Unparalleled 101-500 Valid Test Tutorial by Test4Sure

BONUS!!! Download part of Test4Sure 101-500 dumps for free: https://drive.google.com/open?id=1enbQNjaXhGwoj0Ot55jfYuORlP-zScOd

101-500 study materials like a mini boot camp, you'll be prepared for 101-500 test and guaranteed you to get the certificate you have been struggling to. The product here of LPIC Level1 test, is cheaper, better and higher quality; you can learn 101-500 skills and theory at your own pace; you will save more time and energy. No other 101-500 Study Materials or study dumps will bring you the knowledge and preparation that you will get from the 101-500 study materials available only from Test4Sure. Not only will you be able to pass any 101-500 test, but will gets higher score, if you choose our 101-500 study materials.

How much LPIC-1 Linux Administrator , 101-500 Exam Cost

The price of the LPIC-1 Linux Administrator , 101-500 Exam Fee is $200 USD.

>> 101-500 Valid Test Tutorial <<

Online 101-500 Training Materials - 101-500 Valid Exam Materials

One more thing to give you an idea about the top features of LPIC-1 Exam 101, Part 1 of 2, version 5.0 (101-500) exam questions before purchasing, the Test4Sure are offering free Lpi 101-500 Exam Questions demo download facility. This facility is being offered in all three Lpi 101-500 exam practice question formats.

Introduction to LPIC-1 Linux Administrator , 101-500 Exam

The LPIC **101-500 exam**, is one of qualifying exam to attain accreditation of LPIC 1 Linux Administrator , however, to bag the accreditation aspirants have to pass both 101-500 & 102-500 .Aspirants must have knowledge about :

- Installation and maintenance of Linux workstation, including X11 and setup it up as a network client;
- Perform easy maintenance tasks: help users, add users to a larger system, backup and restore, shutdown and reboot.
- Work at the Linux command line, including common GNU and Unix commands;
- Handle files and access permissions as well as system security; and
- Architecture of a Linux system;

Lpi LPIC-1 Exam 101, Part 1 of 2, version 5.0 Sample Questions (Q162-Q167):

NEW QUESTION # 162
What command should be invoked to give the user sally read and write, but not execute, access to the file strategy.txt using Extended ACL entries?

- A. setfacl -setperm user:sally+rw strategy.txt
- B. setfacl -setperm sally:rw strategy.txt
- C. setfacl -m user:sally:rw strategy.txt
- D. setfacl -m user::sally+rw strategy.txt

Answer: C

NEW QUESTION # 163
Which of the following commands creates an ext3 filesystem on /dev/sdb1? (Choose TWO correct answers.)

- A. /sbin/mkfs -c ext3 /dev/sdb1
- B. /sbin/mkfs -t ext3 /dev/sdb1
- C. /sbin/mke3fs -j /dev/sdb1
- D. /sbin/mke2fs -j /dev/sdb1

Answer: B,D

Explanation:
The correct commands to create an ext3 filesystem on /dev/sdb1 are /sbin/mke2fs -j /dev/sdb1 and /sbin/mkfs - t ext3 /dev/sdb1. These commands format the partition /dev/sdb1 with the ext3 filesystem type. The first command uses the mke2fs utility with the -j option, which enables journaling. The second command uses the mkfs utility with the -t option, which specifies the filesystem type. Both commands are equivalent and can be used interchangeably. The other options are incorrect because they use the wrong syntax or parameters for the commands. Option C is wrong because the -c option for the mkfs command checks the device for bad blocks, not the filesystem type. Option D is wrong because there is no such utility as mke3fs. The correct utility name is mke2fs.

NEW QUESTION # 164
Which of the following commands enables the setuid (suid) permission on the executable /bin/foo?

- A. chmod u-s /bin/foo
- B. chmod 1755 /bin/foo
- C. chmod 4755 /bin/foo
- D. chmod 755+s /bin/foo

