Module II: Users and Group Management

Part I

Differences Between Regular and Administrative Users in Linux:

In Linux, regular users and administrative users have different levels of access and privileges. Here are some of the key differences between the two:

1. Permissions: Regular users have limited permissions, while administrative users have full permissions. Administrative users can access and modify system files and settings, while regular users can only access their own files and settings.
2. Access to commands: Regular users are not able to run certain commands that require root or superuser privileges, while administrative users can run all commands. For example, regular users cannot use the **apt-get** command to install new software, while administrative users can.
3. Access to system files: Regular users can only access their own files, while administrative users can access all files on the system.
4. Access to system settings: Regular users can only access settings that affect their own user account, while administrative users can access and change all system settings.
5. Ability to create new users: Only administrative users have the ability to create new users.
6. Ability to access the root account: Only administrative users have the ability to access the root account, which is the highest level of access on a Linux system.
7. Security: Regular users are less likely to accidentally cause damage to the system because of their limited permissions and access, while administrative users have the potential to cause more damage if they are not careful.
8. User accounts with administrative privileges are called superuser or root account, they have the ability to run any command and make any change to the system. Regular users are also called standard users they are limited in their ability to make changes to the system and run certain commands.

Understanding user; group; and password management in RHEL:

User, group, and password management are important tasks in managing a Red Hat Enterprise Linux (RHEL) system.

User management:

- A user is a person who has an account on a Linux system and can log in to it.
- Each user has a unique username and a set of associated data, such as a user ID (UID), a group ID (GID), and a home directory.
- Users can be added, deleted, and modified using the command line tools like useradd, userdel and usermod.

Group management:

- A group is a collection of users.
- Each user belongs to one or more groups, and each group has a unique group name and a GID.

- Groups can be added, deleted, and modified using the command line tools like groupadd, groupdel and groupmod.

Password management:

- A password is a secret string of characters that is used to authenticate a user.
- Passwords can be set, changed, and expired using the command line tools like passwd, chage.
- It is also important to set good password policies to ensure security of the system.

It is important to note that, in Red Hat Enterprise Linux, the root user has the highest level of access and permissions on the system, and should be used with caution. Additionally, it is important to regularly review and update user and group information, as well as review and enforce password policies to ensure the security of the system.