介紹用戶、群組和許可權一些高級功能 | 開源互助社區

介紹用戶、群組和許可權一些高級功能

火星人 @ 2014-03-09 ,

一、介紹UID和GID

1、每一個使用者的名稱都會有一個相對應的User ID號碼;

2、每一個組的名稱也都會有一個相對應的Group ID號碼;

3、而這些號碼的資料是以數字的形態而儲存在磁碟上;

其實以上三點,通過前面的章節就應該知道了.

二、介紹 /etc/passwd、/etc/shadow、/etc/group這三個儲存驗證資料的檔案

有關驗證方面的資訊是以明碼的方式儲存在下面四個檔案中的:

1、/etc/passwd 這個檔案是使用者的資料庫

2、/etc/shadow 這個檔案儲存使用者密碼的資料庫

3、/etc/group 這個檔案是使用者群組的資料庫

4、/etc/gshadow(在這節課程中不會用到,暫不考慮)

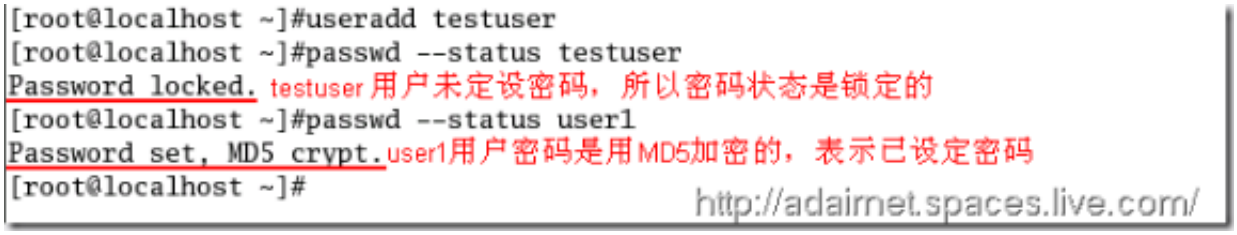
三、介紹系統帳號和系統群組

1、cat /etc/passwd 打開帳號資料庫檔案,其中1-499的UID號和GID號通常是給內建的系統使用者及系統群組使用,而這些的系統使用者及系統群組是對某些服務或應用程式具有控制的許可權,例始:apache這個帳號是針對web服務的,lp帳號是針對印表機的服務的

四、介紹修改密碼及切換不同的使用者

1、修改密碼,可以使用passwd指令,如果在修改密碼時設定了不安全的密碼會被電腦拒絕,但root帳號可以設定不安全的密碼,因為root帳號的許可權是最大的,如下圖所示:

2、使用passwd指令查看用戶的密碼狀態,如下圖:



3、介紹如何使用su指令切換到另一個帳號

例：su user1 切換到user1帳號,如果從root帳號切換到其他普通帳號,不需要輸入密碼,註：一般用戶之間切換需要輸入密碼.

su - user1 切換帳號時,中間加一個 - 表示：不僅要切換到user1,連目前的環境變數也會變成目前user1的環境變數.

su 未指定要切換到哪個帳號, 則會切換到root帳號

su - 加上了- ,也未指定帳號,也是切換到root帳號,並載入root的環境變數

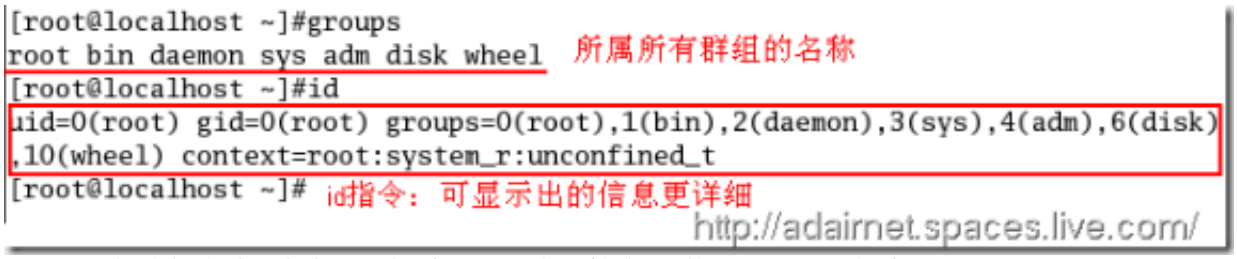
五、介紹查看使用者信息的指令

1、查看目前是使用哪一個帳號登陸的,使用下面的指令：

whoami

2、查看目前使用者帳號屬於哪一群組,可使用下面兩個指令：

groups (只能顯示所屬所有組名稱) 和 id (可以顯示用戶名、組名及UID、GID等信息,這個顯示的要更詳細一些)



