

CSE301 - Linux và phần mềm mã nguồn mở

Bài 07: Quản lý hệ thống tệp tin

dungkt@tlu.edu.vn



Nội dung



- 1) Phân quyền truy cập hệ thống tệp tin
- 2) Danh sách điều khiển truy cập

Mục tiêu bài học



- Phân quyền hệ thống tệp tin trên Linux:
 - Cách đọc quyền tệp tin, thư mục và các liên kết bằng lệnh ls;
 - Hiểu hệ thống số nhị phân được sử dụng bởi mặt nạ cho các tệp mới được tạo
 - Mặt nạ trên các hệ thống Linux là gì và nó được sử dụng để làm gì;
 - Làm thế nào để quản lý quyền truy cập trên các tệp tin và thư mục;
 - Các suid, sgid và sticky bit là gì;

Mục tiêu bài học



- Danh sách điều khiển truy cập:
 - Danh sách kiểm soát truy cập là gì và làm thế nào chúng có thể được đọc từ lệnh ls;
 - Cách đặt quyền cơ bản trên tệp bằng lệnh setfacl;
 - Cách đọc danh sách kiểm soát truy cập bằng lệnh getfacl;
 - Mặt nạ danh sách kiểm soát truy cập là gì và nên đọc nó như thế nào;
 - Mặc định danh sách kiểm soát truy cập là gì và làm thế nào để sử dụng chúng hiệu quả

1. Phân quyền truy cập hệ thống tệp tin



Hiểu biết cơ bản về quyền truy cập



- Trên các hệ thống Linux, các quyền cơ bản được chia thành hai loại:
 - **Quyền sở hữu (Ownership)**: người dùng và nhóm sở hữu tệp, nghĩa là họ đã tạo hoặc họ được chỉ định là chủ sở hữu của tệp hoặc thư mục.
 - **Quyền cho phép (Permission)**: được cung cấp quyền trên một tệp hoặc thư mục, biểu thị tập hợp các hành động mà người dùng có thể thực hiện; tùy thuộc vào tài khoản người dùng đăng nhập và nhóm thuộc về.

Ownership : User & Groups

```
○ ○ ○  
$ whoami  
devconnected  
$ groups  
devconnected sudo administrators
```

The terminal output shows the user 'devconnected' and their groups 'devconnected', 'sudo', and 'administrators'. Dotted arrows point from the text 'User' to the output of 'whoami' and from 'Groups' to the output of 'groups'.

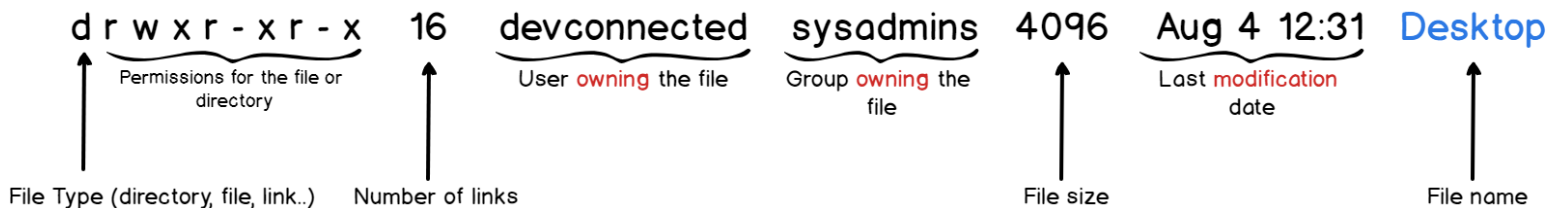
Xem danh sách các quyền truy cập



- Thực hiện với lệnh: `$ ls -al`

```
devconnected@debian-10:~$ ls -al
total 88
drwxr-xr-x 16 devconnected devconnected 4096 Aug  4 12:34 .
drwxr-xr-x  3 root          root          4096 Jul 30 17:31 ..
-rw-----  1 devconnected devconnected  786 Jul 30 17:36 .bash_history
-rw-r--r--  1 devconnected devconnected  220 Jul 29 17:51 .bash_logout
-rw-r--r--  1 devconnected devconnected 3526 Jul 29 17:51 .bashrc
drwx----- 14 devconnected devconnected 4096 Jul 30 14:52 .cache
drwx----- 14 devconnected devconnected 4096 Jul 30 17:44 .config
drwxr-xr-x  2 devconnected devconnected 4096 Jul 30 17:16 Desktop
```

- Biểu thị ý nghĩa của đầu ra:



Chúng ta sẽ chỉ tập trung vào các cột đầu tiên, thứ ba và thứ tư vì các cột khác không liên quan lắm đến các quyền.

