**Users and Groups in Linux**

**Users** - Individuals who use the computer. In both Windows and Linux, users are categorized based on their permissions:

* **Windows Users:**
  1. **Administrator** - Full power.
  2. **Standard** - Less power.
  3. **Guest** - No power.
* **Linux Users:**
  1. **Privileged User** (Administrator/Root) - Full power. **UID = 0**.
  2. **Non-privileged User** - Less power. **RHEL 5,6: UID 500+ | RHEL 7,8,9: UID 1000+**.
  3. **System User** - Automatically created by the system. **RHEL 5,6: UID 1-499 | RHEL 7,8,9: UID 1-999**.

**Creating and Managing Users:**

* Create a user: useradd ankit or adduser ankit
* Set password: passwd ankit
* Create user without a password: passwd -d ankit (-d = delete)
* Delete a user: userdel ankit
* Delete a user with data: userdel -r cloud (-r = recursive)

**Key Files and Directories:**

* **/etc/passwd** - Stores user information.
* **/etc/group** - Stores group information.
* **/etc/shadow** - Stores user password information.
* **/etc/gshadow** - Stores group password information.
* **/home** - Home directories for users.
* **/var/spool/mail** - User email files.

**User Information Example:**

amit:x:1002:1002::/home/amit:/bin/bash

* amit - Username.
* :x: - Encrypted password (stored in /etc/shadow).
* 1002 - User ID (UID).
* :1002 - Group ID (GID).
* :: - Comment field.
* /home/amit - Home directory.
* :/bin/bash - Default shell.

**User Modifications:**

1. Change login name: usermod -l newname oldname (-l = login)
2. Change UID: usermod -u 2000 name (-u = UID)
3. Add comment: usermod -c "IT ADMIN" name (-c = comment)
4. Change home directory: mkdir /data && chmod 777 /data && usermod -d /data cloud (-d = directory)
5. Change shell: usermod -s /sbin/nologin name

**Groups:**

* **Primary Group** - Automatically created (user - cloud, group - cloud).
* **Secondary Group** - Manually created (groupadd HR).

**Group Modifications:**

* Change group name: groupmod -n newname oldname (-n = name)
* Change group ID: groupmod -g 3000 name
* Add user to group: usermod -G sales aa or gpasswd -a aa sales (-a = add)
* Remove user from group: gpasswd -d aa sales (-d = delete)

**Shadow File Example:**

aa:$6$rounds=100000$uYAQpC1H1v8SJntf$ROXptZmOgZ1z5cbcKc5ViulVrsCpDsg3d8ibxxcWNumEciI9CQvRZkhYGTcKOHr8SyK7VKCcZ3GrBEBuKYvZA1:20111:0:99999:7:::

* aa - Username.
* :$6$rounds=100000$... - Encrypted password.
* 20111: - Days since 1/1/1970.
* 0: - Minimum password age.
* 99999: - Maximum password age.
* 7::: - Warning period.

**Changing Password Information:**

* View password info: chage -l aa
* Modify password info: chage aa
  + Minimum password age: 5
  + Maximum password age: 30
  + Warning: 3 days
  + Account expire: 31/12/2025

**Lock/Unlock User:**

* Lock user: usermod -L bb
* Unlock user: usermod -U bb

**Switching and Elevating User Privileges:**

* Switch user: su aa (no password if from privilege to non-privilege)
* Switch user from home directory: su - aa
* Grant non-privileged user elevated commands: sudo
  + Configure sudo permissions: /etc/sudoers or visudo
  + Example entry: root ALL=(ALL) ALL