Servolution Logon Client 3.0 und LDAP

August 2002

Version 3.0 – Build 3.0.x.15

Inhaltsverzeichnis

1. Die LDAP-Funktionalitäten im Überblick 3
2. Die An- und Abmeldung eines Benutzers unter LDAP 4
Logon: 4
Logoff: 4
3. Zusätzliche LDAP Attribute 5
3.1 Das Comtarsia Schema 5
3.2 LDAP-Gruppen 6
3.3 LDAP Verzeichnis und Druckerfreigaben 6
3.4 Profile-Path und Home-Directory 8
3.5 Schritt für Schritt Konfiguration des LDAP Logon Client 9
4. Konfiguration eines OpenLDAP-Servers unter SuSE 8.0 Prof. zur Verwendung mit dem Servolution LDAP Logon Client 14

1. Die LDAP-Funktionalitäten im Überblick

Das Aktivieren der LDAP-Funktionalität des Logon Client ermöglicht die primäre Authentifizierung von Windows-Workstations gegen LDAP.
Dies bietet den Vorteil der zentralen User-Verwaltung im LDAP.
Gemeinsam mit dem Servolution SyncServer werden auch die User-Accounts auf den Ressource-Servern (OS/2, Windows NT/W2K Server, Samba) automatisch angelegt und das Passwort synchronisiert.
Bei Bedarf kann zusätzlich eine Anmeldung gegen eine OS2-Domain erfolgen.

Als Server kann so gut wie jeder LDAP-Server verwendet werden, ein Server mit Unterstützung für LDAP Version 3 wird empfohlen.
Es ist auch möglich einen IBM RACF-Server unter z/os einzusetzen (siehe LDAPServerTyp).

Die Kommunikation mit dem LDAP-Server kann mit SSL verschlüsselt werden und sollte nur im Testbetrieb unverschlüsselt erfolgen. (siehe LDAPEnableSSL)

Ähnlich wie bei OS/2 können bei LDAP zusätzlich zur Authentifizierung weitere User-Informationen abgefragt werden (Gruppenzugehörigkeit, File- und Printer Shares, Homedir), hierfür wird am LDAP-Server die Comtarsia Schema-Erweiterung benötigt (siehe Comtarsia -Schema).

Um eine erhöhte Verfügbarkeit der LDAP-Server zu erreichen, bietet der Client die Möglichkeit, automatisch Failover und LoadBalancing durchzuführen. Die Konfiguration des Clients kann entweder über die Registry oder über einen DNS-Server erfolgen. (siehe Failover und LoadBalancing und LDAPEnableDNS)

Erste Schritte:

- Falls noch kein LDAP-Server zur Verfügung steht, erklärt “ldap-suse” die Konfiguration eines OpenLDAP-Servers unter SuSE Linux Prof. 8.0.
- „quickstart“ beschreibt die notwendigen Schritte, um den Servolution Logon Client für einen LDAP-Login zu konfigurieren.
- „CookbookLDAPSSL“ beschreibt die Grundlagen von SSL, die notwendigen Schritte und Tools, um SSL-Zertifikate für die Clients sowie Server zu erstellen und diese richtig einzuspielen.

Viele Features des Servolution Logon-Clients wie z.B. diverse Exits für Script-Aufrufe stehen natürlich auch bei einer LDAP-Anmeldung zur Verfügung.

2. Die An- und Abmeldung eines Benutzers unter LDAP

Logon:

Nach Angabe im Logon Dialog von Username, Passwort und „LDAP LOGON“ als Domain und Bestätigung durch ENTER oder OK, wird der LDAP Logon gestartet.
Falls mehrere LDAP-Server zur Verfügung stehen und LoadBalancing/Failover aktiviert ist, werden die Server sortiert und der Reihe nach kontaktiert.
Wurde nur ein LDAP-Server in der Registry oder über DNS angegeben, wird immer dieser zum Logon verwendet.
Wird ein funktionierender LDAP-Server gefunden, wird das Paßwort am LDAP Server überprüft.
Stimmt die User/Paßwort Kombination am LDAP Server, wird ein LDAP-Server Logon durchgeführt, der lokale User wird vorbereitet.
Ist noch kein lokaler Benutzer vorhanden, wird dieser mit demselben Usernamen und Paßwort angelegt. Die Gruppenmitgliedschaft am LDAP Server wird abgefragt und nach Möglichkeit auch lokalen Gruppen zugewiesen;
z.B. ist der User am LDAP Server in der Gruppe „Hauptbenutzer“, wird er auch lokal Mitglied der Gruppe „Hauptbenutzer“.
Die Abfrage der Gruppen „PUSERS“ und „WSADMIN“ wird je nach Betriebssystemsprache auf die lokalen Gruppenmitgliedschaften von Hauptbenutzern/Administratoren durchgeführt bzw. auf die lokalen Gruppen Power User/Administrators übertragen;
z.B.: Ist der User im LDAP Mitglied der Gruppe WSADMIN, wird er Mitglied der lokalen Gruppe Administratoren.
Diese Gruppenmitgliedschaften lassen sich beliebig erweitern und werden bei jedem Logon auch auf bereits existierende User aktualisiert.

