Linux LDAP HOWTO

Thomas Bendler (thomas.bendler@informatik.fh-hamburg.de) v0.65-2, 7. Oktober 1999

Dieses HOWTO soll die Installation und Konfiguration eines LDAP Servers auf Basis des OpenLDAP veranschaulichen. Desweiteren finden sich Informationen zum Zugriff auf den LDAP Server.

Inhaltsverzeichnis

1 Einleitung **2**

1.1 Besonderheiten . . . 2

1.2 Neue Versionen . . . 2

1.2.1 Aktuelle Version . . . 3

1.2.2 Zukünftige Versionen . . . 3

1.3 Feedback . . . 3

1.4 Haftung . . . 3

1.5 Copyright . . . 3

2 Eine kleine Einführung in LDAP **3**

2.1 Was ist LDAP? . . . 3

2.2 Welche Informationen kann LDAP zur Verfügung stellen? . . . 4

3 Technische Daten des LDAP Server **4**

4 Installation des OpenLDAP **4**

4.1 Quellen für den OpenLDAP Server . . . 4

4.2 Installation des OpenLDAP Servers . . . 5

4.3 Unterschiede zwischen dem Orginal OpenLDAP Paket und den SuSE rpm-Archiven . . . 5

5 Anpassen der Konfigurationsdateien **6**

5.1 Liste der Konfigurationsdateien . . . 6

5.2 Konfigurieren der ldap.conf . . . 6

5.3 Konfiguration der slapd.conf . . . 6

5.4 Sonstige Konfigurationsdateien . . . 7

6 Erstellen eines Beispielverzeichnisses **7**

6.1 Erstellen der LDIF Dateien . . . 7

6.1.1 Beispiel LDIF firmenstruktur.ldif . . . 8

6.1.2 Beispiel LDIF sales.ldif . . . 9

6.1.3 Beispiel LDIF development.ldif . . . 10

6.1.4 Beispiel LDIF support.ldif 10
6.2 Umwandeln der LDIF Datei in das LDBM Format 11
6.3 Testen des LDAP Servers 11
6.4 Hinzufügen von Datensätzen 11

7 Tuning des LDAP Servers 12

8 Frontends für den LDAP Server 12
8.1 Installation von Web500gw 12
8.2 Konfiguration von Web500gw 13
8.3 Die web500gw.conf 13
8.4 Zugriff auf Web500gw 14
8.5 Weitere Konfigurationsdateien 15

9 Client Zugriff auf LDAP 15
9.1 Konfiguration des Netscape Communinicator 15
9.2 Erweiterte Konfiguration 15

10 Nützliche Tools 15
10.1 LDAP Migration Tools 16
10.2 PAM LDAP Module 16
10.3 kldap 16
10.4 GQ 16

11 Weitere Quellen und Dokumentationen 16
11.1 Adressen im Internet 16
11.2 Bücher 17
11.3 RFC´s 17

1 Einleitung

1.1 Besonderheiten

Dieses HOWTO bezieht sich auf die Installation des OpenLDAP Servers 1.2.4-2 aus der Serie n unter SuSE Linux 6.2. Die Konfiguration unterscheidet sich von der Installation des Orginal OpenLDAP Paketes durch unterschiedliche Verzeichnisse, die per Default in den rpm´s der SuSE Distribution eingestellt sind. In einem gesonderten Kapitel gehe ich auf die einzelnen Unterschiede ein, so daß die Anpassung an die lokalen Gegebenheiten kein Problem sein sollte.

1.2 Neue Versionen

1.2.1 Aktuelle Version

Die aktuelle Version dieses Dokumentes ist auf dem Server des Deutschen Linux HOWTO Projektes unter

`http://www.tu-harburg.de/dlhp/`

zu finden.

1.2.2 Zukünftige Versionen

Die von mir vorgestellte Beispieldatenbank stellt natürlich nur einen kleinen Teil der Möglichkeiten dar, die LDAP bietet. Sie soll in erster Linie als Einstieg dienen und den geneigten Nutzer zum experimentieren animieren. Ich werde versuchen, dieses HOWTO im Laufe der nächsten Zeit zu erweitern, um weitere Möglichkeiten im Umgang mit LDAP aufzuzeigen. Dabei bin ich allerdings auf die Hilfe der LDAP Cracks angewiesen, da ich mich noch nicht allzulange mit LDAP beschäftige. Um dieses Dokument also so vollständig wie möglich zu gestalten, bitte ich funtionierende Verfahren (z.B. Passwort Authentifizierung via LDAP, Roaming, SAMBA und LDAP, etc.) an die unter Feedback angegebende E-Mail Adresse zu senden, damit ich sie so schnell wie möglich in dieses Dokument aufnehmen kann.

