

LDAP – Suche nach Mailadressen

LDAP - Was ist das?

LDAP (Lightweight Directory Access Protocol) ist ein standardisierter Directory Service (Verzeichnisdienst) auf der Basis von TCP/IP, der die hierarchische Verwaltung von Modellen verschiedenster Klassen in einer Datenbank und die Suche nach diesen gestattet. Die unterschiedlichen Klassen (z. B. Personen, Dokumente, Rechnernamen) erlauben eine unterschiedliche Zuordnung von Attributen zu jeder Klasse im Directory. Die Abfrage von Objekten aus der Datenbank erfolgt über ein Protokoll oder entsprechende Gateways, die dieses Protokoll beherrschen. Soweit die Theorie. Die Funktion von LDAP wird im nächsten Abschnitt erklärt.

Anwendung

An der HU wird mit LDAP ein Interface bereitgestellt, mit dem die Suche nach Personen, Mailadressen und Telefonnummern realisiert werden kann. LDAP bietet im Prinzip die gleiche Funktionalität wie der in Banyan VINES bekannte Street Talk-Dienst und soll der primäre Verzeichnisdienst für die HU werden. Im Prinzip stellt der LDAP-Server also ein „Telefonbuch“ für Mailadressen dar.

Einige Mailtools (und es werden immer mehr) haben LDAP-Funktionalität implementiert und bieten die Möglichkeit, vor dem Schreiben einer Mail über einen LDAP-Server die Mailadresse des Empfängers zu ermitteln. Als Suchbegriff wird beispielsweise der Name des Empfängers eingegeben, als Resultat erscheinen die E-Mail-Adresse und weitere Angaben.

Weiterhin bietet ein WWW-Interface (Web500-Gateway von Frank Richter - TU Chemnitz) Zugang zu den Daten des LDAP-Servers. Darüber ist auch die Struktur des Directories einsehbar, also welche Organisationseinheiten existieren und welche Mitarbeiter diesen zugeordnet sind. Für den internen Gebrauch ist das Interface unter <http://ldap.hu-berlin.de:7777/> zu erreichen. Zugriffe zu diesem Gateway von Rechnern außerhalb der HU-Domain können über die Adresse <http://ldap.hu-berlin.de:8888/> erfolgen. Der auf diesem Port laufende Daemon hat eine etwas eingeschränkte Funktionalität.

Über das Web500-Gateway kann auch der Directory-Service der TU Chemnitz abgefragt werden. Über den Punkt **Move upwards** (Steige auf) ist eine weltweite Suche im Directory möglich.

Des Weiteren wurde ein Gateway bereitgestellt, das Clients mit Ph-Interface (z. B. Eudora Light) Anfragen an LDAP gestattet.

Organisatorisches

Die in LDAP bereitgestellten Daten werden direkt aus der zentralen Adressdatenbank der Universität erzeugt. Die Pflege der Daten (Änderungen, Ergänzungen etc.) in der zentralen Adressdatenbank erfolgt dezentral in den Instituten und Einrichtungen der Universität durch die zuständigen VerwaltungsleiterInnen.

Die Daten werden einmal pro Nacht aus der Datenbank gezogen und für den LDAP aufbereitet. Somit ist sichergestellt, dass die Daten im LDAP aktuell sind.

Studierende der Humboldt-Universität haben über ein WWW-Formular die Möglichkeit, ihre Mailadresse und ihre Homepage in den LDAP-Server einzutragen. Zu erreichen ist dieses Formular unter der URL <http://www.hu-berlin.de/ldap/>. Voraussetzung für das Eintragen ist allerdings ein Studierenden-Account am Rechenzentrum.

Konfiguration

In Programmen, die direkt den LDAP-Server kontaktieren, ist es notwendig, eine so genannte Search-Base (auch: Server-Root, Stammverzeichnis, Suchbasis) anzugeben. Ohne diese geht gar nichts.

