Step by Step

LDAP und Samba unter SuSe Linux

von Christian Bartl

LDAP und Samba unter SuSe Linux

1) LDAP-Server

Installation und Vorraussetzungen

Als Betriebssystem dient SuSe 9.1 um LDAP erfolgreich implementieren zu können werden folgende Pakete: openldap2, ldaplib, pam_ldap, webgw, nss_ldap benötigt. Für die Konfiguration dienen die folgenden Config-Files:

/etc/openldap/schema/core.schema
/etc/openldap/schema/inetorgperson.schema
/etc/openldap/sldif.conf

Grundkonfiguration des Servers

Die Grundkonfiguration des LDAP-Servers wird in der /etc/openldap/sldif.conf vorgenommen.

```
database ldbm
suffix "dc=5ait,dc=local"
rootdn "cn=admin,dc=5ait,dc= local"
# Cleartext passwords, especially for the rootdn, should
# be avoided.  See slappasswd(8) and slapd.conf(5) for details.
# Use of strong authentication encouraged.
rootpw secret
# The database directory MUST exist prior to running slapd AND
# should only be accessible by the slapd/tools. Mode 700 recommended.
directory /var/lib/ldap
# Indices to maintain
index   objectClass     eq
```

In diesem Fall ist das Root-Passwort nicht verschlüsselt und steht als Klartext im Config-File. Mit Hilfe des Tools slappasswd kann eine verschlüsseltes Passwort generiert werden. Dieses ersetzt dann einfach das unverschlüsselte Passwort, hier„secret“.

LDAP-Struktur anlegen

Die Grundstruktur unserer LDAP-Umgebung wird ebenfalls mittels Config-File erstellt. Dazu benötigen wir die Datei „infrastruct.ldif“.

```
# Hauptdomäne als Grundstein für die Struktur
dn: dc=5ait,dc=local
objectClass: dcObject
objectClass: organization
description: Haupt
dc= 5ait          //Fehlerquelle
o: 5ait

# Organisation TestLDAP als äquivalent für eine Sub-Domain
dn: o=TestLDAP,dc=5ait,dc= local
objectClass: organization          //Organisation
description: Sub-Domain
o: TestLDAP

# Organisationseinheit für die Benutzer, die für das Adressbuch
# abgelegt werden sollen
dn: ou=addressbook,o=TestLDAP,dc=5ait,dc= local
objectClass: organizationalUnit    //Organisationeinheit
```

```
ou: user

# Organisationseinheit für die Computer
dn: ou=computers, o=TestLDAP,dc=5ait,dc= local
objectClass: organizationalUnit
o: computers
```

Ist die Datei erfolgreich erstellt muss sie noch in LDAP eingespielt werden. Dies geschieht mit folgendem Befehl:

```
ldapadd -x -D cn=admin,dc=5ait,dc=local -W -f infrastruct.ldif
Enter LDAP password:
adding new entry "dc=5ait,dc=local"
adding new entry "o=TestLDAP,dc=5ait,dc= local "

adding new entry "ou=user,dc=5ait,dc= local "
adding new entry "ou=computers,dc=5ait,dc= local "
```

LDAP-Objekte (User) anlegen

Um einen User anlegen zu können wird erneut ein Ldif-File benötigt. Dieses heißt in unserem Fall „av.ldif“

```
dn: cn=chris, ou=user, o=TestLDAP, dc=5it, dc=local
objectClass: top
objectClass: person
objectClass: inetOrgPerson
objectClass: officePerson          //Windowsoffice
objectClass: organizationalRole
objectClass: posixAccount          //wichtig für Samba
uid: chris                    //Userid
uidnumber: 600
gidnumber: 506
homeDirectory: /home/chris
loginShell: /bin/false
cn: chris                     //User
givenName: Christian               //Hauptname
initials: Initialen
sn: Bartl
displayName: Herr Bartl
o: testLDAP
mail: chris@samba.junits
```

Ist das File fertiggestellt wird der User mit dem Befehl ldapadd hinzugefügt.

```
ldapadd -x -D cn=admin,dc=5ait,dc=local -W -f ab.ldif
```

