# Samba4 as Active Directory Domain Controller

After complete the Requeriments and choose the way to install Samba4, you should provisioned Samba4 with with de role of Domain Controller.

The provisioning creates a basic database, and is used when you are configuring your first Samba DC in its own domain. The provision step must be run as a user with permission to write to the install directory. Otherwise you're getting permission denied errors.

*For the rest of this HowTo we assume that:*

```
Installation Directory: /usr/local/samba/ (per default, if you use SerNet
pacakages isn't the same!)
Server Hostname:        redtic-ad1
DNS Domain Name:        redtic.uclv.cu (This will also be your realm)
NT4 Domain Name:        redtic
IP Address:             10.12.112.84
Server Role:            DC
```

To provision a new domain, run:

```
# samba-tool domain provision --use-rfc2307 --interactive
```

This will run the provision tool interactively. Because some settings can't be set interactively, it's recommended to run 'samba-tool domain provision –help' and have a look at the additional possibilities.

The '- -use-rfc2307' option enables your Samba AD automatically to store posix attributes. It also creates NIS information in the AD, that allows you to administrate UIDs/GIDs and other Unix settings (on the “Unix attributes” tab in ADUC). It's easier if you enable this feature during provisioning, than setting this up later by hand. And even if you don't required it (yet), it's not affecting your installation.

#### Important notes on the provisioning

- Unordered List ItemAs of Samba 4.0.0rc1 the provision command uses the Samba Internal DNS server by default. If you would like to use Bind as DNS backend, add - -dns-backend=BIND9_DLZ to the provisioning command. This decision isn't final. You can switch the backend whenever it's necessary.
- If you re-run the provisioning, you need to remove the /usr/local/samba/etc/smb.conf! You may also need to remove the samba database files if they were generated rm -rf /usr/local/samba/private/*
- The admin password need to fulfill the password complexity requirements. This means at least one uppercase letter, one number, and at least eight characters length. If you don't use a complex enough password, the provision script will fail, and you will need to start over with a better password (remove /usr/local/samba/private/ and /usr/local/samba/etc/).
- If your website is example.com, the domain of your AD should be a subdomain if it, like samdom.example.com (or ad.example.com, corp.example.com). Avoid using example.com

internally.

# Configure Kerberos

A Kerberos configuration suitable for Samba 4 has been generated at /usr/local/samba/private/krb5.conf Then do the following:

```
# mv /etc/krb5.conf{,.orig}
# cp /usr/local/samba/private/krb5.conf /etc/
```

For SerNet packages:

```
# mv /etc/krb5.conf{,.orig}
# cp /var/lib/samba/private/krb5.conf /etc/
```

# Configure DNS

A working DNS setup is essential to the correct operation of Samba and AD. Without the right DNS entries, Kerberos won't work, which in turn means that many of the basic features won't work! It is worth spending some extra time to ensure your DNS setup is correct, as debugging problems caused by mis-configured DNS can take a lot of time later on. To manage DNS entries the DNS MMC on a Windows client can be used, or samba-tool on Linux - see DNS Administration for more information.

#### For Bind 9.8 / 9.9

***If you choosed for internal DNS, you can skkip this part***. During provisioning/upgrading, a file ('/usr/local/samba/private/named.conf') was created, that must be included in your Bind named.conf:

```
include "/usr/local/samba/private/named.conf";
```

For SerNet packages:

```
include "/var/lib/samba/private/named.conf";
```

If you are using Samba from SerNet, may be yoy need to adjust the following permissions, to grant access to Bind9 deamon:

```
chgrp bind /var/lib/samba/private/named.conf
chmod g+r /var/lib/samba/private/named.conf

chgrp bind /var/lib/samba/private/dns.keytab
chmod g+r /var/lib/samba/private/dns.keytab
```

```
chgrp bind /var/lib/samba/private/
```

Then follow the instructions in “/var/lib/samba/private/named.txt”

Depending on the Bind version you are running, you should edit '/usr/local/samba/private/named.conf' and enable the right version of the DLZ module.

**DNS Dynamic Updates via Kerberos**

Samba has the capability to automatically update the Bind zone files via Kerberos. To setup dynamic DNS updates you need to have a recent version of Bind installed. It is highly recommended that you run at least version 9.8.0, as that version includes a set of patches from the Samba Team to make dynamic DNS updates much more robust and easier to configure. Please use 9.8 or 9.9 if possible!

To find out what version of Bind you are running, use

```
# named -V
```

If your operating system does not have Bind 9.8 or 9.9, please consider getting it from a package provided by a 3rd party (for example, on Ubuntu there is a ppa available with the newer versions of bind) or compile it by yourself.

