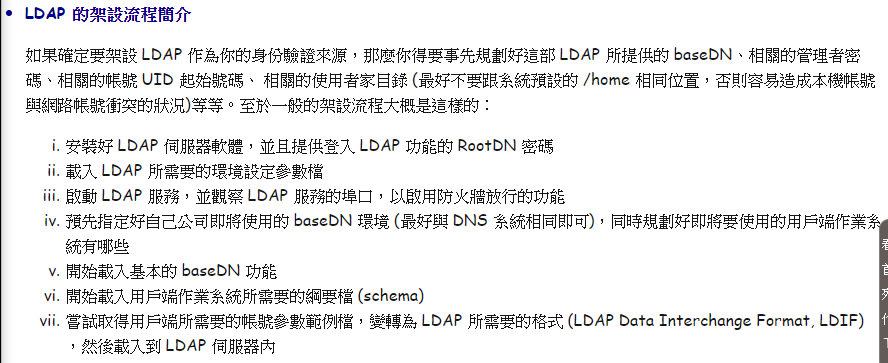
:q

(以下全部都在server底下的root操作)

ssh root@server

yum install wget –y

yum –enablerepo=PowerTools search openldap-servers

wget -q [https://repo.symas.com/configs/SOFL/rhel8/sofl.repo -O /etc/yum.repos.d/sofl.repo](https://repo.symas.com/configs/SOFL/rhel8/sofl.repo%20-O%20/etc/yum.repos.d/sofl.repo)

yum install symas-openldap-clients symas-openldap-servers

yum –enablerepo=PowerTools search migration

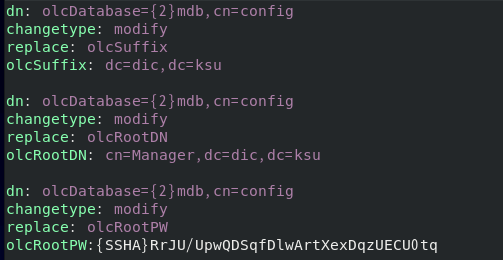
systemctl start slapd

systemctl enable slapd

mkdir ldap

cd ldap

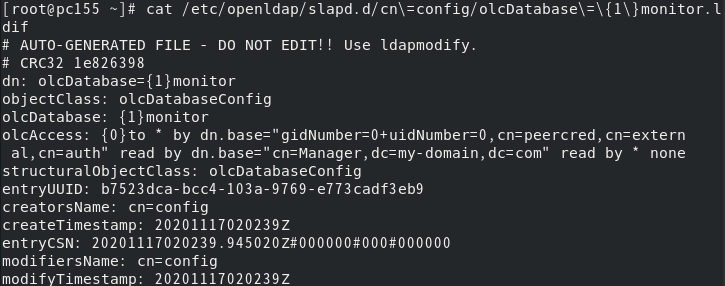
vim basedn.ldif



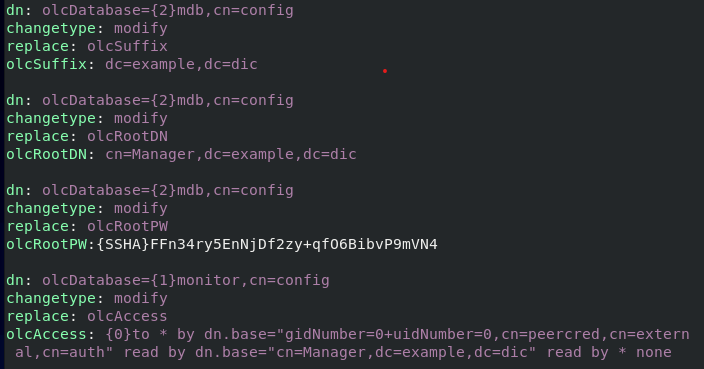
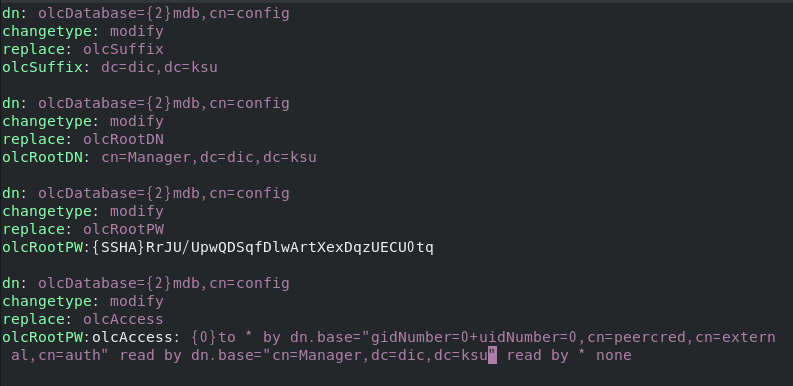
(另開視窗設置密碼)slappasswd