Die User-Assignments, Aliases, Printer und Homedir, des LDAP-Servers werden abgearbeitet und verbunden. (Das Comtarsia.schema wird hiefür benötigt).
Der Desktop wird für den User freigegeben.

Logoff:

Handelt es sich um einen Roaming User, wird das lokale User-Profil mit dem am Server gespeicherten Profil (\\Server\Homedir\profile) synchronisiert.

3. Zusätzliche LDAP Attribute

Gemeinsam mit dem Servolution Logon Client Version 3.0 stellt Comtarsia eine LDAP Schema-Erweiterung zur Verfügung, die eine weitergehende Konfiguration der Clients über den LDAP Server ermöglicht.
Folgende Werte können in der aktuellen Version vom LDAP-Server abgefragt werden:

- Gruppen
- Verzeichnis und Druckerfreigaben
- Profile-Path und Home-Directory

3.1 Das Comtarsia Schema

Das Comtarsia-Schema erweitert jene LDAP-Klasse, welche die User-Daten repräsentiert, z.B.: ‚person'.
Um die Default-Einstellung im Schema zu ändern, muss in der folgenden Zeile ‚person' durch die benötigte ObjectClass ersetzt werden:
objectclass (1.3.6.1. 4.1.13823.1.1.1 NAME 'CLCPerson' SUP person STRUCTURAL

Auf diese Art können File- und Printer-Shares sowie das Home-Directory des Useres über LDAP zugeordnet werden.

Konfiguration für OpenLDAP:
Erweitern von slapd.conf:
include /usr/local/openldap/etc/openldap/schema/comtarsia.schema

Die Datei comtarsia.schema muss in das in slapd.conf definierte Verzeichnis kopiert werden.

Im Verzeichnis „ldap" der Logon Client Distribution befindet sich eine Beispiel-Konfigurationsdatei eines OpenLDAP-Servers.

Die folgenden Objekt-Klassen werden im Comtarsia-Schema definiert und stehen im Logon-Client zur Verfügung:

```
objectclass ( 1.3.6.1.4.1.13823.1.1.1 NAME 'CLCPerson' SUP person
STRUCTURAL
      DESC 'Comtarsia Logon Client Person'
      MAY ( CLCProfilePath $ CLCShareName $ CLCNetworkApplicationName ) )

objectclass ( 1.3.6.1.4.1.13823.1.1.2 NAME 'CLCShare' SUP top STRUCTURAL
      DESC 'Comtarsia Logon Client Share'
      MUST ( CLCShareName $ CLCShareClientPort $ CLCShareRemotePath $
      CLCShareType $ CLCShareServer $ CLCShareRemoteDevice $
CLCShareDescription ) )
```

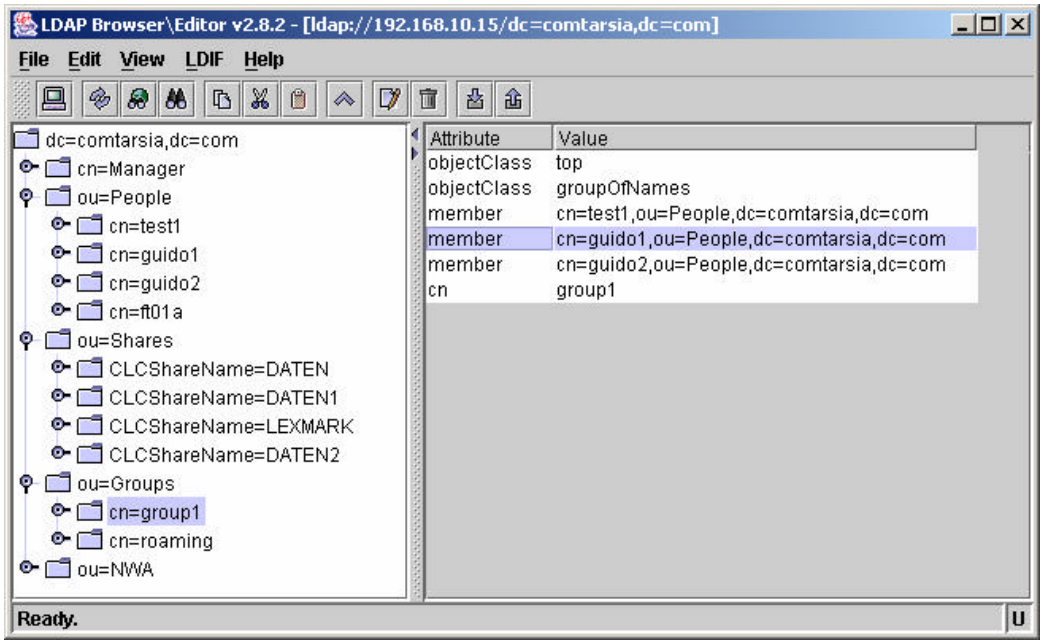
Die benötigte Objekt-Klasse für die Netzwerkapplikationen (allgemeine Beschreibung siehe im OS/2 Teil) sind bereits im Schema vorhanden, die derzeitige Version des LDAP Logon Clients unterstützt diese aber noch nicht.