Hiểu biết về các kiểu tệp Linux



- Trên Linux, mọi thứ đều là tệp, do vậy:
 - Liên kết là tệp, thư mục cũng là tệp.
 - Trong cột đầu tiên đầu ra của lệnh **ls**, chú ý đến **bit đầu tiên**.
 - Các tệp Linux có thể có nhiều loại, nhưng hầu hết chúng là:
 - Tệp (-), thư mục (d) hoặc liên kết (l).

```
devconnected@debian-10:~$ ls -al
total 88
drwxr-xr-x 16 devconnected devconnected 4096 Aug  4 12:34 .
drwxr-xr-x  3 root          root          4096 Jul 30 17:31 ..
-rw-----  1 devconnected devconnected  786 Jul 30 17:36 .bash_history
-rw-r--r--  1 devconnected devconnected  220 Jul 29 17:51 .bash_logout
-rw-r--r--  1 devconnected devconnected 3526 Jul 29 17:51 .bashrc
drwx----- 14 devconnected devconnected 4096 Jul 30 14:52 .cache
drwx----- 14 devconnected devconnected 4096 Jul 30 17:44 .config
drwxr-xr-x  2 devconnected devconnected 4096 Jul 30 17:16 Desktop
```



Type : File

Symbol : -



Type : Directory

Symbol : d



Type : Link

Symbol : l

Hiểu biết về quyền sở hữu tệp



- Hãy chú ý vào cột thứ 3 và cột thứ 4:
 - Cột thứ 3 thể hiện ai là người dùng sở hữu tệp tin (người chủ)
 - Cột thứ 4 thể hiện ai là nhóm sở hữu tệp tin

```
devconnected@debian-10:~$ ls -al
total 88
drwxr-xr-x 16 devconnected devconnected 4096 Aug  4 12:34 .
drwxr-xr-x  3 root          root          4096 Jul 30 17:31 ..
-rw-----  1 devconnected devconnected  786 Jul 30 17:36 .bash_history
-rw-r--r--  1 devconnected devconnected  220 Jul 29 17:51 .bash_logout
-rw-r--r--  1 devconnected devconnected 3526 Jul 29 17:51 .bashrc
drwx----- 14 devconnected devconnected 4096 Jul 30 14:52 .cache
drwx----- 14 devconnected devconnected 4096 Jul 30 17:44 .config
drwxr-xr-x  2 devconnected devconnected 4096 Jul 30 17:16 Desktop
```

Hiểu biết về quyền trên tệp tin



- Quyền trên **tệp tin**:
 - Các quyền được chia thành ba loại: quyền của người dung sở hữu (**u** - owner), quyền của nhóm (**g**roup) và quyền của người dùng khác (**o**ther).
 - Trên mỗi đối tượng, tồn tại cặp 3 kí tự có thể: dấu gạch ngang hoặc rwx.
 - **r**ead: quyền đọc; **w**rite: quyền ghi và **e**xecute cho phép để thực thi tệp.
 - **-** : không có sự cho phép.

Hiểu biết về quyền trên tệp tin



- Xét lại ví dụ: `-rw----- 1 devconnected devconnected 786 Jul 30 17:36 .bash_history`
 - Dấu gạch đầu tiên chỉ ra rằng `.bash_history` là một tệp.
 - Người sở hữu có các quyền sau: `rw-` có nghĩa là người dùng `devconnected` có thể đọc và ghi vào tệp nhưng không có quyền thực thi tệp.
 - Nhóm sở hữu có các quyền sau: `--`, điều đó có nghĩa là nhóm `devconnected` không thể đọc, ghi hoặc thực thi tệp.
 - Những người dùng khác: `---`, quyền tương tự như nhóm `devconnected`

Hiểu biết về quyền trên tệp tin



- Dưới đây là bảng mô tả ý nghĩa về các quyền đọc, ghi và thực thi đối với các tệp.