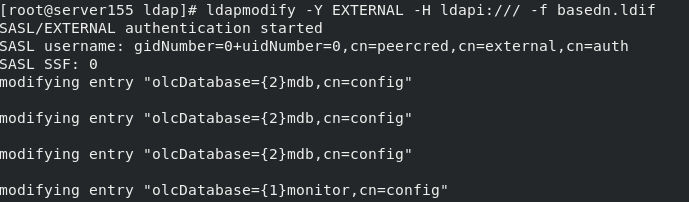
2727175

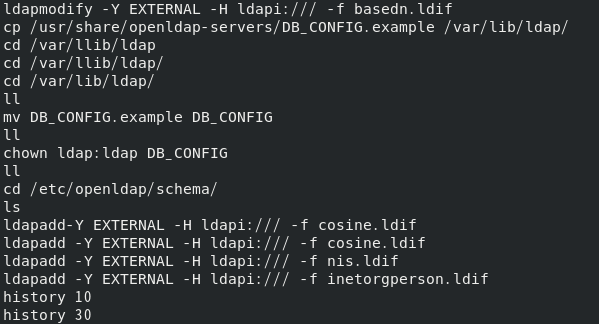
ldapmodify –Y EXTERNAL –H ldapi:/// -f basedn.ldif(另開視窗查看以下)



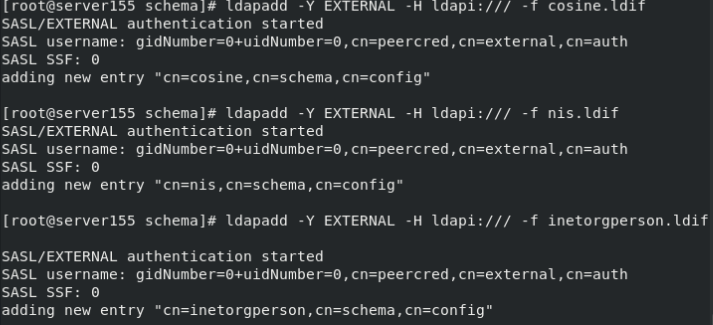
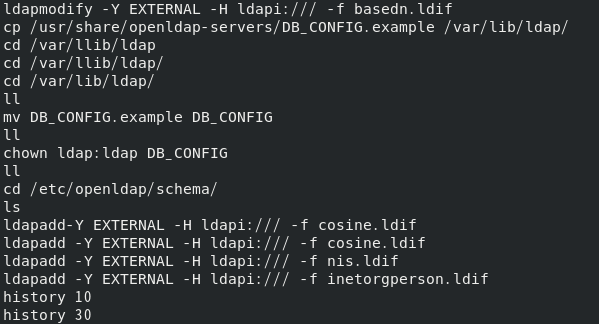
vim basedn.ldif 新增第二張圖的內容,注意:兩個dc要改







