

LAB: umask 與檔案建立權限計算

- 列出目前的 umask

```
linux-zali:~ # cd /home/sles/  
linux-zali:/home/sles # umask
```

- 請觀察系統設定

```
linux-zali:/home/sles # cat /etc/login.defs | grep -i umask
```

- 請建立一個新的檔案和一個新的資料夾，請觀察權限

```
linux-zali:/home/sles # touch rootfile  
linux-zali:/home/sles # mkdir rootdir  
linux-zali:/home/sles # ls -ld root*  
drwxr-xr-x 2 root root 6 11月 24 04:48 rootdir  
-rw-r--r-- 1 root root 0 11月 24 04:48 rootfile
```

- 自訂 umask 為 013，暫時性生效

```
linux-zali:/home/sles # umask 013  
linux-zali:/home/sles # umask
```

- 請再次建立一個新的檔案和一個新的資料夾，請觀察權限

```
linux-zali:/home/sles # touch rootfile2  
linux-zali:/home/sles # mkdir rootdir2  
linux-zali:/home/sles # ls -ld root*  
drwxr-xr-x 2 root root 6 11月 24 04:48 rootdir  
drwxrw-r-- 2 root root 6 11月 24 06:38 rootdir2  
-rw-r--r-- 1 root root 0 11月 24 04:48 rootfile  
-rw-rw-r-- 1 root root 0 11月 24 06:38 rootfile2
```

- 因有修改 umask，所以務必要登出，以免影響

```
linux-zali:/home/sles # exit
```

LAB: SUID

- 請觀察權限

```
linux-zali:~ # ls -l /bin/cat
linux-zali:~ # ls -l /etc/shadow
```

- 以 user1 身份查看 `/etc/shadow`

失敗，因為沒有 **r** 權限

```
linux-zali:~ # su - user1 -c "cat /etc/shadow"
```

- 將 cat 指令加上 SUID 權限，請再次觀察權限

```
linux-zali:~ # chmod u+s /bin/cat
linux-zali:~ # ls -l /bin/cat
linux-zali:~ # ls -l /etc/shadow
```

- 以 user1 身份再次查看 `/etc/shadow`

成功，cat 指令有設定 SUID，執行身份會變成 cat 指令的 Owner → root，因 root 對 /etc/shadow，有 r 的權限，所有可以查看

```
linux-zali:~ # su - user1 -c "cat /etc/shadow"
```

- 請將 /bin/cat 指令的 SUID 權限給移除，請觀察資訊

```
linux-zali:~ # chmod u-s /bin/cat
linux-zali:~ # ls -l /bin/cat
linux-zali:~ # ls -l /etc/shadow
```

- 以 user1 身份再次查看 `/etc/shadow`

失敗，因為沒有 **r** 權限

```
linux-zali:~ # su - user1 -c "cat /etc/shadow"
```

LAB: SGID

目的：建立部門資料夾，不管任何使用者在該目錄下，建立檔案或是資料夾，都能繼承該目錄的群組

- 建立 MIS 群組

```
linux-zali:~ # mkdir /mis  
linux-zali:~ # groupadd mis
```

- 請觀察權限、擁有者以及群組

```
linux-zali:/mis # ls -ld /mis  
drwxr-xr-x 1 root root 0 11月 26 04:19 /mis
```

- 將 /mis 資料夾的群組修改為 mis 群組所有，請觀察權限、擁有者以及群組

```
linux-zali:/mis # chown root:mis /mis  
linux-zali:/mis # ls -ld /mis  
drwxr-xr-x 1 root mis 0 11月 26 04:19 /mis
```

- 在 /mis 資料夾底下，建立一個新檔案，請觀察權限、擁有者以及群組

```
linux-zali:/mis # touch /mis/test  
linux-zali:/mis # ls -l /mis/test  
-rw-r--r-- 1 root root 0 11月 26 04:25 /mis/test
```

- 將 /mis 資料夾加上 SGID，請觀察權限、擁有者以及群組

```
linux-zali:/mis # chmod g+s /mis  
linux-zali:/mis # ls -ld /mis  
drwxr-sr-x 1 root mis 16 11月 26 04:25 /mis
```

- 再次在 /mis 資料夾底下，建立一個新檔案，請觀察權限、擁有者以及群組

```
linux-zali:/mis # ls -l /mis  
總計 0  
-rw-r--r-- 1 root mis 0 11月 26 04:28 test2  
-rw-r--r-- 1 root root 0 11月 26 04:25 test
```

LAB: sticky bit

目的：不管權限為何，都不可以刪除其他人的檔案

- 建立 public 資料夾，並將此資料夾加上 sticky bit，同時也把權限設定為 777

```
linux-zali:/mis # cd ~  
linux-zali:~ # mkdir /public  
linux-zali:~ # chmod 1777 /public
```

- 請觀察權限、擁有者以及群組

```
linux-zali:~ # ls -ld /public  
drwxrwxrwt 1 root root 0 11月 26 04:36 /public
```

* 以 user1 身份，在 /public 資料夾，建立一個新檔案，同時也把權限設定為 777

```
linux-zali:~ # su - user1 -c "touch /public/user1.txt"  
linux-zali:~ # su - user1 -c "chmod 777 /public/user1.txt"
```

- 請觀察 資料夾 的權限、擁有者以及群組

```
linux-zali:~ # ls -ld /public  
drwxrwxrwt 1 root root 18 11月 26 04:39 /public
```

- 請觀察 檔案 的權限、擁有者以及群組

```
linux-zali:~ # ls -l /public  
總計 0  
-rwxrwxrwx 1 user1 users 0 11月 26 04:39 user1.txt
```

- 請以使用者 user2 刪除 /public/user1.txt

失敗，因 /public 目錄有設定 sticky bit 權限，非本人是不能刪除的

```
linux-zali:~ # su - user2 -c "rm /public/user1.txt"  
rm: 無法移除 '/public/user1.txt': 此項操作並不被允許
```

- 請以使用者 user1 刪除 /public/user1.txt ，請觀察權限、擁有者以及群組

成功，因為擁有者是 user1

```
linux-zali:~ # ls -l /public/  
總計 0  
-rwxrwxrwx 1 user1 users 0 11月 26 04:51 user1.txt  
linux-zali:~ # su - user1 -c "rm /public/user1.txt"  
linux-zali:~ # ls -l /public  
總計 0
```