Comtarsia Logon Client 2006

LDAP Handbuch

Installation und Konfiguration des

Comtarsia Logon Client 2006 für

LDAP Directory Server

Version: 4.1.13.4, 04-Jul-2006

Inhaltsverzeichnis

1. Einführung

Der erste Teil dieses Handbuches führt durch die Installation und die grundlegende Konfiguration des Comtarsia Logon Client 2006.
Der zweite Teil dieses Handbuches widmet sich der erweiterten LDAP Konfiguration, inklusive serverspezifischer Einstellungen. Am Ende befinden sich ein Glossar sowie eine Referenzliste mit weiterführener Literatur.

Der **"Schnellstart"** gibt Anweisungen über die benötigten Einstellungen, um den Comtarsia Logon Client2006 für grundlegende LDAP Funktionalitäten, wie User/Passwort Authentifizierung mit einem LDAP Directory Server, zu konfigurieren.

Das Kapitel **"Optionale LDAP Attribute"** gibt eine detailliertere Erklärung und Konfigurationsvorschläge für das optimale Ausnutzen der kompletten Palette von LDAP Funktionalitäten des Comtarsia Logon Clients, unter anderem der Möglichkeit, über LDAP dem Benutzer das Profilverzeichnis, das Benutzerverzeichnis, und diverse Ressourcen zuordnen zu können.

Im Kapitel **"Serverspezifische Konfiguration"** befinden sich sämtliche, auf den jeweiligen Servertyp zugeschnittenen Setupmöglichkeiten, und auch **die Erweiterung des LDAP Schemas durch das Comtarsia LDAP Schema** wird mit besonderer Aufmerksamkeit behandelt.
Die erfolgreiche Integration des Comtarsia Schemas in den LDAP Server ist **ein massgeblicher Schritt bei der Inbetriebnahme** den erweiterten LDAP Funktionalitäten des Comtarsia Logon Client.
Weiters findet sich hier auch eine Beschreibung über SSL/TLS-Konfiguration sowie die Zertifikate-Verwaltung.

2. Logon Client Installation mit InstallShield

2.1 Beginn der Installation

Führen Sie das Comtarsia Logon Client InstallShield Installationsprogramm aus. CLC_2006-4.1.x.x.exe

Die Installationssprache kann ausgewählt werden.

Nach der Installation mit InstallShield wird der Comtarsia Logon Client2006 Konfigurator gestartet.

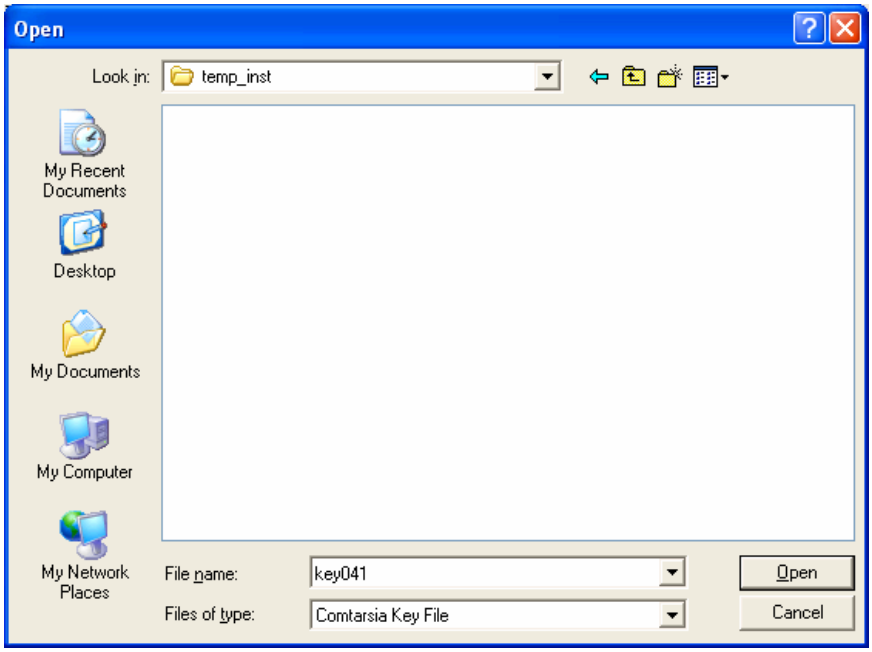
2.2 Der Logon Client Konfigurator

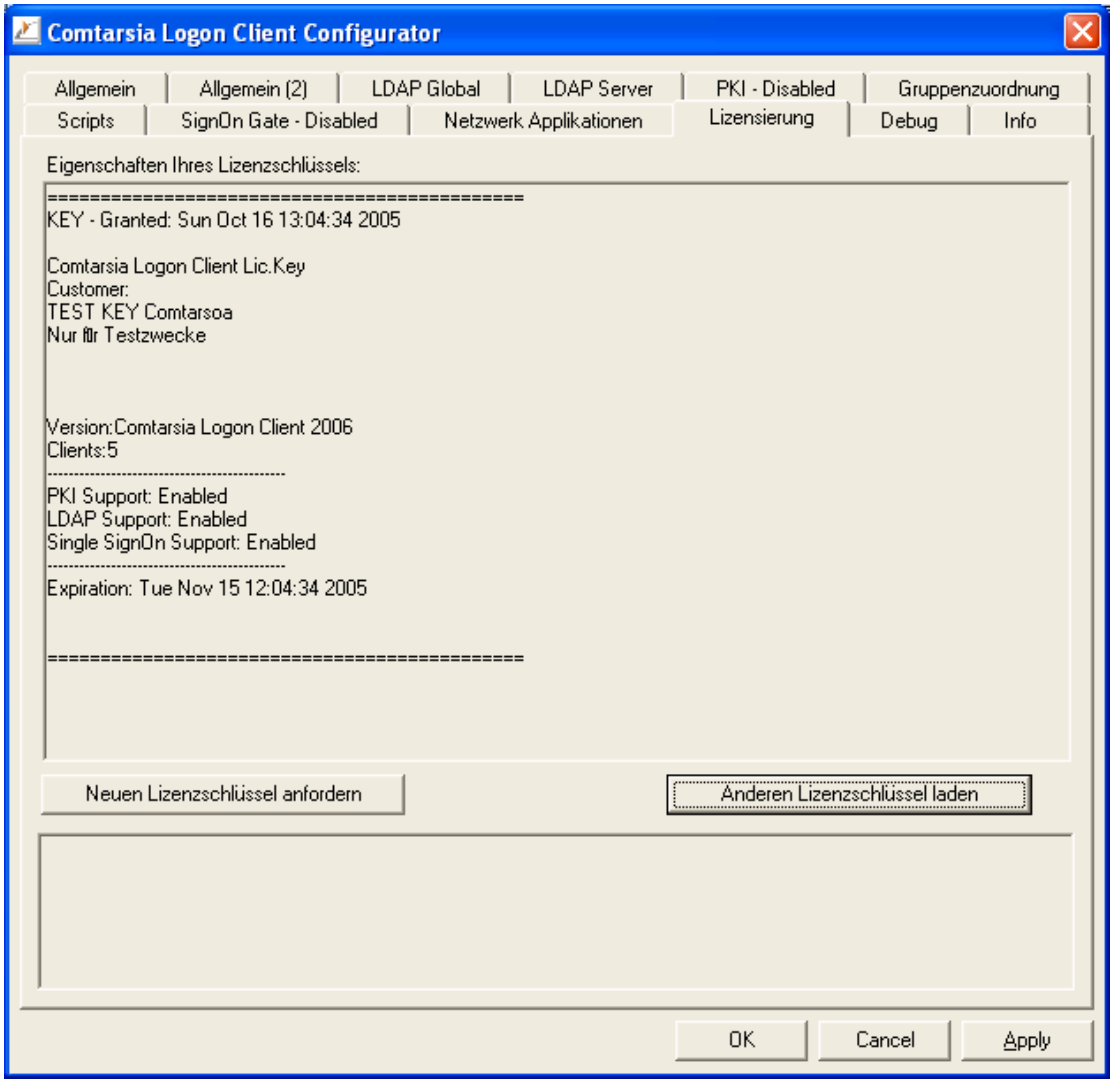
2.2.1 Grundlegende Konfiguration

Der letzte Schritt ist nun, ein Minimum-LDAP-Setup mithilfe des Konfigurator einzurichten (siehe “LDAP Logon Schnellstart”).

2.2.2 Lizensierung

Im Falle einer erworbenen Version des Comtarsia Logon Clients kann der eigene Lizenzschlüssel geladen werden um den Testschlüssel zu ersetzen.





Die Logon Client Testversion bleibt bis zum Ablauf der Gültigkeit des Testschlüssels funktionsfähig.

2.2.3 Neustart

Nach dem Abschluss der Installation ist ein Neustart der Arbeitsstation erforderlich.
Nach dem Neustart steht der Logon Client betriebsbereit zur Verfügung.

3. LDAP Logon Schnellstart

Dieses Kapitel beschreibt die nötigen Konfigurationsschritte des Comtarsia Logon Client, um sich gegen einen LDAP Server erfolgreich authentifizieren zu können.

Es wird ebenfalls eine grundlegende SSL-Konfiguration beschrieben.

Weitere Konfigurationsmöglichkeiten sind in den einschlägigen Kapiteln der bestimmten Servertypen unter **“Serverspezifische Konfiguration” beschrieben.**

3.1 Vorausssetzungen

3.1.1 Client

- Microsoft Windows 2000/XP
- Comtarsia Logon Client2006 installiert

  Installation siehe unter “Installation mit InstallShield”

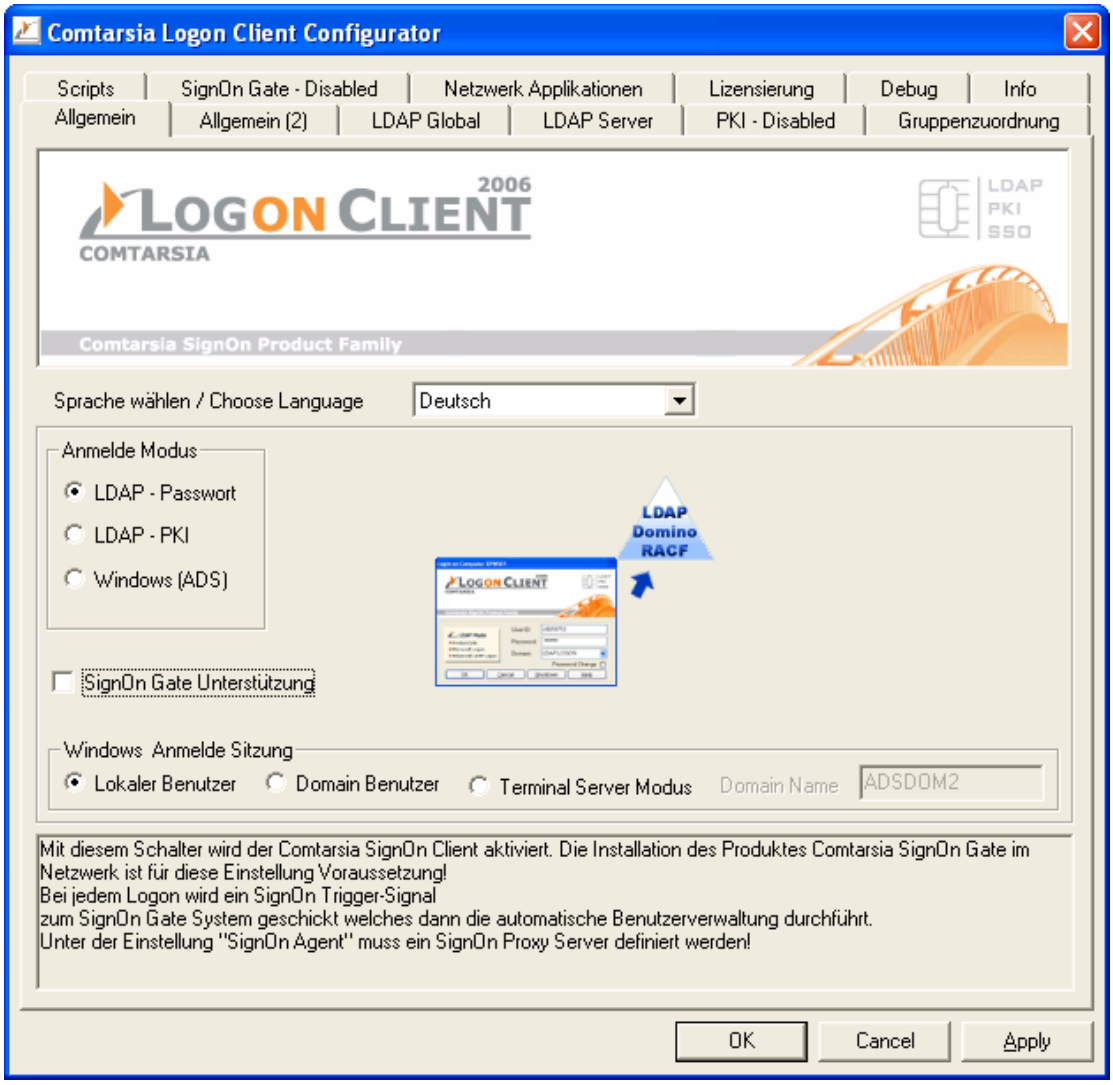
3.1.2 LDAP-Server

Folgende LDAP-Server (LDAP Version 2 und 3) sind zur Zeit unterstützt:

- ✓ Sun One Directory Server
- ✓ iPlanet
- ✓ Netscape Directory Server
- ✓ OpenLDAP
- ✓ IBM RACF Directory Server
- ✓ Lotus Domino
- ✓ Novell eDirectory
- ✓ IBM Directory Server 3.x/4.x
- ✓ IBM Directory Server 5.1

3.2 Erster Schritt: General Konfiguration

Setzen Sie Logon Client run mode auf “LDAP”.



3.3 Zweiter Schritt: Minimal LDAP global Konfiguration

- **LDAP Version**: Standard ist LDAP Version “3”, da seit einigen Jahren die meisten LDAP Server bereits Version 3 verwenden.

  Hier kann „2“ ausgewählt werden, falls der zu verwendende LDAP-Server nur LDAP Version „2“ unterstützt.

- Aktivieren von “**BaseDN anhängen**”. Hierbei gilt es serverspezifische Besonderheiten zu beachten. Für die meisten LDAP Server muss diese Einstellung aktiviert werden.

- Setzen des “**Servertyp**”.

- Konfigurieren der **Benutzer DN**:

- ✓ Benutzer DN Prefix ist “**cn=**” (siehe unten) oder “**uid=**”
- ✓ Benutzer DN Suffix “**,ou=Office_1,ou=Departement_1**”

  Achtung: Eingabe beginnt mit “**,**” !

- ✓ **Base DN** der LDAP Hierarchie, z.B. “**o=Company**” (siehe unten) oder “**dc=companyname, dc=com**”

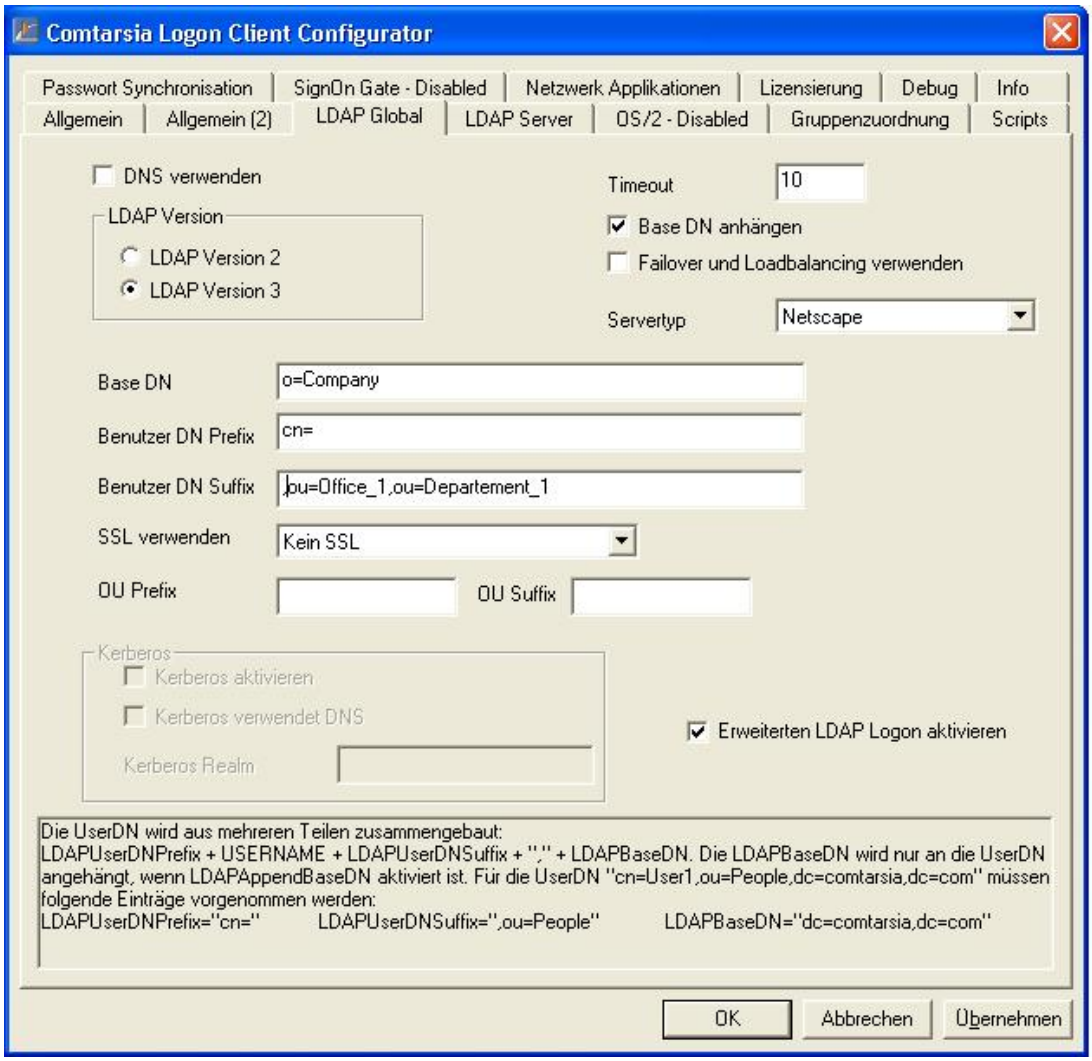
  Die komplette Benutzer DN entsteht folgendermassen:

  BenutzerDN = BenutzerDN Prefix + Benutzername + BenutzerDN Suffix + BaseDN

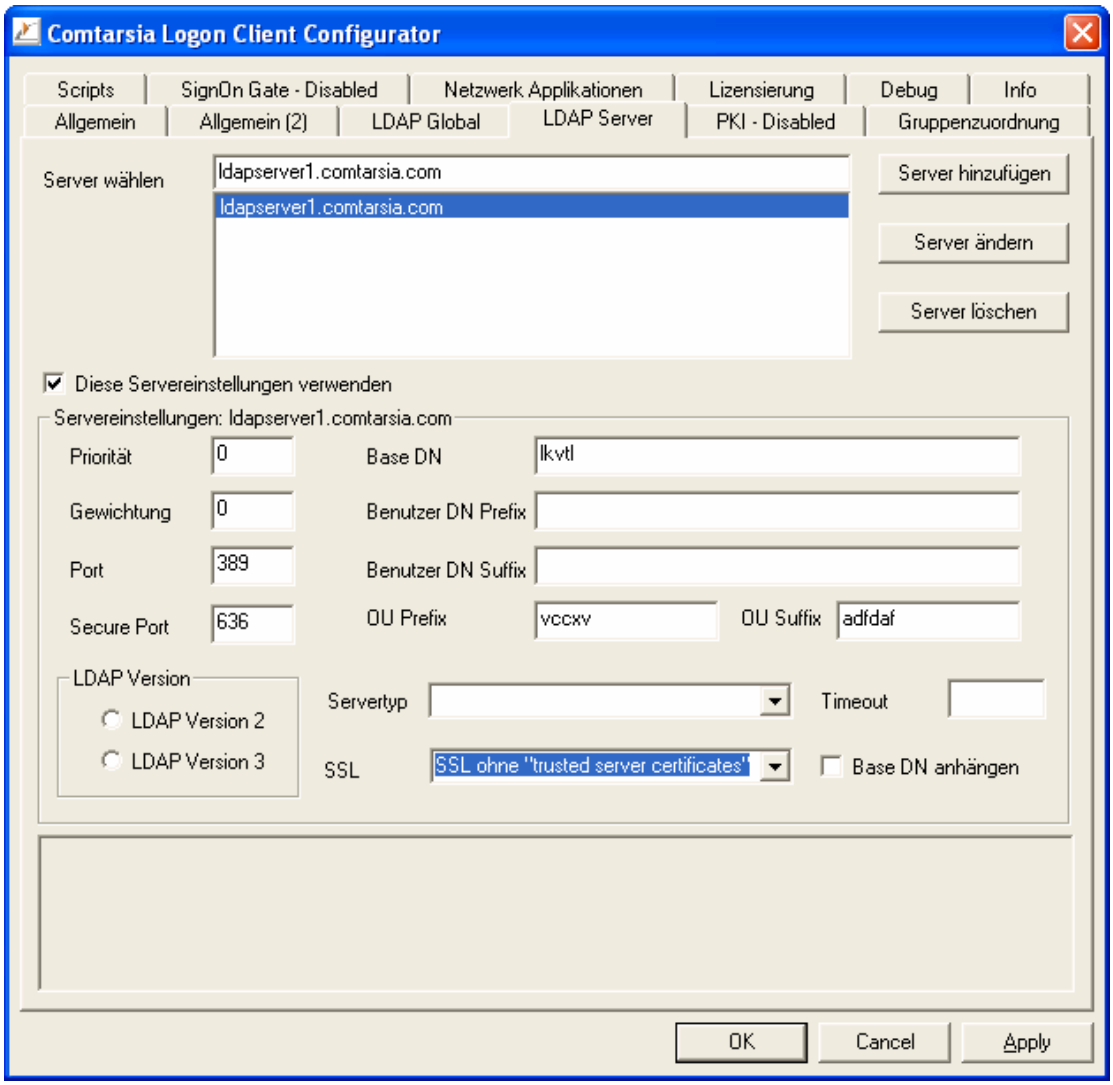
  Beispiel:

  cn=Testbenutzer, ou=Office_1, ou=Departement_1, o=Company

- Für Testzwecke **kann SSL deaktiviert werden** (falls auch der LDAP-Server dies unterstützt)
- Aktivieren von “**Erweiterten LDAP Logon aktivieren**” (optional)



3.4 Dritter Schritt : Setzen des Server-Hostnames



Nach der Eingabe von Hostname oder IP-Adresse des LDAP-Servers kann dieser mittels betätigen der "**Server hinzufügen**"-Schaltfläche übernommen werden.

