Tài khoản NSD và phân quyền truy cập tệp

Nội dung

- Khái niệm NSD và nhóm NSD
- Quản lý NSD và nhóm NSD
- Khái niệm quyền truy cập
- Quyền truy cập của file
- Quyền truy cập của thư mục
- Quản lý quyền truy cập

Khái niệm người sử dụng

- NSD thông thường
- Quản trị
- Nhóm NSD
- Tạo một người sử dụng
  - Tên, Mật khẩu, home của người sử dụng (/home/tên)
  - Nhóm (một người sử dụng có thể thuộc một hoặc nhiều nhóm, tuy nhiên cần phải xác định một nhóm chính)
  - Tất cả các thông tin về người sử dụng được lưu trong file:

  /etc/passwd

/etc/passwd

- **Username:password:UID:GID:Info:Home:Shell**
- **Username**: It is used when user logs in. It should be between 1 and 32 characters in length.
- **Password**: An x character indicates that encrypted password is stored in /etc/shadow file.
- **User ID (UID)**: Each user must be assigned a user ID (UID). UID 0 (zero) is reserved for root and UIDs 1-99 are reserved for other predefined accounts. Further UID 100-999 are reserved by system for administrative and system accounts/groups.
- **Group ID (GID)**: The primary group ID (stored in /etc/group file)
- **User ID Info**: The comment field. It allow you to add extra information about the users such as user's full name, phone number etc. This field use by finger command.
- **Home directory**: The absolute path to the directory the user will be in when they log in. If this directory does not exists then users directory becomes /
- **Command/shell**: The absolute path of a command or shell (/bin/bash). Typically, this is a shell. Please note that it does not have to be a shell.

/etc/shadow

- **User:Pwd:Last pwd change :Minimum:Maximum:Warn:Inactive :Expire**
- User name : It is your login name
- Password: It your encrypted password. The password should be minimum 6-8 characters long including special characters/digits
- Last password change (lastchanged): Days since Jan 1, 1970 that password was last changed
- Minimum: The minimum number of days required between password changes i.e. the number of days left before the user is allowed to change his/her password
- Maximum: The maximum number of days the password is valid (after that user is forced to change his/her password)
- Warn : The number of days before password is to expire that user is warned that his/her password must be changed
- Inactive : The number of days after password expires that account is disabled
- Expire : days since Jan 1, 1970 that account is disabled i.e. an absolute date specifying when the login may no longer be used

Nhóm người sử dụng

- Mỗi người sử dụng có thể thuộc về một hoặc nhiều nhóm
  - Một nhóm = tên nhóm + danh sách các thành viên
  - Khả năng chia sẻ các file giữa những người sử dụng trong cùng một nhóm.
  - Danh sách các nhóm được lưu trữ trong file: /etc/group
  - root có khả năng tạo ra các nhóm bổ xung, ngoài các nhóm mà hệ điều hành đã ngầm định

/etc/group

- **group_name:Password:Group ID (GID): Group List**
- group_name: It is the name of group. 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. It can store encrypted password. This is useful to implement privileged groups. X means passwd is stored in /etc/gshadow
- Group ID (GID): Each user must be assigned a group ID. You can see this number in your /etc/passwd file.
- 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.

/etc/gshadow

- *Group name* — The name of the group. Used by various utility programs as a human-readable identifier for the group.
- *Encrypted password* — The encrypted password for the group. If set, non-members of the group can join the group by typing the password for that group using the newgrp command. If the value of this field is !, then no user is allowed to access the group using the newgrp command. A value of !! is treated the same as a value of ! — however, it also indicates that a password has never been set before. If the value is null, only group members can log into the group.
- *Group administrators* — Group members listed here (in a comma delimited list) can add or remove group members using the gpasswd command.
- *Group members* — Group members listed here (in a comma delimited list) are regular, non-administrative members of the group.

Công cụ

- useradd/mod/del
- passwd
- groupadd/mod/del
- gpasswd
- sg/newgrp
- su
- users/groups
- id

Các quyền

- Mỗi file luôn thuộc về một người sử dụng và một nhóm xác định
  - Người tạo ra file hoặc thư mục sẽ là người sở hữu, nhóm chứa người tạo ra file hoặc thư mục sẽ là nhóm sở hữu đối với file/thư mục.
- Sự phân quyền cho phép xác định rõ các quyền mà người sử dụng có đối với một file hoặc một thư mục.

