QUẢN TRỊ MẠNG

TUẦN 6

BACKUP DOMAIN – CHILD DOMAIN – CENTOS PRIMARY DOMAIN CONTROLLER

Hướng dẫn làm bài:

Samba PDC:

- **OS:** CentOS 7 Minimal server
- **Hostname:** server.unixmen.local
- **IP Address:** 192.168.1.150/24
- **Samba Domain:** UNIXMEN

Client:

- **OS:** Windows 7 32 bit
- **Hostname:** mywindesktop
- **IP Address:** 192.168.1.100/24

Well, now let us dive into the Samba PDC setup.

Installation

Run the following command to install samba packages.

```
yum install samba* -y
```

To verify the version of Samba, enter the following commands:

```
smbd -V


smbclient -V
```

The output will be as below:

```
Version 4.1.1
```

Samba Configuration

Edit samba default configuration file;

```
vi /etc/samba/smb.conf
```

Find the following lines, and make the changes as shown below. Replace UNIXMEN with your own domain name.

```
[Global]

  workgroup = UNIXMEN

  security = user

  domain master = yes

  domain logons = yes

  local master = yes

  preferred master = yes

  passdb backend = tdbsam

  logon path = \\%L\Profiles\%U

  logon script = logon.bat

   add machine script = /usr/sbin/useradd -d /dev/null -g 200 -s
/sbin/nologin -M %u
```

```
[homes]

  comment = Home Directories

  browseable = yes

  writable = yes



[printers]

  comment = All Printers

  path = /var/spool/samba

  printable = Yes

  print ok = Yes

  browseable = No



[netlogon]

  comment = Network Logon Service

  path = /var/lib/samba/netlogon

  browseable = No

  writable = No
```

```
[Profiles]

  path = /var/lib/samba/profiles

  create mask = 0755

  directory mask = 0755

  writable = Yes
```

To make this much simple, move your old **smb.conf** file to a safe location.

```
mv /etc/samba/smb.conf /etc/samba/smb.conf.bak
```

Create a new **smb.conf** file under /etc/samba/ directory;

```
vi /etc/samba/smb.conf
```

and copy/paste the above lines. Don’t forget to change the Domain name with your own.

Save and close the file

Test Samba configuration file syntax errors using the following command:

```
testparm
```

Your output might look like below.

```
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 "[netlogon]"

Processing section "[Profiles]"

Loaded services file OK.

Server role: ROLE_DOMAIN_PDC

Press enter to see a dump of your service definitions



[global]

    workgroup = UNIXMEN

    add machine script = /usr/sbin/useradd -d /dev/null -g 200 -s
/sbin/nologin -M %u

    logon script = logon.bat

    logon path = \\%L\Profiles\%U

    domain logons = Yes

    preferred master = Yes

    domain master = Yes

    idmap config * : backend = tdb
```

```
[homes]

    comment = Home Directories

    read only = No



[printers]

    comment = All Printers

    path = /var/spool/samba

    printable = Yes

    print ok = Yes

    browseable = No



[netlogon]

    comment = Network Logon Service

    path = /var/lib/samba/netlogon

    browseable = No



[Profiles]
```

```
    path = /var/lib/samba/profiles

    read only = No

    create mask = 0755
```

Create the shares with proper permissions which we have mentioned in the **smb.conf** file

```
mkdir -m 1777 /var/lib/samba/netlogon

mkdir -m 1777 /var/lib/samba/profiles
```

Now, create the users whom you want to login to the domain.

```
useradd user1

useradd user2
```

Create Machine accounts:

You need to create **machine account** for every machine in order to allow domain login from Windows machines. The machine account are special accounts with **$** at the end, i.e. **machine$**. The system accounts for machines do not need login shell neither home directory.

Add a new group named “machine” with group id “200”.

```
groupadd -g 200 machine
```

To add a Samba machine account, run the following command:

```
smbpasswd -m -a machine1$
```

Here, **smbpasswd -m ....** – tells that account will be used as NT primary domain controller (Machine account).

Create Samba user accounts:

```
smbpasswd -a root

smbpasswd -a user1

smbpasswd -a user2
```

Here, **'root'** user is the administrator that can be used to join the Windows NT/2000/XP/7 systems to be part of the domain. In this case, do not provide ***smbpasswd*** with the same password as the actual root account on the server. Create a different password to be used solely for creating computer accounts. This will reduce the possibility of compromising the root password.

Start Samba services:

Finally start samba services and enable them to start automatically on every boot.

```
systemctl start smb

systemctl start nmb

systemctl enable smb

systemctl enable nmb
```

Lưu ý nhỏ: nếu không muốn chỉnh firewall, có thể stop và disabled firewall, nếu làm điều này thì không cần quan tâm bước cấu hình firewall.

Firewall Configuration:

Samba uses the following Ports when runs as an Active Directory Domain Controller:

Service	Port	protocol
DNS	53	tcp/udp
Kerberos	88	tcp/udp
End Point Mapper (DCE/RPC Locator Service)	135	tcp
NetBIOS Name Service	137	udp
NetBIOS Datagram	138	udp
NetBIOS Session	139	tcp
LDAP	389	tcp/udp
SMB over TCP	445	tcp
Kerberos kpasswd	464	tcp/udp
LDAPS (only if “tls enabled = yes”)	636	tcp
Dynamic RPC Ports*	1024-5000	tcp
Global Cataloge	3268	tcp
Global Cataloge SSL (only if “tls enabled = yes”)	3269	tcp
Multicast DNS	5353	tcp/udp

Run the following commands one by one to allow Samba ports through firewall.

```
firewall-cmd --permanent --add-port=53/tcp

firewall-cmd --permanent --add-port=53/udp

firewall-cmd --permanent --add-port=88/tcp
```

```
firewall-cmd --permanent --add-port=88/udp

firewall-cmd --permanent --add-port=135/tcp

firewall-cmd --permanent --add-port=137/tcp

firewall-cmd --permanent --add-port=137/udp

firewall-cmd --permanent --add-port=138/udp

firewall-cmd --permanent --add-port=139/tcp

firewall-cmd --permanent --add-port=389/tcp

firewall-cmd --permanent --add-port=389/udp

firewall-cmd --permanent --add-port=445/tcp

firewall-cmd --permanent --add-port=464/tcp

firewall-cmd --permanent --add-port=464/udp

firewall-cmd --permanent --add-port=636/tcp

firewall-cmd --permanent --add-port=1024-5000/tcp

firewall-cmd --permanent --add-port=1024-5000/udp

firewall-cmd --permanent --add-port=3268/tcp

firewall-cmd --permanent --add-port=3269/tcp

firewall-cmd --permanent --add-port=5353/tcp
```

```
firewall-cmd --permanent --add-port=5353/udp
```

Finally restart firewall service.

```
firewall-cmd --reload
```

SELinux Configuration:

Apply the proper SELinux policies to Samba domain controller.

```
setsebool -P samba_domain_controller on

setsebool -P samba_enable_home_dirs on
```

Also to the Samab shares which we have defined in the **smb.conf** file.

