SETTING IPA SERVER ON CENTOS

[centralized authentication system]

steps for installing ipa server:

step1: setting up a static ip address for the server and the host

1)In this lab the server address is

ip: 192.168.0.102
gateway:192.168.0.1
dns: 8.8.8.8

and the client address

ip:192.168.0.103
gateway: 192.168.0.1
dns:192.168.0.102 [server address]

restart the connection to take effect:

5) nmcli device down <NIC/device> / ifdown <NIC>

6) nmcli device up <NIC/device>   / ifup   <NIC>

[important note if you give the client dns to the server address you have to install packages from local repository unless you have a second nic connected to the internet because in order to work with online repository you need a public dns like 8.8.8.8 but if you use the local repo in the client its all fine]

[see the ip address section for the process of giving a static ip address]

step2: set a static host name of the server using ‘hostnamectl’ command

[server]

1) => hostnamectl set-hostname “ipa.it.local”
2) => exec bash

step2: edit the “/etc/hosts” of the server

=> vim /etc/hosts
[add this line

```
    192.168.0.102 ipa.it.local ipa
    192.168.0.103 client1.it.local        client1
```

]

step4: test with ping commnad

1)=> ping ipa.it.local

step5: update the server repository

```
1) =>yum update -y
or [if you use local repository]
yum update disablerepo="*" enablerepo='myrepo'
```

step(add): reboot the system

```
1) =>reboot
```

step6: install “free-Ipa” packages in server machine

[server]

```
1) => yum install disablerepo="*" enablerepo='myrepo' ipa-server bind-dyndb-ldap ipa-server-dns -y
```

[or you can remove all the online repo and add only the local yum repo then the command is]

```
2) => yum install ipa-server bind-dyndb-ldap ipa-server-dns -y
```

step8: install IPA server in server machine

[server]

```
1) => ipa-server-install --setup-dns
```

```
    8-1: Do you want to configure integreted DNS?
         =>yes
    8-2: Server Host name [ipa.test.system]
         =>[Enter]
```

8-3: Please confirm Domain name [test.system]?
=>[Enter]
8-4: Please provide a realm name [TEST.SYSTEM]?
=>[Enter]
8-5: Directory manager password?
=><give_a_password>
example: admin@ipa
8-6: IPA admin Password?
=><give_a_password>
example: admin@redhat
8-7: Do you want to configure DNS Forwarders?
=>yes
8-8: Do you want these servers as DNS Forwarders?
=>yes
8-9: Do you want to search for missing reverse zone?
=>no
8-10: Continue to configure the system with these values?
=>yes

step9: Configure users Home Directory and firewall

[server]

1) =>authconfig –enablemkhomedir –update

step10: adding service to firewall

1) =>firewall-cmd –premanent –add-service=’freeipa-ldap’
1) =>firewall-cmd –premanent –add-service=’ntp’
1) =>firewall-cmd –premanent –add-service=’http’
1) =>firewall-cmd –premanent –add-service=’https’
1) =>firewall-cmd –premanent –add-service=’ldap’

```
1) =>firewall-cmd –premanent –add-service=’ldaps’
1) =>firewall-cmd –premanent –add-service=’kerberos’
1) =>firewall-cmd –premanent –add-service=’kpasswd’
1) =>firewall-cmd –premanent –add-service=’dns’
2) => firewall-cmd –reload
```

step11: checking if everything running

```
1)=>ipactl status
```

step10: adding port to firewall

```
1) =>firewall-cmd --permanent --zone=public –add-port={80/tcp,443/tcp,302/tcp,636/tcp,88/tcp,464/tcp,53/tcp,88/udp,464/udp,53/udp,123/udp}
2) => firewall-cmd –reload
```

step12: initialize the admin user [varify weather the admin user get token from the kerberos] [you can login with just the user and password but to login with kerberos you have to issue the command]

[server]

```
1)=> kinit admin
    [password: ] [same password for installation during FreeIPA]
 2)=> klist
```

step12: reboot the system again

```
2)=> reboot
```

step16: Go to the administration page and login with username and password [server]

username: admin
password: <admin_password>

[go to web browser to url “http://ipa.test.system”]

step16: create a user in the administration page [server]

username: <give a username> / ex: ipa1
Firstname: ipa
lastname : user1
password : <give_password> /ex: redhat@ipa1

step16: setting reverse dns discovery

[server]

in the administration page go to

[NETWORK SERVICES] →[DNS] → [DNS ZONES] → [ADD.ARPA] → [ADD]

RECORD NAME : **103** //because the last number of ip is 103 [192.168.0.**103**]

RECORD TYPE: PTR

HOSTNAME: client1.it.local**.**

[remember the (.) after the client.it.local in the hostname is important]
Thats all the server configuration now we have to configure the client

SETTING IPA CLIENT ON CENTOS

step1: setting up a static ip address for the server and the host
1)In this lab the client address

---

ip: 192.168.0.103
gateway:192.168.0.1
dns:192.168.0.102 [server address]

[see the ip address section for the process of giving a static ip address]

step2: setting up hostname

1) hostnamectl set-hostname client1.it.local

step3: edit the /etc/hosts file

3) vim /etc/hosts

```
192.168.0.103 client1.it.local client1
192.168.0.102 ipa.it.local ipa
```

step4: restart the NIC to take in effect

1) nmcli device down <NIC/device> / ifdown <NIC>
2) nmcli device up <NIC/device>   / ifup   <NIC>

step5: test with ping

1) ping client1.it.local
2) ping ipa.it.local

step5: install ipa-client-packages

8) yum install ipa-client

step5: install ipa-client

9) ipa-client-install [yes]

→authoraize enroll computer : admin
→ password : open12345

10) authconfig –enablemkhomedir –update

11) systemctl enable sssd

12) nslookup client1.it.local

[now logout from the session and login with the domain username and password that the in the server by admin]

