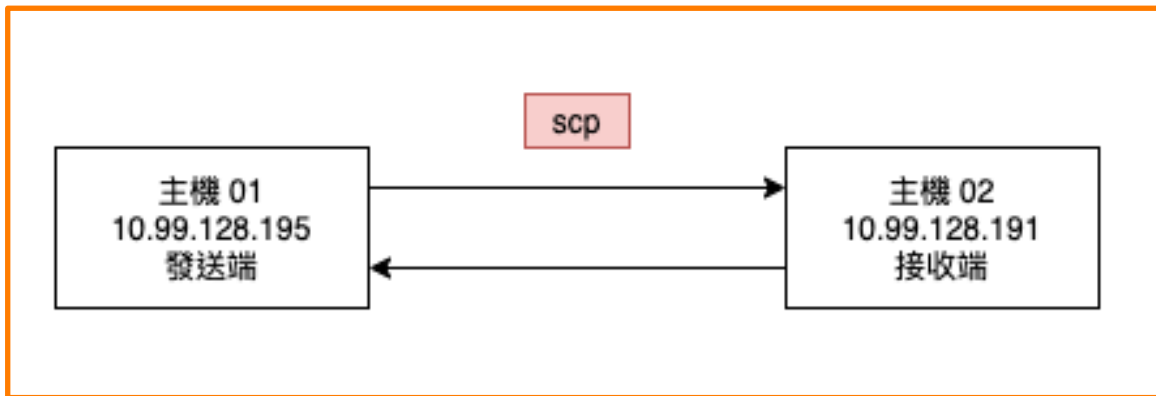


京峰教育 第三次作業 – 0403 課程

[作業一] 練習相關命令, scp, rsync, chmod, setfacl, getfacl

scp

scp 是 secure cp 的縮寫, 是 linux 系統下基於 ssh 登陸遠程機器的安全拷貝命令, 如下圖一是當前使用此命令之場景



圖一、scp 使用場景

scp 傳送本機檔案到遠端機器, 命令使用方式 scp [使用者]@[來源主機]:[要傳送的檔案] [使用者]@[目的主機]:[要傳送的路徑], 如下圖二為傳送端實際操作過程, 下圖三為接收端確認

```
[root@CentOS7 data]# scp ./CentOS7.iso root@10.99.128.191:/tmp/
The authenticity of host '10.99.128.191 (10.99.128.191)' can't be established.
ECDSA key fingerprint is SHA256:HCdJvR2fc/cwAokgZ00luqfYOMZvrixR1dnKt1A80Q.
ECDSA key fingerprint is MD5:e6:5c:13:5e:4f:ba:1d:c9:a5:fa:64:3e:ae:a0:69:88.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.99.128.191' (ECDSA) to the list of known hosts.
root@10.99.128.191's password:
CentOS7.iso
```

圖二、傳送端操作過程

```
[root@Controller yum.repos.d]# cd /tmp
[root@Controller tmp]# ls -lh
total 943M
-rw-r--r-- 1 root root 942M Apr  6 01:58 CentOS7.iso
-rwx----- 1 root root 836 Mar 26 15:25 ks-script-bBFtmg
drwx----- 3 root root 17 Mar 31 10:18 systemd-private-88b851e4e74745dc824b5974c904d72c-chronyd.service-t4hTok
drwx----- 3 root root 17 Mar 31 10:18 systemd-private-88b851e4e74745dc824b5974c904d72c-mariadb.service-4CT0ac
drwx----- 3 root root 17 Mar 26 15:26 systemd-private-bb036b75d6eb48acaf44b028ba03b7c8-chronyd.service-4auS0D
drwx----- 3 root root 17 Mar 31 08:15 systemd-private-cc57b34edfdb44a495bdb64ae4befc6d-chronyd.service-8uFubc
-rw----- 1 root root  0 Mar 26 15:17 yum.log
-rw----- 1 root root 250K Apr  4 00:04 yum save tx.2020-04-04.00-04.q0X3SD.yumtx
```

圖三、接收端確認有無收到檔案

scp 複製遠端檔案到本機, 命令使用方式 scp [使用者]@[目的主機]:[要複製來本機的檔案] [使用者]:[來源主機]:[複製遠端到本機的路徑], 如下圖四為本機確認有無此檔案, 圖五為從遠端機器複製到本機執行後, 確認有無成功複製

```
[root@CentOS7 tmp]# rm -rf *  
[root@CentOS7 tmp]# ls
```

