UNIT 1: INTRODUCTION TO SYSTEM ADMINISTRATION

UNIT STRUCTURE

1.1 Learning Objectives

1.2 Introduction

1.3 Role and Power of System Administrator

1.4 Qualities of Good System Administrator

1.5 Common Administrative Tasks

1.6 Identifying, Configuration and Log Files

1.7 Let Us Sum Up

1.8 Further Readings

1.9 Answer to Check Your Progress

1.10 Model Questions

1.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- describe the need of the system administrator
- explain the usage of su command
- describe the roles and privileges of a system administrator
- describe the skills required for being a system administrator
- learn some system administrative tasks
- learn about the LINUX configuration and log files

1.2 INTRODUCTION

System administration, required in a multiuser system, is the task of administering and monitoring the system when the system is accessed by multiple users. It is usually handled by a trusted person who is responsible for the administration of the whole system. The main job of a system administrator is to ascertain that there is little to complain about the system's performance or service availability. The system administrator operates in super user mode which is called root. The super user has the privilege to

issue any command, access any file, and perform all the functions in the system. root is the user-id for the super user to log on to the multiuser system. The use of root command must be limited due to the following reasons:

- Inexperienced users can cause severe damage to the system.
- The use of root command for non-privileged tasks is needless and may lead to attack.
- Since root can look at anyone's files, it may violate security and privacy of the system.

The screen shot of super user login into the system is depicted in figure 1.1.

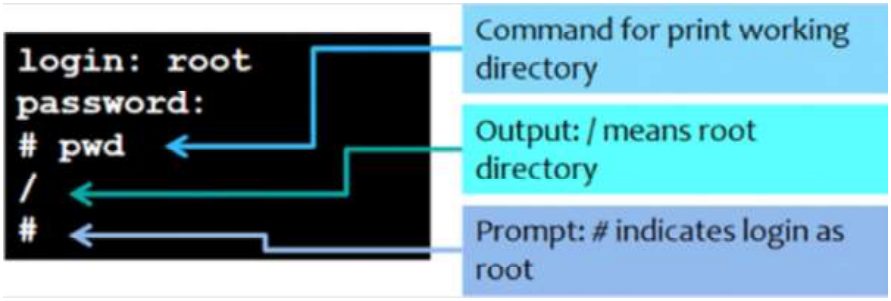


Fig. 1.1 Super user login

The fundamental tasks of the super user includes starting-up & shutting-down the system, creating accounts for new users with necessary environments. Administrative tasks also involve installation of new software, distributing user disk space, taking regular back-ups, keeping system logs, ensuring secure operations and providing network services and web access. The su command is used for becoming super user. It switches from non-privileged account to the super user account. The who am i command is used to view the login name.

The optional argument '-' is used to provide an environment similar to what the user had logged in directly. The su command without '-' argument executes command as root but retains user's current environment.

By using the command shutdown, super user can shut-down or restart the system. The option -h with shutdown command is used for a complete shutdown and the -r option is for restarting the system.

1.3 ROLE AND POWER OF THE SYSTEM ADMINISTRATOR

The System Administrator is responsible for installing the server of the system, updating configuration, operating and maintaining the hardware and software of the system. He/she has to manage failures in the system, troubleshoot and maintain the servers, the user accounts, security, etc. He/she has to accomplish the task of managing the disk space as well as the backup. Also, the job of system administrator is changing the contents of the file or its attributes like its ownership or permission etc. He/she also needs to reset new password and constantly monitor the special services and security of the servers. They are expected to remain informed with the recent knowledge in Linux system in order to assess the hardware and software technologies.