SETTING NFS SERVER ON IPA SERVER

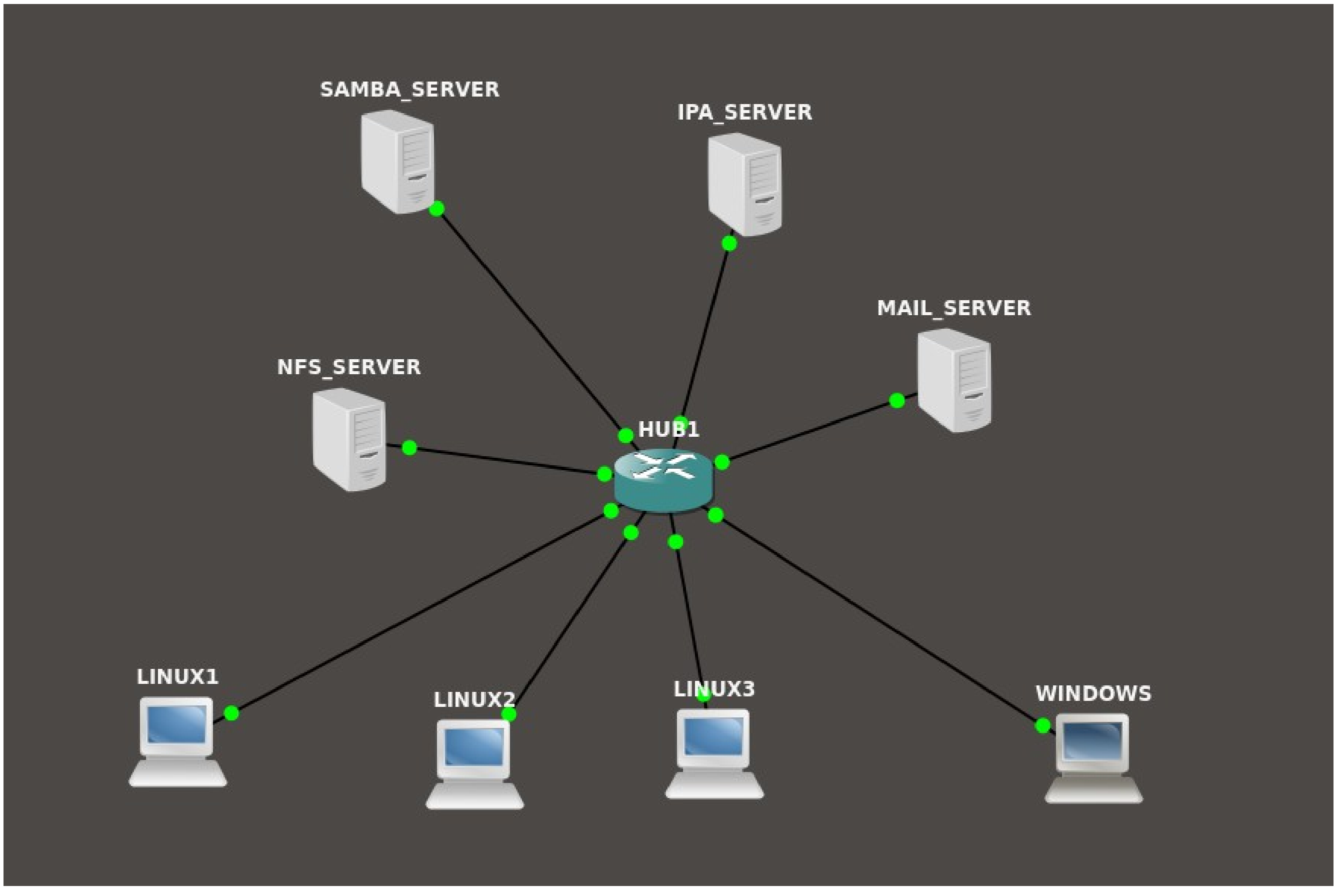
[why installing nfs server]

[because when you login from a computer with a domain user and password and store some file .in ipa server if you login with other computer ,you may login with domain user and password because of the central authentication system(ipa) but you will not find the resources that you make on the other computer with the same domain name,that means your data is not roaming .it stuck with the pc that you use .so it fails to complete the central management cause our target is no matter what ip client pc you are using you can login your domain username and password and also you will get your file .you dont need to sit in the same computer.To make that happen we make a nfs server]

[where we install the nfs server]

[you can install the nfs server in the IPA server. but it is not recommended . Although in this example we use the ipa server as

a nfs server .you can install nfs server at any active ipa client[for example you can install it on “client1”].Basically we choose a client which has a lot of space because all the users resources will save in the nfs server]



STEPS
[nfs server]

step1: choose the server

1) we choose the ipa server as a nfs server [ipa.it.local]

step2: install the nfs server packages

1) sudo yum install nfs-utils

step3: Edit the file /etc/exports

1) vim /etc/exports

```
/home *(rw,sync)
```

step3: start the nfs server

1) systemctl enable nfs-server
2) systemctl start nfs-server

step4: start the rpcbind

1) systemctl enable rpcbind
2) systemctl start rpcbind

step5: adding firewall rules

1) firewall-cmd –permanent –add-service nfs
2) firewall-cmd –reload

step6: see the mounted volume for nfs server

1) showmount -e

[if everything goes right you will see the directory that is mounted]

IPA CLIENT CONFIGURATION

[you have to configure the client1 again to sync data with nfs server]

step1: install the nfs utils packages

1) sudo yum install nfs-utils

step2: edit /etc/auto.master

1) vim /etc/auto.master

add this line:

/home /etc/auto.autofs

---

step3: create /etc/auto.autofs

1) vim /etc/auto.autofs

add this line:

syntax: * <ipa_server>:/home/&

*** ipa:/home/&**

[for example if the client1 is the nfs server the command will be
*** client1:/home/&**

remember, not the whole domain name just the client name is used
]