1.3 Feedback

Bei Fragen und Kommentaren zu diesem Dokument sowie bei Anregungen und Verbesserungsvorschlägen wenden Sie sich bitte an:

Thomas Bendler (`thomas.bendler@informatik.fh-hamburg.de`)

1.4 Haftung

Für die hier vorgestellten Verfahren übernehme ich keine Haftung. Sollten sich Fehler eingeschlichen haben oder Verfahren nicht funtionieren, siehe Feedback.

1.5 Copyright

2 Eine kleine Einführung in LDAP

2.1 Was ist LDAP?

LDAP ist die Abkürzung von *Lightweight Directory Access Protokoll*. Das LDAP entstand ursprünglich als Front End für den X.500 Verzeichnisdienst. Da X.500 als kompletter OSI Stack implementiert ist, war es nicht möglich, diesen Verzeichnisdienst flächendeckend zu implementieren. LDAP ist ein Verzeichnisdienst, der auf dem TCP/IP-Protokoll basiert und somit Resourcenschonender für die Netzwerk Infrastruktur ist. Obwohl LDAP nur einen Teil der Funktionen des DAP zur Verfügung stellt, reicht es aus, um die fehlenden Funktionen vollständig zu emulieren. Basis für LDAP sind die im Abschnitt 11.3 aufgeführten RFC´s.

2.2 Welche Informationen kann LDAP zur Verfügung stellen?

LDAP speichert seine Informationen in einer Baumhierarchie. Diese Hierarchie kann diverse Informationen enthalten. Einen Überblick verschafft RFC 2307, in dem mögliche Inhalte der LDAP Hierarchie spezifiziert sind:

- Benutzer
- Gruppen
- IP Dienste
- IP Protokolle
- RPCs
- NIS Netzwerkgruppen
- Boot-Informationen
- Einhängepunkte für Dateisysteme
- IP Hosts und Netzwerke
- RFC 822 konforme Mail-Aliase

3 Technische Daten des LDAP Server

Der Zugriff auf den LDAP Server erfolgt über das LDAP Protokoll via TCP/IP. Per Default lauscht der `slapd` auf dem Port 389. Dies ist im RFC 1777 spezifiziert. Der LDAP Server speichert seine Informationen in einer baumartigen Struktur. Diese wird auch Directory Information Tree genannt, kurz DIT. Zum Speichern benutzt der LDAP Server Objekte, die er mit Attributen versehen kann. Dadurch kann man die Struktur flexibel an die eigenen Bedürfnisse anpassen. Das RFC 2256 spezifiziert die Standard Objekte des LDAP Servers. Man wird zwar von niemanden gezwungen, diese Vorgaben auch zu benutzen, um aber eine möglichst große Kompatibilität zu erzielen, sollte man diese Vorgaben einhalten.

4 Installation des OpenLDAP

Beschrieben wird im folgenden die Installation des OpenLDAP in der Version 1.2.1. Die Installation zukünftiger Releases sollte sich nicht grundlegend von der hier vorgestellten Methode abweichen. Sollte dies trotzdem der Fall sein, werde ich das in zukünftigen Versionen dieses Dokumentes berücksichtigen.

4.1 Quellen für den OpenLDAP Server

Der Quellcode der aktuellen Version des OpenLDAP Servers in einem komprimierten Archiv finden sich auf der Homepage der OpenLDAP Foundation. Die aktuellen Quellen können von:

```
ftp.OpenLDAP.org:/pub/OpenLDAP/openldap-release.tgz
```

bezogen werden.

Eine einfachere Möglichkeit der Installation bieten sogenannte rpm-Archive. Dies sind bereits kompilierte Pakete, die auf die Besonderheiten der jeweils eingesetzten Distribution zugeschnitten sind. Die jeweilige Installationsprozedur entnehmen Sie bitte Ihrem Handbuch. In der SuSE Distribution ist der OpenLDAP Server in der Serie n zu finden.

4.2 Installation des OpenLDAP Servers

Haben Sie den OpenLDAP mit Hilfe der Distributions eigenen rpm-Archive installiert, können Sie diesen Abschnitt auslassen. Wenn Sie sich die Quellen des OpenLDAP Servers gezogen haben, müssen Sie diese noch installieren. Zu diesem Zweck wechseln Sie in das Verzeichnis, in dem Sie die Quellen gespeichert haben und entpacken Sie die Quellen mit folgendem Kommando:

```
tar xvfz ./openldap-release.tgz
```

Anschließend müssen Sie mit `cd ldap` in das Installationsverzeichnis wechseln. Dort befindet sich die Datei `include/ldapconfig.h.edit`. In ihr kann man den LDAP an die eigenen Bedürfnisse anpassen. In der Regel sollten aber die voreingestellten Werte in Ordnung sein. Nun gehts ans Übersetzten und Installieren des Programmpaketes. Führen Sie dazu folgende Befehle aus:

```
./configure
make depend
make
```

Um die Kompilation zu testen, können noch folgende Anweisungen ausgeführt werden:

```
cd test
make
```

Die Installation des Paketes muß als Superuser (root) mit folgendem Befehl erfolgen:

```
su
make install
```

That´s it. Nun sollte der OpenLDAP Server installiert sein.

