In a Linux system, users refer to individuals or entities that interact with the operating system by logging in and performing various tasks. User management plays a crucial role in ensuring secure access control, resource allocation, and system administration.

A user in Linux is associated with a user account, which consists of several properties defining their identity and privileges within the system. These properties are a username, UID (User ID), GID (Group ID), home directory, default shell, and password.

**Type of Users in Linux**

Linux supports two types of users: system users and regular users.

* **System users** are created by the system during installation and are used to run system services and applications.
* **Regular users** are created by the administrator and can access the system and its resources based on their permissions.

Create Users

Alex, needs to create user accounts for John, Lisa, and Sarah. Alex initiates the process using the useradd command.

For example, to create John's account, Alex executes the command below:

**useradd -u 1002 -d /home/john -s /bin/bash john**

This command creates John's account with uid (-u) as 1002, the home directory (-d) as **/home/john** and sets (-s) **/bin/bash** as his default shell.

Alex can verify the new user account by running the id command:

**id john**

**Password**: User accounts require passwords to authenticate and access the system. CTechCo's users, including John, must create strong passwords to ensure security.

Let's explore how the IT team can enforce password policies and manage user passwords effectively.

**Setting Password Policies:** The IT team can establish password policies to enforce strong passwords, including complexity requirements, password expiration, and account lockouts. These policies can be configured in the **/etc/login.defs** file.

**Changing User Passwords:** Users should be encouraged to change their passwords periodically. They can do so using the passwd command. For example, John can change his password with the following command:

**sudo passwd john**

This command prompts John to enter his current password and then allows him to set a new, secure password.

Alex could take a look at the users on their Linux by running the **cat /etc/passwd** command.

**Delete Users**

To remove her account and associated files, Alex has to utilize the userdel command. For instance, to delete Lisa's account, Alex runs:

**sudo userdel lisa**

This will delete the user account for lisa, along with their home directory and any files or directories owned by the user.

**Modify Users Account**

Create a new group called **development** to manage access to development-related resources. To add John to the development group, the following command can be used:

**sudo usermod -aG development john**

This command adds John to the development group, granting him the necessary access privileges.

The IT team can modify his account accordingly. For example, to change John's default shell to **/bin/zsh**, the following command can be used:

**sudo usermod -s /bin/zsh john**

This command updates John's account to use the new default shell — **/bin/zsh**.

You can run the **cat /etc/passwd** again to see that the shell for john has changed from **/bin/bash** to **/bin/zsh**.

**Group Management**

To create a new group, such as the marketing group, the following command can be used:

**sudo groupadd development**

The command above creates the marketing group, which can be used to grant specific permissions and access to marketing-related resources.

You can also use the command to return a specific group.

**cat /etc/group | grep development**

**How to Assign Users to Groups in Linux**

Once a group is created, users can be added to it. For example, to add Sarah (the marketing manager) to the marketing group, the following command can be used:

**sudo usermod -aG marketing sarahsmith**

This command adds Sarah to the marketing group, enabling her to access the resources associated with that group.

**Principle of Least Privilege**

The principle of least privilege (PoLP) is a fundamental concept in user management. It states that users should only be granted the minimum privileges necessary to perform their tasks effectively.

For example, John is granted administrative privileges using the sudo command only when required for specific tasks. By running the following command, John can execute commands with elevated permissions:

**sudo command**

**Monitoring and Auditing**

Implement monitoring and auditing mechanisms to track user activities and identify potential security breaches. They utilize tools like auditd to collect and analyze system logs, enabling them to detect suspicious activities and take appropriate actions.

For example, the IT team can configure auditd to monitor critical system files and directories, as well as user logins and administrative commands.

Also, to view system logs in Linux, Alex can use the **tail** command. For example, to view the last 10 lines of the system log file, you can use the following command:

**sudo tail /var/log/syslog**