

Lab: Access Control List <ACL>

```
#mount | grep sda
```

<請觀察資訊, 是否有 acl>

```
#mkdir /acl
#touch /acl/test
#echo "echo 1234" >> /acl/test
#chmod 700 /acl/test
```

```
#ls -l /acl
#su - max -c "cat /acl/test"
#su - john -c "cat /acl/test"
```

<以使用者 max 身份查看檔案>失敗
<以使用者 john 身份查看檔案>失敗

```
#getfacl /acl/test
#setfacl -m u:max:r /acl/test
#ls -l /acl
#getfacl /acl/test
```

<查看 test 資訊>
<設定 acl, -m 編輯, FIELD:NAME:PERM>

```
#su - max -c "cat /acl/test"
#su - john -c "cat /acl/test"
```

<以使用者 max 身份查看檔案>成功
<以使用者 john 身份查看檔案>失敗

```
#setfacl -x u:max /acl/test
#ls -l /acl
#getfacl /acl/test
#setfacl -b /acl/test
#ls -l /acl
```

<設定 acl, -x 移除, FIELD:NAME>
<移除所有的 ACL 設定>

練習 acl mask

```
#ls -l /acl
#chgrp users /acl/test
#chmod 764 /acl/test
#ls -l /acl
#su - max -c "cat /acl/test"
#su - john -c "cat /acl/test"
#su - max -c "/acl/test"
#su - john -c "/acl/test"
#ls -l /acl
#setfacl -m user:john:rwX /acl/test
#ls -l /acl
#su - max -c "/acl/test"
#su - john -c "/acl/test"

#getfacl /acl/test
#setfacl -m mask::r-- /acl/test
#getfacl /acl/test
```

<請觀察資訊>
<以使用者 max 身份查看檔案>成功
<以使用者 john 身份查看檔案>成功
<以使用者 max 身份執行檔案>失敗
<以使用者 john 身份執行檔案>失敗

<請觀察資訊, 此時顯示的是 ACL MASK>
<以使用者 max 身份執行檔案>失敗
<以使用者 john 身份執行檔案>成功

<設定 acl mask 為 r-->

```
#su - john -c "/acl/test" <以使用者 john 身份執行檔案失敗, 因受到 acl mask 的限制>
```

練習 default acl

```
#mkdir /acl/dir
#setfacl -d -m u:john:rwX /acl/dir/          <設定 default acl>
#getfacl /acl/dir/                            <請觀察資訊>

#touch /acl/dir/test
#ls -l /acl/dir/                              <請觀察資訊>

#getfacl /acl/dir/test                        <請觀察資訊>
#mkdir /acl/dir/john                          <請觀察資訊>

#ls -l /acl/dir/                              <請觀察資訊>
#getfacl /acl/dir/john/                      <請觀察資訊>
```