

CYBR 4423

Unix/Linux Administration

User

Overview

Understand where user information is stored in Linux

Learn commands to manage users and groups

Basic Concepts

Linux/Unix is built as a multi-user environment

Each user has a unique

- Username, for login

- User ID (UID), an internal numeric value

Each user must also belong to at least one group (called the primary group)

- A group is a collection of users established by the system administrator.

- Users may belong to multiple groups.

- Groups also have unique identifiers, called group IDs (GIDs).

The "root" Account

The "root" user is the versatile system administrator of the OS

often called a super user

Special privileges

The "root" user is allowed to access all files and programs in the system, whether or not it owns them

It has read/write access to all files - regular file permissions do not apply

Its home directory is usually /root

User Information Storage

Linux takes the path of traditional UNIX and keeps all user information in straight text files

/etc/passwd

This file stores the user information including login, encrypted password entry, UID, default group, user information (comma separated, sometimes called GECOS), home directory, and login shell.

/etc/shadow

This file keeps encrypted passwords and password policies.

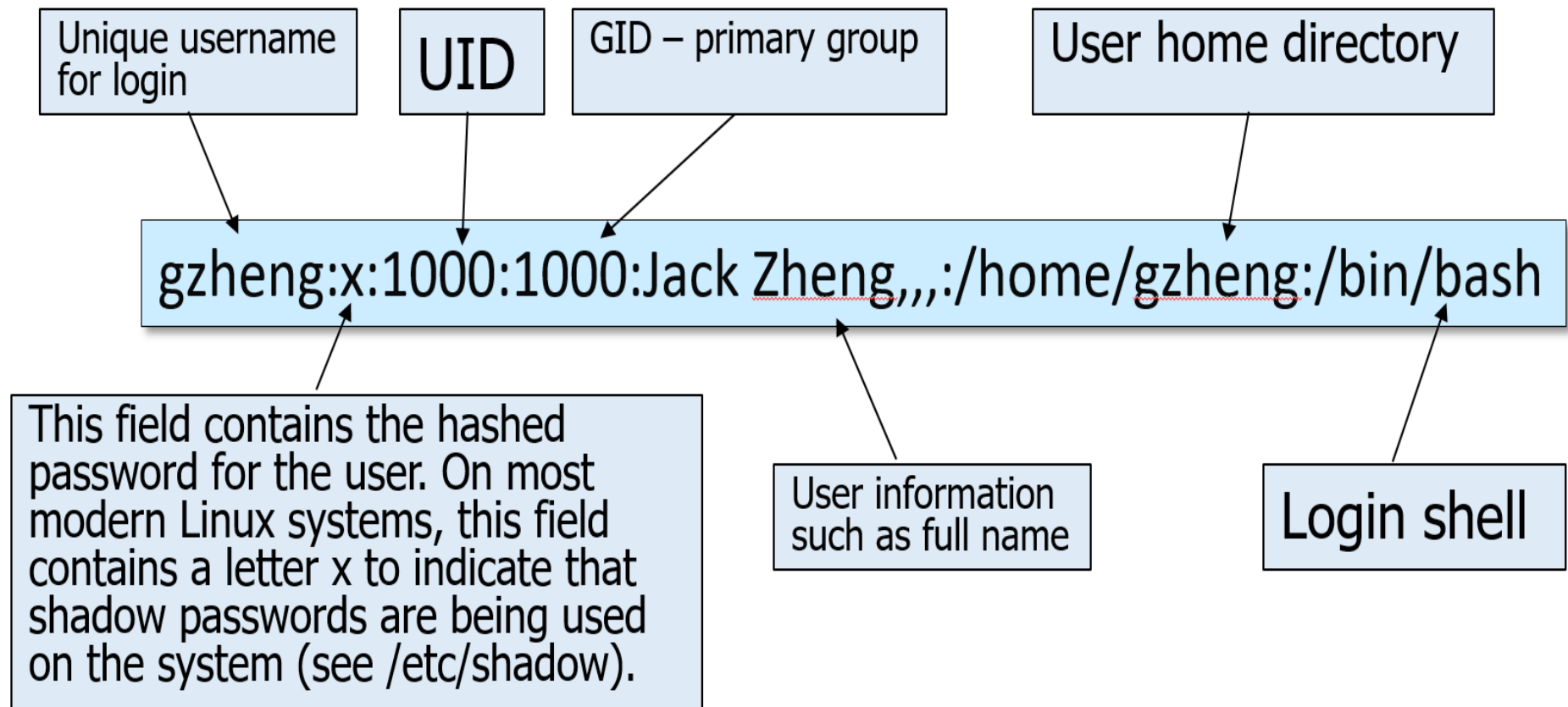
/etc/group

This files keeps information about groups and group members.