4.3 Unterschiede zwischen dem Orginal OpenLDAP Paket und den SuSE rpm-Archiven

Die beiden Pakete sind zwar nach der Installation inhaltlich fast identisch, unterscheiden sich aber gravierend in den verwendeten Pfaden. Folgende Übersicht soll die Unterschiede verdeutlichen:

SuSE rpm-Archive:

```
/etc/openldap/                Konfigurationsdateien
/usr/bin/                     Hilfsdateien
/usr/libexec/openldap/        Server
/sbin/init.d/ldap             Startskript
/usr/doc/packages/openldap/   Dokumentation, zusätzliche Tools
/usr/include/                 Include Dateien
/usr/lib/                     Bibliotheken
/usr/share/openldap/          Dateien für X.500 Gateway
```

OpenLDAP Original:

```
/usr/local/etc/openldap/      Konfigurationsdateien
/usr/local/bin/               Hilfsdateien
/usr/local/sbin/              Server
/usr/src/ldap/doc/            Dokumentation (wenn Installationsverzeichnis)
/usr/local/include/           Include Dateien
/usr/local/lib/               Bibliotheken
/usr/local/share/             Dateien für X.500 Gateway
```

5 Anpassen der Konfigurationsdateien

Die Pfade für die Konfigurationsdateien entnehmen sie bitte dem Abschnitt 4.3. Mit dem OpenLDAP Server werden mehrere Konfigurationsdateien ausgeliefert, die teilweise noch an die lokalen Gegebenheiten angepasst werden müssen.

5.1 Liste der Konfigurationsdateien

```
ldap.conf              Client Konfiguration
ldapfilter.conf        Filterregeln
ldapsearchprefs.conf   Bevorzugte Suchkriterien
ldaptemplates.conf     Templates für Formulare
slapd.conf             Server Konfiguration
slapd.at.conf          Beschreibung der Attribute
slapd.oc.conf          Beschreibung der Objektklassen
```

5.2 Konfigurieren der ldap.conf

In der Datei `ldap.conf` wird die Basis Domain für den Client festgelegt. Für das folgende Beispiel im Abschnitt 6 wird die Basisadresse mit der Domain geleichgesetzt.

```
#
# ldap.conf für Structur Net
#
# Beachten Sie auch man ldap.conf
#
BASE    dc=structure-net,dc=de
HOST    ldap.structure-net.de
```

Was bewirkt die hier vorgestellte `ldap.conf`? Mit der Variable BASE wird die standardmäßig abgefragte Struktur festgelegt. Die Variable HOST gibt den Server an, der standardmäßig abgefragt wird. Über die Variable PORT kann alternativ auch ein anderer Default Port eingestellt werden.

5.3 Konfiguration der slapd.conf

Die Datei `slapd.conf` enthält die Einträge für die Konfiguration des `slapd` Standalone Server. Der `slapd` beantwortet die LDAP Anfragen der Clients. Für das folgende Beispiel bekommt die Datei folgenden Inhalt:

```
#
# slapd.conf für Structure Net (SuSE Style)
#
# Beachten Sie auch "man slapd.conf"
#
# Diese Datei sollte nicht global lesbar sein, da sie ein
# Paßwort enthält.
include         /etc/openldap/slapd.at.conf
include         /etc/openldap/slapd.oc.conf
schemacheck     on
referral        ldap://ldap.infospace.com
pidfile         /var/run/slapd.pid
argsfile        /var/run/slapd.args
```

```
database        ldbm
directory       /var/openldap
suffix          "dc=structure-net,dc=de"
rootdn          "uid=admin,dc=structure-net,c=de"
rootpw          secret
index           cn,sn,uid       pres,eq,approx,sub
index           objectclass     pres,eq
index           default         none
defaultaccess   read
access to attr=userpassword
   by self write
   by dn="uid=admin,dc=structure-net,dc=de" write
   by * compare
```

Was bewirkt die hier vorgestellte `slapd.conf`? Die include Anweisungen bewirken ein Einbinden der angegebenen Dateien. In diesem Fall werden die Objektklassen (oc) und deren Attribute (at) eingelesen. Mit dem schemacheck wird überprüft, ob modifizierte oder neu installierte Daten den Regeln der Objektklassen entsprechen. Ist der ldap nicht in der Lage, eine Anfrage zu beantworten, fragt er den unter referral angegebenden Server. Die Zeilen pidfile und argsfile sind für den laufenden Betrieb (pid=prozess id, args=argumente). Mit dem Schlüsselwort database wird festgelegt, welches Datenbankformat benutzt wird. Es sind auch Abfragen von anderen Datenbanken möglich. Im directory wird spezifiziert, wo die Datenbank zu finden ist bzw. angelegt werden soll. Da dieses Verzeichnis frei wählbar ist, muß es noch von Hand angelegt werden. Dazu reicht ein einfaches:

```
cd /var
mkdir openldap
```