WICHTIG: auf diesem Reiter ist das Eintragen des Servernamens ausreichend, die anderen Konfigurationsoptionen sind für eine Grundkonfiguration nicht notwendig.

3.5 Vierter Schritt: Logon am LDAP Server

Der Computer muss nach der Installation und Grundkonfiguration neu gestartet werden. Wenn nur Änderungen an der Konfiguration vorgenommen worden sind, ist KEIN Neustart notwendig.

Nach dem Neustart(Abmelden) erscheint der Logon Client Logon Dialog. Hier kann der Benutzername und das Passwort eingegeben werden. Als Domäne muss "**LDAP LOGON**" ausgewählt werden und anschliessend kann der Logon mittels „OK" gestartet werden.

Option “Erweiterter LDAP Logon”

Anstatt nach der Eingabe vom Benutzernamen, Passwort und der Domäne “OK” zu drücken, kann auch “**Erweiterter LDAP Logon**” ausgewählt werden. Dies öffnet ein weiteres Dialogfenster, in dem die oben beschriebenen aktuellen Einstellungen **temporär** überschrieben werden können.

Diese Option ermöglicht das einfache Testen von Einstellungen, die von der gespeicherten Konfiguration abweichen. Diese Daten werden nicht gespeichert, und sind nur für einen einzigen Logon gültig.

4. LDAP hebt ab

Auf den Geschmack gekommen?

Das folgende Kapitel beschreibt eine fortgeschrittene Konfiguration und den Gebrauch des Comtarsia Logon Client2006 für LDAP Anmeldungen.

Hinweis: Die folgenden Einstellungen sind für eine einfache Anmeldung am LDAP Server nicht zwingend erforderlich, und können auch ohne dem Comtarsia LDAP Schema verwendet werden.

4.1 Benutzergruppen

Der Comtarsia Logon Client2006 unterstützt die Verwendung von **LDAP user group Objekten**

- objectClass=„**groupOfNames**“ (OID: 2.5.6.9)
- objectClass=„**groupOfUniqueNames**“ (OID: 2.5.6.17).

(Zukünftige Versionen werden eine freie Wahl der Objektklassen anbieten, um auch Spezialfälle abdecken zu können.)

Diese Klassen haben je nach Objektklasse die Attribute "**member**" oder "**uniqueMember**" um die BenutzerDN der Gruppenmitglieder zu speichern.

Der Benutzer muss mit seiner vollen BenutzerDN in das jeweilige Attribut eingetragen sein.

4.1.1 Gruppenzuordnung nach gleichen Namen

Bei einem LDAP Logon mit dem Comtarsia Logon Client2006 werden auch die LDAP Gruppenmitgliedschaften abgefragt.

Ein Benutzer, welcher als Mitglied einer bestimmten LDAP Gruppe identifiziert wurde, wird auch Mitglied der gleichnamigen lokale Gruppe, falls diese auf der lokalen Arbeitsstation existiert. (LDAP Gruppenname = lokaler System-Gruppenname)

Beispiel: Wenn der Benutzer ein Mitglied der Gruppe "Marketing" am LDAP Server ist, er wird auch der lokalen "Marketing" Gruppe zugeordnet.
Hierfür sind keine weiteren Einstellungen erforderlich.

4.1.2 Manuelle Gruppenzuordnung

Durch das Aktivieren der Checkbox Gruppenzuordnung / **"Manuelle Gruppenzuordnung verwenden"** im Konfigurator stehen neue Möglichkeiten um LDAP Gruppenmitgliedschaften in das lokale System zu transferieren zur Verfügung. (Siehe unten).

4.1.2.1 Hauptbenutzer/Administratoren

Die LDAP Gruppen „**WSADMIN**" und „**PUSERS**" sind (von der lokalen Systemsprache abhängig) der equivalenten lokalen Gruppe, d.h. auf einem deutschsprachigen System der Gruppe "Hauptbenutzer", bzw. "Administratoren" zugeordnet. (Siehe **"Individuelle Gruppenzuordnung"**).

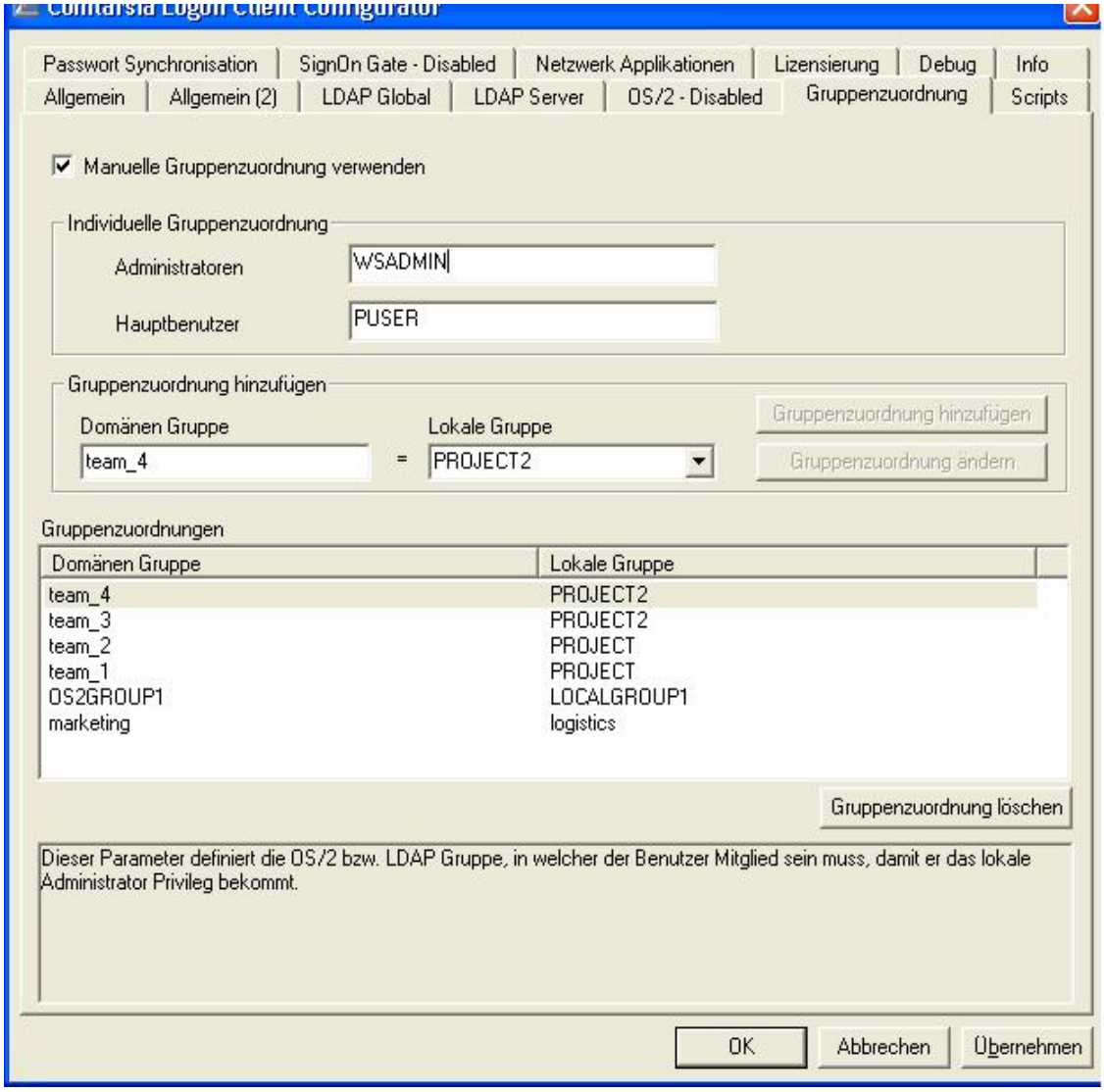
Beispiel: Wenn der LDAP Benutzer Mitglied der "WSADMIN" Gruppe ist, wird er Mitglied der lokalen Gruppe "Administratoren".

Hinweis: diese Gruppen können beliebig (um)benannt werden.

4.1.2.2 Frei konfigurierbare Gruppenzuordnung

Unter **"Gruppenzuordnung hinzufügen"** können beliebige LDAP Gruppen den lokalen Gruppen zugeordnet werden, die Gruppenmitgliedschaft der Benutzer wird von den LDAP Gruppen in die lokalen Gruppen übernommen.

Um das Konfigurieren möglichst einfach zu halten, wenn die gewählte lokale Gruppe noch nicht existiert, fragt der Logon Client Konfigurator in diesen Fällen, ob er die entsprechenden Gruppen anlegen soll.



Die maximale Anzahl an unterstützten Gruppen beträgt 251.

4.2 Wie wird die LDAP BaseDN ermittelt?

Nun ist es Zeit, um mehr darüber zu erfahren, wie der Comtarsia Logon Client2006 den LDAP BaseDN erkennt. Weiters ist es wichtig zu überlegen, welche Settings hierfür geeignet sind.

Ermittlung der BaseDN durch den Comtarsia Logon Client2006:

- Wenn in der **Registry** ein Wert unter LDAPBaseDN eingetragen ist, wird dieser verwendet.

- Wenn der LDAP Server LDAP **Version 3** unterstützt und die LDAP Version im Logon Client Konfigurator auf „3“ gesetzt ist, versucht der Logon Client, die **BaseDN über eine LDAP-Query** zu ermitteln.

Achtung: Die meisten LDAP Server unterstützen mehr als eine BaseDN. Es muss unbedingt sichergestellt sein, dass die für den Logon Client gewünschte BaseDN als erster Eintrag geliefert wird. Überprüfen läßt sich das z.B. mit einem LDAP-Browser

- Falls bis jetzt noch immer keine BaseDN ermittelt werden konnte, wird versucht, die **BaseDN aus dem Domain-Namen** des lokalen Rechners zu ermitteln.
  z.B.: Domain = „company.com“
  BaseDN = „dc = company, dc= com“

5. Optionale LDAP Attribute

5.1 Einführung

Die Comtarsia Schema-Erweiterung ermöglicht über die essentiellen Funktionen wie Benutzername/Passwort und Gruppen-Mitgliedschaften hinaus die Nutzung von weiteren LDAP Funktionen bei der Anmeldung an einem LDAP Server. (Grundkonfiguration siehe "LDAP Logon Schnellstart")

Die zur Zeit unterstützten LDAP Servertypen und die entsprechenden Anleitungen um das Comtarsia LDAP-Schema erfolgreich zu befinden sich im Kapitel "Serverspezifische LDAP Konfigurationen"

Nach einer erfolgreichen Schema-Erweiterung des LDAP-Servers und der Fertigstellung der Logon Client Konfiguration werden folgende Werte vom Logon Client bei einer Anmeldung automatisch vom LDAP Server ermittelt:

1. Verzeichnis- und Druckerfreigaben
2. Profilpfad und Benutzerverzeichnis
3. Netzwerk Applikationen

5.2 LDAP Verzeichnis- und Druckerfreigaben

Das Comtarsia LDAP-Schema definiert die Objektklasse **CLCShare** für die Definition von Verzeichnis- und Druckerfreigaben am LDAP Server.

Beide Freigabetypen können dem LDAP Benutzer (Objekttyp **CLCPerson**) durch Zuordnung und Ausfüllen des Attributfeldes **CLCShareName** zugewiesen werden.

Der Logon Client fragt automatisch alle Zuordnungen beim Einloggen an den LDAP Server ab und verbindet diese mit der Arbeitsstation des Benutzers den in LDAP hinterlegten Spezifikationen entsprechend.

Eine Höchstzahl von 25 Verzeichnis- und 9 Druckerfreigaben (LPT1 – LPT9) werden unterstützt.

5.2.1 Verzeichnisfreigaben

5.2.1.1 Erstellung einer Verzeichnisfreigabe

LDAP Objektklasse: CLCShare.

Um eine Verzeichnisfreigabe zu erstellen, muss zuerst ein neues LDAP-Objekt der Objektklasse „CLCShare" angelegt werden. Anschliessend werden die Attribute wie folgt befüllt:

CLCShareName: Name der Freigabe
CLCShareDescription: Beschreibung

CLCShareServer: Name des Ressourcenservers
CLCShareRemotePath: Pfad am Remote Server (Optional)
CLCShareType: **1 (steht für Verzeichnisfreigabe)**

5.2.1.2 Zuordnen einer Verzeichnisfreigabe zu einem Benutzer

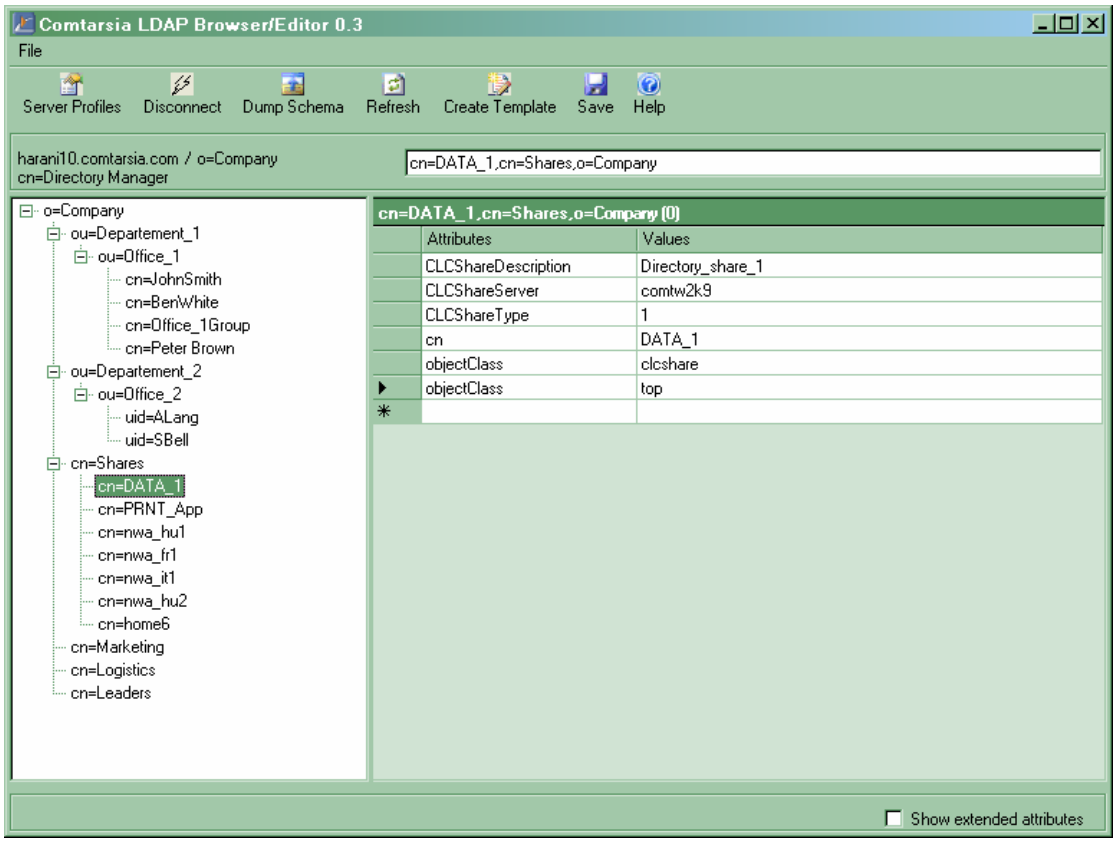
Um eine Verzeichnisfreigabe einem Benutzer zuordnen zu können, muss das Attribut **CLCShareName** dem Benutzerobjekt zugewiesen sein. Tragen Sie den Namen (aber nicht die volle DN!) der Freigabe ins Attributfeld ein.

Laufwerksbuchstaben:

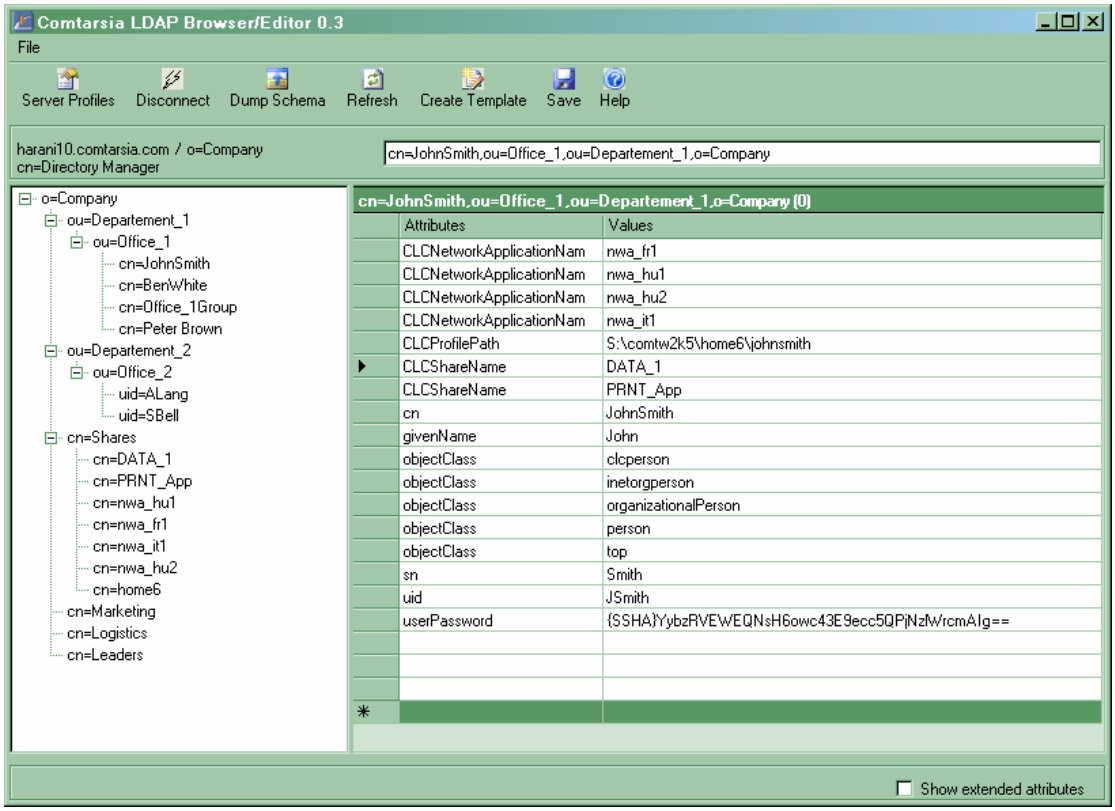
- wenn die Freigabe (z.B. “Daten1”) dem **nächsten freien Laufwerkbuchstaben** zugeordnet werden soll, muss der Name, aber nicht die volle DN in das CLCShareName Feld eingetragen werden.