/etc/passwd

Each line in the file represents information about a user

The lines are made up of various standard fields, each delimited by a colon.



User Information

Username

Usually use lowercase – note this is case sensitive
Use letter, numbers, _ and -

UID

A unique numeric value for a user
"root" is always 0

Home directory

"root" user	/root
Other users	/home/[userid]

This is only for consistency; it can be somewhere else with another directory name.

Login shell

The default way of login
Use "/bin/false" to deny shell login (usually for reserved accounts)

/etc/shadow

Each line in the /etc/shadow file represents information about a user. This information includes:

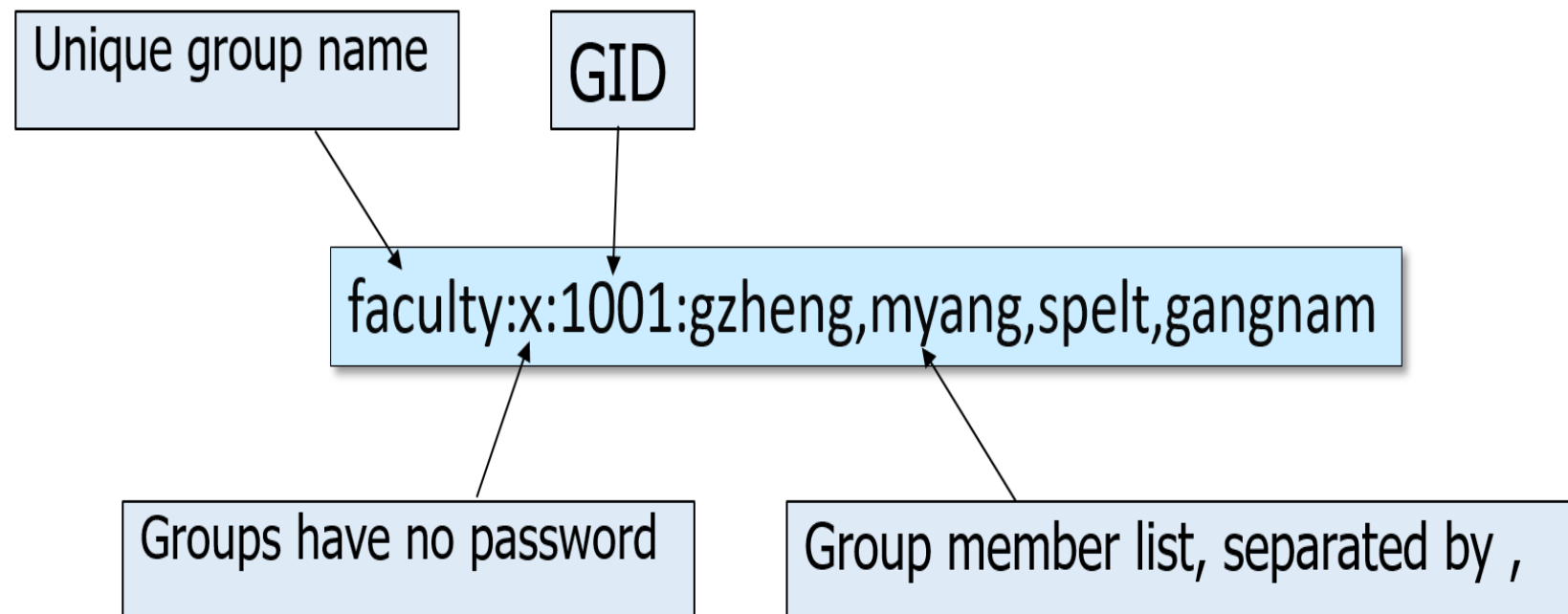
- User login name
- Encrypted password
- Password change and expiration information



/etc/group

Each line in the file represents information about a group

The lines are made up of various standard fields, each delimited by a colon.



Group Information

Group name

If you run "ls -l" command, you will see this name printed in the group field

Password

Generally password is not used, hence it is empty/blank

Group ID (GID)

A unique numeric value for a group

Group list

It is a list of user names of users who are members of the group. The user names, must be separated by commas.

Defaults

/etc/skel

When a new user is created, the default files and directories created in his/her home directory are stored in /etc/skel

This directory can be modified to fit your needs.