The key responsibilities that need to be taken care of by a Linux System Administrator are:

- To setup and maintain user account,
- To monitor system performance,
- To verify that peripherals are working properly,
- To quickly arrange to repair for hardware in occasion of hardware failure,
- To create and manage file systems,
- To install software and patching firmware and software,
- To create a backup and recovery policy,
- To monitor network communication,
- To update system as soon as new version of OS and application software,
- To Setup security policies for users,
- To manage network administration and Database administration

Further, Linux system administrator must participate in various cross training activities, so as to attain a comfort level that supports the database. They might also be involved in training the subordinate team members in system administration and software deployment responsibilities. They retain proper documentation of all the procedures, configurations, programs, etc.

They offer valuable support to the users by answering their technical queries. Many-a-time, they also provide the customer support through e-mail, telephone, knowledge-based programs and other resources.

The system administrator has the power to modify the contents or the attributes of any files owned by other users, initiate or kill any process that are essentially required for running the system, change the password of any user without even entering the old one, setting the system clock, control user's access to scheduling service and networking service.

1.4 QUALITIES OF GOOD SYSTEM ADMINISTRATOR

To become a successful Linux system administrator, one should be a bootstrapper who has high motivation and detail orientation capacity, and also be flexible and ready to follow the instructions given by their superior. The person should be prepared to acquire recent information/ updates and apply the up-to-date technologies that would help the organization to grow. He/she should hold excellent interpersonal skills and should be comfortable working in a team. Further, the quality of identifying the issues related to system and resolving them in an effective way should also be with the individual. He/she must be able to work well under pressure and able to respond and prioritize work according to the stringent deadlines. In concise, a good system administrator should have the following skills:

- Problem-solving skill:
  - Taken up the matter when a computer system malfunctions.
  - Quickly and correctly diagnose the crisis and produce the best solution.
- Analysing skill:
  - Understand the behavior of software.
  - Deployment of software.
  - Troubleshoot the Problems if occur.
- Programming skill:
  - Have the knowledge of different types of programming languages.
  - Scripting or automation of routine tasks.

- Soft-skills:
  - Users to the system should feel comfortable and know that their problems will be fixed in time.
  - Good and healthy interaction among colleagues/team members etc.

1.5 COMMON ADMINISTRATIVE TASKS

User account management: The system administrator can add accounts for new users and removes the accounts of users those are no longer active. The linux commands used for this are:

- useradd
- usermod
- userdel

useradd: Using this command, the administrator can create an account to represent a user who will be working on the system. Each user must authenticate to Linux with an identity that can be used to control their resource access and consumption. User accounts' detail are stored in the **/etc/passwd** file. It is used in the following way:

$ sudo useradd <accountname>

Also, we should not forget to set a password for the created account by using the passwd command.

$ sudo passwd <accountname>

Few common options are used with useradd command:

- --create -home (-m): Adds a home directory.
- --shell (-s): Sets the user's preferred shell if it's different from /bin/bash
- --uid (-u): Specifies a particular user ID (UID)
- --comment (-c): Populates the comment field (usually with the user's full name enclosed in quotes)

usermod:

This command is used to modify the settings of an existing user account. Modifications are necessary when users change their names, request different shells, or need updated password information.

Standard options for usermod includes:

- --comment (-c): Modifies the comment field.
- --home (-d): Modifies home directory information.
- --expiredate (-d): Changes account-expiration settings.
- --login (-l): Modifies the username.
- --lock (-L): Locks a user account.
- --unlock (-U): Unlocks a user account.

Syntax to use this command is:

$ sudo usermod -c <newName> <oldName>

userdel:

We can remove/delete an account representing a user whose role has changed or is no longer with the organization.

To delete a particular account, type:

$ sudo userdel <accountname>

However, before deleting an account, we also have to consider the resources such as the home directory or system mail related to that account.

Few common options associated with userdel that address these resources are:

- --force (-f): Deletes the account (including mail and home directory), even if the user is still logged in
- --remove (-r): Deletes the account (including mail and home directory), but the user must be logged out

Performing backups: The term backup refers to making copies of data that may be used to restore the original if data loss happens. In Linux, tar command is used to backup/restore files. It can also be used to archive a group of files into another file. The following options are used with tar command.

