# Operating Systems

Lecture 06: Managing User and Group Accounts (continued)

# Managing User and Group Accounts

## Configure User Profiles

- User Profiles
  - A user profile is a set of options, preferences, bookmarks, and other user items that characterize a user.
  - User profiles define settings such as network resources, data, attributes, and permissions that the system assigns to a user.
  - These settings are retained for every session. The user can specify a name for the user profile. Otherwise, the profile will be called “Default User.” Each user can create several user profiles for business or personal use.

# Managing User and Group Accounts

## Configure User Profiles

- Modifying Default Options
  - You can modify default options while configuring a user profile. Some commonly modified options include:
  - PS1—This variable stores information about the primary prompt, which is the prompt that is displayed when users log in. This variable may or may not be modified.
  - PS2—This variable stores information about the secondary prompt.
  - PATH—This variable stores information about the search paths for commands. You can modify the PATH if you want to use commands that are not stored in the standard directories.

# Managing User and Group Accounts

## Configure User Profiles

- Hidden Files and Directories
  - Some files and directories in the system are hidden.
  - The ls command lists all files, except hidden files. To display all files, including hidden ones, the ls -a command is used.
  - The names of hidden files and directories start with a period.
  - You can also add a period to the names of directories to hide them. Hidden files are usually those files that require minimal editing

# Managing User and Group Accounts

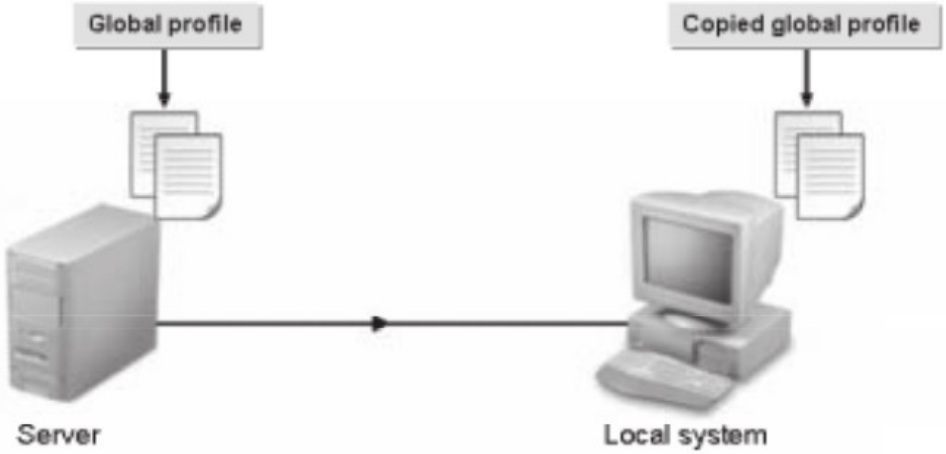
## Configure User Profiles

- The Profile File
  - When a user logs in and starts a new Bash session, several commands need to be typed to customize the user's session.
  - It will be tedious to type these commands every time the user logs in. Therefore, these commands are saved in a special executable file from where Bash will run the commands every time the user logs in.
  - This file is called a profile file because it contains the commands that are used to tailor the session according to the requirements of the user.
  - Individual profiles for every user are available at the ~/.bash_profile or ~/.profile file in the user's home directory, and changes to this file affect the user's customized settings.

# Managing User and Group Accounts

## Configure User Profiles

- Global User Profiles
  - A global user profile is a set of options, preferences, bookmarks, stored messages, attributes, permissions, and other user items that users have access to, on whichever system they log in to.
  - Global user profiles are stored on the server. Each time a user logs in, data in the global profile is copied to the local system. While the user is logged in, any changes made to the settings affect only the local copy of the profile.



# Managing User and Group Accounts

## Configure User Profiles

- Global User Profiles
  - **Skel Directories**
    - When a new user account is created, the skel directory stores a copy of the files and directories that are placed in the home directory of the new user.
    - The skel directory path is **/etc/skel**. This ensures that all new users begin with the same settings.
    - Modifications made to the skel directory affect only the new users.
    - Skel is derived from the word “skeleton” which implies a basic folder structure.

# Managing User and Group Accounts

## Configure User Profiles

- Global User Profiles
  - **Managing the /etc/skel Files**
    - By default, the hidden files for configuring a user's environment are stored in the skel directory.
    - These include **.bash_profile**, **.bashrc**, **.screenrc**, and others.
    - If there are other files that you would like to include in new user accounts, you can add those files to this directory.
    - The files will then be copied to the new users' home directories when new users are created.

# Managing User and Group Accounts

## The userdel Command

- The userdel command allows you to modify the system account files, deleting all entries that refer to the login of an existing user. However, it will not allow you to remove an account if the user is currently logged in. You must kill any running processes that belong to an account before deleting the account.
- The syntax of the userdel command is **userdel [options] {username}**.
- The **-r** option will delete the files in the user's home directory, along with the home directory itself. Files located in other filesystems will have to be searched for and deleted manually.

# Managing User and Group Accounts

## The usermod Command

- The usermod command has options that enable you to modify various user account parameters. You can change a user's name, default groups, UID, or passwords.
- The syntax of the usermod command is usermod [options] {username}.

# Managing User and Group Accounts

## The usermod Command

| Option | Allows You To |
|---|---|
| `usermod -l {new login}{login}` | Modify the login name of the user. |
| `usermod -c "comment" login` | Modify the user's full name, office address, and contact numbers in the password file. Alternatively, you can use the `chfn {user name}` command to modify the details. |
| `usermod -f {number of days} {login}` | Modify the number of days for a password to expire and to disable the account permanently. |
| `usermod -u {new unique user ID} {login}` | Modify the numerical value of a user's ID, which has to be unique. |
| `usermod -d {new login directory} login` | Modify the user's default login directory. |
| `usermod -L {user name}` | Lock the password and suspend the user account temporarily. |
| `usermod -U {user name}` | Unlock the password. |
| `usermod -e {yyyy-mm-dd} {user name}` | Change the expiration date for the user account. |

# Managing User and Group Accounts

## Lock User Login

- In Linux, you can lock a user's login to temporarily prevent a user from logging in to a system. This is done by disabling the user's password using the **passwd -l** command. The user's login is usually locked as a security measure, to prevent unauthorized usage when the user is unavailable

## Temporarily Suspending User Access

- If you need to prevent logging in to a system through an account, but don't want to delete that account, you can edit the /etc/shadow file and replace the existing encrypted password with an asterisk.
- Be sure not to delete the colons on either side of the password because it could corrupt the file. Then, to reactivate the account, remove the asterisk and assign a new password to the user account.

# Managing User and Group Accounts

## Group Management

- Groups, like users, are identified by a system with a unique number known as GID.
- In Linux, users can be members of one primary group and multiple supplemental groups.
- The groupdel and groupmod commands are useful in managing groups
- The syntax of the groupdel command is **groupdel {group name}**
- The syntax of the groupmod command is **groupmod -g {GID}**

# Managing User and Group Accounts

## Group Management

- **Group Account with GID**

  To add a new group to the system with a name of print_users and a GID of 700, enter groupadd -g 700 print_users at the command line.

- **Adding Users to a Group**

  As with users, the group file can be directly edited to add groups. You can use the groupadd command to add users instead of editing the group file.

- The syntax of adding user to a group: sudo usermod -a -G groupName userName

# Managing User and Group Accounts

## Group Management

- **The mkdir Command**
  - The mkdir command allows you to create new directories. The syntax of the command is mkdir {directory name}.
- **The chown Command**
  - The chown command is used to change the user or group that owns one or more files or directories.

# Thanks For Attention