Nun muss für den User nur noch ein entsprechendes Homeverzeichnis mit den benötigten Rechten angelegt werden. Dies erfolgt über folgende Befehle:

```
SambaLDAP:~$ mkdir /home/chris
SambaLDAP:~$ chown -R chris:user /home/chris
SambaLDAP:~$ chmod -R 700 /home/chris
```

LDAP-Objekte verändern

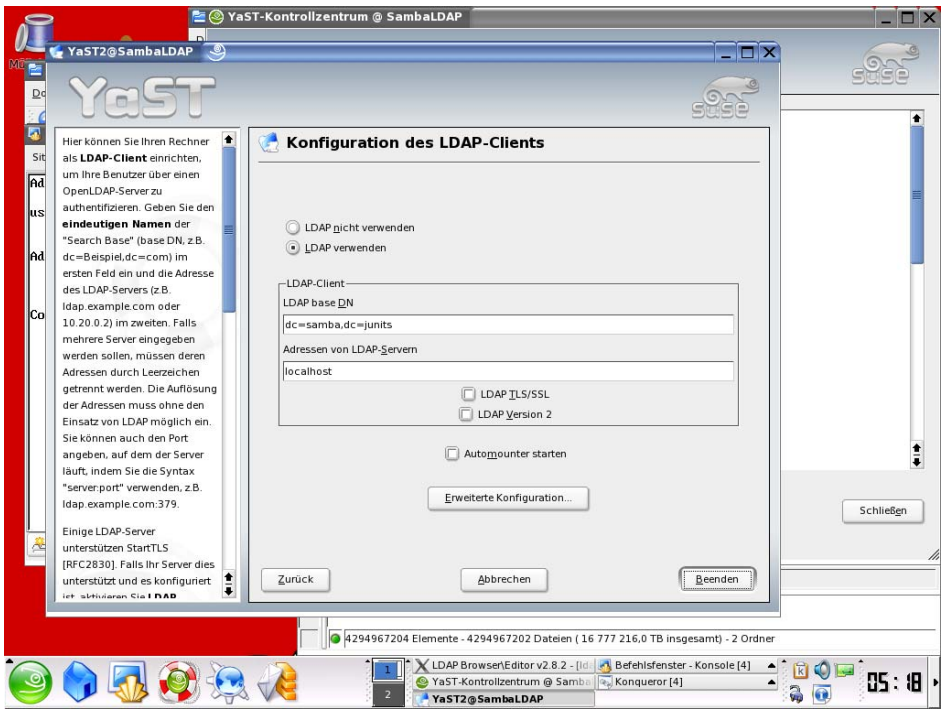
```
ldapmodify -x -D cn=admin,dc=5ait,dc=local -W -f modfile.ldif
```

LDAP-Objekte löschen

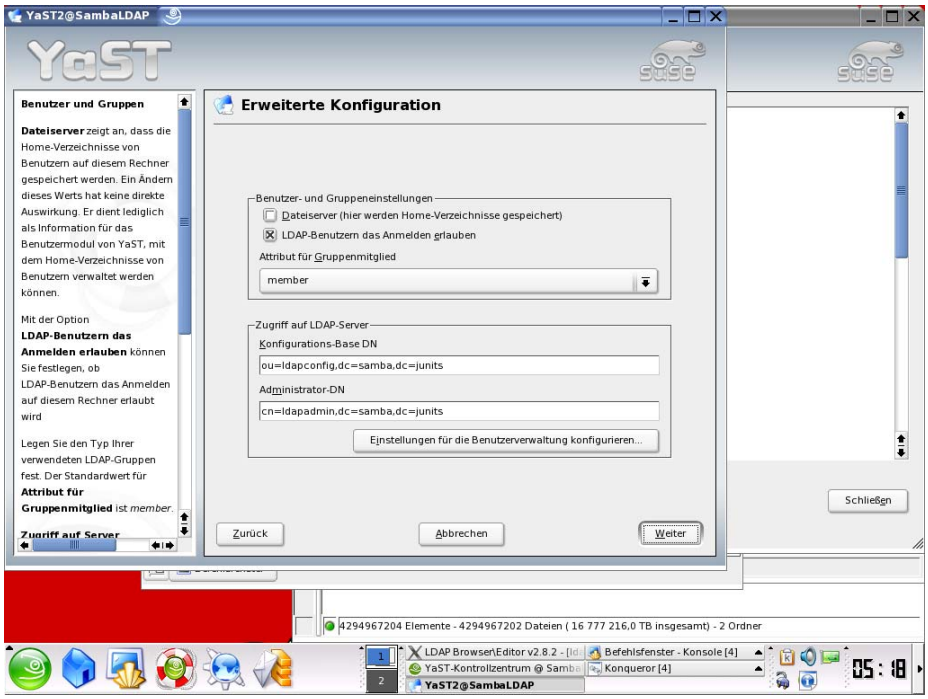
```
ldapdelete -x -D cn=admin,dc=5ait,dc= local -W cn=LDAP-Objekt
```