Quyền	Mô tả
r (read)	Người dùng, nhóm hoặc người khác <u>có thể đọc tệp</u> bằng lệnh như cat hoặc vi (ở chế độ chỉ đọc)
w (write)	Người dùng, nhóm hoặc người khác <u>có thể sửa đổi và lưu tệp</u> bằng các lệnh như nano hoặc vi
x (execute)	Người dùng, nhóm hoặc người khác <u>có thể thực thi</u> tệp. Phần lớn sử dụng cho các tệp script

Hiểu biết về quyền trên thư mục

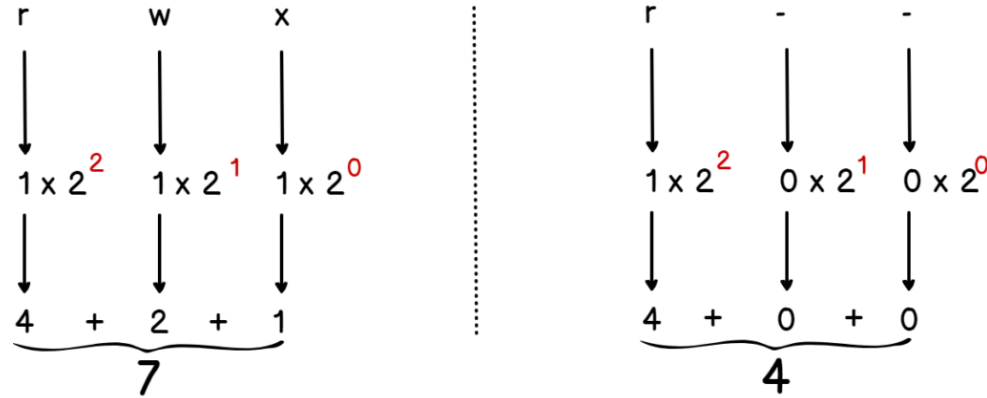


- Dưới đây là bảng mô tả ý nghĩa về các quyền đọc, ghi và thực thi đối với các thư mục.

Quyền	Mô tả
r (read)	Người dùng, nhóm hoặc những người khác <u>có thể liệt kê nội dung</u> của thư mục (ví dụ sử dụng lệnh ls)
w (write)	Người dùng, nhóm hoặc người khác <u>có thể thêm hoặc xóa các tệp</u> khỏi thư mục
x (execute)	Người dùng, nhóm hoặc người khác <u>có thể điều hướng di chuyển qua thư mục</u> (ví dụ sử dụng lệnh cd)

```
drwxr-xr-x  2 devconnected devconnected 4096 Jul 29 17:57 Documents
drwxr-xr-x  3 devconnected devconnected 4096 Aug  4 09:26 Downloads
```

Chuyển đổi quyền từ kí tự sang dạng thập phân



Complete permissions with binary

r - x - w x r - -
534

With chmod



Chế độ umask trong Linux



- Linux mask là mặt nạ đặt quyền cho các tệp mới được tạo trên hệ thống Unix.
- Thực hiện lệnh sau và quan sát:

```
devconnected@debian-10:~$ umask  
0022
```
- Trước khi sử dụng Linux Mask, chế độ mặc định được gọi là **Base Permission**:
 - Các tập tin được tạo ra với quyền mặc định 666, hoặc một quyền 'rw- **rw**- rw-'.
 - Các thư mục được tạo với quyền mặc định 777, hoặc quyền 'rwx rwx rwx'.
- Sau khi sử dụng Linux Mask (để ý 3 số cuối 022):

Umask (viết tắt của user file-creation mode mask hay user-mask): thay đổi thiết lập về quyền hạn mặc định sẽ gán cho file, thư mục khi chúng mới được tạo không?

	Mask = 022	
666		777
- 022		- 022
-----		-----
644		755
or		or
r w - r - - r - -		r w x r w - r w -

Cấp quyền trên hệ thống Linux



- Quyền trên hệ thống Linux có thể được quản lý bằng cách sử dụng ba lệnh: **chmod**, **chown** và **chgrp**.
- Các lệnh đó tương ứng thay đổi quyền của tệp, thay đổi chủ sở hữu của tệp hoặc thay đổi nhóm của tệp.
- **Cảnh báo:**
 - Cần phải có các đặc quyền nâng cao (sudo) để thực hiện các lệnh.
 - Người dùng có thể thay đổi chủ sở hữu hoặc nhóm bằng tài khoản người dùng của mình.

