Active Directory Domain Controller

Using the Samba 4 on Ubuntu 12.04 Server Edition

Step by step Installation and Configuration Guide

Part I

Introduction

What is samba?

Samba is a free software re-implementation of the SMB/CIFS networking protocol, originally developed by Andrew Tridgell. As of version 3, Samba provides file and print services for various Microsoft Windows clients and can integrate with a Windows Server domain, either as a Primary Domain Controller (PDC) or as a domain member. It can also be part of an Active Directory domain.

What is Active Directory Domain Controller?

An AD domain controller authenticates and authorizes all users and computers in a Windows domain type network—assigning and enforcing security policies for all computers and installing or updating software. For example, when a user logs into a computer that is part of a Windows domain, Active Directory checks the submitted password and determines whether the user is a system administrator or normal user.

In the following guide there is a step by step instruction on how to install and configure the Samba 4. It also includes how to join a Windows 7 client and using the AD management tools from the Windows 7 side. I used a lot of snap shot from my setup on a virtual machine and also some notes from the samba wiki: https://wiki.samba.org/index.php/Samba_AD_DC_HOWTO

Part II

Installation

For the successful build of Samba 4 some packages are required.

Therefor the recommended optional development libraries and programs:

- acl -- Required for a successful AD DC deployment. If this library is not included, samba will build successfully, however you will not be able to change ACL's from the windows frontend. You will receive and error when you provision and if you manually create the smb.conf with +s3fs, you will get **Access is denied.** from windows on any attempt to change ACL's.
- xattr
- blkid
- gnutls
- readline
- openldap -- Required to build the Samba3 components with LDAP support. Lacking this library the build will complete but attempts to provision (via upgrade) an Active Directory domain from an existing Samba3 LDAP backend will fail.
- cups -- for printer sharing support
- bsd or setproctitle - for process title updating support

- xsltproc and docbook XSL stylesheets -- Required for building man pages and other documentation

  The following will cover bind, kerberos, and file system tools. If you plan to use the internal DNS server, you do not need bind, but you do still need the package that contains the nsupdate binary.

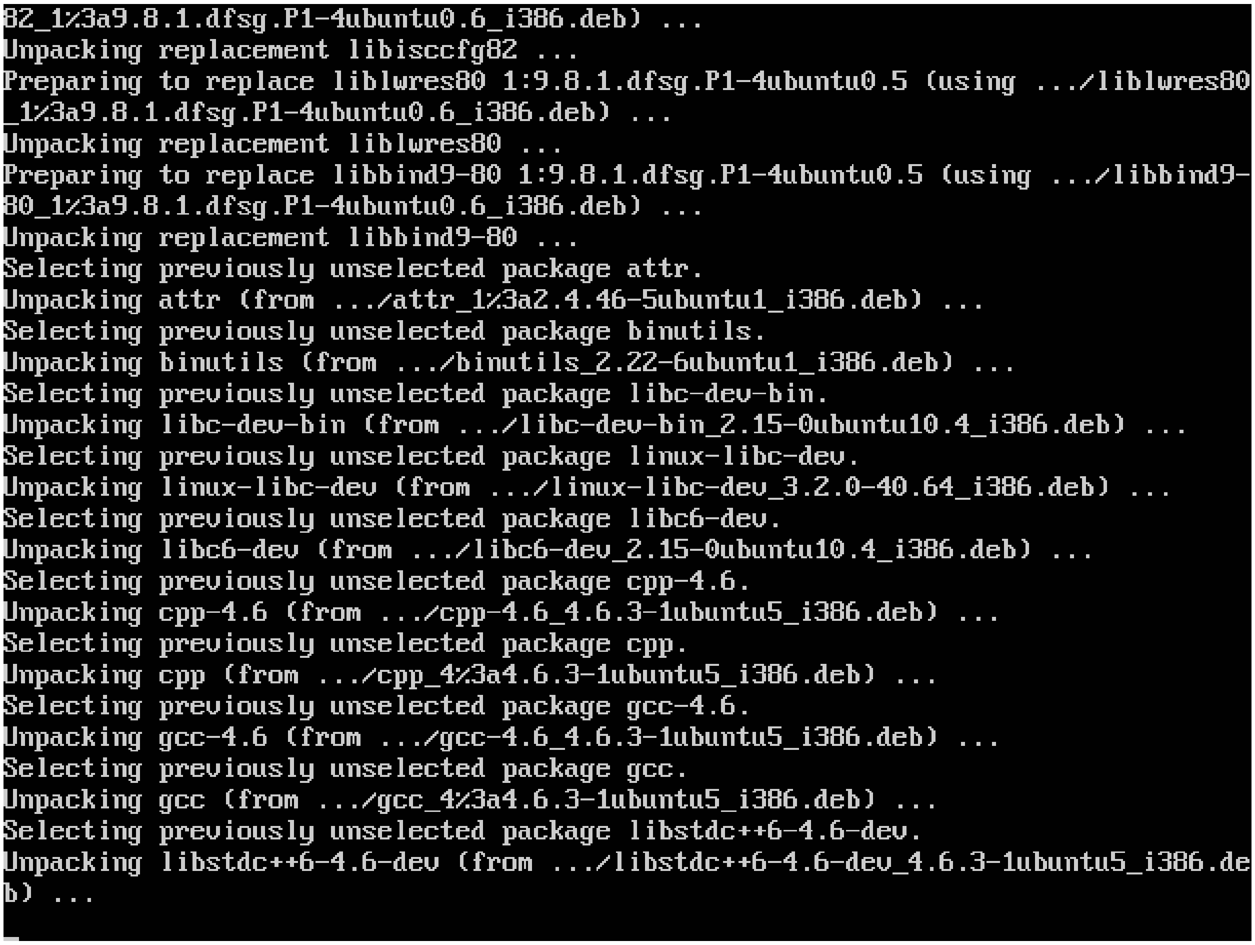
For the Ubuntu Distribution

```
# apt-get install build-essential libacl1-dev libattr1-dev \
   libblkid-dev libgnutls-dev libreadline-dev python-dev \
   python-dnspython gdb pkg-config libpopt-dev libldap2-dev \
   dnsutils libbsd-dev attr krb5-user docbook-xsl libcups2-dev
```

Note: docbook-xsl, xsltproc, and inkscape may be required for building the man pages.

While installing the kerberose, you will be prompted to enter a domain name and you enter the domain name that you will use with the samba server. For me it was samdom.trial.com

These is how it looks when it is successfully installing the above packages:



```
82_1%3a9.8.1.dfsg.P1-4ubuntu0.6_i386.deb) ...
Unpacking replacement libisccfg82 ...
Preparing to replace liblwres80 1:9.8.1.dfsg.P1-4ubuntu0.5 (using .../liblwres80
_1%3a9.8.1.dfsg.P1-4ubuntu0.6_i386.deb) ...
Unpacking replacement liblwres80 ...
Preparing to replace libbind9-80 1:9.8.1.dfsg.P1-4ubuntu0.5 (using .../libbind9-
80_1%3a9.8.1.dfsg.P1-4ubuntu0.6_i386.deb) ...
Unpacking replacement libbind9-80 ...
Selecting previously unselected package attr.
Unpacking attr (from .../attr_1%3a2.4.46-5ubuntu1_i386.deb) ...
Selecting previously unselected package binutils.
Unpacking binutils (from .../binutils_2.22-6ubuntu1_i386.deb) ...
Selecting previously unselected package libc-dev-bin.
Unpacking libc-dev-bin (from .../libc-dev-bin_2.15-0ubuntu10.4_i386.deb) ...
Selecting previously unselected package linux-libc-dev.
Unpacking linux-libc-dev (from .../linux-libc-dev_3.2.0-40.64_i386.deb) ...
Selecting previously unselected package libc6-dev.
Unpacking libc6-dev (from .../libc6-dev_2.15-0ubuntu10.4_i386.deb) ...
Selecting previously unselected package cpp-4.6.
Unpacking cpp-4.6 (from .../cpp-4.6_4.6.3-1ubuntu5_i386.deb) ...
Selecting previously unselected package cpp.
Unpacking cpp (from .../cpp_4%3a4.6.3-1ubuntu5_i386.deb) ...
Selecting previously unselected package gcc-4.6.
Unpacking gcc-4.6 (from .../gcc-4.6_4.6.3-1ubuntu5_i386.deb) ...
Selecting previously unselected package gcc.
Unpacking gcc (from .../gcc_4%3a4.6.3-1ubuntu5_i386.deb) ...
Selecting previously unselected package libstdc++6-4.6-dev.
Unpacking libstdc++6-4.6-dev (from .../libstdc++6-4.6-dev_4.6.3-1ubuntu5_i386.de
b) ...
_
```

In the following steps i will be using the following configurations:

```
Installation Directory: /usr/local/samba
Server Hostname: ubuntuserver (Your linux hostname will be used here)
DNS Domain Name: samdom.trial.com (This will also be your realm)
NT4 Domain Name: samdom
IP Address: 192.168.20.15
Server Role: DC
```

Now we will start the installation process.

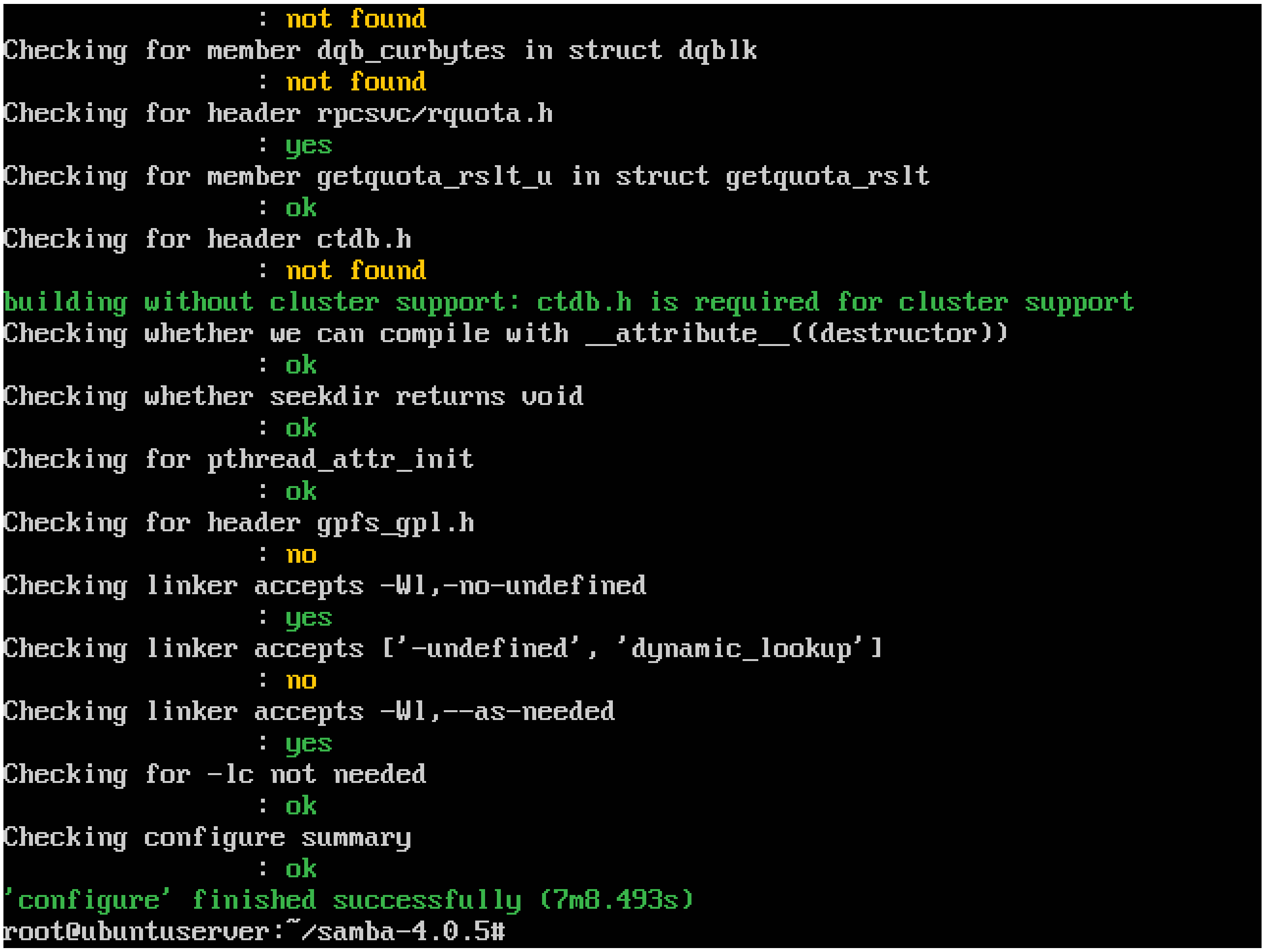
Step 1: Downloading Samba

The first thing to do is download the samba4 binary software, check the last version in the official samba ftp webpage, and download it. To download the samba 4.0.5 stable release and then extract it, use:

```
# wget http://www.samba.org/samba/ftp/stable/samba-4.0.5.tar.gz
# tar xvfz samba-4.0.5.tar.gz
```

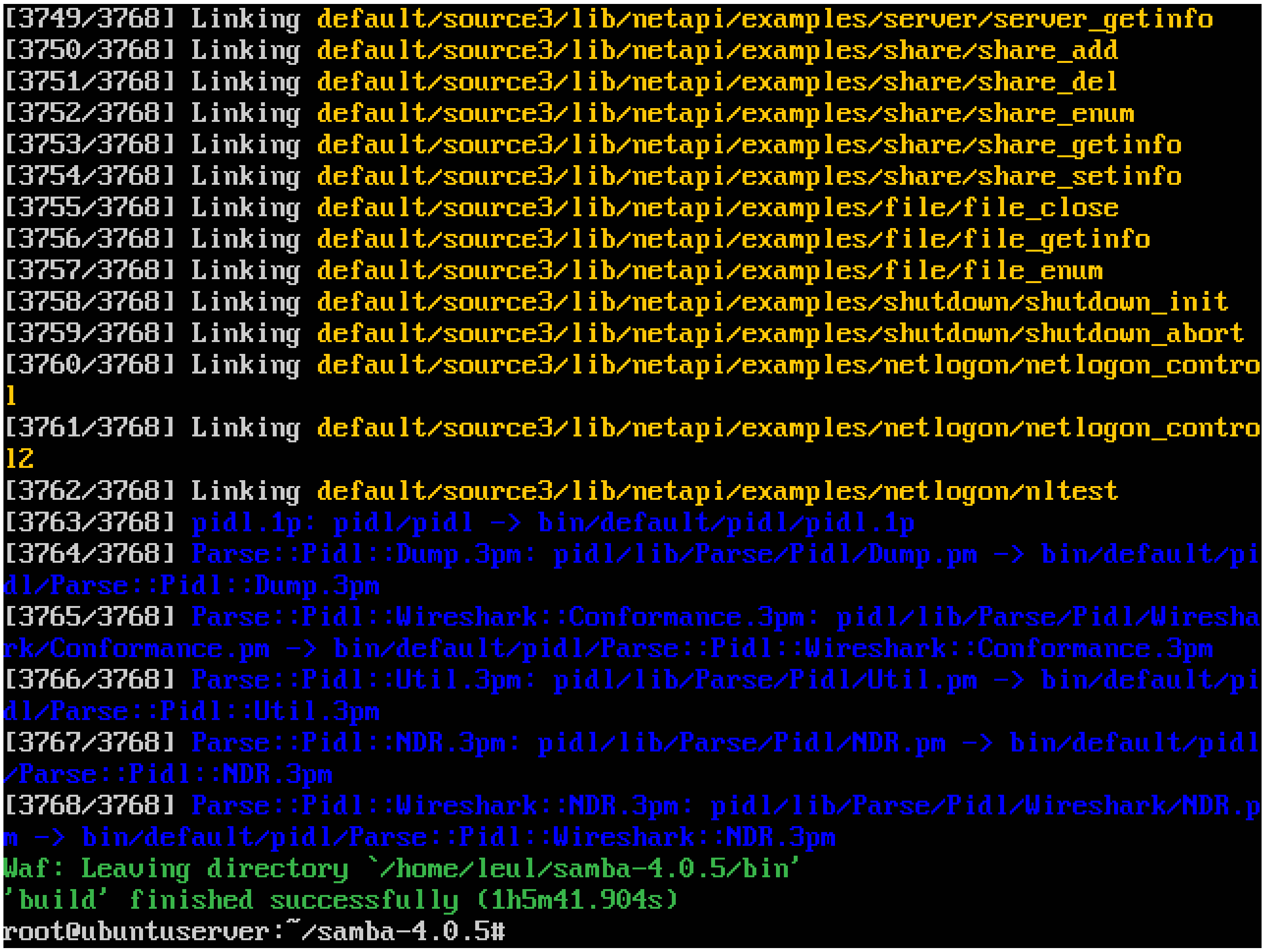
Step 2: Compile Samba

```
# cd samba-4.0.5/
# ./configure
```



```
                : not found
Checking for member dqb_curbytes in struct dqblk
                : not found
Checking for header rpcsvc/rquota.h
                : yes
Checking for member getquota_rslt_u in struct getquota_rslt
                : ok
Checking for header ctdb.h
                : not found
building without cluster support: ctdb.h is required for cluster support
Checking whether we can compile with __attribute__((destructor))
                : ok
Checking whether seekdir returns void
                : ok
Checking for pthread_attr_init
                : ok
Checking for header gpfs_gpl.h
                : no
Checking linker accepts -Wl,-no-undefined
                : yes
Checking linker accepts ['-undefined', 'dynamic_lookup']
                : no
Checking linker accepts -Wl,--as-needed
                : yes
Checking for -lc not needed
                : ok
Checking configure summary
                : ok
'configure' finished successfully (7m8.493s)
root@ubuntuserver:~/samba-4.0.5#
```