3.2 LDAP-Gruppen

In der aktuellen Version es LDAP Logon Clients werden Gruppenobjekte vom Typ „objectClass=groupOfNames“ unterstützt. Dieses Klasse besitzt ein Multivalue-Attribut names „members“, in welchem die einzelnen User-DNs der Mitglieder der Gruppe aufgeführt sind. In zukünftigen Versionen wird die Objekt-Klasse sowie der Name des „member“-Attributes frei in der Registry definierbar sein.

Bei einer Anmeldung an einen LDAP-Server werden alle verfügbaren Gruppen nach der UserDN durchsucht und es werden alle Gruppen, in denen der aktuelle User Mitglied ist, an den Logon-Client übergeben. Die weitere Verwendung der Gruppen erfolgt analog zu OS/2-Gruppen.

Es werden maximal 251 Gruppen pro User unterstützt.

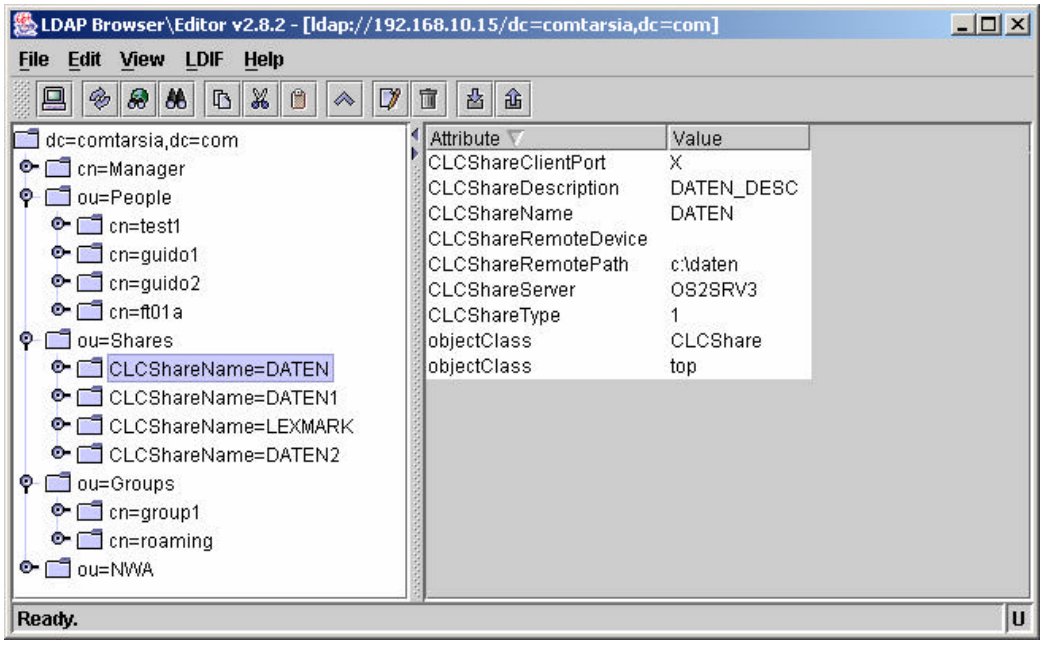


3.3 LDAP Verzeichnis und Druckerfreigaben

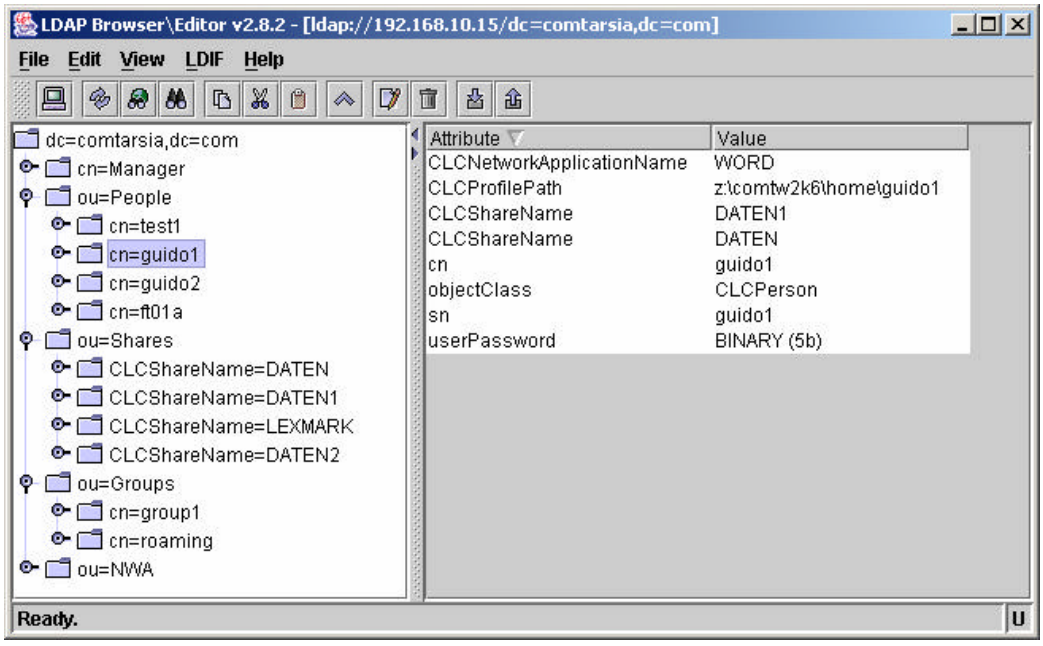
Mithilfe der im Comtarsia-Schema definierten Objekt-Klasse 'CLCShare' können Verzeichnis- und Drucker-Shares am LDAP-Server definiert werden. Diese können Personen-Objekten vom Typ ‚CLCPerson’ zugeordnet werden.
Vorhandene Zuordnungen werden bei einem LDAP-Logon automatisch abgefragt und entsprechend der Angaben auf der Workstation verbunden.