-c to create an archive

-t to display files on archive

-x to extract from archive

-v verbose -display filenames

-z to compress files

-f device name or filename to write to

There are some examples of using tar command as given below:

tar -cvf /dev/st0 backup the entire system to tape

tar -tvf /dev/st0 view the contents of the tape

tar -xvf /dev/st0 restore the entire contents of the file

1.6 IDENTIFYING, CONFIGURATION AND LOG FILES

A Configuration File, also known as a config file, is a unique type of plain text file that is used to control the operations of a program, utility and process. Linux configuration files contain the settings and instructions for different systems, utilities, applications and processes. As the name infers, configuration files contain information about the structure or arrangement of specific parts of the system. They are kept under the /etc directory.

These files are not essentially of any direct use to users. However, they do affect the way a system functions. For example, the fstab file is the filesystem configuration file that includes all the disk partitions and the purpose of each of the partitions. For regular partitions, the conventional mount point may also be listed. The /etc/fstab file is used by mount and other such commands. It is what allows file systems to be mounted automatically at boot time rather than having to mount them all by hand, one at a time.

As a part of system administration tasks, administrator has to frequently modify these files. For instance, every time a new user is added, the /etc/passwd and /etc/group configuration files must be modified.

/etc/passwd is a password file in which each line holds all the information of a single user. A line consists of seven fields, separated by a colon.

- Login name
- Encrypted password
- UID
- Default GID
- GCOS field including full name, office location, extension number, and home phone.

- Home directory
- Login shell

User-id's (UID's) are mapped to the names in this file. Every time a new user is added their information must be added to this file.

/etc/group contains the names of valid groups and the usernames of their members. This file is owned by root and only root may modify it. When a new user is added information on what groups they are a member of must be added here. Group-id's (GID's) are mapped to the group names kept in this file.

Other configuration files include:

/etc/inetd.config, /etc/hosts, /etc/inittab, /etc/hosts.equiv, /etc/export, and /etc/mtab.

/etc/inetd.config is the Internet daemon file. It holds the instructions used by /etc/inetd to manage the network service daemons.

/etc/hosts is the TCP/IP network configuration file. It is accessed by all commands that use the network. The file contains a list of IP addresses, hostnames and hostname aliases.

/etc/inittab is a system configuration file that helps regulate the operation of serial interfaces.

/etc/hosts.equiv contains a list of TCP/IP "trusted" hosts. If machine A is a trusted host of machine B, then all users on machine A may rlogin to machine B without supplying a password.

/etc/export lists all the file systems that are available to other machines via NFS.

/etc/mtab holds information on all mounted file systems.

Linux Log Files

Log files are the set of records that Linux system keeps so that the system administrator keep a track of important events. They contain messages about the server, including the kernel, services and applications running on it. These files can be helpful for troubleshooting system issues.

Most Linux log files are stored in a plain ASCII text file and are kept in the /var/log directory and subdirectory. Logs are generated by the Linux system daemon log, syslogd or rsyslogd.

Viewing Logs:

- First, open the Linux terminal as a root user. This will enable root privileges.
- Use the following command to see the log files:

  $ cd /var/log
- To view the logs, type the following command:

  $ ls

This command displays all Linux log files, such as kern.log and boot.log. These files contain the necessary information for the proper function of the operating system.

Log files are accessed using root privileges. By definition, root is the default account that can access to all Linux files.

Use the following command to access the respective file:

$ sudo less [logname].log

This command displays a timeline of all information related to that operation.