- wenn der Freigabe ein bestimmter Laufwerkbuchstabe zugeordnet werden soll, so kann dieser Buchstabe beim LDAP Attribut an den Freigabenamen angehängt werden, z.B. **“Datas1/G” für den Laufwerkbuchstaben G.**

Diese Abbildung zeigt die Einstellungen einer Verzeichnisfreigabe am LDAP Server:



Diese Abblidung zeigt die Zuweisung einer Verzeichnisfreigabe zu einem Benutzer:



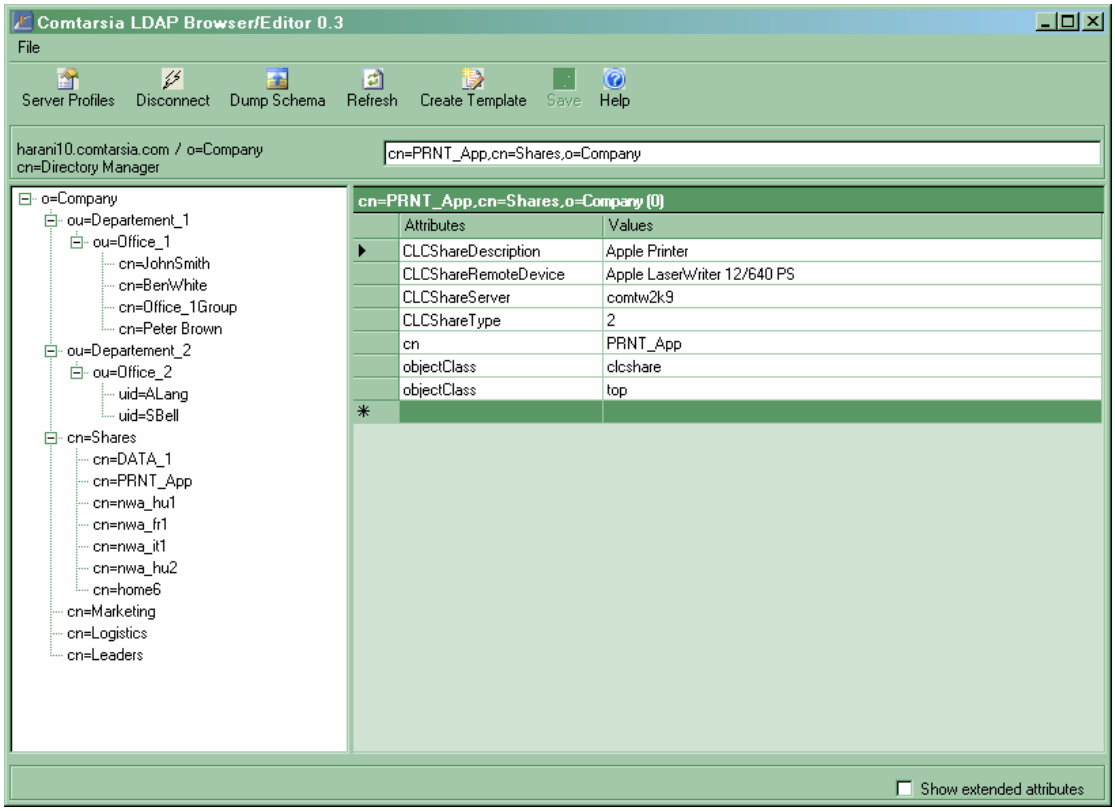
5.2.2 Druckerfreigaben

5.2.2.1 Erstellung einer Windows Netzwerkdrucker-Freigabe

LDAP Objektklasse: CLCShare

Um eine Druckerfreigabe zu erstellen, muss zuerst ein neues LDAP-Objekt der Objektklasse „CLCShare“ angelegt werden. Anschliessend werden die Attribute wie folgt befüllt:

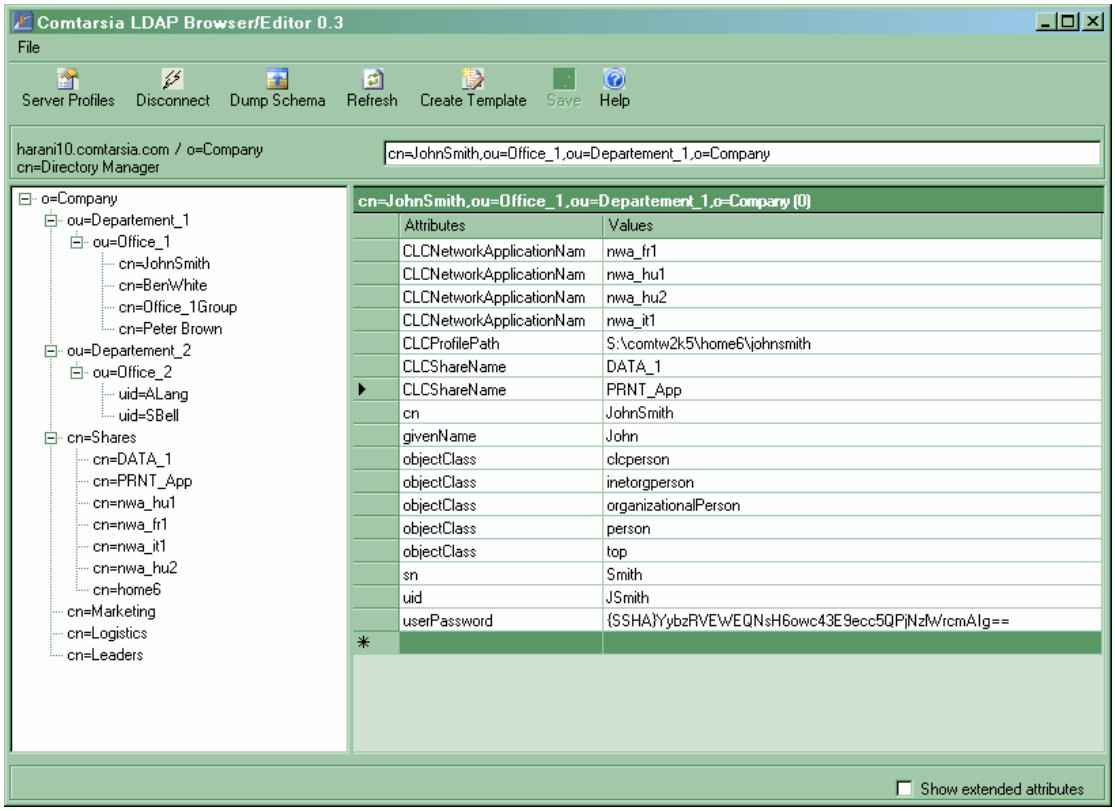
CLCShareName or cn: der Druckername
(z.B. “Printer13”)
CLCShareDescription: **die** Beschreibung des Drucker
CLCShareType: **2 (steht für Druckerfreigabe)**
CLCShareRemoteDevice: - entweder der Freigabename des Druckers (“Printer13”), oder
- der komplette Name des Druckers (“Apple LaserWriter 16/640 PS”).



Der Druckertreiber muss nur am Server installiert sein.

5.2.2.2 Zuordnen einer Druckerfreigabe zu einem Benutzer

Um eine Druckerfreigabe einem Benutzer zuordnen zu können, muss das Attribut **CLCShareName** dem Benutzerobjekt zugewiesen sein. In das Attribut CLCShareName des Benutzers wird der Name der Freigabe (aber nicht die volle DN!) eingetragen.



5.2.2.3 Druckerfreigabe für einen LPT Port erstellen

Um eine Druckerfreigabe für einen LPT Port zu erstellen, muss ein neues Objekt des Types CLCShare angelegt werden, welchen Attributen folgende Werte zugeordnet werden müssen:

CLCShareName or cn: der Druckername
(z.B. “Printer13”)
CLCShareDescription: **die** Beschreibung des Druckers
CLCShareType: **2 (steht für Druckerfreigabe)**
CLCShareRemoteDevice: der Freigabename des Druckers (“Printer13”)

5.2.2.4 Zuordnen einer LPT Druckerfreigabe zum Benutzer

Um eine Druckerfreigabe einem Benutzer zuordnen zu können, muss das Attribut **CLCShareName** dem Benutzerobjekt zugewiesen sein. In das Attribufeld „CLCShareName“ wird der Name der Freigabe (aber nicht den vollen DN!) eingetragen, sowie mit einem “/” getrennt die Portnummer, z.B.: “**Printer13/LPT3**”.

Der Druckertreiber muss am Client Arbeitsplatz installiert werden.

Der Unterschied zwischen den beiden Lösungen ist die Tatsache, dass für Windows Applikationen ein Netzwerkdrucker, für DOS-Applikationen aber ein Drucker am LPT Port nötig ist.

5.3 Benutzerverzeichnis und Profilpfad

Als weitere vorteilhafte Funktionen des Comtarsia Logon Client2006 steht die Möglichkeit zur Verfügung, Benutzerverzeichnis (mit oder ohne Laufwerkbuchstaben) und Profilpfad (auf einem Ort mit dem Benutzerverzeichnis, oder getrennt) während des Logons dem Benutzer zuordnen zu können.

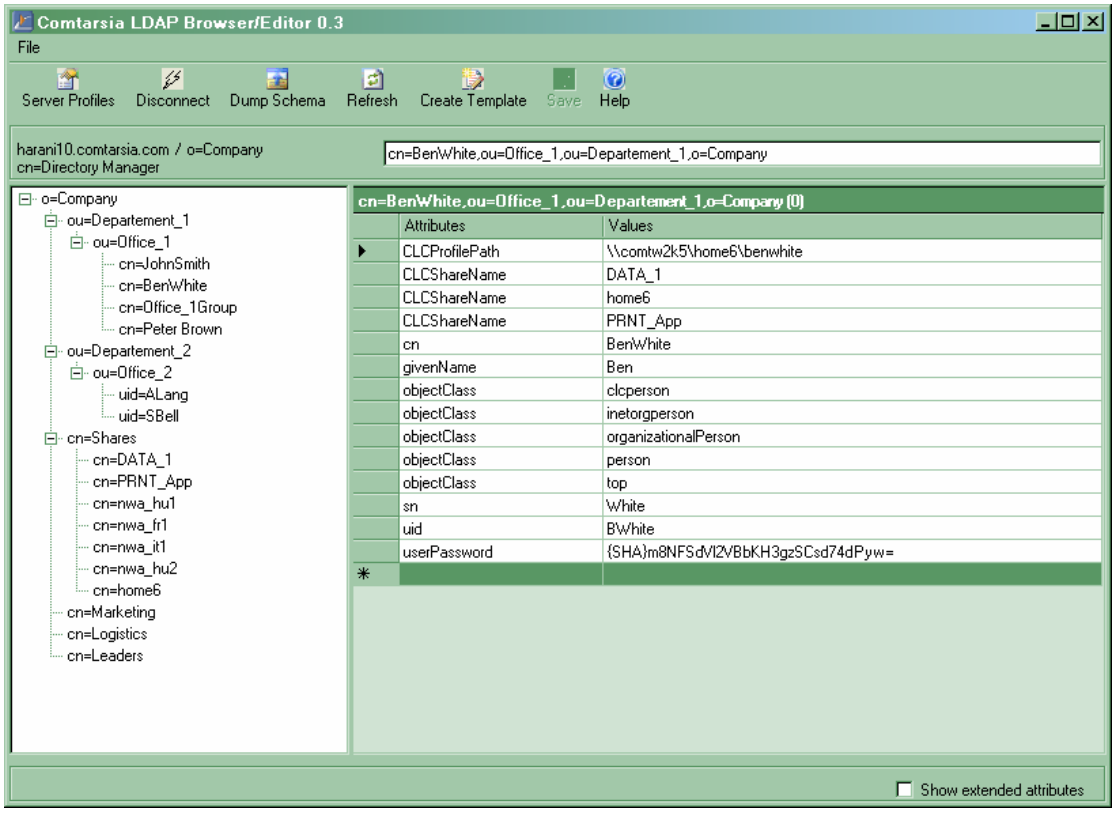
Der Pfad zum Benutzerverzeichnis ist in das Attribut "**CLCProfilePath**" des "**CLCPerson**" Objektes einzugeben.
Dieses Attribut wird bei einer Anmeldung mit dem Comtarsia Logon Client automatisch abgefragt.

Folgende Schreibweisen sind vom Comtarsia Logon Client2006 unterstützt:

\\COMTW2K\HOME\USER1

Der nächste verfügbare Laufwerkbuchstabe wird dem UNC Pfad zugewiesen:
\\COMTW2K\HOME\USER1.

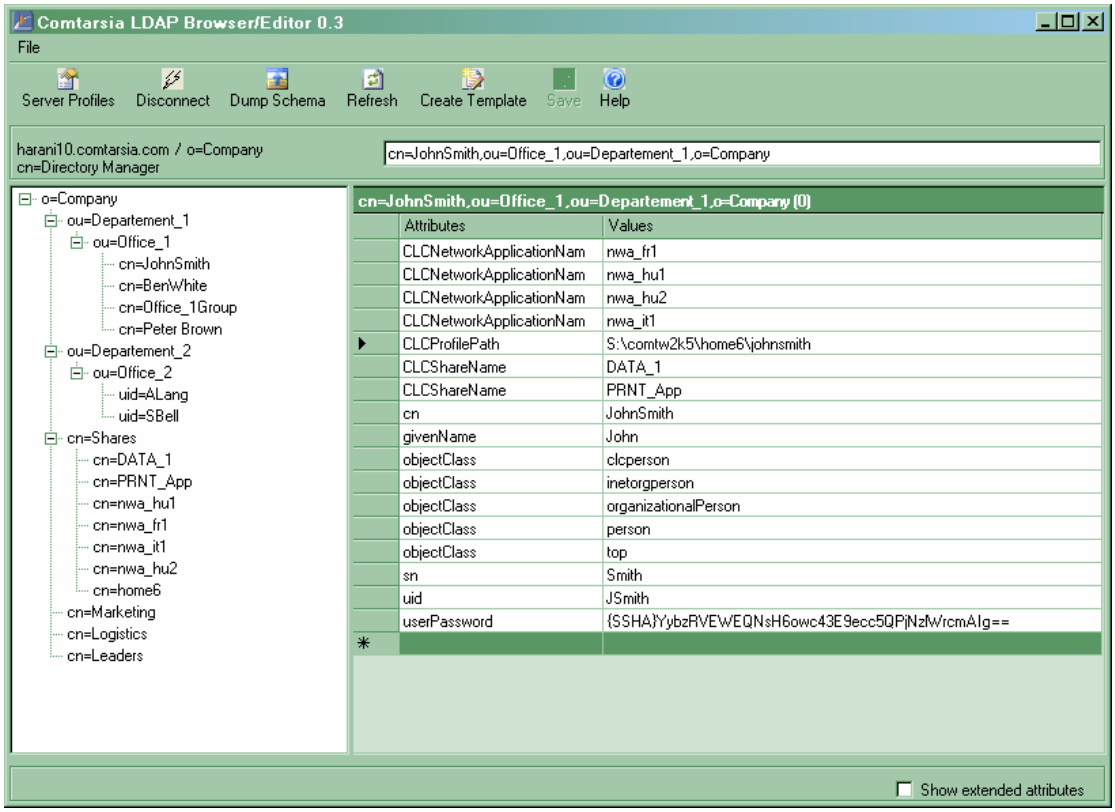
Der Profilpfad ist \\COMTW2K\HOME\USER1\PROFILE.



H:\COMTW2K\HOME\USER1

Der Laufwerkbuchstabe "H:" wird dem UNC Pfad \\COMTW2K\HOME\USER1 zugewiesen.

Der Profilpfad ist H:\COMTW2K\HOME\USER1\PROFILE.



H:\WOMBAT\test3!WOMBAT\profiles\test3

Zeigt auf das Benutzerverzeichnis \\WOMBAT\test3 auf "H:"

Der Profilpfad ist nun \\WOMBAT\profiles\test3.

Soll das Benutzerverzeichnis und Profilpfad getrennt verwaltet werden, so können beide Pfade mit einem „!“ getrennt in das Attribut eingegeben werden.

Hinweis: Wird Samba Ressourceserver verwendet, wird die Seperation von Benutzerverzeichnis und Profilpfad empflohlen.

5.4 LDAP Netzwerkapplikationen

5.4.1 Einführung

Der Comtarsia Logon Client bietet die Möglichkeit LDAP Applikationsdefinitionen zu verwenden, d.h. auf der Grundlage von LDAP Objekten werden automatisch Verknüpfungen zu benötigten Applikationen auf der Arbeitsstation erstellt. Diese Funktionalität wird während der Anmeldung des Benutzers ausgeführt und wird seit der Version 3.0.4.22 vom Comtarsia Logon Client unterstützt.

5.4.2 Erzeugen und Konfigurieren von Netzwerkapplikationen

LDAP Objektklasse: "**CLCNetworkApplication**".

Um eine Netzwerkapplikation zu erstellen, legen Sie einen neuen Objekt an, und ordnen Sie folgende Attribute zu:

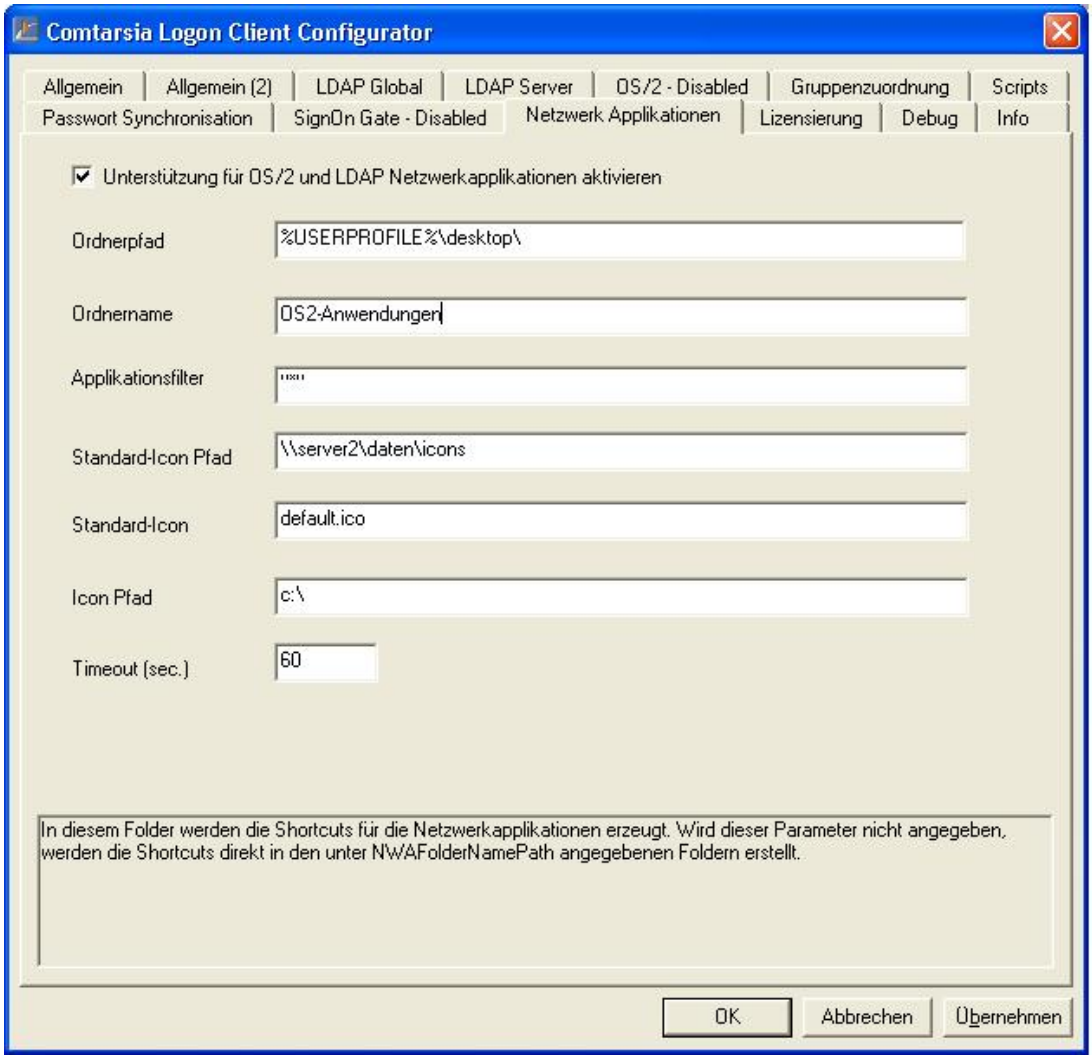
CLCNetworkApplicationDescription: Beschreibung der Netzwerkapplikation
CLCNetworkApplicationCommand: auszuführende Datei der Netzwerkapplikation
CLCNetworkApplicationProgramPosition: Programmverzeichnis
CLCNetworkApplicationCommandParameters: optionale Parameter
CLCNetworkApplicationWorkingDirectory: Arbeitsverzeichnis

Nachfolgend eine Übersicht über die verwendeten LDAP Attribute und ihre Bedeutung auf dem Windows Arbeitsplatz:

LDAP Attribute	**Windows Verknüpfung**
Erforderlich	
cn	nur für LDAP
CLCNetworkApplicationDescription	Beschreibung der Verknüpfung Name der Verknüpfung (*.lnk)
CLCNetworkApplicationCommand	Ziel (z.B. winword.exe)
CLCNetworkApplicationProgramPosition	Programmverzeichnis (absoluter Pfad oder UNC-Pfad)
Optional (müssen nicht definiert werden)	
CLCNetworkApplicationCommandParameters	Programm-Parameter
CLCNetworkApplicationWorkingDirectory	Arbeitsverzeichnis

Diese Funktionalität des Comtarsia Logon Client wurde mit dem Vorbild der IBM OS/2 Netzwerkapplikationen entwickelt; steht nun aber für Windows/LDAP zur Verfügung.

Während der Benutzer-Anmeldung werden die benötigten Applikationen automatisch vom LDAP-Server abgefragt und unter Berücksichtigung der definierten Filterregeln werden Verknüpfungen auf der Arbeitsstation erstellt. Bereits bestehende Verknüpfungen, welche sich im selben Ordner befinden, werden gelöscht, sollten sie mit dem Filter kollidieren.



Sollte sich in dem unter “ProgramPosition” definiertem Verzeichnis bereits eine .lnk-Datei für die jeweilige Applikation (Applikationsname.lnk) befinden, so wird nur diese Datei vom Logon Client auf den Arbeitsplatz kopiert und es werden keine weiteren Aktionen durchgeführt.