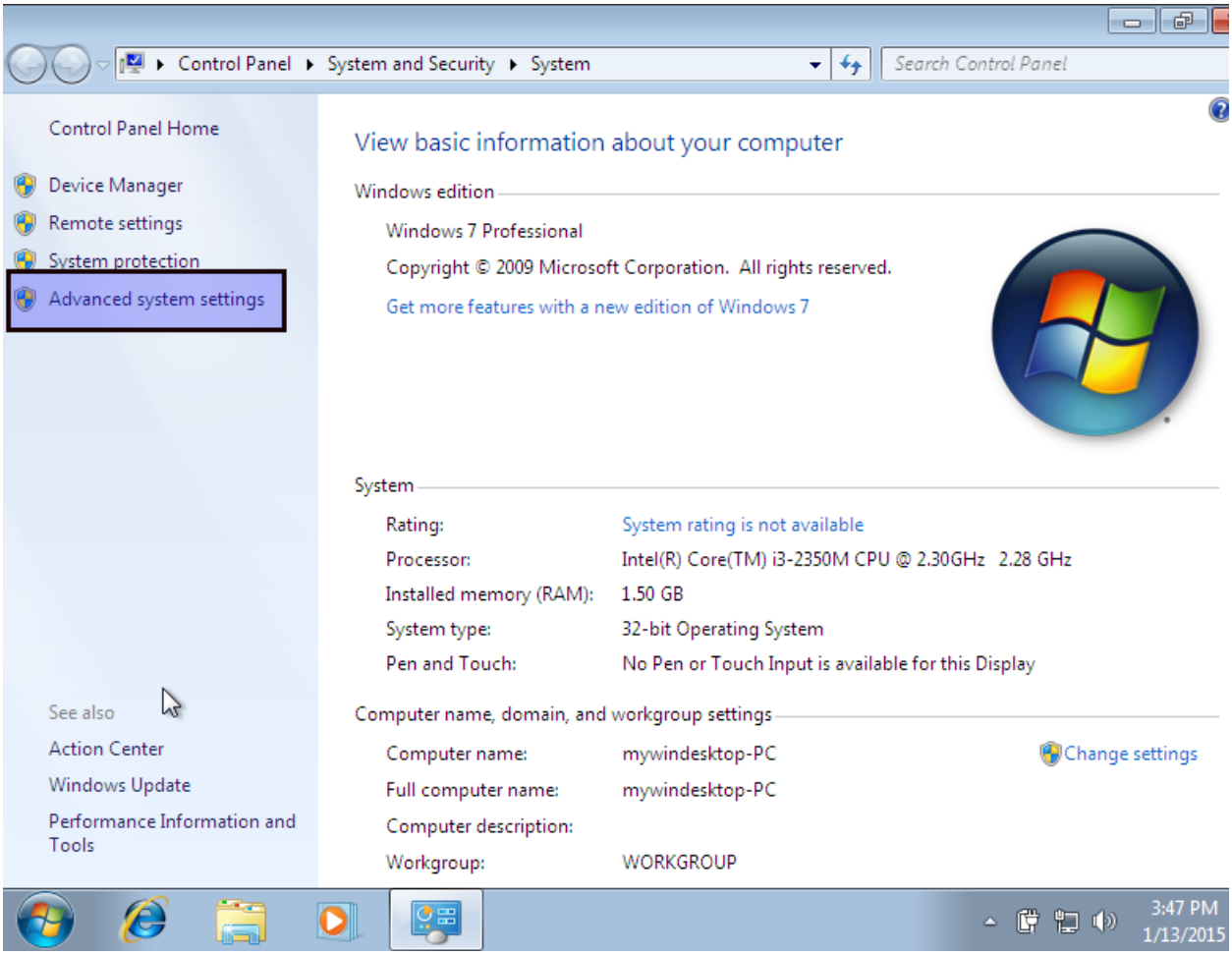
```
chcon -t samba_share_t /var/lib/samba/netlogon

chcon -t samba_share_t /var/lib/samba/profiles
```

If you don’t want to mess up with Firewall and SELinux, simply disable them. Restart your server once you completed all above steps.

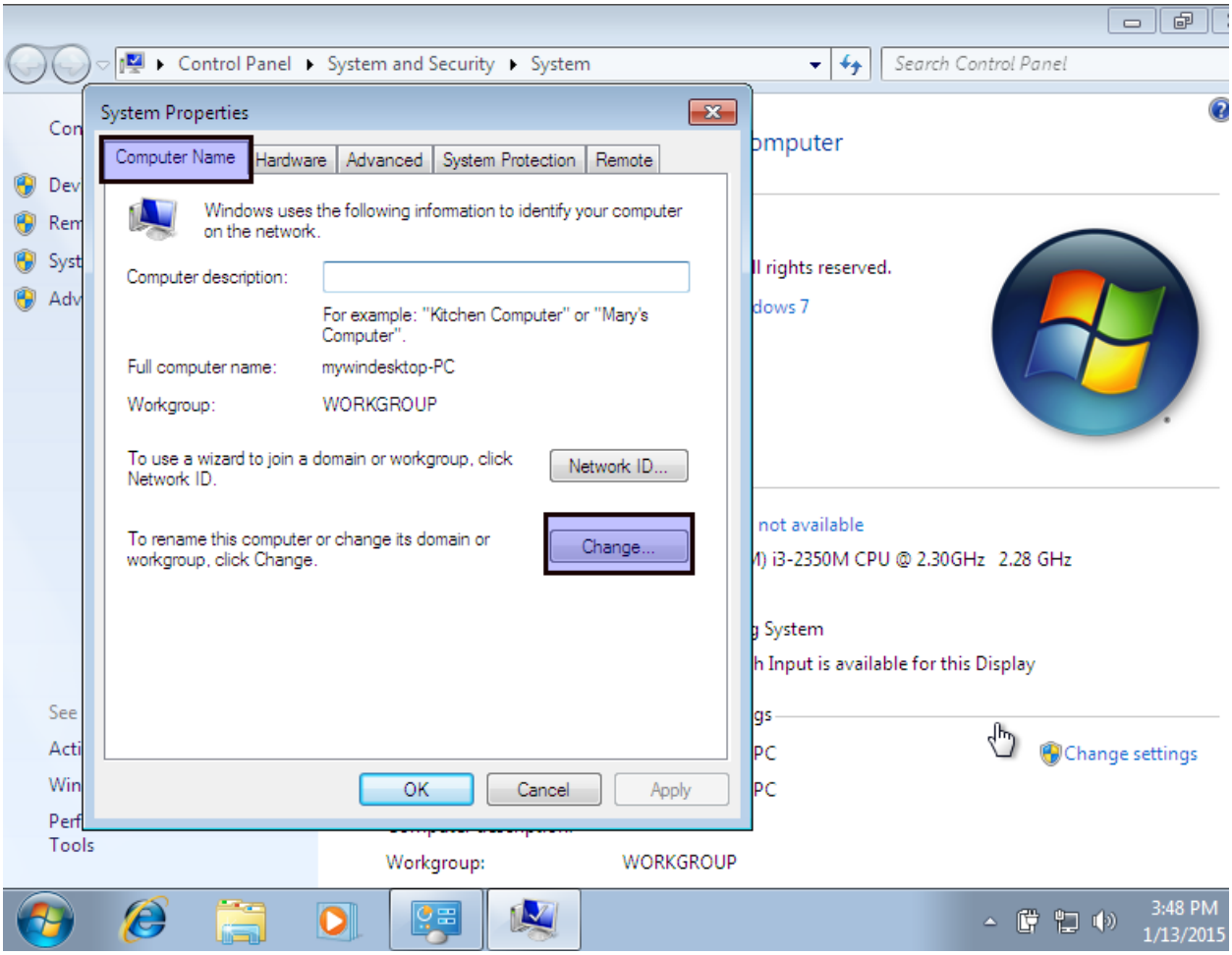
Joining Windows Clients To Samba PDC

Now try to join the samba domain from Windows OS client using the newly created user.

