

## Joining your Ubuntu workstation to the Active Directory

---

One of the biggest problems when putting a Linux machine on the network has been that most large businesses are using Active Directory to authenticate their users and control the workstations. Now we have the ability to join our Linux machines to an active directory, this will assist in mainstreaming Linux as workstations, not only a server. This also allows seamless sharing of files and folders across the network without needing to create separate Samba users as we did last quarter. All steps below are assuming you are logged in through PuTTY as the user root

### Terms:

Name to use during setup	definition
ServerDC	Name of your Domain Controller
contosa.com	Active Directory
ServerDC	Domain Controller
contosa.com	Active Directory domain
192.168.9.100	Domain Controller address (windows)
contosa.com	Kerberos Realm
xxLinux (replace xx with your student number)	Computer name of the Ubuntu workstation
xxLinux.contosa.com	FQDN of the Ubuntu workstation
Serverdc.contoso.com	timeserver (NTP)
Serverdc.contoso.com	DNS Server

### Confirm Connectivity:

The first step will be to ensure our Active Directory Domain can see and hear our Ubuntu machine. Our DNS should be working properly and resolving names. The easiest way to complete this is by using the ping command from the Ubuntu PuTTY terminal, type in

```
root@16Linux:~# ping serverdc.contoso.com
PING SERVERDC.CONTOSO.COM (192.168.9.101) 56(84) bytes of data.
64 bytes from SERVERDC.CONTOSO.COM (192.168.9.101): icmp_seq=1 ttl=128 time=0.471 ms
64 bytes from SERVERDC.CONTOSO.COM (192.168.9.101): icmp_seq=2 ttl=128 time=0.430 ms
64 bytes from SERVERDC.CONTOSO.COM (192.168.9.101): icmp_seq=3 ttl=128 time=0.422 ms
64 bytes from SERVERDC.CONTOSO.COM (192.168.9.101): icmp_seq=4 ttl=128 time=0.373 ms

--- SERVERDC.CONTOSO.COM ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3009ms
rtt min/avg/max/mdev = 0.373/0.424/0.471/0.034 ms
root@16LINUX:~#
```

Connectivity failures when pinging are usually the result of a DNS server or client configuration error. Try using only the server name (serverDC) without contoso.com. If this succeeds, you can still move forward. Troubleshooting help:

1. Use the Windows Server 2008 server (serverDC at 192.168.9.100) for your DNS server. Ensure you can access the Internet (ping 134.39.47.9)
2. On the Ubuntu machine, point your DNS to the Windows Server 2008 DNS server by changing the /etc/resolv.conf file. Below is mine

```
#/etc/resolv.conf

search contoso.com.
nameserver 192.168.9.100
domain contoso.com
```

Resolve any DNS issues before moving forward. Remember to put in the periods when listed.

## Time Settings

Time is essential to Kerberos, which is what Active Directory uses to authenticate. To give us the best opportunity to join the network on the first try, we should sync the time between our Ubuntu and Windows machines. First ensure you have the time program, as well as an up to date system

```
root@16LINUX:~# apt-get install ntp
root@16LINUX:~# apt-get update
root@16LINUX:~# apt-get upgrade
```

Run the command ntpdate:

```
root@16LINUX:~# ntpdate serverdc
24 Apr 13:37:17 ntpdate[31603]: step time server 192.168.9.100 offset -1.736329 sec
```

If you run into an error stating that the NTP socket is in use, exiting, then run

```
root@16LINUX:~# /etc/init.d/ntp stop
* Stopping NTP server ntpd [ OK ]
root@16LINUX:~# ntpdate <yourservename> ex. # ntpdate server01
24 Apr 13:37:17 ntpdate[31603]: step time server 192.168.9.101 offset -1.736329 sec
```

## FQDN

Having a valid Fully Qualified Domain Name is imperative to Active Directory. We will edit the local hosts file of the Ubuntu machine in order to make certain that your FQDN is resolvable by DNS. Open the file `/etc/hosts` and add the following (of course using your proper naming convention).

```
127.0.0.1      localhost
127.0.1.1      16Linux.contoso.com contoso.com contoso
192.168.9.156  16Linux.contoso.com contoso.com contoso
192.168.9.100  serverdc.contoso.com contoso.com contoso
```

## Installing the software

In order to use the Kerberos authentication, you need to install `krb5-user` and `libpam-kerb5`. You will also need to install `samba` and `winbind` to make Ubuntu talk to the Active directory. At the PuTTY terminal, logged in as root, install the packages with the `apt-get` utility.

```
root@16LINUX:~# apt-get install samba winbind
root@16LINUX:~# apt-get install krb5-user libpam-krb5
```

Additional packages `krb5-config`, `libkrb53` and `libkadm55` will also be installed with the above commands. If the `krb5-config` installation presents a prompt for you to enter additional information, follow the guide below. Use uppercase when entering this information.