Es werden maximal 25 Driectory-Shares sowie 9 Drucker-Shares (LPT1 – LPT9) unterstützt.

Dieser Screenshot zeigt die Definition einer Verzeichnisfreigabe am LDAP-Server:



Hier sieht man die Zuordnung eines Shares zu einem User:



3.4 Home-Directory- und Profile-Path

Dem Logon Client kann über eine Variable der Home-Directory- und Profile-Pfad sowie der lokale Laufwerksbuchstabe zugewiesen werden.
Das Benutzerprofil wird im Unterverzeichnis „Profile“ abgelegt.

Der Logon Client unterstützt vier Interpretationen der Home-Directory Zeichenkette.

1.) OS/2 Syntax ohne Drive Letter

\\OS2SRV3\C$\HOME\USER1
Interpretation:
Der nächste freie Laufwerksbuchstabe wird dem UNC Pfad \\OS2SRV3\HOME\USER1 zu gewiesen.
Der Profile-Pfad wird auf \\OS2SRV3\HOME\USER1\PROFILE eingestellt.

2.) OS/2 Syntax mit Drive Letter

H:\OS2SRV3\C$\HOME\USER1
Interpretation:
Der Laufwerksbuchstabe H: wird dem UNC Pfad \\OS2SRV3\HOME\USER1 zu gewiesen.
Der Profile-Pfad wird auf \\OS2SRV3\HOME\USER1\PROFILE eingestellt.

3.) UNC Pfad ohne Drive Letter

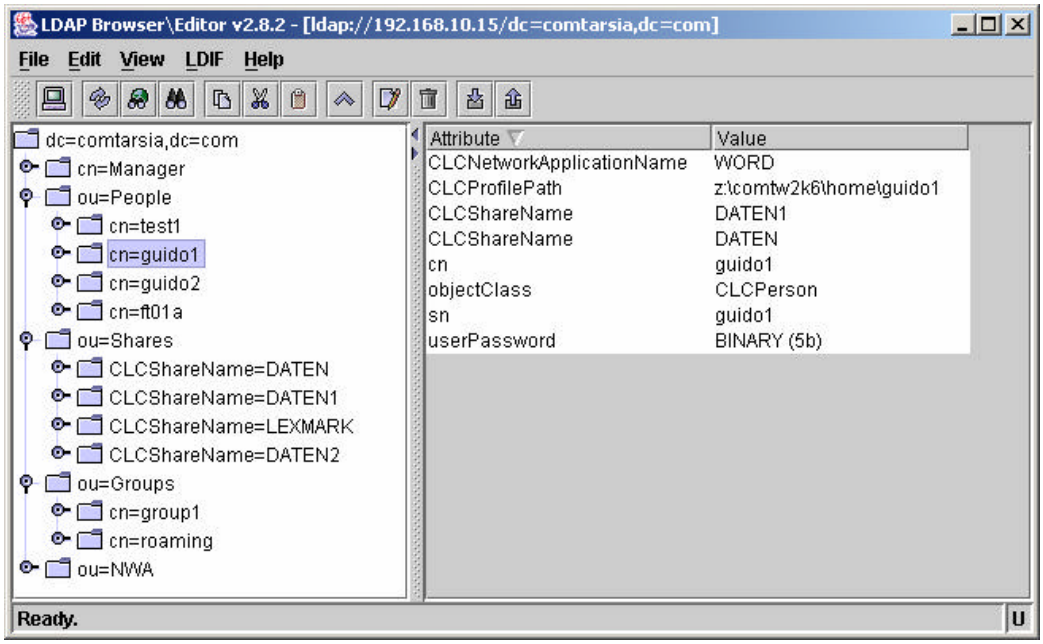
\\COMTW2K\HOME\USER1
Interpretation:
Der nächste freie Laufwerksbuchstabe wird dem UNC Pfad \\COMTW2K\HOME\USER1 zu gewiesen.
Der Profile-Pfad wird auf \\COMTW2K\HOME\USER1\PROFILE eingestellt.
Vorsicht: Das „$“-Zeichen darf in dieser Variante nicht verwendet werden!

