ELSEWEDY UNIVERSITY OF TECHNOLOGY
- POLYTECHNIC OF EGYPT -

Operating System

Lab 5: users management

© Fall 2023 - **Eng. Taghreed Salem – Eng.Nahla Hafez**
Building, office No.
Taghreed.salem@sut.edu.eg

Working With Files and Directories

- These commands can be used to: find out information about files, display files, and manipulate them in other ways (copy, move, delete).

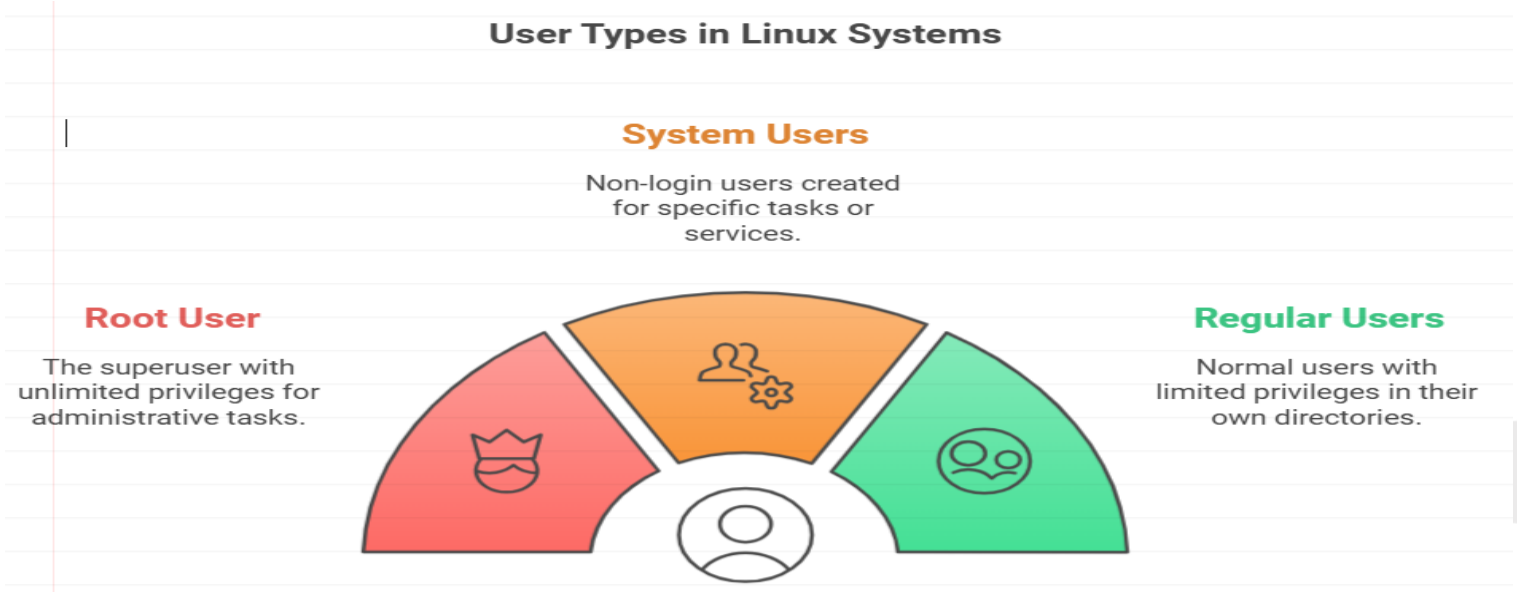
Linux Command	DOS Command	Description
file		Find out what kind of file it is. For example, "file /bin/ls" tells us that it is a Linux executable file.
cat	type	Display the contents of a text file on the screen. For example: cat mp3files.txt would display the file we created in the previous section.
head		Display the first few lines of a text file. Example: head /etc/services
tail		Display the last few lines of a text file. Example: tail /etc/services
tail -f		Display the last few lines of a text file, and then output appended data as the file grows (very useful for following log files!). Example: tail -f /var/log/messages

Working With Files and Directories (cont.)