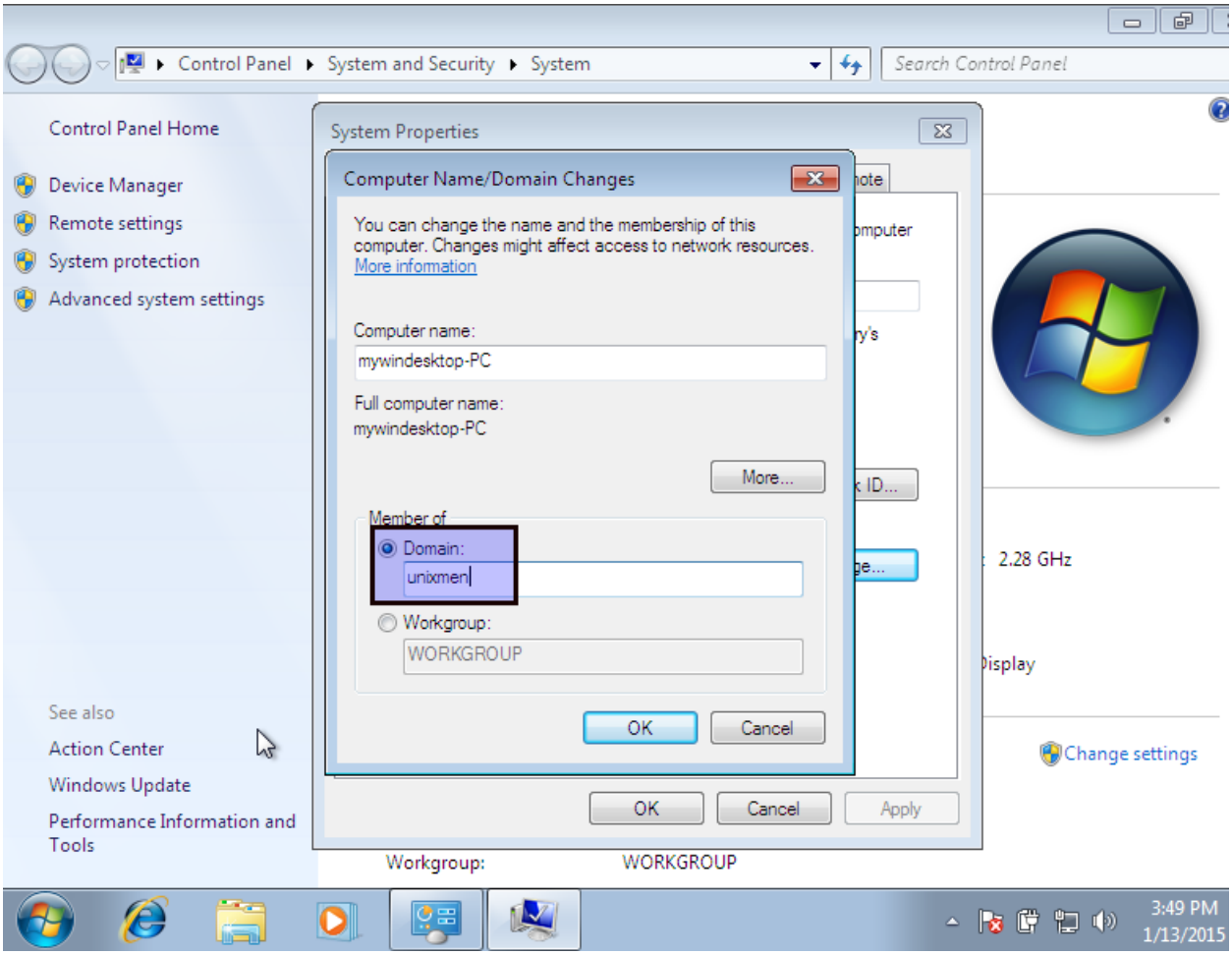
Right click on My Computer, go to **Properties ->Advanced system settings**.



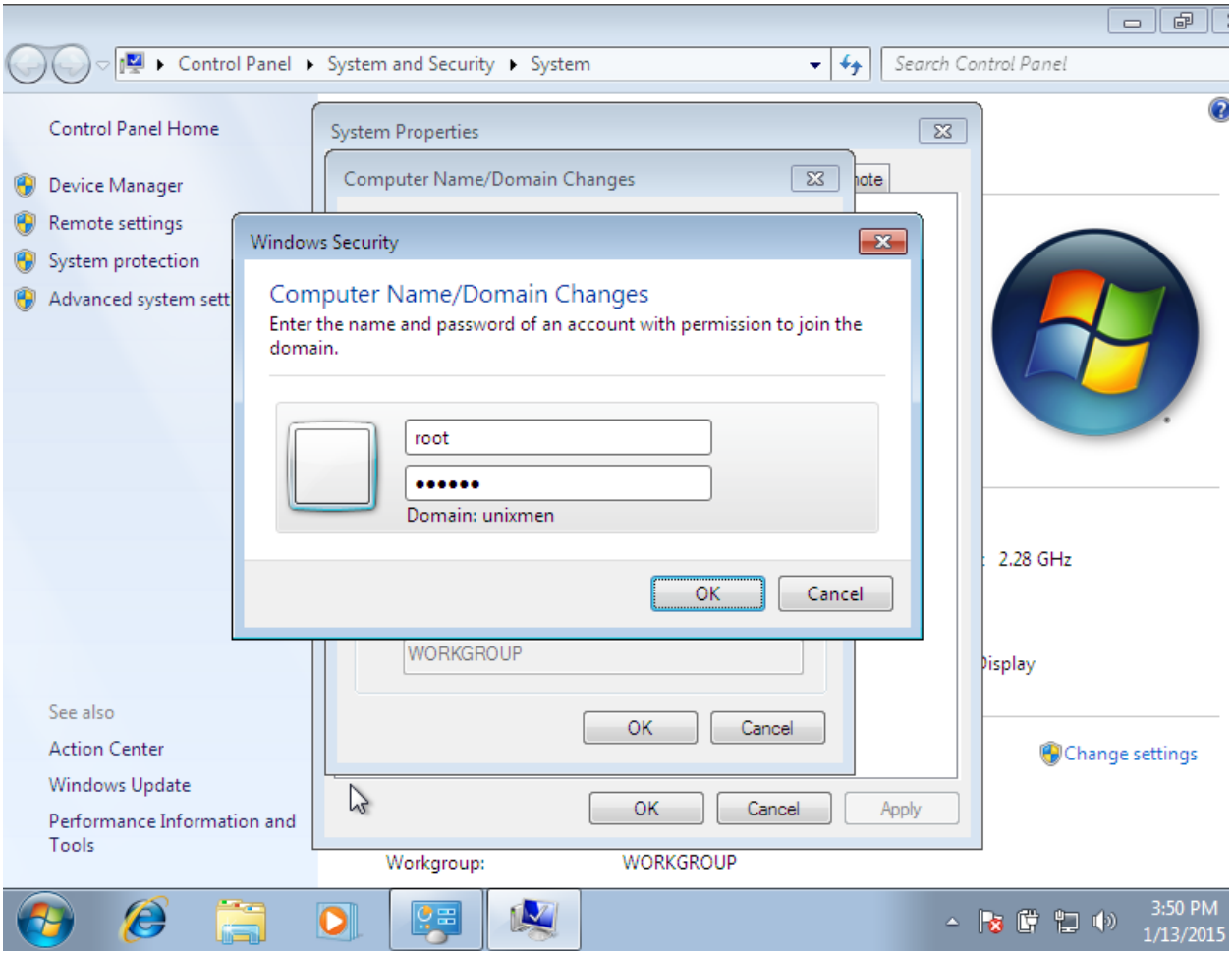
In the **Computer Name** tab, Click on the **Change** button.



In the Domain field, enter your Domain name. In my case, it's **unixmen**.

