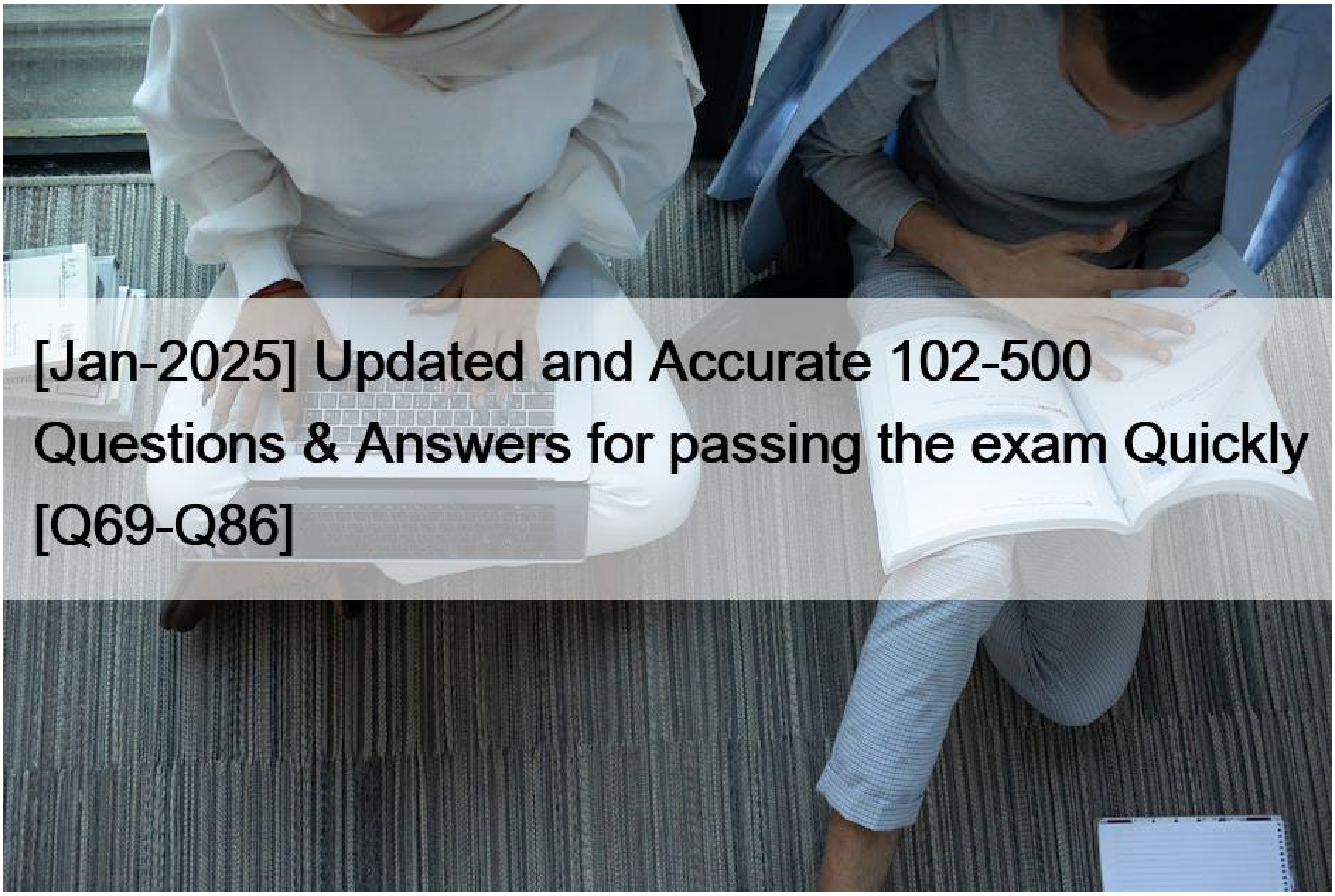
[Jan-2025 Updated and Accurate 102-500 Questions & Answers for passing the exam Quickly [Q69-Q86


[Jan-2025] Updated and Accurate 102-500
Questions & Answers for passing the exam Quickly
[Q69-Q86]

[Jan-2025] Updated and Accurate 102-500 Questions & Answers for passing the exam Quickly
Download Real 102-500 Exam Dumps for candidates. 100% Free Dump Files

QUESTION 69

What is a purpose of an SSH host key?
* It must be sent by any SSH client in addition to a user key in order to identify the client&#8217;s host.
* It provides the server&#8217;s identity information to connecting SSH clients.
* It is the root key by which all user SSH keys must be signed.
* It authenticates any user that logs into a remote machine from the key&#8217;s host.
* It is used by system services like cron, syslog or a backup job to automatically connect to remote hosts.

