

System administration

Table of Contents

Introduction.....	2
Intended Learning Outcomes	2
System Administrator	2
Roles of System Administrator	3
1. User administration.....	3
2. System maintenance.....	3
3. Documentation.....	3
4. System health monitoring	4
5. Backup and disaster recovery	4
6. Application compatibility	4
7. Web service administration and configuration	4
8. Network administration	4
9. Security administration	4
10. Database administration	5
11. Installation and patching	5
12. User training.....	5
Sysadmin certifications and education.....	5
Common skills of system administrators.....	5
References.....	6

Introduction

In this module we discuss system administrator as vital role in an organization applying IT hardware and software services. Common system administrator tasks may range from installation and deployment of servers to providing troubleshooting and technical support for projects.

Intended Learning Outcomes

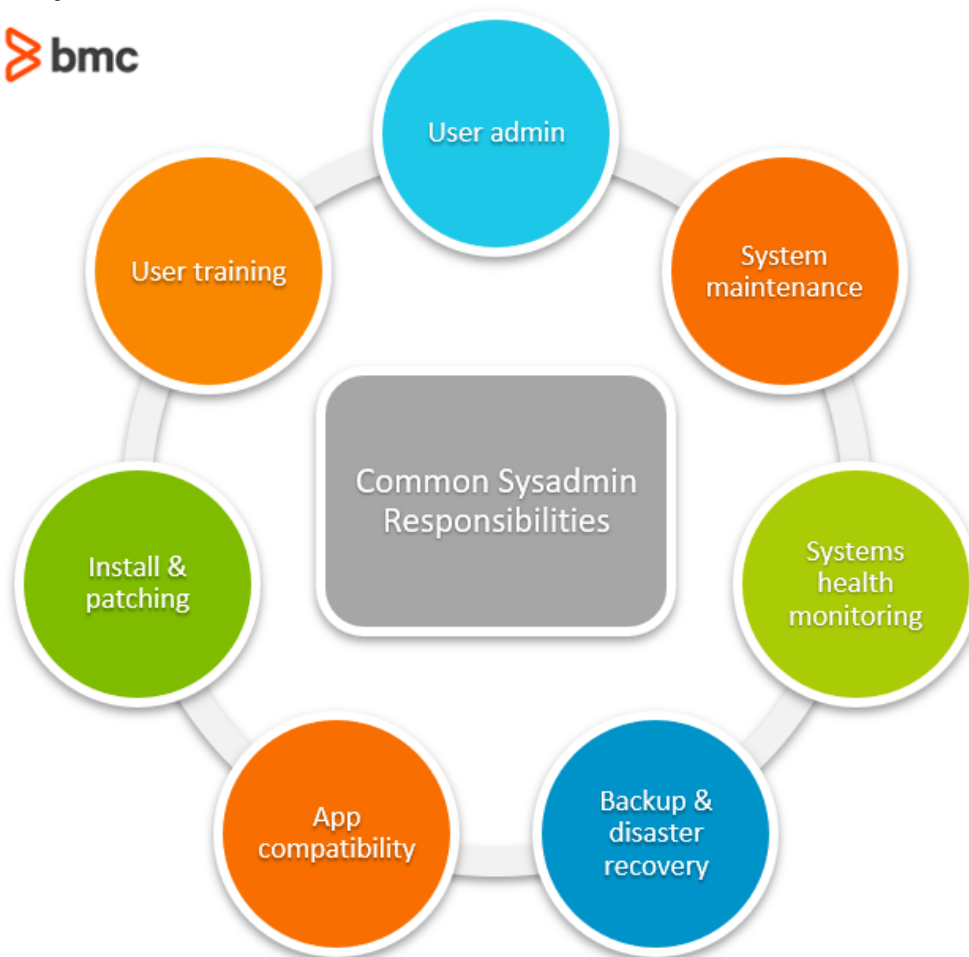
At the end of the module, the students are expected to:

1. Define system administrator.
2. Identify the different roles of system administrator.
3. Identify the education and certifications of system administrators.