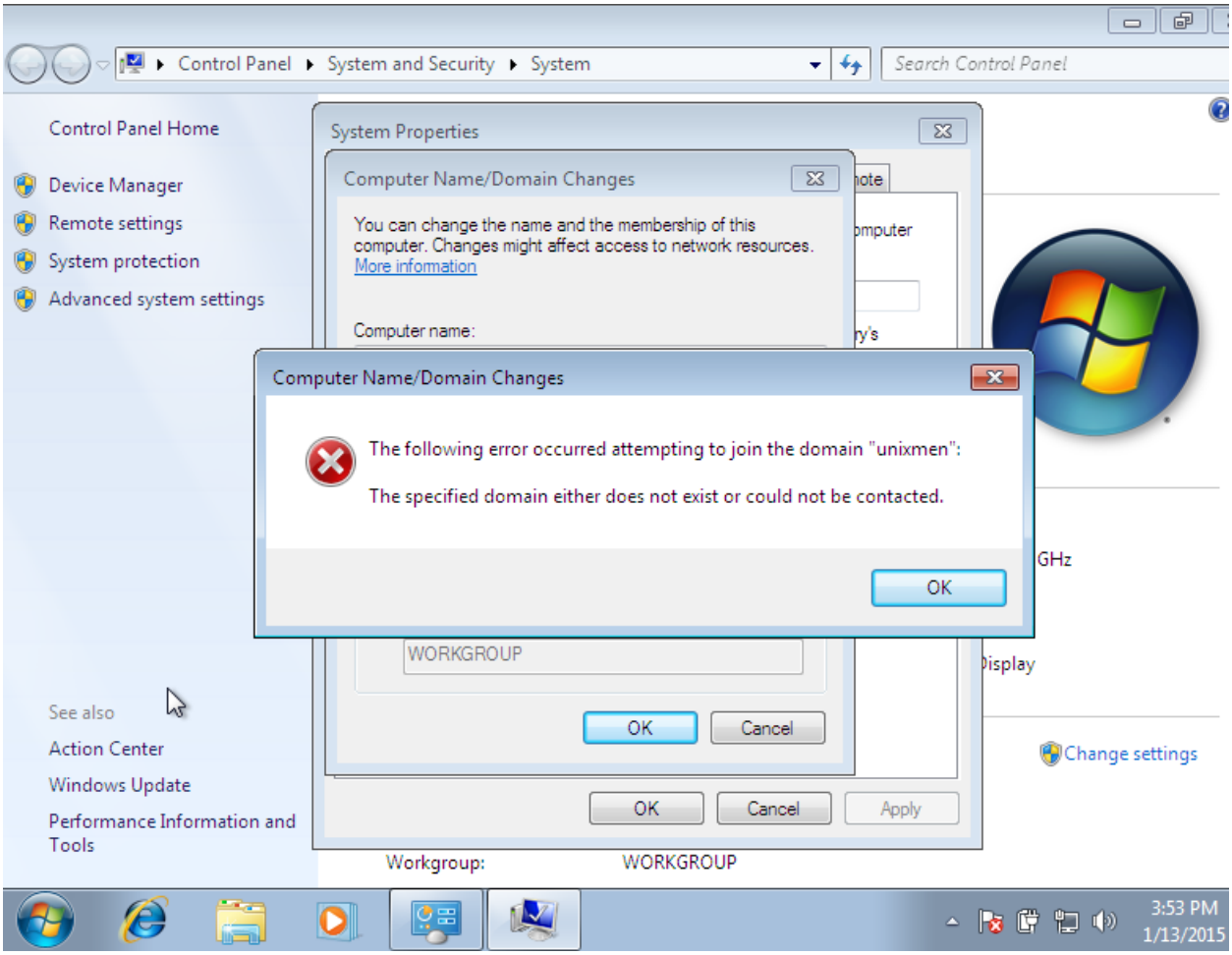


Enter the Samba administrator, which is **root** in our case, and it's password. Not the actual root user password. Enter the root password which we created earlier using **smbpasswd** command.



You may get an error like as shown below.

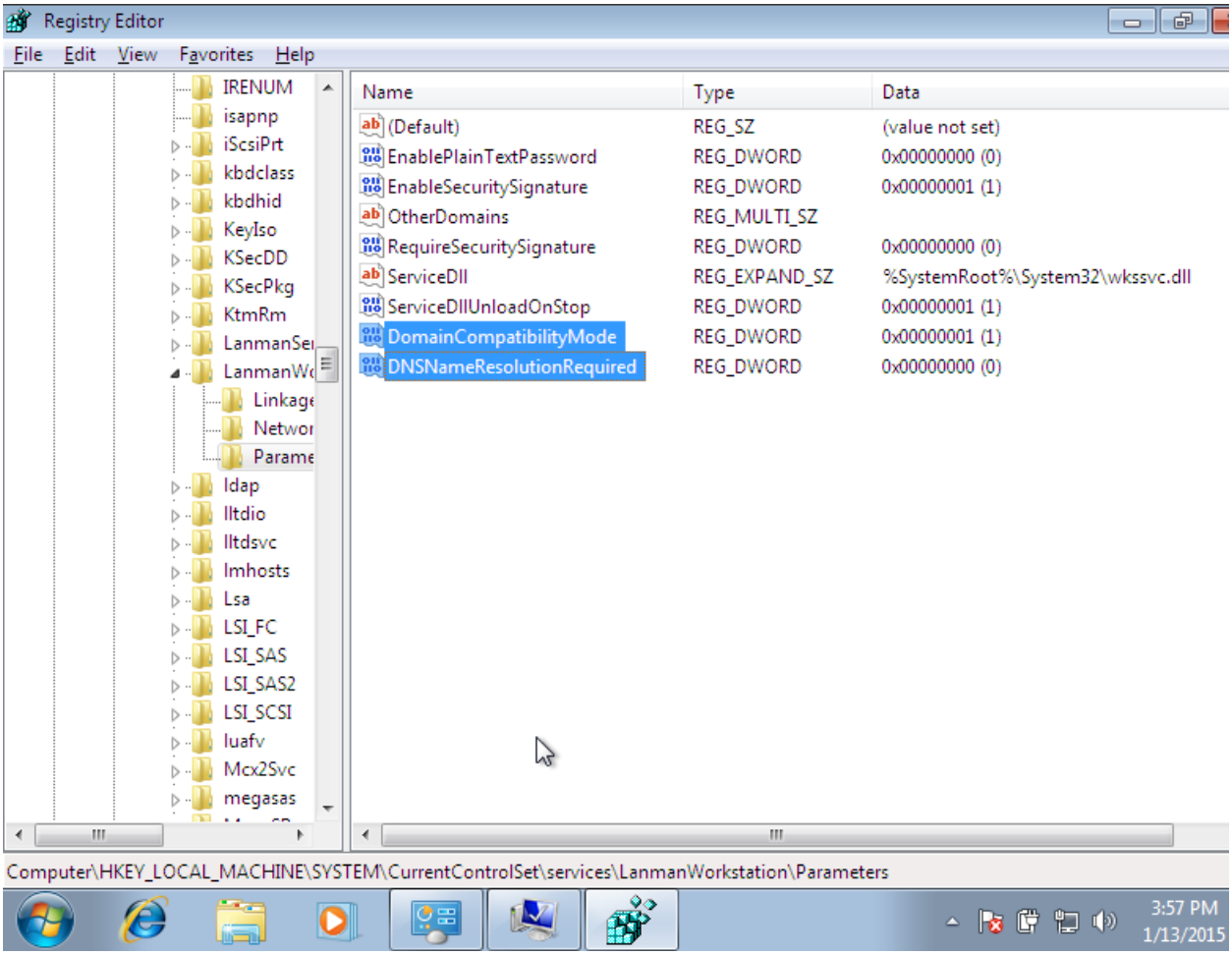
```
"The specified domain either does not exist or could not be contacted"
```