4.) UNC Pfad mit Drive Letter

H:\COMTW2K\HOME\USER1
Interpretation:
Der Laufwerksbuchstabe H: wird dem UNC Pfad \\COMTW2K\HOME\USER1 zu gewiesen.
Der Profile-Pfad wird auf \\ COMTW2K \HOME\USER1\PROFILE eingestellt.
Vorsicht: Das „$“-Zeichen darf in dieser Variante nicht verwendet werden!

Die Home-Directory-String wird im Attribut “CLCProfilePath” des “CLCPerson”-Objektes gespeichert. Das Attribut wird bei einer LDAP-Anmeldung automatisch ausgelesen.

Screenshot eines „CLCPerson“-Objektes mit zugewiesenem ProfilePath:



3.5 Schritt für Schritt Konfiguration des LDAP Logon Client

Dieses Kapitel beschreibt die notwendigen Konfigurationsschritte, um sich mit dem Servolution Logon Client an einem LDAP-Server anzumelden. Es wird hier nur einen Minimalkonfiguration mit SSL beschrieben, Informationen zu weiteren Konfigurationsmöglichkeiten finden sich hauptsächlich in „Zusätzliche LDAP Attribute“ sowie „LDAP Load Balancing“.

Voraussetzungen:
Client: Windows 2000/XP Workstation
Server: LDAP Version 3 Server

Am LDAP-Server muss ein Benutzer-Account für den LDAP-Login bereitstehen.

Nach der Installation des Logon-Clients (siehe Servolution_LogonClient_3.0.doc) müssen die folgenden Registry Variablen angepaßt werden (bevor der Computer neu gestartet wird):

LDAPBaseDN: die BaseDN des LDAP-Trees (z.B.: dc=comtarsia,dc=com)
LDAPEnableSSL: 0 für kein SSL, 1 für SSL Support
LDAPUserDNPrefix: Teil der UserDN vor dem Usernamen
LDAPUserDNSuffix: Teil der UserDN nach dem Usernamen bis zur BaseDN

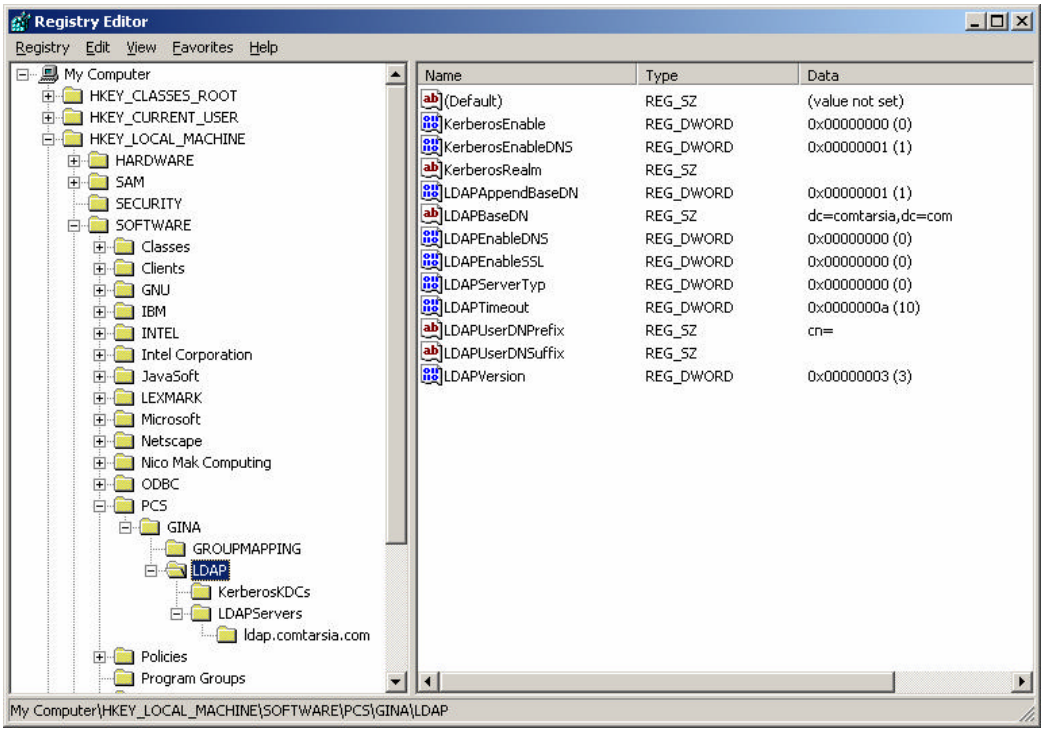
z.B.: UserDN „cn=user,dc=comtarsia,dc=com“
LDAPUserDNPrefix: „cn=“