Die Verzeichnisse welche unter “**NWAFolderNamePath**“ und “**NWAFolderName**“ definiert sind werden vom Logon Client mit Administrator-Berechtigung erzeugt und können sich somit auch in Verzeichnissen befinden, die vom Benutzer selbst nicht beschreibbar sind (z.B. %ALLUSERSPROFILE%).

Die nachfolgende Abbildung zeigt eine konfigurierte LDAP Netzwerkapplikation:

5.4.3 Zuweisung von Icons

Es gibt zwei grundsätzliche Möglichkeiten, Icons für die Netzwerkapplikationen zu hinterlegen.

1) Die Icon-Datei befindet sich im selben Verzeichnis wie die Applikation selbst und das Icon hat den Dateinamen “**applicationname.ico**“

2) Das Icon für die Applikation wird in dem unter “**NWADefaultIconPath**“ hinterlegtem verzeichnis abgelegt.

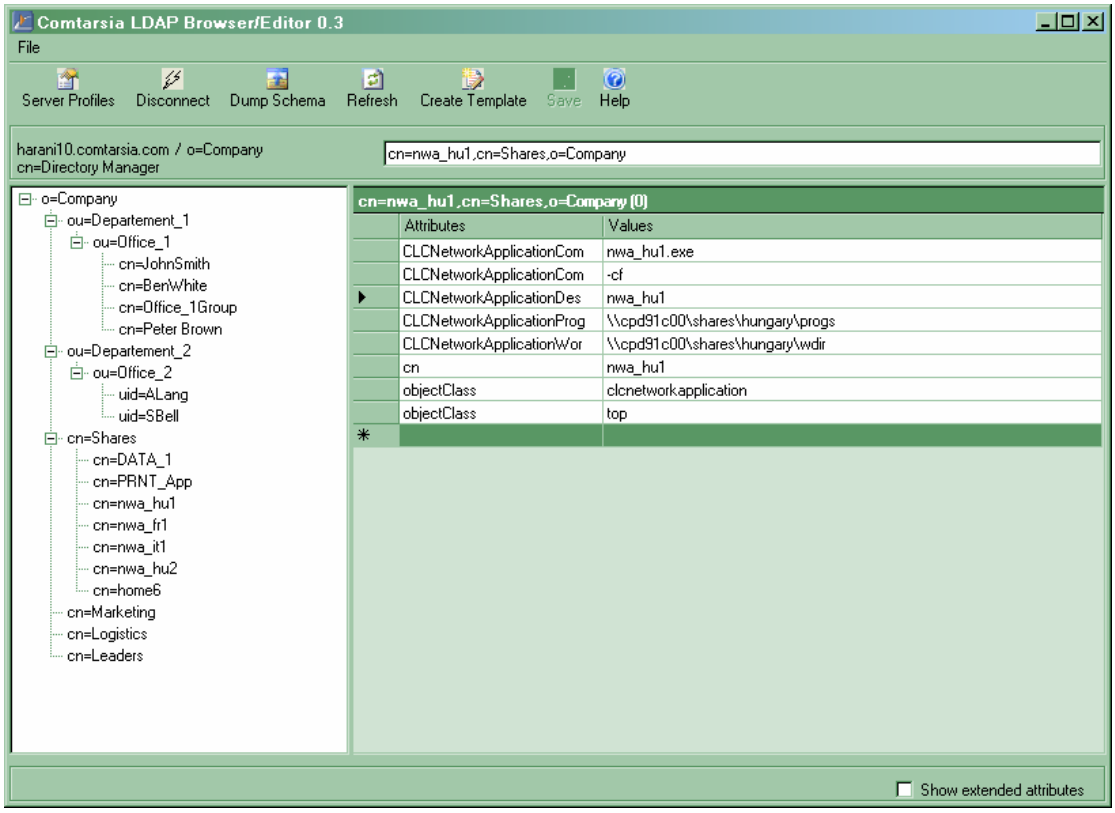
Konnte in den beiden oben beschriebenen Verzeichnissen keine passende Icon-Datei gefunden wird, so wird das "**NWADefaultIcon" im „NWADefaultIconPath**" gesucht und verwendet falls gefunden.

Alle benötigten Icons werden vom Server auf die lokale Arbeitsstation des Benutzers kopiert (in das Verzeichnis "**NWAIconPath**").

Ist im Programmverzeichnis am Server betreits eine Datei namens "**applicationname.lnk**" vorhanden, so wird nur diese auf die lokale Arbeitsstation kopiert.

5.4.4 Zuweisen von Netzwerkapplikationen

Um Netzwerkapplikationen einem Benutzer zuzuweisen, muss das LDAP Attribut **CLCNetworkApplication** dem LDAP Benutzerobjekt zugewiesen werden, in welches der Name der Netzwerkapplikationen eingetragen wird. (nur der Name und NICHT die volle DN).



5.5 Spezielle Comtarsia Attribute

- CLCForcePasswordChange
  Wenn dieses Attribut im Benutzerobjekt vorhanden und auf „1" gesetzt ist, so wird der Benutzer bei einer Anmeldung durch den Logon Client aufgefordert, sein Passwort zu ändern. Anschließend wird dieses Attribut durch den Logon Client wieder auf „0" zurückgesetzt. Eine Anmeldung des Benutzers ohne vorherigem Passwortwechsel ist nicht möglich. Diese

Meldung hat Priorität gegenüber optionalen Policy-Meldungen wie z.B. einer Passwort Expire Warnung.
Der Benutzer benötigt hierfür Schreibberechtigung auf dieses Attribut in seinem Objekt.

6. Erweiterte LDAP Funktionen

6.1 Einführung

Die erweiterten LDAP Funktionen werden vom Logon-Client gehandhabt.
Das Einspielen des Schema-File ist für diese Funktionen nicht notwendig.

6.2 Zuweisen Hardwarespezifischer Administrator-Rechte

Falls ein Benutzer lokale Administratorrechte auf einer oder mehrerer spezifischen Workstations benötigt, kann dies über die Optionen „HwAdminGroup“ und „HwAdminAttribute“ konfiguriert werden.

6.2.1 HwAdminAttribute

Im Registry Key:
HKEY_LOCAL_MACHINE\SOFTWARE\PCS\GINA
"hwadminattribute"=""
wird definiert welches LDAP-Attribut des Benutzerobjektes eine Liste von Rechnernamen enthält auf denen der Benutzer Lokaler Administrator werden darf.

Im LDAP-Attribut des Benutzerobjekts, welches als „HwAdminAttribute“ konfiguriert ist, steht nun eine Liste von Computernamen auf denen der Benutzer lokale Administrator-Rechte benötigt. (zB.: Entwickler -> Entwicklerworkstation)

Zusätzlich muss der Benutzer der „HwAdminGroup“ zugehörig sein.

Beispiel:
„hwadminattribute“ = „workstations“
„hwadmingroup“ = „hwadmin“

Wenn sich nun der Benutzer auf einem Rechner anmeldet, dessen Namen im LDAP-Attribut „workstations“ vorkommt, und der Benutzer der LDAP-Gruppe „hwadmin“ zugehörig ist, wird dieser lokaler Administrator.

6.2.2 HwAdminGroup

Im Registry Key:
HKEY_LOCAL_MACHINE\SOFTWARE\PCS\GINA
"hwadmingroup"=""
wird definiert, welcher LDAP-Gruppe der Benutzer zugehörig sein muss, um HwAdmin werden zu können.

Beispiel:
„hwadmingroup“ = „hwadmin“

Wenn sich nun ein Benutzer auf einem Rechner anmeldet, wird überprüft, ob sich dieser in der Gruppe „hwadmin“ befindet. Wenn zusätzlich der Rechnernamen im „HwAdminAttribute“ vorkommt, wird dieser lokaler Administrator.

6.3 Standortabhängiges Zulassen / Verweigern von Logons

Der „LocationModus“ ermöglicht es, dass sich Benutzer nur bei bestimmten Standorten anmelden dürfen.
Ein LDAP-Benutzerobjekt kann primäre als auch alternative Standorte eingetragen haben, an welchen ein Logon erlaubt ist.

Zusätzlich kann man LDAP-Attribute des Standort-Objekts als Environment-Variablen exportieren, welche zB in „Logon-Scripts“, für vielseitige Zwecke, weiterverwendet werden können.

Anhand des Sub-Domain Part des FQDN des Rechners wird ein „StandortCode“ ermittelt welcher verwendet wird um das „Location-Object“ im LDAP ausfindig zu machen.

Beispiel:
ws1.vie.comtarsia.com → „vie“

In diesem Fall würde die LDAP-Suchanfrage um das Locationobjekt zu ermitteln, folgendermaßen aussehen:
„(&(objectclass=[LocationObjectClass])([LocationObjectCode]=vie)

Anschliessend wird aus dem LocationObject, der Parameter [LocationObjectAttribute] ausgelesen. Wenn dieser in einem der [LocationAllowedAttributes] vorkommt, wird der Logon erlaubt.
Zusätzlich werden die [LocationBasedEnvironment] Variablen als Environment Variablen exportiert.

Um diese Funktion so flexibel wie möglich zu gestalten, ist eine Vielzahl an Parametern zu konfigurieren.

6.3.1 EnableLocation

KEY: HKEY_LOCAL_MACHINE\SOFTWARE\PCS\GINA\LDAP
“EnableLocation” = DWORD:0

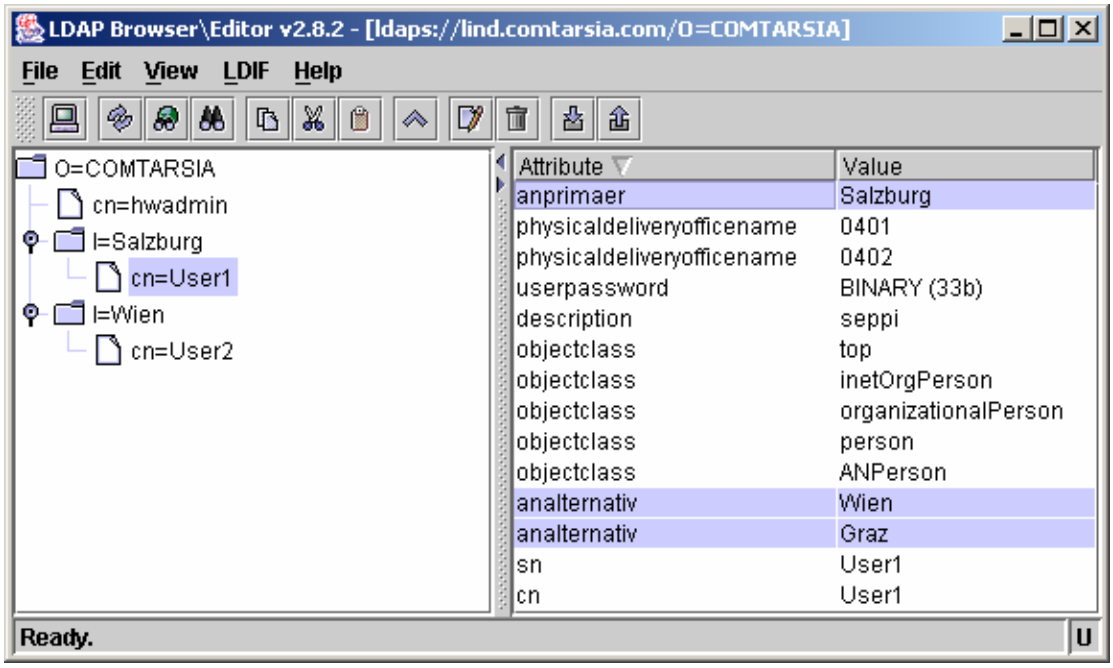
Mittels “EnableLocation” = DWORD:1 kann der „Location-Modus“ aktiviert werden.

6.3.2 LocationAllowedAttributes

KEY: HKEY_LOCAL_MACHINE\SOFTWARE\PCS\GINA\LDAP
“LocationAllowedAttributes” = „“

Gibt an in welchem LDAP-Attribut des Benutzerobjekts definiert ist, bei welchen Standorten der Benutzer sich anmelden darf.

Beispiel:
“LocationAllowedAttributes” = „ANPrimaer, ANAlternativ“

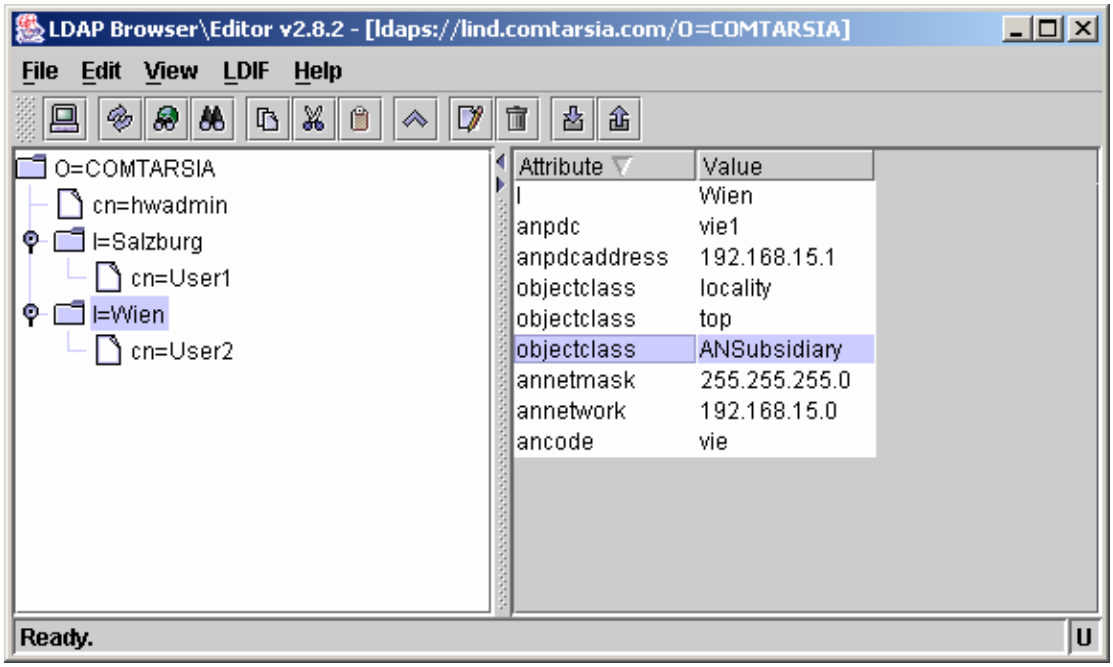


6.3.3 LocationObjectClass

KEY: HKEY_LOCAL_MACHINE\SOFTWARE\PCS\GINA\LDAP
“LocationObjectClass” = REG_SZ: „”

Gibt die Objektklasse des LDAP-Location Objektes an.

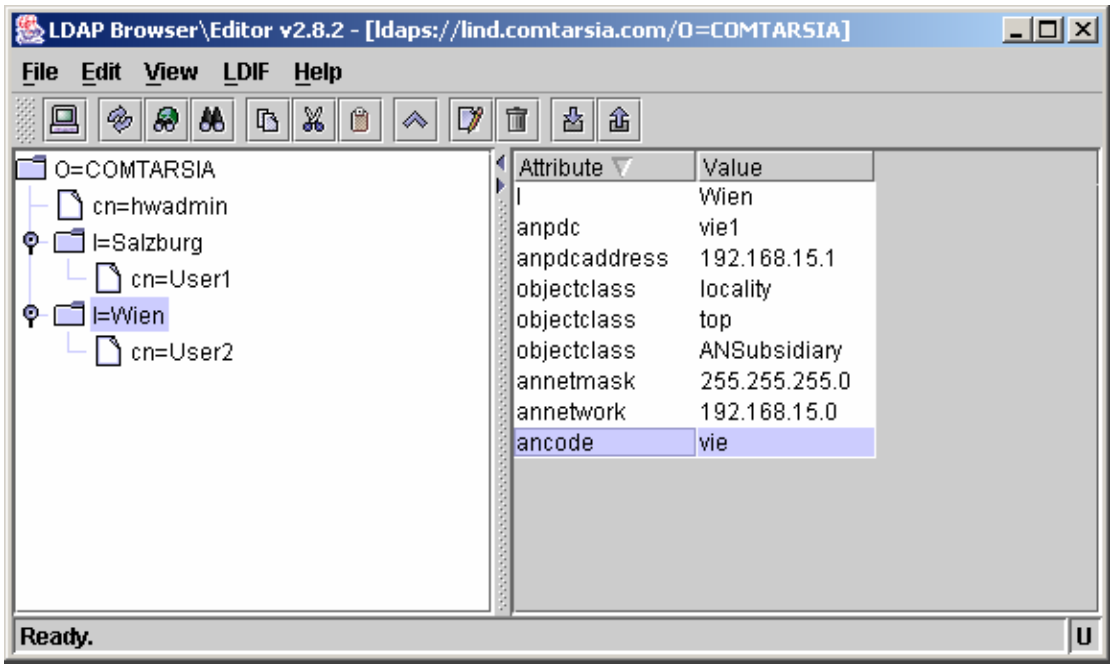
Beispiel:
“LocationObjectClass” = „ANSubsidiary“



6.3.4 LocationObjectCode

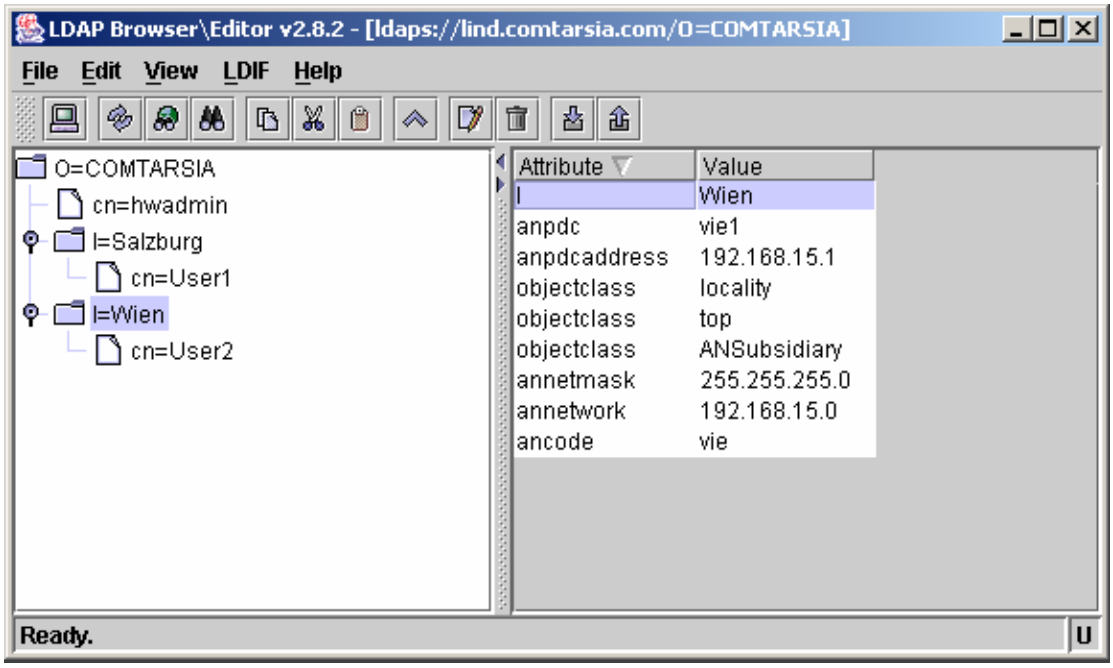
KEY: HKEY_LOCAL_MACHINE\SOFTWARE\PCS\GINA\LDAP
"LocationObjectCode" = REG_SZ: „ANCode"

Gibt das LDAP-Attribut des LocationObjects an, welches den Standortcode enthält. zB.: „vien"



6.3.5 LocationObjectAttribute

KEY: HKEY_LOCAL_MACHINE\SOFTWARE\PCS\GINA\LDAP
"LocationObjectAttribute" = REG_SZ „L"
Gibt an in welchem LDAP-Attribut des LocationObjectsder Standortname vermerkt ist. zB.: „Wien"



6.3.6 LocationBasedEnvironment

KEY: HKEY_LOCAL_MACHINE\SOFTWARE\PCS\GINA\LDAP
“LocationBasedEnvironment” = REG_MULTI_SZ: „“
Mit dieser Einstellung kann man Werte von Attributen des LocationObjects, als Environment Variablen exportieren.

zB.:
“LocationBasedEnvironment” = „L“

Bei der Anmeldung des Benutzers versucht der Logon Client das LDAP Attribut „L“ aus dem Locationobjekt auszulesen und exportiert den Inhalt des Attributes als Environment-Variable „L“.

Bei Bedarf kann auch ein Mapping vorgenommen werden, z.B.:
“LocationBasedEnvironment” = „L=Location“

In diesem Fall wird der Inhalt des LDAP Attributes „L“ als Environment-Variable „Location“ exportiert.

siehe: AttributeBasedEnvironment

6.3.7 Die Variable VALID_LOCATION

Die Variable %VALID_LOCATION% ist immer dann gesetzt, wenn eine Lokationsüberprüfung stattgefunden hat. Ist der aktuelle Benutzer für die Anmeldung an der momentanen Lokation zugelassen, so enthält die Variable den Wert „1“. Findet keine Lokationsüberprüfung statt, zB weil eine lokale Anmeldung durchgeführt wurde, so ist diese Variable nicht gesetzt.