A DNS keytab file was automatically created during provisioning/updating. Add the following' tkey-gssapi-keytab' option to the 'options' section of your named.conf.options:

```
options {
      [...]
        tkey-gssapi-keytab "/usr/local/samba/private/dns.keytab";
      [...]
 };
```

For SerNet packages:

```
options {
      [...]
        tkey-gssapi-keytab "/var/lib/samba/private/dns.keytab";
      [...]
 };
```

Restart Bind to have the included file being used. Check the logfiles for errors and problems. If available, you can 'run named-checkconf' to help you fix any problems with your Bind configuration.

```
# service bind9 restart
```

# Check your DNS configuration

Check your 'resolv.conf' that is pointing to your domain and Samba4 DC IP:

```
domain redtic.uclv.cu
search redtic.uclv.cu
nameserver 10.12.112.84 #Samba4-DC-IP
```

# Starting Samba

Samba doesn't yet have init scripts included for each platform when you compiled it, but write one for your platform should not be difficult.

Download the Samba4 init script from http://repos.uclv.edu.cu/samba-resources/samba4 (Ubuntu use start job)

```
# wget http://repos.uclv.edu.cu/samba-resources/samba4
# cp samba4 /etc/init.d/
# cd /etc/init.d/
# chmod +x samba4
# update-rc.d samba4 defaults
```

For Ubuntu do the same, but download from:
http://anonscm.debian.org/gitweb/?p=pkg-samba/samba.git;a=blob_plain;f=debian/samba-ad-dc.upstart;hb=HEAD

```
 # wget -O /etc/init/samba4
http://anonscm.debian.org/gitweb/?p=pkg-samba/samba.git;a=blob_plain;f=debian/
samba-ad-dc.upstart;hb=HEAD
```

If you have a init script o job start named samba4, you can start samba4 as a service:

```
# service samba4 start
```

**If you installed Samba4 SerNet, you must enable Samba4 as a service**:

```
# nano /etc/default/sernet-samba
```

Then locate the line 'SAMBA_START_MODE="none"' and change "none" for "ad". To start Samba4:

```
# service sernet-samba-ad start
```

If you are running Samba as a developer you may find the following more useful:

```
# samba -i -M single -d2
```

If you are using SerNet packages, you should create this directory before type the above command:

```
mkdir /var/run/samba
```

To save the output on a screen and a file log:

```
# samba -i M single -d2 | tee ~/samba4.log
```

To see more information in stdout change number '2' for a higher number, for example 5.

# Testing Samba

### Testing Connectivity to Your Samba AD DC

To list the shares on your Samba server:

```
# smbclient -L localhost -U%
```

To test that authentication is working, you should try to connect to the netlogon share, using the Administrator account created during provisioning. The output of the command should be similar to what is shown below:

```
# smbclient //localhost/netlogon -Uadministrator -c 'ls'
```

### Testing DNS

To test that DNS is working properly, run the following commands and compare the output to what is shown:

```
# host -t SRV _ldap._tcp.redtic.uclv.cu.
_ldap._tcp.redtic.uclv.cu has SRV record 0 100 389 redtic-ad1.redtic.uclv.cu.

# host -t SRV _kerberos._udp.redtic.uclv.cu.
_kerberos._udp.redtic.uclv.cu has SRV record 0 100 88 redtic-
ad1.redtic.uclv.cu.

# host -t A redtic-ad1.redtic.uclv.cu.
redticad1.redtic.uclv.cu has address 10.12.112.84
```

### Testing/Debugging dynamic DNS updates

The way the automatic DNS update in Samba works, is that the provision will create a file '/usr/local/samba/private/dns_update_list', which contains a list of DNS entries that Samba will try to

dynamically update at startup and every 10 minutes thereafter using the 'samba_dnsupdate' utility. Updates will only happen if the DNS entries do not already exist. Remember that you need the 'nsupdate' utility from Bind the distribution for all these to work.

To test o debug DNS updates:

```
# samba_dnsupdate --verbose --all-names
```

#### Testing Kerberos

The simplest test is to use the kinit command as follows:

```
# kinit administrator
```

To verify that Kerberos is working, and that you received a ticket, run:

```
# klist
```

***Note:*** If provision generated a password and you forgot it or didn't save it in some way, you can use samba-tool user setpassword administrator as root to reset it.

You can also test Kerberos from a remote client, but you must first configure the client's krb5.conf and resolve.conf as shown previously.

***Note:*** If you are using a client behind NAT then you have to add the following to the krb5.conf on the domain controller:

```
[kdc]
    check-ticket-addresses = false
```

**Testing Samba config** For testing Samba config you can use the following commands:

```
# testparm
# samba-tool testparm
```

## Improve some configurations

#### To disables this messages:

```
 /usr/local/samba/sbin/smbd: Unable to connect to CUPS server localhost:631 -
Connection refused
 /usr/local/samba/sbin/smbd: failed to retrieve printer list:
NT_STATUS_UNSUCCESSFUL
```

Edit your smb.conf (/usr/local/samba/etc/smb.conf) and add in [global] sections:

```
# Disable CUPS errors
printing = bsd
printcap name = /dev/null
```

### Change log level

To change the log level value permanent you can add the following in /usr/local/samba/etc/smb.conf inside [global] sections:

```
log level = 3
```