What are the Kerberos servers for your realm?

```
serverdc.CONTOSO.COM
```

What is the administrative server for your Kerberos realm?

```
serverdc.CONTOSO.COM
```

Ensure each package was successfully installed before moving on. If there are errors, try running the update for `apt-get` and then re-running the installs.

```
root@16LINUX:~# apt-get update
```

# Kerberos

Verify that your Kerberos file has been appropriately configured by opening the file `/etc/krb5.conf`. There is a lot of information in there that you do not need, but what is important is that you have the following (note – case is VERY important to Linux):

```
[logging]
    default = FILE10000:/var/log/krb5lib.log

[libdefaults]
    default_realm = CONTOSO.COM
    kdc_timesync = 1
    ccache_type = 4
    forwardable = true
    proxiable = true

[realms]
    CONTOSO.COM = {
        kdc = SERVERDC.CONTOSO.COM
        admin_server = SERVERDC.CONTOSO.COM
        default_domain = CONTOSO.COM
    }

[domain_realm]
    .contoso.com = CONTOSO.COM
    contoso.com = CONTOSO.COM
```

In my file, I deleted all the other information listed in here.

## Testing 1.2.3.....

Now that Kerberos is installed and configured, test to ensure you are talking to your domain controller and have the authority to be granted a Kerberos ticket. You will use the command `kinit` to get a ticket, the command `klist` to view the ticket, the command `kdestroy` to remove the ticket. You will use an account that is only available at your Windows Server 2008 Active Directory, use the account `studentxx` (replace the `xx` with your student number). The point is to allow authentication between the Ubuntu box and the AD.

```
root@16LINUX:~# kinit student01
Password for student01@CONTOSO.COM:
```

```
root@16Linux:~# klist
Ticket cache: FILE:/tmp/krb5cc_o
Default principal: student01@CONTOSO.COM
Valid starting Expires Service principal
04/27/10 12:12:40 04/27/10 22:12:39 krbtgt/CONTOSO.COM@CONTOSO.COM
renew until 04/28/10 12:12:40
root@16Linux:~#
```

If you have a ticket, you know that Kerberos is installed and configured correctly. You can release the ticket with the command **kdestroy** if you choose.

## Join AD domain

**\*\* warning - do not start this portion unless you can complete through the PAM Section. If you log out in the midst of this operation, you will not be able to log back in without rebooting into "rescue mode" and editing the pam.d files with vi. \*\***

### Required software

You need to install the **winbind** and **samba** packages. The packages **smbfs** and **smbclient** are useful for mounting network shares and coping files. The package *smbfs* is optional, but includes useful client utilities, including the **smbmount** command. Also useful is the *smbclient* package, which includes an FTP-like client for SMB shares. We have only installed samba and winbind. That is all that is necessary for our purposes.

### Join

The first step in joining the Active Directory domain is to edit `/etc/samba/smb.conf` file. This file has lots of "stuff" in it. You will need to ensure that all of the following is listed properly inside the `[global]` section.

```
#===== Global Settings =====
```

```
[global]

## Browsing/Identification ###
    security = ads
    realm = CONTOSO.COM
    password server = 192.168.9.100

# Change this to the workgroup/NT-domain name your Samba server will
part of
    workgroup = CONTOSO

#
    winbind separator = +
    idmap uid = 10000-20000
    idmap gid = 10000-20000
    winbind enum users = yes
    winbind enum groups = yes
    template homedir = /home/%D/%U
    template shell = /bin/bash
    client use spnego = yes
    client ntlmv2 auth = yes
    encrypt passwords = yes
    winbind use default domain = yes
    restrict anonymous = 2
    users = @"Domain Users"
```

The "winbind use default domain" parameter is useful in single-domain enterprises and makes winbind assume that all user authentications should be performed in the domain to which winbind is joined.

