http://www.mandrakeuser.org/docs/connect/csamba6.html

DocIndex

Search

Main - DocIndex - Connectivity

SAMBA VI: As a Domain Controller

Related Resources:

Samba: An Introduction
Just what is SMB?
Samba HOWTO Collection
Using SAMBA
`man smb.conf`

Revision / Modified: Dec. 18, 2001
Author: Buchan Milne

This section contains information on the latest features available in Samba, which allow you get the most out of your linux server, and allow you to integrate it into a large Windows network, or to form the basis of a Windows/Linux network.

A "Windows NT Domain" is a workgroup of Windows computers that has a Windows (or linux, as you will see below) Server which provides authentication services to the rest of the machines in the network. The domain controller stores information relating to the users and computers in the domain, including their Relative Security IDs (similar to uid's in unix) and their domain passwords. When deciding whether to grant access to a specific user, client machines will query the domain controller (if a local account does not exist), and if the supplied information is correct, the domain controller will return a token to the client, allowing the user access.

As with a workgroup, the name of the domain a linux/samba machine is a member of is determined by the `workgroup` paramater in `smb.conf`

Running A Linux Primary Domain Controller

Since early releases of Samba 2, Samba has been able to provide limited domain controlling features, allowing you to get many (and an ever increasing number) of the features for which you would normally need a Windows (Windows NT 4 or Windows 2000) Server. Since Samba-2.2.0, Samba has also been able to be a domain controller for Windows 2000 clients. The features available include:

- Domain accounts
- Network profiles
- Login scripts (highly customizable)
- Defining Domain Admins (and Domain Guests in Samba>= 2.2.2
- User and computer policies
- Providing domain authentication services for certain Windows servers such as Microsoft SQL Server

Why would you want to use Samba as a Domain Controller? Firstly you don't need to buy copies of Windows Server, but even more substantial, you don't need client access licenses per machine in your Domain. Also, by using Samba on Unix instead of a Windows Domain Controller, you can cater to both Windows and Unix desktop machines or member servers.

Features not implemented yet

Unfortunately, since Microsoft publishes very little information on how they implement features, the samba team must spend a lot of time reverse-engineering Windows networking. As such the following features are either not implemented at all or under development:

- Domain Groups
- Integration with Microsoft Exchange Server (this is however possible with Samba-TNG, which forked from Samba about a year ago).
- PDC-BDC relationships with Windows NT or Samba, and Active Directory replication with Windows 2000.
- Domain Trusts (apparently this might also be possible with Samba-TNG).

Configuration options required

To control a windows domain, you need the following entries in your 'smb.conf' file:

```
domain logons = yes
security = user
os level = 33
```

and a valid `[netlogon]` section to define the netlogon share.

The default 'smb.conf' file that ships with Mandrake 8.1 has many of these options commented out with recommended values, so I will not discuss them much further. Note that by using 'ntlogon', you can easily customize login scripts per

user, per machine, per group, per operating system simultaneously. Sample configuration for this is also included.

You will need to reload Samba for the changes to take effect:

```
service smb reload
```

Joining Machines To The Domain

To access certain features of a domain (for example authentication of network clients and authentication of users at logon), each machine of the domain needs to be set to consult the domain controllers of the domain. For full domain membership, machines need to have an account made for them in the domain.

Windows 9x

Windows 9x machines do not implement full domain membership, so joining them to the domain is the easiest. Navigate to the Network section of the control panel (Start ->Settings->Control Panel->Network), select the Configuration tab, highlight "Client for Microsoft Networks" and click the Properties button. Check "Log onto Windows NT Domain", and enter the domain name in the text field. Click all the OK buttons and reboot!