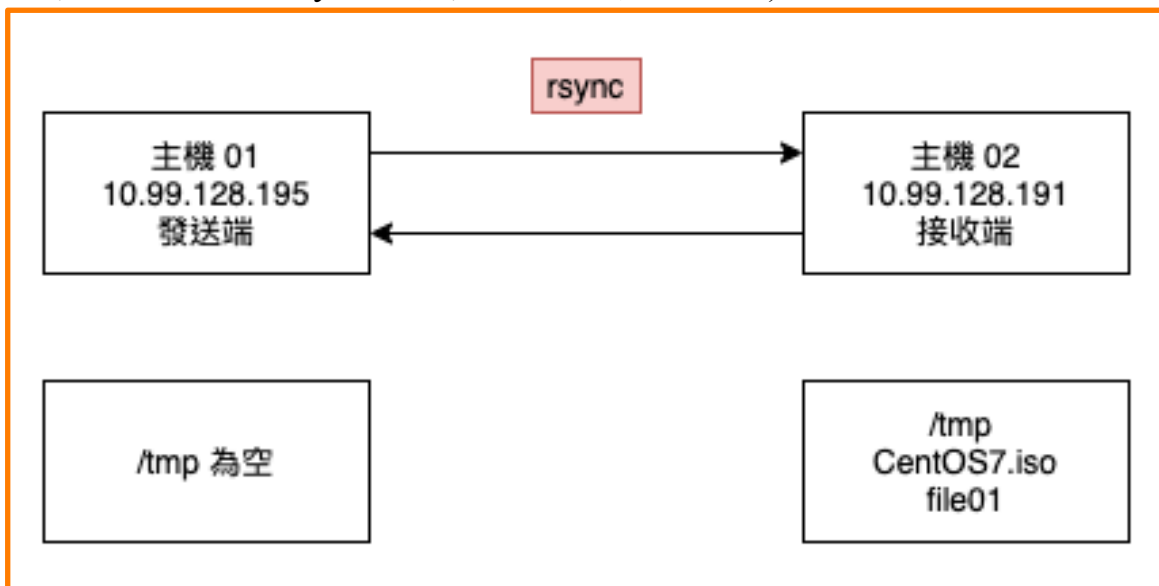
圖四、確認本機當前無檔案

```
[root@CentOS7 tmp]# scp root@10.99.128.191:/tmp/CentOS7.iso /tmp/  
root@10.99.128.191's password:  
CentOS7.iso 100% 942MB 85.4MB/s 00:11  
[root@CentOS7 tmp]# ls -lh  
total 942M  
-rw-r--r-- 1 root root 942M Apr 6 14:15 CentOS7.iso
```

圖五、從遠端拷貝檔案至本機

rsync

rsync 同步遠端機器的資料, 用此方式傳輸檔案至本機較 scp 有效率, 在第一次會將整個資料夾複製下來, 之後若針對此資料夾再次傳輸時, 會先比對一次, 若有的資料則不進行傳送, 針對沒有的資料才傳, 而 rsync 在傳送時也會進行壓縮及解壓縮, 所以較為有效率, 圖六為使用此命令之場景, 圖七要同步之目的主機資料夾狀況, 圖八為來源端與目的端進行資料的同步, 需加上 -r 參數(遞歸整個目錄), 以及確認同步完成資料夾狀態 (要特別注意一點兩端主機皆必須安裝 rsync 套件, 否則無法成功運行)



圖六、使用 rsync 命令場景

```
[root@Controller tmp]# ls -lh  
total 943M  
-rw-r--r-- 1 root root 942M Apr 6 01:58 CentOS7.iso  
-rw-r--r-- 1 root root 11 Apr 6 02:28 file01
```

