LDAPv3 (Lightweight Directory Access Protocol)

- Kurzakte -

Konfiguration des Servers

Installation	
• Installation der Pakete openldap2, openldap2-client, nss_ldap, pam_ldap, yast2_ldap_client, ldapcpplib als Mindestvoraussetzung • grafische Tools: directory_administrator (LDAP-Manager), gq (LDAP-client für GTK)	
Konfiguration	
/usr/sbin/slapd	• Binärdatei des Serverdienstes
/etc/openldap/slapd.conf	• Serverkonfigurationsdatei • Laden der Schemata mit Klassen- und Attributdefinitionen und Access Controls
/var/lib/ldap/	• enthält die Dateien der laufenden LDAP-Datenbank und DB_CONFIG
/etc/openldap/ldap.secret	• enthält das Passwort für das simple bind von PAM • nur in Verbindung mit der Anweisung rootbinddn in der ldap.conf möglich
/etc/openldap/schema	• Schemadateien für Objekte und Attribute der Datenbank
/etc/openldap/certificates	• Ablegen des Server-Zertifikats für eine SSL-Verbindung zum LDAP-Server
Start als Stand-Alone-Dienst	
zum Test per Hand: `/usr/lib/openldap/slapd -f /etc/openldap/slapd.conf -h ldap://127.0.0.1:389 -u ldap -g ldap –d 4` (f für conf-Datei, h für Prot0koll, IP und Port, u und g für Identität des Dienstes, d für Log-Level)	
/etc/init.d/ldap rcldap (SUSE)	• start | stop | restart | reload | status - Skript startet/stoppt ldap manuell • Schnelltest mit ldapsearch -x
insserv ldap (SUSE) chkconfig ldap	• automatischer Start durch Symlink im Runlevelverzeichnis • alternativ mit Runleveleditor im Yast
/etc/sysconfig/openldap	• enthält bei SUSE die Startparameter für das init-Skript
Kontrolle	
/var/log/messages	• hier landen die Log-Meldungen
strings /var/lib/ldap/*	• prüft die LDAP-Datenbank auf Inhalt
Hilfsprogramme zum SLAPD-Servermanagement	
slappasswd -u	• erzeugt verschlüsseltes Passwort - SSHA (default), SHA, CRYPT, MD5, SMD5 • wird mittels cut and paste in die slapd.conf bei rootpw eingetragen
slapcat	• wandelt den Inhalt der SLAPD-Datenbank ins LDIF-Format um (für slapadd)
slapadd	• fügt Einträge im LDIF-Format (z.B. von slapcat) zur LDAP-Datenbank hinzu
db_recover	• repariert defekte Datenbank
Hilfsprogramme (LDAP-Clients) zum Management der LDAP-Datenbank	
ldapadd	• Hinzufügen von Objekten zur LDAP-Datenbank in Form einer LDIF-Datei (oder mehrere) • LDAP arbeitet mit UTF-8 (Unicode) → evtl. iconv zum Umkodieren verwenden. `ldapadd –c -x -D <dn des Administrators> -W -f <datei>.ldif`
ldapmodify	• Modifizieren eines bestehenden Datensatzes • Syntax wie ldapadd • ohne Option –f sind Änderungen direkt von der Shell möglich
ldapmodrdn	• Umbenennen kompletter Objekte • In der 1. Zeile der ldif-Datei wird der DN angegeben und in der 2. nur der neue Name

ldapsearch	• Durchsuchen und Auslesen von Daten
	`ldapsearch –s scope –h host –p port –b base filter`
	`ldapsearch -x -b dc=...,dc=de "(objectClass=*)"`
	`ldapsearch -x -D "cn=Manager,dc=bla,dc=de" –W`
	`ldapsearch sn=Meier homephone`

ldapdelete	• Löschen von Datensätzen `ldapdelete -x -D <dn des Administrators> -W cn=username,ou=abteilung,dc=...,dc=de`
ldappasswd	• Setzen des verschlüsselten Benutzerpassworts in der LDAP-Datenbank `ldappasswd –x –D“cn=…,dc=…“ –W -S`
Dokumentation	
man: slapd-bdb (5) slapd-ldbm (5), slapd.access (5), slapd.conf (5), slapd.plugin (5), slapd.replog (5), slapadd (8), slapcat (8), slapd (8), slapindex (8), slappasswd (8), slurpd (8),	

Elemente des Directory Information Tree (DIT)

Container
Root (Wurzelelement des Verzeichnisbaums, das nicht real existiert),
c (country),
o (Organization)
ou (OrganizationalUnit), und
dc (domainComponent).
Blatt Diese Objekte sitzen am Ende eines Astes. Ihnen sind keine anderen Objekte untergeordnet. Beispiele sind Person, InetOrgPerson oder groupofNames.

