

Managing Users and Groups

Managing User Accounts

Managing User Accounts



- The management of users in all linux system is governed by multiple files. These files dictate how the users will be created and what configuration applies to these users.
- Understanding the purpose of these files is canonical to the understanding of how users and groups work on in Linux.

`/etc/login.defs`
`/etc/default/useradd`
`/etc/skel/`
`/etc/passwd`
`/etc/shadow`
`/etc/group`

The /etc/passwd file

The /etc/passwd file



- The /etc/passwd file stores information about every account in a Linux system.
- Each line in the passwd file represents a user. When an account is created, a new entry is added.
- Entries in the passwd file contains 7 fields divided by a :
- The /etc/passwd file's record fields

Field No.	Description
1	User account's username.
2	Password field. Typically this file is no longer used to store passwords. An x in this field indicates passwords are stored in the /etc/shadow file.
3	User account's user identification number (UID).
4	User account's group identification number (GID)
5	Comment field. This field is optional. Traditionally it contains the user's full name.
6	User account's home directory.
7	User account's default shell. If set to /sbin/nologin or /bin/false, then the user cannot interactively log into the system.

Creating a user with useradd

Creating a user with useradd



- **-md** are the options needed for adding a home directory to the new user.
- **/home/student** is the new user's home directory.
- **-s** used for specifying the users login shell.
- **/bin/bash** the new user's login shell
- **student** the user's username.

```
adrian@server-inspiron:~$ sudo useradd -md /home/student -s /bin/bash student
[sudo] password for adrian:
adrian@server-inspiron:~$ _
```

Short	Long	Descriptions
-d	--delete	Removes the account's password.
-e	--expire	Sets an account's password as expired. User is required to change account password at next login.
-i	--inactive	Sets the number of days after a password has expired and has not been changed until the account will be deactivated.
-l	--lock	Places an exclamation point (!) in front of the account's password within the /etc/shadow file, effectively preventing the user from logging into the system via using the account's password.
-n	--minimum	Sets the number of days after a password is changed until the password may be changed again.
-S	--status	Displays the account's password status.
-u	--unlock	Removes a placed exclamation point (!) from the account's password within the /etc/shadow file.
-w	--warning or --warndays	Sets the number of days a warning is issued to the user prior to a password's expiration.
-x	--maximum or --maxdays	Sets the number of days until a password change is required. This is the password's expiration date.

Managing Groups

Managing Groups

- Groups are organizational structures that are part of Linux's discretionary access control (DAC).
- DAC is the traditional Linux security control, where access to a file, or any object, is based upon the user's identity and current group membership.
- When a user account is created, it is given membership to a particular group, called the account's default group.

```
adrian@server-inspiron:~$ cat /etc/passwd | grep "adrian"  
adrian:x:1000:1000:adrian:/home/adrian:/bin/bash  
adrian@server-inspiron:~$ cat /etc/group | grep ^"adrian"  
adrian:x:1000:  
adrian@server-inspiron:~$
```

Next (→)