Be sure to restart the Samba and Winbind services after changing the `/etc/samba/smb.conf` file. You need to perform the following tasks in order:

```
root@16LINUX:~# /etc/init.d/winbind stop
root@16LINUX:~# /etc/init.d/samba restart
root@16LINUX:~# /etc/init.d/winbind start
```

Repeat the above tasks if you ever need to make changes to the Samba or Winbind configuration files.

Request a valid Kerberos TGT for an account using **kinit**, which is allowed to join a workstation into the AD domain. Use an account that has Domain Admin privileges on the Active Directory Domain. To save complication, I have created an account in the Active Directory called root with the password of `cislsTheBest!` Use it to join the directory with the `net ads join` command.

```
root@16LINUX:~# kinit root
Password for root@CONTOSO.COM:
```

```
root@16LINUX:~# net ads join
Using short domain name -- CONTOSO.COM
Joined '16Linux to realm 'CONTOSO.COM'
```

## Testing

At your Windows Server 2008 server, check to see if your Ubuntu machine is displayed under Active Directory Users and Computers. It should be located under the computer section. If there is a red X next to it, there is some trouble, and you need to go back to these steps to see if there is something listed incorrectly in your configuration files.

## Setup Authentication

**We need to configure the nsswitch configuration file.**

Edit the file: `/etc/nsswitch.conf` to add the winbind to our authentication as well as add hosts: files dns to avoid the settings in `/etc/hosts` to be ignored.

```
passwd:      compat winbind
group:       compat winbind
shadow:      compat

hosts:       files dns
# mdns4_minimal [NOTFOUND=return] dns mdns4
networks:    files

protocols:   db files
services:    db files
ethers:      db files
rpc:         db files

netgroup:    nis
```

Be sure to restart the Samba and Winbind services after changing configuration file. You need to perform the following tasks in order:

```
root@16LINUX:~# /etc/init.d/winbind stop
root@16LINUX:~# /etc/init.d/samba restart
root@16LINUX:~# /etc/init.d/winbind start
```

## Testing

At the Ubuntu machine, we can see if we are getting information from the Window Active Directory by using the following commands:

```
root@16Linux:~# wbinfo -u
16LINUX\dunn
16LINUX\root
administrator
guest
krbtgt
studentg1
studentg2
studentg3
domain12$
studento1
studento2
studento3
studento4
root@16Linux:~# wbinfo -g
domain computers
domain controllers
schema admins
enterprise admins
cert publishers
domain admins
domain users
domain guests
group policy creator owners
ras and ias servers
allowed rodc password replication group
denied rodc password replication group
read-only domain controllers
enterprise read-only domain controllers
dnsadmins
dnsupdateproxy
dhcp users
dhcp administrators
students
root@16LINUX:~#
```

I can see the *Active Directory* groups and users from the Windows Server 2008 domain controller above. We have joined the Active directory. Next is to allow us to use our authentication from AD on our Ubuntu boxes.

## Testing again

Check Winbind nsswitch module with **getent**.

```
root@16Linux:~# getent passwd
root:x:0:0:root:/root:/bin/bash
```



```

... (lots of stuff)
administrator:*.10000:10000:Administrator:/home/CONTOSO/administrator:/bin/bash
guest:*.10001:10001:Guest:/home/CONTOSO/guest:/bin/bash
krbtgt:*.10002:10000:krbtgt:/home/CONTOSO/krbtgt:/bin/bash
ServerDC:*.10003:10000:ServerDC:/home/CONTOSO/ServerDC:/bin/bash
doris:*.10004:10000:Doris:/home/CONTOSO/doris:/bin/bash
root@16LINUX:~# getent group
root:x:0:
daemon:x:1:
bin:x:2:
... (lots more stuff)
domain admins:x:10006:ServerDC,administrator
domain users:x:10000:
domain guests:x:10001:
group policy creator owners:x:10007:ServerDC,administrator
dnsupdateproxy:x:10008:
BUILTIN\administrators:x:10010:16LINUX\root,ServerDC,administrator
BUILTIN\users:x:10011:

```

## PAM

With this config you can access the workstation with local accounts or with domain accounts. On the first login of a domain user a home directory will be created. This PAM configuration assumes that the system will be used primarily with domain accounts. If the opposite is true (i.e., the system will be used primarily with local accounts), the order of *pam\_winbind.so* and *pam\_unix.so* should be reversed. When used with local accounts, the configuration shown here will result in a failed authentication to the Windows/Samba DC for each login and sudo use. This can litter the DC's event log. Likewise, if local accounts are checked first, the */var/log/auth.log* will be littered with failed logon attempts each time a domain account is accessed.