<u>step4: start the autofs process</u>

1) systemctl enable autofs
2) systemctl start autofs

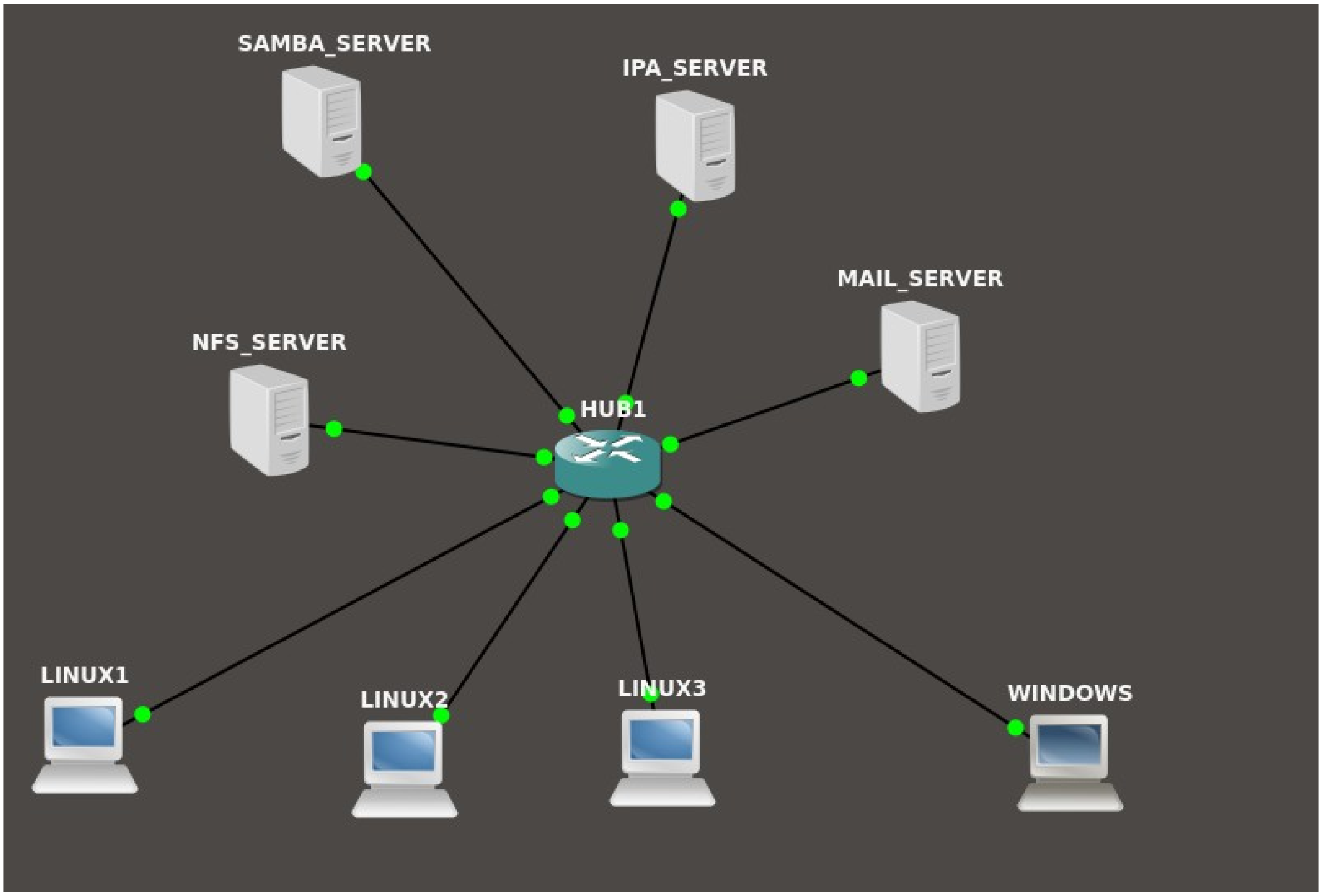
[after that you can login with any ipa client with domain and password and you will find your own resources]

SAMBA SERVER WITH IPA SERVER IN CENTOS 7

installing samba server(server side configuration):

requirements :

1) **Centos server , ip: 192.168.0.50**
2) **client (ubuntu or centos), ip: 192.168.0.100**
3) **internet connection**


SAMBA_SERVER
IPA_SERVER
MAIL_SERVER
NFS_SERVER
HUB1
LINUX1
LINUX2
LINUX3
WINDOWS

step1:

1) Create two user ‘smbuser1’ and ‘smbuser2’ with the IPA server. You can add it with the web interface or with the terminal.[this have to be done with the IPA server]

The samba server have to be a client of the IPA server . We make a client of the IPA server a samba server. And we have to add user from the IPA server and also add this user as a samba client . All the user creation is done by the IPA server. samba server will add the user as a samba user while creating the server.

step2:

update repository and install the necessary samba packages

```
=> yum update -y
=>yum install samba samba-client samba-common
```

step3:

Create a directory and give proper permission for that user and group

```
    =>mkdir /share
    =>chmod 777 /share
```

step4:

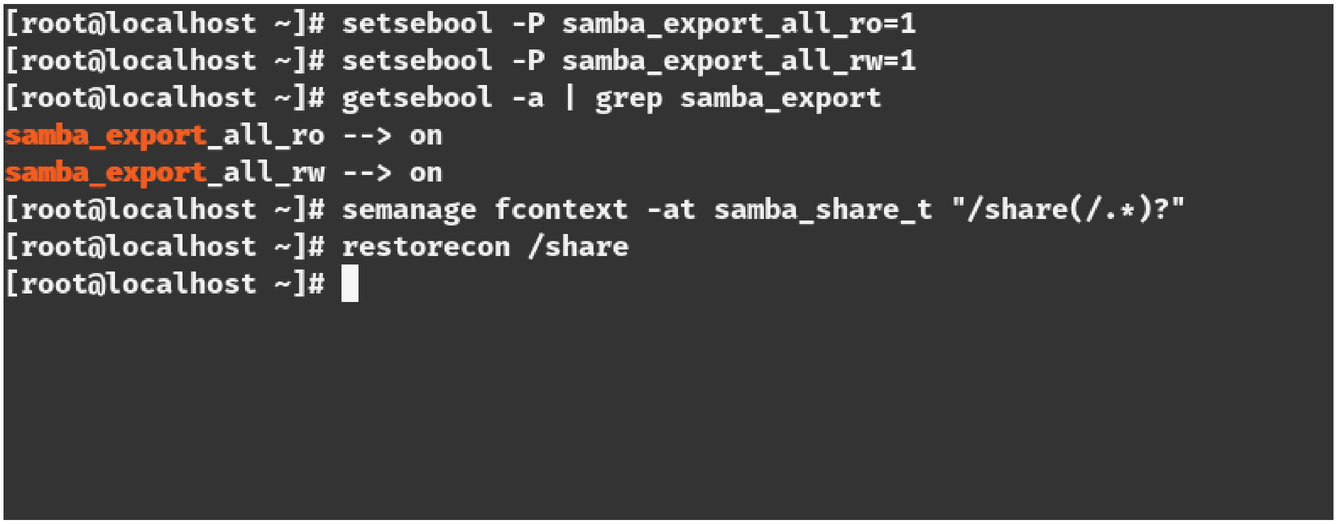
we have to add the user of the test group to the samba

```
=>smbpasswd -a smbuser1

=>smbpasswd -a smbuser2
```

step5:

Configure SElinux .you can either disable the SEinux or set the proper Boolean value and security otherwise it will not let you connect to the server. In this we are not going to disable SElinux we will change the Boolean value.

```
=> setsebool -P samba_export_all_ro=1 samba_export_all_rw=1
=> getsebool –a | grep samba_export
=> semanage fcontext –at samba_share_t "/share(/.*)?"
=> restorecon /share
```



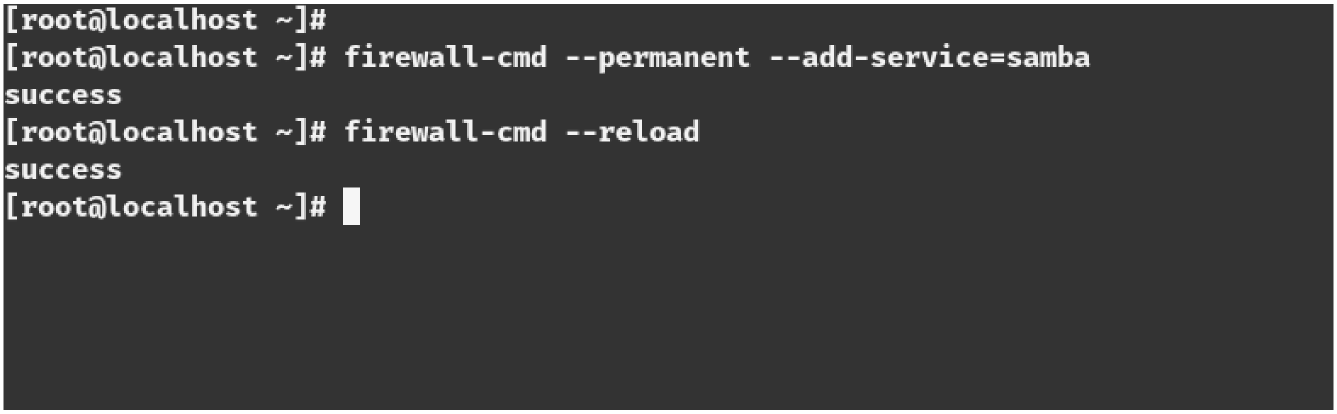
```
[root@localhost ~]# setsebool -P samba_export_all_ro=1
[root@localhost ~]# setsebool -P samba_export_all_rw=1
[root@localhost ~]# getsebool -a | grep samba_export
samba_export_all_ro --> on
samba_export_all_rw --> on
[root@localhost ~]# semanage fcontext -at samba_share_t "/share(/.*)?"
[root@localhost ~]# restorecon /share
[root@localhost ~]#
```

step6:

we have to change the firewall settings for allowing the connection

=>firewall-cmd –permanent –add-service=samba

=>firewall-cmd –reload



```
[root@localhost ~]#
[root@localhost ~]# firewall-cmd --permanent --add-service=samba
success
[root@localhost ~]# firewall-cmd --reload
success
[root@localhost ~]#
```

step7:

This is the most important path of the part.we need to edit the configuration of the samba share

=> vim /etc/samba/smb.conf

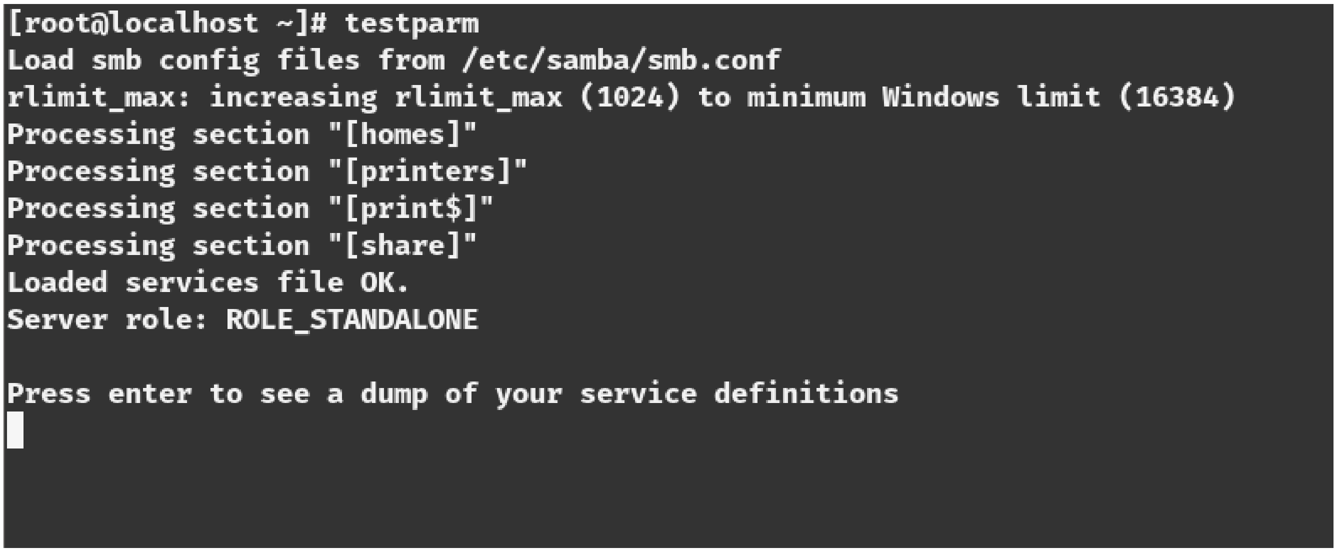
```
[share]

comment=Directory for for samba share
browsable=yes
path=/share
writable = no
write list = smbuser1
```