Quyền truy cập

- r : đọc
  - Cho phép hiển thị nội dung của file hoặc thư mục
- w : ghi
  - Cho phép thay đổi nội dung của file
  - Cho phép thêm hoặc xóa các file trong một thư mục
- x : thực thi
  - Cho phép thực thi file dưới dạng một chương trình
  - Cho phép chuyển đến thư mục cần truy cập

Các nhóm người sử dụng

- Có 3 nhóm người sử dụng đối với 1 file/ thư mục:
  - u (người sở hữu) : người sở hữu duy nhất của file
  - g (group) : những người sử dụng thuộc nhóm chứa file
  - o (others) : những người sử dụng khác, không phải là người sở hữu file cũng như không thuộc nhóm chứa file.
- Mỗi nhóm người sử dụng sẽ có một tập các quyền (r, w, x) xác định.

Ví dụ

```
$ ls -l
----rw-rw- 1 tuananh  user1   16 Feb 10 19:12 test1.txt
-rw-rw-rw- 1 tuananh  user1   16 Feb 10 19:12 test2.txt
drw-r--r-- 2 tuananh  user1  512 Feb 10 19:14 vanban
$ whoami
tuananh
$ cat test1.txt
cat: test1.txt: Permission denied
$ cat test2.txt
Un fichier de test
$ cp test2.txt vanban
cp: vanban: Permission denied
```

Các lưu ý

- Để có thể thêm các file, cần phải có quyền « w » đối với thư mục
- Để có thể xóa, thay đổi nội dung hoặc di chuyển 1 file, người sử dụng cũng cần phải có quyền « w » đối với thư mục
- Việc xóa một file còn phụ thuộc vào quyền đối với thư mục chứa file đó
- Để bảo mật các dữ liệu, người sở hữu file thậm chí có thể bỏ cả quyền đọc « r » đối với tất cả mọi người sử dụng khác.
- Để hạn chế quá trình truy cập vào hệ thống file, người sử dụng có thể bỏ quyền thực thi (x) đối với thư mục gốc của hệ thống file.

Một số quyền đặc biệt đối với các file thực thi

- set-uid: -rw**s** --- ---
  - Chương trình được chạy dưới quyền của người sở hữu
- set-gid: - --- rw**s** ---
  - Chương trình được chạy bởi các người sử dụng thuộc cùng nhóm với người sở hữu
- bit sticky
  - Với thư mục: chỉ có root và chủ sở hữu được xóa các tệp bên trong, người dùng khác không xóa được kể cả khi có quyền rwx
  - Với tệp: thực thi với bộ nhớ được nạp một lần

Ví dụ

```
$ ls -l /etc/shadow
-rw-rw---- 1 root  root  568 Feb 10 19:12 shadow
$ ls -l /bin/passwd
-rwsrws--x 1 root  root 3634 Feb 10 19:12 passwd
```

- Khi một người sử dụng thông thường gọi lệnh /bin/passwd, xem như người đó được « mượn » quyền root để thay đổi mật khẩu trong file /etc/shadow

Thay đổi quyền truy cập (1)

$chmod <mode> <files>

```
set_uid set-gid sticky user group other
                        rwx   --x   --x
   1       1       0    111   001   001
           6            7     1     1
```

```
$ chmod  6711  test
$ ls -l test
-rws--s--x  1  tuananh  user1  Mar 10 10:20  test
$ chmod  711  test
$ ls -l test
-rwx--x--x  1  tuananh  user1  Mar 10 10:20  test
```

Thay đổi quyền truy nhập (2)

$chmod <ugoa><+-=><rwsx> <files>

- u | g | o | a (all)
- Operation
  - + (thêm 1 hoặc 1 số quyền vào tập các quyền file đã có)
  - - (bỏ 1 hoặc 1 số quyền khỏi tập các quyền file đã có)
  - = (gán mới 1 hoặc 1 số quyền cho file)
- Quyền = r | w | x | s