7. Serverspezifische LDAP Konfigurationen

7.1 Netscape Directory Server LDAP-Schema

7.1.1 Das Comtarsia Schema

Das Comtarsia LDAP Schema wird gemeinsam mit dem Comtarsia Logon Client ausgeliefert und dient zur Erweiterung des LDAP Schemas eines LDAP-Servers. (genaue Anweisungen siehe unten)

Nachdem das Comtarsia LDAP Schema in den LDAP Server eingespielt wurde, steht nun der volle Umfang der Comtarsia Logon Client Funktionalitäten zur Verfügung: Verzeichnis- und Druckerfreigaben, Netzwerkapplikationen, Benutzerverzeichnis, Profile Pfad und vieles mehr.

Um diese erweiterten Funktionalitäten zu nutzen, müssen die LDAP Benutzerobjekte mit der entsprechenden CLC-Objektklasse sowie den benötigten CLC-Attributen erweitert werden. Die Benutzer können weiterhin in der gewohnten LDAP-Administrationsoberfläche verwaltet werden und es steht der volle Funktionsumfang des Comtarsia Logon Client zur Verfügung.

Es existieren zwei verschiedene Varianten des Comtarsia LDAP Schemas:

- Die erste Version ist primär für Neuinstallationen gedacht, in welchen erst nach diesem Schritt die Directory-Server-Benutzer angelegt werden.

  Das Benutzerobjekt besteht hier aus der "**structural object class CLCPerson"**, welche standardmässig von der Objektklasse „inetorgperson" abgeleitet ist (dies kann, wenn benötigt, auf eine beliebige andere structural object class geändert werden).
  Die CLC LDAP-Attribute können einem Objekt vom Typ CLCPerson zugewiesen werden.

- Die zweite Version des Comtarsia LDAP Schemas steht für LDAP Server zur Verfügung, welche eine bereits bestehende Benutzerdatenbank haben und nur um die Comtarsia spezifischen Attribute erweitert werden sollen.
  Die Benutzer bekommen die "**auxiliary object class"** CLCPerson zugewiesen, wodurch es möglich wird, CLC LDAP-Attribute den Benutzern zuzuweisen.

7.1.2 Einbinden des Comtarsia Schema

Der LDAP-Server muss beendet werden.

Die Comtarsia Schema-Datei muss in das Schema-Verzeichnis des Netscape Servers kopiert werden (...\config\schema).

Started des LDAP-Servers. Die Comtarsia-spezifischen LDAP Objekte und Attribute stehen nun zur Verfügung.

7.1.3 Das CLCPerson Benutzerobjekt

7.1.3.1 Erzeugen eines neuen „CLC Person“ Benutzers

(Verwendung der **structural** „CLCPerson“ object class)

Um einen neuen Benutzer herzustellen auf den entsprechenden Container klicken (z.B.People), „**New**“ auswählen.
„**Other**“ aus der Liste wählen, => **CLCPerson**.
Felder mit Benutzerdaten ausfüllen.

Auf “**Advanced Properties**” => “**Add attribute**” klicken;
CLC-Attribute aus der Liste wählen, dazugeben, Felder mit entsprechenden Daten ausfüllen.

7.1.3.2 Erweitern eines bestehenden Benutzers

(Unter Verwendung der Schema-Datei **auxiliary** „CLCPerson“ object class)

Wenn sich die LDAP-Datenbank bereits in Produktion befindet und Benutzerkonten beinhält, bietet diese Variante die Möglichkeit, die bestehenden Benutzerobjekte mit einer „auxiliary object class“ zu erweitern.

Auxiliary Objekt Klassenname: CLCPerson.
Attribute: CLCShareName, CLCProfilePath, CLCNetworkApplication

Benutzer auswählen => „**Advanced Properties**“ im Directory.

Auf „**Object class**“ klicken => „**Add value**“.
„**CLCPerson**“ aus der Liste auswählen und hinzufügen.

Jetzt können die Comtarsia LDAP-Attribute dem Benutzern zugeordnet werden.
„**Add Attribute**“ auswählen, CLCShareName, CLCProfilePath und CLCNetworkApplication hinzufügen, Felder mit entsprechenden Daten ausfüllen.
Vorausgesetzt, dass die **CLC LDAP** Objekte (Verzeichnis und Druckershares, Netzwerkapplikationen,etc.) **schon angelegt** sind, alle (wie oben beschrieben) konfigurierte Benutzer sind in der Lage die Freigaben zugeteilt bekommen, und die Ressourcen nach dem Logon mit Comtarsia Logon Client2006 zu verwenden.

7.1.3.3 Unterstützung für “Password expiration”

Der Comtarsia Logon Client2006 bietet Unterstützung für die Netscape/iPlanet/Sun One Directory Server Password Policies.
Eine eventuelle Passwort-Warnung des Servers wird dem Benutzer während des Logons dargestellt und es wird die Möglichkeit geboten, einen Passwortwechsel durchzuführen, bevor dass Passwort endgültig abläuft.

7.2 IBM Directory Server 5.1

Dieses Kapitel beschreibt die minimalen Konfigurationsschritte eines IBM Directory Server 5.1 zur Zusammenarbeit mit dem Comtarsia Logon Client. Weitere Informationen bezüglich des IBM Directory Servers finden sich in der Online-Hilfe sowie in den Referenzen am Ende dieses Dokumentes. [1]

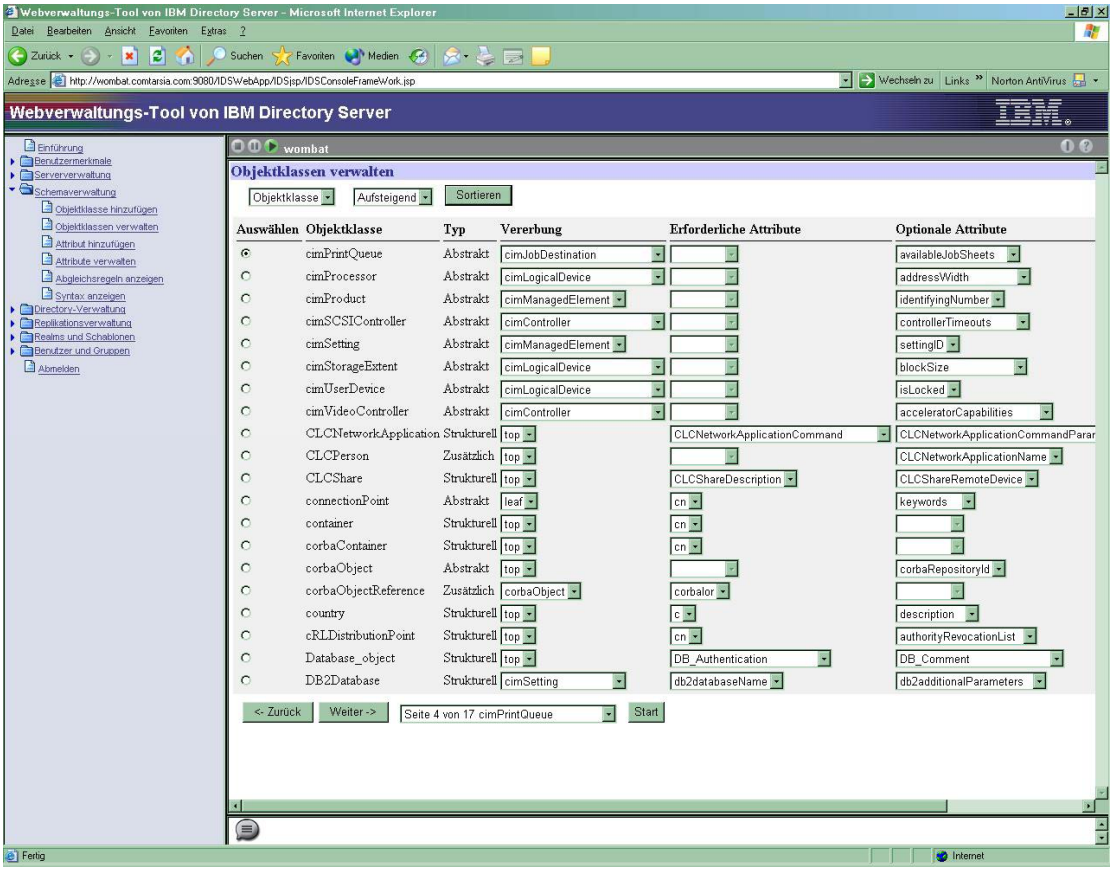
7.2.1 Verwendung des Comtarsia LDAP-Schema

Mit dem Tool "/usr/bin/**ldapxcfg", im Abschnitt** "**Manage schema files**" kann die Comtarsia Schema Datei zu den bestehenden LDAP Schema Dateien des IBM Directory Server hinzugefügt werden.
Es wird empfohlen, diese Datei im vom Server vorgeschlagenen Verzeichnis abzulegen. (unter UNIX z.B.: /etc/ldapschema/comtarsia.schema.ibmds)

Als nächstes muss der Directory Server neu gestartet werden, um die neuen LDAP Objekte und Attribute zu aktivieren.

Die folgende Objektklassen (und die entsprechende Attribute) werden unter "**Schema Verwaltung**/ Objektklassen Verwalten auf der Webverwaltungs-Tool GUI erscheinen:

- **CLCNetworkApplication**: Strukturell
- **CLCPerson**: Zusätzlich
- **CLCShare**: Strukturell

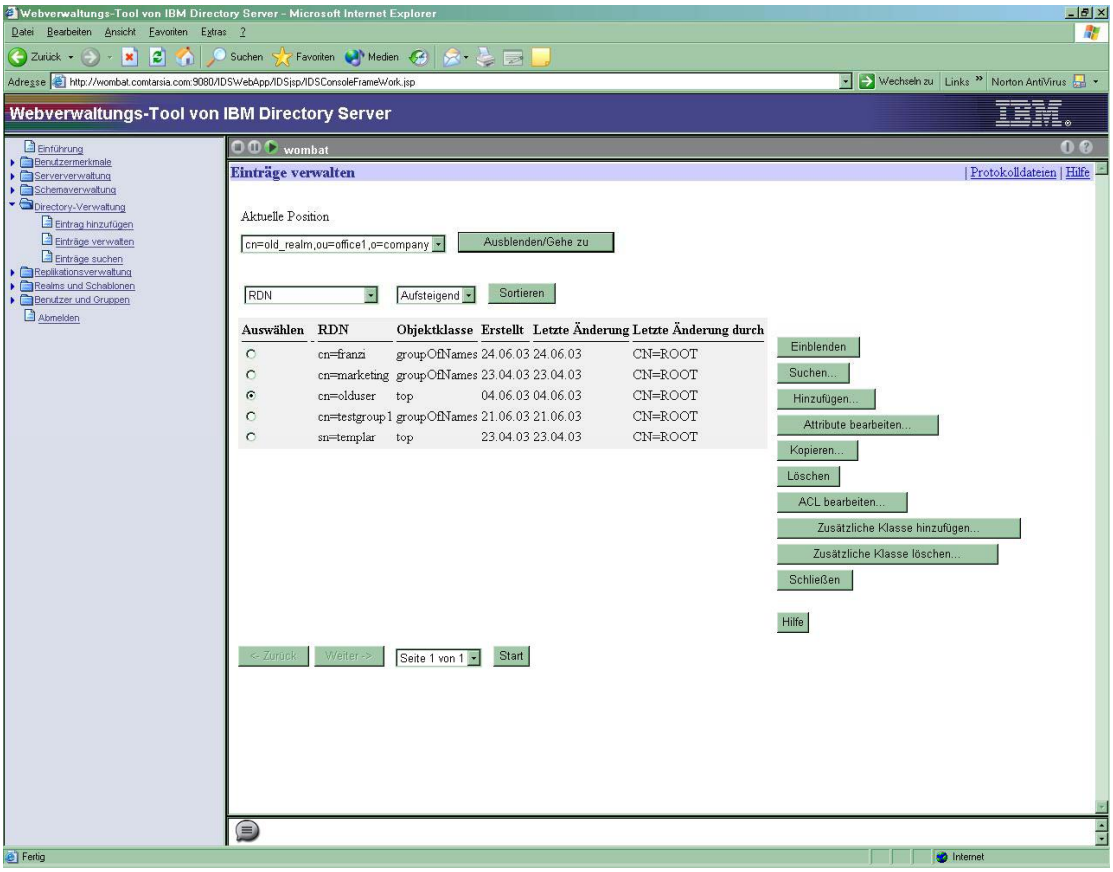


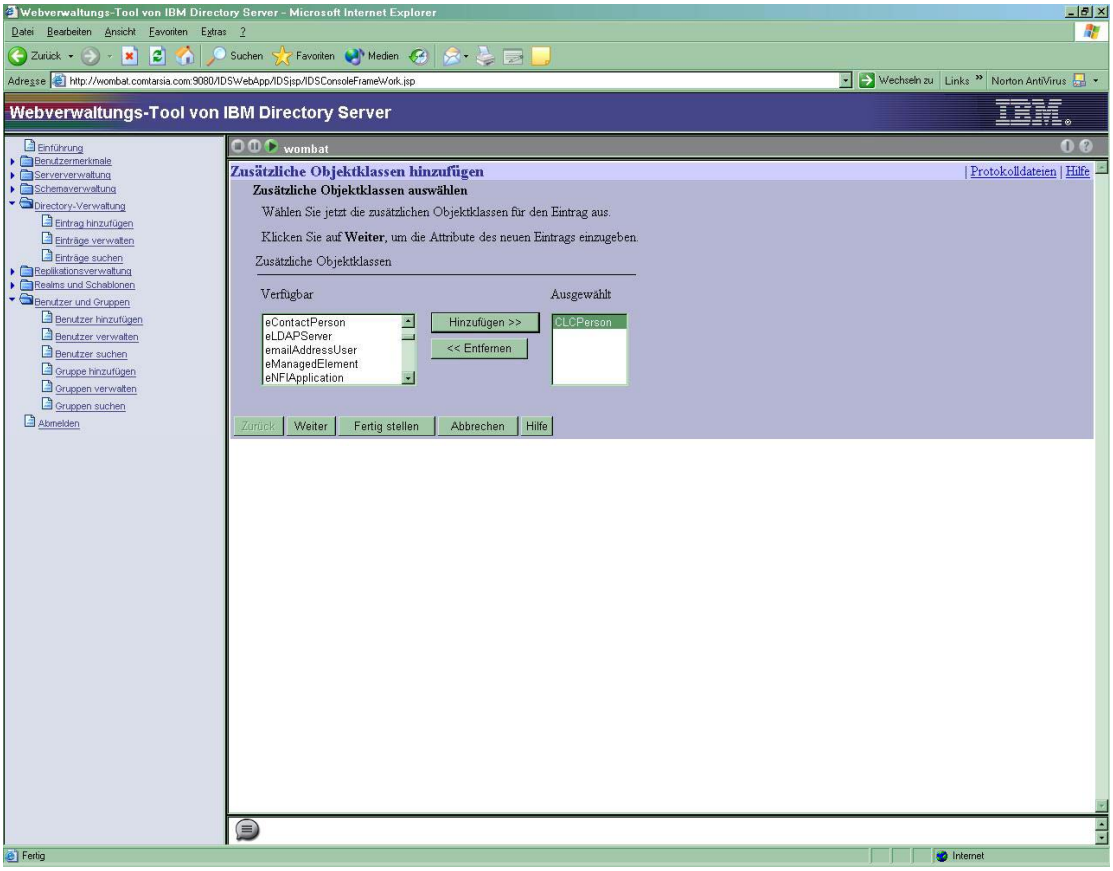
7.2.2 Hinzufügen von Attributen zu Benutzern

Um CLC LDAP-Attribute den Benutzerobjekten hinzufügen zu können, muss diese zuerst mit der **“CLCPerson” auxiliary object class** erweitert werden.

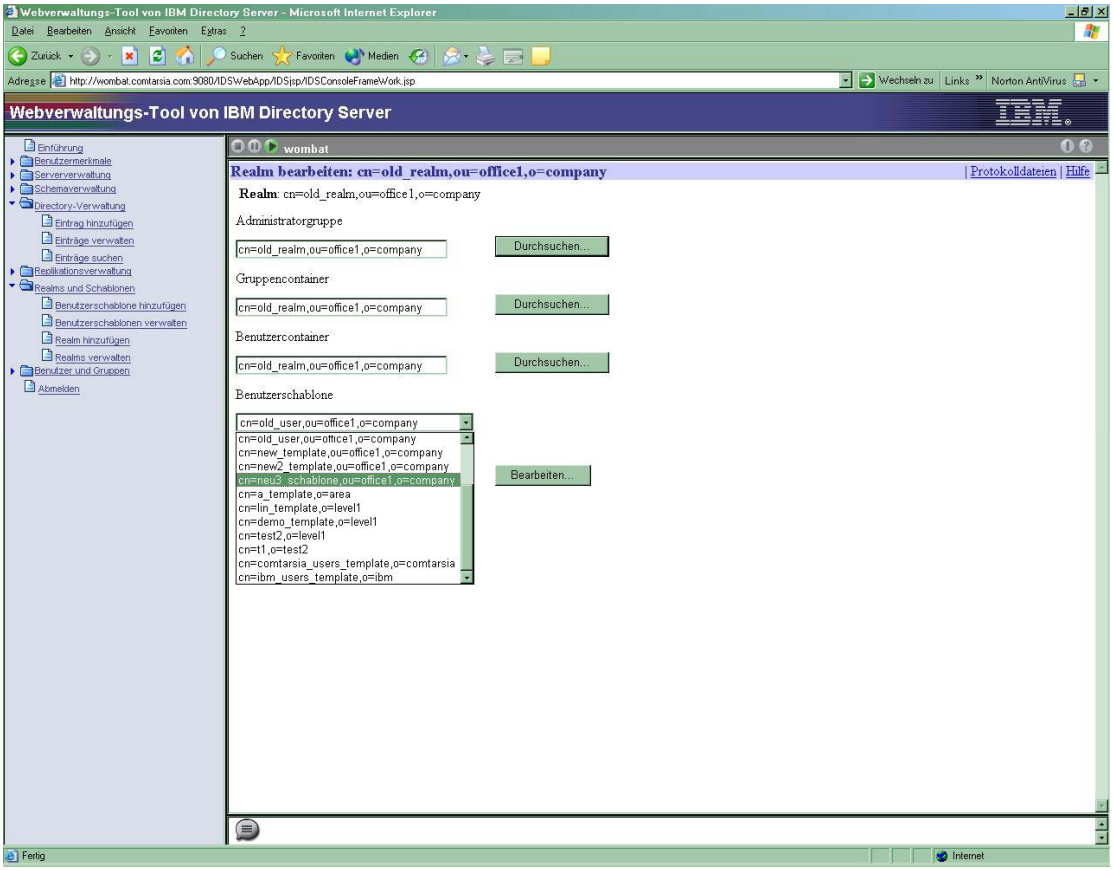
Es sollte zwischen Benutzer, die bereits vor dem Einspielen des Comtarsia Schema angelegt worden sind und Benutzern die nach der Schema-Erweiterung weitere angelegt wurden unterschieden werden: es gibt unterschiedliche Lösungen für beide.

Schon angelegte Benutzer können unter „Directory Verwaltung“ => Einträge Verwalten, geändert werden.





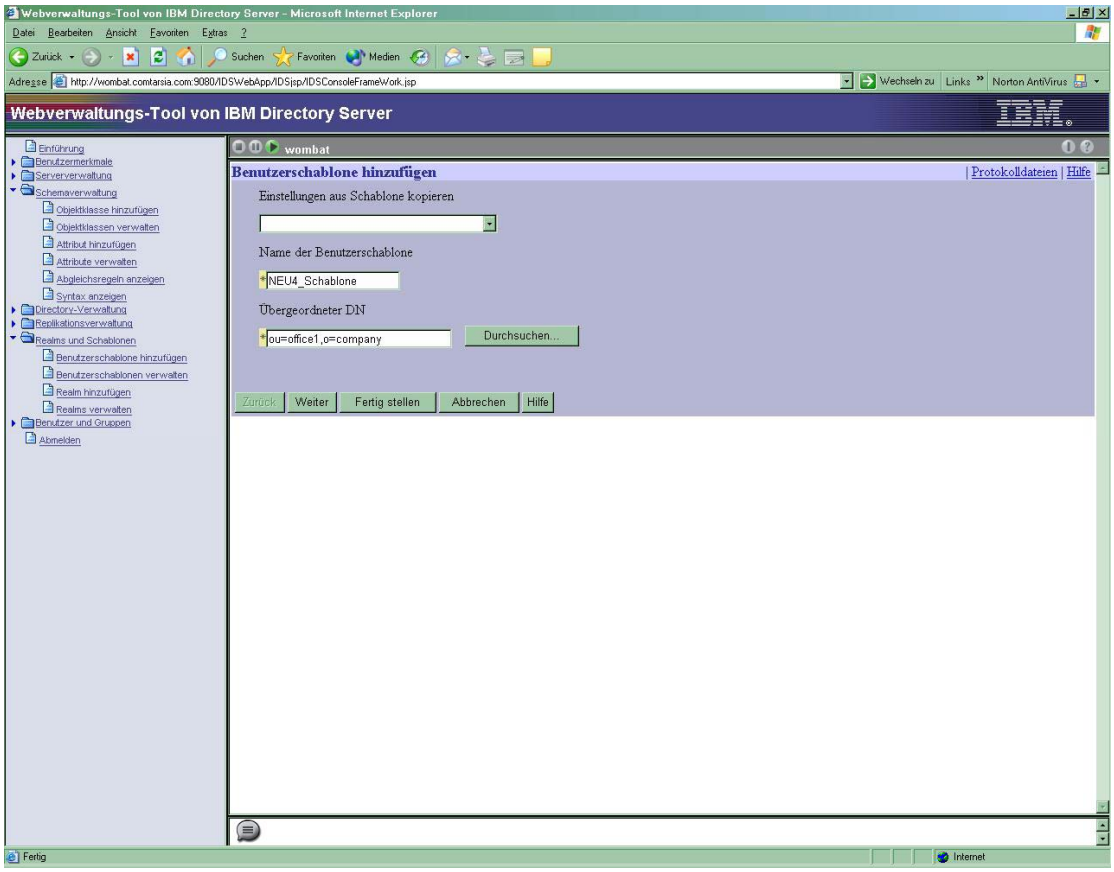
Unter “Other attributes” sind die CLC LDAP-Attribute verfügbar zur Zuweisung. Falls viele bestehende Benutzerkonten erweitert werden sollen, bietet sich an, ein neues Benutzertemplate zu erzeugen, welches bereits die CLC LDAP-Attribute beinhält. Das bereits bestehende Benutzertemplate kann durch das neue ersetzt werden.