System Administrator

- A person responsible for setting up and maintaining a system or a server.
- A person who manages the computer systems in an organization.

Roles of System Administrator



1. User administration

- Support reliable and effective use of complex IT systems by end users (internal or external).
- Manages user groups and user accounts for a centralized user management.

2. System maintenance

- Responsible for the availability of IT systems.
- Troubleshoots and fix issues that comprise system performance or access to an IT service.
- Tasks includes regular system improvements, such as upgrades on evolving end-user and business requirements.

3. Documentation

- Maintains records of IT assets usage.
- Plans for future IT investments and upgrades documenting:
 - End-user requests

- Business requirements
 - IT issues
- Documentation also underpins regulatory compliance.

4. System health monitoring

- Most IT issues go unnoticed until the impact reaches end users therefore system admin monitor system health and identify anomalous network behavior, which may include sensitive activities such as unauthorized network access and data transfer.
- As administrators you may need advance tools for monitoring.

5. Backup and disaster recovery

- Scheduled backup
- Plans disaster recovery strategies
- Facilitate end-users in accessing data that may have been deleted or unavailable.

6. Application compatibility

- Ensures that software systems and feature releases are compatible with the IT infrastructure. Example:
 - Testing server load performance
 - Install/upgrade hardware components

7. Web service administration and configuration

- Sysadmins regularly perform web service administration and configuration management activities, including ensuring that configuration changes are documented and follow organizational policies associated with access and cybersecurity.
- Refer to this reference on web services:

IBM. (n.d.). *What is a web service?* © Copyright IBM Corporation 2019. Retrieved January 5, 2022, from <https://www.ibm.com/docs/en/cics-ts/5.1?topic=services-what-is-web-service>

8. Network administration

- Maintains network integrity by following network interactions follow organizational policies and protocols.
- Requires a background in networking or network engineering to perform mission-critical network administration activities if you do not have a separate network department.

9. Security administration

- Network monitoring and analysis
- Identity and access management
- Maintaining security of hardware components
- Managing software licensing, updates, and patching

10. Database administration

- Maintains integrity, performance, and efficiency of database systems.
- Database management may include migration, design, configuration, installation, and security of the organization's data assets.

11. Installation and patching

- Responsible for managing, troubleshooting, licensing, and updating hardware and software assets.
- You make sure that appropriate measures are proactively followed in response to unforeseen issues such as IT downtime or zero-day exploits.

12. User training

- Sometimes you conduct trainings programs to bring users up to date with new software installations or IT system changes.

Sysadmin certifications and education

Courses may be:

Computer Science or Information Technology

With certifications such as:

- Microsoft Windows Server and Desktop Certifications
- CompTIA Network+ and A+
- Unix
- Linux
- Cloud certifications (new)

Common skills of system administrators

- Subject matter expertise on the following areas:
 - Computer systems
 - Networks
 - Hardware and software troubleshooting
 - Databases
 - Web services
- Problem solving since you will be the first person called upon to deal with a problem
- Strong interpersonal and communication skills (both written and verbal). You will be talking with both technical and non-technical persons.

References

1. Raza, M. (2019, October 14). *Sysadmin: Role, Responsibilities, Job Description & Salary Trends*. BMC Blogs. Retrieved January 5, 2022, from <https://www.bmc.com/blogs/sysadmin-role-responsibilities-salary/>
2. Direct Link from Job Portals: <https://www.indeed.com/recruitment/job-description/system-administrator>

Linux File Permission

Table of Contents

Introduction.....	2
Intended Learning Outcomes.....	2
Check Permission.....	2
Permission Settings.....	2
Change Permission.....	3
Define File Permission with Symbolic Mode.....	4
Define File Permission in Octal/Numeric Mode	5
Changing User File and Group Ownership.....	5
Summary	6
References	6
Install the Apache	6
Install MySQL	6
Install PHP	7

Introduction

The Linux file system derives its implementation from Unix, released in 1973, and is much older than Windows. When AT&T first designed Unix, disk space was premium, and each bit on the hard drive mattered. To maximize disk space, each file could only have three sets of permissions – access permissions for everyone, access permissions for its “owning group,” and access permission for its “owning user.”