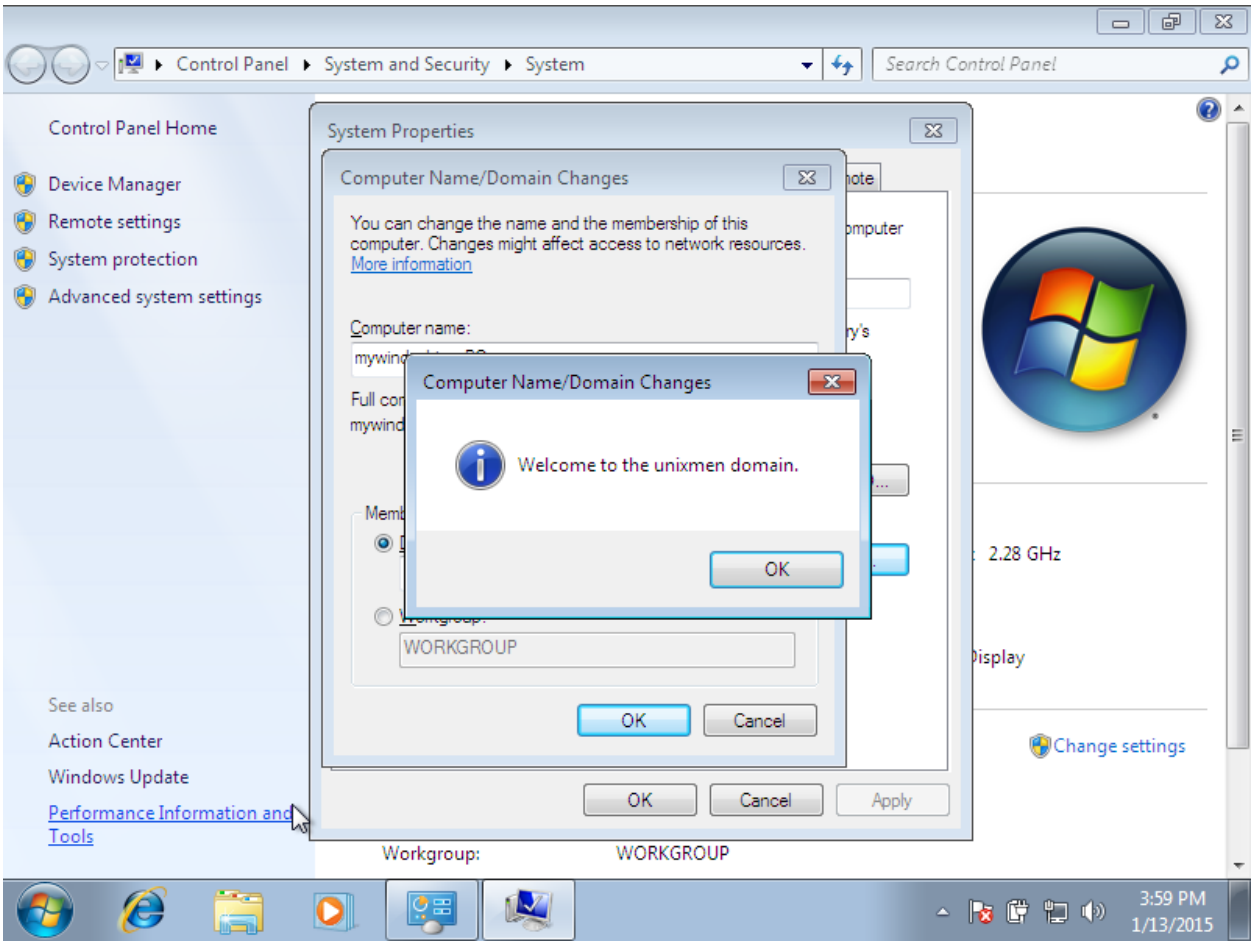
Don’t worry. We can easily fix this error by doing the following tricks.

To get rid of this error, open the windows registry. Go to **HKEY_LOCAL_MACHINE -> SYSTEM -> CurrentControlSet -> Services -> LanmanWorkstation -> Parameters**.

Create new two DWORD values called **“DomainCompatibilityMode”** and **“DNSNameResolutionRequired”**. And set values for **“DomainCompatibilityMode”** as **1(one)** and **“DNSNameResolutionRequired”** as **0(zero)**. Refer the below screenshot.



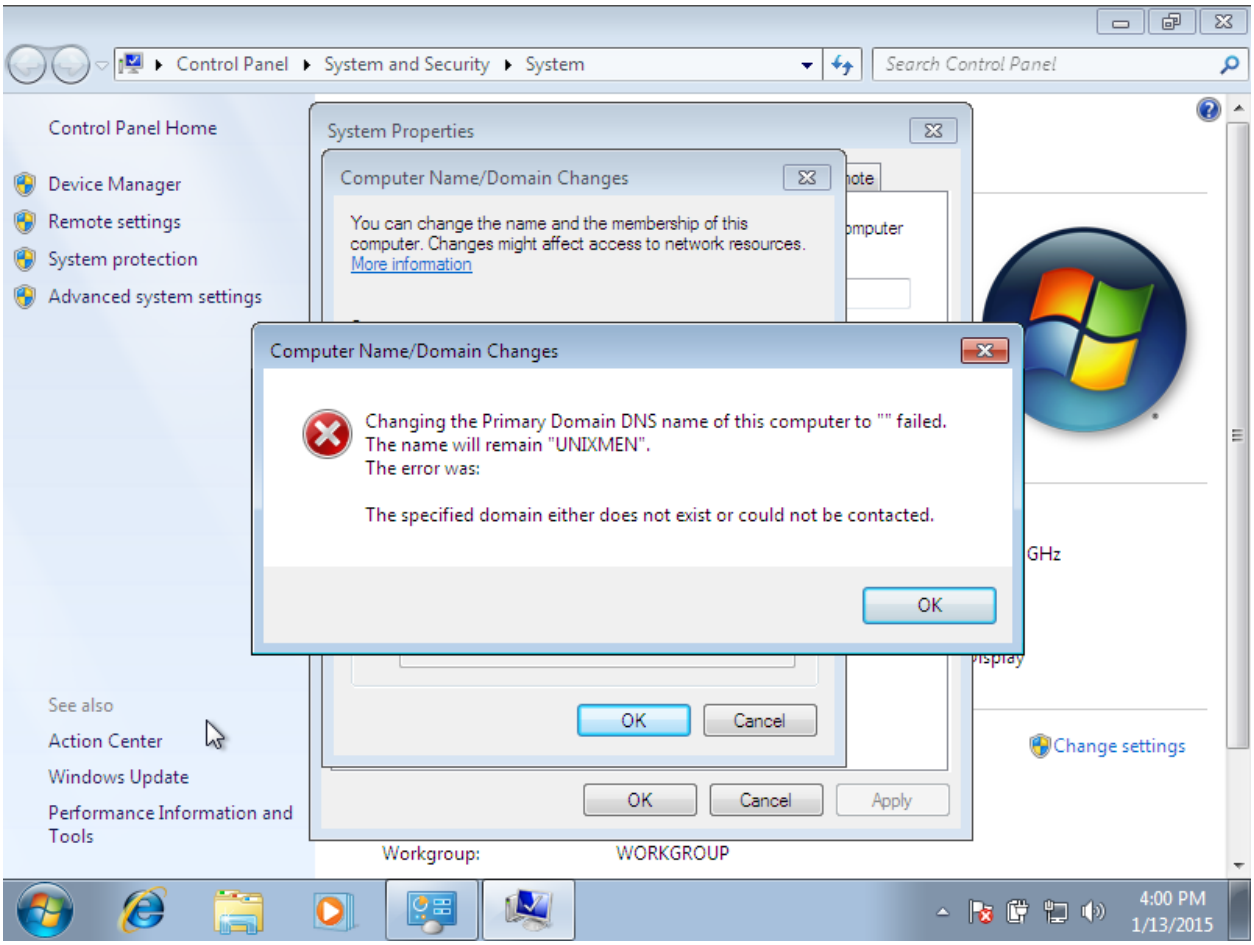
Now, you'll be able to join your windows client to domain.



Click Ok to continue.

Opps! Again error!!