3、查看當前系統中有哪些帳號登陸這台主機中,可使用以下三個指令：

users 和 who 和 w

·users 指令只能顯示使用者帳號的名稱；

·who 指令不但可以顯示使用者帳號名稱,還可以顯示帳號登陸的時間點及從哪裡登陸進來的；

·w 指令可以顯示的內容包括who指令顯示的內容,還包括使用者在使用什麼指令佔用的CPU都可以知道;

也就是說只記住w指令就可以了.

4、查詢使用者的登陸時間及重開機時間的歷史記錄,可使用下面的指令:

last

六、介紹預設的檔案許可權

1、檔案的預設許可權為666,666的許可權為 owner(rw)、group(rw)、other(rw),所有都沒有x許可權.

2、目錄的預設許可權為777,777的許可權為 owner(rwx)、group(rwx)、other(rwx).

註:這兩個預設的許可權不是在建立新的檔案和目錄時所產生的最后許可權

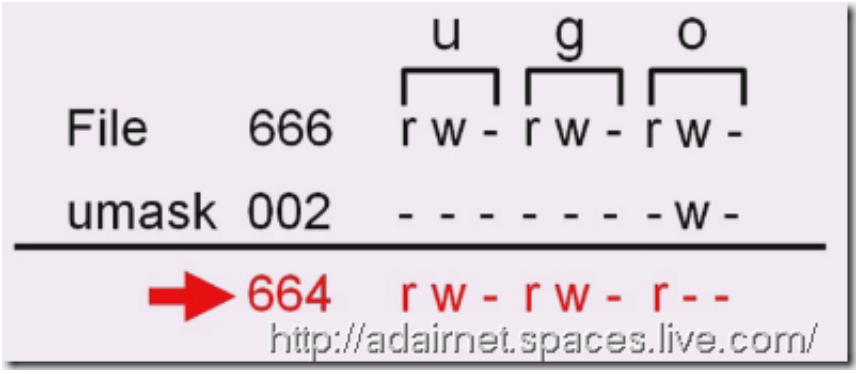
3、最后的許可權需要經遮罩來擋掉檔案及目錄里某些預設的許可權,產會對檔案及目錄產生最后的許可權.

4、預設情況下在沒有管理許可權的一般使用者上遮罩(umask)是002(例如user1是一般使用者,使用umask指令查看umask是0002,這四位中的第一位先不用考慮,后三位才是預設的遮罩值.)

5、root帳號使用的遮罩(umask)是022.

例:umask(遮罩)的使用方法如下圖:

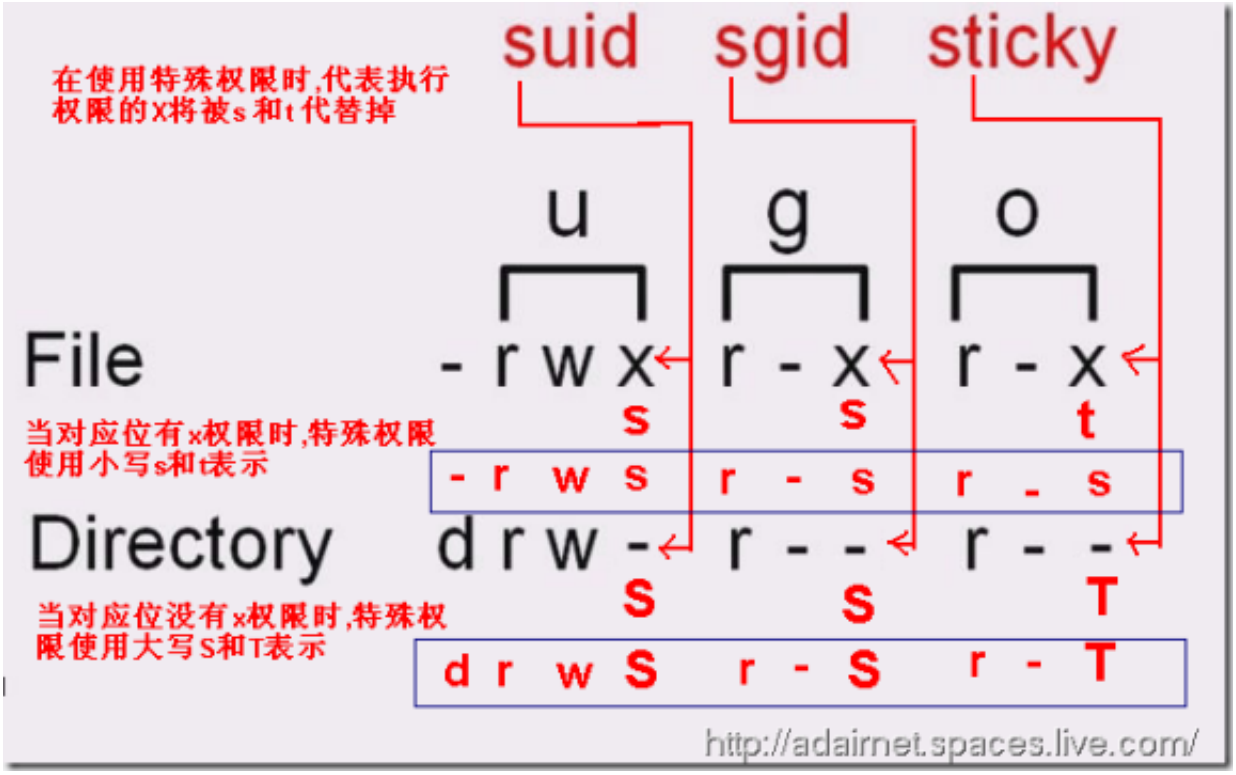
註:下面的方式並不是使用減法的方式運算的,只是去掉相對應位的許可權,如果原來沒有的許可權保持不變.這樣通過umask可以很輕鬆的決定在建立檔案和目錄時最后的許可權.



示例如下圖:設root帳號的umask為077(就是只有root帳號對自己建立的檔案及目錄有讀寫許可權)

七、介紹特殊許可權

1、特殊許可權又稱為第四個許可權,在特殊許可權中又分為三種許可權,分別為:suid、sgid、sticky,



2、使用chmod和nautilus（就是在圖形界面下） 指令來設定特殊許可權

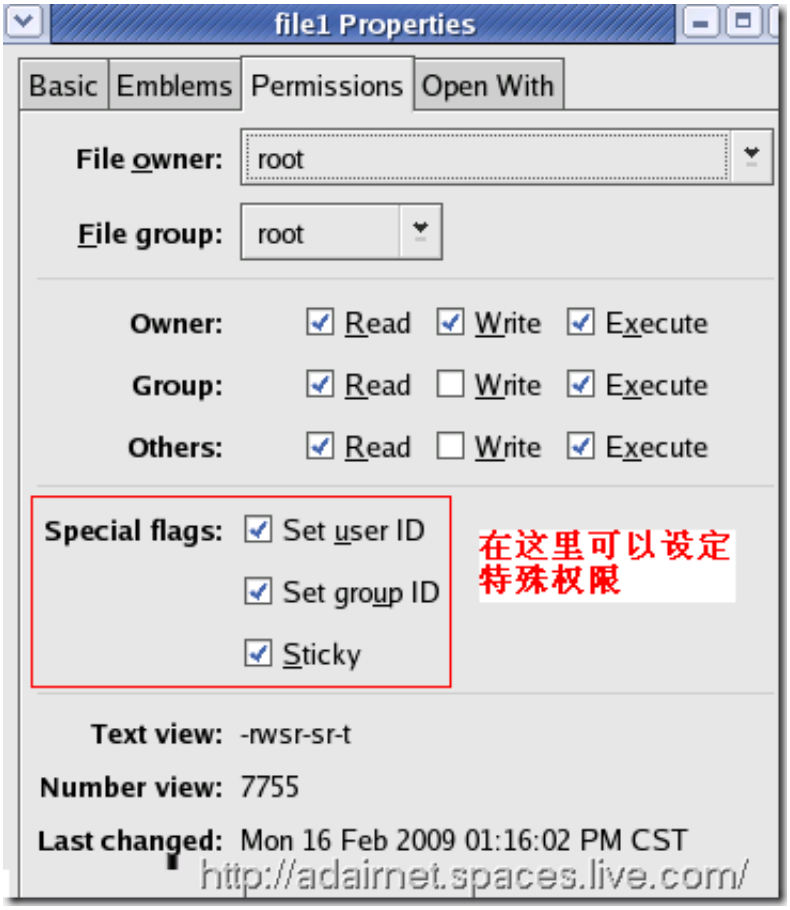
```
[root@localhost ~]# ls -l file*
-rwxr-xr-x  1 root root 0 Feb 16 13:11 file1 先准备两个档案,注意这两个档案权限的区别
-rwxr-xr--  1 root root 0 Feb 16 13:11 file2
[root@localhost ~]# chmod u+s file1  为file1档案加入suid权限
[root@localhost ~]# ls -l file*
-rwsr-xr-x  1 root root 0 Feb 16 13:11 file1 在这时可以看到file1档案u栏里面的x变成了小写的s
-rwxr-xr--  1 root root 0 Feb 16 13:11 file2
[root@localhost ~]# chmod g+s file2 为file2档案加入sgid权限
[root@localhost ~]# ls -l file*
-rwsr-xr-x  1 root root 0 Feb 16 13:11 file1
-rwxr-sr--  1 root root 0 Feb 16 13:11 file2 在这时可以看到file2档案g栏位里面的x变成了小写的s
[root@localhost ~]# chmod o+t file2  为file2档案加入sticky权限
[root@localhost ~]# ls -l file*
-rwsr-xr-x  1 root root 0 Feb 16 13:11 file1
-rwxr-sr-T  1 root root 0 Feb 16 13:11 file2 在这时可以看到file2档案o栏位里面,由于原来没有x权限,所以将 — 变成了大写的 T 了
[root@localhost ~]#
http://adairnet.spaces.live.com/
```