LDAPUserDNSuffix: „“
LDAPBaseDN: „dc=comtarsia,dc=com“

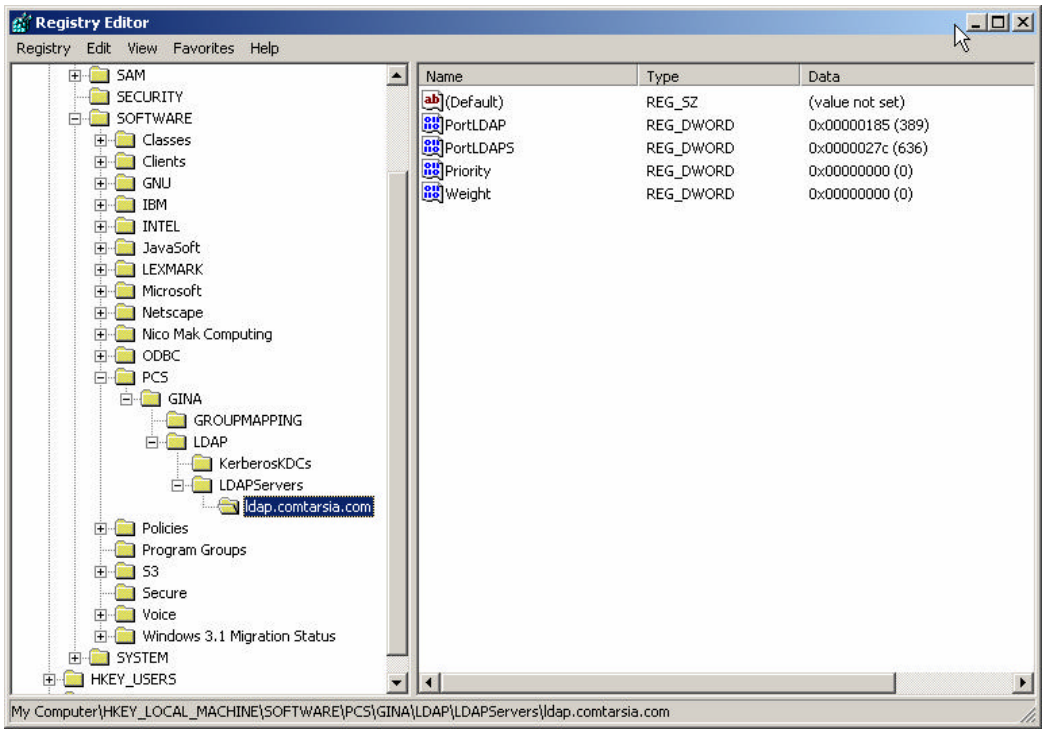
Weite Informationen zu den Registry-Einstellungen finden sich direkt bei der Beschreibung der einzelnen Registry-Werte im Handbuch (siehe Servolution_LogonClient_3.0.doc).

Für einen RACF-LDAP-Server muss der LDAPServerTyp auf „4“ gesetzt werden.

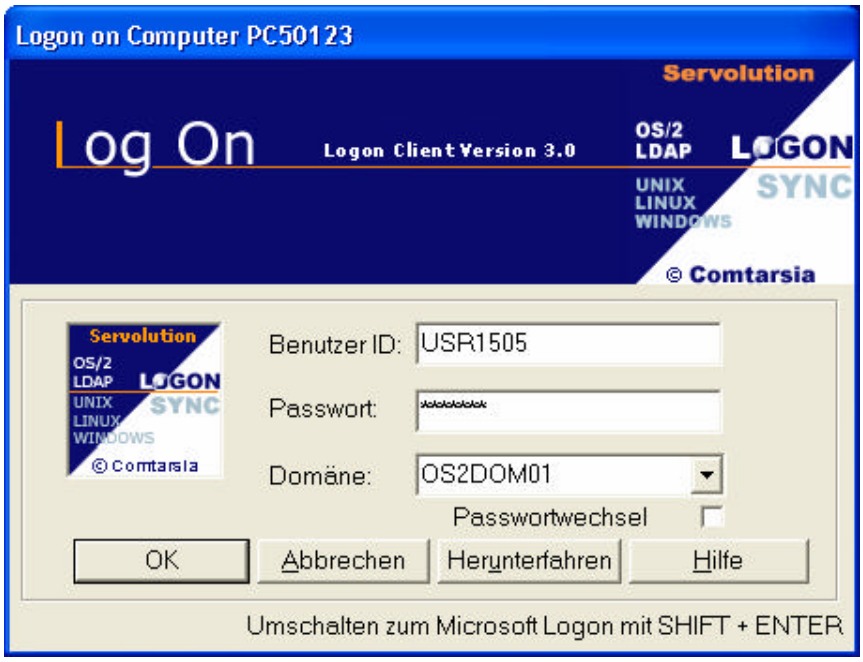
Wenn s ich der Client mit SSL zum Server verbinden soll, muss LDAPEnableSSL auf „1“ gesetzt werden. Weiterführende Informationen zu SSL mit dem Logon Client finden sich in der Datei „CookbookLdapSSLLogonClient.doc“.