以下ldapadd有順序之分

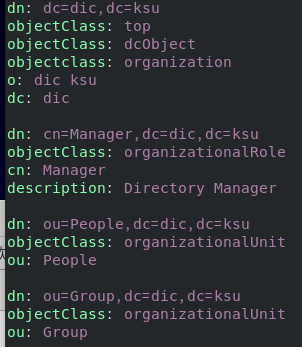


檢查是否設定好: slaptest –u

cd ~

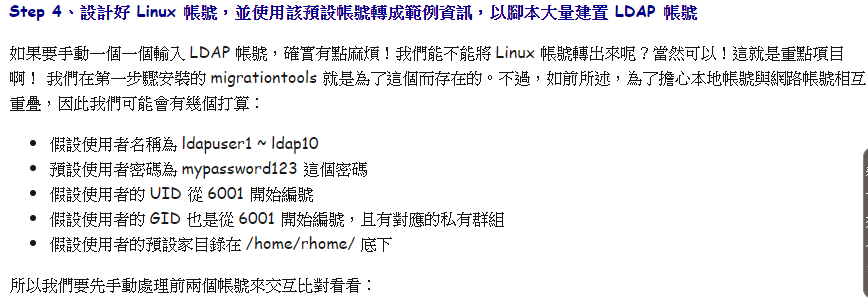
cd ldap

vim base.ldif



ldapadd -x -W -D "cn=Manager,dc=dic,dc=ksu" -f /root/ldap/base.ldif

2727175



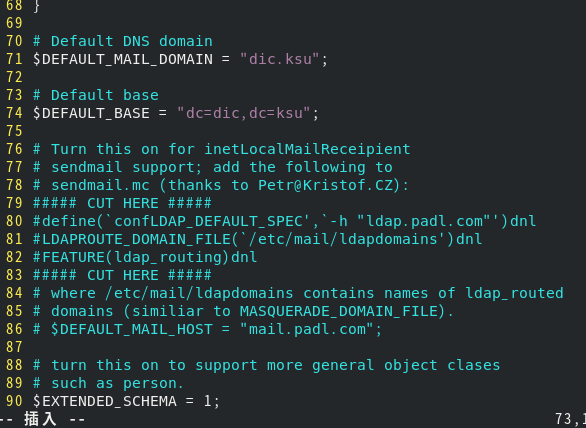
(到跟目錄)cd

(?wget http://mirror.centos.org/centos/7/os/x86\_64/Packages/migrationtools-47-15.el7.noarch.rpm

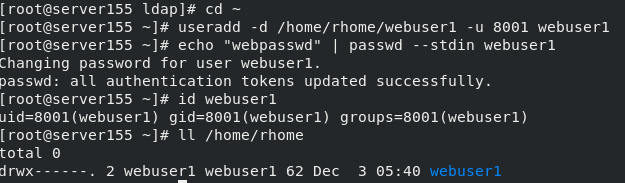


mkdir /home/rhome

**vim /usr/share/migrationtools/migrate\_common.ph**



新增帳號



[root@localhost ldap]# **grep ldapuser /etc/passwd > user.txt**

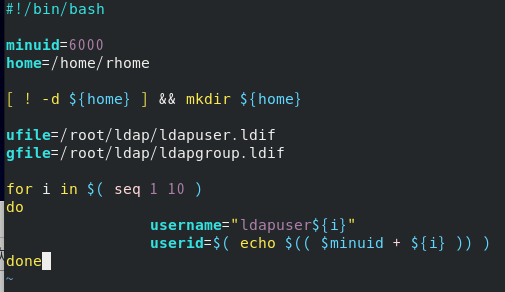
[root@localhost ldap]# **grep ldapuser /etc/group > group.txt**

[root@localhost ldap]# **/usr/share/migrationtools/migrate\_passwd.pl user.txt > user.ldif**

[root@localhost ldap]# **/usr/share/migrationtools/migrate\_group.pl group.txt > group.ldif**