Die unter suffix angegebende Struktur legt fest, welche Anfragen über die lokale Datenbank beanwortet werden können. Die rootdn und rootpw Einträge spezifizieren den Administrator der Datenbank. Mit Hilfe der index Anweisung wird der Datenbank mitgeteilt, wie sie Indexe anlegen soll. Zum Schluß werden noch die Zugriffsrechte auf den LDAP Server festgelegt. Standardmäßig erhält jeder Benutzer Lesezugriff auf die Datenbank. Verändern dürfen die Benutzer nur ihren eigenen Eintrag. Diese Aktion wird über das Attribut userpassword verifiziert. Der Benutzer admin darf alle Einträge unterhalb structure-net verändern. Ein Vergleich ist jedem gestattet.

5.4 Sonstige Konfigurationsdateien

Wie man bereits in der Konfigurationsdatei `slapd.conf` sehen kann, werden zwei Konfigurationsdateien eingebunden (`slapd.at.conf`, `slapd.oc.conf`). Diese müssen in diesem Beispiel nicht verändert werden. Die Dateien enthalten die Objektklassen und die Attribute für die Objektklassen. Die standardmäßig gegebenden Dateien sind für die meisten Standard Anwendungen ausreichend. Für weitere Informationen konsultieren Sie bitte die entsprechenden Manual Pages.

Sollen die Benutzer ihre Einträge selbst verändern können, so empfielt sich noch eine Anpassung der `ldaptemplates.conf` an die eigene Bedürfnisse. Sie stellt die Standard-Einstellungen zur Verfügung.

6 Erstellen eines Beispielverzeichnisses

6.1 Erstellen der LDIF Dateien

Nach der Installation und Konfiguration des LDAP Servers muß dieser mit Daten gefüttert werden. Das folgende Beispiel erklärt den LDAP Server anhand einer fiktiven Firma mit mehreren Abteilungen. Die einzelnen Felder müssen den lokalen Gegebenheiten nur angepaßt werden, um eine simple Konfiguration aufzusetzten.

Für das folgende Beispiel wird im Verzeichnis `/etc/openldap` das Unterverzeichnis `ldif/` angelegt. In diesem Verzeichnis kann mit jedem x-beliebigen Editor, der ASCII unterstützt, eine Datei mit dem Namen `firmenstruktur.ldif` erstellt werden. Der Name und das Verzeichnis für die Beispiel LDIF-Dateien sind beliebig. Es müssen für den Fall, das andere Namen oder Pfade verwendet werden, diese nur an die lokalen Gegebenheiten angepaßt werden.

Das Beispiel erstellt den DIT (Directory Information Tree) für die fiktive Firma Structure Net in Deutschland; hoffentlich gibts die wirklich nicht. Die Firma Structure Net bekommt drei Abteilungen spendiert: Sales, Development und Support. Jeder Abteilung werden zwei Mitarbeiter zugeordnet. Daraus ergibt sich folgende Struktur:

```
DE
|
+-- Structure Net --+
                    |
                    +-- Sales --+-- Mitarbeiter 1 (Axel Hueser)
                    |           |
                    |           +-- Mitarbeiter 2 (Jared Wiener)
                    |
                    +-- Development --+-- Mitarbeiter 3 (Thomas Bendler)
                    |                 |
                    |                 +-- Mitarbeiter 4 (Thomas Lippert)
                    |
                    +-- Support --+-- Mitarbeiter 5 (Elmar Mueller)
                                  |
                                  +-- Mitarbeiter 6 (Enrico Lemke)
```

Um das Beispiel übersichtlich zu gestalten und dem Nutzer zu zeigen, welche Einträge für was verantwortlich sind, habe ich die Beispiel LDIF in eine Datei für die Firmenstruktur und in eine Datei pro Abteilung aufgeteilt. Der admin Account muß natürlich schon in der Firmenstrukur angegeben werden, da sonst keine weiteren Einträge über `ldapadd` möglich sind; doch dazu später mehr.

6.1.1 Beispiel LDIF firmenstruktur.ldif

```
dn: dc=structure-net, dc=de
objectclass: organization
objectclass: top
o: Structure Net
l: Hamburg
postalcode: 21033
streetadress: Billwiese 22

dn: ou=Sales, dc=structure-net, dc=de
objectclass: organizationalunit
ou: Sales
description: Verkauf
telephonenumber: 040-7654321
facsmiletelephonenumber: 040-7654321

dn: ou=Development, dc=structure-net, dc=de
objectclass: organizationalunit
ou: Development
description: Verkauf
telephonenumber: 040-7654321
facsmiletelephonenumber: 040-7654321
```

```
dn: ou=Support, dc=structure-net, dc=de
objectclass: organizationalunit
ou: Support
description: Verkauf
telephonenumber: 040-7654321
facsmiletelephonenumber: 040-7654321

dn: uid=admin, dc=structure-net, dc=de
objectclass: person
objectclass: organizationalperson
objectclass: inetorgperson
cn: admin
cn: Systemverwalter
cn: Thomas Bendler
sn: Bendler
uid: admin
mail: tbendler@structure-net.de
l: Hamburg
postalcode: 21033
streetadress: billwiese 22
telephonenumber: 040-7654321
facsmiletelephonenumber: 040-7654321
```