An SSH host key is a cryptographic key used for authenticating computers in the SSH protocol. Host keys are key pairs, typically using the RSA, DSA, or ECDSA algorithms. Public host keys are stored on and/or distributed to SSH clients, and private keys are stored on SSH servers. Each host (i.e., computer) should have a unique host key. Host keys are used for authentication towards the connecting client, analogous to user SSH keys. Host keys are generated using asymmetric encryption algorithms like RSA, DSA, or ECDSA algorithms12. When a client connects to the host, the host sends its public host key to the client, and the client verifies that the host key matches the one stored in its known hosts file. If the host key is unknown or has changed, the client will display a warning and prompt the user to accept or reject the host key. This is to prevent man-in-the-middle attacks, where an attacker intercepts the connection and pretends to be the legitimate host. The other options are either incorrect or irrelevant to the purpose of an SSH host key. Reference:

What is an SSH Host Key & How are They Configured?, What are SSH Host Keys? section SSH Host Key Management Demystified, What are SSH host keys? section What is SSH host key &#8211; omnisecu.com, first paragraph

QUESTION 70

Which of the following words is used to restrict the records that are returned from a SELECT query based on a supplied criteria for the values in the records?
* LIMIT
* FROM
* WHERE
* IF
The correct keyword for restricting the records that are returned from a SELECT query based on a supplied criteria for the values in the records is WHERE. The WHERE clause is used to filter records based on one or more conditions. The syntax of the WHERE clause is:

SELECT column1, column2, &#8230; FROM table_name WHERE condition;

The condition can be a logical expression that evaluates to true, false, or unknown. The condition can also use comparison operators, logical operators, and wildcards to specify the criteria. For example, the following query selects all the records from the employees table where the salary is greater than 50000:

SELECT * FROM employees WHERE salary > 50000;

The other options are incorrect because they have different purposes in SQL:

LIMIT is used to specify the maximum number of records to return from a query. For example, the following query returns only the first 10 records from the employees table:

SELECT * FROM employees LIMIT 10;

FROM is used to specify the table or tables from which to retrieve data. For example, the following query selects all the columns from the employees table:

SELECT * FROM employees;

IF is used to execute a block of code conditionally. For example, the following query updates the salary of an employee based on their performance:

UPDATE employees SET salary = IF(performance = &#8216;excellent&#8217;, salary * 1.1, salary) WHERE employee_id = 123;
Reference:

https://bing.com/search?q=SQL+statements+restrict+records+based+on+criteria

https://stackoverflow.com/questions/11611931/sql-query-to-select-records-based-on-criteria

QUESTION 71

Which of the following SQL statements will select the fields name and address from the contacts table?
* SELECT (name, address) FROM contacts;
* SELECT (name address) FROM contacts;
* SELECT name, address FROM contacts;
* SELECT name address FROM contacts;
The correct syntax for selecting specific columns from a table in SQL is to use the SELECT keyword followed by a comma-separated list of column names and then the FROM keyword followed by the table name. Therefore, the only option that follows this syntax is C. SELECT name, address FROM contacts; The other options are incorrect because they either use parentheses around the column names, which are not needed, or they omit the comma between the column names, which causes a syntax error. Reference: https://www.sqltutorial.org/sql-select/

https://www.w3schools.com/mysql/mysql_select.asp

QUESTION 72

Why is the xhost program considered dangerous to use?
* It makes it difficult to uniquely identify a computer on the network.
* It allows easy access to your X server by other users.
* It logs sensitive information to syslog.
* It makes your computer share network resources without any authentication.
* It is a graphical DNS tool with known exploits.
The xhost program is used to add and delete host names or user names to the list allowed to make connections to the X server1. In the case of hosts, this provides a rudimentary form of privacy control and security. It is only sufficient for a workstation (single user) environment, although it does limit the worst abuses1. However, if xhost is used togrant access to everyone, even if they aren&#8217;t on the list (i.e., access control is turned off), then any user on the network can connect to your X server and monitor your keystrokes, capture your screen, or run malicious programs2. This is why xhost is considered dangerous to use and should be avoided in favor of more secure methods, such as xauth or ssh23. References:

* xhost linux command man page &#8211; commandlinux.com

* Linux Xhost Command Help and Examples &#8211; Computer Hope

* xhost(1) &#8211; Arch manual pages

QUESTION 73

Which configuration file would be edited to change default options for the OpenSSH server?
* /etc/ssh/sshd_config
* /etc/ssh/ssh
* /etc/ssh/server
* /etc/ssh/ssh_config
* /etc/ssh/ssh_server
The configuration file for the OpenSSH server is called sshd_config. It is typically located in /etc/ssh on most

*NIX systems, but is /etc/sshd_config in the case of MacOS X and perhaps other systems. OpenSSH has two different sets of configuration files: one for client programs (ssh, scp, and sftp) and one for the server daemon (sshd). System-wide SSH configuration information is stored in the /etc/ssh/ directory1. References: 1: Where is the configuration file for OpenSSH server?

