

Join your Ubuntu Server to the Active Directory Domain

Likewise Open simplifies the necessary configuration needed to authenticate a Linux machine to an Active Directory domain. Based on **winbind**, the **likewise-open** package takes the pain out of integrating Ubuntu authentication into an existing Windows network.

Installation

There are two ways to use Likewise Open, **likewise-open** the command line utility and **likewise-open-gui**. This section focuses on the command line utility.

To install the **likewise-open** package, open a terminal prompt and enter:

```
sudo apt-get install likewise-open
```

Joining a Domain

The main executable file of the **likewise-open** package is `/usr/bin/domainjoin-cli`, which is used to join your computer to the domain. Before you join a domain you will need to make sure you have:

- Access to an Active Directory user with appropriate rights to join the domain.
- The *Fully Qualified Domain Name* (FQDN) of the domain you want to join. If your AD domain does not match a valid domain such as `example.com`, it is likely that it has the form of `domainname.local`.
- Remove DNS services from the Linux server with the command

```
apt-get remove bind9
```

Then restart the server

```
shutdown -r now
```

- DNS for the domain setup properly. In a production AD environment this should be the case. Proper Microsoft DNS is needed so that client workstations can determine the Active Directory domain is available. For this operation, the nameserver must be listed as the Windows Server, so edit the file `/etc/resolv.conf` to remove any other nameserver. It should look somewhat like the following, substituting your domain and IP information

```
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by
resolvconf(8)
#       DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
search dunn.local
nameserver 192.168.9.90
```

If you made changes to this file, restart the networking with the following command before proceeding

```
/etc/init.d/networking restart
```

To join a domain, from a terminal prompt enter:

```
sudo domainjoin-cli join example.com Administrator
```



Replace *example.com* with your domain name, and *Administrator* with the appropriate Enterprise administrator user name.

You will then be prompted for the user's password. If all goes well a *SUCCESS* message should be printed to the console.



After joining the domain, it is necessary to reboot before attempting to authenticate against the domain.

After successfully joining an Ubuntu machine to an Active Directory domain you can authenticate using any valid AD user. To login you will need to enter the user name as 'domain\username'. For example to ssh (or PuTTY) to a server joined to the domain enter:

example\username, so my putty session would look like:

```
login as: dunnent\doris
Last login: Sun Apr 24 22:50:04 2011 from 192.168.10.30
DUNNENT\doris@DunnUbuntu:~$
```



If configuring a Desktop the user name will need to be prefixed with domain\ in the graphical logon as well.

Manage how Ubuntu interacts with the windows environment by manipulating the samba configuration file `/etc/samba/smbd.conf`. Update the following areas to reflect your domain structure.

```
##### Global Settings #####
[global]

## Browsing/Identification ##

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

##### Domains #####

# Is this machine able to authenticate users. Both PDC and BDC
# must have this setting enabled. If you are the BDC you must
# change the 'domain master' setting to no
#
domain logons = yes
#
# The following setting only takes effect if 'domain logons' is set
```

```

# It specifies the location of the user's profile directory
# from the client point of view)
# The following requires a [profiles] share to be setup on the
# samba server (see below)
; logon path = \\%N\profiles\%U
# Another common choice is storing the profile in the user's home directory
# (this is Samba's default)
  logon path = \\%N\%U\profile

# The following setting only takes effect if 'domain logons' is set
# It specifies the location of a user's home directory (from the client
# point of view)
  logon drive = H:
  logon home = \\%N\%U

# The following setting only takes effect if 'domain logons' is set
# It specifies the script to run during logon. The script must be stored
# in the [netlogon] share
# NOTE: Must be store in 'DOS' file format convention
; logon script = logon.cmd

# This allows Unix users to be created on the domain controller via the SAMR
# RPC pipe. The example command creates a user account with a disabled Unix
# password; please adapt to your needs
; add user script = /usr/sbin/adduser --quiet --disabled-password --gecos "" %u

# This allows machine accounts to be created on the domain controller via the
# SAMR RPC pipe.
# The following assumes a "machines" group exists on the system
add machine script = /usr/sbin/useradd -g machines -c "%u machine account" -d /var/lib/samba -s /bin/false %u

# This allows Unix groups to be created on the domain controller via the SAMR
# RPC pipe.
add group script = /usr/sbin/addgroup --force-badname %g

```

Read through the configuration file and make changes you determine to be appropriate on your domain.

The **domainjoin-cli** utility can also be used to leave the domain. From a terminal:

```
sudo domainjoin-cli leave
```

Troubleshooting

- When I attempted this lab, I received the error: **Lsass Error [code 0x00080047]**
I uninstalled and then reinstalled Likewise-open, rebooted and on the next attempt to join the domain it worked.
- If the client has trouble joining the domain, double check that the Microsoft DNS is listed first in `/etc/resolv.conf`. For example:

```
nameserver 192.168.10.90
```

- For more information when joining a domain, use the `--loglevel verbose` or `--advanced` option of the **domainjoin-cli** utility:

```
sudo domainjoin-cli --loglevel verbose join example.com Administrator
```

- If an Active Directory user has trouble logging in, check the `/var/log/auth.log` for details.
- When joining an Ubuntu Desktop workstation to a domain, you may need to edit `/etc/nsswitch.conf` if your AD domain uses the `.local` syntax. In order to join the domain the `"mdns4"` entry should be removed from the `hosts` option. For example:

```
hosts: files mdns4_minimal [NOTFOUND=return] dns mdns4
```

Change the above to:

```
hosts: files dns [NOTFOUND=return]
```

Then restart networking by entering:

```
sudo /etc/init.d/networking restart
```

You should now be able to join the Active Directory domain.

Reference: <https://help.ubuntu.com/10.04/serverguide/C/likewise-open.html>
<http://www.linux.com/learn/tutorials/336477-how-to-join-a-ubuntu-machine-to-a-windows-domain>

In your lab journal write a paragraph describing what this means in a business environment. How would the simple integration of Ubuntu desktops impact the corporate network?