6.1.2 Beispiel LDIF sales.ldif

```
dn: uid=ahueser, ou=Sales, dc=structure-net, dc=de
objectclass: person
objectclass: organizationalperson
cn: Axel Hueser
sn: Hueser
uid: ahueser
mail: ahueser@structure-net.de
l: Hamburg
postalcode: 21033
streetadress: billwiese 22
telephonenumber: 040-7654321
facsmiletelephonenumber: 040-7654321

dn: uid=jwiener, ou=Sales, dc=structure-net, dc=de
objectclass: person
objectclass: organizationalperson
cn: Jared Wiener
sn: Wiener
uid: jwiener
mail: jwiener@structure-net.de
l: Hamburg
postalcode: 21033
streetadress: billwiese 22
telephonenumber: 040-7654321
facsmiletelephonenumber: 040-7654321
```

6.1.3 Beispiel LDIF development.ldif

```
dn: uid=tbendler, ou=Development, dc=structure-net, dc=de
objectclass: person
objectclass: organizationalperson
objectclass: inetorgperson
cn: tbendler
cn: Systemverwalter
cn: Thomas Bendler
sn: Bendler
uid: tbendler
mail: tbendler@structure-net.de
l: Hamburg
postalcode: 21033
streetadress: billwiese 22
telephonenumber: 040-7654321
facsmiletelephonenumber: 040-7654321

dn: uid=tlippert, ou=Development, dc=structure-net, dc=de
objectclass: person
objectclass: organizationalperson
cn: Thomas Lippert
sn: Lippert
uid: tlippert
mail: tlippert@structure-net.de
l: Hamburg
postalcode: 21033
streetadress: billwiese 22
telephonenumber: 040-7654321
facsmiletelephonenumber: 040-7654321
```

6.1.4 Beispiel LDIF support.ldif

```
dn: uid=emueller, ou=Support, dc=structure-net, dc=de
objectclass: person
objectclass: organizationalperson
cn: Elmar Mueller
sn: Mueller
uid: emueller
mail: emueller@structure-net.de
l: Hamburg
postalcode: 21033
streetadress: billwiese 22
telephonenumber: 040-7654321
facsmiletelephonenumber: 040-7654321

dn: uid=elemke, ou=Support, dc=structure-net, dc=de
objectclass: person
objectclass: organizationalperson
cn: Enrico Lemke
sn: Lemke
uid: elemke
mail: elemke@structure-net.de
l: Hamburg
postalcode: 21033
```

```
streetadress: billwiese 22
telephonenumber: 040-7654321
facsmiletelephonenumber: 040-7654321
```

Die vorgestellte Datenbank ist natürlich weder sonderlich umfangreich noch besonders trickreich. Doppelte Datensätze wie z.B. Admin und Bendler, die sich auf die selbe Person beziehen, können auch über Verweise aufgelöst werden. So kann man z.B. eine Gruppe People erstellen, in der man alle bekannten Personen unterbringt. In den Gruppen Sales, Development und Support trägt man dann Verweise auf diese Personen ein.

6.2 Umwandeln der LDIF Datei in das LDBM Format

Als nächstes muß die LDIF Datei ins LDBM Format konvertiert werden. Dazu dient der Befehl `ldif2ldbm`. In der SuSE Distribution ist dieser unter `/usr/sbin/` zu finden. Der Befehl lautet also:

```
ldif2ldbm -i /etc/openldap/ldif/firmenstruktur.ldif \
          -f /etc/openldap/slapd.conf
```

Sollten sich irgendwelche Dateien nicht in den Standardpfaden befinden, so kann man so nach den Dateien suchen lassen:

```
find / -name <Dateiname>
```

Ist die LDIF Datei konvertiert, muß der LDAP Server gestartet werden. SuSE stellt dafür ein init-Skript zur Verfügung:

```
/sbin/init.d/ldap start
```

Wenn der LDAP Server wunschgemäß läuft, kann dieser auch automatisch gestartet werden, indem man die Variable START_LDAP in der `rc.config` auf yes setzt.

Ist kein Startskript vorhanden, wird der LDAP Server mit folgendem Kommando gestartet:

```
slapd -f /usr/local/etc/openldap/slapd.conf
```

6.3 Testen des LDAP Servers

Um den LDAP Server zu testen, kann man jetzt eine Anfrage an selbigen schicken. Dies geschieht mit folgendem Befehl:

```
ldapsearch objectclass=\*
```

Der Server sollte nun eine Struktur, wie in der Datei `firmenstruktur.ldif` beschrieben, als Rückantwort übergeben.