Answer: C

Explanation:
The correct command to enable the setuid (suid) permission on the executable /bin/foo is:
B). chmod 4755 /bin/foo
The chmod command is used to change the permissions of files and directories in Linux. The chmod command can take either a symbolic or a numeric mode to specify the new permissions. The numeric mode is composed of four digits, each representing a

different set of permissions: the first digit is for the special permissions, such as setuid, setgid, and sticky bit; the second digit is for the user permissions; the third digit is for the group permissions; and the fourth digit is for the others permissions. Each digit can range from 0 to 7, where 0 means no permissions, 1 means execute permission, 2 means write permission, 4 means read permission, and the sum of these values means a combination of permissions. For example, 5 means read and execute permissions, and 6 means read and write permissions.
The setuid permission is a special permission that allows an executable to run with the privileges of the owner of the file, instead of the user who launched it. The setuid permission is represented by the value 4 in the first digit of the numeric mode. For example, to enable the setuid permission on an executable file, use the following command:
chmod 4xxx file
where xxx is the combination of the user, group, and others permissions.
In this question, the executable file is /bin/foo, and the desired permissions are:
* setuid permission enabled
* user permissions: read, write, and execute
* group permissions: read and execute
* others permissions: read and execute
Therefore, the numeric mode for these permissions is 4755, where:
* 4 means setuid permission enabled
* 7 means user permissions: read, write, and execute
* 5 means group permissions: read and execute
* 5 means others permissions: read and execute
The correct command to enable the setuid permission on /bin/foo with these permissions is:
chmod 4755 /bin/foo
This command will change the permissions of /bin/foo to -rwsr-xr-x, where the s in the user section indicates the setuid permission.
The other options are not correct because:
* A. chmod 1755 /bin/foo: This command will enable the sticky bit, not the setuid permission, on /bin
/foo. The sticky bit is another special permission that prevents users from deleting or renaming files that they do not own in a shared directory. The sticky bit is represented by the value 1 in the first digit of the numeric mode. For example, to enable the sticky bit on a directory, use the following command:
chmod 1xxx directory
where xxx is the combination of the user, group, and others permissions.
* C. chmod u-s /bin/foo: This command will disable the setuid permission, not enable it, on /bin/foo. The u-s option is a symbolic mode that means remove the setuid permission from the user permissions. For example, to disable the setuid permission on an executable file, use the following command:
chmod u-s file
* D. chmod 755+s /bin/foo: This command is not valid because it mixes the numeric and the symbolic modes, which are not compatible. The 755 is a numeric mode that means user permissions: read, write, and execute; group permissions: read and execute; others permissions: read and execute. The +s is a symbolic mode that means add the setuid and setgid permissions to the user and group permissions, respectively. The chmod command does not accept both numeric and symbolic modes at the same time, and it will fail with an error message saying:
chmod: invalid mode: '755+s' Try 'chmod --help' for more information.
References:
SetUID, SetGID, and Sticky Bits in Linux File Permissions - GeeksforGeeks How to use special permissions: the setuid, setgid and sticky bits - Linux Tutorials - Learn Linux Configuration chmod(1): change file mode bits - Linux man page

NEW QUESTION # 165
Which of the following commands will write a message to the terminals of all logged in users?

- A. yell
- B. mesg
- C. print
- D. wall
- E. bcast

Answer: D

Explanation:
The wall command is a command-line utility that displays messages to all logged-in users on the terminal12.
The wall command takes the following basic syntax:
$ wall OPTION { file | message }
The OPTION can be one of the following:

* -n or --nobanner: Suppress the banner (the header line with the hostname, date, and time) from the output. This option can only be used by the root user.
* -v or --version: Display version information and exit.
* -h or --help: Display help message and exit.
The file or message argument is the source of the message to be displayed. If a file is specified, the wall command will read the message from the file. If a message is specified, the wall command will read the message from the standard input. The message can be terminated by pressing Ctrl+D.
The other commands in the options are not valid or do not have the same functionality as the wall command:
* bcast: There is no such command in Linux.
* mesg: This command is used to control write access to the terminal. It does not send messages to other users.
* print: This command is used to print files or data to a printer. It does not send messages to other users.
* yell: There is no such command in Linux.
:
1: How to Send a Message to Logged Users in Linux Terminal - Tecmint 2: How to Send Broadcast Messages to Users in Linux Terminal

NEW QUESTION # 166
FILL BLANK
Following the Filesystem Hierarchy Standard (FHS), where should binaries that have been compiled by the system administrator be placed in order to be made available to all users on the system? (Specify the full path to the directory.)

Answer:

Explanation:
/usr/local/bin/

NEW QUESTION # 167
.....

myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, Disposable vapes

P.S. Free & New 101-500 dumps are available on Google Drive shared by Test4Sure: https://drive.google.com/open?id=1enbQNjaXhGwoj0Ot55jfYuORlP-zScOd