Linux Command	DOS Command	Description
Cp	copy	Copies a file from one location to another.Example: cp mp3files.txt /tmp (copies the mp3files.txt file to the /tmp directory)
Mv	rename, ren, move	Moves a file to a new location, or renames it. For example: mv mp3files.txt /tmp (copy the file to /tmp, and delete it from the originallocation)
rm	del	Delete a file. Example: rm /tmp/mp3files.txt
mkdir	md	Make Directory. Example: mkdir /tmp/myfiles/
rmdir	rd, rmdir	Remove Directory. Example: rmdir /tmp/myfiles/

Users types :

- **Root User** :The root user is the superuser with unlimited privileges. The root account is used for administrative tasks like installing software, managing system files, and configuring settings .The root user's UID is always 0.
- **System Users** :These are non-login users created by the system or software packages for performing specific tasks or services (e.g., nobody, www-data).They usually have UIDs between 1 and 999 (for most Linux distributions).
- **Regular Users** :These are normal users with limited privileges, typically assigned UIDs starting from 1000.Regular users have permissions mainly within their own directories.



User Management Commands:

Command	Description
useradd	Creates a new user account
usermod	is used to modify an existing user account on a Linux system
passwd	Changes a user's password.
deluser	Used to delete user
groupadd	Creates a new group.

- Note : Both sudo and su are commands used in Linux to execute commands with elevated privileges, but they serve different purposes and operate in distinct ways.
- sudo : sudo stands for "superuser do" and allows a permitted user to execute a command as the superuser (root) or another user, as specified by the security policy.
- su :su stands for "substitute user" or "switch user." It allows a user to switch to another user account, typically the root user, without needing to log out.

Lab 1 : User management :

1. **Understanding User Types:** Identify the current user

Check your current user: *whoami*

Displays the user's UID, GID, and group memberships: *id*

2. Switching to the Root User: Switch to the root user using *su – root*

then Enter your standard user password when prompted

3. Set new password for root : use command *sudo passwd root* and follow the prompit and use this command to set password for the first time for the root from the standard user.

4. switching to standard user from the root : *su - username*

5. Create a New Standard User: first switch to the root user then type *sudo adduser newuser* to create new user called (newuser).

You will be prompted to set a password for the new user. Enter a secure password and confirm it when asked and to back the previous user write *exit* .

6. Show all users from the root : use command *getent passwd* to list all users accounts on the system.

7. Delete user : use sudo userdel username to delete user called username.

Group management

- **Group management**: in Linux is a way to organize and control user permissions for accessing files, directories, and system resources. Groups allow administrators to apply permissions to multiple users at once, improving both security and manageability.
- **Types of Groups in Linux:**

1.*Primary Group* : Each user has one primary group, typically with the same name as the username. When the user creates files or directories, they are assigned to this primary

2.*Secondary (Supplementary) Groups* : Users can belong to multiple secondary groups, giving them additional access to specific files and directories shared with these groups.

Lab2 : Group management :

1. **Create new group** : from root use *sudo groupadd groupname.*
2. **Create Two New Users:** sudo adduser user1 , sudo adduser user2
3. **Add the Users to the Group:**
   sudo usermod -aG groupname user1
   sudo usermod -aG groupname user2
4. **Verify the Group Memberships** : use id command .
5. **Remove user from group :** sudo gpasswd -d username groupname
6. **Remove group :** sudo groupdel groupname
7. **Add regular user to sudo group(make regular user as superuser) :** sudo usermod -aG sudo username

Note: The ***sudo*** *group* in Linux is a special user group that grants members permission to run commands with elevated (root) privileges using the sudo command. This allows users in the sudo group to execute administrative tasks without needing to log in as the root user, enhancing system security and control.