Windows NT 4

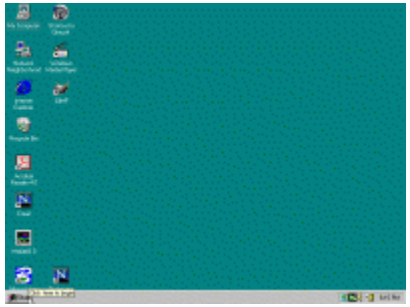
Windows NT machines have a full domain implementation, and better default security. Each machine keeps its own password, which controls which machines may authenticate from the domain. Thus each machine needs its own entry in the 'smbpasswd' file. At present, Samba needs to have a Unix account for every entry in the 'smbpasswd' file, so this means that each computer needs a Unix account on the Domain Controller. Machine accounts are differentiated from user accounts by appending a $ to the end of the machine's name. For Windows NT clients, you can create these accounts manually.*See the Windows 2000 section for how you can make this simpler!*

To make a domain machine account, issue the following commands on the Domain Controller as 'root':

```
useradd -d /dev/null -g machines -c 'Machine Account' -s /bin/false -M <NETBIOS_NAME>$
smbpasswd -am <NETBIOS_NAME>
```

You can customize this, by specifying the UID for the account, or changing the group. The group "machines", however, is created during Samba installation for this purpose.

To join the domain, follow the steps below:



- Start ->Settings->Control Panel->Network
- Select the identification tab, click the "change" button and enter the domain name and computer name.
- Click "OK"
- After a short pause (0-10 seconds), you should be greeted by a "Welcome to <DOMAIN>" message and asked to reboot.
- Log in on a domain account

Warning, larger image goes offsite to http://ranger.dnsalias.com, a slow machine somewhere in Africa.

Windows 2000

Windows 2000 is slightly different to Windows NT. If you joined a Windows NT workstation to the network as above, you may have noted a check-box "Make an account for this machine in the domain", which we didn't use. This allows you (after some more configuration) to have machine accounts made on the fly, and is the only way you can join a Windows 2000 machine to a domain.

At present the only user that can create computer accounts automatically is "root". This means you must make an 'smbpasswd' (as 'root') for 'root' with:

```
smbpasswd -a
```

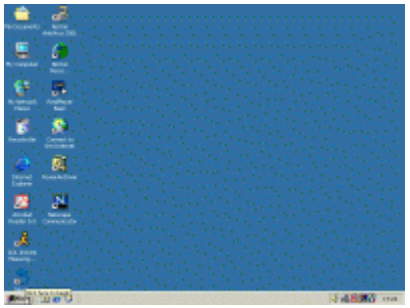
It is suggested that you use a different password than the real Unix password for "root" for security reasons.

To be able to join a Windows 2000 machine to the domain (or create accounts on the fly for Windows NT), you need the following entries in your 'smb.conf':

```
add user script = /usr/sbin/useradd -d /dev/null -g machines -c 'Machine Account' -s /bin/false -M
%u
```

Note the absence of the $ in this script, Samba automatically adds the $ for you when it is configured as a domain logon server.

To actually join the machine to the domain, follow the steps below:



- Start ->Settings->Network and Dial-up Connections
- Click the "Advanced" menu, select "Identification"+
- Click the "Properties" button, enter your domain and computer name, and click "OK"
- You will now be prompted for a user account with rights to join a machine to the domain, use "root" as the user name, and the password you entered above.
- After a short pause (10-30 seconds), you should be greeted by a

"Welcome to <DOMAIN>" message and asked to reboot.

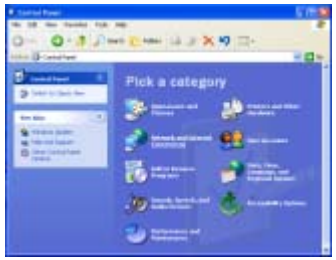
- Log in on a domain account

Warning, larger image goes offsite to http://ranger.dnsalias.com, a slow machine somewhere in Africa.

Windows XP

As of Samba-2.2.2 Windows XP is supported as a domain member, after applying this change to the registry on Windows XP boxes. If you have set your Samba PDC up to allow Windows 2000 to join, it should work.