Cấp quyền trên hệ thống Linux



- Sử dụng **chmod** thay đổi quyền trên tệp: Lệnh chmod sửa đổi các quyền của một tệp bằng cách sử dụng dạng thập phân hoặc dạng biểu tượng.

chmod 421 devconnected
Command Binary form Folder or directory

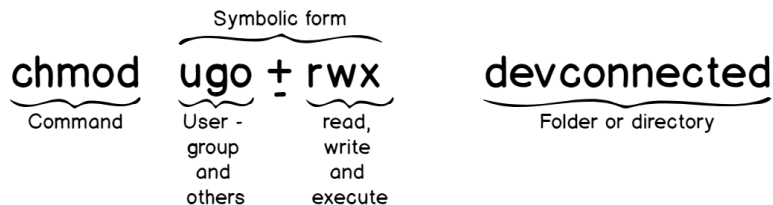
- Một số ví dụ:

Lệnh	Kết quả
chmod 777 file	r w x r w x r w x (không nên dùng!)
chmod 444 file	r - - r - - r - - (quyền chỉ đọc read-only)
chmod 421 file	r - - - w - - - x (người sở hữu có thể đọc, nhóm sở hữu có thể ghi, người dùng khác có thể thực thi)
chmod 000 file	- - - - - - - - (không có bất cứ quyền gì)

Cấp quyền trên hệ thống Linux



- Sử dụng **chmod** thay đổi quyền trên tệp: Lệnh chmod sửa đổi các quyền của một tệp bằng cách sử dụng dạng thập phân hoặc dạng biểu tượng.



- Một số ví dụ:

Lệnh	Kết quả
chmod u+rw file	Thêm quyền đọc, ghi và thực thi cho người sở hữu tệp
chmod go+r file	Thêm quyền đọc cho người sở hữu và nhóm sở hữu
chmod o+rx file	Thêm quyền đọc và thực thi cho người dùng khác
chmod u-r file	Loại bỏ quyền đọc đối với người sở hữu tệp

Cấp quyền trên hệ thống Linux



- Sử dụng **chgrp** để thiết lập thuộc tính nhóm cho 1 tệp hoặc thư mục (đổi tài khoản nhóm).

chgrp users devconnected
Command group Folder or directory

- Một số ví dụ:

Lệnh	Kết quả
chgrp users file1	Chỉ định users làm nhóm cho tệp1
chgrp -R users directory1	Thiết lập users là nhóm cho thư mục directory và cả con của nó
chgrp -c users file1	Chỉ định nhóm users cho tệp1 và hiển thị kết quả thay đổi trong terminal

Hiểu biết về SUID và GUID



- SUID (Set owner User ID up on execution) là một loại file permission đặc biệt.
 - Thông thường một file trong linux khi chạy thì sẽ được kế thừa từ user đang log in.
 - SUID sẽ cấp quyền "tạm thời" cho user chạy file quyền của user tạo ra file (owner). Nói một cách khác, user chạy sẽ có UID và GID của người tạo ra file, khi chạy 1 file hay command.
- Ví dụ về SUID: `$ ls -l /usr/bin/su`

```
devconnected@debian-10:~$ ls -l /usr/bin/su
-rwsr-xr-x 1 root root 63568 Jan 10 2019 /usr/bin/su
```

Hiểu biết về SUID và GUID



- Một số ví dụ về SUID:
 - **passwd command**: Khi thay đổi password chúng ta dùng passwd command, là utility được tạo bởi root. Command passwd sẽ cố để thay đổi một số file như /etc/passwd hay là /etc/shadow. Những file đó cũng là những file được tạo bởi root và chỉ được nhìn bởi root, tuy nhiên vì passwd đã được set SUID nên bạn có thể thực hiện câu lệnh mà không cần sudo.
 - **ping command**: Với ping command, khi chạy ping thì ping phải tạo socket files và mở port để gửi, nhận IP packet. User thông thường không có quyền mở file socket cũng như port. Do ping đã được set SUID nên bất kì user nào cũng có thể làm được thao tác này.