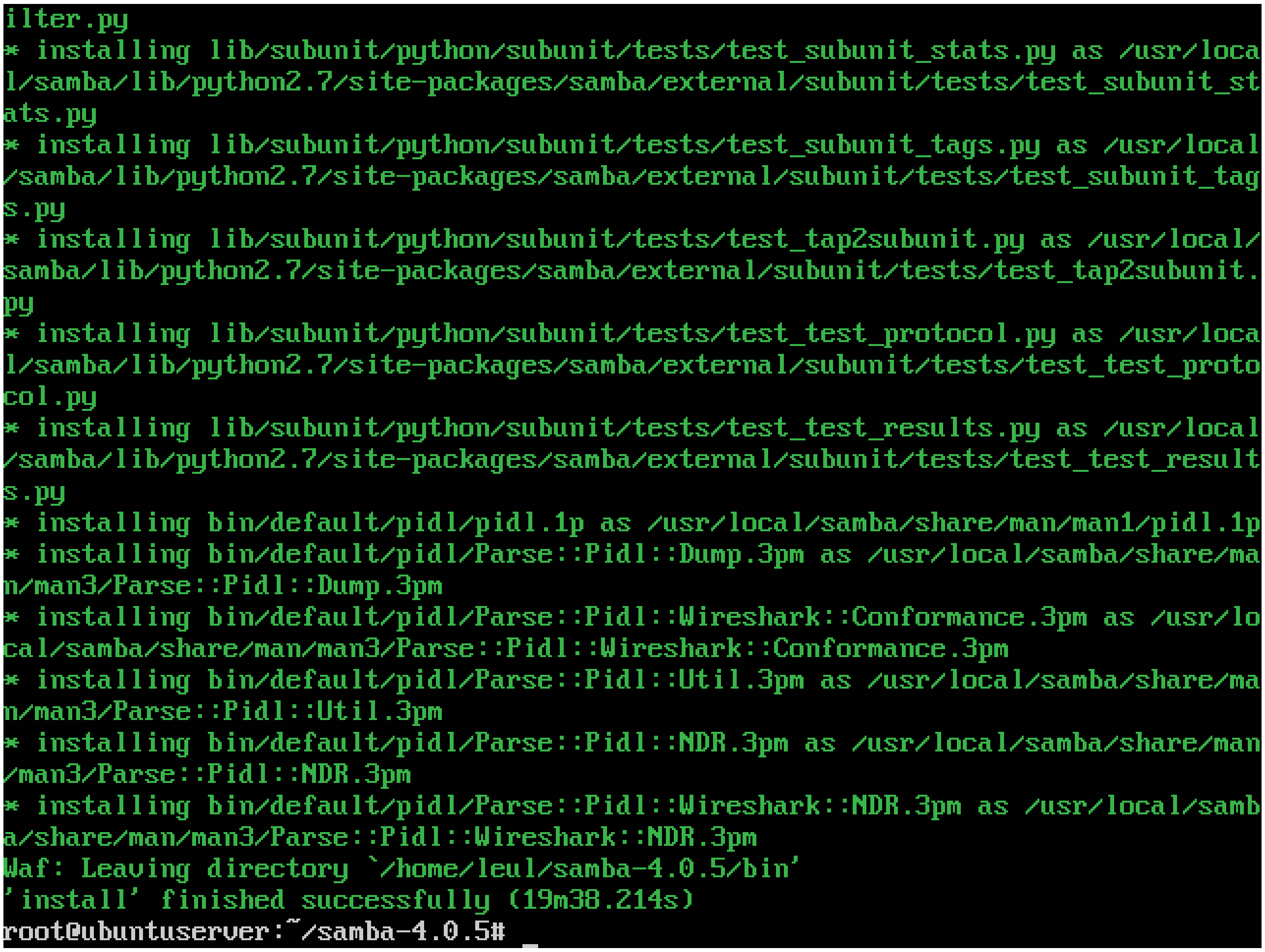
# make



```
[3749/3768] Linking default/source3/lib/netapi/examples/server/server_getinfo
[3750/3768] Linking default/source3/lib/netapi/examples/share/share_add
[3751/3768] Linking default/source3/lib/netapi/examples/share/share_del
[3752/3768] Linking default/source3/lib/netapi/examples/share/share_enum
[3753/3768] Linking default/source3/lib/netapi/examples/share/share_getinfo
[3754/3768] Linking default/source3/lib/netapi/examples/share/share_setinfo
[3755/3768] Linking default/source3/lib/netapi/examples/file/file_close
[3756/3768] Linking default/source3/lib/netapi/examples/file/file_getinfo
[3757/3768] Linking default/source3/lib/netapi/examples/file/file_enum
[3758/3768] Linking default/source3/lib/netapi/examples/shutdown/shutdown_init
[3759/3768] Linking default/source3/lib/netapi/examples/shutdown/shutdown_abort
[3760/3768] Linking default/source3/lib/netapi/examples/netlogon/netlogon_contro
l
[3761/3768] Linking default/source3/lib/netapi/examples/netlogon/netlogon_contro
l2
[3762/3768] Linking default/source3/lib/netapi/examples/netlogon/nltest
[3763/3768] pidl.1p: pidl/pidl -> bin/default/pidl/pidl.1p
[3764/3768] Parse::Pidl::Dump.3pm: pidl/lib/Parse/Pidl/Dump.pm -> bin/default/pi
dl/Parse::Pidl::Dump.3pm
[3765/3768] Parse::Pidl::Wireshark::Conformance.3pm: pidl/lib/Parse/Pidl/Wiresha
rk/Conformance.pm -> bin/default/pidl/Parse::Pidl::Wireshark::Conformance.3pm
[3766/3768] Parse::Pidl::Util.3pm: pidl/lib/Parse/Pidl/Util.pm -> bin/default/pi
dl/Parse::Pidl::Util.3pm
[3767/3768] Parse::Pidl::NDR.3pm: pidl/lib/Parse/Pidl/NDR.pm -> bin/default/pidl
/Parse::Pidl::NDR.3pm
[3768/3768] Parse::Pidl::Wireshark::NDR.3pm: pidl/lib/Parse/Pidl/Wireshark/NDR.p
m -> bin/default/pidl/Parse::Pidl::Wireshark::NDR.3pm
Waf: Leaving directory `/home/leul/samba-4.0.5/bin'
'build' finished successfully (1h5m41.904s)
root@ubuntuserver:~/samba-4.0.5#
```

Step 3: Installing Samba

# make install



```
ilter.py
* installing lib/subunit/python/subunit/tests/test_subunit_stats.py as /usr/loca
l/samba/lib/python2.7/site-packages/samba/external/subunit/tests/test_subunit_st
ats.py
* installing lib/subunit/python/subunit/tests/test_subunit_tags.py as /usr/local
/samba/lib/python2.7/site-packages/samba/external/subunit/tests/test_subunit_tag
s.py
* installing lib/subunit/python/subunit/tests/test_tap2subunit.py as /usr/local/
samba/lib/python2.7/site-packages/samba/external/subunit/tests/test_tap2subunit.
py
* installing lib/subunit/python/subunit/tests/test_test_protocol.py as /usr/loca
l/samba/lib/python2.7/site-packages/samba/external/subunit/tests/test_test_proto
col.py
* installing lib/subunit/python/subunit/tests/test_test_results.py as /usr/local
/samba/lib/python2.7/site-packages/samba/external/subunit/tests/test_test_result
s.py
* installing bin/default/pidl/pidl.1p as /usr/local/samba/share/man/man1/pidl.1p
* installing bin/default/pidl/Parse::Pidl::Dump.3pm as /usr/local/samba/share/ma
n/man3/Parse::Pidl::Dump.3pm
* installing bin/default/pidl/Parse::Pidl::Wireshark::Conformance.3pm as /usr/lo
cal/samba/share/man/man3/Parse::Pidl::Wireshark::Conformance.3pm
* installing bin/default/pidl/Parse::Pidl::Util.3pm as /usr/local/samba/share/ma
n/man3/Parse::Pidl::Util.3pm
* installing bin/default/pidl/Parse::Pidl::NDR.3pm as /usr/local/samba/share/man
/man3/Parse::Pidl::NDR.3pm
* installing bin/default/pidl/Parse::Pidl::Wireshark::NDR.3pm as /usr/local/samb
a/share/man/man3/Parse::Pidl::Wireshark::NDR.3pm
Waf: Leaving directory `/home/leul/samba-4.0.5/bin'
'install' finished successfully (19m38.214s)
root@ubuntuserver:~/samba-4.0.5# _
```

Part III

Configuring Samba

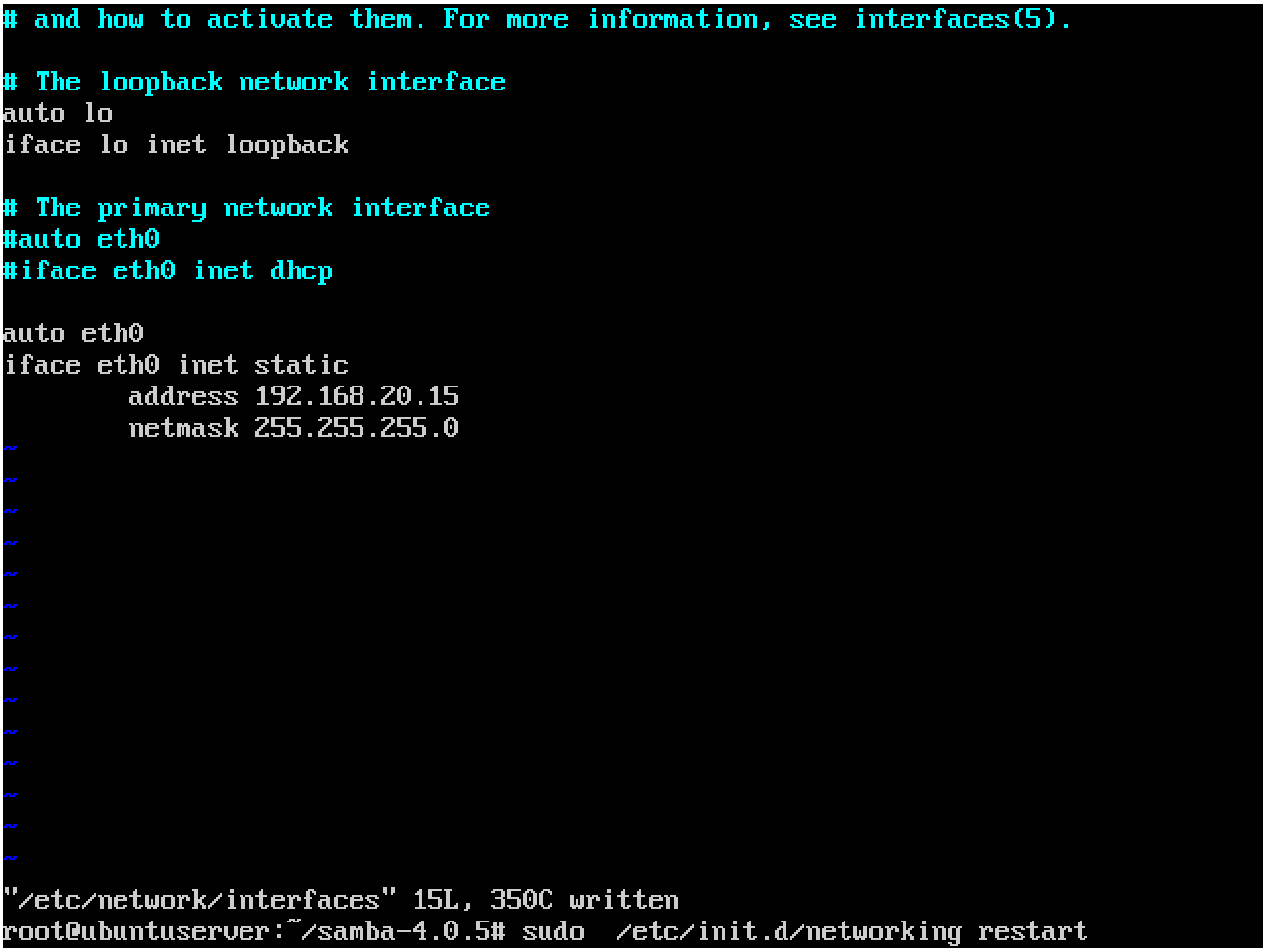
Step 1: Provision Samba

The provision step sets up a basic user database, and is used when you are setting up your Samba server in its own domain.

Before you start the provision, you should change the network setting to static.

You can simply edit the interfaces file

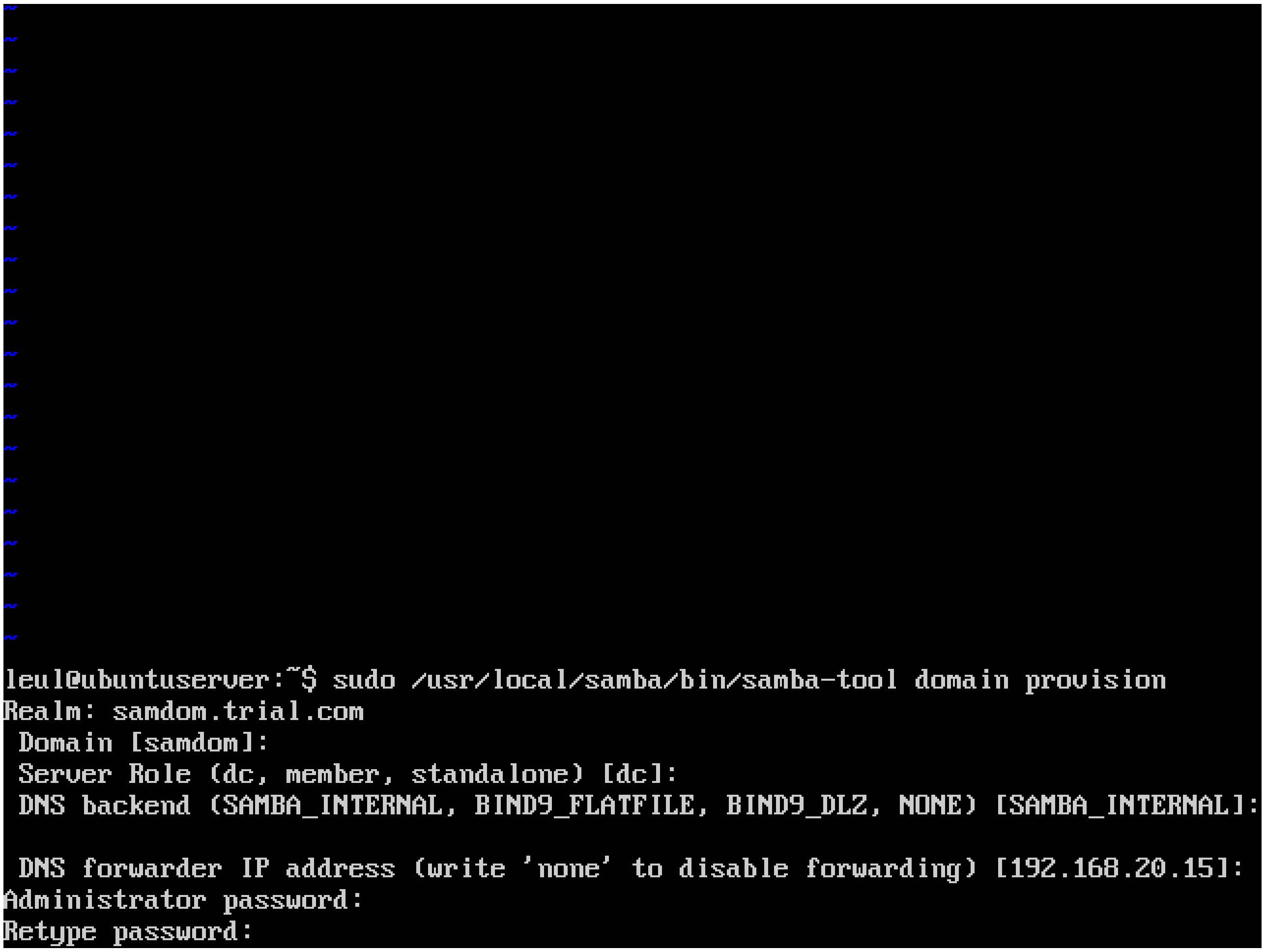
```
# vim /etc/networking/interfaces
```



```
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
#auto eth0
#iface eth0 inet dhcp

auto eth0
iface eth0 inet static
        address 192.168.20.15
        netmask 255.255.255.0
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"/etc/network/interfaces" 15L, 350C written
root@ubuntuserver:~/samba-4.0.5# sudo  /etc/init.d/networking restart
```

