RHSA1

Red hat System Administration 1

osama-amin98

Osama Amin

- Cloud Engineer at Eventum IT Solutions
- ITI Instructor
- RHCSA
- CKA

Course Plan

Day 02

- User and group administration
- Managing Users
- Ownership and Permissions
- Umask
- Sudo
- Shutdown and Reboot
- LAB 2

Notes
Before LAB

User and Group

- Root super user - full system access uid=0
- system users 1-999
- normal users 1000+

Files:

- /etc/passwd information about each user in the system
- /etc/shadow hash passwords of the users
- /etc/group information about each group in the system

- Each user has 1 primary group and (n) of secondary groups

- When you create a user the system create a group named the same name of the user and assign this group as a primary group of this user

Managing Users and Groups

useradd [options] username	To add user
usermod [options] username	To Modify existing user
userdel [options] username	To delete user
groupadd [options] groupname	To add group
passwd <username>	To change password
chage [options] username	To change user password expiry information
Su - <username>	To Switch user

Ownership and Permissions

Effects of Permissions on Files and Directories

Permission	Effect on files	Effect on directories
r (read)	File contents can be read.	Contents of the directory (the file names) can be listed.
w (write)	File contents can be changed.	Any file in the directory can be created or deleted.
x (execute)	Files can be executed as commands.	The directory can become the current working directory. You can run the cd command to it, but it also requires read permission to list files there.

Ownership and Permissions

- **chmod [OPTIONS] [ugoa...][+-=][rwx] FILE/DIR** **to change permissions**
- u user, g group, o other, a all (for user, group, other, all)
- + add, - remove, = set exactly (for add, remove, set exactly)
- r read, w write, x execute (for read, write, execute)

- **chmod ### FILE/DIR** **(numeric way)**
- READ 4
- WRITE 2
- EXECUTE 1

To Change Ownership:

- chown user dir/file
- chown :group dir/file
- chown user:group dir/file

- **Umask:**
- To control the initial permissions of the file or dir, the default value is 0002
- file = 666-002 = 644 (rw-rw-r--)
- dir = 777-002 = 775 (rwxrwxr-x)

- **Reboot commands:**
- init 6
- reboot
- systemctl reboot
- shutdown -r now

Shutdown commands:

- init 0
- poweroff
- systemctl poweroff
- shutdown -h now

LAB 02

1. Create a user account with the following attribute
   Username: ali
   Fullname/comment: ali iti
   Password: ali

2. Create a user account with the following attribute
   Username: baduser
   Full name/comment: Bad User
   Password: baduser

LAB 02

3. Create a supplementary (Secondary) group called pgroup with group ID of 30000
4. Create a supplementary group called badgroup
5. Add ali user to the pgroup group as a supplementary group
6. Modify the password of ali’s account to *password*
7. Modify ali’s account so the password expires after 30 days
8. Lock bad user account so he can't log in
9. Delete bad user account
10. Delete the supplementary group called badgroup.

LAB 02

11. Create a folder called myteam in your home directory and change its permissions to read only for the owner.
12. Log out and log in by another user
13. Try to access (by cd command) the folder (myteam)
14. Using the command Line: Change the permissions of oldpasswd file to give owner read and write permissions and for group write and execute and execute only for the others (using chmod in 2 different ways)
15. Change your default permissions to be no permission to everyone then create a directory and a file to verify.

LAB 02

16. Create a file with permission 444. Try to edit in it and to remove it? Note what happened
17. What is the difference between the “x” permission for a file and for a directory?
18. What are the minimum permission needed for:

    Copy a directory (permission for source directory and permissions for target parent directory)

    Copy a file (permission for source file and and permission for target parent directory)

    Delete a file

    Change to a directory

    List a directory content (ls command)

    View a file content (more/cat command)

    Modify a file content