



Samba and LDAP in 30 Minutes

Configuring LDAP and a Samba-PDC on RHEL4

by Jens Kühnel
Bad Vilbel, Germany
freelance SuSE- and RedHat-Trainer

book author „Samba 3 -
Wanderer zwischen den Welten“



Overview

- LDAP
 - Schema
 - slapd.conf
- smbldap-tools
 - smbldap_conf.pm
 - smbldap-populate.pl
- Samba
 - smb.conf



LDAP-Schema

- The „Building-Plan“ has to be updated

```
cp /usr/share/doc/samba-3.0.*/LDAP/samba.schema \  
  /etc/openldap/schema/samba.schema
```

- Add the Schema to */etc/openldap/slapd.conf*

```
include          /etc/openldap/schema/samba.schema
```



Add Access-Rights in slapd.conf

```
access to attrs=userPassword,sambaLMPassword,\  
sambaNTPassword,shadowLastChange  
by dn.children="ou=admin,dc=example,dc=com" write  
by self write  
by anonymous auth  
by * none  
access to *  
by dn.children="ou=admin,dc=example,dc=com" write  
by * read
```



suffix and root Account in slapd.conf

- Adjust suffix and rootdn:

```
suffix      "dc=example,dc=com"
```

```
rootdn     "cn=Manager,dc=example,dc=com"
```

- Use the programm slappasswd to create password-hash:

```
rootpw     {SSHA}GLYiF62wn1O6iHYJCHDriCSjFGj
```



Speedup with Indexing

- Indexing improves Speed

index sambaSID,sambaPrimaryGroupSID,sambaDomainName eq



Smbldap-tools

- Put in File `~/.rpmmarcos`:

```
%_solve_pkgdir http://192.168.0.2/rhel4/RedHat/RPMS/
```

```
%_solve_name_fmt % {?_solve_pkgdir}%%{NAME}-\
%%{VERSION}-%%{RELEASE}.%%{ARCH}.rpm
```

- Installing smbldap-tools

```
rpm -ivh --aid http://www.kuehnel.org/smbldap-tools.rpm
```



Smbldap_conf.pm

- Change the SID
 - Take the output of *net getlocalsid* and add it like:
\$SID='S-1-5-21-3516781642-1962875130-3438800523';
- Change Suffix and Login
 - \$suffix
 - \$binddn
 - \$bindpasswd



Start LDAP and populate

- Start LDAP

/etc/init.d/ldap start

- Create the LDAP-Groups and -Users

smbldap-populate.pl



Create a Admin-Account-File

```
ldapadd -cxW -D „cn=Manager,dc=....“
```

```
Password: securePassword
```

```
dn: ou=admin,dc=example,dc=com
```

```
objectclass: organizationalUnit
```

```
ou: admin
```

```
dn: cn=samba,ou=admin,dc=example,dc=com
```

```
objectclass: person
```

```
cn: samba
```

```
sn: Samba-Admin-User
```

```
userPassword: verysecure
```



Using LDAP as a Auth-Source

- Authconfig

- Add LDAP as both User- and Password-Source

```
authconfig --enableldap --enableldapauth \
```

```
--ldapservers=127.0.0.1 --ldapbasedn=dc=example,dc=com
```



Adding Samba

- Adjusting the following options
 - *Workgroup=Domainname*
 - *Ldap admin=cn=samba,ou=admin,....*
 - *Ldap suffix=....*
- Add the following options:
 - *Passdb backend=ldapsam:ldap://127.0.0.1/*
 - *Domain master = yes*
 - *Domain logon = yes*
 - *Ldap {group,user,machine} suffix = \
ou={Groups,People,Computers}*



Automatic Adding to the LDAP

- *add user script = /usr/sbin/smbldap-useradd.pl -m %u*
- *delete user script = /usr/sbin/smbldap-userdel.pl -r %u*
- *add machine script = /usr/sbin/smbldap-useradd.pl -w %u*
- *add group script = /usr/sbin/smbldap-groupadd.pl -a %g*
- *delete group script = /usr/sbin/smbldap-groupsript.pl %g*
- *add user to group script = /usr/sbin/smbldap-groupmod.pl \
-m %u %g*
- *delete user from group script = /usr/sbin/smbldap-\
groupmod.pl -x %u %g*



LDAP-Password

- Giving Samba the right to write into the LDAP-Directory
- *smbpasswd -w verysecure*



Ready to join

- Old version you need root with a SMB password
- With newer Versions you need to add rights to your account