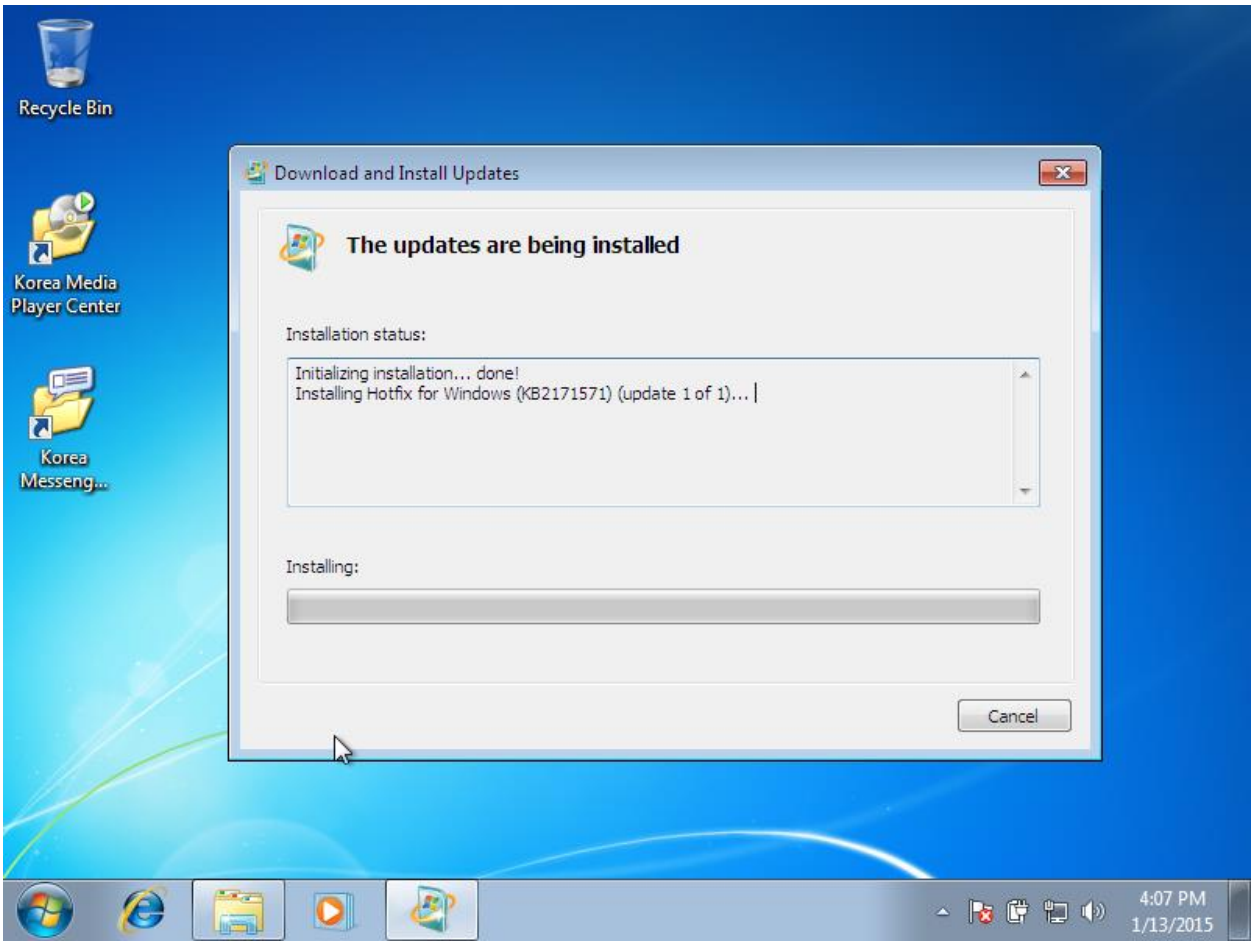
```
Changing the Primary Domain DNS name of this computer to "" failed.
The name will remain "UNIXMEN".

 The error was:



The specified domain either does not exist or could not be
contacted
```



Simply click Ok to ignore this message. Don’t restart now.

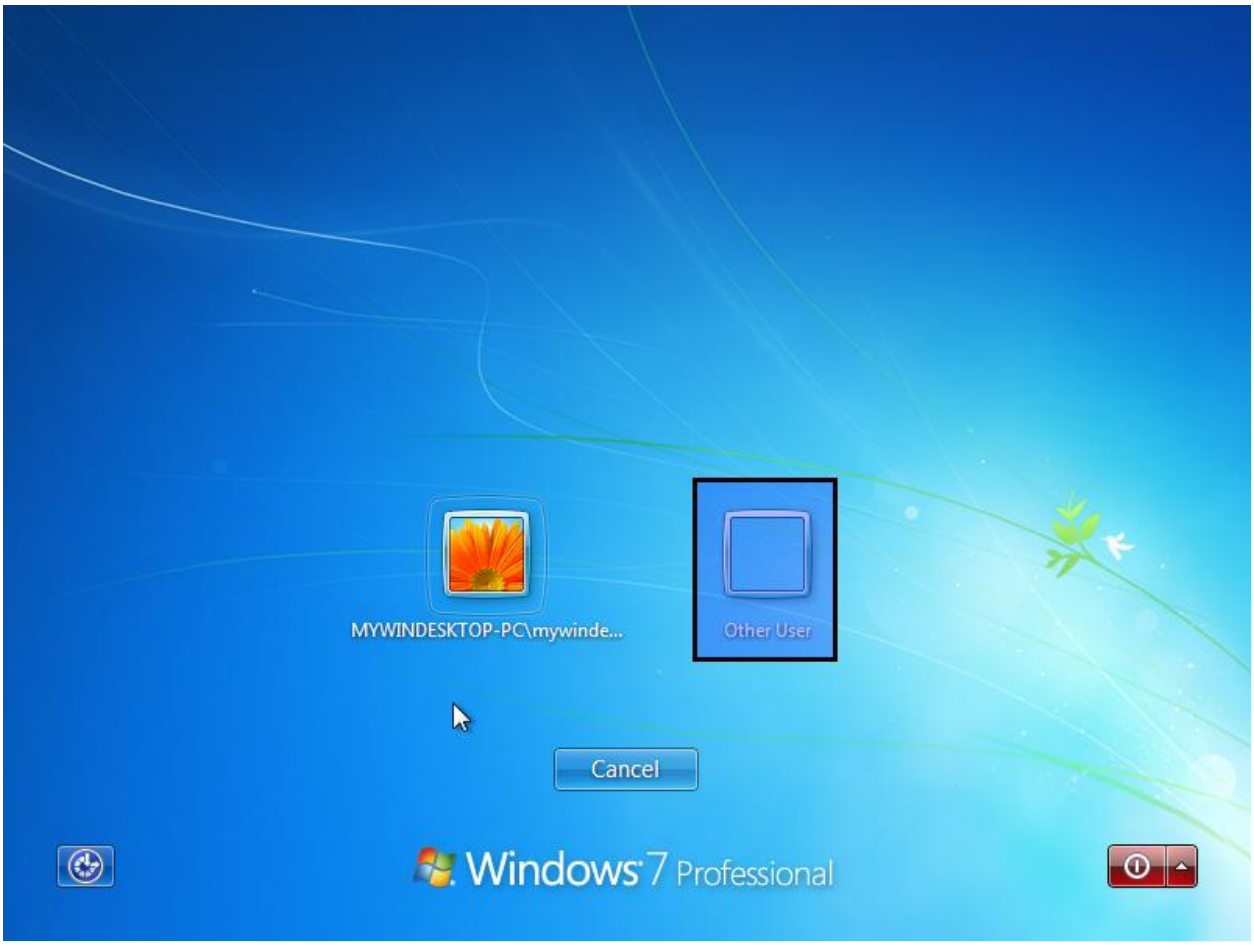
Download and install a **hotfix** from the following link to prevent this error in future.

