Linux Servers

Classroom Assignment 2 – Users, groups, owners and permissions

Mikael Romanov

Document your commands or take screenshots. Answer questions in english or finnish.

1. Users

Add new user accounts with the names *admin* and *sulo*. Also add user with your own student-id (ex. e6210). Set a password for all users. Keep names lowercase.

Here I added 3 new users with the command **adduser**.

```
[root@localhost ~]# adduser admin
[root@localhost ~]# adduser sulo
[root@localhost ~]# adduser k1521
```

Because the adduser command doesn't add a password for a user, we have make it separetaly with **passwd** command:

```
[root@localhost ~]# passwd admin
Changing password for user admin.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@localhost ~]# passwd sulo
Changing password for user sulo.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@localhost ~]# passwd k1521
Changing password for user k1521.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

Check with the id command what user ids are assigned to users?

Since the user are not administrative, the id starts from 1000 > ****:

```
login as: admin
admin@192.168.1.103's password:
[admin@localhost ~]$ id -u
1000
[admin@localhost ~]$ su - sulo
Password:
[sulo@localhost ~]$ id -u
1001
[sulo@localhost ~]$ su - k1521
Password:
[k1521@localhost ~]$ id -u
1002
```

2. Group and sudo

Add a group named engineers and add your student-id account to the group (as a secondary group). Wheel-group is already created, add the admin account to that group. Log on as admin and test that you can use sudo now. Log on as sulo and check what error message you get when you try to use sudo?

In the future assignments, use the admin account and sudo when configuring.

Centos has a default group called wheel, which gives sudo privlidges for user. I added **admin** to the **wheel** group with command usermod –aG groupname username. –a adds user to a supplementary group and it is suggested to only use with the –G option (groupname):

```
[root@localhost ~]# usermod -aG wheel admin
[root@localhost ~]# groupadd engineers
[root@localhost ~]# usermod -aG engineers k1521
```

Here I'm testing that the **Admin** has sudo privlidges

```
[admin@localhost ~]$ sudo passwd k1521
Changing password for user k1521.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

And the results of a non sudoer is here, the attempt will be logged and can be viewed later on:

```
[sulo@localhost ~]$ sudo passwd k1521

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for sulo:
sulo is not in the sudoers file.  This incident will be reported.
```

3. Permissions

Create a directory /home/help. Set the following for the folder:

- Owner admin
- Group engineers
- Permissions: Owner and group has all, others have read and execute.

Set the permissions numerically.

I made a folder called help in /home/ with the command **mkdir.** Then changed the owner and group with command **chown** (chown owner:group file/folder). After that I changed the permission numerically with **chmod** (user,group,other). 4 = read 2=write and 1=execute. Can be changed also with chmod u=rwx,g=rwx,o=rx.

```
[admin@localhost ~]$ mkdir help
[admin@localhost ~]$ sudo chown admin:engineers help
[admin@localhost ~]$ sudo chmod 775 help
[admin@localhost ~]$ ls -lah
total 16K
drwx------. 5 admin admin     4.0K Oct 13 20:35 .
drwxr-xr-x. 5 root  root        41 Oct 13 20:17 ..
-rw-r--r--. 1 admin admin       18 Mar  6  2015 .bash_logout
-rw-r--r--. 1 admin admin      193 Mar  6  2015 .bash_profile
-rw-r--r--. 1 admin admin      231 Mar  6  2015 .bashrc
drwxrwxr-x. 3 admin admin       17 Oct 13 20:23 .cache
drwxrwxr-x. 3 admin admin       17 Oct 13 20:23 .config
drwxrwxr-x. 2 admin engineers    6 Oct 13 20:35 help
```

I made the folder to a wrong directory so i moved it:

```
[admin@localhost ~]$ sudo mv help /home/
```

Log on as your student-id account and make a new file in the help directory. Log on as sulo and test that you can read the file but cannot modify it or create new files in the directory.

Here I'm testing with k1521 that I can make a file :

```
[k1521@localhost home]$ cd help
[k1521@localhost help]$ touch help.txt
[k1521@localhost help]$ ls -l
total 0
-rw-rw-r--. 1 k1521 k1521 0 Oct 13 20:41 help.txt
```

Here I'm testing with sulo that I can't make a file or modifie a existing one:

```
[sulo@localhost help]$ touch doesntwork.txt
touch: cannot touch 'doesntwork.txt': Permission denied
[sulo@localhost help]$ nano help.txt
```

```
[ Error writing help.txt: Permission denied ]
```

4. Locking/unlocking user

Lock the password for user sulo and test that you cannot log on. Remove the lock.

Here I locked sulos password with **passwd –l username** (-l=lock)

```
[admin@localhost help]$ sudo passwd -l sulo
[sudo] password for admin:
Locking password for user sulo.
passwd: Success
[admin@localhost help]$ su sulo
Password:
su: Authentication failure
```

I restored the password with **passwd –u** (-u=unlock)

5. Configuration file example

Configure NTP. Open */etc/chrony.conf* and determine what syntax is used (what marks a comment, how is a parameter configured). What lines mark the used NTP servers? Comment these lines and add a new line that makes the NTP server *ntp.labranet.jamk.fi*.

```
[admin@localhost help]$ sudo nano /etc/chrony.conf
```

The commenting syntax is a #. I commented the ntp servers and added a new line:

```
# Use public servers from the pool.ntp.org project.
# Please consider joining the pool (http://www.pool.ntp.org/join.html).
#server 0.centos.pool.ntp.org iburst
#server 1.centos.pool.ntp.org iburst
#server 2.centos.pool.ntp.org iburst
#server 3.centos.pool.ntp.org iburst
ntp.labranet.jamk.fi
```

6. Logs

Find in the logs or journal (use grep or journalctl):

- When the system has booted
  /var/log/messages

```
Oct  5 20:27:59 localhost rsyslogd: [origin software="rsyslogd" swVersion="7.4.7" x-pid="556" x-info="http://www.rsyslog.com"] start
```

- When you created the admin account
  /var/log/secure

```
Oct 13 20:17:26 localhost useradd[2490]: new group: name=admin, GID=1000
Oct 13 20:17:26 localhost useradd[2490]: new user: name=admin, UID=1000, GID=1000, home=/home/admin, shell=/bin/bash
```

- When sulo tried to use sudo and when he tried to log with the locked password
  /var/log/secure

```
Oct 13 20:44:52 localhost sudo: admin : TTY=pts/0 ; PWD=/home/help ; USER=root ; COMMAND=/bin/passwd -l sulo
Oct 13 20:45:05 localhost unix_chkpwd[3945]: password check failed for user (sulo)
Oct 13 20:45:05 localhost su: pam_unix(su:auth): authentication failure; logname=admin uid=1000 euid=0 tty=pts/0 ruser=admin rhost=  user=sulo
```