Für die HU lautet die Search-Base:

```
o=Humboldt-Universitaet zu Berlin,c=de
```

Der Name des LDAP-Server lautet:

```
ldap.hu-berlin.de
```

Der Port des LDAP-Server:

```
389
```

Konfigurationsbeispiele für einige Mail-Programme:

Eudora Light 3.0x

Eudora Light verfügt nicht über eine LDAP-Implementation. Es unterstützt lediglich Anfragen an Ph-Server. Ph ist ebenfalls ein Verzeichnisdienst. Durch die Installation eines Gateways sind aber auch Anfragen von Ph-Clients an den LDAP-Server möglich. Unter **Tools – Option – Hosts** ist in der Zeile **Ph ldap.hu-berlin.de** einzutragen. Über **Tools – Directory Services** (Ctrl-Y) können Anfragen an den Verzeichnisdienst gestellt werden.

Die Suche nach Mailadressen kann auch mit dem Adressbuch von Netscape durchgeführt werden. Wenn Eudora als Default-Mailtool registriert ist, genügt ein Klick auf den Link der Mailadresse des potentiellen Empfängers im Netscape-Adressbuch, um Eudora zu starten und die ausgewählte Mailadresse in der To-Zeile in Eudora erscheinen zu lassen.

Eudora Pro 4.0.1

- **Tools – Directory Services – Protocols – LDAP** auswählen;
- **New Database** anklicken;
- **Name:** HU-LDAP
- **Hostname:** ldap.hu-berlin.de
- **Port:** 389
- die Option *This server requires me to logon* nicht aktivieren;
- Die Karte **Search Options** anwählen;
- **Search Timeout** auf etwa eine Minute einstellen
- **Search Base:** o=Humboldt-Universitaet zu Berlin, c=de

Abschließend die Konfiguration beenden und unter *Databases* die Verwendung von HU-LDAP aktivieren.

Netscape Navigator 4.05

- **Edit – Preferences** öffnen;
- **Mail & Groups – Directory** anklicken;
- **Description:** HU-LDAP
- **LDAP-Server:** ldap.hu-berlin.de
- **Search-Root:** o=Humboldt-Universitaet zu Berlin, c=de
- **Port Number:** 389
- **Maximum Nunner of Hits:** 150
- **Secure** nicht aktivieren;
- **OK**
- Mittels der Pfeil-Buttons HU-LDAP an den Anfang der Liste setzen;
- **OK**
- unter **Edit – Search Directory** können Anfragen an den LDAP-Server gestellt werden;

Netscape Navigator 4.5

Automatische Konfiguration:

In den meisten Fällen kann die LDAP-Konfiguration automatisch erfolgen. Dazu muss einfach die URL `ldap://ldap.hu-berlin.de/o=Humboldt-Universitaet zu Berlin, c=de` im Browser aufgerufen werden. Normalerweise zeigt Netscape dann eine Seite mit Attributen

an und fragt, ob die Einstellungen zu den lokalen LDAP-Einstellungen hinzugefügt werden sollen. Dies ist zu bestätigen. Anschließend mittels **BACK-** oder **ZURÜCK-Button** zur vorhergehenden Seite zurückkehren. Die Benutzung des Dienstes erfolgt über das Adressbuch.

Manuelle Konfiguration:

- **Communicator – Address Book** anklicken, das Adressbuch wird geöffnet;
- Im Adressbuch **File – New Directory** auswählen;
- **Description** HU-LDAP oder einen anderen Namen eintragen;
- **LDAP Server:** ldap.hu-berlin.de angeben;
- Bei **Search Root:** o=Humboldt-Universitaet zu Berlin, c=de eingeben;
- **Port Number:** 389
- **Secure** und **Login with Name and Password** nicht aktivieren;
- Mit **OK** die Konfiguration beenden.