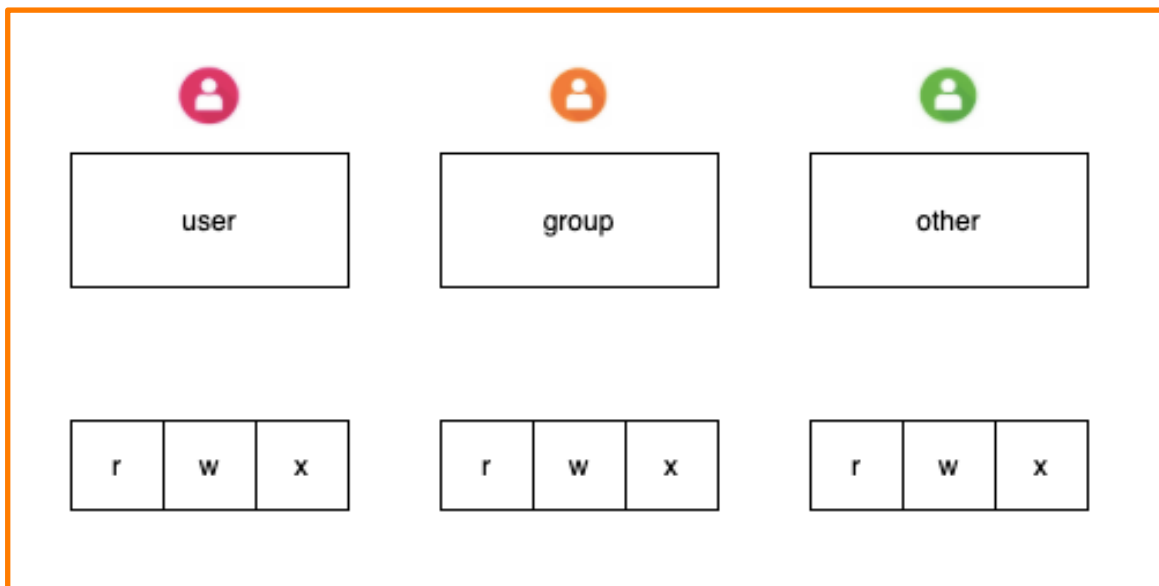
圖七、要同步目的主機目錄狀況

```
[root@CentOS7 tmp]# ls
[root@CentOS7 tmp]# rsync -r root@10.99.128.191:/tmp/ /tmp
root@10.99.128.191's password:
[root@CentOS7 tmp]# ls -lh
total 943M
-rw-r--r--. 1 root root 942M Apr  6 14:36 CentOS7.iso
-rw-r--r--. 1 root root  11 Apr  6 14:36 file01
```

圖八、使用 rsync -r 命令由遠端將目錄下之資料拷貝回本機

chmod

chmod 命令是用來修改檔案屬性, 可以針對檔案或目錄修改使用者、群組、其他人的讀取、寫入、執行等權限, 場景如下圖九, 預設目錄權限為 755, 如下圖十, 檔案權限為 644, 如下圖十一[r(read) = 4、w(write) = 2、x(execute) = 1]



圖九、chmod 使用場景

預設檔案目錄 755, other 有 x 權限是為了讓其他使用者可以進入其目錄

```
[root@CentOS7 tmp]# mkdir testFolder
[root@CentOS7 tmp]# ls -l
total 0
drwxr-xr-x. 2 root root 6 Apr  6 15:51 testFolder
```

圖十、預設目錄權限 755

預設檔案權限 644, 除了檔案擁有者可以針對此檔案寫入外, 其他群組的使用者以及其他使用者, 皆只有讀取的權限, 不可寫入, 如下圖十二

```
[root@CentOS7 testFolder]# touch filepermission
[root@CentOS7 testFolder]# ll
total 0
-rw-r--r--. 1 root root 0 Apr  6 15:53 filepermission
```

圖十一、預設檔案權限 644

```
[root@CentOS7 ~]# useradd otheruser
[root@CentOS7 ~]# echo "123456" | passwd --stdin otheruser
Changing password for user otheruser.
passwd: all authentication tokens updated successfully.
[root@CentOS7 ~]# su otheruser
[otheruser@CentOS7 root]$ cd /tmp/
.font-unix/ .ICE-unix/ testFolder/ .Test-unix/ .X11-unix/ .XIM-unix/
[otheruser@CentOS7 root]$ cd /tmp/
.font-unix/ .ICE-unix/ testFolder/ .Test-unix/ .X11-unix/ .XIM-unix/
[otheruser@CentOS7 root]$ cd /tmp/testFolder/
[otheruser@CentOS7 testFolder]$ ll
total 0
-rw-r--r--. 1 root root 0 Apr  6 15:53 filepermission
[otheruser@CentOS7 testFolder]$ echo "otheruser can't write the filepermission file."
otheruser can't write the filepermission file.
[otheruser@CentOS7 testFolder]$ echo "otheruser can't write the filepermission file." >> filepermission
bash: filepermission: Permission denied
```

圖十二、其他用戶不可對 644 檔案權限的檔案寫入

修改其他使用者可以針對 filepermission 進行寫入, 多增加 w 權限, 如下圖十三

```
[root@CentOS7 testFolder]# chmod o+w filepermission
[root@CentOS7 testFolder]# ll
total 0
-rw-r--rw-. 1 root root 0 Apr  6 15:53 filepermission
```

