Module II: Users and Group Management

Part III

Creating User and Group by using command in RHEL:

In Red Hat Enterprise Linux (RHEL), users and groups can be created, modified, and deleted using command line tools.

To create a user, the command "useradd" can be used. The basic syntax is:

useradd [options] username

For example, to create a user named "john" with a home directory in the default location, the command would be:

useradd john

To create a user with a specific UID and GID, you can use the -u and -g options respectively:

useradd -u 1001 -g 1001 john

To create a group, the command "groupadd" can be used. The basic syntax is:

groupadd [options] groupname

For example, to create a group named "marketing":

groupadd marketing

To add a user to a group, the command "usermod" can be used with the -aG option. The basic syntax is:

usermod -aG groupname username

For example, to add user "john" to the "marketing" group:

usermod -aG marketing john

It is important to note that these commands must be run as the root user or with sudo privilege.

Commands of Modify User and Group in Linux:

In Linux, users and groups can be modified using command line tools like usermod and groupmod.

To modify a user, the command "usermod" can be used. The basic syntax is:

usermod [options] username

For example, to change the home directory of a user named "john" to a new location:

usermod -d /home/john2 -m john

To change the UID and GID of a user, you can use the -u and -g options respectively:

usermod -u 1002 -g 1002 john

To modify a group, the command "groupmod" can be used. The basic syntax is:

groupmod [options] groupname

For example, to change the name of a group named "marketing" to "sales":

groupmod -n sales marketing

To remove a user from a group, you can use the -G option with usermod and exclude the group from the list of groups:

usermod -G group1,group2 john

This command will remove user 'john' from all the other groups except group1 and group2.

It is also possible to remove a user from a group by using the command 'gpasswd' with the -d option:

gpasswd -d john groupname

This command will delete user 'john' from the groupname.

Home Directories and /etc/skel

The /etc/skel directory contains default environment files for new accounts. The useradd command and the Red Hat User Manager copies these files to the home directory for new users. The contents of /etc/skel may vary. While the standard files in this directory are hidden, administrators are free to add more files for new users. Standard files from one copy of /etc/skel are described in Table.

File	Purpose
.bashrc	This basic bash configuration file may include a reference to the general /etc/bashrc configuration file. Can include commands to run when the bash shell is started. One example is an alias such as **rm='rm -i'**.
.bash_logout	This file is executed when you exit a bash shell and can include commands appropriate for this purpose, such as commands for clearing a screen.
.bash_profile	Configures the bash startup environment. Appropriate place to add environment variables or modify the directories in your user account PATH.
.gnome2/	Includes settings for the GNOME Desktop Environment
.kde/	Specifies settings for the K Desktop Environment. Not added to /etc/skel and not copied to user home directories if KDE is not installed.
.mozilla/	Includes options associated with the Firefox web browser, developed by the Mozilla project.

/etc/bashrc

The /etc/bashrc file is used for aliases and functions, on a system-wide basis. Open this file in the text editor of your choice. Read each line in this file. Even if you don't understand the programming commands, you can see that this file sets the following bash shell parameters for each user. For example:

■ It assigns a value of umask, which creates the default permissions for newly created files. It supports one set of permissions for root and system users (with user IDs below 200), and another for regular users. (Officially, RHEL reserves all user IDs above 500 for regular users; however, that is not reflected in /etc/bashrc.)

■ It assigns and defines a prompt, which is what you see just before the cursor at the command prompt.

■ It includes settings from *.sh files in the /etc/profile.d/ directory. The settings here are supplemented by the .bashrc file in each user's home directory. The settings are supplemented by the .bash_profile and .bash_logout files in each user's home directory.

The Proper Use of the su Command:

The "su" command in Linux and Unix-like operating systems is used to switch the current user to another user, usually to gain root or superuser privileges. The basic syntax of the command is:

su [username]

For example, if a user wants to switch to the root user, they would run the command:

su root

The user will then be prompted to enter the root user's password. If entered correctly, the user will now be logged in as the root user and will have all the privileges and permissions of the root user.

It is important to use the su command properly to avoid security risks.

1. Always log in as a regular user and only use su when necessary.
2. Never run commands as the root user unless it is absolutely necessary.
3. Use the "su -" option instead of just "su" to switch to the root user's environment fully.
4. Avoid logging in as the root user directly.
5. Always use "sudo" command instead of "su" when possible.

Using the su command improperly can lead to serious security issues, such as giving unauthorized users access to sensitive information or allowing them to make changes to the system that could cause problems. Therefore, it is important to use the su command with care and to always be aware of the risks involved.

Limit Access to su in RHEL:

In RHEL 6, you can limit access to the **su** command by modifying the **/etc/pam.d/su** file.

1. Open the **/etc/pam.d/su** file in a text editor.
2. Look for the line that starts with **auth** and ends with **pam_wheel.so use_uid**.
3. Change **pam_wheel.so use_uid** to **pam_wheel.so use_uid group=wheel**.
4. Save and close the file.
5. Add users to the **wheel** group that you want to allow to use the **su** command.
6. All other users will now be denied access to the **su** command.

Note: This will only limit access to the command line, GUI based su or sudo will still work.