QUESTION 74

Identify the statement that would create a default route using a gateway of 192.168.1.1.

* netstat -add default gw 192.168.1.1
* route add default gw 192.168.1.1
* ip route default 192.168.1.1
* route default gw 192.168.1.1
* ifconfig default gw 192.168.1.1 eth0

QUESTION 75

Of the ways listed, which is the best method to temporarily suspend a user&#8217;s ability to interactively login?

* Use passwd -d username to give the user an empty password.
* Use chage to expire the user account.
* Change the user&#8217;s password.
* Add the command exit to the user&#8217;s .login file.

The chage command can be used to change the expiration date of a user account. By setting the expiration date to a past date, the user account will be disabled and the user will not be able to login interactively. This is a temporary method, as the expiration date can be changed back to a future date or removed to re-enable the user account. The other options are either permanent, insecure, or ineffective. Option A is insecure, as it allows anyone to login as the user without a password. Option C is permanent, as it changes the user&#8217;s password without saving the original one. Option D is ineffective, as it only affects the user&#8217;s .login file, which is used by the csh and tcsh shells, and not by other shells such as bash or zsh. Therefore, option B is the best method to temporarily suspend a user&#8217;s ability to interactively login.
References:https://linuxconfig.org/disabling-user-logins-to-linux-system

https://askubuntu.com/questions/282806/how-to-enable-or-disable-a-user

QUESTION 76

Which of the following commands shows all active systemd timers?

* systemctl-timer show
* timectl list
* systemctl -t
* systemctl list-timers
* timeq

The command systemctl list-timers shows all active systemd timers, which are units that can be used to schedule the execution of other units at specific times or after certain intervals. The output of the command includes the following columns:

* NEXT: The next time the timer will trigger.

* LEFT: The time left until the next trigger.

* LAST: The last time the timer triggered.

* PASSED: The time passed since the last trigger.

* UNIT: The name of the timer unit.

* ACTIVATES: The name of the unit that is activated by the timer.

For example, the following output shows two active timers: apt-daily.timer and apt-daily-upgrade.timer, which are used to perform automatic updates on Debian-based systems.

NEXT LEFT LAST PASSED UNIT ACTIVATES Mon 2021-11-15 06:00:00 UTC 9h left Sun 2021-11-14

06:00:01 UTC 20h ago apt-daily.timer apt-daily.service Mon 2021-11-15 06:23:51 UTC 9h left Sun

2021-11-14 06:23:51 UTC 20h ago apt-daily-upgrade.timer apt-daily-upgrade.service 2 timers listed.

The other commands in the options are either invalid or unrelated to systemd timers:

* systemctl-timer show is not a valid command. To show the details of a specific timer unit, the command systemctl show unit.timer can be used, where unit is the name of the unit that is activated by the timer.

* timectl list is not a valid command. To list the available time zones, the command timedatectl

* list-timezones can be used. To list the current time and date settings, the command timedatectl can be used without any arguments.

* systemctl -t is not a complete command. To list all units of a specific type, the command systemctl -t type can be used, where type is the name of the unit type, such as service, timer, socket, etc.

* timeq is not a valid command. It may be confused with the time command, which measures the time taken by a command or program to execute.

References:

* LPIC-1 Exam 102 Objectives, Topic 107: Administrative Tasks, Subtopic 107.2: Automate system administration tasks by scheduling jobs, Weight: 4, Key Knowledge Areas: Use cron and systemd timers to run jobs at regular intervals and to use anacron to manage system cron jobs.Objective: Use systemd timers to run jobs at regular intervals and to use anacron to manage system cron jobs.

* LPIC-1 Exam 102 Learning Materials, Topic 107: Administrative Tasks, Subtopic 107.2: Automate system administration tasks by scheduling jobs, Section 107.2.3: systemd timers, Page 21-22.

QUESTION 77

What output is produced by the following command sequence?

echo `1 2 3 4 5 6&#8242; | while read a b c; do

echo result $c $b $a;

done

* result: 6 5 4
* result: 1 2 3 4 5 6
* result: 3 4 5 6 2 1
* result: 6 5 4 3 2 1
* result: 3 2 1

QUESTION 78

In order to bypass print filters using lpr, which of following switches should be used:
* lpr -o nofilter
* lpr -l
* lpr -o raw
* lpr -r

QUESTION 79

Which of the following states can NetworkManager show regarding the system&#8217;s network connectivity?

(Choose two.)
* up
* portal
* full
* login-required
* firewalled

QUESTION 80

What can be specified with useradd? (Choose two.)
* Commands the user can run using sudo.
* The absolute path to the user&#8217;s home directory.
* Which printers are available for the new user.
* The SSH keys used to login to the new account.
* The numeric user ID (UID) of the user.

The useradd command is used to create new user accounts in Linux. It has many options that can be specified to customize the user creation process. Two of these options are:

* -d, &#8211;home HOME_DIR: This option allows the user to specify the absolute path to the user&#8217;s home directory. The default is to append the username to the base directory specified by the HOME variable in /etc/default/useradd, or /home by default. The directory does not have to exist but will not be created if it is missing12

* -u, &#8211;uid UID: This option allows the user to specify the numeric user ID (UID) of the user. The UID must be unique and not already in use by another user. The default is to use the next available UID from the range specified by the UID_MIN and UID_MAX variables in /etc/login.defs13 References: 1: useradd(8) &#8211; Linux man page 2: How to Create Users in Linux (useradd Command) | Linuxize 3: Linux Useradd Command Help and Examples &#8211; Computer Hope

QUESTION 81

Which command, available with all MTAs, is used to list the contents of the MTA&#8217;s mail queue? (Specify ONLY the command without any path or parameters.)
mailq, /usr/bin/mailq, sendmail -bp, /usr/sbin/sendmail -bp, /usr/lib/sendmail -bp, sendmail,

/usr/sbin/sendmail, /usr/lib/sendmail

QUESTION 82

After adding a new email alias to the configuration, which command must be run in order to ensure the MTA knows about it? (Specify the command without any path but including all required parameters.)
newaliases, sendmail -bi

QUESTION 83

Which of the following is a valid IPv6 address?
* 2001:db8:3241::1
* 2001::db8:4581::1
* 2001:db8:0g41::1
* 2001%db8%9990%%1
* 2001.db8.819f..1

QUESTION 84

The system&#8217;s timezone may be set by linking /etc/localtime to an appropriate file in which directory? (Provide the full path to the directory, without any country information)
/usr/share/zoneinfo/

Explanation:

The /usr/share/zoneinfo directory contains the binary time zone files that are used by the system to determine the local time for any region. The files are organized in subdirectories by continent, country, or ocean. Some files represent the standard time zones, while others may have historical or political variations. To set the system&#8217;s timezone, one can create a symbolic link from /etc/localtime to the appropriate file in the

/usr/share/zoneinfo directory. For example, to set the timezone to America/New_York, one can use the command sudo ln -sf /usr/share/zoneinfo/America/New_York /etc/localtime. Alternatively, one can use the timedatectl command to set the timezone without creating the link manually. References:

* How to Set or Change the Time Zone in Linux | Linuxize

* 4 Ways to Change the Timezone in Linux &#8211; wikiHow

QUESTION 85

Which file contains the date of the last change of a user&#8217;s password?
* /etc/gshadow
* /etc/passwd
* /etc/pwdlog
* /etc/shadow
* /var/log/shadow

The /etc/shadow file contains the encrypted passwords and other information for each user account on a Linux system. The third field in each line of this file is the date of the last password change, expressed as the number of days since Jan 1, 1970. This information is used by the system to determine when a user must change their password, based on the password aging policy. The /etc/shadow file can be viewed and modified by the root user or by using the chagecommand123. The other files listed in the options do not store the date of the last password change. The /etc/gshadow file contains the encrypted passwords for group accounts4. The

/etc/passwd file contains the basic information for each user account, such as the user name, user ID, group ID, home directory, login shell, etc., but not the password5. The /etc/pwdlog file does not exist by default on most Linux systems, and it is not related to the password change date. The /var/log/shadow file also does not exist by default on most Linux systems, and it is not related to the password change date. References: https://www.redhat.com/sysadmin/password-changes-chage-command https://www.golinuxcloud.com/check-last-password-change-expiration-linux/

QUESTION 86

Where is the system journal stored?
* /var/ jlog/ and /var/jlogd/
* /proc/log and /proc/klog
* /run/Iog/journal/or/var/log/journal/
* /var/log/syslog.bin or /var/log/syslog-jrn
* /etc/system/journal / or /usr/1ib/sysLend/journal/

The LPIC-1 Exam 102, Part 2 of 2, version 5.0, is designed to test the candidate's ability to perform various tasks related to Linux system administration. 102-500 exam consists of 60 multiple-choice and fill-in-the-blank questions that must be completed within 90 minutes. To pass the exam, candidates must demonstrate their proficiency in managing Linux systems, including configuring hardware and software, managing users and groups, implementing security measures, and troubleshooting various issues. The LPIC-1 certification is an excellent starting point for individuals seeking to build a career in Linux system administration, and passing the 102-500 exam is a crucial step towards achieving that goal.

Earning the LPIC-1 certification requires passing both the Lpi 101-500 and Lpi 102-500 exams. Successful candidates will receive a digital certification and badge, which they can display on their online profiles and resumes to showcase their skills and expertise in Linux administration.