Hiểu biết về SUID và GUID

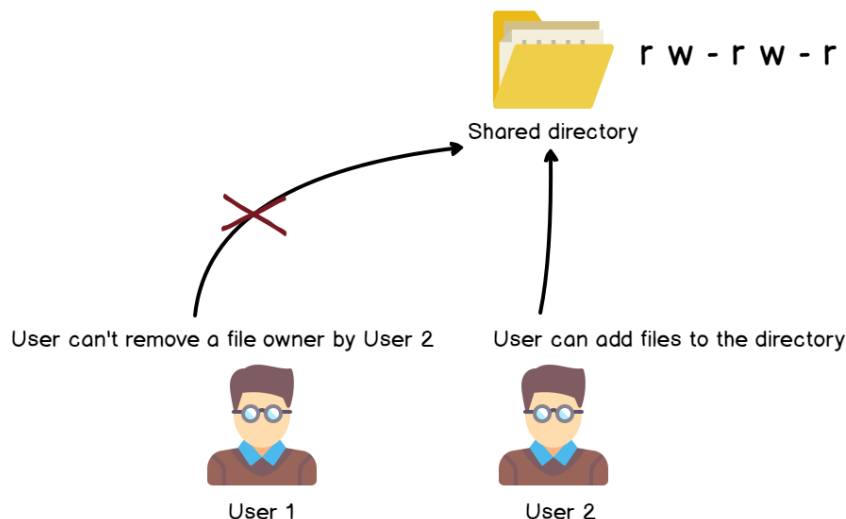


- Thiết lập SUID:
 - Có thể dùng kí tự hoặc số để thiết lập
 - `chmod u+s file1.txt`
 - `chmod 4750 file1.txt`
 - Sau khi thiết lập SUID:
- GUID có cách tư duy tương tự như SUID

Hiểu biết về Sticky Bit



- **sticky bit** được dùng để tinh chỉnh quyền truy cập file trên những thư mục được chia sẻ.
- Xem xét ví dụ sau:



Bài toán: Tôi muốn có thể thêm tệp vào thư mục, cũng như sửa đổi nội dung của chúng, nhưng tôi không muốn người dùng khác di chuyển hoặc xóa tệp của mình (ngay cả khi họ sở hữu tệp quyền tự thêm tệp tin).

Hiểu biết về Sticky Bit



- Thiết lập **sticky bit**:
 - `chmod +t directory1` (adds the sticky bit to the directory1)
 - `chmod -t directory1` (removes the sticky bit from the directory1)

```
devconnected@debian-10:~$ ls -l test
-----rwt 1 devconnected devconnected 0 Aug  5 18:06 test
```

Trên dòng cấp phép, sticky bit được biểu thị bằng chữ thường t (hoặc chữ hoa T nếu không thiết lập quyền thực thi cho other) ở cuối của nó.

2. Danh sách điều khiển truy cập



ACL – Danh sách điều khiển truy cập



- Danh sách kiểm soát truy cập được sử dụng trên các hệ thống tệp Linux để đặt các quyền tùy chỉnh và được cá nhân hóa hơn trên các tệp và thư mục. ACL cho phép chủ sở hữu tệp hoặc người dùng đặc quyền cấp quyền cho người dùng cụ thể hoặc cho các nhóm cụ thể.

Trong Linux, như bạn có thể biết, các quyền được chia thành ba loại: một cho chủ sở hữu của tệp, một cho nhóm và một cho các nhóm khác.

Tuy nhiên, trong một số trường hợp, bạn có thể muốn cấp quyền truy cập vào một thư mục (ví dụ: quyền thực thi) cho một người dùng cụ thể mà không phải đưa người dùng này vào nhóm của tệp.

Đây chính xác là lý do tại sao danh sách kiểm soát truy cập được phát minh.

```
antoine@debian-10:~/acl$ getfacl acl-file
# file: acl-file
# owner: antoine
# group: antoine
user::rw-
user:antoine:rw-
group::r--
mask::rw-
other::r--

antoine@debian-10:~/acl$
```

Liệt kê Danh sách điều khiển truy cập



- Trên Linux, danh sách kiểm soát truy cập không được bật khi tạo tệp hoặc thư mục mới trên máy chủ (trừ khi thư mục mẹ có một số ACL được xác định trước).
- Để xem danh sách điều khiển truy cập có được xác định cho một tệp hoặc thư mục hay không, hãy chạy lệnh ls và tìm kiếm một ký tự của + + ở cuối dòng.

```
antoine@debian-10:~/acl$ ls -l
total 0
-rw-rw-r--+ 1 antoine antoine 0 Sep 21 15:05 acl-file
-rw-r--r-- 1 antoine antoine 0 Sep 21 15:05 file
antoine@debian-10:~/acl$
```



THẢO LUẬN & HỎI ĐÁP