[root@localhost ldap]# **cat user.ldif**

vim adduser.sh



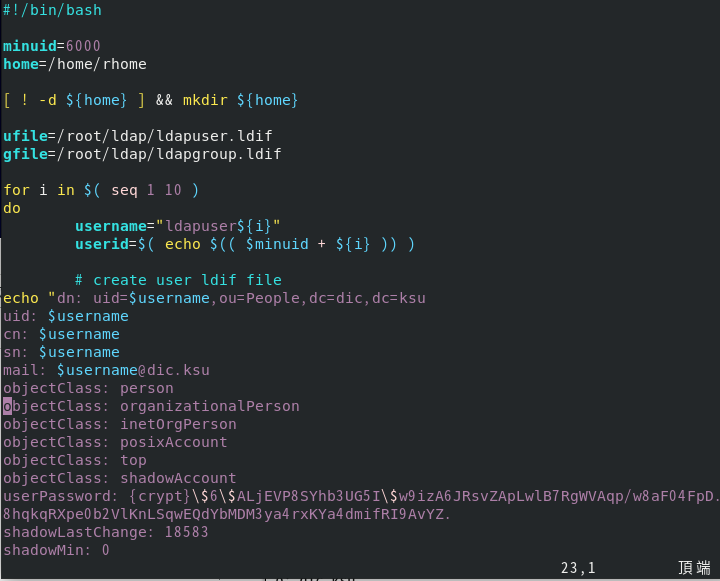
(讀檔進來):r user.ldif

:r group.ldif

:1,$s/6001/\$userid/g

:1,$s/ldapuser1/\$username/g

(最後完成以下檔adduser.sh)





sh adduser.sh

\*\*記得$前面+\ 還有要改/home/rhome改成指定目錄ex: /rhome/

(將以下檔案的dn前面加一行)

vim ldapuser.ldif

vim ldapgroup.ldif

(password:2727175)



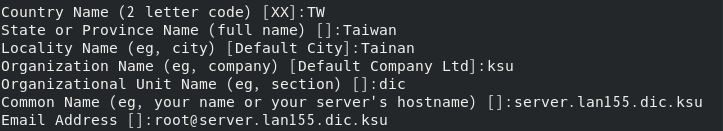
(使用 ldapsearch 檢驗 LDAP 的查詢功能)



* **Step 6、建立 LDAP Server / Client 連線時所需要的公私鑰檔案：**

**cd /etc/openldap/certs/**

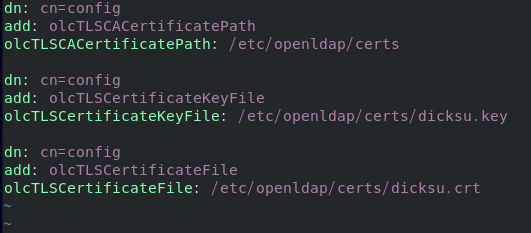
**openssh req –new –x509 –nodes –out dicksu.crt –keyout dicksu.key –days 3650**



