Samba AD Domain Controller

Active Directory (AD) Domain Controller (DC) is what we need in order to create a central login (authentication) server. We can have that by using samba - a software that implements SMB/CIFS protocol, which is used by all DOS and Windows versions.

This is my personal note on how to create a central login server to be used in FTK-E labs with computer facilities. I'll be using Slackware for this, but any OS that runs samba should be able to achieve the same thing. I started experimenting this on FreeBSD.

Since samba is available in the default Slackware installation, I'll jump straight to creating a samba AD DC.

Create a fixed-IP server machine

As with any server machine, we need a fixed IP assigned to the target machine.

- on Slackware, edit `/etc/rc.d/rc.inet1.conf` (for those using rc.networkmanager, disable that)
  - do not forget to assign gateway here!
- also, set a domain and nameserver in `/etc/resolv.conf`
  - actually, we only need nameserver? (i use google's)
- add host information in `/etc/hosts`

Create new Windows Domain (Provisioning?)

- `samba-tool domain provision –use-rfc2307 –interactive`
  - obviously, this process is interactive - need a few info but should be familiar
  - i used: google's nameserver as forwarder, my uni's domain but with my own sub-domain
- `ln -sf /var/db/samba4/private/krb5.conf /etc/`
  - OR, copy if you want to keep a 'pristine' copy of the 'original'

Start samba

- we need to execute `samba` (not `smbd`)
  - `/etc/rc.d/rc.samba` actually executes `smbd` and `nmbd`
  - so, best thing to do is add `samba` (with full path) to `rc.local`?
  - simply type `samba` as root to start
- to check if it is running, type `smbclient -L localhost -U%`
- to check authentication,

```
smbclient //localhost/netlogon -UAdministrator -c 'ls'
```

- to check DNS and stuffs,

```
host -t SRV _ldap._tcp.<domain-name>
host -t SRV _kerberos._udp.<domain-name>
host -t A <server-name>.<domain-name>
```

Management

- to remove administrator account expiry

```
samba-tool user setexpiry administrator --noexpiry
```

- to list user accounts,

```
samba-tool user list
```

- to create user account,

```
samba-tool user add [username] [password]
```

On Windows Client

- point DNS to samba machine
- go to domain/workgroup settings and enter the previously set domain name
    - reboot and select 'other user' from the newly set domain
- get Remote Server Administration Tool (RSAT) to manage on Windows machine
    - i use windows 8, for example, so the RSAT tool is here

This works... but still trying to get folder redirection (@remote profile?) to work. At the moment (20160903), all stuff will be deleted once the user logoff. Perfect for most cases, but we do not want the students to lose their files :(Refer this.

From:
http://azman.my1matrix.cc/ - **Azman @MY1**

Permanent link:
http://azman.my1matrix.cc/doku.php?id=notes:samba_dc

Last update: **2026/02/08 03:46**