Hinweise:

Unter **Edit – Preferences – Mail & Newsgroups – Addressing** kann dann die primäre Verwendung des zuvor konfigurierten LDAP-Servers eingestellt werden. Die Einstellungen im Communicator für LDAP können individuell angepasst werden. Eine detaillierte Beschreibung befindet sich unter `http://developer.netscape.com/docs/manuals/communicator/ldap45.htm`. In der Abbildung 1 finden Sie ein Beispiel, wie die Suche mit dem Adressbuch individuell angepasst werden kann.

Outlook Express 5

- **Tools – Accounts** anklicken und die Karte **Directory Service** auswählen;
- den Button **Add** anklicken und **Directory Service** selektieren;
- im danach erscheinenden Fenster unter *Internet directory (LDAP) Server* ldap.hu-berlin.de eintragen;

Ausgehend von der obigen Konfigurationsanleitung hier nun ein Beispiel, damit die Attribute **ou** (Einrichtung), **Group** und **Description** angezeigt und bei der erweiterten Suche verwendet werden können. Zuerst Netscape beenden. Dann im File `~/netscape/preferences.js` (UNIX), bzw. `\Programme\Netscape\Users\Default\prefs.js` (Windows) hinter der Zeile

```
user_pref("ldap_2.servers.HULDAP.serverName", "ldap.hu-berlin.de");
```

für den LDAP-Server die folgenden vier Zeilen einfügen:

```
user_pref("ldap_2.servers.HULDAP.attributes.custom1", "Description:description");
user_pref("ldap_2.servers.HULDAP.attributes.nickname", "Description:description");
user_pref("ldap_2.servers.HULDAP.attributes.o", "Department:ou");
user_pref("ldap_2.servers.HULDAP.attributes.l", "Section:group");
```

Für die Strings **Description**, **Department** und **Section** können auch andere Bezeichnungen gewählt werden, z. B. **Sachgebiet/Funktion**, **Institut/Fachbereich** und **Abteilung**. Anschließend Netscape neu starten und das Adressbuch öffnen. Das Resultat der Änderung sollte nun dort zu sehen sein.

Abb. 1: Konfigurationsbeispiel für Netscape Communicator 4.5

- *My LDAP server requires me to log on* nicht aktivieren;
- **Next**
- die Einstellung, ob Adressen mittels Directory Service überprüft werden sollen, ist optional;
- **Next – Finish**
- In der Karte **Directory Service** erscheint nun der zuvor kreierte Eintrag – **Properties** anklicken und die Karte **Advanced** wählen – unter *Search Base* `o=Humboldt-Universitaet zu Berlin,c=de` eintragen;
- **OK – Close**
- Einträge im LDAP können nun unter **Tools – Address Book – Edit – Find People** gesucht werden. Unter **Look In** den anfangs angelegten Directory Server (`ldap.hu-berlin.de`) einstellen.

Outlook Express 5 kommt offenbar mit umfangreichen Antworten vom Server nicht zurecht und bringt einen Fehler. In diesem Fall sollte die Anfrage präzisiert werden, z. B. durch Hinzufügen des Anfangsbuchstaben des Vornamens (Bsp.: *H Mustermann* statt *Mustermann*).

Outlook 98

- **Extras – Konten – Hinzufügen – Verzeichnisdienst** anklicken;
- *Internetverzeichnisserver*: `ldap.hu-berlin.de`
- *LDAP-Server erfordert Anmeldung* nicht aktivieren;
- Das Aktivieren des Punktes **Überprüfen der Adressen mit Verzeichnisdienst durchführen** ist optional.
- **Name des Internetverzeichnisdienstes**: LDAP HU
- **Fertigstellen**
- Unter **Extras – Konten – Verzeichnisdienst – LDAP HU – Eigenschaften – Erweitert** als Suchbasis `o=Humboldt-Universitaet zu Berlin,c=de` eintragen;
- Personen und Mailadressen können dann über **Extras – Adressbuch – Suchen** ermittelt werden.