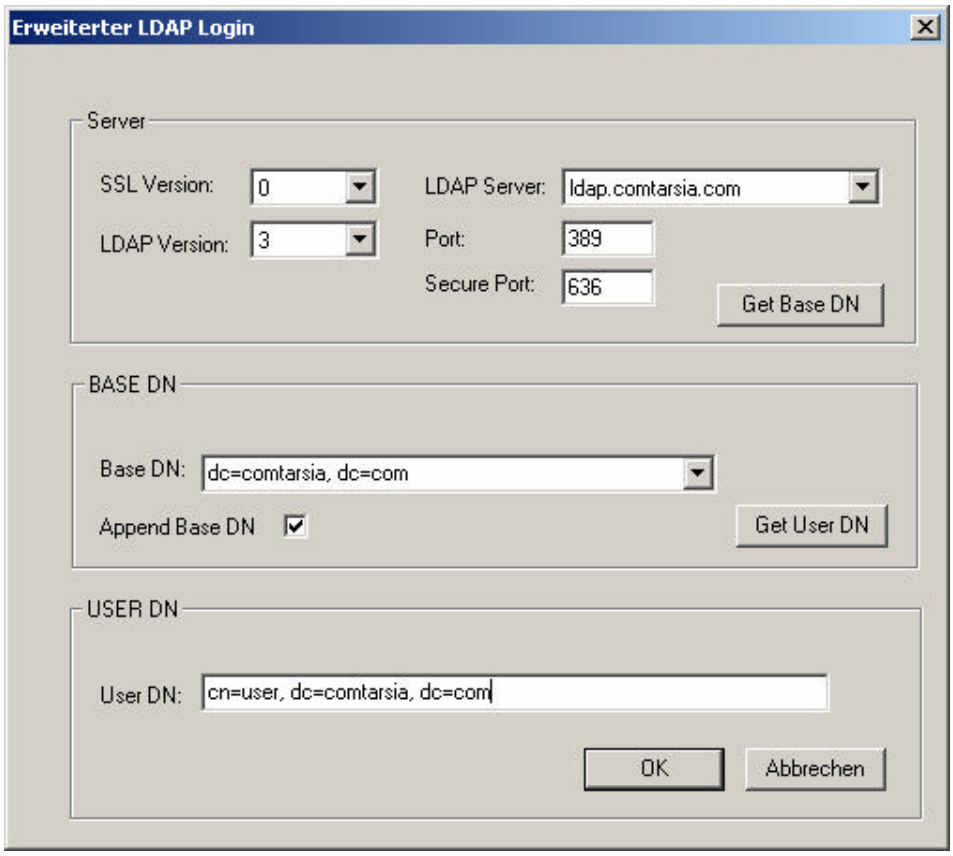
In der Registry unter LDAP\LDAPServers befinden sich die LDAP-Server. Statt „ldap.comtarsia.com“ wird der Hostname oder die IP-Adresse des LDAP-Servers eingetragen. Bei Bedarf können auch die Port-Adressen angepaßt werden.



Nach der Durchführung aller erforderlichen Einstellungen wird der Computer neu gestartet. Anschließend kommt der LDAP-Logon Dialog.
Benutzer und Passwort müssen eingetragen werden.
Als Domain kann entweder „LDAP LOGIN“ für einen reinen LDAP-Login gewählt werden, oder es wird eine OS/2 Domain angegeben, dann wird nach der LDAP Anmeldung zusätzlich eine OS/2 Anmeldung an diese primäre Domäne durchgeführt.
Alle weiteren OS/2 Funktionalitäten (z.B.: Passwort Synchronisation) funktionieren in der LDAP-Version analog wie im OS/2 Logon Client (siehe Servolution_LogonClient_3.0.doc).



Nach der Eingabe von Username/Passwort/Domain kann man statt auf „OK“ auch „Erweiterter LDAP Login“ auswählen. In diesem Fall wird ein weiterer Dialog geöffnet, der es erlaubt, diverse LDAP-Konfigurationsdaten dynamisch zu verändern. (Diese Einstellungen werden nicht gespeichert und sind nur für einen Login aktiv). Diese Funktion dient hauptsächlich zum Testen und wird im endgültigen Release nur mehr Administratoren zur Verfügung stehen.