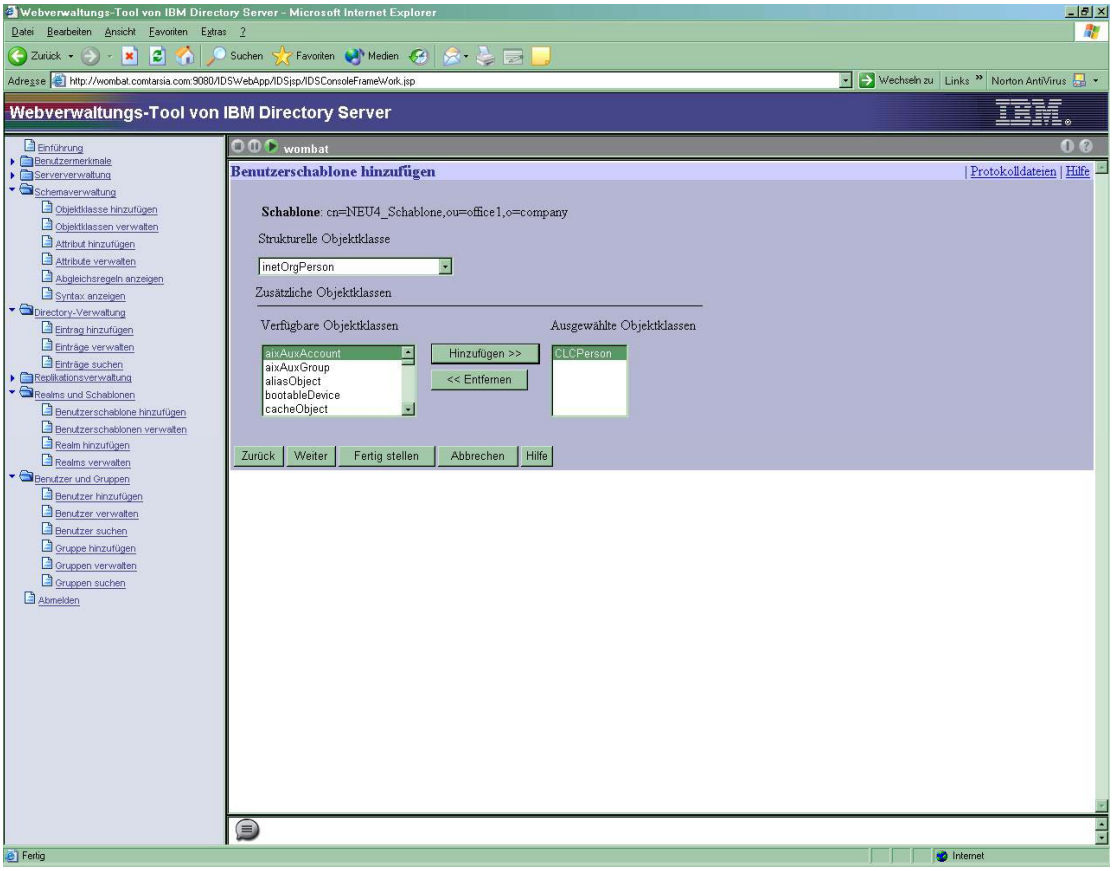
Die Hilfs-Objektklasse “CLCPerson” wird in diesem Fall dem neuen Benutzer-Template hinzugefügt, siehe „Realms Verwalten/Realm bearbeiten“.

Neue Benutzer
Wird die Benutzerdatenbank neu erzeugt, werden neue Realms basierend auf den neuen Templates erzeugt. Neue Benutzer haben automatisch die CLC LDAP-Attribute verfügbar.

7.2.3 Erzeugen eines neuen Benutzer-Templates

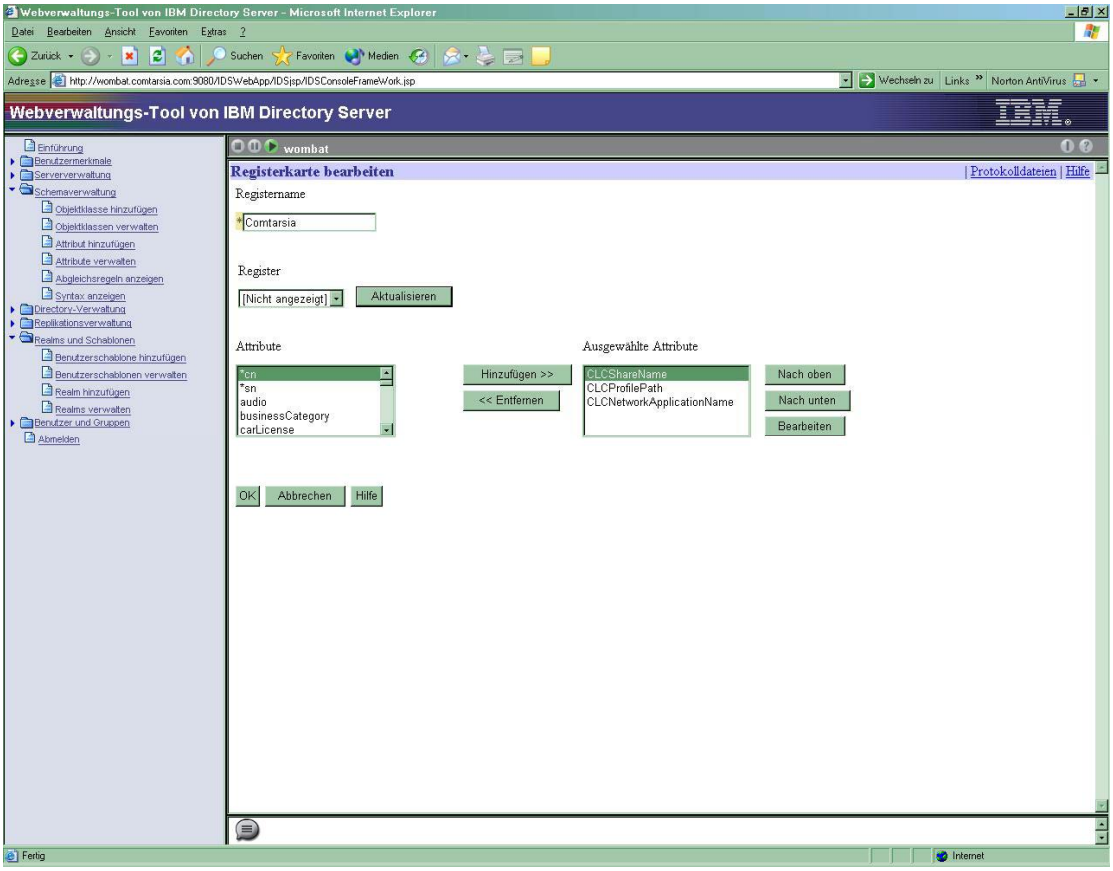


Fügen Sie “CLC Person” Behelfsklasse hinzu.



Die nächsten Schritte:

- Für dieses Beispiel wird das “Naming attribute” auf “**cn**” geändert
- Im Reiter “Required” muss das Attribut “**userPassword**” hinzugefügt werden
- Ein neuer Reiter Namens “Comtarsia” wird erzeugt. Dieser enthält die Comtarsia-spezifischen LDAP-Attribute.
  Diese können an der Registerkarte (an dem Reiter) eingegeben werden.

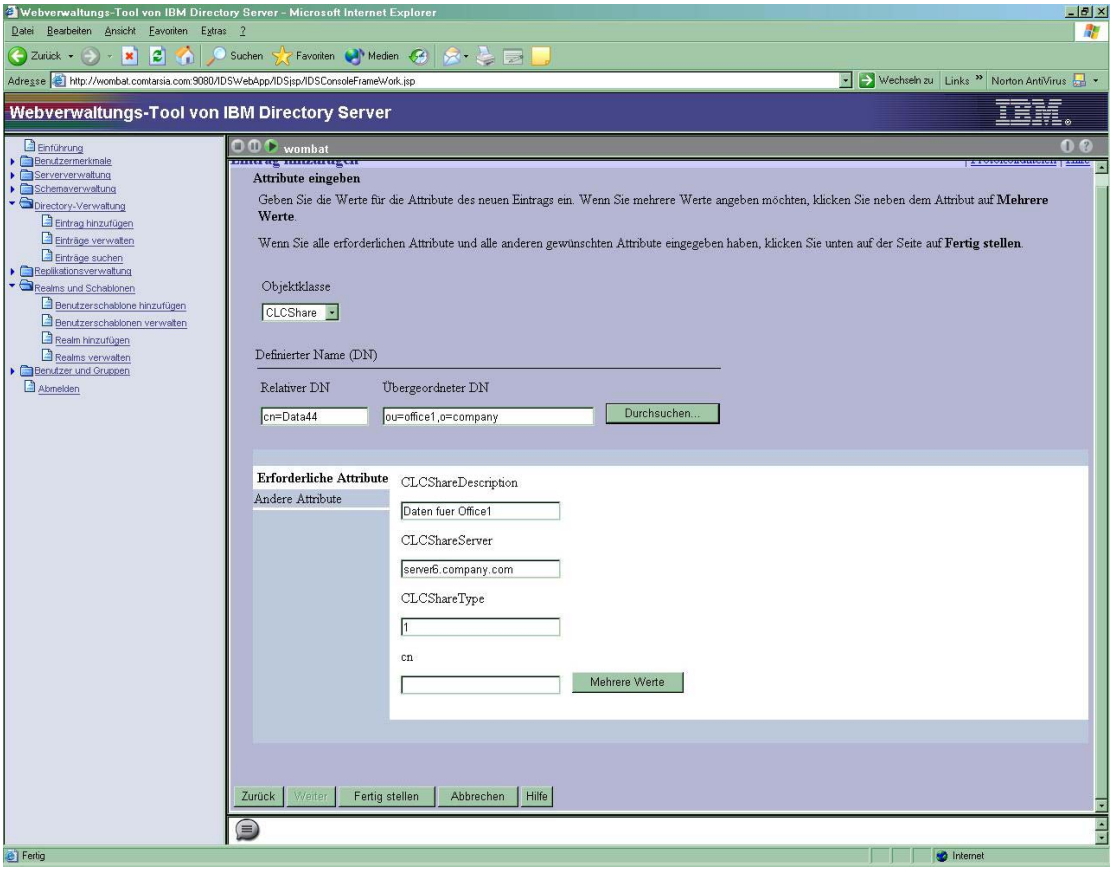


Neue Realms werden basierend auf diesem Template erzeugt, oder bestehende Realms können mit diesem Template erweitert werden.
In beiden Fällen stehen die Comtarsia spezifischen Attribute sofort zur Verfügung.

7.2.4 Erzeugen von Freigaben und Netzwerkapplikationen

Freigaben werden unter dem Menüpunkt “Directory Management/**Add an entry/Structural object class**” erzeugt.
Nach der Auswahl von “**CLCShare**” als structural object class können die LDAP-Attribute mit Daten befüllt werden.

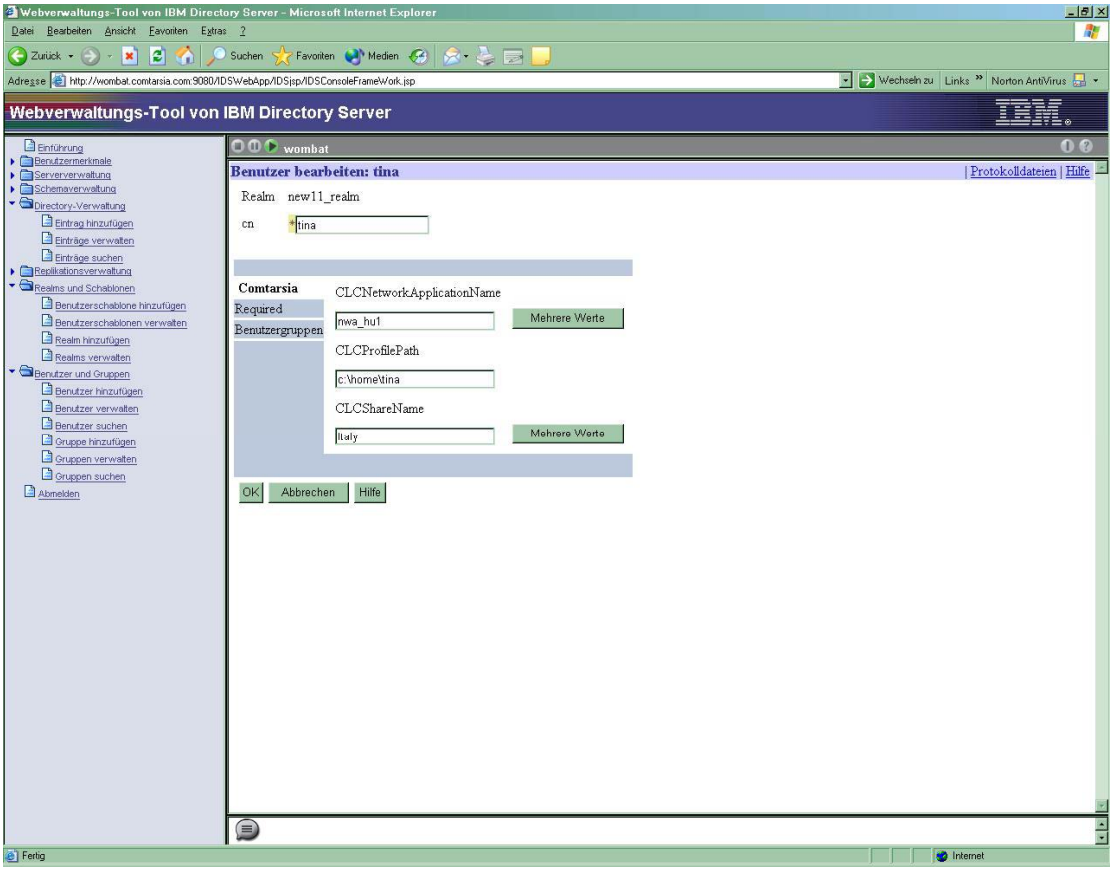
Um Netzwerkapplikationen zu erzeugen wird als “ **Structural object class“** “**CLCNetworkApplication**” ausgewählt. Anschliessend müssen die Attribute entsprechend befüllt werden.



WICHTIG:
Zur Zuweisung von Freigaben oder Netzwerkapplikationen zu einem Benutzer ist es nötig, die zum Benutzerobjekt gehörenden Comtarsia LDAP-Attribute zu befüllen.

Um einen bestehenden Benutzer zu überarbeiten, wird unter "/Users and Groups/Manage users" der Benutzer ausgewählt und unter „Edit user" können die Attribute auf dem zuvor angelegten Reiter „Comtarsia" bearbeitet werden. (Voraussetzung ist, das dass Template dem entsprechenden Realm zugeordnet wurde).

Bei neuen Benutzern können die Attribute direkt während des Anlege-Vorgangs befüllt werden. (Für weitere Informationen siehe [4]).


Webverwaltungs-Tool von IBM Directory Server – Microsoft Internet Explorer
Webverwaltungs-Tool von IBM Directory Server
wombat
Benutzer bearbeiten: tina
Protokolldateien | Hilfe
Realm new11_realm
cn *tina
Comtarsia
Required
Benutzergruppen
CLCNetworkApplicationName
nwa_hu1
Mehrere Werte
CLCProfilePath
c:\home\tina
CLCShareName
Italy
Mehrere Werte
OK
Abbrechen
Hilfe
Einführung
Benutzermerkmale
Serververwaltung
Schemaverwaltung
Directory-Verwaltung
Eintrag hinzufügen
Einträge verwalten
Einträge suchen
Replikationsverwaltung
Realms und Schablonen
Benutzerschablone hinzufügen
Benutzerschablonen verwalten
Realm hinzufügen
Realms verwalten
Benutzer und Gruppen
Benutzer hinzufügen
Benutzer verwalten
Benutzer suchen
Gruppe hinzufügen
Gruppen verwalten
Gruppen suchen
Abmelden

7.2.5 Passwort Richtlinien

Der Comtarsia Logon Client bietet volle Unterstützung für alle Passwort-Richtlinien-Einstellungen des IBM Directory Servers 5.1.

Relevante Meldungen des LDAP-Servers (Passwort-Wechsel, Passwort-Expire, Gesperrtes Benutzerkonto, etc.) werden zur Logon-Zeit dem Benutzer zur Darstellung gebracht und es werden entsprechende Aktionen angeboten. (z.B.: Passwort-Wechsel).

Die Überprüfung des Passwort-Syntaxes durch des Server wird ebenfalls unterstützt und der Benutzer wird bei Verfehlungen informiert.

Für weitere Informationen über die LDAP Password Policy siehe unter IETF Internet draft in [5].

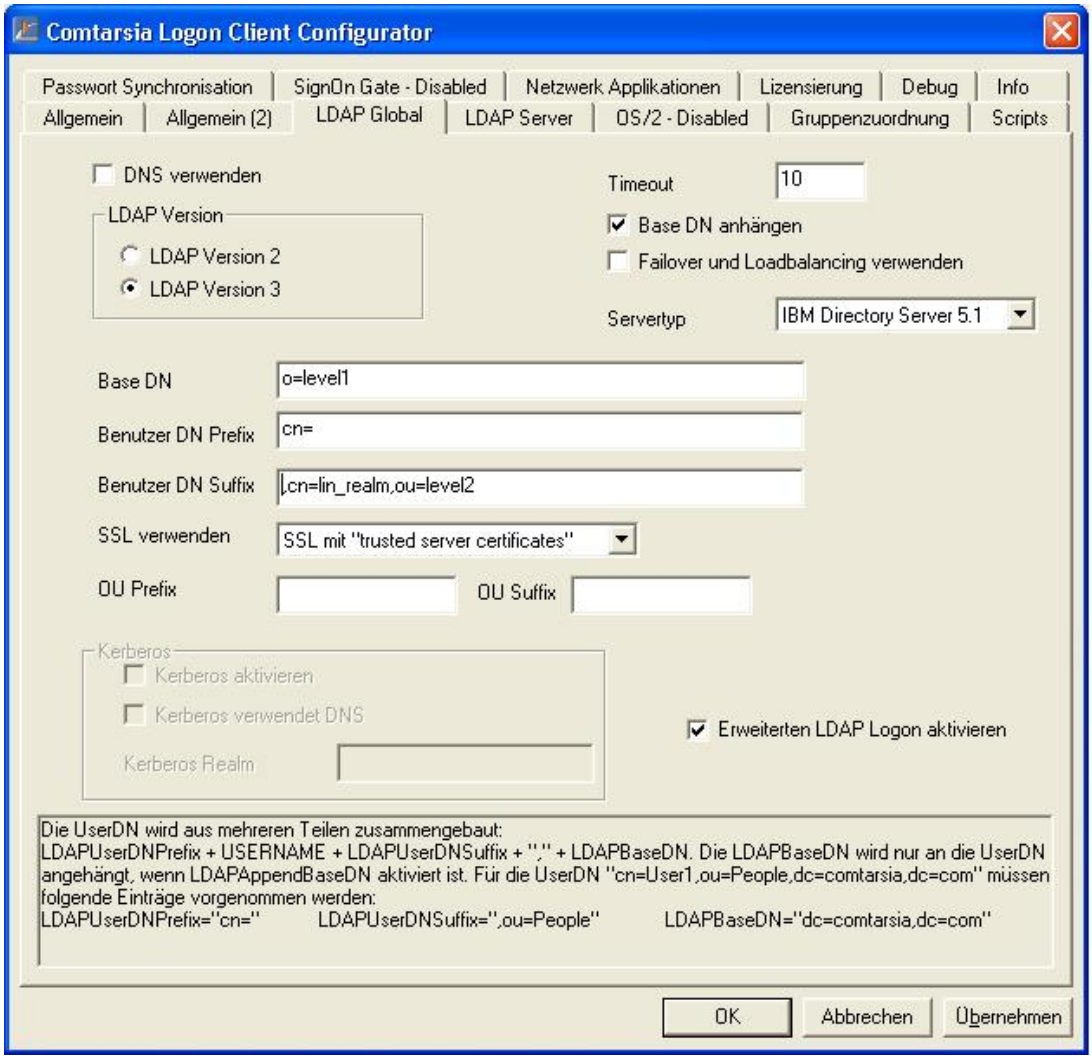
7.2.6 IBM DS specific settings on the Logon Client (Wichtigste Einstellungen des Logon Clients zur Anmeldung an einem IBM DS)

Nachfolgend eine Beschreibung der wichtigsten Einstellungen des Logon Client Konfigurators zur Anmeldung an einen IBM Directory Server.