Then start the provision

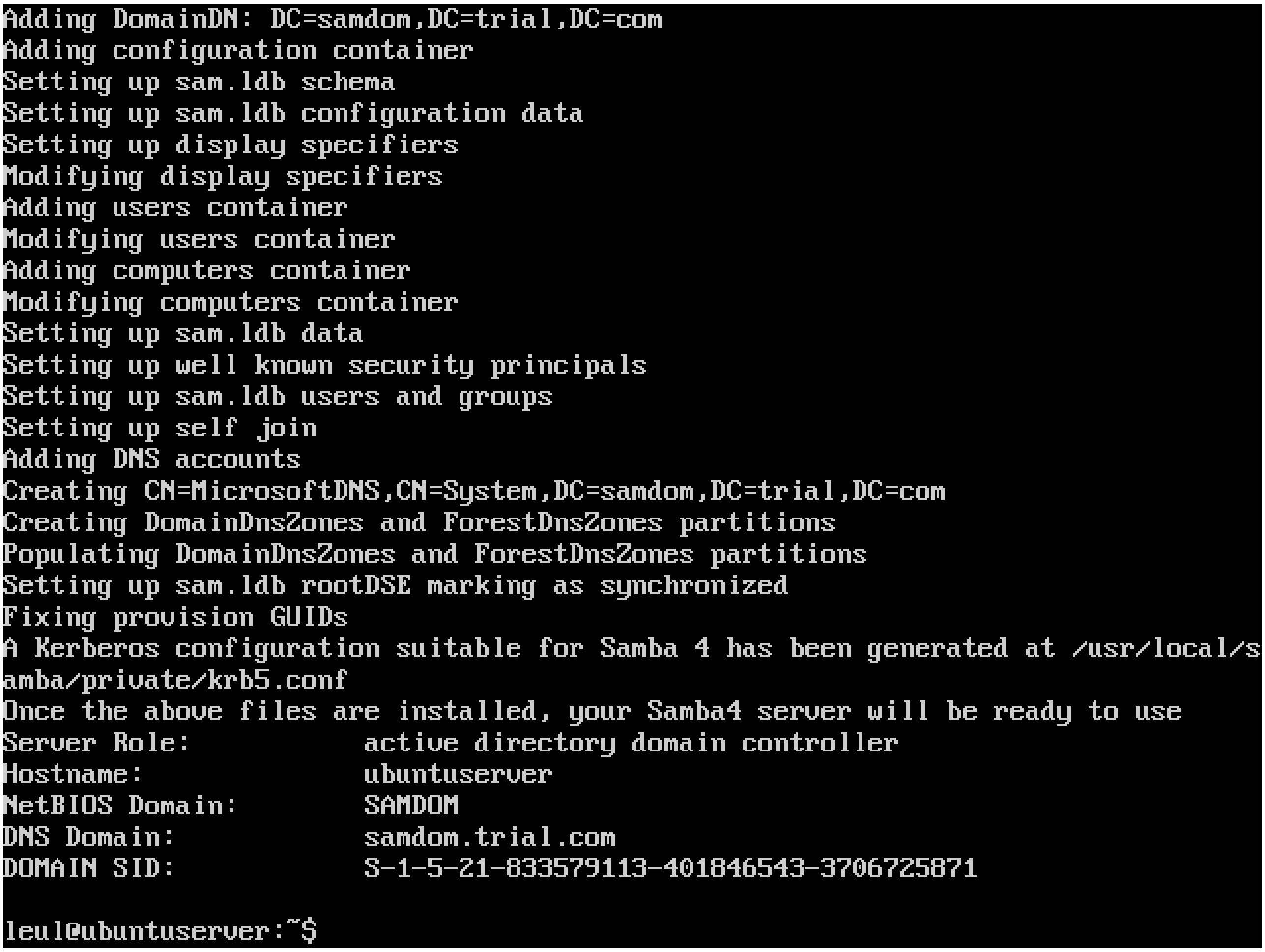
```
# /usr/local/samba/bin/samba-tool domain provision
```



```
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
leul@ubuntuserver:~$ sudo /usr/local/samba/bin/samba-tool domain provision
Realm: samdom.trial.com
 Domain [samdom]:
 Server Role (dc, member, standalone) [dc]:
 DNS backend (SAMBA_INTERNAL, BIND9_FLATFILE, BIND9_DLZ, NONE) [SAMBA_INTERNAL]:

 DNS forwarder IP address (write 'none' to disable forwarding) [192.168.20.15]:
Administrator password:
Retype password:
```

Here the options in the box brackets '[ ]' are chooses by default so you can just press enter if you want them.

If the provision is successful you will get a screen like this.



```
Adding DomainDN: DC=samdom,DC=trial,DC=com
Adding configuration container
Setting up sam.ldb schema
Setting up sam.ldb configuration data
Setting up display specifiers
Modifying display specifiers
Adding users container
Modifying users container
Adding computers container
Modifying computers container
Setting up sam.ldb data
Setting up well known security principals
Setting up sam.ldb users and groups
Setting up self join
Adding DNS accounts
Creating CN=MicrosoftDNS,CN=System,DC=samdom,DC=trial,DC=com
Creating DomainDnsZones and ForestDnsZones partitions
Populating DomainDnsZones and ForestDnsZones partitions
Setting up sam.ldb rootDSE marking as synchronized
Fixing provision GUIDs
A Kerberos configuration suitable for Samba 4 has been generated at /usr/local/s
amba/private/krb5.conf
Once the above files are installed, your Samba4 server will be ready to use
Server Role:           active directory domain controller
Hostname:              ubuntuserver
NetBIOS Domain:        SAMDOM
DNS Domain:            samdom.trial.com
DOMAIN SID:            S-1-5-21-833579113-401846543-3706725871

leul@ubuntuserver:~$
```

If you made an error with provision you need to first remove the smb.conf file and start over with the provision:

```
# rm /usr/local/samba/etc/smb.conf
```

Step 2: Starting you Samba AD DC

```
# /usr/local/samba/sbin/samba
```

That will run Samba in 'standard' mode, which is suitable for production use. Samba doesn't yet have init scripts included for each platform, but making one for your platform should not be difficult. There are some example scripts (for RedHat/Fedora, Debian and Ubuntu) on the Samba4/InitScript page.

If you are running Samba as a developer you may find the following more useful:

```
# /usr/local/samba/sbin/samba -i -M single
```

This will start `samba` with all log messages printed to stdout, and restricting it to a single process. That mode of operation makes debugging `samba` with `gdb` easier.

If you want to launch it under `gdb`, run `samba` as follows:

```
# gdb --args /usr/local/samba/sbin/samba -i -M single
```

You can see what version of Samba, if any, is in your `PATH` variable by running the following:

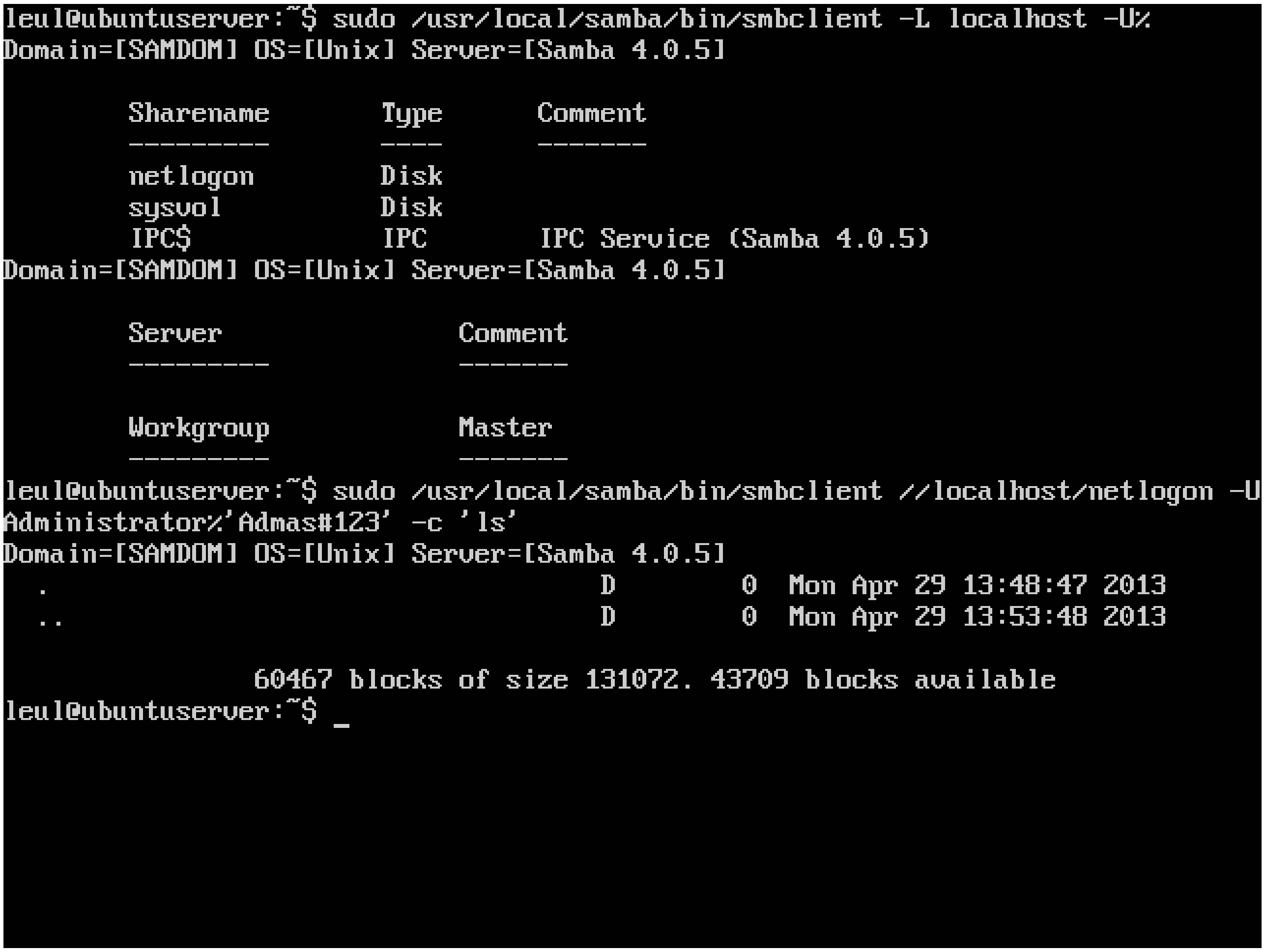
```
# samba -V
```

Step 3: Testing connectivity to your Samba AD DC

You can do this by the following commands:

```
$ /usr/local/samba/bin/smbclient --version
$ /usr/local/samba/bin/smbclient -L localhost -U%
$ smbclient //localhost/netlogon -UAdministrator%'p4$$word' -c 'ls'
```

You should get an output similar to this:



```
leul@ubuntuserver:~$ sudo /usr/local/samba/bin/smbclient -L localhost -U%
Domain=[SAMDOM] OS=[Unix] Server=[Samba 4.0.5]

        Sharename       Type      Comment
        ---------       ----      -------
        netlogon        Disk
        sysvol          Disk
        IPC$            IPC       IPC Service (Samba 4.0.5)
Domain=[SAMDOM] OS=[Unix] Server=[Samba 4.0.5]

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

        Workgroup            Master
        ---------            -------
leul@ubuntuserver:~$ sudo /usr/local/samba/bin/smbclient //localhost/netlogon -U
Administrator%'Admas#123' -c 'ls'
Domain=[SAMDOM] OS=[Unix] Server=[Samba 4.0.5]
  .                                   D        0  Mon Apr 29 13:48:47 2013
  ..                                  D        0  Mon Apr 29 13:53:48 2013

                60467 blocks of size 131072. 43709 blocks available
leul@ubuntuserver:~$ _
```

Step 4: Configure DNS

A working DNS setup is essential to the correct operation of Samba. Without the right DNS entries, Kerberos won't work, which in turn means that many of the basic features of Samba won't work.

It is worth spending some extra time to ensure your DNS setup is correct, as debugging problems caused by mis-configured DNS can take a lot of time later on.

Samba's Internal DNS Server

If you specified `--dns-backend=SAMBA_INTERNAL` or did not specify any backend at all when you provisioned, there is no further setup required for the DNS server, however you used any other --dns-backend= option in your provision line see using bind as your dns backend for additional setup instructions. After you have dns configured, you still need to configure your `/etc/resolv.conf` as shown in Configure /etc/resolv.conf

If you want the internal DNS server to forward requests it isn't responsible for, then add the following to your smb.conf:

```
dns forwarder = {IP-Address of the DNS you want to forward to}
```

Warning: If you are running X windows on your machine, networkmanager could be spawning dnsmasq or if you are using another DNS server, check the logs for lines like:

```
Failed to bind to 0.0.0.0:53 TCP - NT_STATUS_ADDRESS_ALREADY_ASSOCIATED
```

If you need to disable this you can open `/etc/NetworkManager/NetworkManager.conf` in your favorite editor as root, and comment out the line `dns=dnsmasq`, then `restart network-manager`

Configure /etc/resolv.conf

For all the local DNS lookups to resolve correctly, we need to modify the server's `/etc/resolv.conf` file. The following example should be sufficient to have DNS resolve properly:

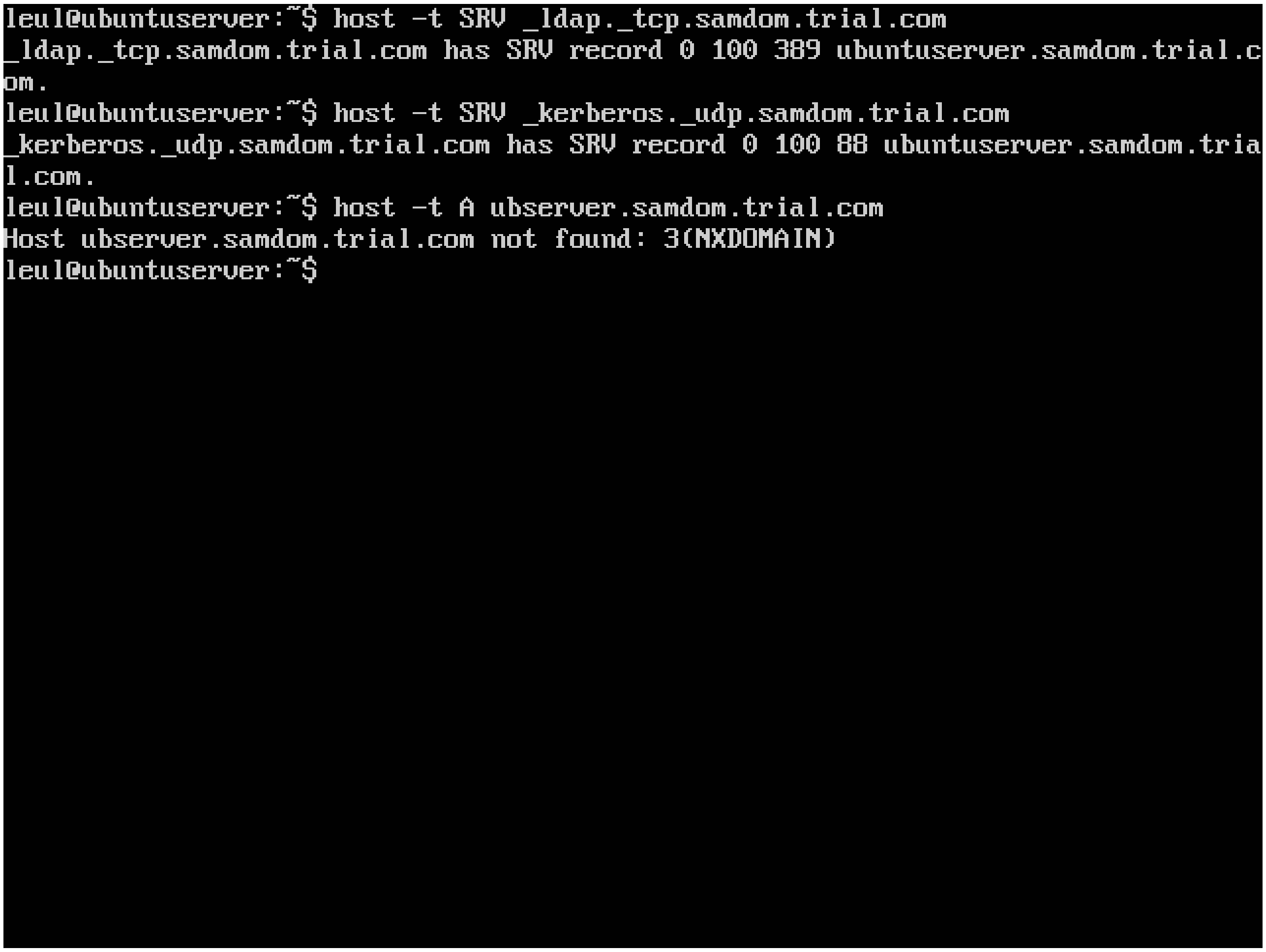
```
domain samdom.trial.com
nameserver 192.168.20.11
```

Note: Remember to change the IP Address to your Samba server's IP Address

- Note: If your server is set up to receive its IP configuration via DHCP, the `/etc/resolv.conf` file might be automatically updated. Refer to your distribution's documentation on how to stop this behavior.

Testing DNS

To test that DNS is working properly, run the following commands and compare the output to what is shown:



```
leul@ubuntuserver:~$ host -t SRV _ldap._tcp.samdom.trial.com
_ldap._tcp.samdom.trial.com has SRV record 0 100 389 ubuntuserver.samdom.trial.c
om.
leul@ubuntuserver:~$ host -t SRV _kerberos._udp.samdom.trial.com
_kerberos._udp.samdom.trial.com has SRV record 0 100 88 ubuntuserver.samdom.tria
l.com.
leul@ubuntuserver:~$ host -t A ubserver.samdom.trial.com
Host ubserver.samdom.trial.com not found: 3(NXDOMAIN)
leul@ubuntuserver:~$
```

Step 5: Configure Kerberos

Kerberos configuration is handled by the `krb5.conf` file. This file is typically located in the `/etc` directory, please refer to your distribution documentation for the location of this file on your system. There is a sample file located at `/usr/local/samba/share/setup/krb5.conf` that is a suitable replacement for an existing file. This file is generated by provision and will look similar to the following:

```
[libdefaults]
    default_realm = SAMDOM.TRIAL.COM
    dns_lookup_realm = false
    dns_lookup_kdc = true
```

- Note: If you have forgotten your realm, running `samba-tool testparm --suppress-prompt | grep realm` will let you know what you used.