Datenschutz

Der Behördliche Datenschutzbeauftragte der Humboldt-Universität wurde über das Verfahren informiert und hat es genehmigt (28.05.99).

Die via LDAP bereitgestellten Daten sind weltweit abrufbar. Die Grundlage der Daten im LDAP ist die zentrale Adressdatenbank. Am RZ werden an den Daten keine inhaltlichen Veränderungen vorgenommen. Durch das RZ erfolgt lediglich die Aufbereitung der Daten und die Bereitstellung des Dienstes. Die inhaltliche Verantwortung für die Richtigkeit der Daten liegt in den Einrichtungen der Universität.

Um ein vollständiges Abziehen der Daten zu verhindern, ist die Anzahl der Sätze, die pro Anfrage ausgegeben werden, auf 150 begrenzt. Außerdem ist der Zugriff auf die Daten über WEB-Gateway von außer-

halb nur mit eingeschränktem Funktionsumfang möglich (keine Vcards, keine Adresslisten, eingeschränkte Suche).

Das `ph2ldap`-Gateway kann nur aus dem Netz der HU abgefragt werden.

Bei Studierenden besteht beim Eintragen in die Datenbank die Möglichkeit, die Abfrage einzuschränken, so dass Informationen nur ausgegeben werden, wenn die Anfrage aus dem Netz der HU (Campus HU, Charité) kommt.

Von MitarbeiterInnen können HU-intern (Campus HU und Charité) alle Datensätze aus dem LDAP abgefragt werden, auch wenn keine Zustimmungserklärung vorliegt. Lediglich bei Abfragen, die von außerhalb der HU-Domain an den LDAP gestellt werden, werden Einträge, bei denen die Zustimmung nicht vorliegt, ausgeblendet (gefiltert). Auch dieses nun veränderte Verfahren wurde vom Datenschutzbeauftragten genehmigt.

Hinweise, Details und Probleme

Der LDAP-Server kann auch unter der bisherigen Search-Base `o=HU Berlin` erreicht werden.

Wenn Sie LDAP zum ersten Mal benutzen, überprüfen Sie zuerst die Angaben zu Ihrer eigenen Person.

In der Datenbank erfasste reine VINES-Mailadressen (*Name@Gruppe@Org*) werden nicht angezeigt. Die Ausgabe fehlerhafter Mailadressen (Adressen mit Umlauten, Leerzeichen etc.) wird unterdrückt.

Der am RZ installierte LDAP beruht auf einem freien Server von `Openldap`, der auf Linux rennt (AMD-K6 - 350 MHz). Der zuvor eingesetzte Directory-Server von Netscape konnte aus lizenzrechtlichen Gründen nicht betrieben werden.

Diverse Probleme bei der Darstellung von Umlauten sind derzeit leider nicht vermeidbar. Dies liegt an den von den Clients verwendeten Zeichensätzen, da sowohl ISO-Latin1 als auch UTF-8 verwendet werden. Von daher ist es notwendig, bei einem Attributwert mit Umlauten jeweils zwei Zeilen zu speichern, für jeden Zeichensatz eine. Außerdem wird eine weitere Zeile mit Umschreibung der Umlaute gespeichert.

Die Aktualisierung der LDAP-Daten erfolgt jeden Morgen gegen 05:30 Uhr. In dieser Zeit steht der LDAP-Server für etwa 3 Minuten nicht zu Verfügung.

Die im WEB500-Gateway dargestellten Namen der Organisationseinheiten (OE) entstammen dem OKZ-Verzeichnis (Organisationkennziffern) der Universität. Im LDAP werden lediglich die Namen zu den OKZ verwendet, nicht jedoch die OKZ selbst. Eine vollständige Abbildung der OKZ-Struktur war nie Ziel dieses LDAP-Servers oder des Web500-Gateways.

Jens-Uwe Winks
winks@rz.hu-berlin.de