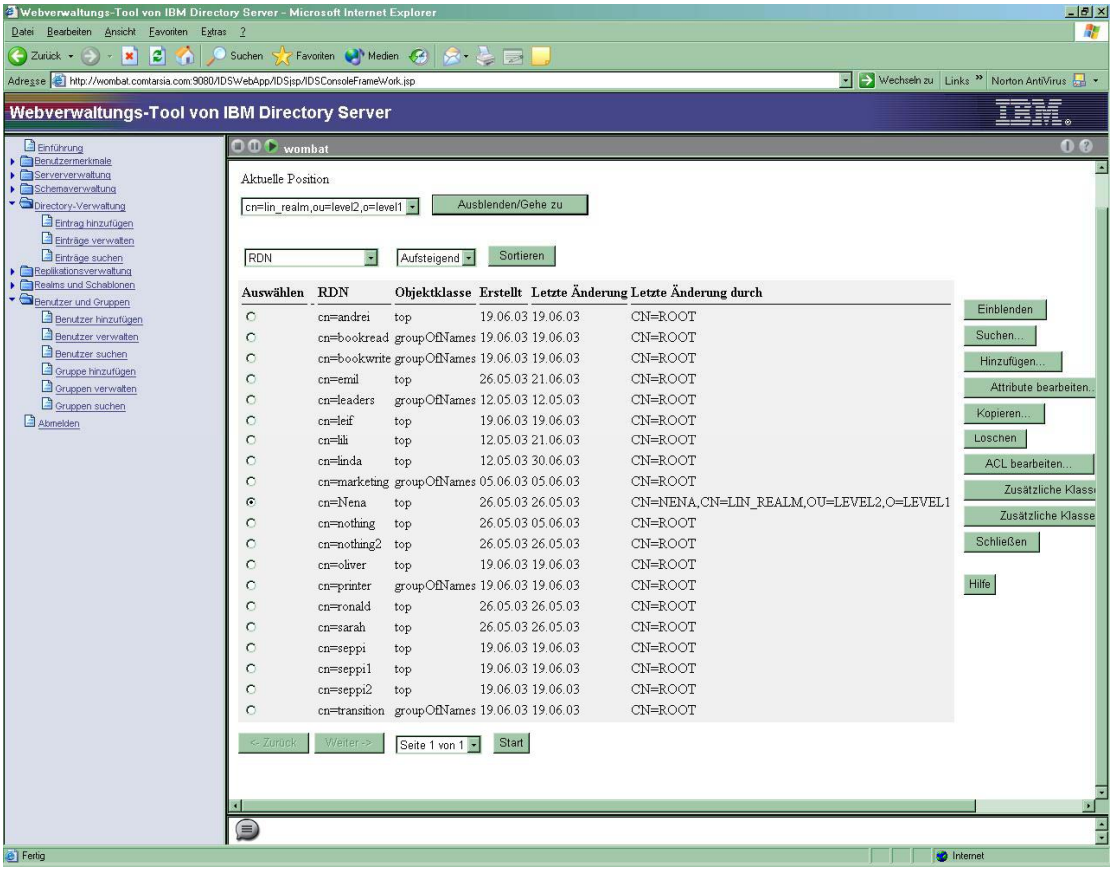
LDAP Global

- Aktivieren von "**Append BaseDN**" (für weitere Informationen siehe Kapitel **4.2** **)**
- Server Typ: **IBM Directory Server 5.1**
- Die Benutzer-DN ergibt sich aus den folgenden Einstellungen
    - Base DN, in diesem Beispiel "**o=level1**"
    - User DN Prefix "**cn=**"
    - User DN Suffix ist der verbleibende Teil zwischen Benutzername und der BaseDN, beginnend mit einem ","; z.b: "**,cn=lin_realm,ou=level2**"

Hiermit ergibt sich diese Benutzer-DN:
cn="username",cn=lin_realm,ou=level2,o=level1



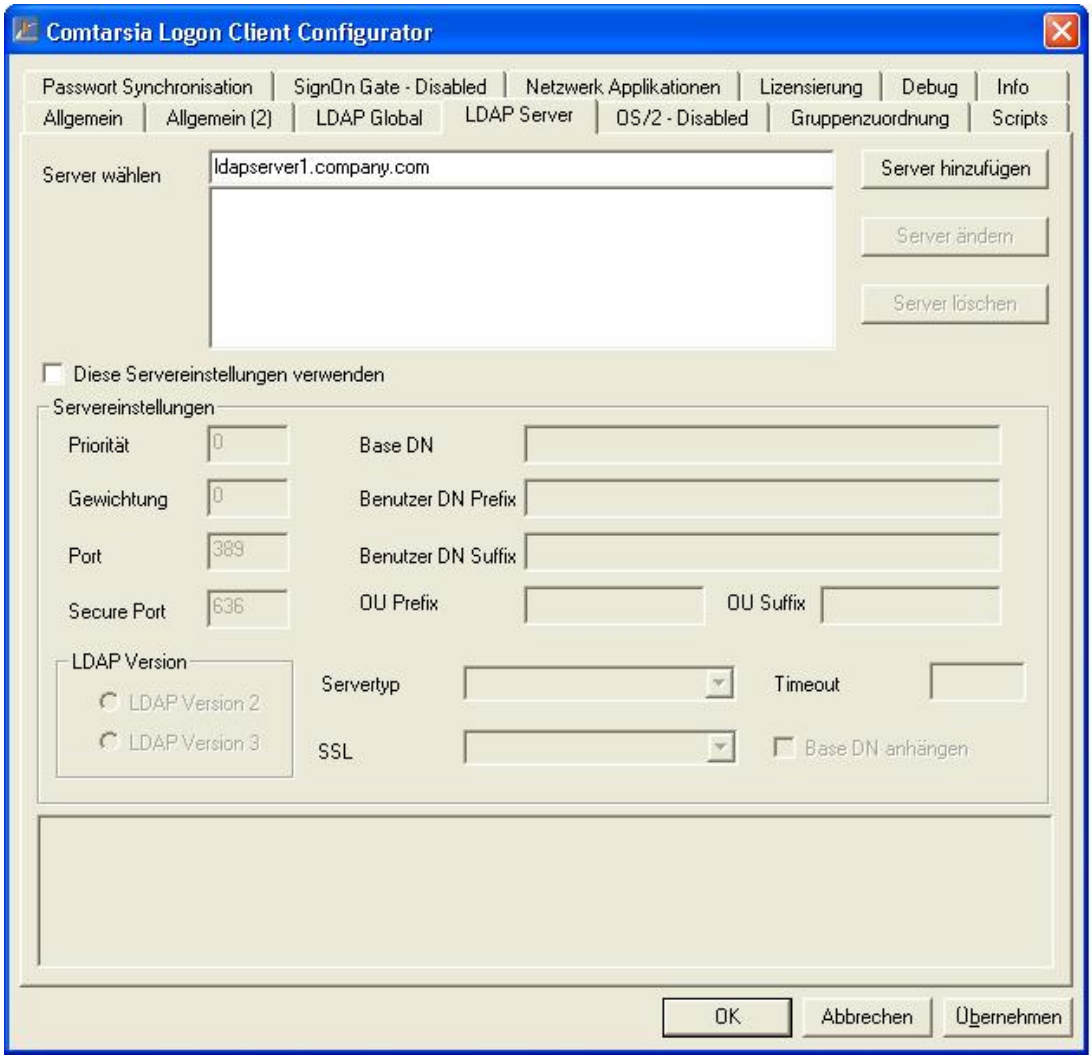
Die nachfolgende Abblidung zeigt ein Benutzerobjekt im Kontext der Verzeichnisstruktur, entsprechend den zuvor vorgenommenen Einstellungen.



LDAP Server

Nun muss noch der Hostname des LDAP-Servers wie in der unten gezeigten Abbildung eingetragen werden.

Der Logon Client ist nun für eine LDAP-Anmeldung bereit.



SSL-Konfiguration

Informationen zur SSL-Konfiguration des IBM Directory Server 5.1 finden sich unter [6].

Obwohl eine funktionierende SSL-Konfiguration und weiterführend auch SSL-Kommunikation für die Zusammenarbeit von Directory Server und Logon Client nicht zwingend notwendig ist, wird trotzdem empfohlen, im Produktionsbetrieb ausschliesslich SSL zu verwenden.

7.3

IBM Directory Server 5.1 unter Red Hat 7.3 installieren

Voraussetzung: Abgeschlossene Installation von RedHat 7.3

7.3.1 Installation

Installation aller Directory Server rpm-Pakete. [2]

Installation des **Clients:**
>rpm -ihv ldap-clientd-5.1-1.i386.rpm

Installation des LDAP **Servers**:
>rpm -ihv ldap-serverd-5.1-1.i386.rpm

Wenn die Installation erfolgreich gewesen ist, erscheint folgende Meldung:
ldap-clientd-5.1-1
ldap-serverd-5.1.1

Die sprachenabhängige Meldungen, bzw. Dokumente werden wie folgt installiert (an der Kommandozeile eingegeben):
>rpm -ihv ldap-msg-xxx-5.1-1.i386.rpm
>rpm -ihv ldap-html-xxx-5.1-1.i386.rpm

Das Web Administraton Tool mit aktiviertem SSL ist mit diesem Befehl an der Kommandozeile zu installieren:
>rpm -ihv ldap-webadmind-5.1-1.i386.rpm

Installation des gskbas-5.0-4.rpm für **SSL Konfiguration**:
>rpm –ihv gskbas-5.0-4.rpm

7.3.2 Start

Den Directory **Server** starten:
>**ibmslapd**

Um den Webserver zu starten / stoppen:
>appsrv/bin/start(stop)Server.sh server1

Die GUI für die LDAP-Server Administration steht nun unter
>http://ldapsrv.comtarsia.com:9080/IDSWebApp/IDSjsp/Login.jsp
zur Verfügung.

Die SSL Konfiguration kann mit dem GSKit 5.0 durchgeführt werden:
>**gsk5ikm**.

7.4 Lotus Domino

Voraussetzungen:
Lotus Domino ab Release 5
Comtarsia Logon Client2006 Build >= 3.1.27.4

Installation und Konfiguration von Lotus Domino 6 für die Verwendung mit dem Comtarsia Logon Client2006

Dieses Kapitel beschreibt eine erforderliche Minimalkonfiguration des Lotus Domino Directory Servers um mit dem Comtarsia Logon Client2006 optimal zusammenarbeiten zu können.
Weitere Information über Lotus Domino finden sich in der Notes Client Online Hilfe oder in den Referenzen am Ende dieses Dokumentes.

Für einen Testbetrieb mit dem Comtarsia Logon Client ist die Verwendung von SSL nicht zwingend erforderlich, bei einem Produktiveinsatz wird die Verwendung von SSL dringend empfohlen.

7.4.1 Domino Schreibzugriffsberechtigung via LDAP

Die folgenden Konfigurationsschritte sind erforderlich, damit ein Client sein Domino-Passwort über LDAP ändern kann.
Achtung: bei Domino Release 6 werden Passwort-Änderungen über LDAP erst nach einigen Minuten aktiv, bei Domino Release 6.5 werden Passwort-Änderungen sofort aktiv.

- Domino Administrator öffnen
- „Configuration“ -> Directory-> LDAP -> Settings wählen
- Beim ersten Zugriff erscheint die Frage, ob ein neues Dokument erstellt sein soll, dies muss mit “yes” beantwortet werden.
- LDAP auswählen
- „Allow LDAP-User write access“ auf “yes” stellen und speichern
- Den Domino Server neu starten

7.4.2 SSL Konfiguration

Um eine Kommunikation mit dem Domino Server über SSL zu ermöglichen, muss dieser über ein SSL-Zertifikat verfügen.
Die zum Testen einfachste Lösung ist, ein selbsterzeugtes “Self-Signed” Zertifikat zu generieren.

1. „Server Certificate Admin Database“ (certsrv.nsf) öffnen und die Option “Create Keyring with self signed certificate” auswählen um ein “Self Signed Certificate” zu erstellen.
2. Domino Administrator öffnen
3. Der Key-Dateiname ist nun zu konfigurieren:

Configuration->Server->Current Server Document->
Ports->Internet Ports->SSL keyfile name (Key-Datei)

4. Im Document Server->Current Server Document->Ports->Internet Ports->Directory ist “SSL Port Status” auf “enabled” zu setzen und “SSL Name and Password” auf muss auf “yes” gesetzt sein.

Weitere Information über die Domino SSL Konfiguration siehe unter [3,4].

7.4.3 Installation des Comtarsia Templates

Dieser Schritt ist optional und wird nicht benötigt, wenn der Domino Server nur zur Authentifizierung/Passwortwechsel/Gruppenzuordnungen verwendet werden soll.

Mittels des Comtarsia Templates können Attribute wie Netzwerklaufwerke und Zuordnungen sowie Netzwerkapplikationen bequem in der gewohnten Domino-Oberfläche für alle Arbeitsplätze verwaltet werden.

Die Comtarsia spezifischen Designelemente sind erst ab Domino Release 6 auch über die Web-Oberfläche administrierbar.

7.4.3.1 Signen des Comtarsia Templates

- Domino Administrator öffnen
- Wechseln in die “Files-View”
- Rechte Maustaste auf “clcnames.ntf”->Sign
- “Active Server’s ID” / sign ”All design Documents”
- Dies erstellt einen Admin Request welcher mittels “tell adminp process new” sofort ausgeführt werden kann

7.4.3.2 Kopieren der Comtarsia Designelemente

In der Template-Datei „clcnames.ntf“ befinden sich die Comtarsia spezifischen Designelemente

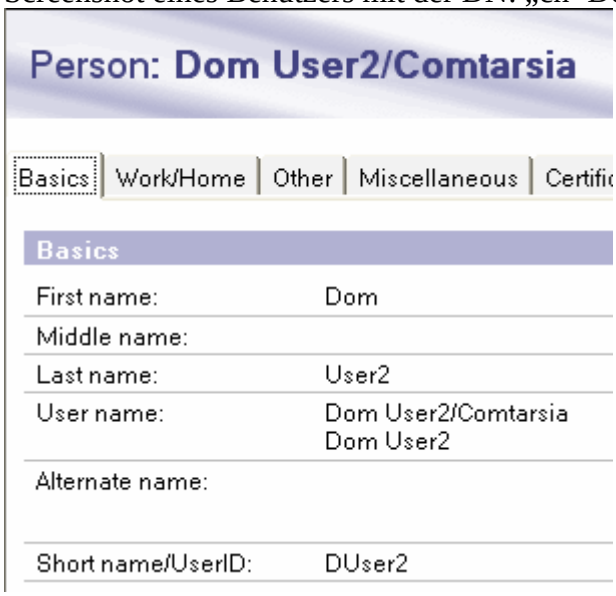
- Öffnen von „names.nsf“ und „clcnames.ntf“ im Domino Designer
- Alle Designelemente der „clcnames.ntf“ in die „names.nsf“ kopieren (2 Forms, 2 Views, 1 Shared Code/Agent, 3 Subforms)
- Im „names.nsf“ unter Subforms „$PersonExtensibleSchema“ auf hidden setzen (unter Eigenschaften)
- Die Rollen „CLCCreator“ und „CLCModifier“ in die ACL der „names.nsf“ eintragen und der „Admin“ Gruppe sowie der „Localdomainservers“ Gruppe zuweisen
- Auf der Konsole den Befehl „load updall –r names.nsf“ ausführen

7.4.4 Hierarchische Objekte

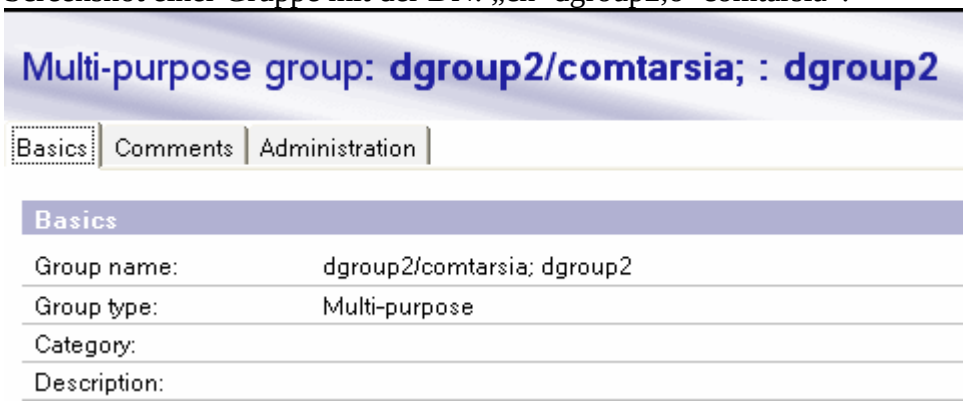
Damit die Domino Objekte im LDAP hierarchisch gegliedert sind, muss die Domain mit Fullname-Attribut angegeben werden.

Bei Benutzer und Gruppen-Objekten muss im Fullname-Attribut sowohl der hierarchische Name als auch der flache Name angegeben werden.
WICHTIG: Der hierarchische Name muss an erster Stelle im Fullname-Attribut stehen.

Screenshot eines Benutzers mit der DN: „cn=Dom User2,o=comtarsia“:

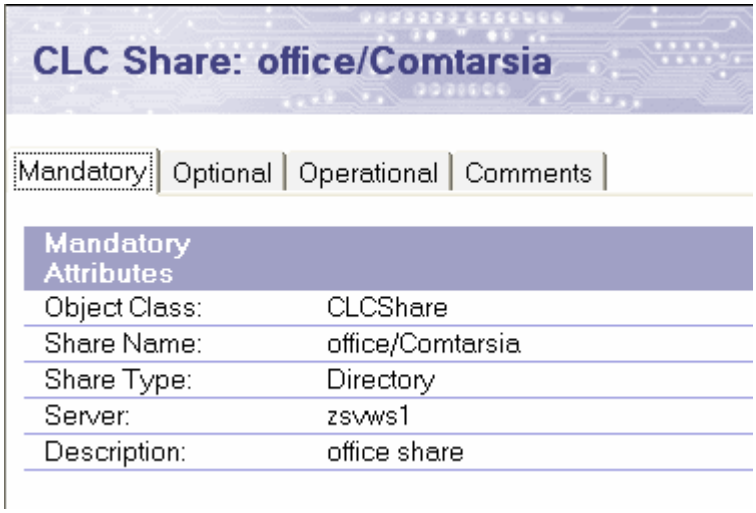


Screenshot einer Gruppe mit der DN: „cn=dgroup2,o=comtarsia“:

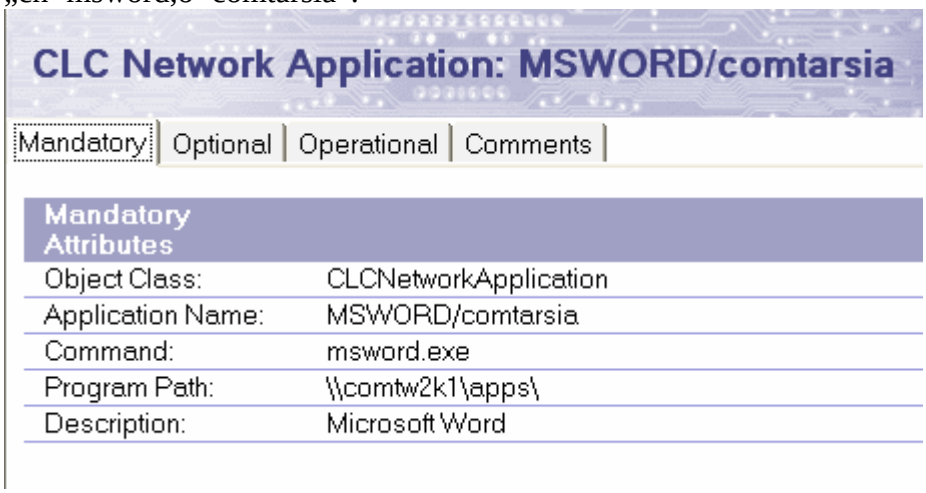


Bei Share bzw. Netzwerkapplikationsobjekten ist es ausreichend, nur den hierarchischen Namen im Fullname-Attribut einzutragen.

Screenshot eines CLCShare-Objektes mit der DN: „cn=office,o=comtarsia“:



Screenshot eines CLCNetworkApplication-Objektes mit der DN: „cn=msword,o=comtarsia“:



7.4.5 Konfiguration des Logon Client für den Domino LDAP Server

Eine Anmeldung des Logon Client an den Domino LDAP Server kann sowohl über den ShortName als auch über den/einen FullName erfolgen.

Eine LDAP BaseDN kann nur dann verwendet werden, wenn sowohl die Benutzer als auch die Gruppen hierarchisch angelegt sind. In diesem Fall muss auch im FullName Feld des Benutzers der Name mit voller Hierarchie enthalten sein z.B.:
Test User/Comtarsia
Test User

Für eine Anmeldung mit dem Domino ShortName gibt es zwei Möglichkeiten:
UserDN: uid=SHORTNAME oder
UserDN: SHORTNAME
Weitere Informationen zur Konfiguration von Lotus Domino zur Unterstützung des ShortName-Logons finden sich in der Reference-List am Ende dieses Handbuches.