Testing Kerberos

The simplest test is to use the `kinit` command as follows:

```
$ kinit administrator@SAMDOM.TRIAL.COM
Password:
```

- Note: You must specify your domain realm `SAMDOM.EXAMPLE.COM` in **uppercase letters**
- Note: Depending on your distribution `kinit` may just return you to a prompt, however, some distributions may return something like **Warning: Your password will expire in 41 days on Thu Mar 28 04:38:35 2013.**

To verify that Kerberos is working, and that you received a ticket, run the following:

```
$ klist
Ticket cache: FILE:/tmp/krb5cc_1000
Default principal: administrator@SAMDOM.TRIAL.COM

Valid starting     Expires            Service principal
02/10/13 19:39:48  02/11/13 19:39:46  krbtgt/SAMDOM.TRIAL.COM@SAMDOM.TRIAL.COM
```

If either `kinit` or `klist` do not exist on your system, refer to Samba_4_OS_Requirements on how to install the necessary packages.

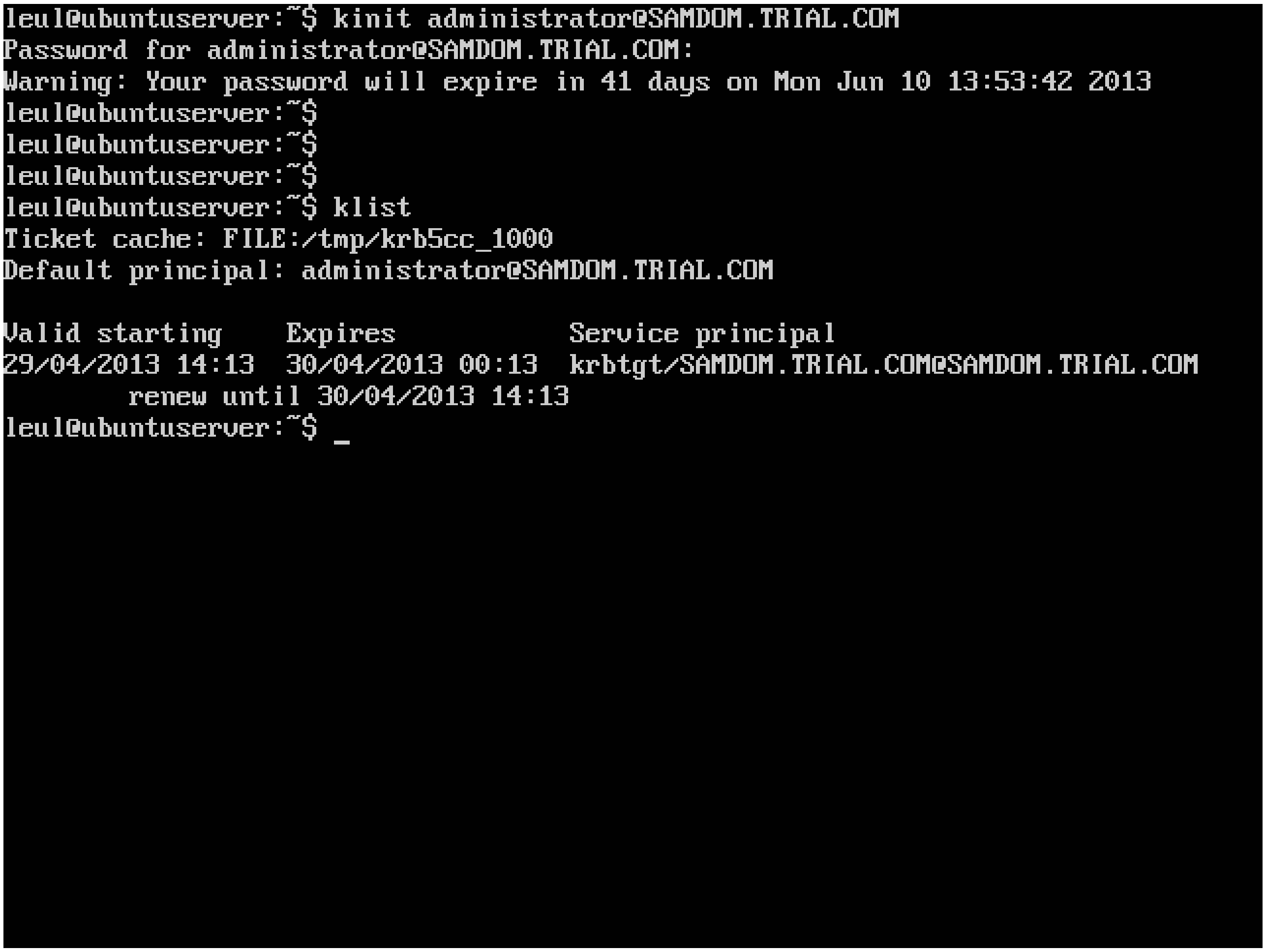
You can also test Kerberos form a remote client, but you must first configure the client's `krb5.conf` and `resolve.conf` as shown previously.

- Note: If you are using a client behind NAT then you have to add the following to the `krb5.conf` on the domain controller server:

```
[kdc]
    check-ticket-addresses = false
```

- Note: If provision generated you a password and you forgot it or didn't get it saved in some way, you can use "samba-tool user setpassword administrator" as root to reset it.

For the above tests your output should be similar to this:

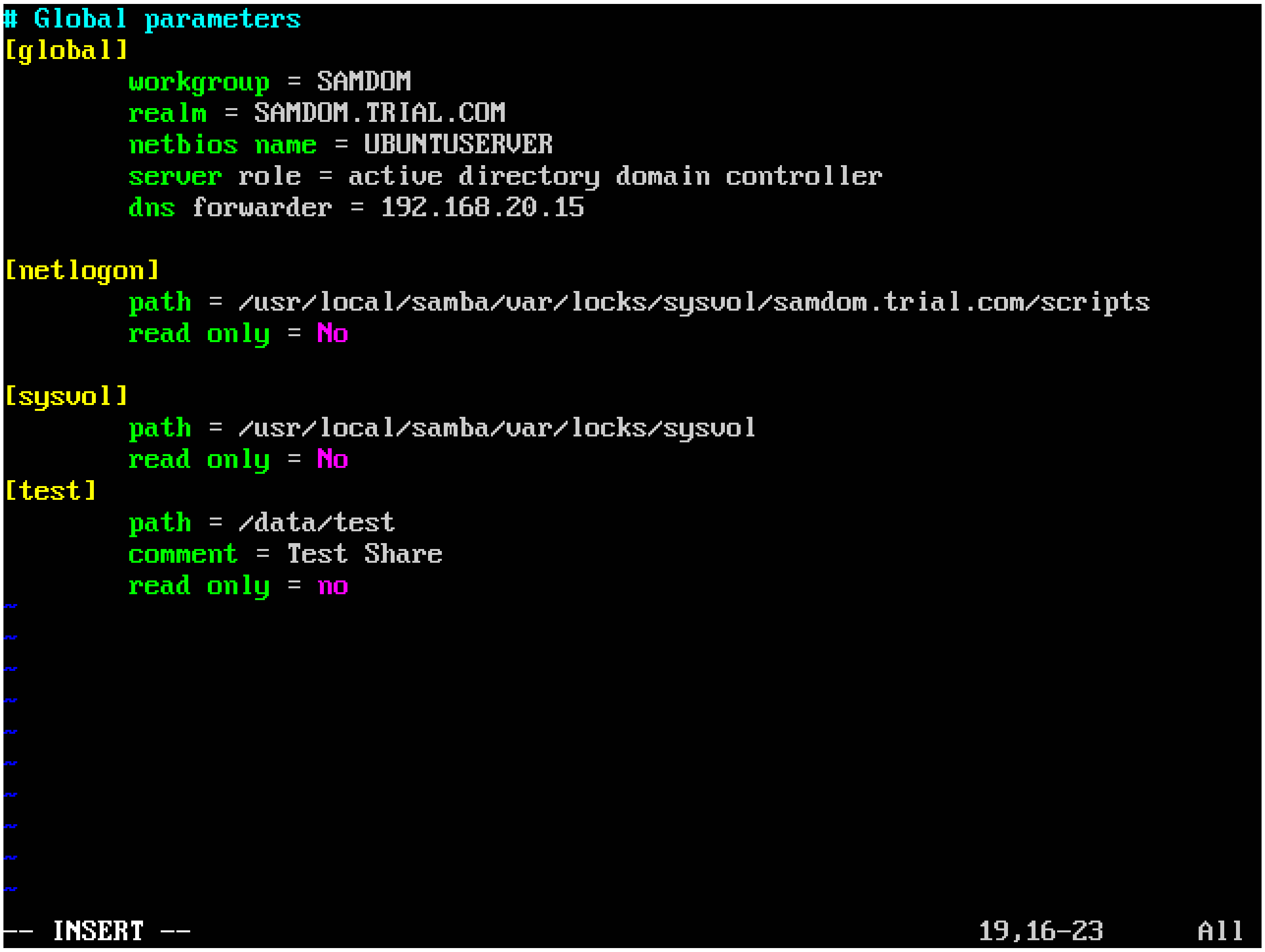


```
leul@ubuntuserver:~$ kinit administrator@SAMDOM.TRIAL.COM
Password for administrator@SAMDOM.TRIAL.COM:
Warning: Your password will expire in 41 days on Mon Jun 10 13:53:42 2013
leul@ubuntuserver:~$
leul@ubuntuserver:~$
leul@ubuntuserver:~$
leul@ubuntuserver:~$ klist
Ticket cache: FILE:/tmp/krb5cc_1000
Default principal: administrator@SAMDOM.TRIAL.COM

Valid starting    Expires           Service principal
29/04/2013 14:13  30/04/2013 00:13  krbtgt/SAMDOM.TRIAL.COM@SAMDOM.TRIAL.COM
        renew until 30/04/2013 14:13
leul@ubuntuserver:~$ _
```

Setup a basic File Share

The provisioning will create a very simple `/usr/local/samba/etc/smb.conf` file with no non-system shares by default. The system sysvol and netlogon shares should be created for you , as these are needed for a domain controller.

If you are also using the server as a file server, or you have some other reason to share files then you should create such shares as needed. For example:



```
# Global parameters
[global]
        workgroup = SAMDOM
        realm = SAMDOM.TRIAL.COM
        netbios name = UBUNTUSERVER
        server role = active directory domain controller
        dns forwarder = 192.168.20.15

[netlogon]
        path = /usr/local/samba/var/locks/sysvol/samdom.trial.com/scripts
        read only = No

[sysvol]
        path = /usr/local/samba/var/locks/sysvol
        read only = No
[test]
        path = /data/test
        comment = Test Share
        read only = no
~
~
~
~
~
~
~
~
~
~

-- INSERT --                                                    19,16-23      All
```

Part IV

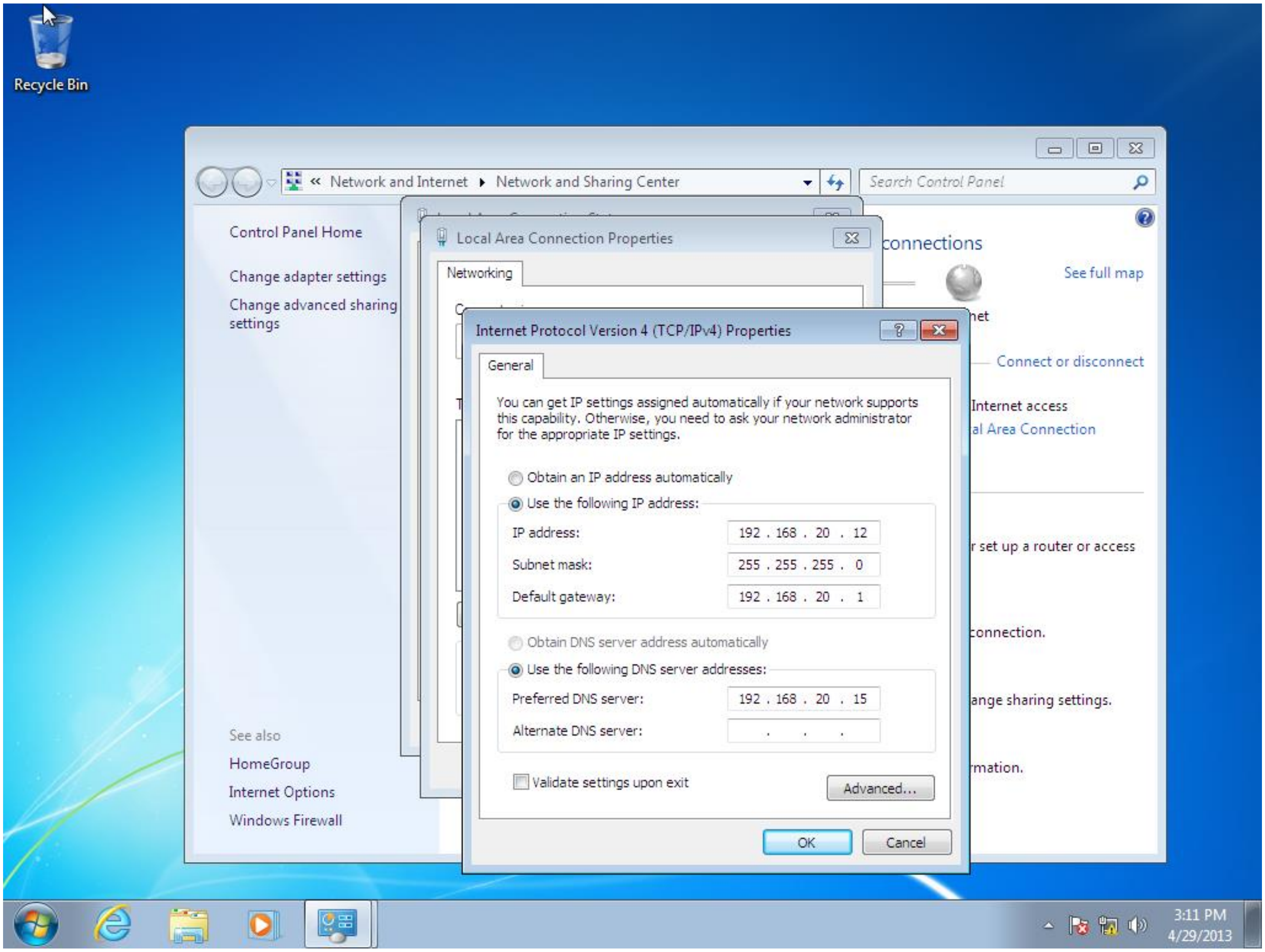
Configure a Windows Client to join our Samba Active Directory

Active Directory is a powerful administration service which enables an Administrator to centrally manage a network of Windows 2000, Windows XP Pro, Windows 2003, Windows Vista Business Edition, and Windows 7 Professional (and up) effectively. To test the real Samba capability, we use Windows XP Pro as testing environment (Windows XP Home doesn't include Active Directory functionality and won't work).

Step 1: Configure DNS Setting for Windows

On the network and sharing > double click on Local Area Connection > select Properties > choose the IPV4 settings > add an IP address and make the DNS server the IP of the Samba Server

Here is a snap shot:



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

IP address: 192 . 168 . 20 . 12
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 20 . 1

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

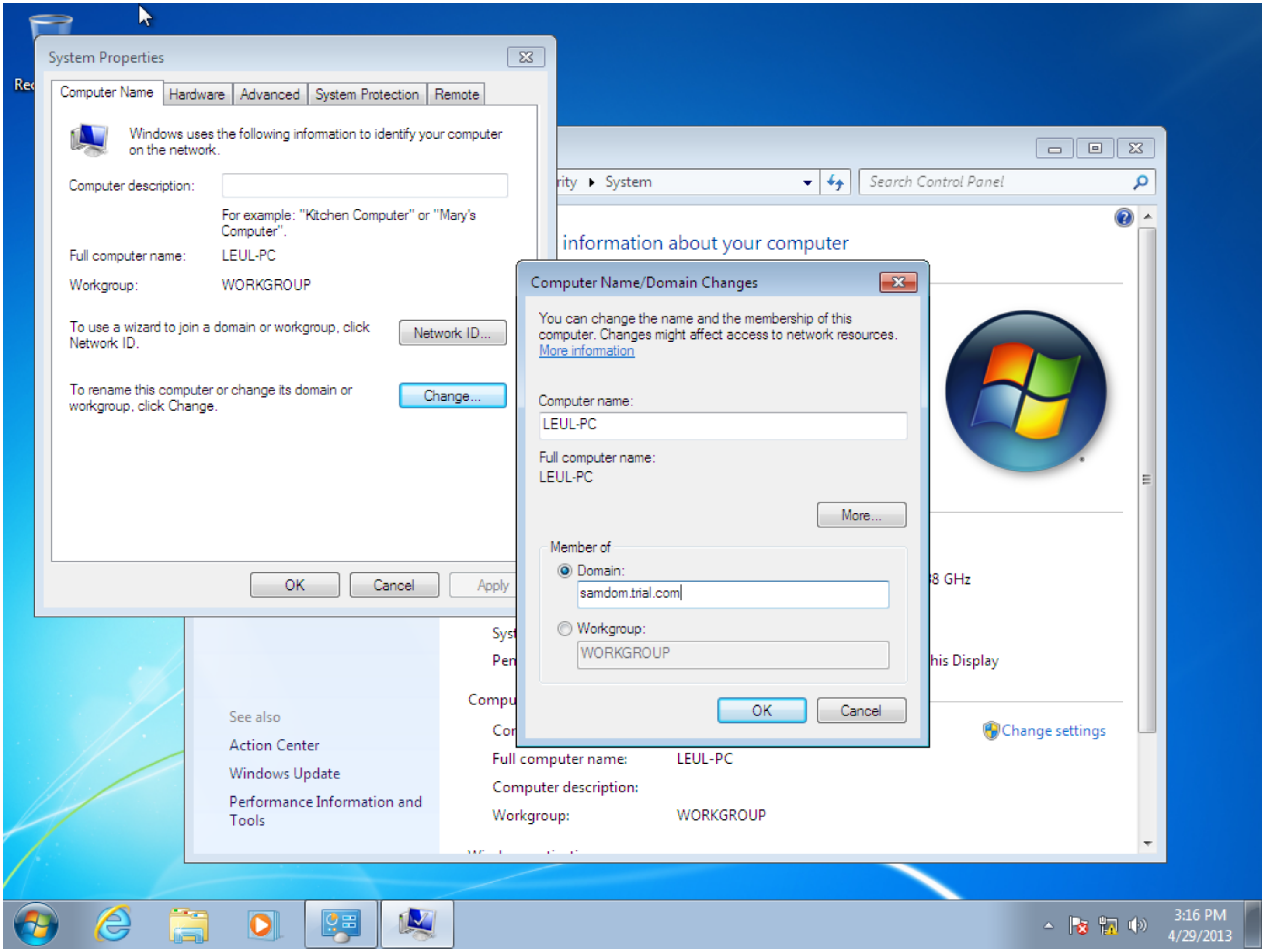
Preferred DNS server: 192 . 168 . 20 . 15
Alternate DNS server: . . .