- Download Hotfix

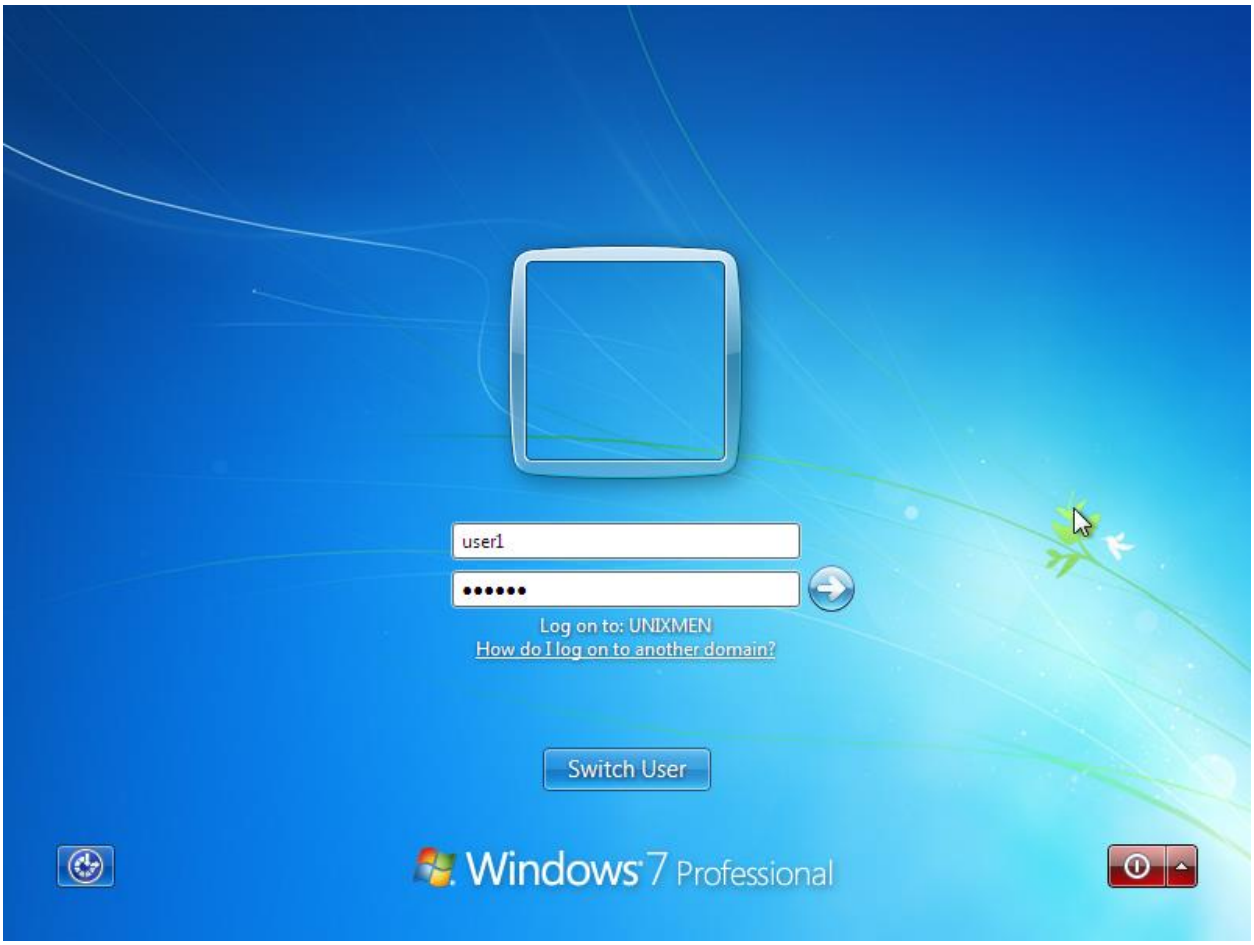


After installing the fix, restart the Windows OS machine and you will able to login to Samba domain now.

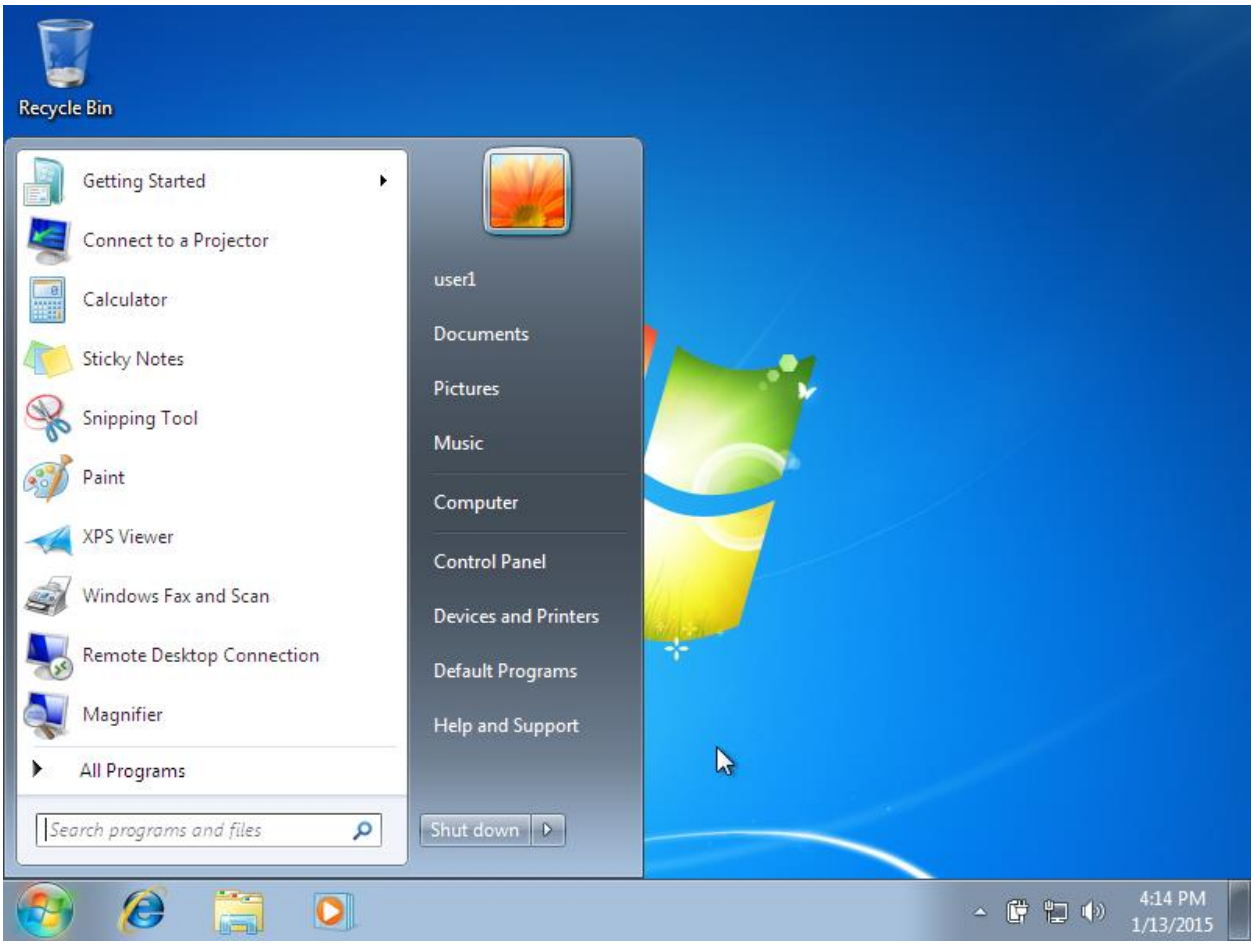
Press CTRL+ALT+Del keys, Click **Switch user**, and select **Other user** option.