圖十三、新增其他使用者有寫入權限 w

驗證其他使用者可以針對 filepermission 進行寫入, 如下圖十四

```
[otheruser@CentOS7 testFolder]$ ll
total 0
-rw-r--rw-. 1 root root 0 Apr  6 15:53 filepermission
[otheruser@CentOS7 testFolder]$ echo "otheruser can't write the filepermission file." >> filepermission
[otheruser@CentOS7 testFolder]$ tail filepermission
otheruser can't write the filepermission file.
```

圖十四、其他使用者寫入成功

chmod 有 t 權限, 默認/tmp 目錄權限擁有 t 權限, 在此目錄下權限 777, 雖然其他使用者擁有 w 權限, 但不可刪除其他使用者的檔案, 意味著自己只能刪除自己的檔案, 如下圖十五為/tmp 權限顯示擁有 t 權限, 圖十六為 otheruser1234 試圖刪除 otheruser8888 的檔案, 但是失敗

```
[root@CentOS7 ~]# ll /
total 16
lrwxrwxrwx. 1 root root 7 Mar 31 22:15 bin -> usr/bin
dr-xr-xr-x. 5 root root 4096 Mar 31 23:23 boot
drwxr-xr-x. 2 root root 25 Apr 3 14:03 data
drwxr-xr-x. 18 root root 3060 Mar 31 23:30 dev
drwxr-xr-x. 74 root root 8192 Apr 6 16:13 etc
drwxr-xr-x. 5 root root 65 Apr 6 16:12 home
lrwxrwxrwx. 1 root root 7 Mar 31 22:15 lib -> usr/lib
lrwxrwxrwx. 1 root root 9 Mar 31 22:15 lib64 -> usr/lib64
drwxr-xr-x. 2 root root 6 Apr 11 2018 media
drwxr-xr-x. 2 root root 6 Apr 11 2018 mnt
drwxr-xr-x. 2 root root 6 Apr 11 2018 opt
dr-xr-xr-x. 173 root root 0 Mar 31 23:30 proc
dr-xr-xr-x. 3 root root 124 Apr 6 13:57 root
drwxr-xr-x. 24 root root 640 Apr 4 11:22 run
lrwxrwxrwx. 1 root root 8 Mar 31 22:15 sbin -> usr/sbin
drwxr-xr-x. 2 root root 6 Apr 11 2018 srv
dr-xr-xr-x. 13 root root 0 Mar 31 23:30 sys
drwxrwxrwx. 7 root root 144 Apr 6 16:57 tmp
drwxr-xr-x. 13 root root 155 Mar 31 22:15 usr
drwxr-xr-x. 19 root root 267 Mar 31 23:30 var
```

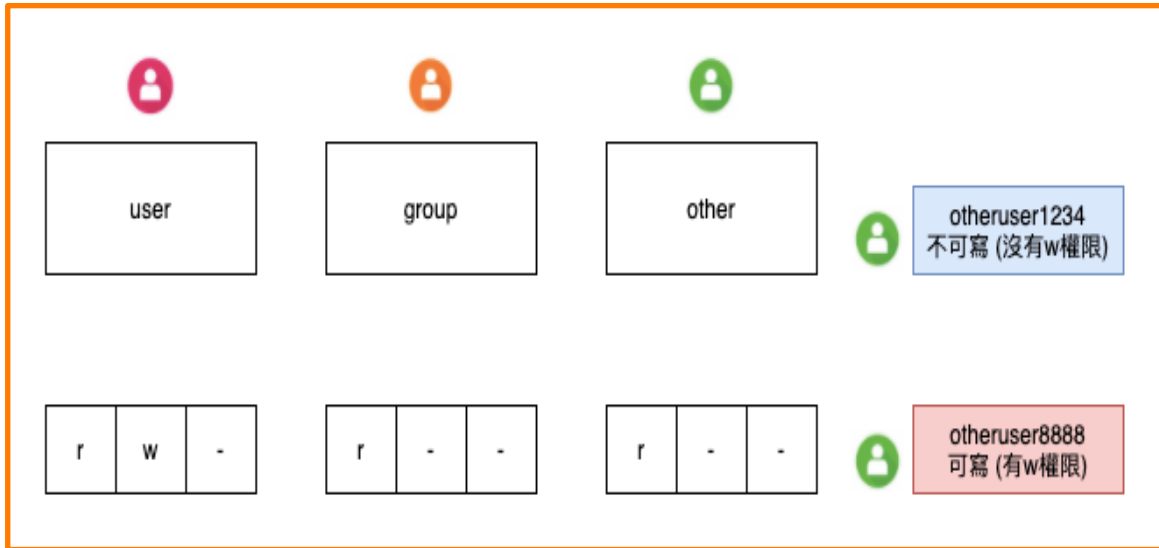
圖十五、/tmp 擁有 t 權限

```
[otheruser1234@CentOS7 tmp]$ ll
total 0
-rw-rw-r--. 1 otheruser1234 otheruser1234 0 Apr 6 16:57 1234-file
-rw-rw-r--. 1 otheruser8888 otheruser8888 0 Apr 6 16:56 8888-file
-rw-r--r--. 1 root root 0 Apr 6 16:56 root-file
[otheruser1234@CentOS7 tmp]$ rm -rf 8888-file
rm: cannot remove '8888-file': Operation not permitted
```