2) LDAP-Client einrichten

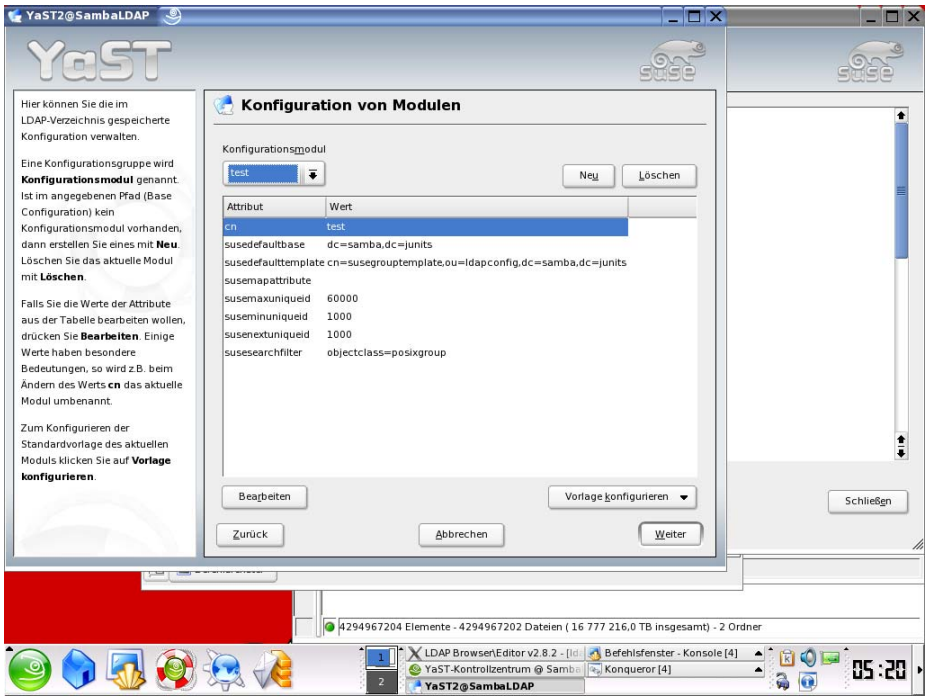
Um sich nun per Workstation und über LDAP am Server anmelden zu können, muss der Client für LDAP konfiguriert werden. Dies geschieht unter SuSe am einfachsten mittels YAST. Die erforderlichen Einstellungen finden sich unter Yast -> Netzwerkdienste -> LDAP-Client.



Geben Sie alle erforderlichen Daten an. Hier ist die DN „dc=samba,dc=junits“ und die Adresse des LDAP-Servers ist die jeweilige IP. Es wird keine Verschlüsselung verwendet, also entfernen Sie das Häckchen bei „LDAP TLS/SSL“



Gehen Sie nun unter erweiterte Konfiguration und hier unter „Einstellungen für die Benutzerverwaltung konfigurieren“.



Nun fügen Sie über „Neu“ ein Konfigurationsmodul für User und für Gruppen hinzu. Die Standardeinstellungen müssen für unser Beispiel nicht verändert werden.

3) Samba

Samba ist ein Filesharing Dienst der auch von Windows-Clients gelesen werden kann. Dieser wird bei LDAP vor allem für das zu Verfügung stellen von Homelaufwerken der LDAP-User benötigt. Außerdem erfolgt natürlich die Benutzerverwaltung für die Zugriffe auf Freigaben über LDAP.

Konfiguration von Samba

Diese wird in der Datei /etc/samba/smb.conf vorgenommen.

```
[global]
   # Arbeitsgruppenname, NetBios-Name und Serverbezeichung, über die
   # Samba im Netzwerk angesprochen werden kann
   workgroup = TestLDAP
   netbios name = SambaLDAP
   server string = SambaLDAP

   # Mit 'logon script' wird das Anmeldeskript definiert, das während
der
   # Anmeldung abgearbeitet werden soll (bsp. Verbinden von
Netzlaufwerken).
   # Dagegen gibt 'logon path' den Netzwerkpfad für das
servergespeicherte
   # Profil an. Hinter der Variable %U wird der Benutzername
maskiert.
   # 'logon drive' gibt den Laufwerks-Buchstaben an, mit dem das
unter
   # 'logon home' definierte Heimatverzeichnis verbunden werden soll.
   logon script = %G.bat
   logon path = \\SambaLDAP\%U
   logon home = \\SambaLDAP\profile\%U
   logon drive = H:

   # Angaben zum Domänen-Suffix und der DN für den LDAP-
Administrator,
   # dessen Namen frei gewählt aber später für die Konfiguration des
   # LDAP-Servers wieder verwendet werden muss. Zusätzlich die
Suffixes,
   # die an Benutzer bzw. Computer angehängt werden soll. (Diese
beiden
   # Angaben spielen im wesentlichen für das Programm smbpasswd eine
Rolle.)
   ldap suffix = dc=5it,dc=local
   ldap admin = "dn=ldapadmin,dc=samba,dc=junits"
   ldap user suffix = "ou=user,o=TestLDAP "
   ldap machine suffix = "ou=computer,o=TestLDAP "

   # Vorgaben, nach denen Samba im LDAP-Verzeichnis nach Einträgen
suchen
   # soll. Das '&' leitet eine einfache UND-Verknüpfung ein, wodurch
nach
   # der mathematischen Aussagenlogik also beide Bedingungen (jeweils
in
   # runden Klammern angegeben) erfüllt sein müssen. In diesem Fall
muss
   # der gesuchte Eintrag als ein sambaAccount deklariert sein und
dessen
   # uid dem Namen des sich anmeldenden Benutzers (%u) entsprechen.
   ldap filter = (&(objectclass=sambaaccount)(uid=%u))

[homes]
   # Wenn die Freigabe in der Netzwerkumgebung angezeigt werden soll,
muss
   # 'browseable' auf 'yes' gesetzt werden. Soll es den Benutzern
ermöglicht
   # werden, auf diesen Freigaben zu schreiben, muss 'writeable' den
Wert
```

```
   # 'yes' erhalten. Als gültiger Benutzer, der auf diese Freigabe
zugreifen
   # darf, wird der aktuelle Service (%S) anerkannt - er enthält den
   # Anmeldenamen.
   browseable = no
   valid users = %S
   writeable = yes

[netlogon]
   # 'path' enth?lt den lokalen Pfad zum Verzeichnis, das freigegeben
werden
   # soll. 'comment' definiert einen optionalen Kommentar zur
Freigabe.
   comment = Anmeldeskript
   path = /home/netlogon
   write list = root
```

Adminzugriff

Da der User LDAPAdmin noch keinen Zugriff auf den Samba-Dienst hat wird dies über folgende Befehlszeilen erledigt:

```
/usr/local/samba/bin/smbpasswd -w <password>
/usr/local/samba/bin/pdbedit -a -u ldapadmin
```

User hinzufügen

```
/usr/local/samba/bin/pdbedit -a -u chris –w
```

Verknüpfung zwischen LDAP und Samba

Damit der LDAP-Server und der Samba-Server miteinander kommunizieren können muss noch eine Einstellung vorgenommen werden. Im Normalfall würde der Samba-Server die Passwörter mit den lokal eingerichteten Benutzern vergleichen. Einige Einstellung in „nsswitch.conf“ veranlassen diesen aber die Passwörter nicht Lokal sondern mit dem LDAP-Server zu verifizieren.

```
Passwd: files ldap
Shadow: files ldap
Goup: files ldap
```

4) Theorie

Tutorial mit dessen Hilfe diese Übung gemeistert wurde:

http://www.mykleines.de/netzwerker/network.php?file=smbldap

OpenLDAP Workshop:

http://www.mitlinx.de/ldap/index.html?http://www.mitlinx.de/ldap/workshop_openldap.htm