This PAM configuration does not acquire a Kerberos TGT at login. To acquire a ticket, use *kinit* after logging in, and consider using *kdestroy* in a logout script.

Edit the file: */etc/pam.d/common-account*

```

account sufficient pam_winbind.so
account required pam_unix.so

```

Edit the file: */etc/pam.d/common-auth*

```

auth sufficient pam_winbind.so
auth sufficient pam_unix.so nullok_secure use_first_pass
auth required pam_deny.so

```

Edit the file: */etc/pam.d/common-session*

```

session required pam_unix.so
session required pam_mkhomedir.so umask=0022 skel=/etc/skel

```

Edit the file: */etc/pam.d/sudo*

```
auth sufficient pam_winbind.so
auth sufficient pam_unix.so use_first_pass
auth required pam_denied.so
```

```
@include common-account
```

## Final configuration

Each domain needs a directory in /home/.

```
root@16LINUX:~# mkdir /home/CONTOSO
```

**Log in through PuTTY with the domain account prior to logging in through the graphical desktop. This will create the home directory on the Linux machine.**

## One last thing

If you want to be able to use an active directory account, to manage your Ubuntu box, you need to add it to the sudoers file. I suggest creating a group in active directory called LinuxAdmins and adding any users you would like to have admin rights on the Linux boxes there. Make the Domain Group a sudoer in your Ubuntu, by editing the file /etc/sudoers (using the command 'visudo')

```
root@16LINUX:~# visudo
```

A very strange looking editor will open. Add the following line to the end of the file

```
%LinuxAdmins    ALL=(ALL) ALL
```

Press Ctrl-X to end, answer yes, enter to confirm file location. Then at the terminal prompt, type Q to answer the question Now What?

LinuxAdmins is the group from your active directory. Be aware that spaces in the group name are not allowed.

## Usage

Because we included "winbind use default domain" in the *smb.conf*, we may log in using only our Active Directory username.

```
login as: student01
student01@192.168.9.156's password:
Linux 16Linux 2.6.31-20-generic-pae #58-Ubuntu SMP Fri Mar 12 06:25:51 UTC 2010 i686

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/

System information as of Tue Apr 27 12:26:30 PDT 2010

System load: 0.0      Memory usage: 39%  Processes:   150
Usage of /: 10.5% of 28.27GB  Swap usage:  0%   Users logged in: 2



Graph this data and manage this system at https://landscape.canonical.com/

Last login: Tue Apr 27 11:45:21 2010 from 192.168.9.61
student01@16Linux:~$
```

## Resources

<https://help.ubuntu.com/community/ActiveDirectoryWinbindHowto>  
[http://wiki.randompage.org/index.php/Using\\_Samba\\_on\\_Debian\\_Linux\\_to\\_authenticate\\_against\\_Active\\_Directory](http://wiki.randompage.org/index.php/Using_Samba_on_Debian_Linux_to_authenticate_against_Active_Directory)  [Using Samba on Debian Linux to authenticate against Active Directory](http://wiki.randompage.org/index.php/Using_Samba_on_Debian_Linux_to_authenticate_against_Active_Directory) on randompage.org.  
[http://wiki.samba.org/index.php/Samba\\_&\\_Active\\_Directory](http://wiki.samba.org/index.php/Samba_&_Active_Directory)

### Automated Methods (oops – didn't I tell you about this?)

The <https://help.ubuntu.com/community/ActiveDirectoryWinbind-SADMS>  [SADMS](https://help.ubuntu.com/community/ActiveDirectoryWinbind-SADMS) package allows for automated joining to Active Directory through a GUI interface.  
<http://sadms.sourceforge.net/>  <http://sadms.sourceforge.net/>