□ Validate settings upon exit

Step 2: Joining Windows Clients to the Domain

In my computer > click the system properties tab > change settings > under the Computer name Tab > change domain or workgroup > select domain > enter the name of the domain you chose on Samba > enter the Administrative password.

Here is a snap shot



System Properties

Windows uses the following information to identify your computer on the network.

Computer description:

For example: "Kitchen Computer" or "Mary's Computer".

Full computer name: LEUL-PC

Workgroup: WORKGROUP

To use a wizard to join a domain or workgroup, click Network ID.

To rename this computer or change its domain or workgroup, click Change.

Computer Name/Domain Changes

You can change the name and the membership of this computer. Changes might affect access to network resources. More information

Computer name: LEUL-PC

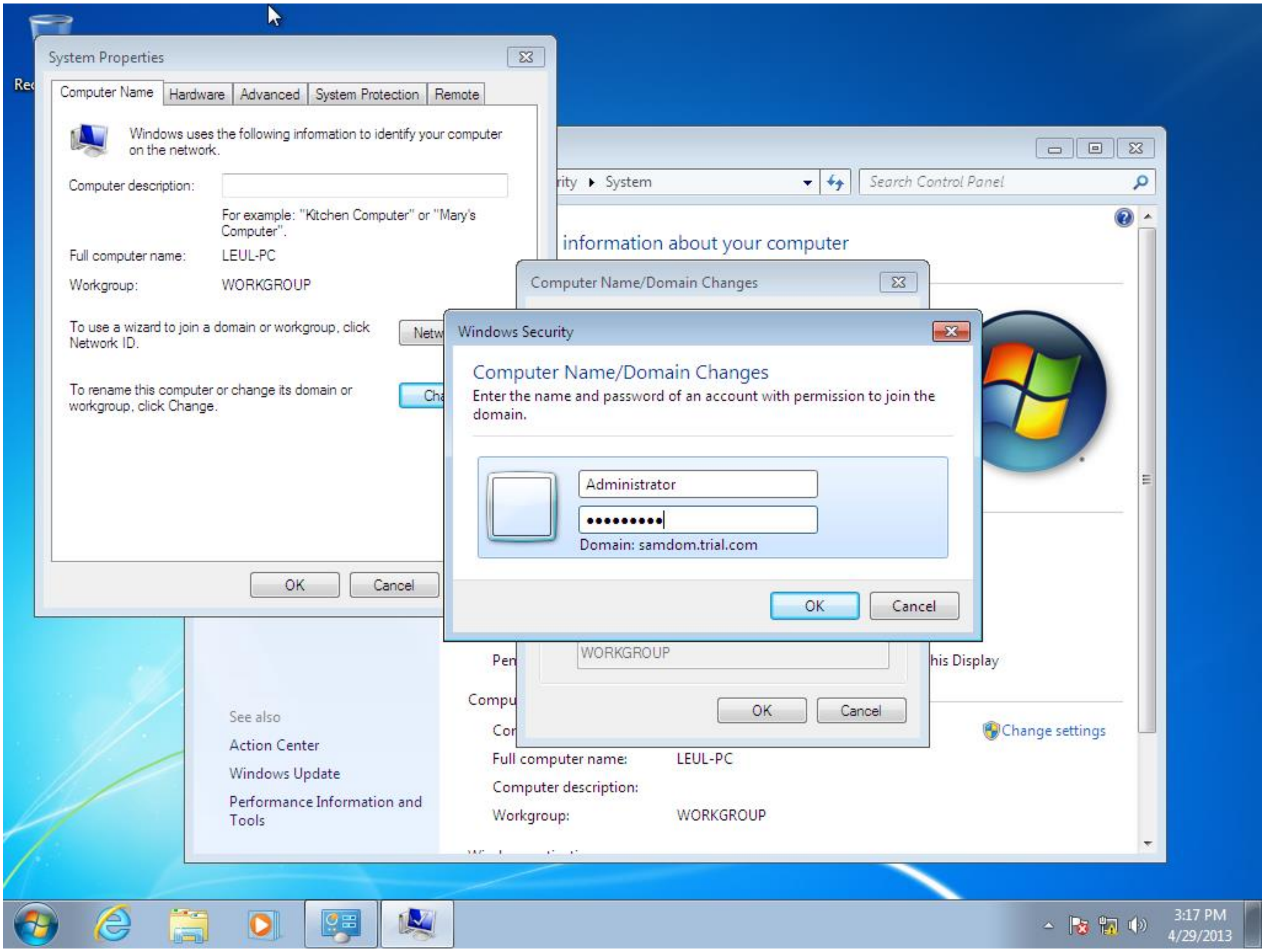
Full computer name: LEUL-PC

Member of

● Domain: samdom.trial.com

○ Workgroup: WORKGROUP

Then you would need to login to the domain, here is another snap shot:



System Properties

Windows uses the following information to identify your computer on the network.

Computer description:

For example: "Kitchen Computer" or "Mary's Computer".

Full computer name: LEUL-PC

Workgroup: WORKGROUP

To use a wizard to join a domain or workgroup, click Network ID.

To rename this computer or change its domain or workgroup, click Change.

Windows Security

Computer Name/Domain Changes

Enter the name and password of an account with permission to join the domain.

Administrator

•••••••••

Domain: samdom.trial.com

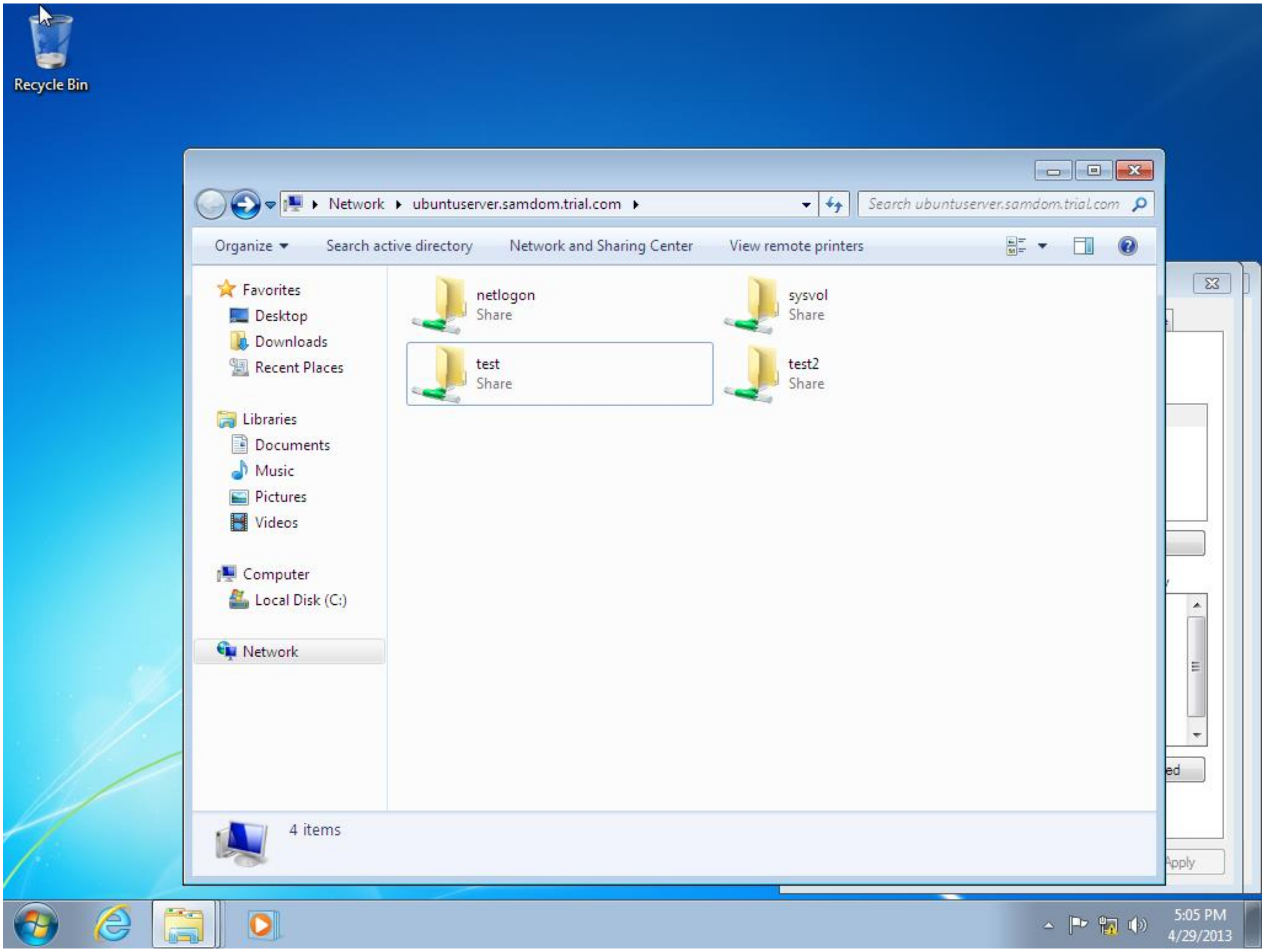
Note: the username to join the domain would be ‘Administrator’

You will be prompted to restart the computer, then restart it.

To view the shares from the windows side:

Ctrl + Alt + Del > Login as the Administrator

On the search on the start button > write \\hostname.domainname



For this example it will be \\ubuntuserver.samdom.trial.com

To create users you will have two options one is using the samba tool and the other is using AD management form windows side.

From the samba side:

Adding users with samba tool

Adding Users into Samba Active Directory

Unlike Samba 3, Samba 4 does not require a local Unix user for each Samba user that is created.

To create a Samba user, use the following command:

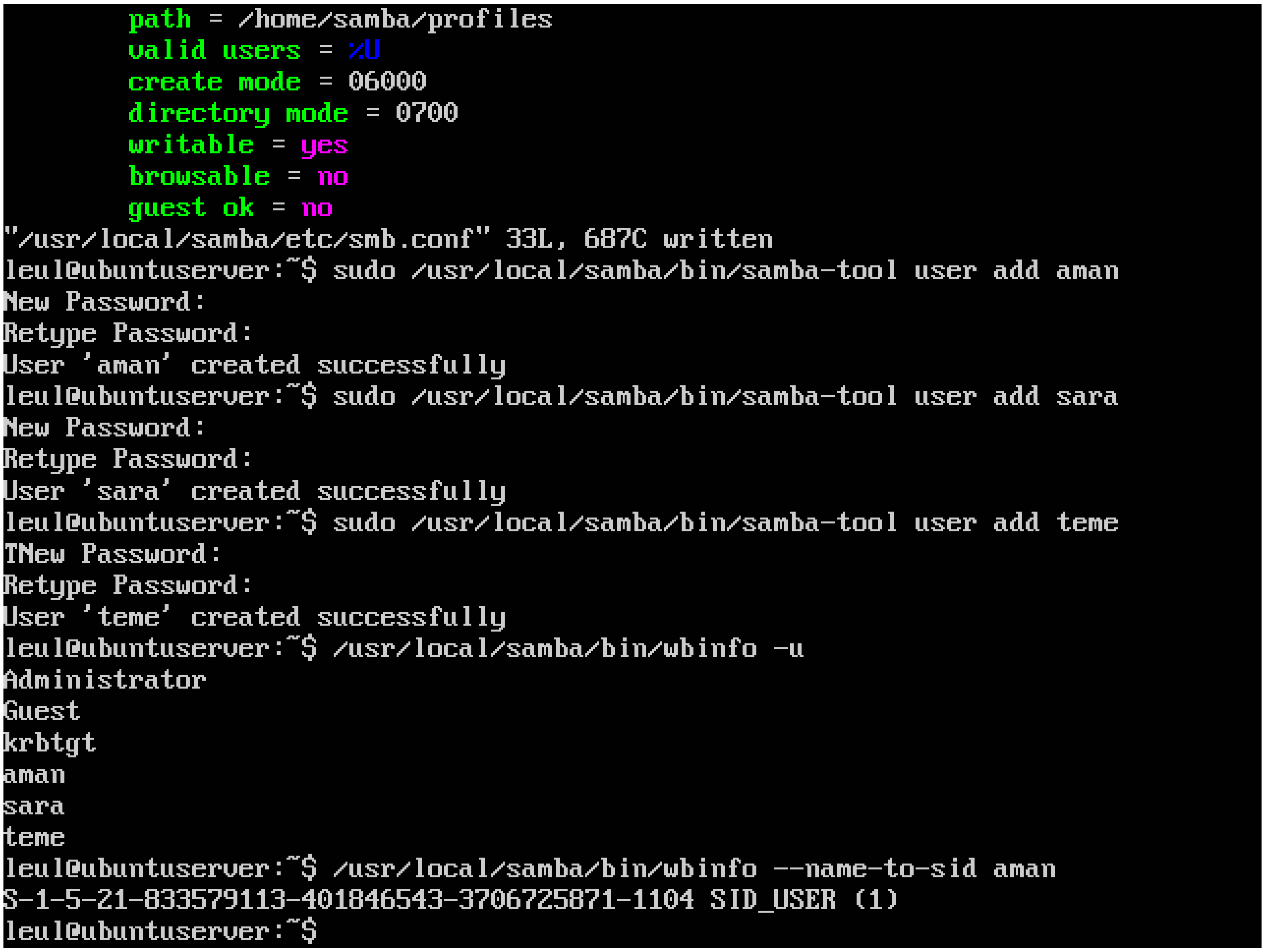
```
/usr/local/samba/bin/samba-tool user add USERNAME
```

To inspect the allocated user ID and SID, use the following command:

```
$ /usr/local/samba/bin/wbinfo --name-to-sid USERNAME
S-1-5-21-4036476082-4153129556-3089177936-1005 SID_USER (1)
```

```
$ /usr/local/samba/bin/wbinfo --sid-to-uid S-1-5-21-4036476082-4153129556-3089177936-1005
3000011
```

Here is a snap shot: (after the line saying “/usr/local/samba/etc/smb.conf” 33L, 687c written”)



```
        path = /home/samba/profiles
        valid users = %U
        create mode = 06000
        directory mode = 0700
        writable = yes
        browsable = no
        guest ok = no
"/usr/local/samba/etc/smb.conf" 33L, 687C written
leul@ubuntuserver:~$ sudo /usr/local/samba/bin/samba-tool user add aman
New Password:
Retype Password:
User 'aman' created successfully
leul@ubuntuserver:~$ sudo /usr/local/samba/bin/samba-tool user add sara
New Password:
Retype Password:
User 'sara' created successfully
leul@ubuntuserver:~$ sudo /usr/local/samba/bin/samba-tool user add teme
TNew Password:
Retype Password:
User 'teme' created successfully
leul@ubuntuserver:~$ /usr/local/samba/bin/wbinfo -u
Administrator
Guest
krbtgt
aman
sara
teme
leul@ubuntuserver:~$ /usr/local/samba/bin/wbinfo --name-to-sid aman
S-1-5-21-833579113-401846543-3706725871-1104 SID_USER (1)
leul@ubuntuserver:~$
```