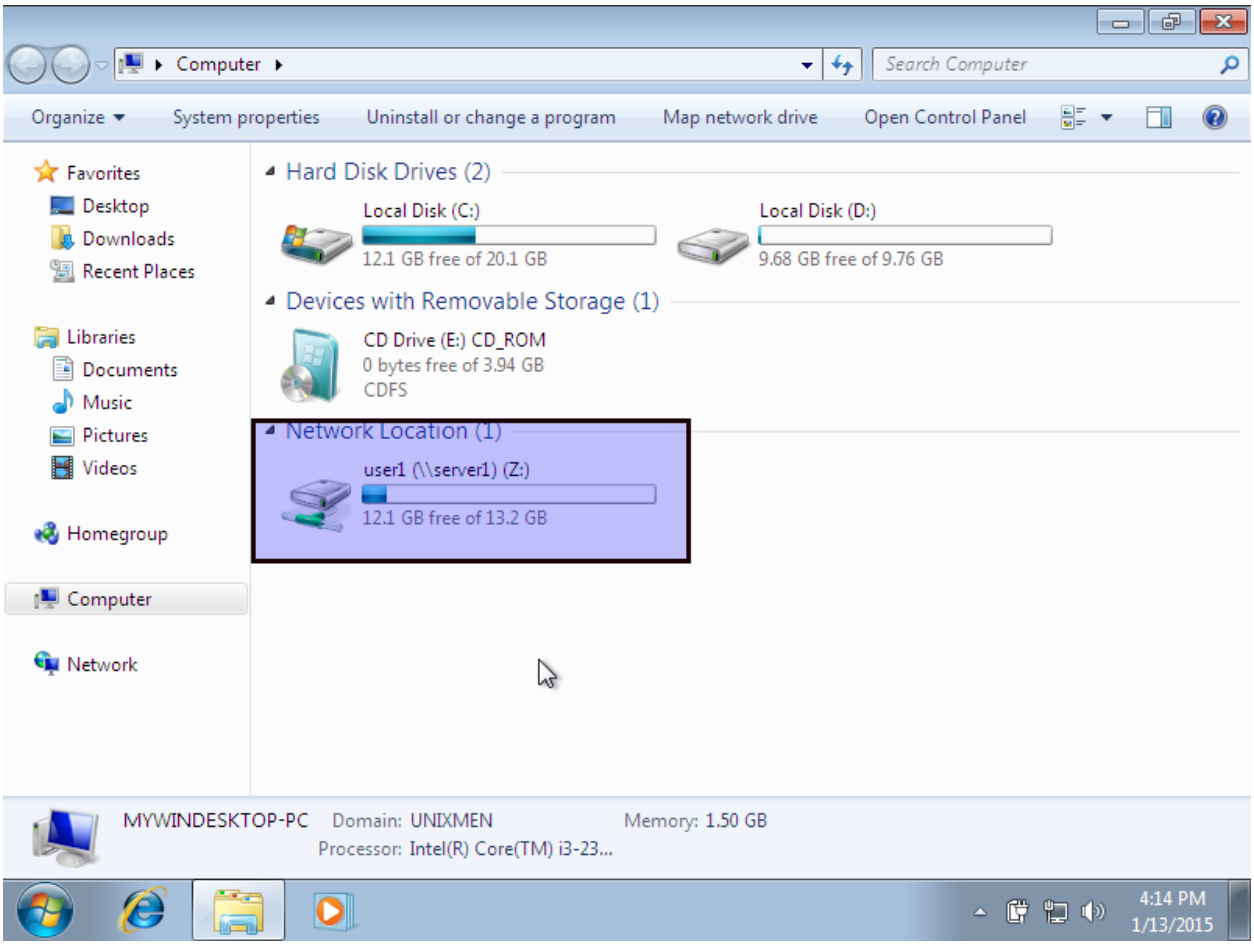
Enter the user name and password. Remember we already have created two users namely **user1** and **user2** in our previous steps.



That’s it. The new user will be able to login to the domain now.



Please note that, a network drive will be automatically created for the each user. The users can store their personal files/folders in that network folder if they want.



You access the samba users roaming profiles in the following location in the Samba server.

```
ls /var/lib/samba/profiles
```

Sample output:

```
user1.V2  user2.V2
```

Viewing individual users profiles:

```
ls /var/lib/samba/profiles/user1.V2/
```

Sample output:

```
AppData    Desktop     Downloads   Links   NTUSER.DAT   Pictures      Sea
rches
```

```
Contacts    Documents    Favorites    Music    ntuser.ini    Saved
Games  Videos
```

At this stage you have a fully operational Samba Domain Controller on CentOS 7. That’s it. Start using your Samba PDC. Good luck!

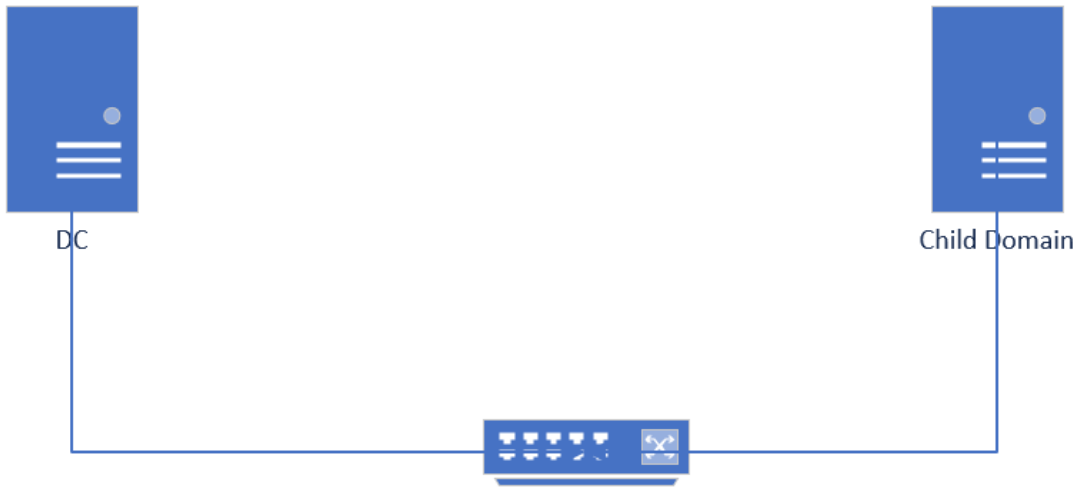
Bài tập

Cho sơ đồ như sau:

Theo sơ đồ trên, cả 2 máy server đều sử dụng windows server 2012. Hãy thực hiện:

- Tự lựa chọn IP và gán cho các máy.
- Hãy tự cấu hình DNS trên máy DC, tên miền tùy chọn.
- Hãy nâng máy DC lên làm máy quản lý miền.
- Hãy gia nhập DC backup vào domain đã nâng cấp.
- Hãy thực hiện nâng cấp DC backup thành 1 DC đồng hành với DC chính.

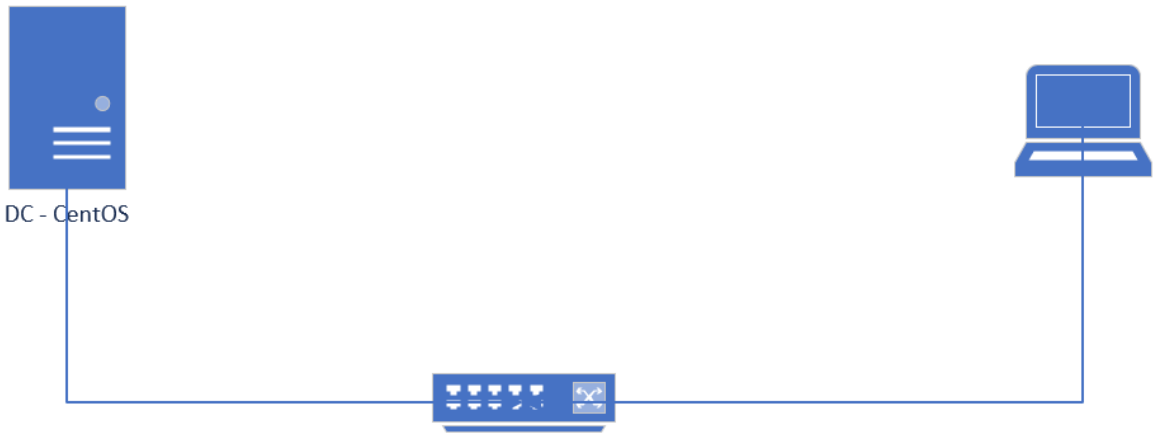
Từ mô hình thứ 2:



Từ domain đã có sẵn, hãy thực hiện tạo thêm 1 child domain, với tên miền tùy chọn.

Bài 2:

Cho mô hình:



Hãy nâng cấp máy CentOS lên thành máy DC. Tên miền tùy chọn, sau đó hãy gia nhập máy trạm vào trong miền.