Linux user management is an essential task to manage linux servers.

User Accounts: In Linux, each user is associated with a user account, which contains information about the user, such as their username, user ID (UID), group ID (GID), home directory, and login shell. User accounts are stored in the /etc/passwd file.

Group Management: Users are often organized into groups, which can simplify permission management. Group information is stored in the /etc/group file.

Usernames: Usernames are used to log in to the system. They should be unique and adhere to certain rules (e.g., no spaces or special characters). To create a new user, you can use the useradd or adduser command. For example:
sudo useradd username

Setting Passwords: Users should have strong passwords. You can set or change a user's password using the passwd command:
sudo passwd username

User Permissions: Linux uses a permission system to control access to files and directories. You can assign user-specific permissions using the chmod command and group-specific permissions using chown.
chmod +rx <file name>
chown <user:group> < file name >

Home Directories: Each user typically has a home directory where they store their files. By default, the home directory is located in /home/username. You can set the home directory when creating a user or change it using the usermod command.
For example, to change a user's home directory, you can use:
sudo usermod -d </new/home/directory> <username>

User Information: You can view user account information using the id or finger commands, or by inspecting the /etc/passwd file.

User Deletion: To delete a user, use the userdel command. Be cautious when deleting users, as their files may be removed as well unless you specify the --remove option.
sudo userdel username
sudo userdel -r username

User Groups: Users can belong to one or more groups. To add a user to a group, use the usermod or gpasswd command:
sudo usermod -aG groupname username

User Locking and Unlocking: To temporarily disable a user's account, you can lock it using the passwd command with the -l option:
sudo passwd -l username
To unlock, use the -u option
sudo passwd -u username

User Expiration: You can set an expiration date for a user account using the chage command. This can be used for temporary accounts.
sudo chage -E YYYY-MM-DD username

User Privileges: Some users may need administrative privileges. In Linux, this is often managed using the sudo command. Users in the sudoers file can execute commands as superusers. Granting sudo privileges to users is done by adding entries to the **/etc/sudoers** file using the **visudo** command.

Password Policies: Linux systems can implement password policies, such as minimum password length, complexity, and expiration rules, using the Pluggable Authentication Module (PAM).

Monitoring and Logging: It's essential to monitor user activities and log login attempts and actions. Tools like auditd and system logs (/var/log/auth.log) can be helpful.
SSH Key Authentication: Instead of passwords, users can use SSH keys for secure authentication. You can manage SSH keys in the ~/.ssh/authorized_keys file in the user's home directory.

User Authentication and Login Options: Manage authentication methods and login options through the /etc/security/access.conf and /etc/pam.d configuration files.