Part V

Samba AD management

You can manage your Samba AD just like a windows AD using the windows tools

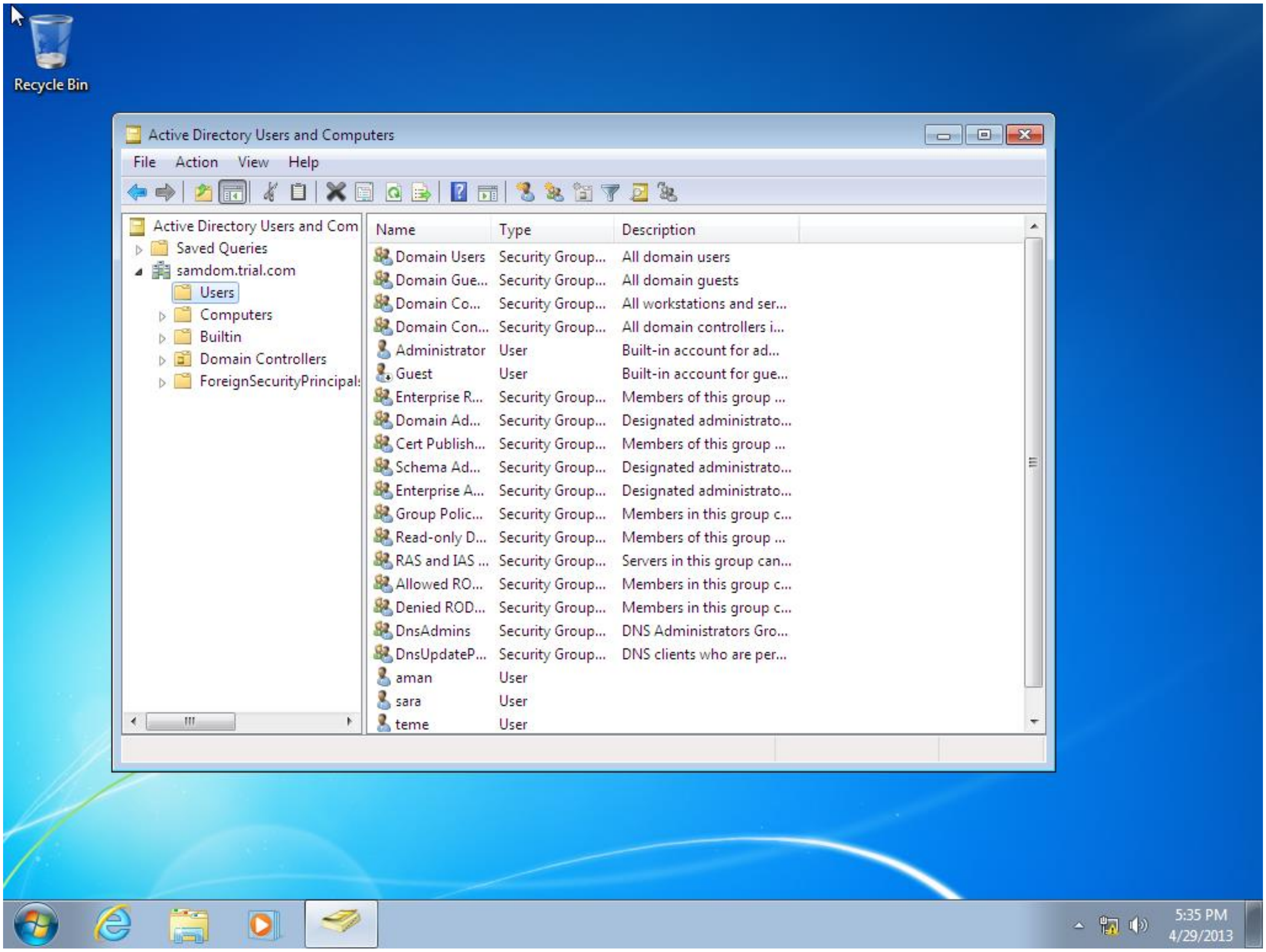
Step 1: Installing Windows Remote Administration Tools onto Windows

Windows Vista/7/8

1. Download the Windows Remote Administration Tools from:
   - http://www.microsoft.com/downloads/details.aspx?FamilyId=9FF6E897-23CE-4A36-B7FC-D52065DE9960&displaylang=en (Vista)
   - http://www.microsoft.com/downloads/details.aspx?FamilyID=7D2F6AD7-656B-4313-A005-4E344E43997D&displaylang=en (Windows 7)
   - http://www.microsoft.com/download/details.aspx?id=28972 (Windows 8)
2. Follow the "Install RSAT" instructions

- Note: After installing, you have to enable the features in "Turn Windows features on or off" in "Programs" of the Control Panel!).

Step 2: Viewing Samba Active Directory Content

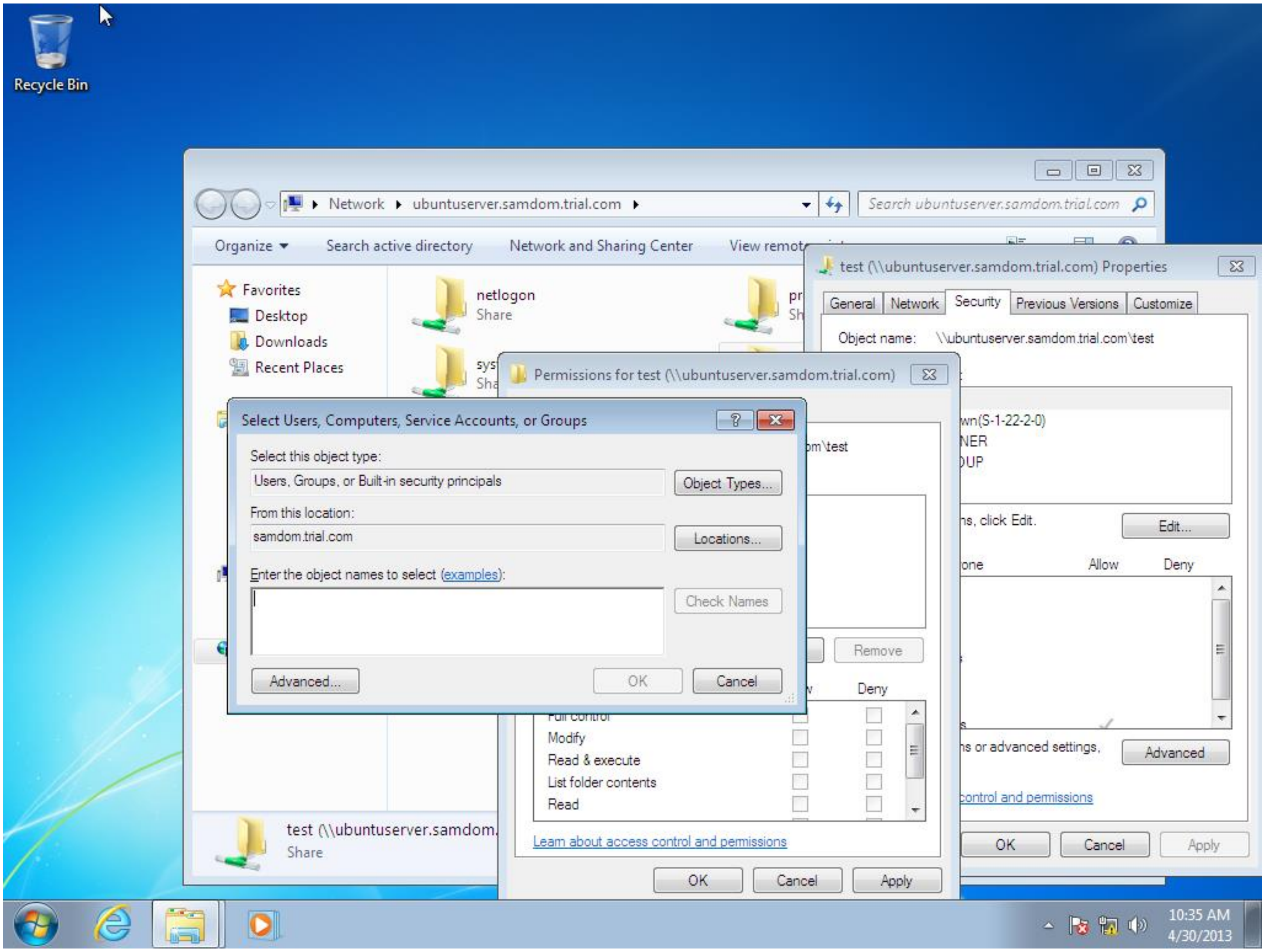


Name	Type	Description
Domain Users	Security Group...	All domain users
Domain Gue...	Security Group...	All domain guests
Domain Co...	Security Group...	All workstations and ser...
Domain Con...	Security Group...	All domain controllers i...
Administrator	User	Built-in account for ad...
Guest	User	Built-in account for gue...
Enterprise R...	Security Group...	Members of this group ...
Domain Ad...	Security Group...	Designated administrato...
Cert Publish...	Security Group...	Members of this group ...
Schema Ad...	Security Group...	Designated administrato...
Enterprise A...	Security Group...	Designated administrato...
Group Polic...	Security Group...	Members in this group c...
Read-only D...	Security Group...	Members of this group ...
RAS and IAS ...	Security Group...	Servers in this group can...
Allowed RO...	Security Group...	Members in this group c...
Denied ROD...	Security Group...	Members in this group c...
DnsAdmins	Security Group...	DNS Administrators Gro...
DnsUpdateP...	Security Group...	DNS clients who are per...
aman	User	
sara	User	
teme	User	

Setting access permissions to different users and groups on shared files and folders can be done form the windows side.

Log on as the Administrator > right click on the share> Properties> Security tab > edit

Here you can add, delete, edit the accessing privileges of users and groups:



Recycle Bin
Network ▸ ubuntuserver.samdom.trial.com ▸
Search ubuntuserver.samdom.trial.com
Organize ▾
Search active directory
Network and Sharing Center
View remot
Favorites
Desktop
Downloads
Recent Places
netlogon
Share
test (\\ubuntuserver.samdom.trial.com) Properties
General
Network
Security
Previous Versions
Customize
Permissions for test (\\ubuntuserver.samdom.trial.com)
Select Users, Computers, Service Accounts, or Groups
Object Types...
Locations...
Check Names
Advanced...
OK
Cancel
Remove
Deny
Full control
Modify
Read & execute
List folder contents
Read
Learn about access control and permissions
Apply
Edit...
Allow
Advanced
test (\\ubuntuserver.samdom.
Share
10:35 AM
4/30/2013

Object name: \\ubuntuserver.samdom.trial.com\test

Select this object type: Users, Groups, or Built-in security principals

From this location: samdom.trial.com

Enter the object names to select (examples):

Setting Up Roaming Profiles

1. You will need to create a share for the profiles, typically named `profiles`. Edit the `/usr/local/samba/etc/smb.conf` to include:

```
[profiles]
      path = /usr/local/samba/var/profiles
      read only = no
```

2. Create the directory above using:

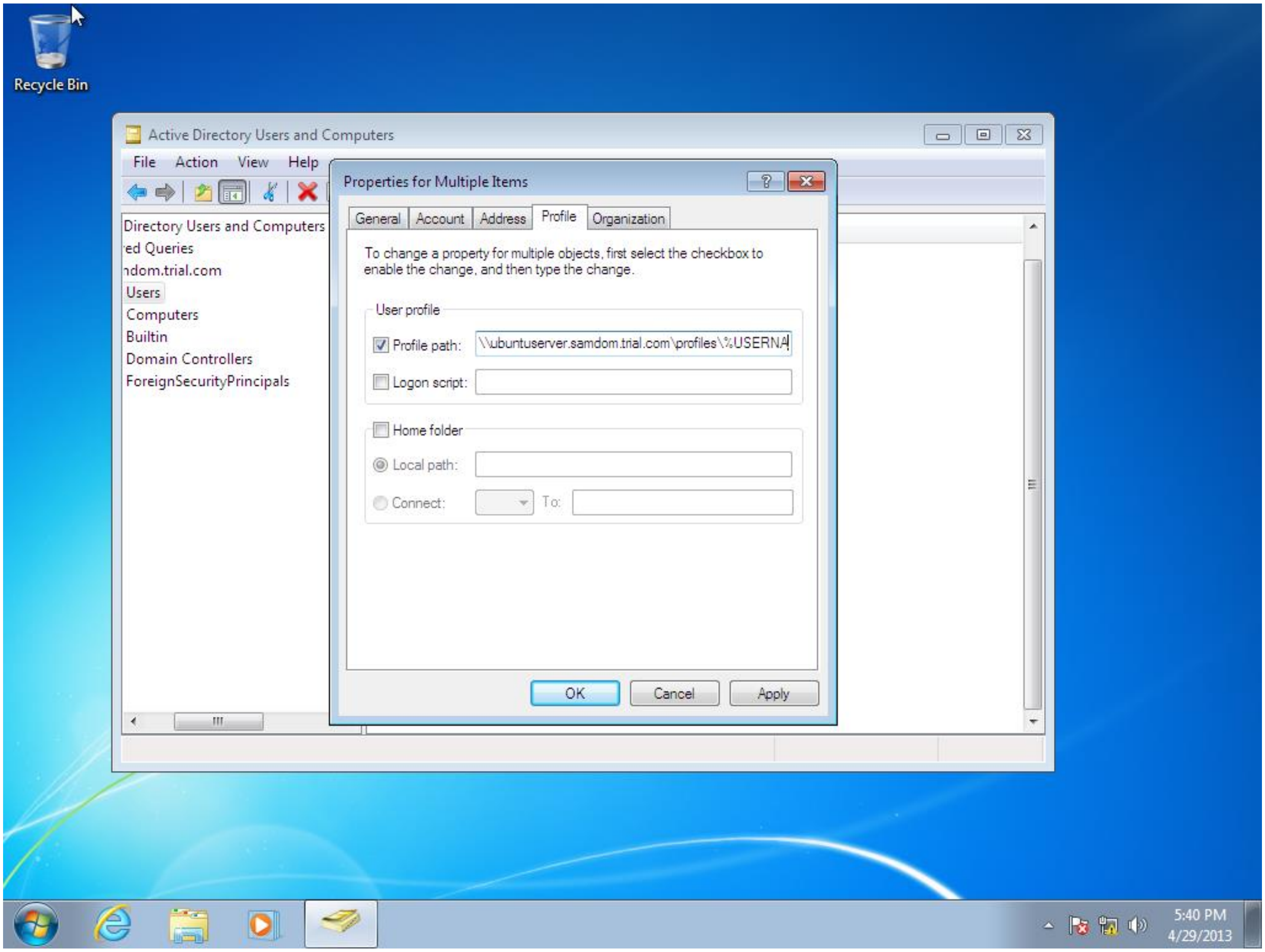
```
$ sudo mkdir /usr/local/samba/var/profiles
```

3. In Windows, start *Active Directory Users and Computers*, select all the users, right click, and hit properties

4. Under the profile tab, in the *Profile path*, type the path to your share along with %USERNAME% as follows:

```
\\sambaserver.samdom.example.com\profiles\%USERNAME%
```

5. click OK, logout and login as one of those users. When you logout again, you should see that the profile has been synced onto the samba server.



To change a property for multiple objects, first select the checkbox to enable the change, and then type the change.

User profile

☑ Profile path: \\ubuntuserver.samdom.trial.com\profiles\%USERNA

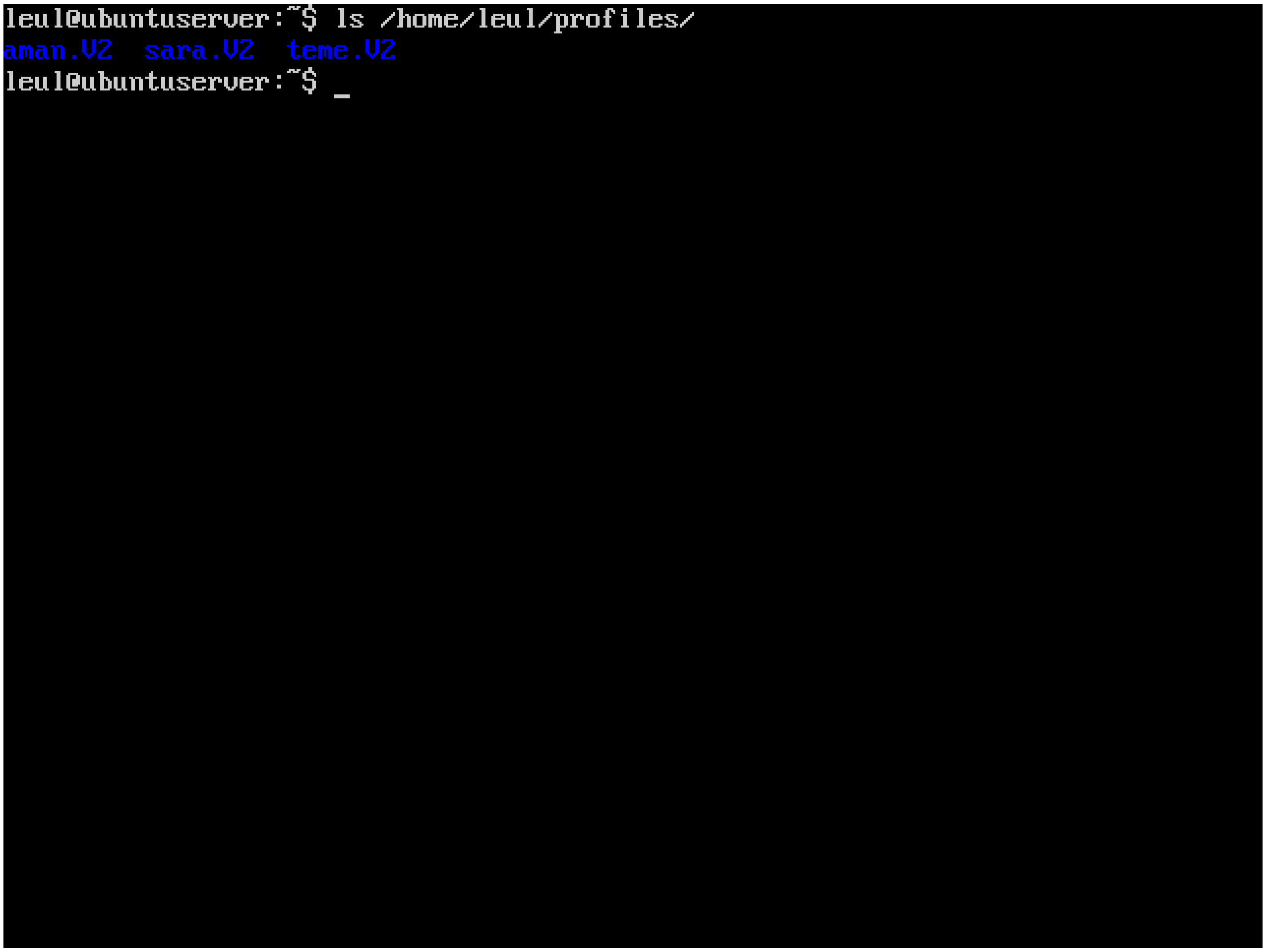
□ Logon script:

□ Home folder

● Local path:

○ Connect: To:

And from the samba side on the profiles directory you should be able to view something similar to this:



```
leul@ubuntuserver:~$ ls /home/leul/profiles/
aman.V2  sara.V2  teme.V2
leul@ubuntuserver:~$ _
```

Adding Organization Units (OU) Into a Samba Domain

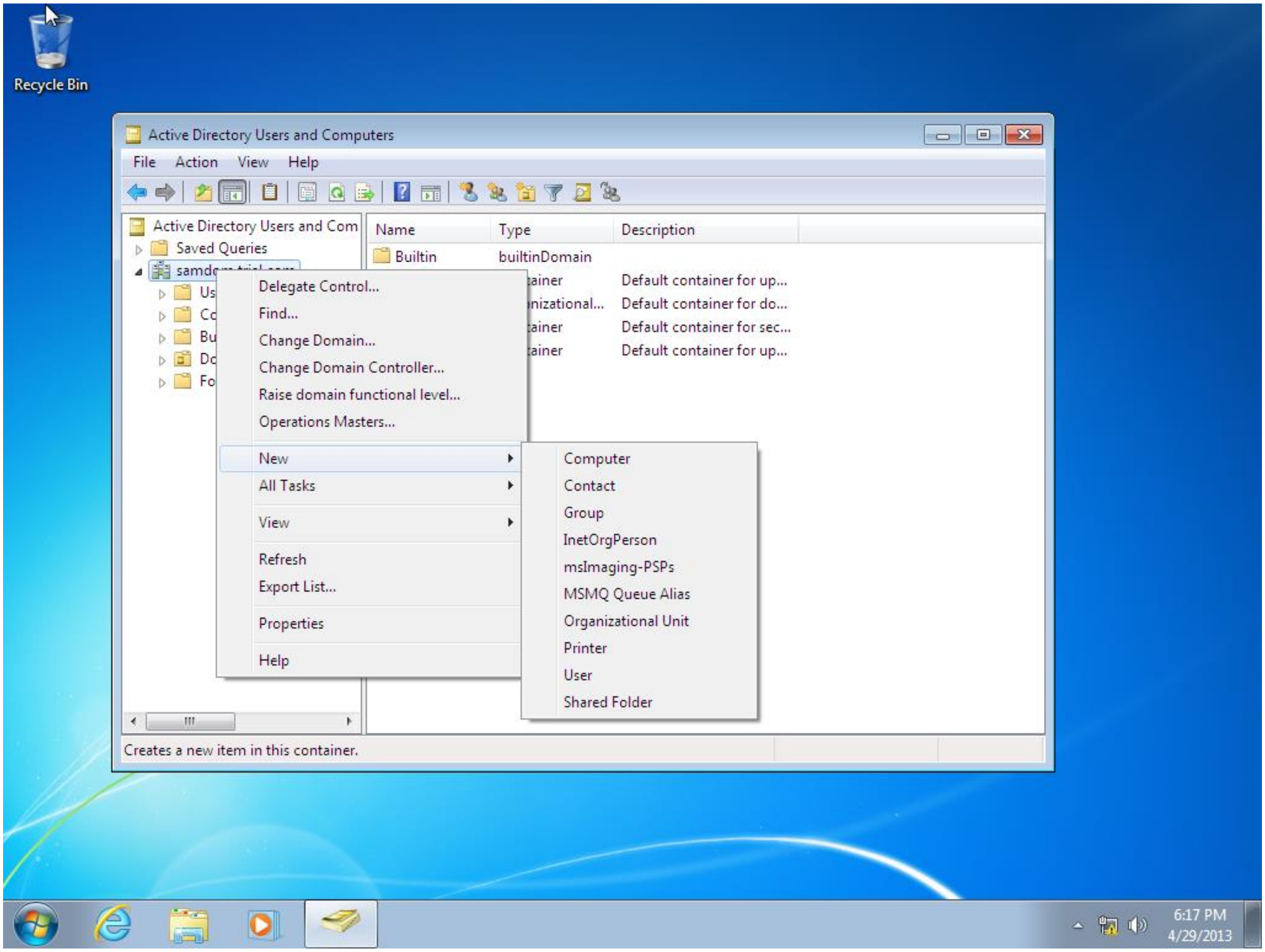
The Organizational Unit (OU) is a powerful feature in Active Directory. This is a type of container which allows you to drag & drop users and/or computers into it.

We can link several types of group policies to an OU, and the settings will push out to all users/computers that sit under the OU. Withing a single domain, you can have as many OUs and sub-OUs as you'd like. The result is that it can greatly reduce administrative overhead since you are able to manage everything via an OU.

To add OUs, Users and Groups from the AD management

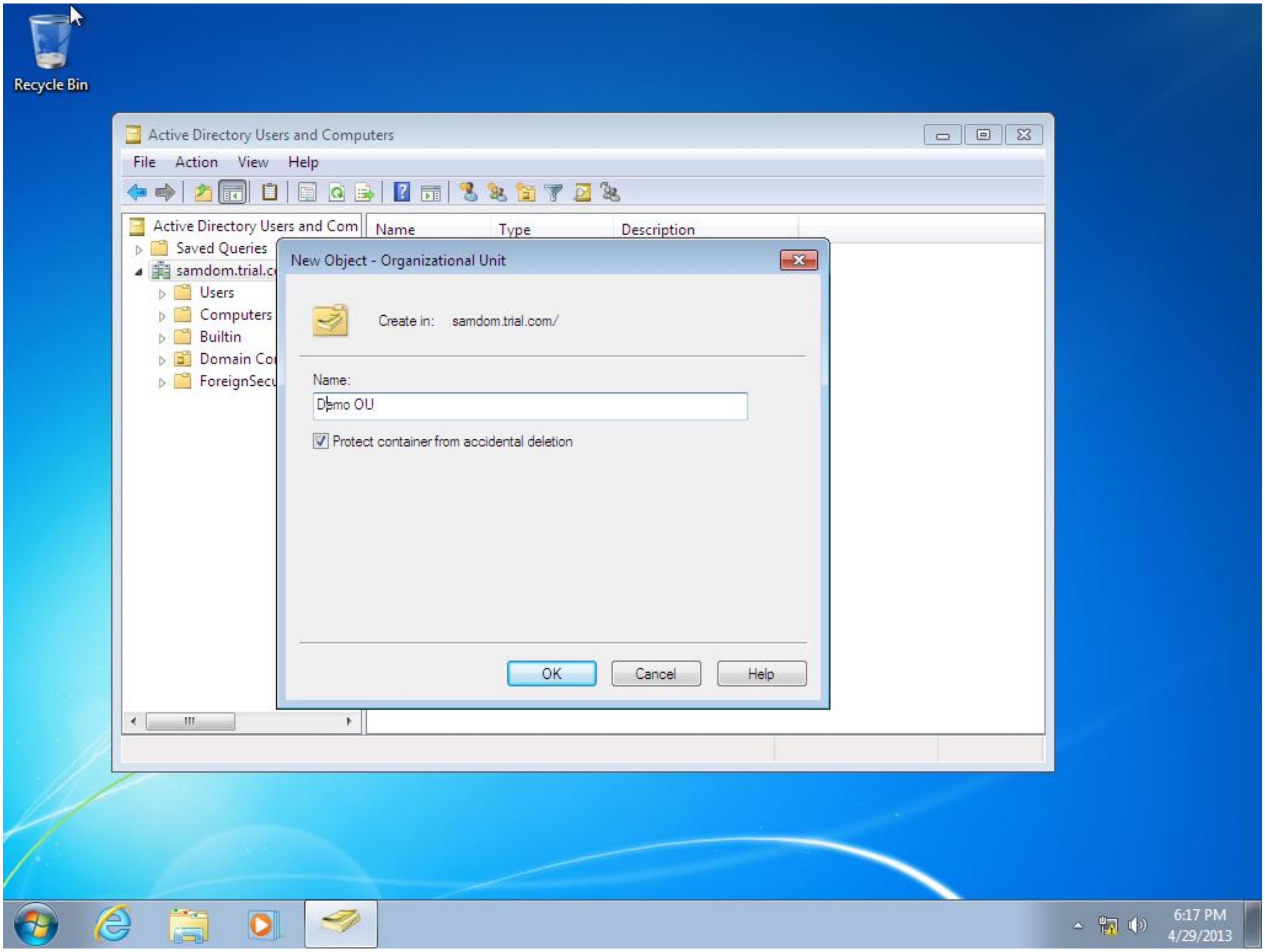
>Start > Active Directory users and computers > right click on the domain name

Here is a snap shot:



Here is a Demo Organizational Unit:

And to add users and groups to it, you just need to drag and drop inside the window after it is created.



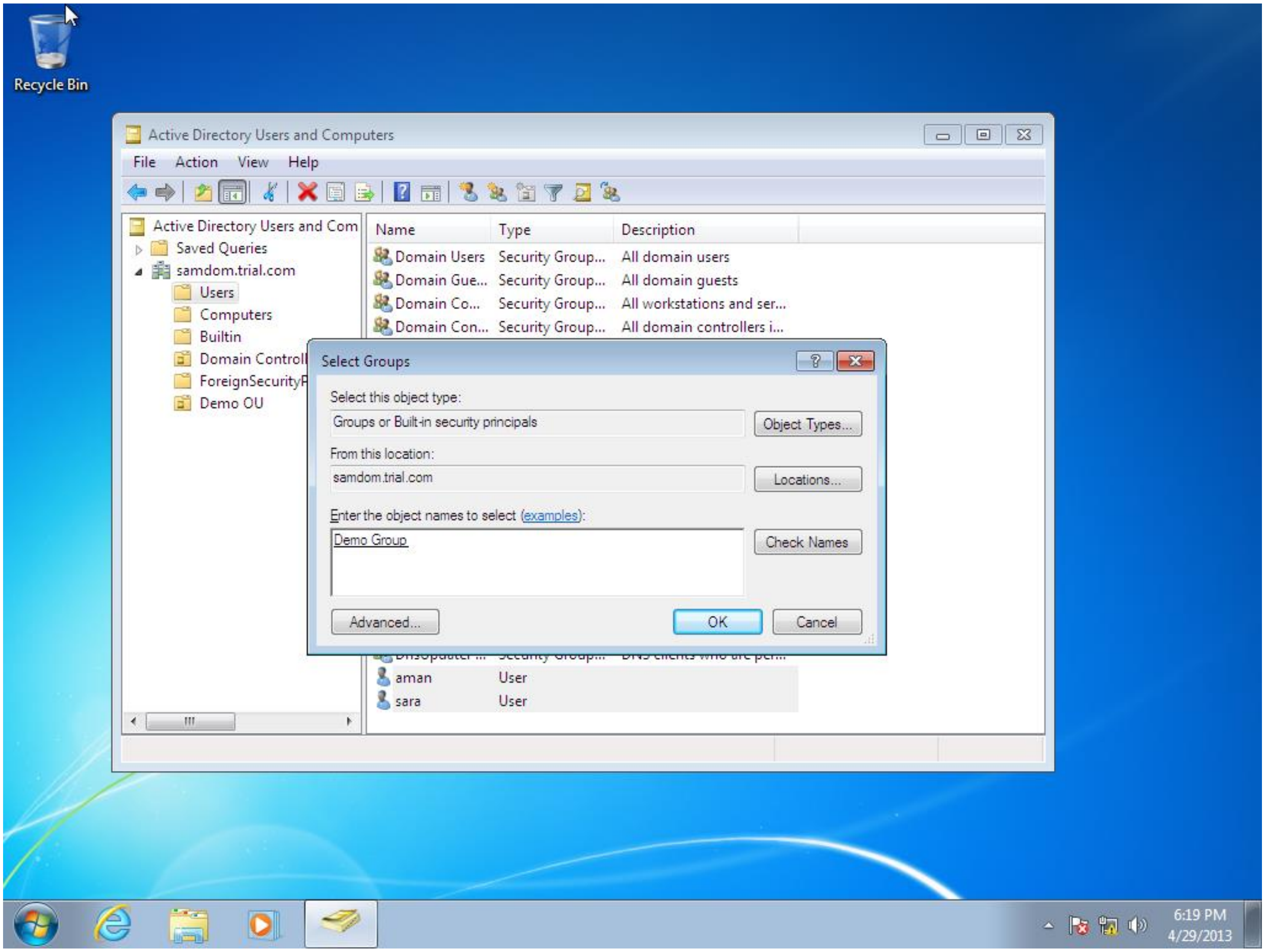
New Object - Organizational Unit

Create in: samdom.trial.com/

Name: Demo OU

☑ Protect container from accidental deletion

Adding a Demo Group:



Name	Type	Description
Domain Users	Security Group...	All domain users
Domain Gue...	Security Group...	All domain guests
Domain Co...	Security Group...	All workstations and ser...
Domain Con...	Security Group...	All domain controllers i...
aman	User	
sara	User	

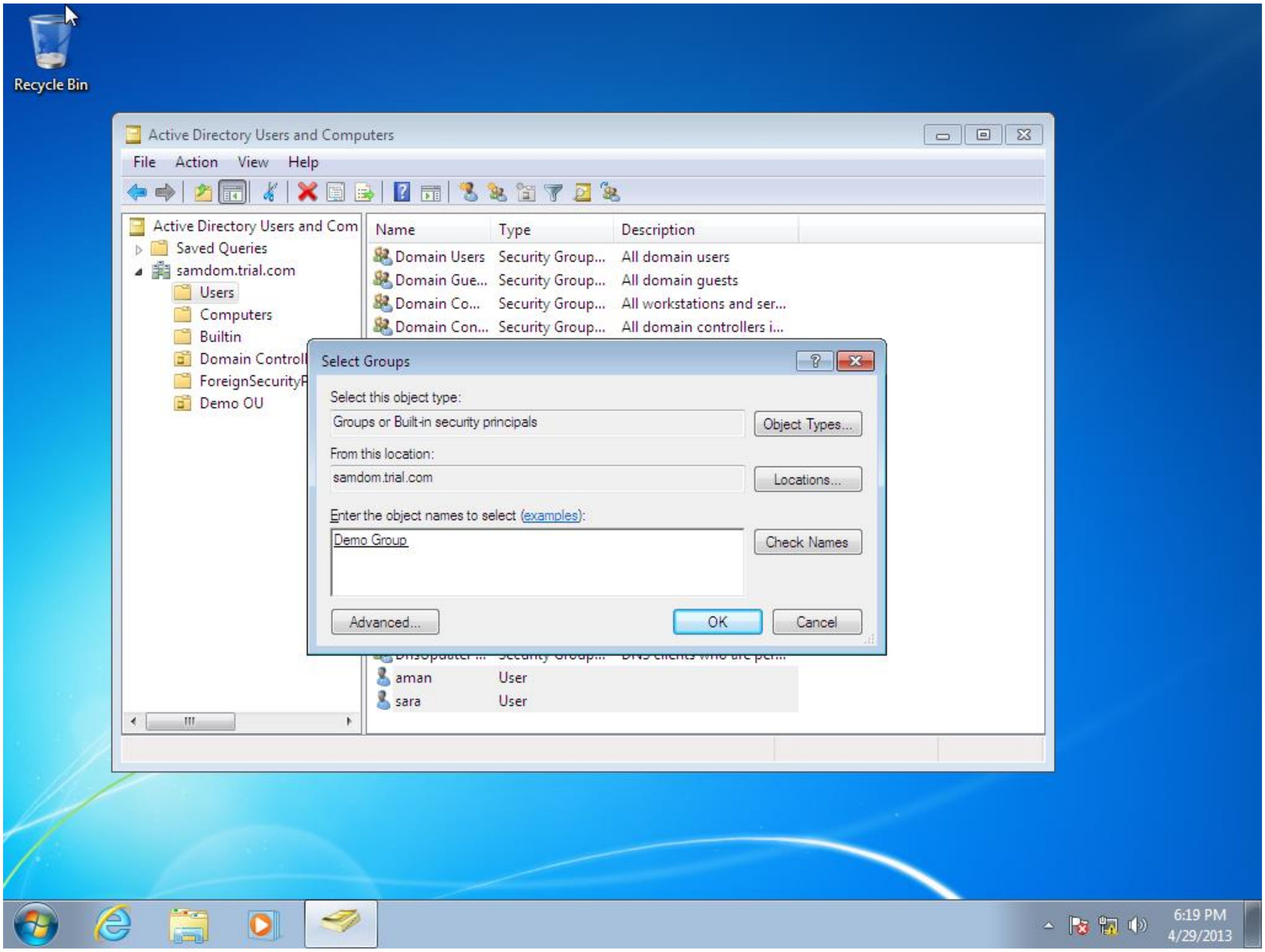
Select this object type:
Groups or Built-in security principals

From this location:
samdom.trial.com

Enter the object names to select (examples):
Demo Group

To add users to a Group:

Select the users > right click > choose Add to a group



Name	Type	Description
Domain Users	Security Group...	All domain users
Domain Gue...	Security Group...	All domain guests
Domain Co...	Security Group...	All workstations and ser...
Domain Con...	Security Group...	All domain controllers i...
aman	User	
sara	User	