Modifications only effect new users and does not change anything for existing users

Common files for new users: .bashrc, .profile

/etc/default/useradd

Default values for account creation.

User Management Tools

User admin

useradd, userdel, usermod
passwd (assign password)

Group admin

groupadd, groupdel, groupmod

User/group query

id, groups, grep (from /etc/passwd)
who, w

Others

su, sudo

useradd - Add New Users

Options:

- d Home directory
- s Starting program (shell)
- g Primary group assigned to the users
- G Other groups the user belongs to
- m Create the user's home directory (mkdir)

Example: To add a new user with

a login name of "roger"

home directory of "/home/roger"

will create the home directory

a primary group of "students"

a second group of "assistants"

starting shell of "/bin/bash"

Note space is optional between
the option letter and the value

```
#> useradd -gstudents -Gassistants -s/bin/bash -d/home/roger -m roger
```



usermod - Change User Info

Options (the same as the useradd):

- d home directory
- p password
- g Primary group assigned to the users
- G Other groups the user belongs to
- a append other groups, only used with -G

Example: change user "roger"

Change the main group to "assistants"

Also add "roger" to the group "students" and "staff" (and remove from other groups)

```
#> usermod -gassistants -Gstudents,staff roger
```

Other groups are separated by comma, no space between

userdel - Delete Users

Options:

-r Remove home directory as well

Example

Remove the user 'roger' and his home directory

```
#> userdel -r roger
```

passwd – Password Admin

Options

- a, --all
report password status on all accounts, must used with -S
- S, --status
report password status on the named account
- e, --expire
force to expire the password for the named account – forcing change of password
- l, --lock
lock the password of the named account
- u, --unlock
unlock the password of the named account

Example

Reference

```
#> passwd roger
```

```
#> passwd -Sa
```



Group Admin

groupadd

groupmod

```
#> groupadd student_group
```

gro

-n for new group name

```
#> groupmod -n students student_group
```

```
#> groupdel students
```

su - Switch User

su

Switch to another user without logging out

To return to original user, enter "exit"

Example:

To switch to root account

```
#> su
```

To switch to the user 'roger'

```
#> su roger
```

sudo (su+do)

Elevate the user's privilege to "root" when required (for example, when installing software), if the current user belongs to the "sudo" group, or in the /etc/sudoers file

Example

```
#> sudo passwd root
```

Lock/Unlock "root" Account

Enable root account

With any "sudo" group user, enter:

```
sudo passwd root
```

Relocking the root account

If you decide you want to lock the root account after unlocking it, give the command

```
sudo passwd -l root
```

You can unlock it again with the preceding command.

User/Group Query

"id" command

Get a user's UID, GID, and groups information

"groups" command

Get all groups a user is in

Search for users

Use grep with a phrase or regex to search /etc/passwd

Get group members

Use grep with a phrase or regex to search /etc/groups

User Monitoring

"w" and "who"

Displays information about the users currently on the machine, and their processes

"who am i" or "whoami"

Display the current username

/var/log/auth.log

This log file records user login history

Change Owner and Groups

chown – change file owner

chown [user] [file]

```
#> chown gzheng file1
```

chgrp – change user group of a file

2 ways

```
#> chgrp faculty file1  
#> chown :faculty file1
```

faculty is the group

Limitations

Limitations of the traditional Linux permission system

File oriented, not user oriented

Only one user and one group can be granted rights to a file or directory at one time.

Alternatives

Access Control List (ACL)

[FilePermissionsAcls](#)

[News](#)

Summary

Key concepts

User, group, UID, GID
Shadow (password)

Files summary

/etc/passwd, /etc/group, /etc/shadow
/etc/skel/, /etc/default/useradd
/var/log/auth.log

Commands summary

useradd, userdel, usermod, adduser
passwd
groupadd, groupdel, groupmod
who, w, id, groups
su, sudo
chown, chgrp

Good Readings and Resources

[Quick reference](#)

[Command list](#)

group and passwd file

[Understanding etc passwd file format](#)

[Understanding etc group file](#)

[Why shadow the passwd file?](#)

Scripting user management

Newusers

Chage

More on shadow file and encoded password and expiration

Utilities

mkpasswd

Scripting user management

- access control list

Password policy

check password strength using regex

Never ever login as root for non admin related tasks

Always use a regular user account for all normal tasks

Admin tasks

- Create new accounts
- Lock or delete accounts
- Create groups
- Assign users to groups
- Reset passwords
- Set password policy
- Query uses and groups