Konzepte von Betriebssystem-Komponenten Schwerpunkt Sicherheit

Unix-Benutzerverwaltung:

Grundlagen, OpenLDAP

Daniel Bast

daniel.bast@gmx.net

Überblick

- Klassische Benutzerverwaltung
- OpenLDAP
  - Verzeichnisdienste
  - LDAP im Detail
  - Zugangskontrolle
  - Anwendung
  - Beurteilung

Klassische Benutzerverwaltung

Aufbau der Datei: `/etc/passwd`

- Besteht aus Zeilen in der Form:

```
Login-ID:Pwd:UID:GID:Kommentar:Verzeichnis:Shell
```

- Beispiel:

```
karl:x:235:100:Karl Müller:/usr/karl/:/bin/sh
```

Klassische Benutzerverwaltung

Aufbau der Datei: `/etc/shadow`

- Besteht aus Zeilen in der Form:

```
Login-ID:Passwort:letzte Änderung:Min:Max:
     Vorwarnzeit:Inaktiv:Verfall:unbenutzt
```

- Beispiel:

```
sikamuel:*:11680:5:180:10:20:3:0
```

Klassische Benutzerverwaltung

Aufbau der Datei: `/etc/group`

- Besteht aus Zeilen in der Form:

  ```
  Name:Passwort:Group-ID:User-Liste
  ```

- Beispiel:

  ```
  studenten::200:sidabast,sikamuel
  ```

Weitere Konfigurationsdateien

- `/etc/profile`
- `/etc/aliases`
- `/etc/auto.master`
- `/etc/hosts`
- `/etc/networks`

Beurteilung

- Positiv:
  - transparent
  - schnell
  - Betriebssicher
- Negativ:
  - Synchronisationsprobleme
  - Pflegeaufwand linear zur Rechneranzahl
  - nicht erweiterbar
  - Unix-spezifisch

Überblick

- Klassische Benutzerverwaltung
- OpenLDAP
  - Verzeichnisdienste
  - LDAP im Detail
  - Zugangskontrolle
  - Anwendung
  - Beurteilung