Ví dụ

```
$ ls -l test.txt
-rw-rw-r-- 1 tuananh user1  150 Mar 19 19:12 test.txt
$ chmod o+w test.txt
$ ls -l test.txt
-rw-rw-rw- 1 tuananh user1  150 Mar 19 19:12 test.txt
$ chmod a-rw test.txt
$ ls -l test.txt
---------- 1 tuananh user1  150 Mar 19 19:12 test.txt
$ cat test.txt
cat: test.txt: Permission deniedZ
```

Định nghĩa các quyền ngầm định khi tạo ra 1 file

- Mỗi chương trình tạo tệp sẽ đặt một số quyền ngầm định ban đầu
  - VD: touch, echo, vi, gedit mặc định quyền rw-rw-rw-
- Thay đổi quyền ngầm định của 1 file khi tạo ra có thể được xác định bằng lệnh umask

$umask mode

- mode có bit 1 tương ứng với quyền sẽ bị cấm.

$umask 022

  - Số 0 có nghĩa là quyền của người sử dụng không bị hạn chế so với quyền mặc định
  - Số 2 =010 có nghĩa là quyền ghi (w) bị hạn chế.
- Quyền mặc định rw-rw-rw với umask 022 sẽ tạo ra file với quyền rw-r--r--

Thay đổi người sở hữu và nhóm

$chown [-R] <user> <files>

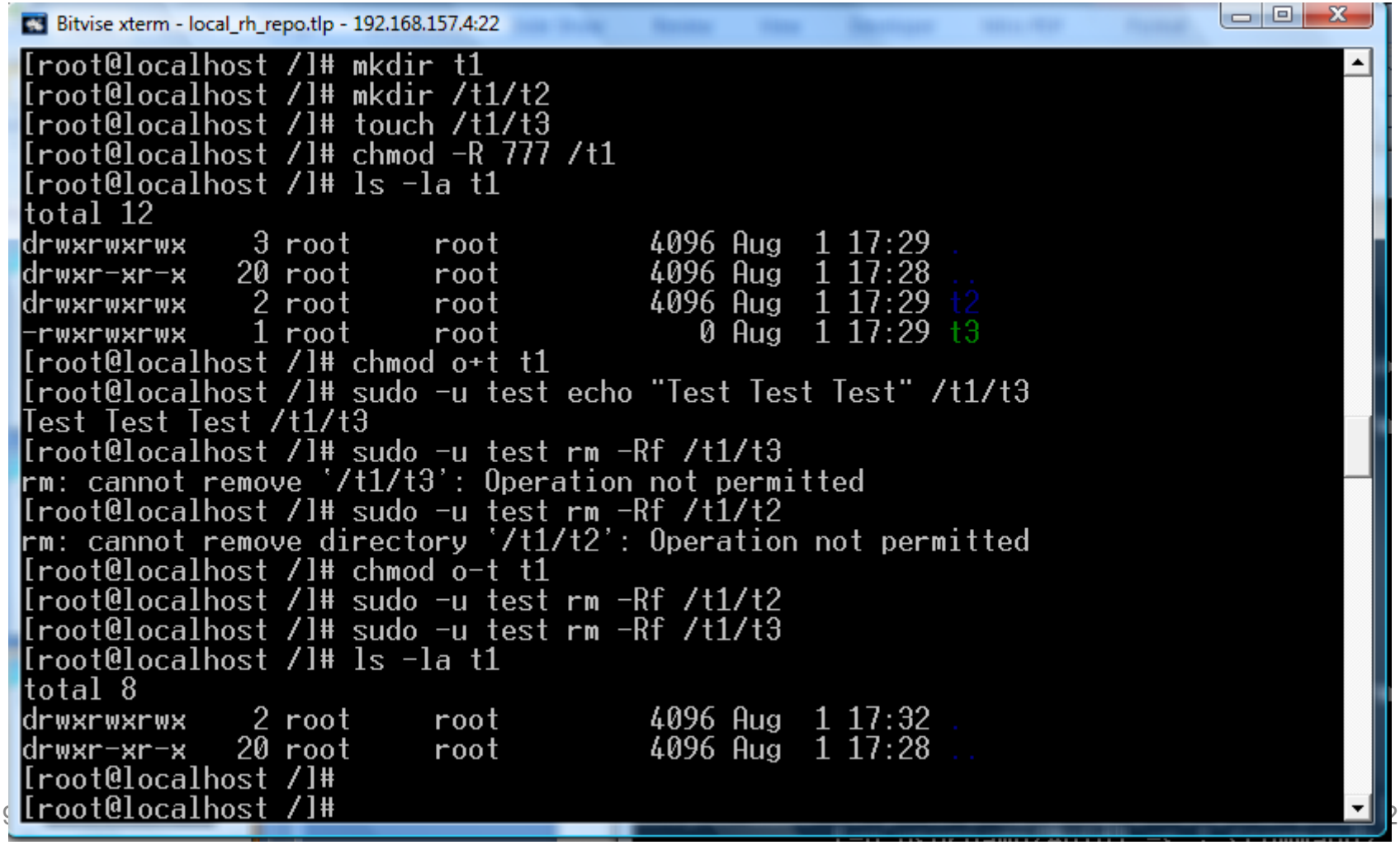
- Thay đổi người sở hữu của file

$chgrp <group> <files>

- Thay đổi nhóm của file
- Có thể sử dụng tùy chọn –R để lặp lại việc thực hiện các lệnh (ví dụ thực hiện việc thay đổi quyền sở hữu hoặc nhóm của mọi file trong cùng một thư mục)

- Các lệnh trên chỉ dành cho những người sử dụng có quyền root

Sticky bit example



Sticky bit example

```
[root@localhost /]# chmod o-t /t1
[root@localhost /]# ls -la /t1
total 12
drwxrwxrwx    3 root     root         4096 Aug  1 17:20 .
drwxr-xr-x   20 root     root         4096 Aug  1 17:19 ..
drwxr-xr-x    2 root     root         4096 Aug  1 17:20 t2
-rw-r--r--    1 root     root            0 Aug  1 17:20 t3
```

```
[test@localhost test]$ rm -Rf /t1/t2
[test@localhost test]$ rm -Rf /t1/t3
[test@localhost test]$ ~
```

Bài tập

- Tạo một tệp mới