To join the domain, follow the steps below:



Start->Settings->Control

Click "Network Connections"

Select "Advanced" ->

Panel. Click "Network and Internet Connections"

"Network Identification"

Click the "Change" button

Select the "Domain" button, and enter your domain name

Enter "root" and root's smbpasswd

Welcome to your domain

Warning, larger images go offsite to http://ranger.dnsalias.com, a slow machine somewhere in Africa.

Making Your Life Easier

There are some features of Windows networking which make life as a Windows Admin bearable, and allow you to get some of the functionality a decent Unix-only network would provide. The three easy ones to implement are Network profiles, home directories and login scripts. Computer and User policies can also be applied, but that is left as an exercise. *Hint: See the Samba-HOWTO-Collection for more info*.

Network Profiles and Home Directories

Network profiles are similar to the dot-files in your home directory, allowing you to keep you desktop and application settings between machines joined to a domain. Note that the entire contents of the profile is copied across the network at logon time, so you should take care that the profile does not get too large. Also, Windows NT has been known to corrupt profiles, so care is suggested *Hint: never choose "Use local profile" under Windows NT*

The home directory is often made available and can be set to be automatically mapped by Windows NT and Windows 2000 using the `logon path` and `logon drive` configuration entries as shown below.

```
logon path = <UNC>          #Path where windows NT stores user profiles
```

```
logon home = <UNC>          #Path where windows 9x stores user profiles
logon drive = <Drive_name>:     #The drive name mapped to the share section of logon path
```

Login Scripts

Login scripts are a powerful way of ensuring that certain things happen on your client machines when users log in. The scripts are standard DOS-type batch scripts, and are typically used to:

- Map network drives to shares
- Set registry entries
- Copy configuration files
- Perform computer maintenance

The login script is defined by the following entry in 'smb.conf':

```
logon script = <FILE_NAME>
```

Where <FILE_NAME> is a relative path to a file accessible in the `[netlogon]` share. <FILE_NAME> can take the standard Samba macros such as %U (user), %m (Client Netbios Name), %G (primary group of %U), which makes it relatively easy to customize the scripts.

Another method of customizing the login scripts is by using the 'ntlogon' utility, which processes a configuration file, and then generates a batch file based on the user, group, computer, and operating system of the client machine. Be aware that this requires ntlogon to be run as root! This can be accomplished with the following entry for `login script`:

```
logon script = %U.bat
```

and the following entries in the definition of the `[netlogon]` share

```
root preexec = /usr/bin/ntlogon -u %U -g %G -o %a -d /var/lib/samba/netlogon \
        && chmod 644 /var/lib/samba/netlogon/%U.bat;
root postexec = rm -f /var/lib/samba/netlogon/%U.bat
```

Domain Groups

There is very limited support for domain groups in Samba, only sufficient to be able to run a domain. The `domain admin group` parameter specifies users who will have domain admin rights. Domain Admin rights include Local Admin rights on every machine in the domain (and should include the ability to join machines to the domain, but not in this version of Samba). The argument is a space-separated list of user names or group names (groupnames must have an @ sign prefixed). For example:

```
domain admin group = <USER1> <USER2> @<GROUP>
```

Going Enterprise!

Although Samba does not support Domain Trusts at the moment, it is possible (if you are using only Samba PDCs) to create an environment which would appear use Domain Trusts. By implementing a Lightweight Directory Access Protocol (LDAP) server, you can provide consistent user names, UIDs, GIDs, and group memberships across many different Unix machines. It is also possible to export and import the smbpasswd's Samba uses to/from LDAP (via Perl scripts which can be run as cron jobs). All the Domain Controllers can then update the smbpasswd's from the LDAP server. For WAN setups, you can use LDAP's replication protocol to replicate the directory between locations, and run Domain Controllers on either side.

In future, Samba will be able directly store its passwords in LDAP.

section index top

Legal: All texts on this site are covered by the GNU Free Documentation License. Standard disclaimers of warranty apply. Copyright LSTB (Tom Berger) and Mandrakesoft 1999-2002.