Intended Learning Outcomes

At the end of the module, the students are expected to:

1. Learn how to check file permission in Linux
2. Apply file permission to files in Linux

Check Permission

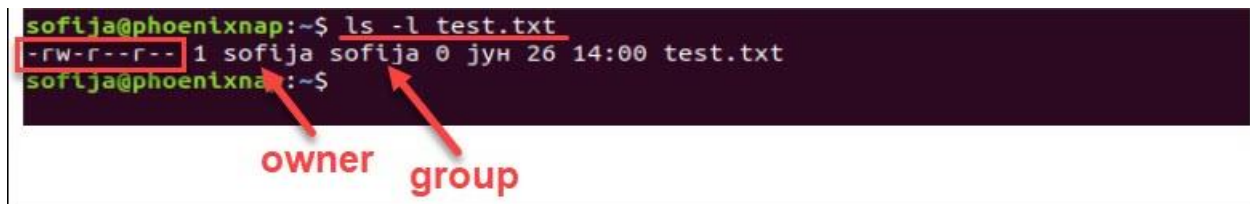
You can check the file permission in your ls command. Add the option -l to see the information in the long list format.

Syntax:

```
ls -l [filename]
```

Example:

```
ls -l test.txt
```



```
softja@phoenixnap:~$ ls -l test.txt
-rw-r--r-- 1 softja softja 0 jyh 26 14:00 test.txt
softja@phoenixnap:~$
```

owner group

The output provides the following information:

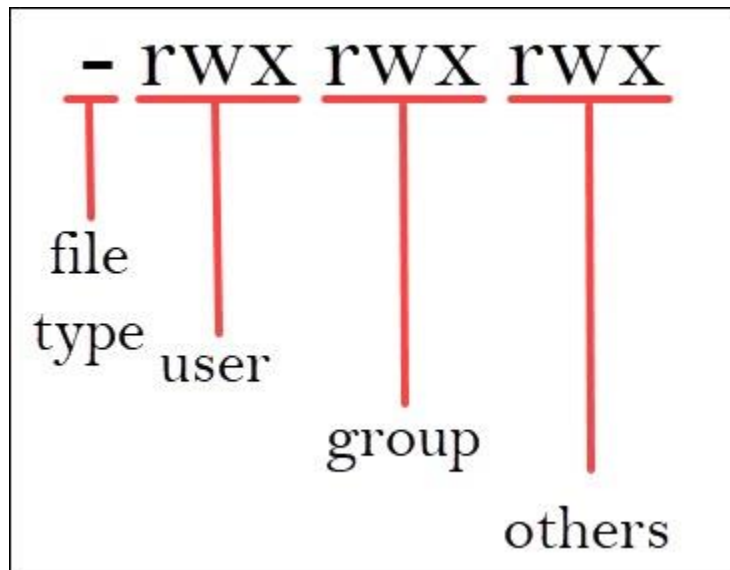
- File permission
- The owner (creator) of the file
- The group to which the owner belongs to
- The date of creation of the file

Permission Settings

It shows the permission settings, grouped in a string of characters (-, r, w, x) classified into four sections:

1. **File type.** There are three possibilities for the type. It can either be a regular file (-), a directory (d) or a link (l).

2. **File permission of the user (owner)**
3. **File permission of the owner's group**
4. **File permission of other users**



The characters **r**, **w**, and **x** stand for **read**, **write**, and **execute**.

The categories can have all three privileges, just specific ones, or none at all (represented by `-`, for denied).

Users that have **reading permission** can see the content of a file (or files in a directory). However, they cannot modify it (nor add/remove files in a directory). On the other hand, those with **writing privileges** can edit (add and remove) files. Finally, being able to **execute** means the user can run the file. This option is mainly used for running scripts.

The previous example showed that `test.txt` is a regular file with reading and write permission assigned to the owner but gives read-only access to the group and others.

```
sofijs@phoenixnap:~$ ls -l test.txt
-rw-r--r-- 1 sofijs sofijs 0 jyh 26 14:00 test.txt
sofijs@phoenixnap:~$
```

The permissions `-rw-r--r--` are circled in red, and a red arrow points to a callout box containing the same permissions: `-rw-r--r--`.