Schemata zur Festlegung der Objekttypenzur LDAP-Organisation

```
Core.schema                zwingend erforderlich
organizationalPerson       optional: Adressfelder, Faxnummer
inetorgperson.schema       optional: Internetattribute wie Mail, URL, Zertifik.
nis.schema                 optional: enthält Objekt posixAccount
cosine.schema und rfc2307bis.schema    zum Ersatz von NIS
Weitere verfügbare Schemata im Verzeichnis /etc/openldap/schema/.
Achtung: unbedingt die Reihenfolge im Sinne der Vererbungslinien beachten (schema-
files lesen! – SUP-Deklarationen der Oberklasse)
```

/etc/slapd.conf

1. Schemata

```
include /etc/openldap/schema/core.schema
```

2. Zugangsregeln

```
access to <what> by <who> <access>
```

Beachte: Falls keine „access to"-Regel oder keine „by <who>"-Anweisung greift, ist der Zugriff verboten.

<what> (Objekt oder Attribut der Zugangsregelung)

Reihenfolge beachten – erste zutreffende Regel gilt (spezielle Regeln zuletzt)

- ganze Verzeichnisäste
- ganze Regionen mit regexp

<who> (zugangsberechtigte Benutzergruppen)

Reihenfolge beachten – erste zutreffende Regel gilt

- ausnahmslos alle Benutzer
- anonymous nicht authentifizierte („anonyme") Benutzer
- users authentifizierte Benutzer
- self Benutzer, die mit dem Zielobjekt verbunden sind
- dn.regex=<regex> Alle Benutzer, auf die dieser reguläre Ausdruck zutrifft

<access> (Art des Zugriffs)

Werden dort höhere oder gleiche Rechte gewährt als der Client anfordert, wird dem Client der Zugang erlaubt. Fordert der Client höhere Rechte als dort angegeben, erhält er keinen Zugang.

- none Zutritt verboten
- auth x zur Kontaktaufnahme (z.B. Kennwortzugriff zur Authentifiz., aber kein Lesezugriff)
- compare c zum vergleichenden Zugriff auf Objekte
- search s zur Anwendung von Suchfiltern (kein Suchergebnis, nur Erfolgsaugabe)
- read r Leserecht (Ausgabe eines Suchergebnisses)
- write w Schreibrecht

```
Beispielsregel :
access to dn.regex="ou=([^,]+),dc=suse,dc=de"
by dn.regex="cn=administrator,ou=$1,dc=suse,dc=de" write
by user read
by * none
```

Diese Regel besagt, dass zu allen ou-Einträgen nur der jeweilige Administrator schreibenden Zugang hat. Die übrigen authentifizierten Benutzer sind leseberechtigt und der Rest der Welt erhält keinen Zugang.

Datenbankspezifische Anweisungen in slapd.conf

```
database bdb                        # Datenbanktyp (auch: meta für Metatree)
directory /var/lib/ldap             # Pfad auf die Datenbank
allow bind_v2                       # Zugriff älterer Client-Progs gestatten
suffix "dc=sonne,dc=de"             # Verantwortlichkeitsbereich des Servers
rootdn "cn=admin,dc=sonne,dc=de"    # Festlegen des Administrators
rootpw secret                       # Klartextpasswort des Administrators
index objectClass eq                # definiert zu indizierende Attribute
```

LDIF – LDAP Data Interchange Format

Syntax:

- eine Zeile muss am Zeilenanfang beginnen (keine Leerzeichen erlaubt)
- jeder Datensatz wird durch eine Leerzeile getrennt
- jedes Attribut auf eine extra Zeile
- Keine Leerzeichen am Zeilenende (Datenkette wird sonst nach Base64 kodiert)
- Leerzeilen dürfen keine Tabs oder Leerzeichen enthalten!!!
- das Eingabeformat muss UTF-8 sein (umwandeln mit iconv oder mmencode –Base 64-)

Aufbau

- es ist erforderlich, immer die Objektklasse top anzugeben (generelle Klasse ohne eigenen MUST-Attribute)
- es ist mindestens eine Klasse neben "top" erforderlich
- in einem Eintrag darf nur **eine** STRUCTURAL-Klasse aufgerufen werden (aber mehrere AUXILIARY)
- Vererbungslinie bei den Objektklassen beachten (zuerst Objekte der Root-Klasse)
- das Attribut zum Aufbau des Distinguished Name muss noch einmal in der Attributliste auftauchen
- MUST-Attribute der Objektklassen müssen vorhanden sein, MUST-Attribute sind kumulativ

Bsp.:
objectclass: inetorgperson
objectclass: posixgroup
→ ungültiger Eintrag, da die Objektklasse posixgroup eine als STRUCTURAL deklarierte Klasse ist und nicht von person abstammt (nis.schema)

Beispiel für eine LDIF-Datei

```
# Die Organisation FOOBAR
dn: dc=foobar,dc=de
objectClass: dcObject
objectClass: organization
o: FOOBAR AG
dc: foobar
# Die Organisationseinheit Entwicklung (devel)
dn: ou=devel,dc=foobar,dc=de
objectClass: organizationalUnit
ou: devel
# Die Organisationseinheit Dokumentation (doc)
dn: ou=doc,dc=foobar,dc=de
objectClass: organizationalUnit
ou: doc
# Die Organisationseinheit Interne EDV (it)
dn: ou=it,dc=foobar,dc=de
objectClass: organizationalUnit
ou: it
```

```
ldapadd -x -D cn=admin,dc=foobar,dc=de -W -f beispiel.ldif
Enter LDAP password:
adding new entry "dc=foobar,dc=de"
adding new entry "ou=devel,dc=foobar,dc=de"
adding new entry "ou=doc,dc=foobar,dc=de"
adding new entry "ou=it,dc=foobar,dc=de"
```