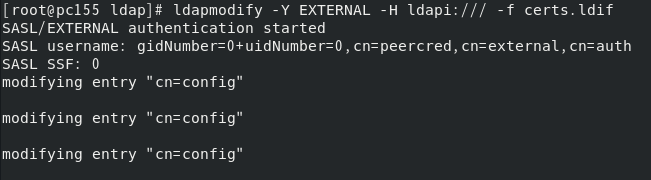
**chown ldap:ldap dicksu.\***

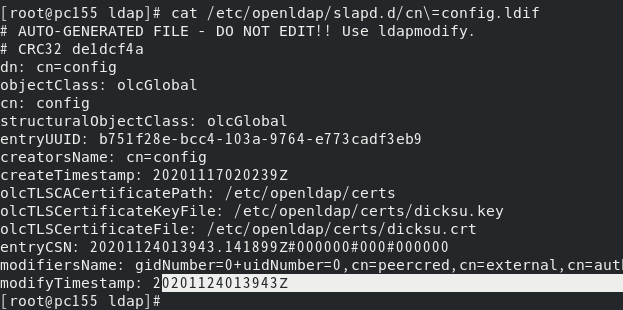
到root/ldap/

vim certs.ldif



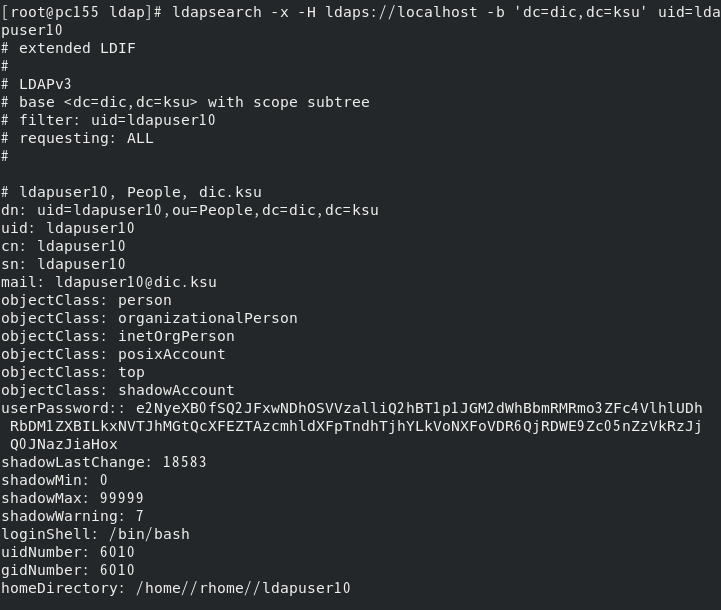
**ldapmodify -Y EXTERNAL -H ldapi:/// -f certs.ldif**

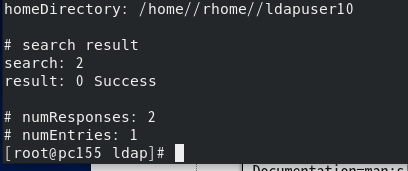




systemctl restart slapd

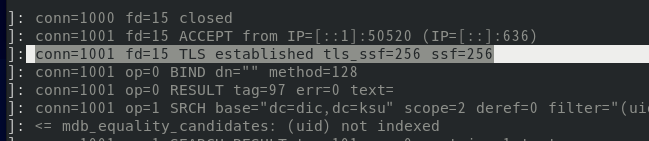






systemctl status slapd

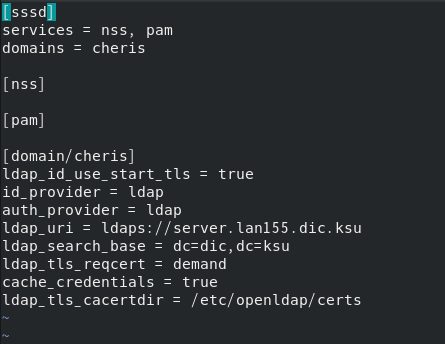
(插入以下這行)



* **Step 8、伺服器本機也使用 LDAP 作為帳號驗證**

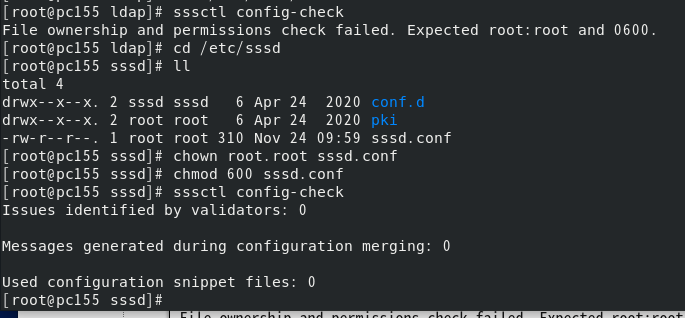
yum install sssd sssd-ldap sssd-tools –y

vim /etc/sssd/sssd.conf



會檢查是否跟之前key一樣

sssctl config-check會因權限出錯



[root@localhost ~]# **vim /etc/openldap/ldap.conf**

TLS\_REQCERT allow

BASE dc=dic,dc=ksu

URI ldaps://127.0.0.1

TLS\_CACERT /etc/openldap/certs/dicksu.crt

[root@localhost ~]# **ldapsearch -x 'uid=ldapuser1'**

**systemctl restart sssd**



* **Step 9、讓用戶端使用 LDAP Server 作為帳號驗證來源之一**

(在client/root底下)

yum install sssd sssd-ldap sssd-tools symas-openldap-clients –y

cd /etc/openldap/certs/

scp server:/etc/openldap/certs/dicksu.crt .