Das zu verwendende Passwort ist im “Internet-Password” Feld im Personendokument festgelegt.

Logon Client Konfiguration:

- Option AppendBaseDN ist deaktiviert
- Das Feld UserDNPrefix ist bei ShortName-Anmeldung auf “uid=” oder “” gesetzt, bei FullName-Anmeldung auf „cn=“
- LDAP Server-Typ ist “Domino”
- LDAPEnableSSL ist entsprechend der Domino Konfiguration gesetzt

Jetzt kann sich der Comtarsia Logon Client an den Domino LDAP Server authentifizieren.

7.5 Konfiguration eines OpenLDAP-Servers unter SuSE 8.0 Prof.

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 #
```

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.

7.6 Cookbook - SSL Zertifikat Installation

7.6.1 Einleitung

Der Comtarsia Logon Client unterstützt ab Release 3.0 auch LDAP. Um die Vertraulichkeit der übertragenen Daten (Benutzerpasswörter, Benuterberechtigungsdaten, usw.) zwischen Logon Client und LDAP Server zu gewährleisten, ist es möglich SSL Verschlüsselung einzusetzen.
SSL (Secure Socket Layer) wurde ursprünglich von Netscape entwickelt. Inzwischen unterstützen viele namhafte Softwarehersteller diese Protokoll für Datenverschlüsselung und für elektronische Unterschriften.

SSL beruht auf asymmetrische Verschlüsselung (Private Key / Public Key) und der Verwendung von X.509 Zertifikaten am Server bzw am Client.
Dabei sind folgende Kombinationen möglich:

a) Am Server wird ein so genanntes Self Signed Certificate verwendet, der Client verwendet kein Zertifikat.
b) Der Server verfügt über ein CA (Certificate Authority) Signed Certificate, dann ist am Client zumindest das CA Zertifikat erforderlich um die Echtheit des Server Zertifikates zu überprüfen. (Server Authentication)
c) Der Server verfügt über ein CA Signed Certificate, der Client verwendet ein Self Signed Certificate und benötigt zusätzlich das CA Zertifikat (zu Prüfung des Server Zertifikates).
d) Sowohl Client als auch Server verfügen über CA Signed Certificates, dann muss dem Client ebenfalls das CA Zertifikat zur Verfügung gestellt werden, damit es dem Server möglich ist, die Echtheit des Client Zertifikates zu überprüfen. (man spricht von Client Authentication).

7.6.2 Herstellerstandards für X.509 Zertifikate

Folgende Hersteller verwenden eigene Normen und Formate zum Erzeugen und Speichern von Zertifikaten und PKI- (Public Key Infrastructure) Keys.

RSA (Rhivest, Shamir, Adelman): unterstützt PKCS#n Standards. Entwickelten das nach ihnen benannte asymmetrische RSA Verschlüsselungs Verfahren.

Netscape: Unterstützt PKCS#11- Cryptographic Token Interface Standard, PKCS#7 zum Speichern von Zertifikaten und für Certifikate Revokation List, PKCS#12 zum Austausch von Zertifikaten und PKI Keys, keyX.db und certX.db als permenter Speicher für Zertifikate und PKI Keys im Dateisystem (Key- bzw Certifikate Store). Zur asymmetrischen Verschlüsselung wird das RSA Verfahren unterstützt.
Verfügbare Tools: certutil, signtool, …

OpenSSL: Unterstützt folgende Formate: PKCS#7, PKCS#12, X509.
Als asymmetrische Verfahren werden sowohl RSA als auch Diffie-Hellman (DH) verwendet. Zum Signieren wird DSA (Digital Signature Algorithm) unterstützt. Als encoding type für Zertifikate stehen bei OpenSSL das DER Format, das PEM Format (base64 encoded version of DER) und das NET Format zur Verfügung.
Verfügbare Tools: openssl x509, openssl pkcs7, openssl crl2pkcs7, openssl pkcs12, openssl genrsa, …

Sun Java Secure Socket Extensions (JSSE): unterstützt PKCS#7 (PEM encoded) für den Import von signierten Zertifikaten in der Java Key Store. Verfügbare Tools: keytools, java signer-ein Programm zum signieren von Java Archiven (.jar),…

Microsoft Cryptographic Service Provider: Unterstützt kein PKCS#11! Verwendet ein eigenes Verfahren zum Zugriff auf Key- und Certifikate Store. Das Erstellen von Client Zertifikaten erfolgt über Microsoft Certificate Services. Ein Certificate Request muss über eine bestimmte Web Page am Internet Information Server (IIS) der Zertifizierungsstelle gemacht werden. Diese Page stößt auch die Generierung des Private/Public Key Paares im Key Store an. Der signierte CSR kann als PKCS#7 eingespielt werden. Microsoft unterstützt auch das PKCS#12 Format zum Import/Export von Client und Server Zertifikaten samt Keys in bzw aus dem Microsoft Key Store.
Als PKI Verschlüsselungsverfahren werden sowohl RSA als auch Diffie-Hellman unterstützt. Verwendeter encoding type des MS-CSP ist das DER Format für PKCS#7.
Microsoft verwaltet einen Certificate Store mit dem Namen „MY“ pro Benutzer im Benutzerprofil. Zusätzlich gibt es systemweite Certificate Stores für den jeweiligen Arbeitsrechner (und für Services). Zertifikate und Keys werden sowohl als Dateien im Dateisystem als auch in der Registry abgelegt.
Verfügbare Tools: certutil, certificate snap in für Management Console (mmc), certificate management im IE, MS Certificate Services (bei Windows 2000 Server).

(Die obige Liste stellt keine Anspruch auf Vollständigkeit.)

7.6.3 SSL und Comtarsia Logon Client

Um möglichst hohe Konformität und Kompartibilität mit dem Zielbetriebsystem des Comtarsia Logon Clients zu erreichen (Windows), um etwaige Synergieeffekte (Wiederverwendung zur Verfügung gestellter Client Zertifikate von anderen Applikationen) und der Möglichkeit der Verwendung von Smart-Cards ausnützen zu können wurde entschieden, für den Comtarsia Logon Client den Microsoft Cryptographic Service Provider zu verwenden.
Um jedoch eine zu starke Herstellerabhängigkeit zu verhinden, ist geplant eine automatische Funktion zum Import, Export und Austausch von gebräuchlichen Zertifikat- bzw. Key -Formaten im Logon Client zu implementieren.
Angestrebt wird hier die Verwendung der Formate PKCS#7 bzw PKCS#12 die wie oben erwähnt sowohl von RSA, Netscape, OpenSSL, Sun JSSE als auch Microsoft unterstützt werden.

Es ist angedacht ein weiteres Zusatzprodukt (mit graphischer Oberfläche) zu entwickeln, welches es ermöglicht direkt auf Key und Zertifikat Stores andere Hersteller zuzugreifen (etwa Netscape’s certX.db und keyX.db) um Zertifikate bzw Keys mit dem Microsoft Certificate Store austauschen zu können, und damit z.B. die Vorbereitung von automatischer Softwareverteilung zu erleichtern.

7.6.4 Technische Realisierung

In obiger Dokumentation wird nur von der Verwendung asymmetrischer Keys gesprochen.
Aus Gründen der Einfachheit der Darstellung wurde verschwiegen, dass asymmetrische Verschlüsselung nur dem Austausch von symmetrischen

Schlüsseln dient (man spricht von s.g. „Session Keys“), mit denen die übertragenen Daten nun tatsächlich verschlüsselt werden.
Grund für die Verwendung der symmetrischen Schlüssel ist der geringere Ver- bzw. Entschlüsselungsaufwand (erforderliche Rechenleistung).
Wie oben erähnt wird im Logon Client der Microsoft SSL Stack verwendet.
Das Architekturmodell von Microsoft implementiert diese Funktionalität mit der s.g. CryptAPI, die ähnlich PKCS#11 aus einer abstrakten Definition von Schnittstellen und Funktionsaufrufen besteht. Die Funktionsaufrufe der CryptAPI werden an einen „Cryptographic Service Provider (CSP)“ weitergeleitet, der die Ver- und Entschlüsselung der Daten (bzw. alle SSL relevanten Funktionen) übernimmt. Er wird als eigenes Modul bereitgestellt.
Standardmässig hat Windows 2000 den „Microsoft Base Cryptographic Provider” mitinstalliert. Dieser unterstützt jedoch nur symmetrische Schlüssellängen von 40 bzw. 56 Bit (DES), da die amerikanischen Exportbestimmungen einen Verkauf von US Produkten, die stärkere Verschlüsselung unterstützen, außerhalb der USA bis dato untersagten.
Diese Bestimmung ist nun nicht mehr gültig, es ist daher zu empfehlen, mittels Windows Update den „Microsoft Enhaunced Cryptographic Provider“ bzw. den „Microsoft Strong Cryptographic Provider“, die beide 128 Bit asymmetrische Schlüssellänge ermöglichen, einzuspielen [1].
Der Logon Client unterstützt alle drei Provider und wählt im Fall des Vorhandenseins mehrer CSPs jenen aus, der die größte Datensicherheit gewährleistet.

Bevor nun SSL Verschlüsselung verwendet werden kann sind folgende Voraussetzungen zu erfüllen:
Am jeweiligen LDAP Server muss SSL aktiviert sein und ein Server Zertifikat vorhanden sein, entweder ein Self Signed Certificate oder aber auch ein CA Signed Certificate
(siehe Einleitung Punkt a) bzw. b)).
Zusätzlich kann am Client auch entweder ein Self Signed- oder ein CA Signed Certificate eingespielt werden
(Einleitung Punkte c) und d)).
Die Zertifikate und die zugehörigen Private Keys (nur für Client bzw. Server Zertifikat, nicht aber beim CA Zertifikat) müssen in den s.g. Certificate Store am Client bzw. Server eingespielt werden. Dies kann am Client mit dem mitgelieferten Programm import_key.exe bewerkstelligt werden, dessen Verwendung weiter unten erläutert wird. Am Server erfolgt dass Einspielen gemäß Herstellerangaben (exemplarisches HowTo für OpenLDAP befindet sich bei der mitgelieferten Dokumentation).
Eine Beschreibung wie eine Certificate Authority überhaupt erst hergestellt werden kann, folgt nun.

7.6.5 Erstellen einer Testumgebung

Als Software zur Erstellung der Test Certificate Authority wurde Openssl gewählt, weil diese geschützt durch die GNU Public Licence im Internet frei verfügbar ist, als Standardsoftware angesehen werden kann, dadurch jede Menge Doku im Internet vorhanden ist und Openssl sowohl unter Unix (Linux) wie auch unter Windows (durch Verwendung von cygwin, siehe www.redhat.com/cygwin) lauffähig ist.

[1] Die hier erwähnten Provider sind RSA Full Provider, die der Ldap Logon Client verwendet.

Nach der Installation von Openssl z.B.: unter /usr existiert ein Unterverzeichnis /usr/ssl das die Konfigurationsdatei openssl.cnf beinhält.

Eine gute Dokumentation für Openssl Version 0.9.2b findet man unter http://www.dfn-pca.de/certify/ssl/handbuch/ossl092/ossl092.html.

7.6.5.1 Erzeugen ein Root Certificate Authority:

```
openssl req -out ca.pem -new -x509
```
-erzeugt CA file "ca.pem" und CA key "privkey.pem"
```
openssl crl2pkcs7 -nocrl -certfile ca.pem -out ca.p7b -inform PEM -
outform DER
```

7.6.5.2 Erzeugen eines Server Zertifikates/Key Paares:

```
openssl genrsa -out server.key 1024
openssl req -key server.key -new -out server.req
openssl x509 -req -in server.req -CA CA.pem -CAkey privkey.pem -
CAserial file.srl -out server.pem
```
-Inhalt der Datei "file.srl" ist eine Zweistellige Nummer z.B.: "00"

7.6.5.3 Erzeugen eines Client Zertifikates/Key Paares:

```
openssl genrsa -out client.key 1024
openssl req -key client.key -new -out client.req
openssl x509 -req -in client.req -CA CA.pem -CAkey privkey.pem -
CAserial file.srl -out client.pem
```
-Inhalt der Datei "file.srl" ist eine Zweistellige Nummer z.B.:"00"

7.6.5.4 Konvertieren eines Zertifikates in PKCS#12 Format

```
openssl pkcs12 -export -in client.pem -inkey client.key -keyex -
CAfile ca.pem -name "client" -out client.pfx
```

7.6.5.5 Überprüfen eines Zertifikates

openssl.exe x509 -text -noout -sha1 -fingerprint -in clien.pem

7.6.5.6 Import eines Zertifikates

Das erzeugte Client Zertifikat, der zugehörige Private Key und das CA Zertifikat (falls vorhanden) kann mit import_key folgendermassen in den Key Store des Clients importiert werden.

```
USAGE: import_key -s<format_option> [-v] [<options>]
    -s<format_option>                    Switch between PKCS7 and PKCS12
format
    -v                                   Use verbose mode

  PKCS7 format options (-sPKCS7):
    -f<pkcs#7_file>                      PKCS#7 certificate file
    -k<keyfile>                          PEM format private key (not
encrypted)
    -C                                   Certificate only.
    -A                                   Add certificate to the CA store

  PKCS12 format options (-sPKCS12):
    -f<pkcs#12_file>                     PKCS#12 certificate and key file.
    -p<pkcs#12_password>                 PKCS#12 password.

  examples:
    to import a pkcs#12 certificate and key into the user store:
      import_key -sPKCS12 -v -fclient.pfx -psecret

    to import a pkcs#7 certificate and a PEM encoded key into the user
store:
      import_key -sPKCS7 -v -fclient.p7b -kclient.key
    to import a pkcs#7 certificate without a key into the user store
      import_key -sPKCS7 -v -C -fserver.p7b
    to import a pkcs#7 certificate without a key into the system store (CA)
      import_key -sPKCS7 -v -A -fca.pem
```

Unterstützte Formate:

Bei Import eines Client Zertifikates werden die Formate PKCS#12 für Zertifikat und Key bzw. PKCS#7 für Zertifikat und PEM nur für Key (ohne Passwort Verschlüsselung) unterstützt.

z.B.: `import_key –sPKCS12 –fMyClientCert.pfx –pSECRET`
`import_key –sPKCS7 –fMyClientCert.p7b -kMyPrivateKey.pem`

Der Import eines Certificate Authority Zertifikates muß mittel PKCS#7 erfolgen.
z.B.: `import_key –sPKCS7 –fMyCACert.p7b –A`

7.6.5.7 Unterstützte Sicherheitsmodi im Logon Client

Der Logon Client unterscheidet folgende Sicherheitseinstellungen:

0: Keine SSL Verschlüsselung

1: Self Signed Server Zertifikat wird akzeptiert, kein Client Zertifikat vorhanden.

2: CA Signed Server Zertifikat erforderlich, kein Client Zertifikat vorhanden.

3: CA Signed Server Zertifikat erforderlich, Self Signed- oder CA Signed Client Zertifikat vorhanden.

Beim Auffinden der Zertifikate im Certifikate Store verwendet der Logon Client folgenden Algorithmus:

Das Client Zertifikat wird im „My-“ User Certificate Store des jeweiligen Benutzers gesucht. Zuerst wird versucht ein Zertifikat zu finden dessen ‚Subject Name’ mit dem Benutzernamen des aktuell angemeldeten Benutzers zu finden.
Misslingt der Versuch, wird das erste Zertifikat genommen, dass sich im User Certificate Store befindet.

Das CA Zertifikat (falls verwendet) muß sich entweder im „Root-“ User Certificate Store (nur für den aktuellen Benutzer zugänglich) oder im „Root-“ System Certificate Store (für alle Benutzer dieser Maschine zugänglich) befinden. CA Zertifikate die mit import_key.exe mit aktivierter Option –A importiert werden, werden immer im „Root-“ System Certificate Store abgelegt.

8. REFERENCE LISTS

8.1 Domino Directory Server Reference List

[1] Domino Short-Names:
http://www-12.lotus.com/ldd/doc/domino_notes/Rnext/help6_admin.nsf/f4b82fbb75e942a6852566ac0037f284/b6ebd85402ab04ea85256c1d0039955c?OpenDocument

http://www-12.lotus.com/ldd/doc/domino_notes/Rnext/help6_admin.nsf/f4b82fbb75e942a6852566ac0037f284/c2b8e9676cb9d73c85256c1d00393778?OpenDocument

[2] Default Domain Document:
http://www-12.lotus.com/ldd/doc/domino_notes/Rnext/help6_admin.nsf/f4b82fbb75e942a6852566ac0037f284/62b8e37b261352b685256c1d003954b8?OpenDocument#413064780829246853

[3] Setting up SSL on a Domino server:
http://www-12.lotus.com/ldd/doc/domino_notes/Rnext/help6_admin.nsf/f4b82fbb75e942a6852566ac0037f284/0efb035694124113852 56c1d00398e86?OpenDocument

[4] Setting up Notes and Internet clients for SSL authentication:
http://www-12.lotus.com/ldd/doc/domino_notes/Rnext/help6_admin.nsf/f4b82fbb75e942a6852566ac0037f284/438e83bd82998bfe85256c1d00399165?OpenDocument

[5] Customizing the LDAP service configuration:
http://www-12.lotus.com/ldd/doc/domino_notes/Rnext/help6_admin.nsf/f4b82fbb75e942a6852566ac0037f284/055defea478ecc6585256c1d003937eb?OpenDocument

[6] Domino Directory Services:
http://www-12.lotus.com/ldd/doc/domino_notes/Rnext/help6_admin.nsf/b3266a3c17f9bb7085256b870069c0a9/a7be0edb2008082385256c1d0039335a?OpenDocument

8.2 IBM Directory Server 5.1 Reference List

[1] Product documentation home:
http://www-3.ibm.com/software/network/directory/library/index.html#v51

[2] Installation:
ftp://ftp.software.ibm.com/software/network/directory/library/v51/ldapinst.htm#HDRLINCLI

[3] Password Policy
ftp://ftp.software.ibm.com/software/network/directory/library/v51/admin_gd.htm#Header_116

[4] SSL configuration
ftp://ftp.software.ibm.com/software/network/directory/library/v51/admin_gd.htm#Header_84

[5] Adding an entry
ftp://ftp.software.ibm.com/software/network/directory/library/v51/admin_gd.htm#Header_260

[6] LDAP Password Policy RFC
http://www.ietf.org/internet-drafts/draft-behera-ldap-password-policy-06.txt

8.3 Open LDAP

http://www.OpenLDAP.org/

9. Glossary

OID **(Object identifiers) Objektbezeichner,** eine hierarchisch aufgebaute Sequenz von Integerzahlen, die für zahlreiche Protokolle verwendet werden. Sämtliche LDAP-Objekte besitzen eine eindeutige OID. Die Definition basiert auf dem [ITU-T X.208] Standard.

RACF **Resource Access Control Facility** - ist ein IBM Sicherheits-Management Produkt für die Mainframe Betriebssysteme OS/390 (MVS) und VM.

RFC **Request for Comments** – sind durchnummerierte Serien von formalen Internet Dokumenten (oder teilw. Standards), die aus Erarbeitung und kontinuierlicher Überprüfung von interessierten Beteiligten und Fachausschüssen resultiert. Manche RFCs sind rein informativ. Bei denjenigen Dokumenten, welche Internet Standard werden, werden keine weitere Kommentare und/oder Änderungen zugelassen. Änderungen können eingeführt werden, in einem solchen Fall lösen Folge-RFCs die früheren teilweise oder ganz ab.
Die Universität von Southern California betreut ein komplettes Register aller von der Internet Engineering Task Force (IETF) herausgegebenen RFCs.

LDAP **Lightweight Directory Access Protocol** wurde als offener Standard für globale oder lokale Verzeichnisdienste im Netzwerk und/oder im Internet entwickelt. Das Wort Protokoll ist der Schlüssel der Definition, da LDAP weder Software noch Hardware ist. LDAP ist ein Protokoll, welches definiert, wie Client und Server miteinander kommunizieren.
LDAP ist in einer Serie von Requests For Comments (bekannt als RFC-s, siehe oben) beschrieben. Eine sehr verlässliche Quelle von LDAP RFCs ist unter

OpenLDAP, http://www.OpenLDAP.org/ zu finden, wo sie frei zum Download erhältlich sind.
Die wichtigsten RFCs im Bereich LDAP sind RFC 1777 für LDAPv2 and RFC 2251 für LDAPv3.

SSL **Secure Sockets Layer**, ist die Standard-Sicherheitstechnologie um verschlüsselte Verbindungen zwischen Client und Server zu erstellen. Diese Verbindung stellt sicher, dass der gesamte Datenfluss geschützt und unangetastet bleibt. SSL ist ein Industriestandard. Um ein SSL Verbindung herzustellen, benötigt der Server ein SSL-Zertifikat.

TLS **Transport Layer Security Protocol**. Das TLS Protokoll stellt einen Datenschutz für die Kommunikation über das Internet zur Verfügung. Dieses Protokoll ermöglicht Client/Server Applikationen auf solche Art und Weise die Daten zu übertragen, dass die Daten vor unbefugten Abhören, Eingriffen und Verfälschungen geschützt bleiben. Das Protokoll besteht aus zwei Schichten: „TLS Record Protocol“ und „TLS Handshake Protocol“.

CLC **Abkürzung von Comtarsia Logon Client** – es wird meistens in Verbindung mit CLC Configurator, oder mit Comtarsia Logon Client2006 spezifischen Objektklassen, z.B. “CLCPerson” verwendet.