圖十六、otheruser1234 刪除檔案 8888-file 失敗

setfacl & getfacl

setfacl 可以細化其他使用者的權限給予, 比如說一般預設檔案權限為 644, 所有的其他使用者並無法進行寫入動作, 但有例外的情況, 需要給予特定的其他使用者擁有寫入權限, 這時候可以用 setfacl 進行權限授與, 如圖十七為使用場景



圖十七、setfacl 使用場景

創建使用者 otheruser1234, otheruser8888, 如圖十八

```
[root@CentOS7 testFolder]# useradd otheruser1234
[root@CentOS7 testFolder]# useradd otheruser8888
[root@CentOS7 testFolder]# echo "123456" | passwd --stdin other1234
passwd: Unknown user name 'other1234'.
[root@CentOS7 testFolder]# echo "123456" | passwd --stdin otheruser1234
Changing password for user otheruser1234.
passwd: all authentication tokens updated successfully.
[root@CentOS7 testFolder]# echo "123456" | passwd --stdin otheruser8888
Changing password for user otheruser8888.
passwd: all authentication tokens updated successfully.
```

圖十八、創建測試其他使用者

使用 setfacl 針對 otheruser8888 對 filepermission 擁有寫入權限, 如圖十九

```
[root@CentOS7 testFolder]# ll
total 4
-rw-r--rw-. 1 root root 47 Apr  6 16:01 filepermission
[root@CentOS7 testFolder]# getfacl filepermission
# file: filepermission
# owner: root
# group: root
user::rw-
group::r--
other::rw-

[root@CentOS7 testFolder]# setfacl -m u:otheruser8888:rw- filepermission
```

圖十九、setfacl 修改權限

測試 otheruser1234 對 filepermission 沒有寫入權限, 如下圖二十

```
[otheruser@CentOS7 testFolder]$ su otheruser1234
Password:
[otheruser1234@CentOS7 testFolder]$ ll
total 4
-rw-r--r--+ 1 root root 47 Apr  6 16:27 filepermission
[otheruser1234@CentOS7 testFolder]$ echo "this is content write by otheruser1234" >> filepermission
bash: filepermission: Permission denied
```

圖二十、otheruser1234 沒有寫入權限

測試 otheruser8888 擁有寫入權限, 如下圖二十一

```
[otheruser8888@CentOS7 testFolder]$ ll
total 4
-rw-rw-r--+ 1 root root 47 Apr  6 16:27 filepermission
[otheruser8888@CentOS7 testFolder]$ getfacl filepermission
# file: filepermission
# owner: root
# group: root
user::rw-
user:otheruser8888:rw-
group::r--
mask::rw-
other::r--

[otheruser8888@CentOS7 testFolder]$ echo "this is content write by otheruser8888" >> filepermission
[otheruser8888@CentOS7 testFolder]$ tail filepermission
otheruser can't write the filepermission file.
this is content write by otheruser8888
```

圖二十一、otheruser8888 擁有寫入權限

用 ll 指令以及 getfacl 指令進行確認, 如下圖二十二, 多了一個+號, 表示可以用 getfacl 進行其他使用者的權限展開

```
[root@CentOS7 testFolder]# getfacl filepermission
# file: filepermission
# owner: root
# group: root
user::rw-
user:otheruser8888:rw-
group::r--
mask::rw-
other::rw-

[root@CentOS7 testFolder]# ll
total 4
-rw-rw-rw-+ 1 root root 47 Apr  6 16:01 filepermission
```

圖二十二、getfacl 進行權限展開