chown ldap:ldap dicksu.crt

scp server:/etc/sssd/sssd.conf .

vim sssd.conf

sssctl config-check

systemctl restart sssd

authselect current

id ldapuser1

cd /etc/openldap

scp server:/etc/openldap/ldap.conf .

ldapsearch –x

ldapsearch -x uid=ldapuser1

authselectl select sssd --force

systemctl restart sssd

id ldapuser1/2

su –ldapuser1



**7.5： 分享檔案系統的 NFS 伺服器**

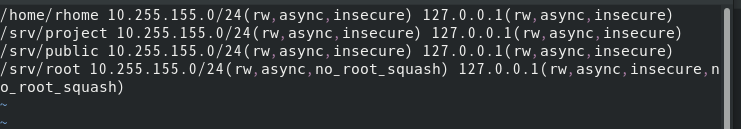
(從cllient連到server/root)

yum install nfs-utils

ll /home/rhome (會有1-10的ldap)

mkdir /home/rhome

vim /etc/exports



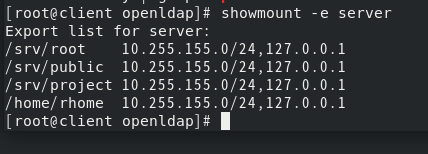
mkdir /srv/{project,public,root}

ll /srv

systemctl restart nfs-server

systemctl enable nfs-server

(在client察看結果)



mkdir /home/rhome

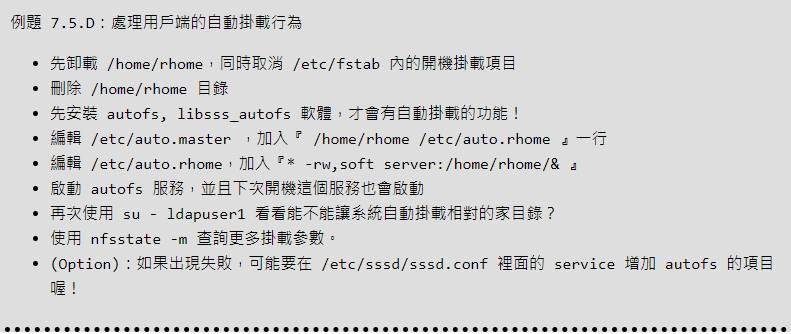
mount –t nfs server:/home/rhome /home/rhome

查看

fg

ls/home/rhome/

ls /home/rhome/ldapuser1

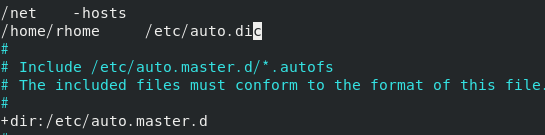


yum install autofs –y

umount /home/rhome

rmdir /home/rhome

vim /etc/auto.master

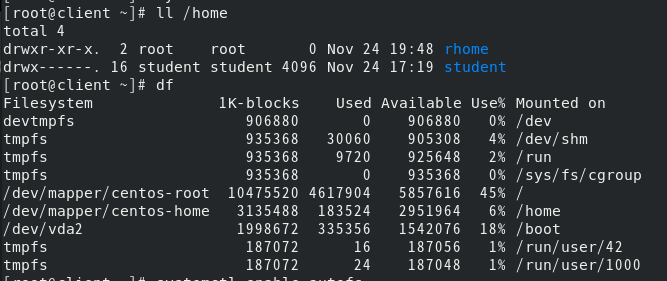


vim /etc/auto.dic

 (右邊&等同左邊\*)

systemctl restart autofs

systemctl enable autofs



su – ldapuser1(以下出現最後一行server代表掛載成功)