其實在設定特殊許可權時,也可以使用數字來設定特殊許可權,suid(4)、sgid(2)、sticky(1)

```
[root@localhost ~]# ls -l file*                    suid  sgid  sticky
-rwxr-xr-x  1 root root 0 Feb 16 13:11 file1        (4)   (2)   (1)
-rwxr-xr--  1 root root 0 Feb 16 13:11 file2
[root@localhost ~]# chmod 2755 file1 设定sgid权限，sgid权限代有数字为2
[root@localhost ~]# ls -l file1
-rwxr-sr-x  1 root root 0 Feb 16 13:11 file1
[root@localhost ~]# chmod 7755 file1 设定suid,sgid,sticky三种权限，将三种代表数相加得7
[root@localhost ~]# ls -l file1
-rwsr-sr-t  1 root root 0 Feb 16 13:11 file1
[root@localhost ~]#  其中设定权限时使用的四位数字中，第一位就是特殊权限所对应数字的总和
                     后面的分别是user,group,other三种权限所代表数字的和
http://adairnet.spaces.live.com/
```

執行nautilus也就是打開視窗,在圖形界面下修改檔案的特殊許可權,操作過程如下：

選中檔案、點擊滑鼠右鍵,在彈出的菜單中點擊屬性（properties）,再點選許可權(permissions)如下圖：



八、介紹特殊許可權對執行檔有什麼作用

１、在特殊許可權里,可以將suid,sgid這兩個特殊許可權設置在執行檔上：

suid:這個特殊許可權可以讓使用者在執行帶有suid 這個特殊許可權的執行檔時,是以檔案擁有者的身份在執行,而不是以執行者本身的許可權來執行.

sgid：同suid類似,同樣不論哪個使用者在執行帶有sgid特殊許可權的執行檔時,會以存檔的群組身份來執行.

九、介紹特殊許可權對目錄有什麼作用

1、在特殊許可權里,有sgid、sticky這兩個特殊許可權設定在目錄上：

sticky ：可以讓設有這個特殊許可權目錄里的檔案只有檔案的擁用者及root才可以刪除這個檔案,而不是看write的許可權來決定的.

sgid： 這個特殊許可權是讓設有這個許可權目錄的群組成員才有許可權在這個目錄里,建立新的檔案

通常我們常會對一個專案的目錄,設定sticky和sgid這兩個特殊許可權,例如：現有一個專案組ProjectA,參與人員有user1、user2及一個專案經理Manager,這時專案經理可以在建立專案目錄project目錄時,將sticky和sgid這兩個特殊權許可權設定上,擁有者為manager,所屬群組為project,project許可權如drwxrws--T,project組的成員都可以在這個目當里建立檔案,但有sticky的許可權,所有成員只能刪除自己建立的檔案,這樣可以防止誤刪別人的檔案,達到保護的目的.

轉自：http://adairnet.spaces.live.com/blog/cns!F5DC2937B72C0783!359.entry