6.4 Hinzufügen von Datensätzen

Nun gehts an das Hinzufügen von Datensätzen. Dazu werden die bereits erstellten LDIF Dateien benutzt. Das Hinzufügen geschieht mit Hilfe des Befehls `ldapadd`. Dies geschieht folgendermaßen:

```
ldapadd -v -D dn="uid=admin,dc=structure-net,dc=de" \
        -w secret -f /etc/openldap/ldif/sales.ldif
ldapadd -v -D dn="uid=admin,dc=structure-net,dc=de" \
        -w secret -f /etc/openldap/ldif/development.ldif
ldapadd -v -D dn="uid=admin,dc=structure-net,dc=de" \
        -w secret -f /etc/openldap/ldif/support.ldif
```

Auf diese Weise können auch weitere Einträge hinzugefügt werden. Eine etwas komfortablere Variante stellt das X.500 Webgateway, da welches als Frontend beschrieben wird.

7 Tuning des LDAP Servers

Es gibt unterschiedliche Möglichkeiten, den LDAP Server zu tunen. Die Möglichkeiten, den LDAP Server zu tunen, beziehen sich in erster Linie auf die LDBM Datenbank. Deutliche Performancegewinne lassen sich aber erst in Verbindung mit großen Datenbeständen erzielen. Das *The SLAPD and SLURPD Administration Guide* bietet einen Überblick der Möglichkeiten zum Tunen des LDAP Servers. Weitere Informationen finden sich im FAQ-O-MATIC auf der Homepage des OpenLDAP Projektes.

8 Frontends für den LDAP Server

Da auf Dauer die Bedienung des LDAP Servers mit Hilfe der mitgelieferten Tools wie z.B. `ldapmodify` relativ umständlich ist, sehnt man sich nach einem grafischen Interface zur Modifizierung und Abfrage der LDAP Datenbank. Ich habe dazu das X.500 Webgateway installiert. Das X.500 Webgateway bietet eine komfortable Möglichkeit, auf den LDAP Server via einem Browser zuzugreifen. Es erlaubt auch die Paßwort gestützte Modifikation der Einträge.

8.1 Installation von Web500gw

Das Web500gw wird von Frank Richter, Technische Universität Chemnitz entwickelt. Es basiert auf dem Gopher-LDAP Gateway (go500gw) Implementierung von Tim Howes. Erweiterungen stammen von Mark Smith, Rakesh Patel, Rutgers University und Hallvard B Furuseth, Universität Oslo. Das Web500gw kann unter folgender Adresse bezogen werden:

```
ftp.tu-chemnitz.de/pub/Local/urz/web500gw/web500gw.tgz
```

Die Installation des Quellcodes wird in der mitgelieferten `INSTALL`-Datei beschrieben. Ich gehe im folgenden nicht auf die Installation des Gateways ein, da dies den Rahmen des Dokumentes sprengen würde. Dem geneigten Benutzer sei die Online Hilfe empfohlen, die unter

```
http://www.tu-chemnitz.de/~fri/web500gw/
```

zu finden ist. Die Benutzer von SuSE Linux haben es dort ein bißchen einfacher. Sie müssen nur web500gw aus der Serie n installieren. Das Gateway kann dann kompfortabel über das Skript `/sbin/init.d/webgw` gestartet werden. Soll das Gateway automatisch beim Hochfahren gestartet werden, muß es in die Datei `rc.config` eingetragen werden. Alternativ kann das Gateway auch mit `web500gw` gestartet werden. Dies bietet sich auch zur Fehlersuche an, da man mit den Parametern `-v -d 32` das Verhalten des Gateways kontrollieren kann.

8.2 Konfiguration von Web500gw

Nach der Installation von Web500gw muß das Gateway konfiguriert werden, damit es den lokalen Gegebenheiten Rechnung trägt. Wesentlich hierfür ist die Datei `web500gw.conf` im Verzeichnis `/etc/web500`. Bei SuSE wird web500gw standardmäßig unter `/usr/local` installiert. Im folgenden habe ich eine beispielhafte Konfigurationsdatei für den Beispiel LDAP Server abgedruckt. Das Anpassen der restlichen Konfigurationsdateien ist optional. Eine entsprechende Dokumentation ist in der Online Hilfe zu finden.

8.3 Die web500gw.conf

```
#
# web500gw.conf erstellt von Thomas Bendler 13.08.1999
#

# Standard Port für web500gw - dies kann durch das Flag -p geändert werden
port: 8888

# Standard LDAP Server - dies kann durch das Flag -x geändert werden
ldapserver: ldap.structure-net.de

# Standard LDAP Port - dies kann durch das Flag -P geändert werden
ldapport: 389

# Erlaube die Nutzung von anderen LDAP Servern
otherservers: no

# Maximales Zeitlimit für LDAP Anfragen in Sekunden
timelimit: 30

# Maximale Anzahl der Ergebnisse bei Anfragen außerhalb der Basis DN.
sizelimit: 0

# Standard Basis DN
# kann durch die ACCESS Regeln geändert werden
homedn: dc=structure-net,dc=de

# Was macht web500gw, wenn keine Basis DN angegeben wurde
rootishome: on: /M = "dc=structure-net,dc=de", / = "X.500 root"

# Anbindung über spezifizierte DN
# kann durch die ACCESS Regeln geändert werden
web500dn: dc=structure-net,dc=de

# ... und das Paßwort für web500dn (simple auth)
web500pw:

# Anzeige eines Eintrages, wenn Suche erfolgreich war
showonematch: yes

# Try a UFN search if a search value contains a comma
# Boolean value - Default is yes
ufnsearch: on

# Durchsuche Subtree nach folgenden Klassen
```

```
subsearch: organization, organizationalUnit

# Send "Last-Modified:" HTTP header if entry has a "lastModifiedTime"
# attribute. Boolean value - Default is yes
lastmodified: on

# Send "Expire:" HTTP header: default: -1 == don't expire
# 0 == expire now (no caching), > 0 == expire after seconds
expires: 3600

# Pfad der Dateien
etcdir:       /etc/web500

g3togif: /usr/local/bin/g3togif
jpegtogif: /usr/bin/djpeg -gif

# wenn Robots anfragen sende folgende Zeile
robots: User-agent: *
Disallow: /

# Maximale Anzahl von Werten für ein Attribut
maxvalues: 5

# access: Name : Pattern : rights : sizelimit : def-lang : Ho-
medn : Bind_as : Bind-PW : suffix

access: Local       : .*\.structure-net\.de$ : full : 50 : de : : : :.internal
access: German      : .*\.de$                : read : 50 : de : c=DE :::
access: World       : .*                     : read : 50 : en : / : : :

# language: HTTP-Content-Language : pattern for Accept-Language : suf-
fix for lang spec files
language: de : de.* : .de
language: fr : fr.* : .fr
language: en : .* :

# Browser abhängige Konfiguration
#browser: Name : User-Agent pattern : options : def. display flags : navigation
browser: Mozilla : Mozilla/* : html32           : table   : top,menu
browser: Lynx    : Lynx.*    : forms,mailto     : oneline : bottom,small
browser: Other   : .*        : forms,mailto,img : list    : top,list
```

8.4 Zugriff auf Web500gw

Auf das Web500gw kann mit jedem handelsüblichen Browser zugegriffen werden. In dem Beispiel ist die URL folgende:

```
http://ldap.structure-net.de:8888/
```

Wenn das Gateway richtig konfiguriert ist, sollte nun ein Auswahlmenü erscheinen. Dort ist auch die Online Hilfe integriert.

8.5 Weitere Konfigurationsdateien

Um das Gateway an die lokalen Gegebenheiten anzupassen, sollte man einen Blick in die restlichen Konfigurationsdateien werfen und zum Beispiel Vorgaben und E-Mail Adressen an die lokalen Gegebenheiten anpassen. Desweiteren kann auch eine Modifizerung der Templates notwendig sein, wenn man z.B. via member auf andere Einträge verweisst. Diese Einträge wurden in der Version, die mir vorlag, standardmäßig nicht angezeigt.

9 Client Zugriff auf LDAP

Beispielhaft für den Zugriff auf den LDAP Server sei hier der Netscape Communicator beschrieben. Der Communicator bietet unterschiedlich Möglichkeiten, um auf den LDAP Server zuzugreifen. Im folgenden werde ich mich auf die Abfrage der Adressen, die im Beispiel erzeugt wurden, beschränken. Da der LDAP Server in der Lage ist, fast alles in seiner Baumhierachie zu speichern, ist es natürlich auch möglich, Profile der einzelnen Benutzer zu speichern. Möglichkeiten und Wege dies zu realisieren, werde ich in einer zukünftigen Version dieses Dokumentes berücksichtigen.

9.1 Konfiguration des Netscape Communinicator

Die Konfiguration des Netscape Communicators gestaltet sich relativ einfach. Voraussetzung für die Benutzung des LDAP Servers ist eine Version ab 4.5.

Ist diese installiert, muß als erstes das Adressbuch geöffnet werden. Dies findet sich unter `communicator, adress book`. Nun öffnet sich ein Fenster, in dem bereits drei Verzeichnisse eingetragen sind: Netcenter, InfoSpace und Verisign. Ein Klick mit der rechten Maustaste auf `Netcenter` öffnet ein Popup Fenster, in dem `New Directory ...` ausgewählt werden muß. Nun müssen in das erscheinende Formular folgende Daten eingetragen werden (ich beziehe mich auf das Beispiel aus Sektion 4 und 5, gegebenfalls müssen die Einträge an die lokale Konfiguration angepaßt werden): eine Beschreibung des Dienstes unter `description` (z.B. Structure Net), der Name des `LDAP Servers` (`ldap.structure-net.de`) und zu guter letzt der `Server Root` (c=DE, c=US). In diesem Feld werden die Länder spezifiziert, die durchsucht werden. Optional kann noch das Feld `Login with name and password` aktiviert werden, falls die einzelnen Benutzer in der Lage sein sollen, Ihre Daten selbsttätig zu ändern.

Der LDAP Server kann jetzt über das search Feld befragt werden. Gibt man nun z.B. den Nachnamen an, erscheint eine Liste der Personen, die im sn Feld diesen Namen stehen haben.

9.2 Erweiterte Konfiguration

Um das Adressbuch an die lokalen Gegebenheiten anzupassen, sind noch weitere Einstellungen möglich. Eine detailierte Anleitung findet sich auf der Web-Site von Netscape unter folgender Adresse:

```
http://developer.netscape.com/docs/manuals/communicator/ldap45.htm
```

10 Nützliche Tools

Neben dem vorgestellten Netscape Communicator und Web500gw als Client bzw. Front End zum LDAP Server existieren noch weitere Tools, um die Arbeit mit dem LDAP Server zu erleichtern. Im folgenden habe ich ein paar zusammengestellt. Diese Liste erhebt keinen Anspruch auf Vollständigkeit.

10.1 LDAP Migration Tools

Die LDAP Migration Tools sind eine Sammlung von PERL-Skripten, die bei der Konvertierung von vorhandenen Datenbanken ins LDAP Format (bzw. ins LDIF Format) behilflich sind. So kann man z.B. die `/etc/passwd` Datei ins LDIF Format überführen. Die LDAP Migration Tools sind erhältlich unter:

    http://www.padl.com/tools.html

Die Migration Tools sind vor allem dann hilfreich, wenn man den LDAP Server z.B. zur Benutzer Authentifizierung nutzen will. Soll der LDAP Server nur als Adressbuch verwendet werden, sind die Tools nicht notwendig.

10.2 PAM LDAP Module

Um den LDAP Server als erste Instanz für User Authentifizierungen zu nutzen, wird ein gesicherter Transport vorausgesetzt. Dies wird mit Hilfe des Pluggable Authentification Module (PAM) API erreicht. Die PAM sind unter folgender Adresse erhältlich:

    http://www.padl.com/pam_ldap.html

10.3 kldap

Kldap ist ein Client für den LDAP Server, der z.B. die Struktur der Baumhierachie visualisieren kann. Um Kldap für SuSE Linux zu kompilieren, muß das Makefile angepaßt werden. Ein angepaßtes Makefile kann beim Autor bezogen werden (via E-Mail). Nährere Informationen und die Möglichkeit zum Download finden sich unter:

    http://www.mountpoint.ch/oliver/kldap

10.4 GQ

GQ ist das äquivalent für Kldap unter Gnome. Nährere Informationen und die Möglichkeit zum Download finden sich unter:

    http://biot.com/gq/

11 Weitere Quellen und Dokumentationen

Leider sieht die derzeitige Situation in Bezug auf die LDAP-Dokumentation nicht sehr rosig aus. Es gibt zwar die ein oder andere brauchbare Dokumentation, sie sind allerdings nicht einfach zu finden. Ich habe daher eine Link Liste und eine Bücherliste mit Informationen zu LDAP zusammengestellt, auf die sich im wesentlichen auch dieses HOWTO stützt. In diesem Zusammenhang möchte ich mich auch nochmal für hilfreiche Beiträge aus dem USENET zu diesem Thema bedanken.

11.1 Adressen im Internet

OpenLDAP HomePage

    http://www.openldap.org/

LDAP Einführung im Linux Magazin

`http://www.linux-magazin.de/ausgabe.1998.09/LDAP/ldap.html`

slapd und slurpd Administrator´s Guide

`http://www.umich.edu/~dirsvcs/ldap/doc/guides/`

Introducing to Directory Service (X.500)

`http://www.nic.surfnet.nl/surfnet/projects/x500/introducing/`

Linux Driectory Service

`http://www.rage.net/ldap/`

11.2 Bücher

- Implementing LDAP by Mark Wilcox
- LDAP: Programming Directory-Enabled Applications with Lightweight Directory Access Protocol by Howes and Smith
- Understanding and Deploying LDAP Directory Servers by Howes, Smith, and Good

11.3 RFC´s

- RFC 1558: A String Representation of LDAP Search Filters
- RFC 1777: Lightweight Directory Access Protocol
- RFC 1778: The String Representation of Standard Attribute Syntaxes
- RFC 1779: A String Representation of Distinguished Names
- RFC 1781: Using the OSI Directory to Achieve User Friendly Naming
- RFC 1798: Connectionless LDAP
- RFC 1823: The LDAP Application Programming Interface
- RFC 1959: An LDAP URL Format
- RFC 1960: A String Representation of LDAP Search Filters
- RFC 2251: Lightweight Directory Access Protocol (v3)
- RFC 2307: LDAP as a Network Information Service