Erweiterter LDAP Login
Server
SSL Version:
0
LDAP Server:
ldap.comtarsia.com
LDAP Version:
3
Port:
389
Secure Port:
636
Get Base DN
BASE DN
Base DN:
dc=comtarsia, dc=com
Append Base DN
Get User DN
USER DN
User DN:
cn=user, dc=comtarsia, dc=com
OK
Abbrechen

4. Konfiguration eines OpenLDAP-Servers unter SuSE 8.0 Prof. zur Verwendung mit dem Servolution LDAP Logon Client

Folgende rpm-Pakete werden benötigt:
- openldap2-client-2.0.23-53
- openldap2-2.0.23-53
- openssl-0.9.6c-29 (nur für ssl support)

Ob diese Pakete installiert sind, kann hiermit überprüft werden:

```
ngc4321:/home/stefan # rpm -q -a | grep openldap
openldap2-client-2.0.23-53
openldap2-2.0.23-53
ngc4321:/home/stefan # rpm -q -a | grep openssl
openssl-0.9.6c-29
openssl-devel-0.9.6c-29
ngc4321:/home/stefan #
```

Bei Bedarf können diese Pakete mit dem "yast" oder direkt mit "rpm" nachinstalliert werden.

Die OpenLDAP-Konfigurationsdateien befinden sich unter /etc/openldap.
LDAP Client-Tools befinden sich unter /usr/bin.
Der LDAP-Server (slapd) befindet sich im Verzeichnis /usr/lib/openldap.

Anpassen der Konfiguration:
ldap.conf:

```
BASE    dc=comtarsia, dc=com
```

slapd.conf:

Access Control, jeder User darf seinen Eintrag modifizieren, andere lesen, und das Feld userPassword anonym lesen (für auth):

```
access to *
 by self write
 by users read
 by anonymous auth
```

ldfb database definitions:

```
suffix          "dc=comtarsia,dc=com"
rootdn          "cn=Manager,dc=comtarsia,dc=com"
```

SSL: Für die Verwendung von SSL müssen die folgenden Zeilen an das Ende der slapd.conf Datei hinzugefügt werden:

```
# Certificates
TLSCertificateFile      /etc/openldap/server.pem
```

TLSCertificateKeyFile /etc/openldap/server.pem
TLSCACertificateFile /etc/openldap/server.pem

Erzeugen des SSL-Keys:
openssl req -new -x509 -nodes -out server.pem -keyout server.pem -days 365

In dem folgenden Dialog sollte "Common Name" der Hostname des LDAP-Servers sein.

```
ngc4321:/etc/openldap # openssl req -new -x509 -nodes -out server.pem -keyout
server.pem -days 365
Using configuration from /usr/share/ssl/openssl.cnf
Generating a 1024 bit RSA private key
......++++++
.............++++++
writing new private key to 'privkey.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:AT
State or Province Name (full name) [Some-State]:Vienna
Locality Name (eg, city) []:Vienna
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Comtarsia
Organizational Unit Name (eg, section) []:SD
Common Name (eg, YOUR name) []:ngc4321.comtarsia.com
Email Address []:stefan@comtarsia.com
ngc4321:/etc/openldap #
```

Eventuell muss noch die OpenSSL-Konfiguration unter /usr/share/ssl/openssl.cnf angepaßt werden.
Von der Seite http://servolution.comtarsia.com kann eine Version von openssl.exe mit passender Konfiguration für Windows heruntergeladen werden.

Starten des OpenLDAP-Servers:
ohne SSL: /etc/init.d/ldap start
mit SSL: cd /usr/lib/openssl
./slapd -h "ldap:/// ldaps:///"
oder ./slapd -d 9 -h "ldap:/// ldaps:///" für debugging output

Jetzt ist der OpenLDAP-Server fertig konfiguriert, es müssen nur noch LDAP-Daten importiert

werden. Für die Administration empfiehlt sich eine LDAP-GUI,
wie z.B.: http://www.iit.edu/~gawojar/ldap/index.html (benötigt JAVA JRE 1.4)
Sie melden sich als Manager an (cn=Manager,dc=comtarsia,dc=com;
passowrd=secret) und importieren
folgendes ldif-File:

```
dn: dc=comtarsia,dc=com
dc: comtarsia
objectClass: organization
objectClass: dcObject
o: comtarsia

dn: cn=Manager, dc=comtarsia,dc=com
objectClass: person
sn: Manager
cn: Manager

dn: cn=user1, dc=comtarsia,dc=com
objectClass: person
sn: user1
cn: user1
userPassword: test
```

Der Import des LDIF-Files ist auch direkt über die Command Line möglich (siehe "man ldapadd")
Um weitere User hinzuzufügen, impotieren Sie ein LDIF-File in folgender Form:

```
dn: cn=user1, dc=comtarsia,dc=com
objectClass: person
sn: user1
cn: user1
userPassword: test
```

Jetzt ist auch die Anmeldung mit User-Accounts möglich, diese sollten auch in der Lage sein, ihre eigenen Attribute zu modifizieren (z.B.: userPassword); falls nicht, wurde die ACL in sldapd.conf nicht richtig gesetzt.

Waren alle vorhergehenden Schritte erfolgreich, steht einer Anmeldung mit dem LDAP Logon Client nichts mehr im Wege. (weitere Infos unter LDAP-Quickstart).