Tools:

- **MigrationTools** von www.padl.com wandelt Systemdateien (passwd, group, shadow, hosts) ins LDIF-Format (Konfigdatei migrate_common.ph – Anpassen vor allem der Vaiablen DEFAULT_MAL_DOMAIN, DEFAULT_BASE, DEFAULT_MAIL_HOST)
    - Tipp: ./migrate_all_online bei laufendem LDAP-Server
- **cpu** von cpu.sourceforge.net erzegt komfortabel neue Posix-User und –Gruppen:
  cpu useradd paul (Konfigdatei /etc/cpu.cfg)

Konfiguration des Clients (auch auf LDAP-Server selbst !)

<table>
<tr><th colspan="2">Installation</th></tr>
<tr><td colspan="2">Installation der Pakete pam_ldap und nss_ldap
pam_ldap: für die Vermittlung zwischen Loginprozessen und LDAP-Verzeichnis
nss_ldap: Anpassung der Namensauflösung der glibc über den nsswitch-Mechanismus</td></tr>
<tr><th colspan="2">Konfiguration</th></tr>
<tr><td>/etc/openldap/ldap.conf
export LDAPCONF=…</td><td>• setzt systemweite Standardwerte für die LDAP-Clients (Zugriff auf libldap.so)
• enthält Infos (IP, Port, Wurzel) für LDAP-Kommandozeilenprogramme, das LDAP-PAM- und das Yast-LDAPModul
• alternativ über Variable LDAPCONF (in /etc/profile)</td></tr>
<tr><td>~/.ldaprc</td><td>• optionales userspezifisches Konfigurationsfile, dass die systemweiten Standardwerte überschreibt</td></tr>
<tr><td>/etc/ldap.conf</td><td>• Konfigurationsdatei für die LDAP-PAM-Module (pam_ldap.so), den LDAP-Nameservice (nss_ldap) und das shadow-package</td></tr>
<tr><td>/etc/pam.d/</td><td>• Hauptkonfigurationsverzeichnis der Konfigurationsdateien für Pluggable Authentication Modules (PAM)
• Definition von PAM-Authentifizierungsregeln für jeden Login-Dienst bzw. Programm gegen die frisch eingerichtete LDAP-Datenbank
• Beispielsdateien liegen unter /usr/share/doc/packages/pam_ldap/pam.d/
• Bsp.: Einfügen der folgenden Zeilen in die /etc/pam.d/sshd
<code>auth sufficient pam_ldap.so</code>
<code>password required pam_ldap.so use_authtok</code></td></tr>
<tr><td>/lib/security/pam_ldap.so</td><td>• Bibliothek für alle LDAP-Dienste</td></tr>
<tr><td>/etc/security/pam_unix2.conf</td><td>• konfiguriert das SUSE-eigene LDAP-fähige PAM-Modul
• Einfügen folgender Zeilen:
<code>auth: use_ldap nullok</code>
<code>account: use_ldap</code>
<code>password: use_ldap nullok</code>
<code>session: none</code></td></tr>
<tr><td>/etc/nsswitch.conf</td><td>• wird vom Modul nss_ldap aktualisiert
• Folgende Einträge:
<code>passwd: files ldap</code>
<code>shadow: files ldap</code>
<code>group: files ldap</code>
• weisen die Resolver-Bibliothek der glibc an, als Quelle für die Authentifizierung zuerst die lokalen und dann die ldap-Datenbank auszuwerten (Auflösung uid zu loginname)</td></tr>
<tr><td>/etc/passwd
/etc/group</td><td>• Soll verhindert werden, dass sich normale, per LDAP verwaltete Benutzer auf dem Server mit ssh oder login einloggen können, müssen /etc/passwd und /etc/group um eine Zeile ergänzt werden.
/etc/passwd um +::::::/sbin/nologin und
/etc/group um +:::</td></tr>
<tr><th colspan="2">Initialisierung der LDAP-Authentifizierung</th></tr>
<tr><td>/etc/init.d/nscd</td><td>• Neustart des Caching daemon für die LDAP-Anmeldung</td></tr>
<tr><th colspan="2">Kontrolle</th></tr>
<tr><td>getent passwd</td><td>• listet alle authentifizierbaren Accounts (lokal + ldap!)</td></tr>
<tr><th colspan="2">Dokumentation</th></tr>
<tr><td colspan="2">man: ldapadd (1), ldapcompare (1), ldapdelete (1), ldapmodify (1), ldapmodrdn (1), ldappasswd (1), ldapsearch (1), ldapwhoami (1), ldap.conf (5), ldif (5)</td></tr>
</table>