

Question: 75

Which of the following Linux Distributions is derived from Red Hat Enterprise Linux?

A. Raspbian
B. openSUSE
C. Debian
D. Ubuntu
E. CentOS

Answer: E

Explanation:
CentOS is a Linux distribution that is derived from Red Hat Enterprise Linux (RHEL). CentOS stands for Community Enterprise Operating System and it aims to provide a free, enterprise-class, community-supported computing platform that is functionally compatible with RHEL. CentOS is one of the most popular Linux distributions for servers and cloud computing. Raspbian, openSUSE, Debian and Ubuntu are other Linux distributions that are not derived from RHEL, but have their own origins and development histories. Raspbian is based on Debian and optimized for the Raspberry Pi. openSUSE is a community project sponsored by SUSE Linux and other companies. Debian is one of the oldest and most influential Linux distributions, and Ubuntu is derived from Debian and sponsored by Canonical Ltd. Reference:
Linux Essentials - Linux Professional Institute (LPI) 1
Linux Essentials Version 1.6 Update - Linux Professional Institute (LPI) 2
Free LPI 010-160 Questions - Pass LPI 010-160 - Pass4Success 3
LPI Linux Essentials Study Guide: Exam 010 v1.6, 3rd Edition 4

Question: 76

Which of the following statements is true about Free Software?

A. It is developed by volunteers only.
B. It may be modified by anyone using it.
C. It must always be available free of charge.
D. It only runs on Linux.
E. It is only distributed as a compiled binary.

Answer: B

Explanation:
The correct statement about Free Software is that it may be modified by anyone using it. This is one of the four essential freedoms of Free Software, which are: the freedom to run the program as you wish, for any purpose; the freedom to study how the program works, and change it so it does your computing as you wish; the freedom to redistribute copies so you can help your neighbor; and the freedom to distribute copies of your modified versions to others1. Access to the source code is a precondition for these freedoms1.
The other statements are false for the following reasons:
Free Software is not developed by volunteers only. It can be developed by anyone, including individuals,

companies, organizations, or communities. Some Free Software developers are paid for their work, while others do it as a hobby or for social benefit1.
Free Software does not have to be available free of charge. It can be sold or given away for any price. The term "free" refers to the users' freedom, not the price of the software1. However, Free Software users have the freedom to redistribute copies, so they can obtain the software at no charge from someone who has a copy1.
Free Software does not only run on Linux. It can run on any operating system that supports it, such as Windows, MacOS, BSD, or Android. Linux is an example of a Free Software operating system, but not the only one1.
Free Software is not only distributed as a compiled binary. It can also be distributed as source code, or both. In fact, Free Software must provide access to the source code, otherwise the users cannot study or modify the software1.
Reference:
What is Free Software? - GNU Project - Free Software Foundation

Question: 77

How is a new Linux computing instance provisioned in an IaaS cloud?

A. The standard Linux installer has to be run through a remote console.
B. After buying a Linux distribution, its vendor delivers it to a cloud instance.
C. The installation has to be prepared in a local virtual machine which is then copied to the cloud.
D. The cloud hosting organization provides a set of pre-prepared images of popular Linux distributions.
E. A provider-specific configuration file describing the desired installation is uploaded to the cloud provider.

Answer: D

Explanation:
In an Infrastructure as a Service (IaaS) cloud, the provider offers virtualized computing resources such as servers, storage, and network over the internet. The user can provision and manage these resources according to their needs. One of the common ways to provision a new Linux computing
instance in an IaaS cloud is to use a pre-prepared image of a Linux distribution provided by the cloud hosting organization. An image is a snapshot of a virtual machine that contains the operating system and other software components. The user can choose from a variety of images that suit their requirements and launch a new instance from the image. This way, the user does not have to install and configure the Linux operating system from scratch, which saves time and effort. Some examples of cloud hosting organizations that provide pre-prepared images of popular Linux distributions are Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), and
DigitalOcean. Reference: Linux Essentials - Topic 108: Cloud Computing and Linux Essentials - Topic 108: Cloud Computing - Exam Objectives

Question: 78

What are the differences between a private web browser window and a regular web browser window? (Choose three.)

A. Private web browser windows do not allow printing or storing websites.
B. Private web browser windows do not store cookies persistently.
C. Private web browser windows do not support logins into websites.
D. Private web browser windows do not keep records in the browser history.
E. Private web browser windows do not send regular stored cookies.

Answer: BDE

Explanation:
A private web browser window is a mode of browsing that prevents the browser from saving your browsing history, cookies, and other site data, or information entered in forms. However, it does not prevent websites, your employer or school, or your internet service provider from tracking your online activity. The main differences between a private web browser window and a regular web browser window are:
Private web browser windows do not store cookies persistently. Cookies are small files that websites use to store information on your device, such as your preferences, login status, or tracking data. In a regular web browser window, cookies are stored until they expire or you delete them. In a private web browser window, cookies are deleted when you close all private windows.
Private web browser windows do not keep records in the browser history. The browser history is a list of web pages that you have visited in the past. In a regular web browser window, the browser history is saved and can be accessed by anyone who uses the same device or profile. In a private web browser window, the browser history is not saved and cannot be viewed by anyone.
Private web browser windows do not send regular stored cookies. When you visit a website in a regular web browser window, the browser sends any cookies that are stored for that website. This allows the website to recognize you and provide personalized content or services. When you visit a website in a private web browser window, the browser does not send any cookies that are stored in regular windows. This prevents the website from identifying you or linking your activity across different sessions.
Reference: Browse in private - Computer - Google Chrome Help, Browse InPrivate in Microsoft Edge - Microsoft Support, Private Browsing: What Is It and How to Use It | Edge Learning Center

Question: 79

What is the preferred source for the installation of new applications in a Linux based operating system?

A. The vendor's version management system
B. A CD-ROM disk
C. The distribution's package repository
D. The vendor's website
E. A retail store

Answer: C

Explanation:
The distribution's package repository is the preferred source for the installation of new applications in a Linux based operating system. A package repository is a collection of software packages that are maintained by the distribution and can be easily installed, updated, or removed using a package manager. Package repositories offer several advantages, such as:

They ensure compatibility and stability with the system and other packages.

They provide security updates and bug fixes for the packages.

They reduce the risk of malware or corrupted files.

They simplify the dependency management and configuration of the packages.

The other sources are not preferred because they may not offer these benefits and may cause problems with the system. The vendor's version management system, the vendor's website, or a CD- ROM disk may contain packages that are not compatible with the distribution or may conflict with other packages. A retail store may not have the latest or the most suitable packages for the system. Reference:

Linux Essentials - Linux Professional Institute (LPI), section 1.3 Installing, Updating and Removing Software Packages

LPI Linux Essentials Study Guide: Exam 010 v1.6, 3rd Edition, chapter 4 Working on the Command Line, section 4.2 Managing Software

Table of Contents - Linux Professional Institute Certification Programs, section 1.3 Installing, Updating and Removing Software Packages

Question: 80

Which of the following tar options handle compression? (Choose two correct answers.)

A. -bz
B. -z
C. -g
D. -J
E. -z2

Answer: BD

Explanation:

Question: 81

Which of the following keys can be pressed to exit less?

A. 1
B. x
C. e
D. q
E. !

Answer: D

Explanation: