



Free Questions for [SCA_SLES15](#) by [actualtestdumps](#)

Shared by [Reynolds](#) on [29-01-2024](#)

For More Free Questions and Preparation Resources

[Check the Links on Last Page](#)

Question 1

Question Type: MultipleChoice

What are the three permissions available on posix file systems? (Choose three)

Options:

- A- Read
- B- Sharable
- C- Edit
- D- Change
- E- User
- F- All
- G- Write
- H- Execute

Answer:

A, G, H

Explanation:

<https://documentation.suse.com/sles/12-SP4/html/SLES-all/cha-security-acls.html>

The three permissions available on posix file systems are read, write, and execute. The read permission allows the user to view the contents of a file or directory. The write permission allows the user to modify or delete a file or directory. The execute permission allows the user to run a file as a program or change into a directory. Reference: <https://documentation.suse.com/sles/15-SP3/html/SLES-all/sec-file-permissions.html#sec-file-permissions-types>

Question 2

Question Type: MultipleChoice

Assuming the default value for umask, which statements regarding permissions are true? (Choose two)

Options:

- A-** The permissions on new files would be set to 444.
- B-** The permissions on new files would be set to 754.

- C-** The permissions on new directories would be set to 770.
- D-** The permissions on new directories would be set to 755.
- E-** The permissions on new files would be set to 644.
- F-** The permissions on new directories would be set to 666.

Answer:

D, E

Explanation:

Assuming the default value for umask, which is 022, the permissions on new files would be set to 644 and the permissions on new directories would be set to 755. The umask value is subtracted from the base permissions of 666 for files and 777 for directories to determine the actual permissions. For example, $666 - 022 = 644$ for files and $777 - 022 = 755$ for directories. Reference: <https://documentation.suse.com/sles/15-SP3/html/SLES-all/sec-file-permissions.html#sec-file-permissions-umask>

Question 3

Question Type: MultipleChoice

For programs to leverage PolKit they are split into two separate processes. Which statements below are true regarding these two PolKit processes? {Choose two}

Options:

- A- The Policy Agent process runs in the System Context.
- B- The Policy Agent process runs in the User Session.
- C- The Mechanism process runs in the System Context.
- D- The Mechanism process runs in the User Session.
- E- The Authentication Agent runs in the System Context.
- F- The D-Bus runs in the User Session.

Answer:

A, C

Explanation:

For programs to leverage PolKit they are split into two separate processes. The statements below that are true regarding these two PolKit processes are:

The Mechanism process runs in the System Context.

The Policy Agent process runs in the User Session.

The Mechanism process is responsible for performing privileged actions on behalf of unprivileged users. It runs as root in the System Context and communicates with PolKit via D-Bus. The Policy Agent process is responsible for requesting authorization from users when they attempt to perform privileged actions. It runs as a normal user in the User Session and communicates with PolKit via D-Bus.

Reference: <https://documentation.suse.com/sles/15-SP3/html/SLES-all/sec-polkit.html#sec-polkit-processes>

Question 4

Question Type: MultipleChoice

Select the valid device types. (Choose two)

Options:

- A- Pipe
- B- null
- C- Redirect
- D- udev

E- Network

F- Character

G- Block

Answer:

F, G

Explanation:

The valid device types are character and block devices. Character devices are devices that transfer data byte by byte, such as keyboards, mice, terminals, etc. Block devices are devices that transfer data in fixed-size blocks, such as disks, CD-ROMs, etc. Pipe, null, redirect, udev, and network are not device types but rather concepts or components related to devices or device management.

Reference: <https://documentation.suse.com/sles/15-SP3/html/SLES-all/sec-devices.html>

Question 5

Question Type: MultipleChoice

The openSUSE Leap version of Linux is designed for which types of user environments? (Choose two)

Options:

- A- Environments requiring High-Availability
- B- Desktop power users
- C- Users requiring only secure terminal access
- D- Data Center environments
- E- Developers

Answer:

B, E

Explanation:

The openSUSE Leap version of Linux is designed for desktop power users and developers. It is a community-driven distribution that offers a stable and reliable operating system with cutting-edge software and tools. It is suitable for personal use, development, testing, and experimentation. It is not intended for high-availability or data center environments that require enterprise-level support and security. Reference: <https://en.opensuse.org/Portal:Leap>

Question 6

Question Type: MultipleChoice

What is the default port a VNC Client uses to connect?

Options:

- A- TCP 5901
- B- DP 5901
- C- TCP 5801
- D- DP 5801

Answer:

A

Explanation:

https://en.wikipedia.org/wiki/Virtual_Network_Computing#:~:text=VNC%20by%20default%20uses%20TCP,Java%2Denabled%20web%2Dbrowser.

VNC by default uses TCP port 5900+N,[6][7] where N is the display number (usually :0 for a physical display). Several implementations also start a basic HTTP server on port 5800+N to provide a VNC viewer as a Java applet, allowing easy connection through any Java-enabled web-browser. Different port assignments can be used as long as both client and server are configured accordingly. A HTML5 VNC client

implementation for modern browsers (no plugins required) exists too.[8]

The default port a VNC Client uses to connect is TCP 5901. This port corresponds to the first display number (:1) of the VNC server. Each display number has its own port number, starting from 5900. For example, display :2 uses port 5902, display :3 uses port 5903, and so on. The user can specify a different port number if needed. Reference: <https://documentation.suse.com/sles/15-SP3/html/SLES-all/sec-vnc-connect.html>

Question 7

Question Type: MultipleChoice

Which option for zypper will list the available patches?

Options:

- A- zypper showpatch
- B- zypper patch
- C- zypper lp
- D- zypper list-patch

E- zypper lu

Answer:

C

Explanation:

The option for zypper that will list the available patches is zypper lp. This command will display a table of patches that are applicable to your system but not yet installed. It will show the patch name, category, severity, summary, and status for each patch. You can use zypper patch to install all available patches or zypper patch-info to get more details about a specific patch. Reference: <https://documentation.suse.com/sles/15-SP3/html/SLES-all/sec-zypper.html#sec-zypper-patches>

Question 8

Question Type: MultipleChoice

What should you do if you want to define alias commands so that each time you open a terminal window those aliases are available from the command prompt?

Options:

- A- Create a file named `-.alias` and put your alias commands in That file.
- B- This cannot be done since aliases are session specific only.
- C- List all your aliases you have defined by entering the `alias --list` command and piping the output to the `-.Abashrc` file.
- D- Modify the `/etc/.history/USER_NAME` file to include your alias commands.
- E- When you create the alias initially, specify the `--keep` parameter.

Answer:

A

Explanation:

If you want to define alias commands so that each time you open a terminal window those aliases are available from the command prompt, you should create a file named `-.alias` and put your alias commands in that file. The `-.alias` file is one of the files that are sourced by the bash shell when it starts. It can contain alias definitions and other customizations for your shell environment. Reference: <https://documentation.suse.com/sles/15-SP3/html/SLES-all/cha-bash.html#sec-bash-startup>

Question 9

Question Type: MultipleChoice

Which of the following configuration files have a format that is compatible with the system logging facility in SUSE Linux Enterprise?
(Choose two)

Options:

- A- /etc/syslog.conf
- B- /etc/syslog-ng
- C- /var/log/syslog-ng.conf
- D- /etc/rsyslog.conf
- E- /ar/log/kernel-log

Answer:

A, D

Explanation:

The configuration files that have a format that is compatible with the system logging facility in SUSE Linux Enterprise are `/etc/syslog.conf` and `/etc/rsyslog.conf`. These files contain rules that specify how to filter and process log messages from different sources and destinations. The `/etc/syslog.conf` file is used by the traditional `syslogd` daemon, while the `/etc/rsyslog.conf` file is used by the more

advanced rsyslogd daemon. SUSE Linux Enterprise uses rsyslogd by default, but it can also read /etc/syslog.conf for backward compatibility. Reference: <https://documentation.suse.com/sles/15-SP3/html/SLES-all/cha-syslog.html#sec-syslog-config>

Question 10

Question Type: MultipleChoice

You want ensure an ext3 filesystem is checked every 50 times it is mounted. Which command would you use?

Options:

- A- dumpe2fs
- B- mkfs
- C- fdisk -o
- D- tune2fs

Answer:

D

Explanation:

The command that is used to ensure an ext3 file system is checked every 50 times it is mounted is tune2fs. The tune2fs command can be used to adjust various parameters of an ext2, ext3, or ext4 file system. The -c option can be used to set the maximum number of mounts between two file system checks. For example, tune2fs -c 50 /dev/sda1 will set the check interval to 50 mounts for /dev/sda1. Reference: <https://documentation.suse.com/sles/15-SP3/html/SLES-all/sec-tune2fs.html>

Question 11

Question Type: MultipleChoice

Which command is used to view the manual pages?

Options:

- A- help -man
- B- doc -man
- C- man
- D- show

E- info

Answer:

C

Explanation:

You can view manual pages by running the `man` command followed by a specific command name. If the `man` command is not installed on your system, install it by running `zypper install man`.

<https://documentation.suse.com/sles/15-GA/html/SLES-all/pre-sle.html>

The command that is used to view the manual pages is `man`. The `man` command will display the formatted documentation for a given command, function, or file. The manual pages are organized into sections based on their type and purpose. The user can specify the section number and the name of the item to view its manual page. Reference: <https://documentation.suse.com/sles/15-SP3/html/SLES-all/sec-cli-help.html#sec-cli-help-man>

To Get Premium Files for SCA_SLES15 Visit

https://www.p2pexams.com/products/sca_sles15

For More Free Questions Visit

<https://www.p2pexams.com/suse/pdf/sca-sles15>