Change Permission

You will, at some point, want to modify the permission settings of a file/directory. To do this, the command we need will be `chmod`

Syntax:

```
chmod [permission] [file_name]
```

There are two ways to define permission:

1. using **symbols** (alphanumeric characters)
2. using the **octal notation method**

Define File Permission with Symbolic Mode

To specify permission settings using alphanumeric characters, you'll need to define accessibility for the user/owner (**u**), group (**g**), and others (**o**).

Type the initial letter for each class, followed by the equal sign (=) and the first letter of the read (**r**), write (**w**) and/or execute (**x**) privileges.

To set a file, so it is public for reading, writing, and executing, the command is:

```
chmod u=rwx,g=rwx,o=rwx [file_name]
```

To set permission as in the previously mentioned **test.txt** to be:

- read and write for the user
- read for the members of the group
- read for other users

Use the following command:

```
chmod u=rw,g=r,o=r test.txt
```

Note: There is no space between the categories; we only use commas to separate them.

Another way to specify permission is by using the octal/numeric format. This option is faster, as it requires less typing, although it is not as straightforward as the previous method.

Instead of letters, the octal format represents privileges with numbers:

- **r**(ead) has the value of **4**
- **w**(rite) has the value of **2**
- **(e)x**(ecute) has the value of **1**
- **no permission** has the value of **0**

The privileges are summed up and depicted by one number. Therefore, the possibilities are:

- **7** – for read, write, and execute permission
- **6** – for read and write privileges

- 5 – for read and execute privileges
- 4 – for read privileges
- 3
- 2
- 1

As you have to define permission for each category (user, group, owner), the command will include three (3) numbers (each representing the summation of privileges).

For instance, let's look at the test.txt file that we symbolically configured with the `chmod u=rw,g=r,o=r test.txt` command.

The same permission settings can be defined using the octal format with the command:

```
chmod 644 test.txt
```



Define File Permission in Octal/Numeric Mode

Note: If you need a more in-depth guide on how to use Chmod In Linux to change file permissions recursively, read our [Chmod Recursive](#) guide.

Changing User File and Group Ownership

Aside from changing file permissions, you may come across a situation that requires **changing the user file ownership** or even **group ownership**.

Performing either of these tasks requires you first need to switch to superuser privileges. Use one of the options outlined in the previous passage.

To change the **file ownership** [use the chown command](#):

```
chown [user_name] [file_name]
```

Instead of `[user_name]` type in the name of the user who will be the new owner of the file.

To change the **group ownership** type in the following command:

```
chgrp [group_name] [file_name]
```

Instead of `[group_name]` type in the name of the group that will be the new owner of the file.

Summary

This module taught us that every operating system could change the file permission. In Linux, its format dates back from Unix.

We also explored how to change the file permission using a symbolic mode or through octal or numeric mode.

References

- Palczewski, A. (2014, June 14). *Linux vs Windows File Permissions*. ApHarmony. Retrieved December 13, 2021, from <https://www.apharmony.com/software-sagacity/2014/06/linux-vs-windows-file-permissions/>
- Simic, S. (2021, August 2). *Linux File Permission Tutorial: How to Check and Change Permissions*. Knowledge Base by PhoenixNAP. Retrieved December 13, 2021, from <https://phoenixnap.com/kb/linux-file-permissions>

Installing the LAMP

Install the Apache

```
sudo apt install apache2  
sudo ufw app list
```

Install MySQL

```
sudo apt install mysql-server
```

to test if the mySQL is installed

- `sudo mysql`
- type `exit` if you want to end mySQL

Install PHP

```
sudo apt install php libapache2-mod-php php-mysql
```

to verify:

```
php -v
```

Target for Thursday

1. Configure the VM IP Address
 - Temporary IP
 - Static IP
 - DHCP IP
2. Configure Apache
 - Upload a simple PHP file
3. Deploy a database of #2
4. Access and test the website using the main machine