- Cho biết quyền sử dụng của các nhóm đối tượng trên tệp
- Thay đổi quyền sử dụng của các nhóm đối tượng sao cho: chủ sở hữu chỉ có quyền ghi, nhóm sở hữu chỉ có quyền đọc, người dùng khác không có quyền gì
- Đổi chủ sở hữu về cho root

Suid bit-example

```
[root@localhost t1]# cat test2.c
#include <stdio.h>
main(int argc, char **argv)
{
  FILE *f;
    f = fopen("t1", "w");
    if (f == NULL) {
      exit(1);
    }
    fwrite("Testing only", sizeof(char), 12, f);
    fclose(f);
  }
[root@localhost t1]# gcc test2.c
[root@localhost t1]# ls -la
total 28
drwxrwxrwx    2 root     root         4096 Aug  1 19:46 .
drwxr-xr-x   20 root     root         4096 Aug  1 17:28 ..
-rw-r--r--    1 root     root            0 Aug  1 18:55 aaaaaat1
-rwxr-xr-x    1 root     root        11897 Aug  1 19:46 a.out
-r-sr-xr-x    1 root     root            3 Aug  1 18:41 test1
-rw-r--r--    1 root     root          196 Aug  1 19:45 test2.c
```

Suid bit-example

```
[root@localhost t1]# sudo -u test ./a.out
[root@localhost t1]# ls -la
total 32
drwxrwxrwx    2 root     root         4096 Aug  1 19:46 .
drwxr-xr-x   20 root     root         4096 Aug  1 17:28 ..
-rw-r--r--    1 root     root            0 Aug  1 18:55 aaaaaat1
-rwxr-xr-x    1 root     root        11897 Aug  1 19:46 a.out
-rw-r--r--    1 test     test           12 Aug  1 19:46 t1
-r-sr-xr-x    1 root     root            3 Aug  1 18:41 test1
-rw-r--r--    1 root     root          196 Aug  1 19:45 test2.c
[root@localhost t1]# chmod u-s a.out
[root@localhost t1]# ls -la a.out
-rwxr-xr-x    1 root     root        11897 Aug  1 19:46 a.out
[root@localhost t1]# rm -rf t1
[root@localhost t1]# sudo -u test ./a.out
[root@localhost t1]# ls -la t1
-rw-r--r--    1 test     test           12 Aug  1 19:47 t1
```