

Join Samba 3 to Your Active Directory Domain

By Carla Schroder

A popular thing to do with Samba these days is to join a Samba 3 host to a Windows Active Directory domain. You may freely set up any number of Samba servers in a Windows network without joining them to the domain. The advantages of domain membership are central management and authentication, and single sign-on. Using Winbind allows Linux clients to log on to the AD domain without requiring local Linux system accounts, which is a lovely time- and hassle-saver.

Presumably you already have a functioning Active Directory domain, and know how to run it. AD is very dependent on DNS (domain name system) so I'll assume your DNS house is also in order. On your Linux box you'll need Samba 3, version 3.0.8 or newer. Plus MIT Kerberos 5, version 1.3.1 or newer, and OpenLDAP. (The Samba documentation states that Heimdal Kerberos, version 0.6.3 or newer, also works. The examples in this article use MIT Kerberos.) Debian users need the *krb5-user*, *krb5-config*, *krb5-doc*, and *libkrb53* packages. Red Hat and Fedora users need the *krb5* and *krb5-client* RPMs.

First you should verify that your Samba installation has been compiled to support Kerberos, LDAP, Active Directory, and Winbind. Most likely it has, but you need to make sure. The **smbd** command has a switch for printing build information. You will see a lot more lines of output than are shown here:

```
root@windbag:/usr/sbin# cd /usr/sbin
root@windbag:/usr/sbin# smbd -b | grep LDAP
HAVE_LDAP_H
HAVE_LDAP
HAVE_LDAP_DOMAIN2HOSTLIST
...
root@windbag:/usr/sbin# smbd -b | grep KRB
HAVE_KRB5_H
HAVE_ADDRTYPE_IN_KRB5_ADDRESS
HAVE_KRB5
...
root@windbag:/usr/sbin# smbd -b | grep ADS
WITH_ADS
WITH_ADS
root@windbag:/usr/sbin# smbd -b | grep WINBIND
WITH_WINBIND
WITH_WINBIND
```

If you are in the unfortunate position of missing any of these, which will be indicated by a blank line, you need to recompile Samba. See Chapter 37 of the The Official Samba-3 HOWTO and Reference Guide.

Configure and Test Kerberos

Let's say our Active Directory domain server is *bigserver.domain.net*, and the Samba server is named *samba1*. This is the absolute minimum Kerberos configuration file, */etc/krb5.conf*, for connecting to this domain:

```
'libdefaults'
default_realm = DOMAIN.NET
```

Join Samba 3 to Your Active Directory Domain

By Carla Schroder

```
'realms' DOMAIN.NET = {  
kdc = bigserver.domain.net  
}  
'domain_realms'  
.kerberos.server = DOMAIN.NET
```

Use uppercase where it shows. Now try to connect, and mind your cases:

```
# kinit Administrator@DOMAIN.NET  
Password for Administrator@DOMAIN.NET
```

Configure /etc/hosts

Even if your DNS servers are perfect in every way, it is a good idea to add important servers to your local `/etc/hosts` file. It speeds up lookups and provides a fallback in case the DNS servers go down:

```
192.168.10.5 bigserver.domain.net bigserver
```

Configure Samba

This example `smb.conf` shows a basic setup for a printer server and home shares. Shares are configured in the usual manner, only the *global* section changes when you join to an AD domain.

```
# Global parameters  
'global'  
workgroup = BIGSERVER  
realm = DOMAIN.NET  
preferred master = no  
server string = Samba file and print server  
security = ADS  
encrypt passwords = yes  
log level = 3  
log file = /var/log/samba/%m  
max log size = 50  
winbind separator = +  
printcap name = cups  
printing = cups  
idmap uid = 10000-20000  
idmap gid = 10000-20000  
  
'homes'  
comment = Home Directories  
valid users = %S  
read only = No  
browseable = No  
  
'printers'  
comment = All Printers  
browseable = no  
printable = yes  
guest ok = yes
```

Join Samba 3 to Your Active Directory Domain

By Carla Schroder

The workgroup is the name of your AD domain. Server string is a comment describing the server, make this anything you want. Log level runs from 0, for no logging, to 10, extreme logging. See **man smb.conf** for the rest.

Save your changes and run

```
$ testparm
```

This checks *smb.conf* for syntax errors. Any errors must be corrected before going ahead. Then start up Samba:

```
# /etc/init.d/samba start
```

Finally, join your Samba machine to Active Directory:

```
# net ads join -U Administrator
Administrator's password:
Joined 'SAMBA1' to realm 'DOMAIN.NET.'
```

Hurrah! Success. The Samba box will now appear as a machine account under "Computers" in your AD console. Now stop Samba until the final steps are completed.

Enabling Windbind

Debian users may need to install the *winbind* package separately. RPM users will find it in the *samba-common* RPM. First, edit */etc/nsswitch.conf*. The first three lines are the most important; the others vary according to your system:

passwd:	compat winbind
group:	compat winbind
shadow:	compat
hosts:	files dns wins
networks:	files dns
protocols:	db files
services:	db files
ethers:	db files
rpc:	db files

Save your changes, and fire up windbind and Samba:

```
# winbind
# /etc/init.d/samba start
```

Now verify that windbind is working. These commands pull lists of users and groups from the AD domain controller:

```
# wbinfo -u
BIGSERVER+Administrator
BIGSERVER+Guest
```

Join Samba 3 to Your Active Directory Domain

By Carla Schroder

```
BIGSERVER+cschroder  
BIGSERVER+mhall
```

```
# wbinfo -g  
BIGSERVER+Domain Computers  
BIGSERVER+Domain Admins  
BIGSERVER+Domain Guests  
BIGSERVER+Domain Users
```

This command verifies that logins and passwords are coming from the AD server, and not the local machine:

```
# getent passwd  
BIGSERVER+cschroder:x:1000:1000:,,,:/home/BIGSERVER/cschroder:/bin/bash
```

If winbind is not working and local authentication is still active, they will not have the BIGSERVER+ prefix. Finally, as root run **net ads info** to display the AD server information.

Troubleshooting

If you've gotten this far and everything works, your Samba server is now a fully-fledged member of your Active Directory domain, and can be managed like any other AD object. A nice bonus is you may have local Linux accounts on the Samba box that are not visible in Active Directory; which means your Samba admins can SSH directly into the Samba server for admin chores, and not have to fuss with AD roadblocks.

A good troubleshooting guide is chapter 9 of "Samba-3 by Example" (Adding UNIX/LINUX Servers and Clients). Also refer to chapter 12 (Identity Mapping) of "The Official Samba-3 HOWTO and Reference Guide" to learn about winbind in greater depth.

Resources

- Many good Samba books and howtos here.
- Network Installation of Windows Printers from Samba tells how to automatically install Windows printers from Samba.
- Chapter 23 of the Linux Cookbook covers Samba basics in depth, including printing and file sharing, and connecting from both Windows and Linux clients.