It is be noted that log files are stored in plain text and hence, they can be viewed by using the following standard commands:

zcat - Displays all the contents of logfile.gz

zmore - lists the file in pages, without decompressing the files

zgrep - Searches inside a compressed file

grep - Finds all occurrences of a search term in a file or filter a log file

tail - produces the last few lines of files

Log files can provide a lot of information about the operations of a system. Most directories can be grouped into one of four categories:

- System Logs
- Event Logs
- Application Logs
- Service Logs

  Many of these logs can be located in the var/log subdirectory.
- System Logs

  Systems log files contain the most significant amount of information

about system functionality. The most common log files include:

- /var/log/boot.log: System Boot log (the boot log stores all information related to booting operations)
- /var/log/auth.log: Auth logs (the authentication log stores all authentication logs, including successful and failed attempts)
- /var/log/httpd/: Apache access and error logs
- /var/log/mysqld.log: MySQL database server log file
- /var/log/debug: Debug logs (the debug log stores detailed messages related to debugging and is useful for troubleshooting specific system operations)
- /var/log/daemon.log: Daemon logs (the daemon log contains information about events related to running the Linux operation)
- /var/log/maillog: Mail server logs (the mail log stores information related to mail servers and archiving emails)
- /var/log/kern.log: Kernel logs (the kernel log stores information from the Ubuntu Linux kernel)
- /var/log/yum.log: Yum command logs
- Event logs

An event log refers to a "log book" that is analyzed and monitored for higher level network intelligence. It can capture many different types of information. For example, it can capture all logon sessions to a network, along with account lockouts, failed password attempts, etc.

- Application Logs

Application logs store information relevant to any application that is executed. These includes error messages, signs of system compromise, and browser identification string. Log files that fall into this category include CUPS Print System logs, Rootkit Hunter log, Apache HTTP server logs, Samba SMB server logs, and X11 server log.

- Service logs

Service logs provides diagnostic information about the resources in your occupancy. When you enable logging on resources, you receive information about the resource in a log file. This information allows you to analyze, optimize, and troubleshoot your resources.



CHECK YOUR PROGRESS

Q 1: Choose the correct options from the followings:

i) The process of starting up a computer is known as

a) Boot Loading b) Boot Record c) Boot Strapping

d) Booting

ii) The shell used for Single user mode shell is:

a) bash b) csh c) ksh d) sh

iii) Which is the only partition mounted in Single user mode

a) boot b) usr c) root d) tmp

iv) Which command is used to restart the Linux system?

a) shutdown -h b) shutdown -r c) restart

d) none of these

v) Which Linux command is used for becoming a super user?

a) su b) man c) who d) None of these



1.7 LET US SUM UP

- System administrator is the person who is responsible for setting up and maintaining the system or server.
- The root account has full (unrestricted) access, so he/she can do anything with the system.
- The system administrator is responsible for user administration, maintaining system, verify whether peripherals are working properly or not, quickly arrange repair for hardware on the occasion of hardware failure, monitor system performance, create file systems, install software.
- Administrator can create a backup and recovery policy.
- The system administrator also monitors network communication, updates system as soon as new version of OS and application software comes out, implements the policies for the use of the computer system and network setup security policies for users.
- A system admin must have a strong grasp of computer security, e.g.

firewalls and intrusion detection systems.

- A system administrator should have problem solving skill, analyzing skill, programming skill and soft skills.
- A configuration file, also known as a config file, is a unique type of plain text file that is used to control the operations of a program, utility or process.
- Log files are a set of records that Linux keeps for the system administrators to keep track of important events.



1.8 FURTHER READINGS

1) S. Das (2012). Your UNIX/Linux: The Ultimate Guide. (Third Edition). (Science/Engineering/Math). McGraw-Hill.
2) Christopher Negus (2012). Linux Bible. (8th Edition). Wiley.



1.9 ANSWERS TO CHECK YOUR PROGRESS

Ans to Q No 1: i) c ii) d iii) c iv) b v) a



1.10 MODEL QUESTIONS

Q 1: What is called System administration and why is it required for multiuser system?

Q 2: Explain the responsibility of a system administrator in detail.

Q 3: Mention the skills required for a good administrator.

Q 4: Write the application of sudo and who am I commands.

Q 5: What is the purpose of configuration file and log file?

Q 6: What are the Linux commands used for user management?

*** ***** ***