---

step8:

Test the configuration with the ‘testparm’ command.if there is any error in the configuration this command will tell you that

=>testparm



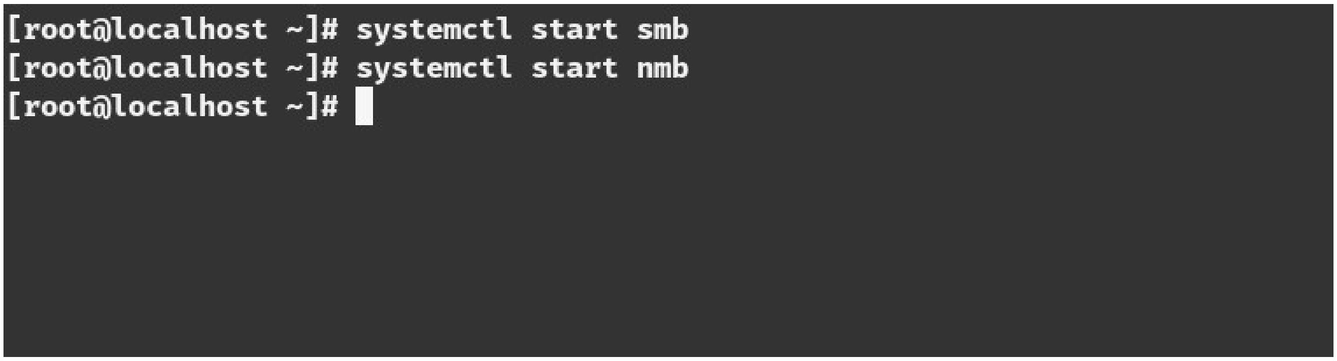
```
[root@localhost ~]# testparm
Load smb config files from /etc/samba/smb.conf
rlimit_max: increasing rlimit_max (1024) to minimum Windows limit (16384)
Processing section "[homes]"
Processing section "[printers]"
Processing section "[print$]"
Processing section "[share]"
Loaded services file OK.
Server role: ROLE_STANDALONE

Press enter to see a dump of your service definitions
```

step9:

restart the samba server to make the change the in effect

=>systemctl start smb

=>systemctl start nmb



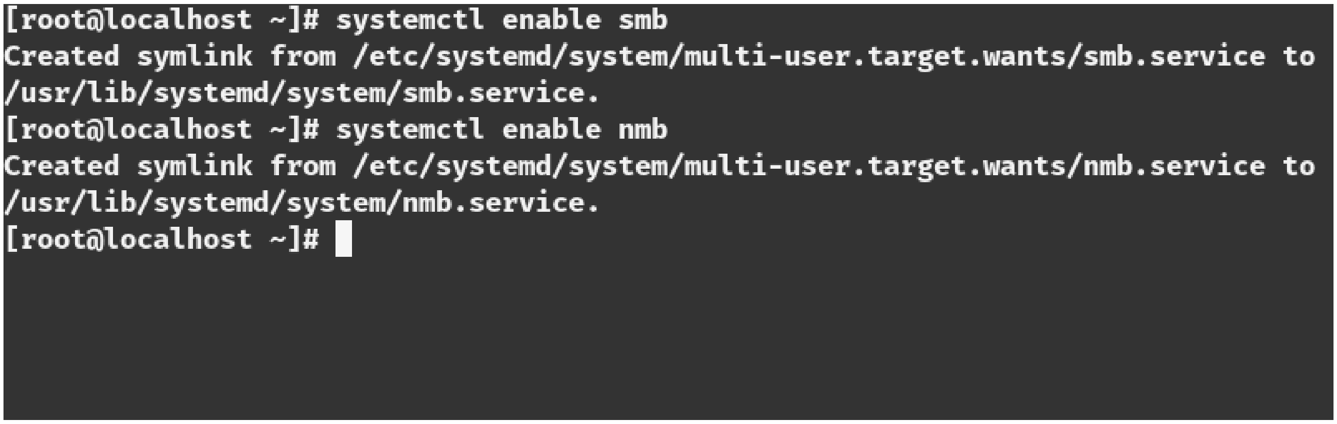
```
[root@localhost ~]# systemctl start smb
[root@localhost ~]# systemctl start nmb
[root@localhost ~]# 
```

step10:

we have to enable the smb and nmb service to make start this on boot time

=>systemctl enable smb

=>systemctl enable nmb

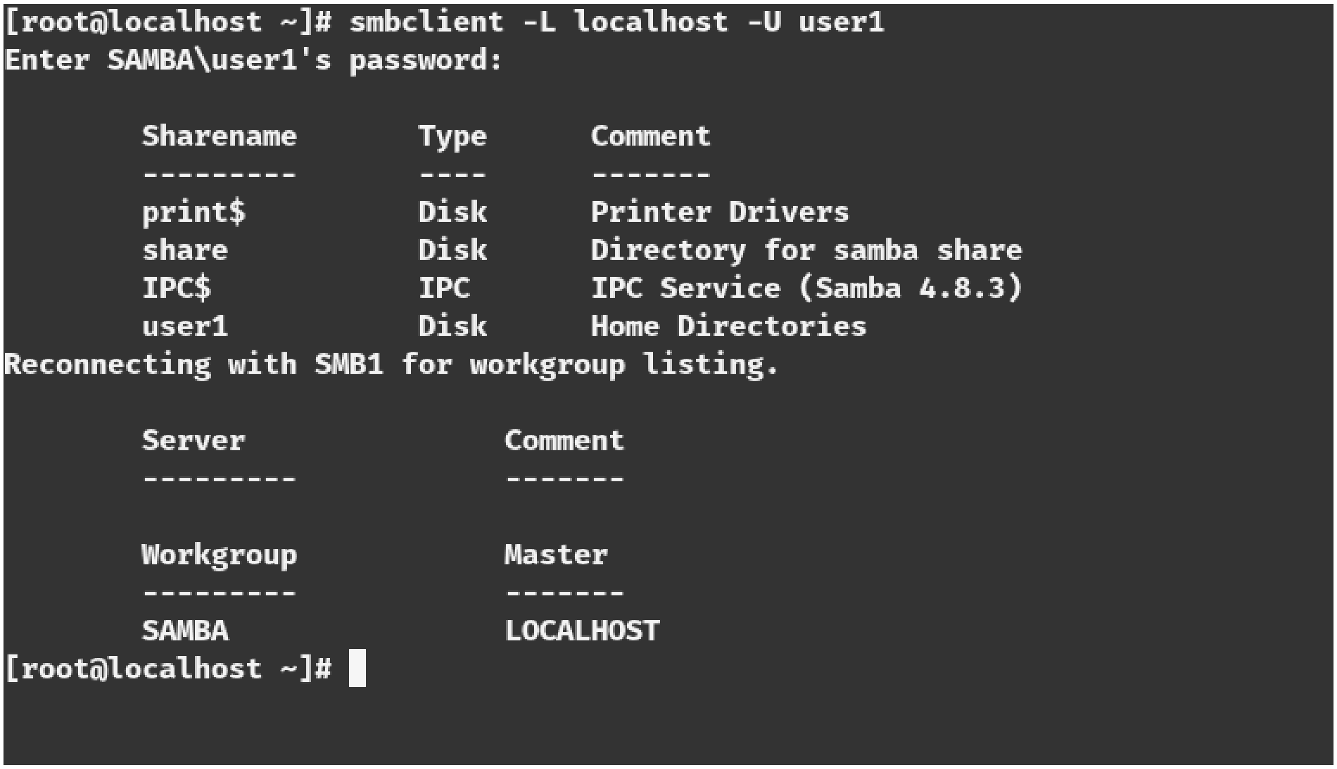


```
[root@localhost ~]# systemctl enable smb
Created symlink from /etc/systemd/system/multi-user.target.wants/smb.service to
/usr/lib/systemd/system/smb.service.
[root@localhost ~]# systemctl enable nmb
Created symlink from /etc/systemd/system/multi-user.target.wants/nmb.service to
/usr/lib/systemd/system/nmb.service.
[root@localhost ~]#
```

step11:

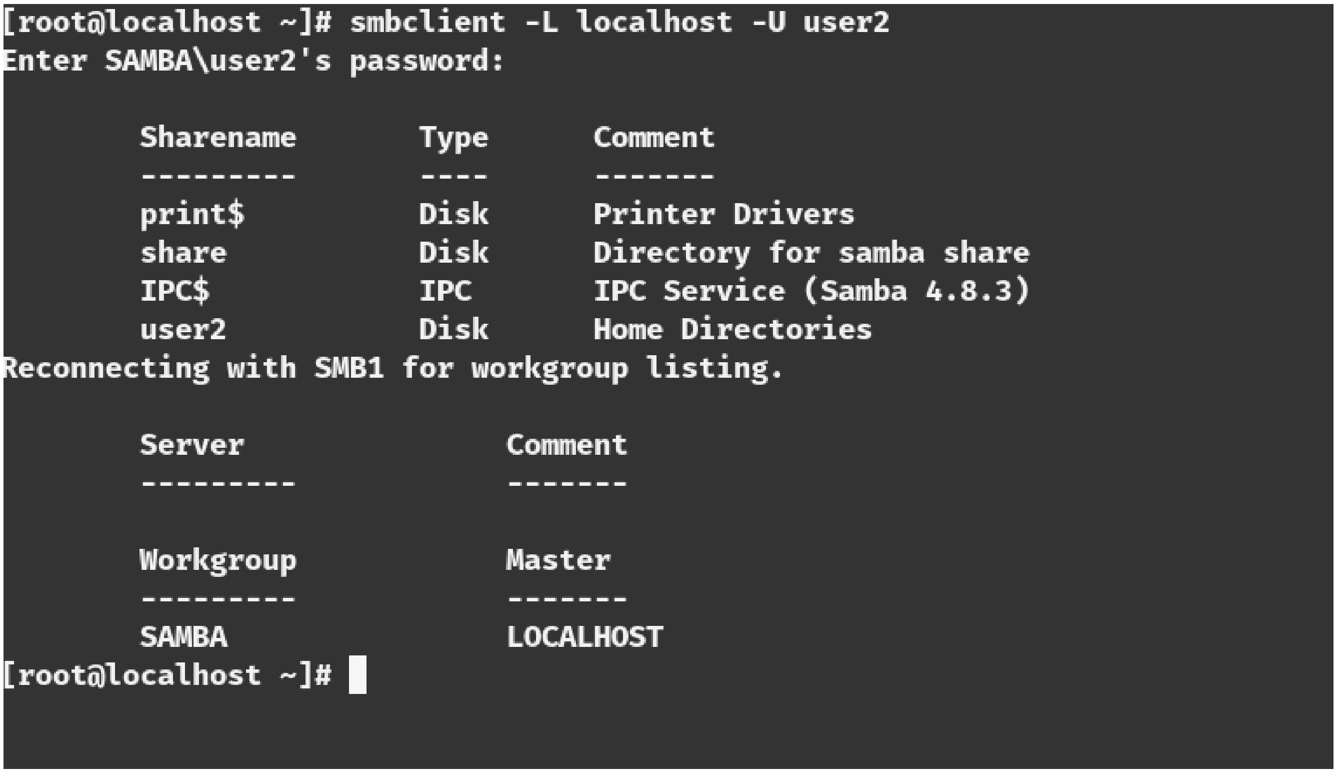
Test the connection from the server

=>smbclient -L localhost -U smbuser1



```
[root@localhost ~]# smbclient -L localhost -U user1
Enter SAMBA\user1's password:

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        share           Disk      Directory for samba share
        IPC$            IPC       IPC Service (Samba 4.8.3)
        user1           Disk      Home Directories
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        SAMBA                LOCALHOST
[root@localhost ~]#
```