Select this object type:
Groups or Built-in security principals

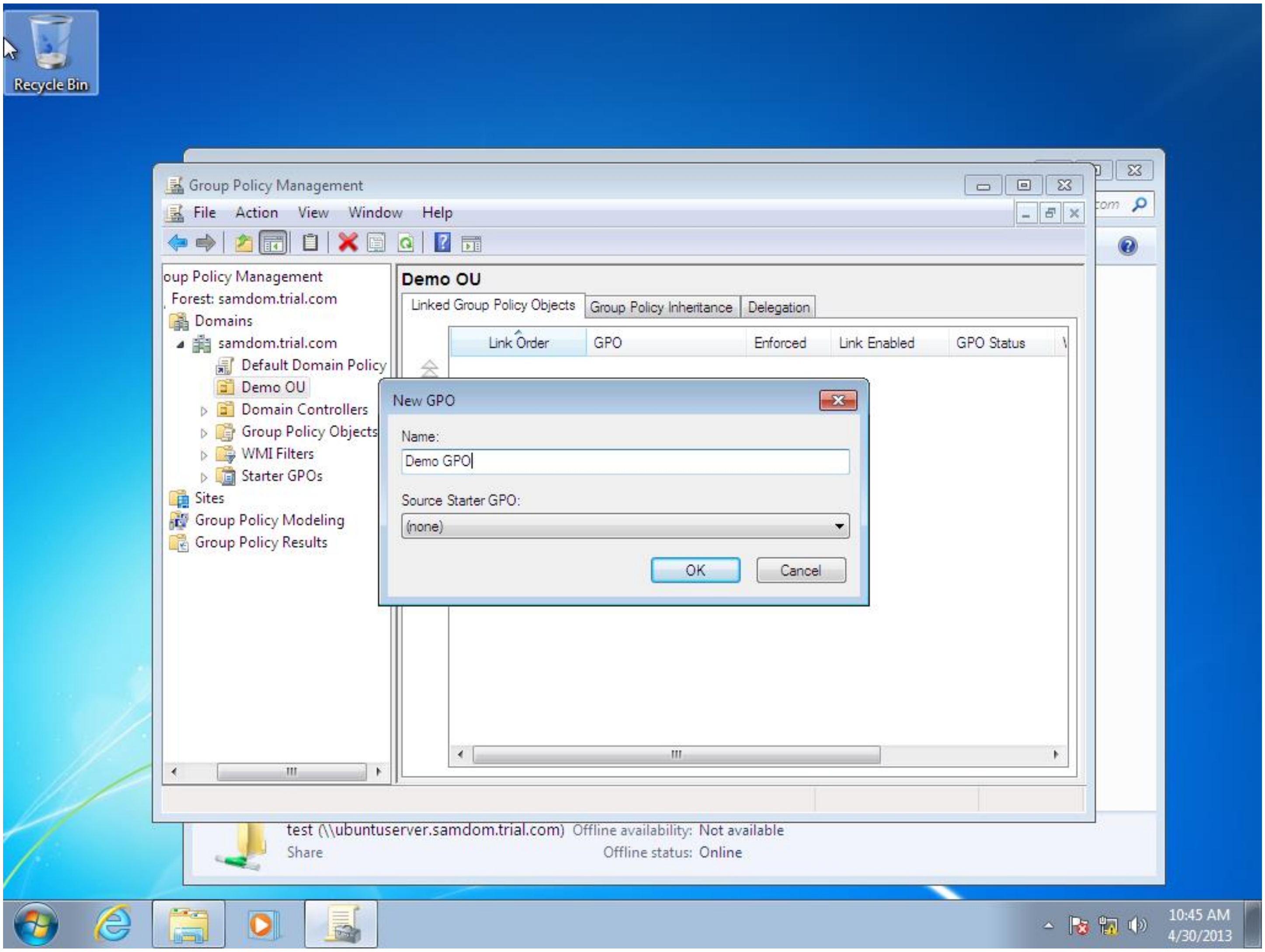
From this location:
samdom.trial.com

Enter the object names to select (examples):
Demo Group

Implementing Group Policies (GPO) in A Samba Domain

To add a GPO

Go to Start > Group Policy Management > Right click on one Organizational Unit > Create a GPO in this Domain



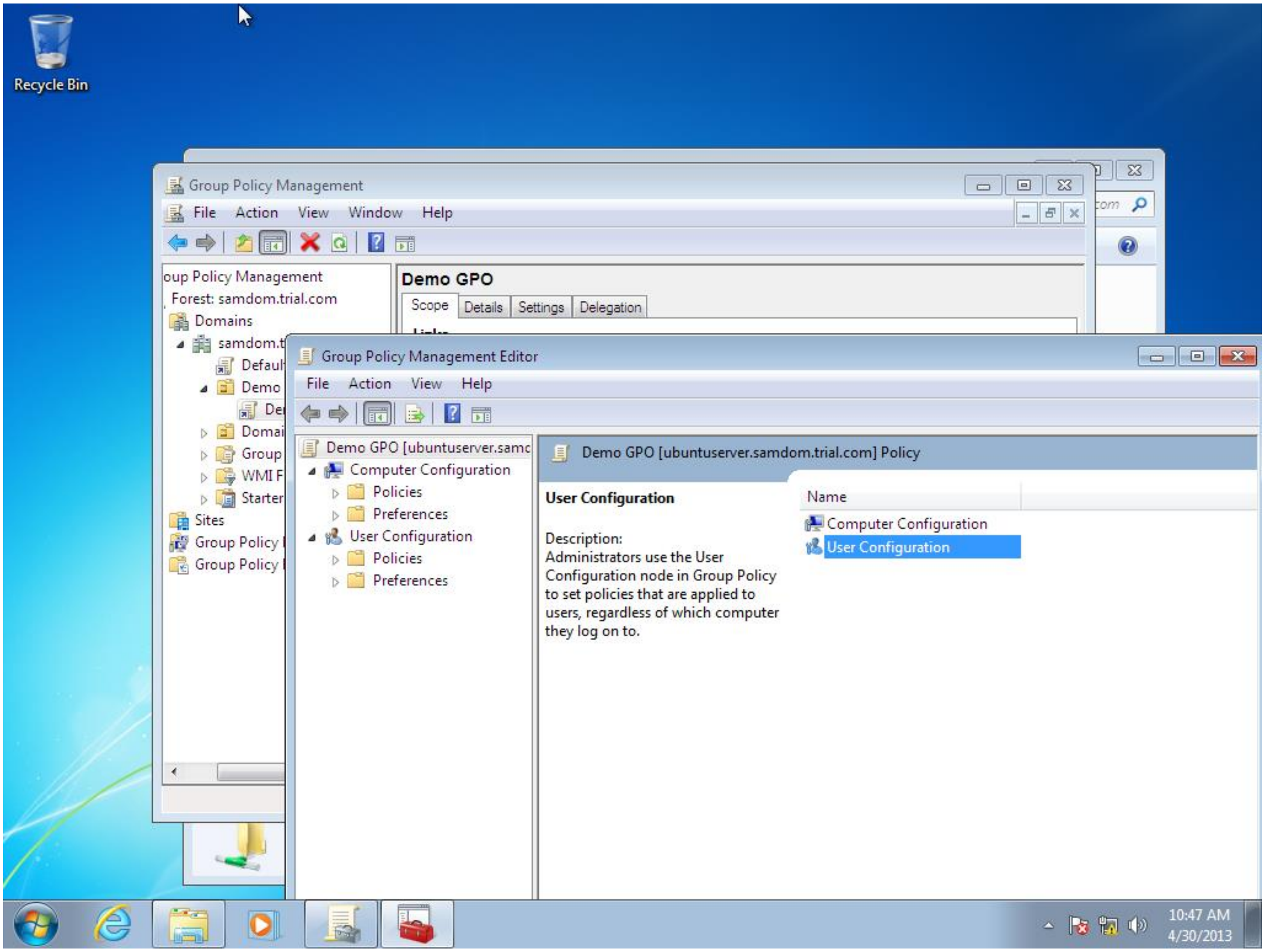
New GPO

Name: Demo GPO

Source Starter GPO: (none)

>Right click on the new GPO > Edit

>User Configuration



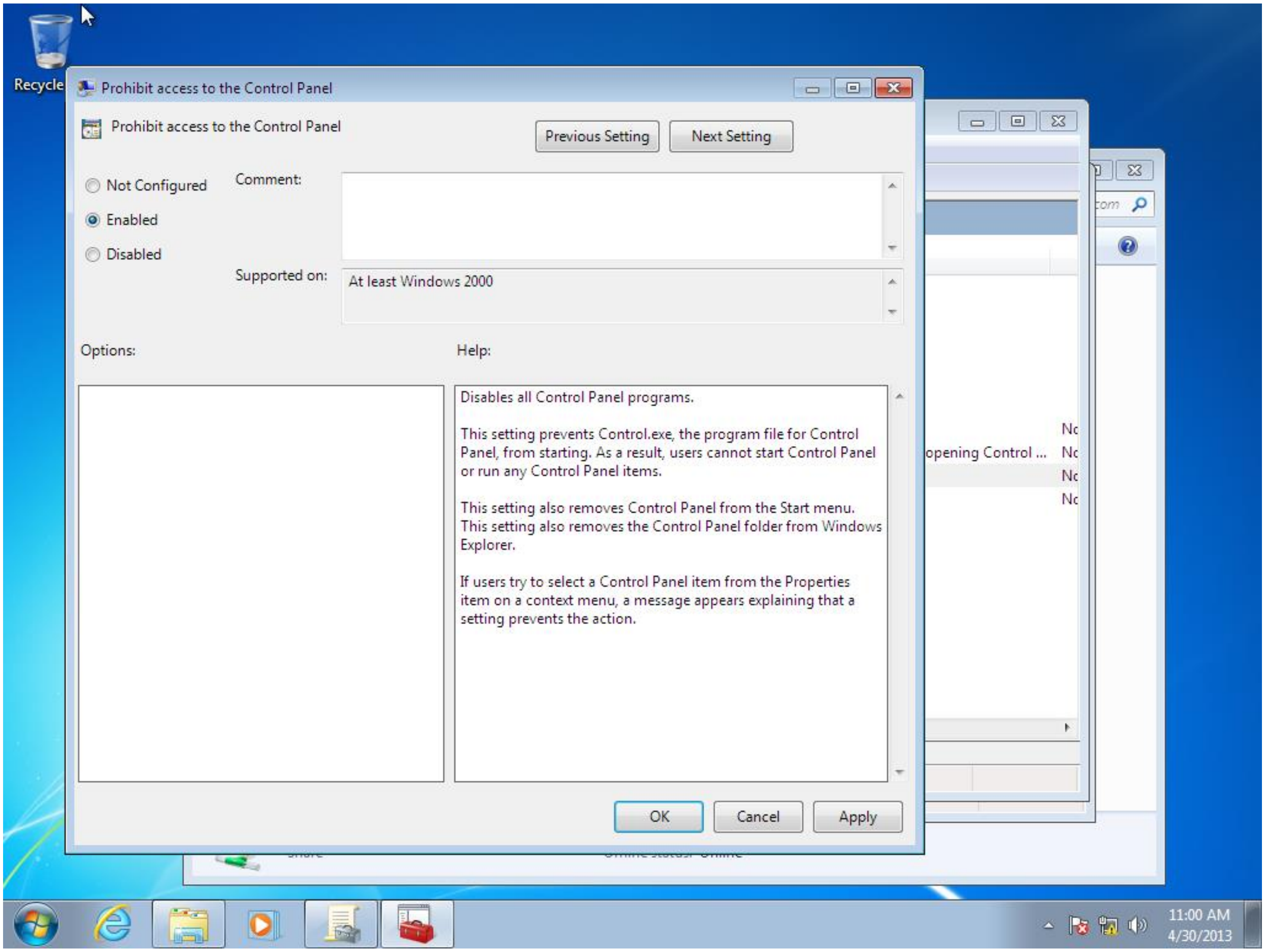
User Configuration

Description:
Administrators use the User Configuration node in Group Policy to set policies that are applied to users, regardless of which computer they log on to.

>Policies> administrative templates

Here is an example to prohibit access to the control panel for the Demo OU I created earlier

>control panel > prohibit access to the control panel > enable



Prohibit access to the Control Panel

○ Not Configured
● Enabled
○ Disabled

Supported on: At least Windows 2000

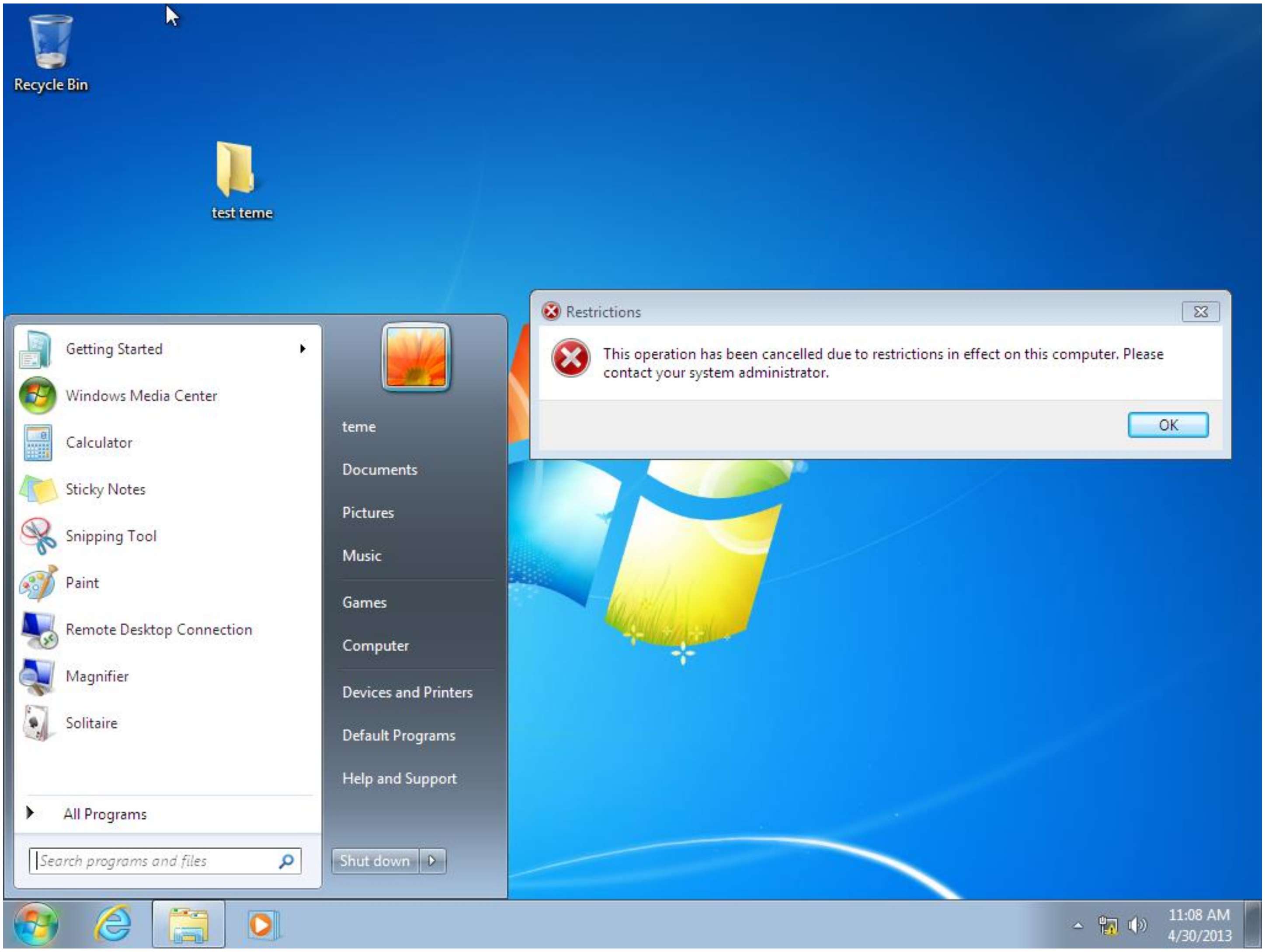
Disables all Control Panel programs.

This setting prevents Control.exe, the program file for Control Panel, from starting. As a result, users cannot start Control Panel or run any Control Panel items.

This setting also removes Control Panel from the Start menu. This setting also removes the Control Panel folder from Windows Explorer.

If users try to select a Control Panel item from the Properties item on a context menu, a message appears explaining that a setting prevents the action.

Therefore one of the user in this Demo OU (“teme”) has no access to the Control Panel :
Here is how ‘teme’s’ window look when he tries to open the control panel :



Restrictions

This operation has been cancelled due to restrictions in effect on this computer. Please contact your system administrator.

OK

Part VII

Conclusion

While working on this project there were a lot of problems faced. Some of which are:

1, getting a stable version: after trying the 4.0.X versions for a few time, I finally managed to work on the 4.0.5 version which is final released stable version (as of the time this manual is written).

2, DNS server: while testing the connectivity to the AD DC both the samba internal DNS and the Bind DNS were running so I uninstalled the Bind DNS and it solved it.

3, accessing the shares: while trying to access the shares I was using only the domain name for the path and this resulted in an “Element Not found Error” finally I discovered that I should use the path :

\\hostname.domainname

4, after the samba was installed I tried to install the dependency packages for samba4 again, this crashed the samba4 and was not able to make it work again. So I did a clean install of the operating system and the samba4. So I recommend to install the dependencies before compiling samba 4.

5, resolv.conf: after installing samba, every time I reboot the system the resolv.conf file was empty. So I edited the head file and it was stable after that. The file is located here:

/etc/resolvconf/resolv.conf.d/head

6, setting acl from the samba side was somehow impossible: since samba4 doesn’t use local users on the Linux side, you can’t use setfacl or getfacl. You have to set acl from the ‘samba-tool ntacl’ but since the man page for this is not available, it is easier to set the acl from the windows AD management side.

7, while roaming profiles: I used different names on the smb.conf file and the path from the windows side. One was profiles and the other was profile this created a confusion in the system and none of the data was being saved. It took a lot of my time trying to identify this simple mistake.