=>smbclient -L localhost -U user2



```
[root@localhost ~]# smbclient -L localhost -U user2
Enter SAMBA\user2's password:

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        share           Disk      Directory for samba share
        IPC$            IPC       IPC Service (Samba 4.8.3)
        user2           Disk      Home Directories
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        SAMBA                LOCALHOST
[root@localhost ~]#
```

installing samba Client(linux client):

step1:

install packages in the client

=>yum update -y

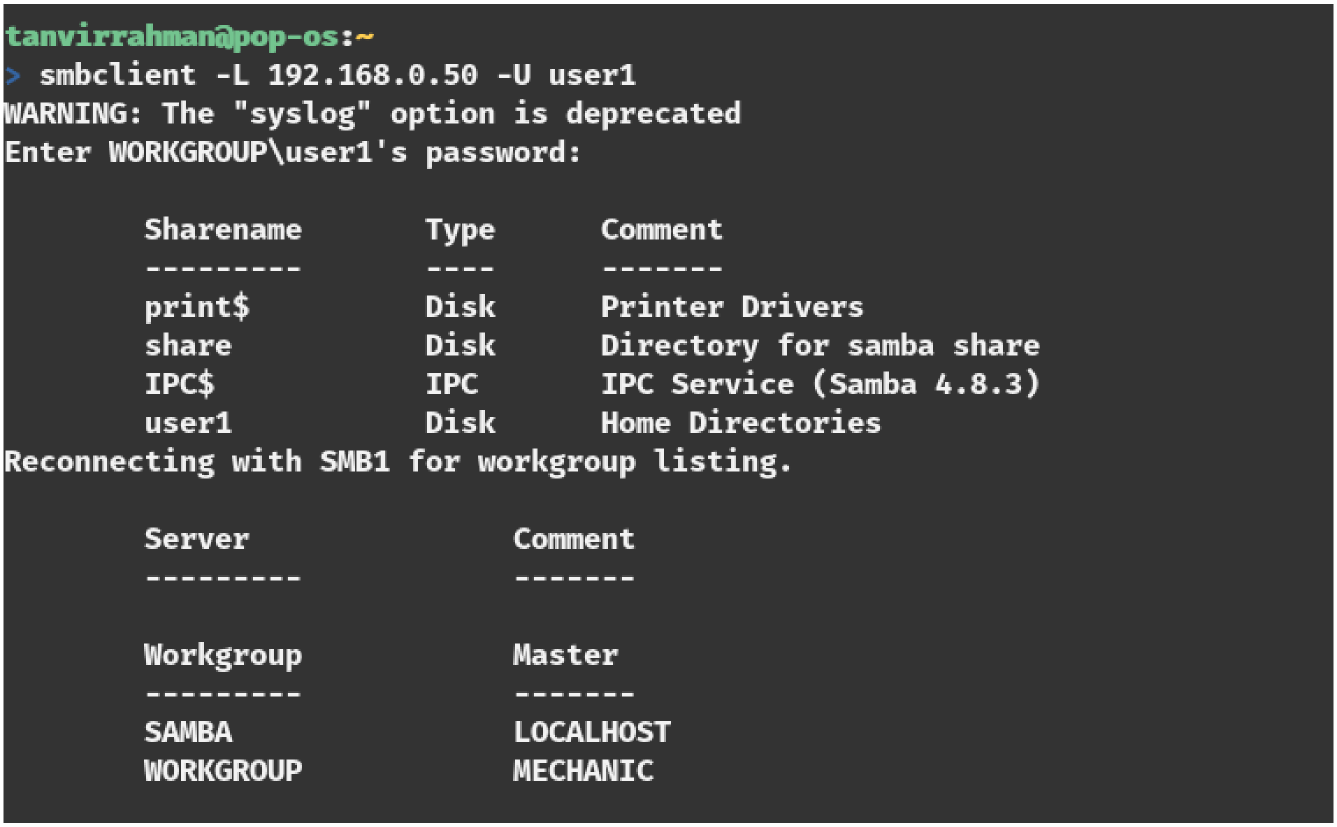
```
=>yum  install samba samba-client samba-common -y
```

```
=>yum install cifs-utils -y
```

step2:

Test the connection from the client

```
=>smbclient -L 192.168.0.50 -U smbuser1
```



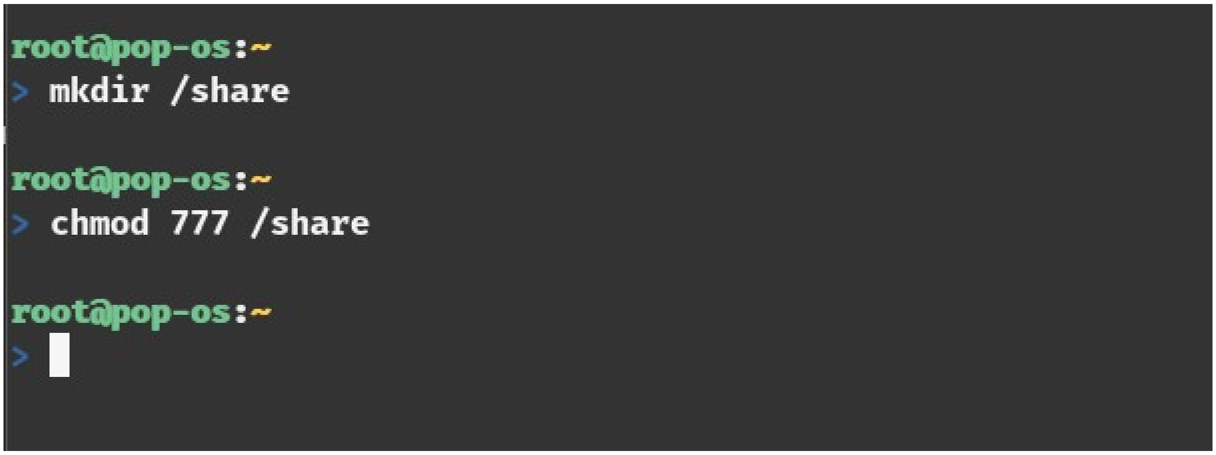
```
tanvirrahman@pop-os:~
> smbclient -L 192.168.0.50 -U user1
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\user1's password:

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        share           Disk      Directory for samba share
        IPC$            IPC       IPC Service (Samba 4.8.3)
        user1           Disk      Home Directories
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        SAMBA                LOCALHOST
        WORKGROUP            MECHANIC
```

step3:

make the directory for mounting and give the proper permission

=>mkdir /share

=>chmod 777 /share

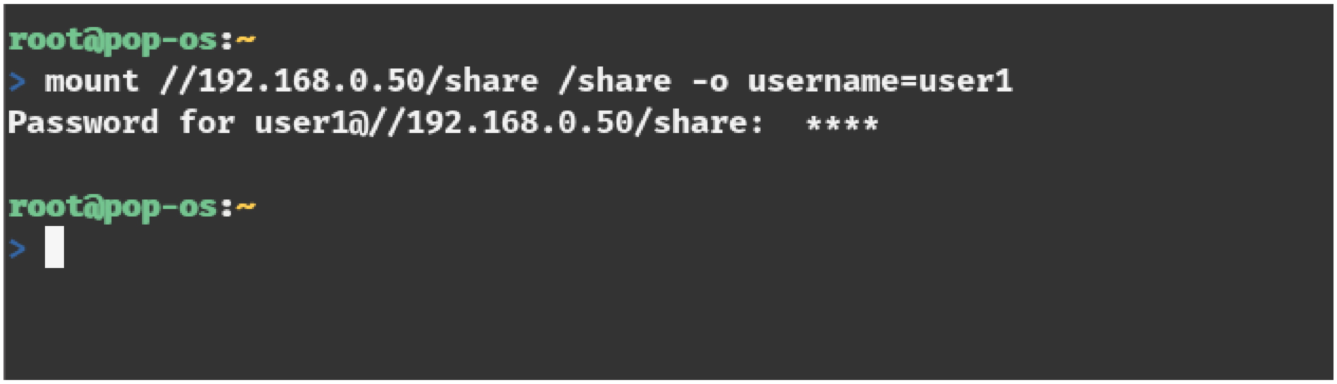


```
root@pop-os:~
> mkdir /share

root@pop-os:~
> chmod 777 /share

root@pop-os:~
> 
```

step4:

mount the the network share

=>mount //192.168.0.50/share /share -o username=smbuser1



```
root@pop-os:~
> mount //192.168.0.50/share /share -o username=user1
Password for user1@//192.168.0.50/share:  ****

root@pop-os:~
> 
```

step5:

see the the network share

=>mount | grep cifs

Additional step(permanent mount):

adding a credential file in /share folder

=> vim /share/.smbcredentials

```
username=smbuser1

password=<password_for_user_1>
```

adding an entry to the ‘/etc/fstab’ file

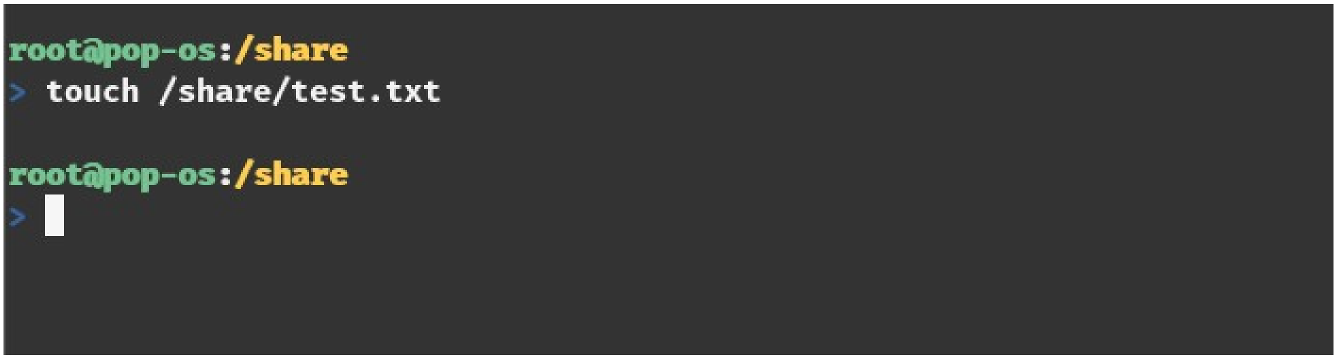
=>vim /etc/fstab

```
//192.168.0.50/share /share cifs credentials=/share/.smbcredentials
```

Test the share:

create a file in the /share folder from the client side

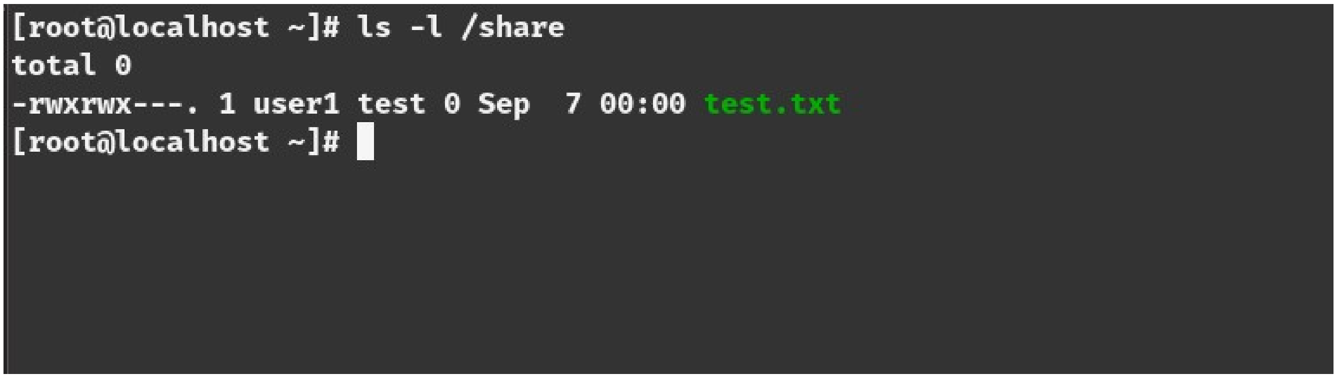
=>touch /share/test.txt



```
root@pop-os:/share
> touch /share/test.txt

root@pop-os:/share
> 
```

Now test from the server side

=>ls -l /share



```
[root@localhost ~]# ls -l /share
total 0
-rwxrwx---. 1 user1 test 0 Sep  7 00:00 test.txt
[root@localhost ~]# 
```