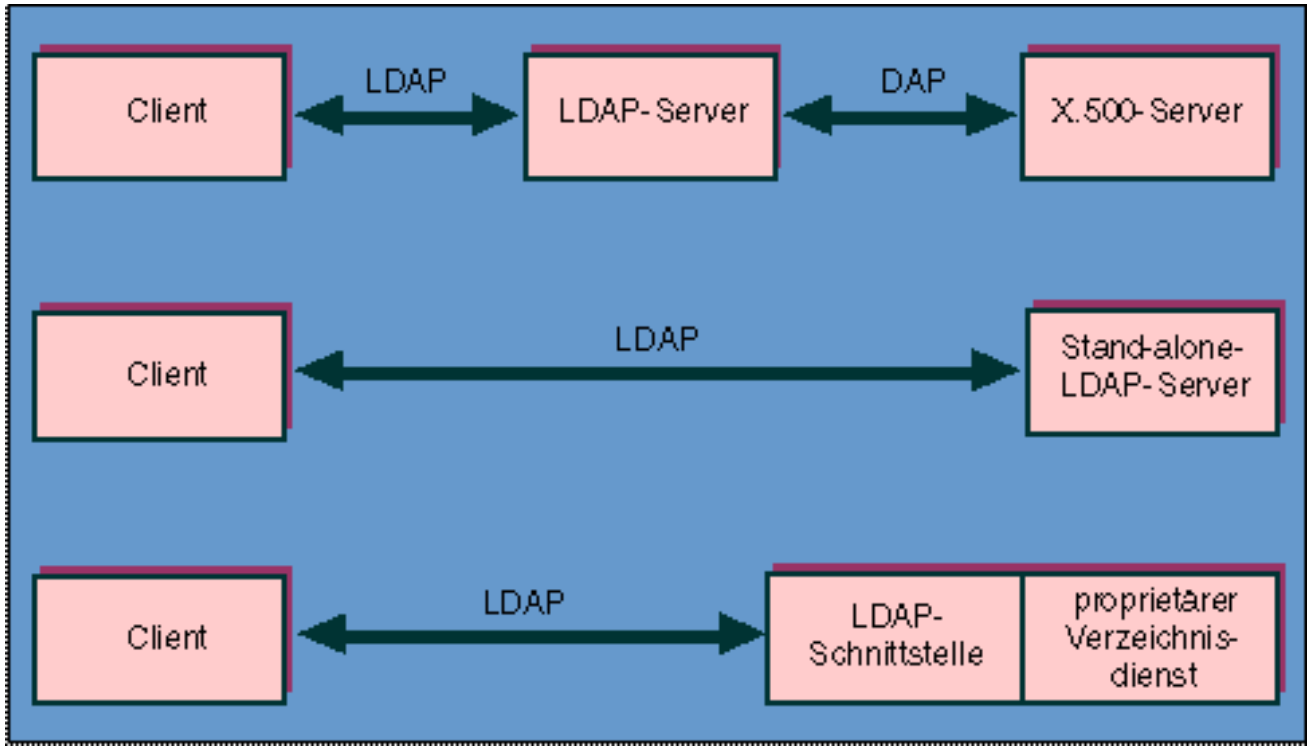
Einleitung

- Rechnerinfrastrukturen immer komplexer
- Anforderungen an einen Informationsdienst
  - plattformunabhängig
  - zentral u. lokal wartbar
  - einfach handhabbar
  - sicher
  - effektiv

LDAP ein Verzeichnisdienst

- LDAP:
  - Lightweight Directory Access Protocol
  - 1995 an der University of Michigan als Alternative zu X.500DAP entwickelt
  - Ursprünglich nur Zugriffsprotokoll auf X.500 Server

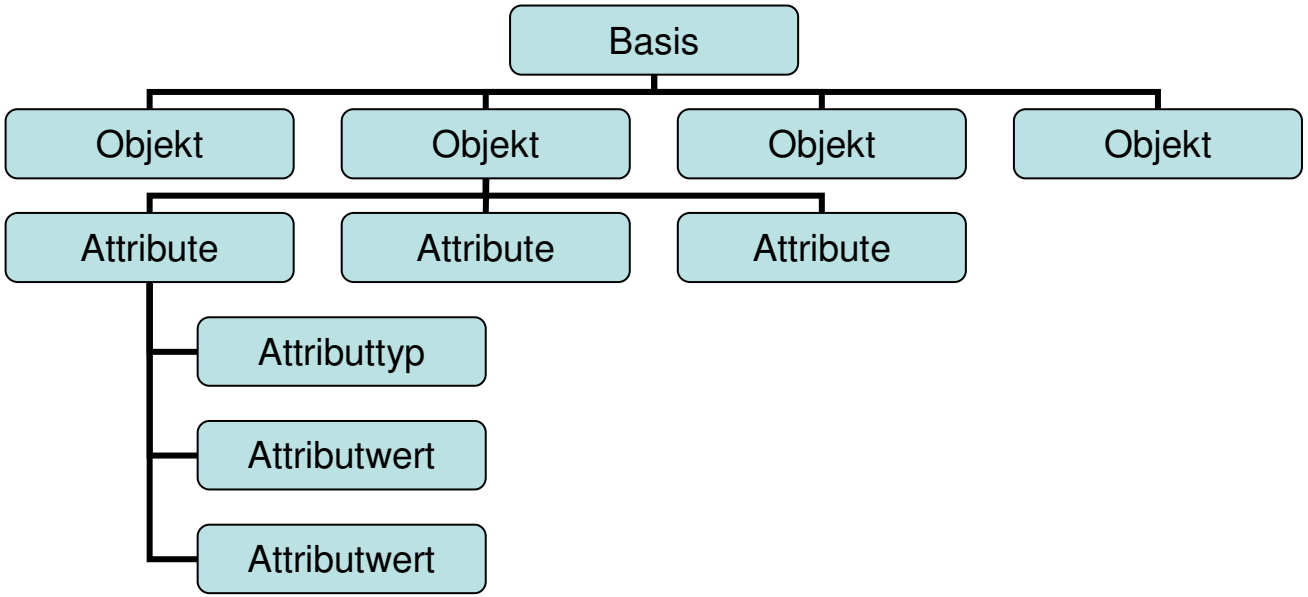
LDAP ein Verzeichnisdienst



LDAP-Informationsmodell: Objekt und Attribut

- Ein Datensatz ist ein Objekt
- Ein Objekt besteht aus Attributen
- Ein Attribut besteht aus Attributtyp und Attributwert
- Es kann als Single- oder Multivalued definiert werden
- Ein Attributtyp hat eine zugehörige Attributsyntax
- Ein Attributtyp kann verschieden Vergleichsregeln haben:
  - Equality
  - Substring
  - Ordering
  - Extensible

LDAP-Informationsmodell: Beispiel



LDAP-Informationsmodell: Schema

- Schema = Ansammlung von Objektklassen, Attribute, Syntaxen und Vergleichsregeln für eine bestimmten Zweck

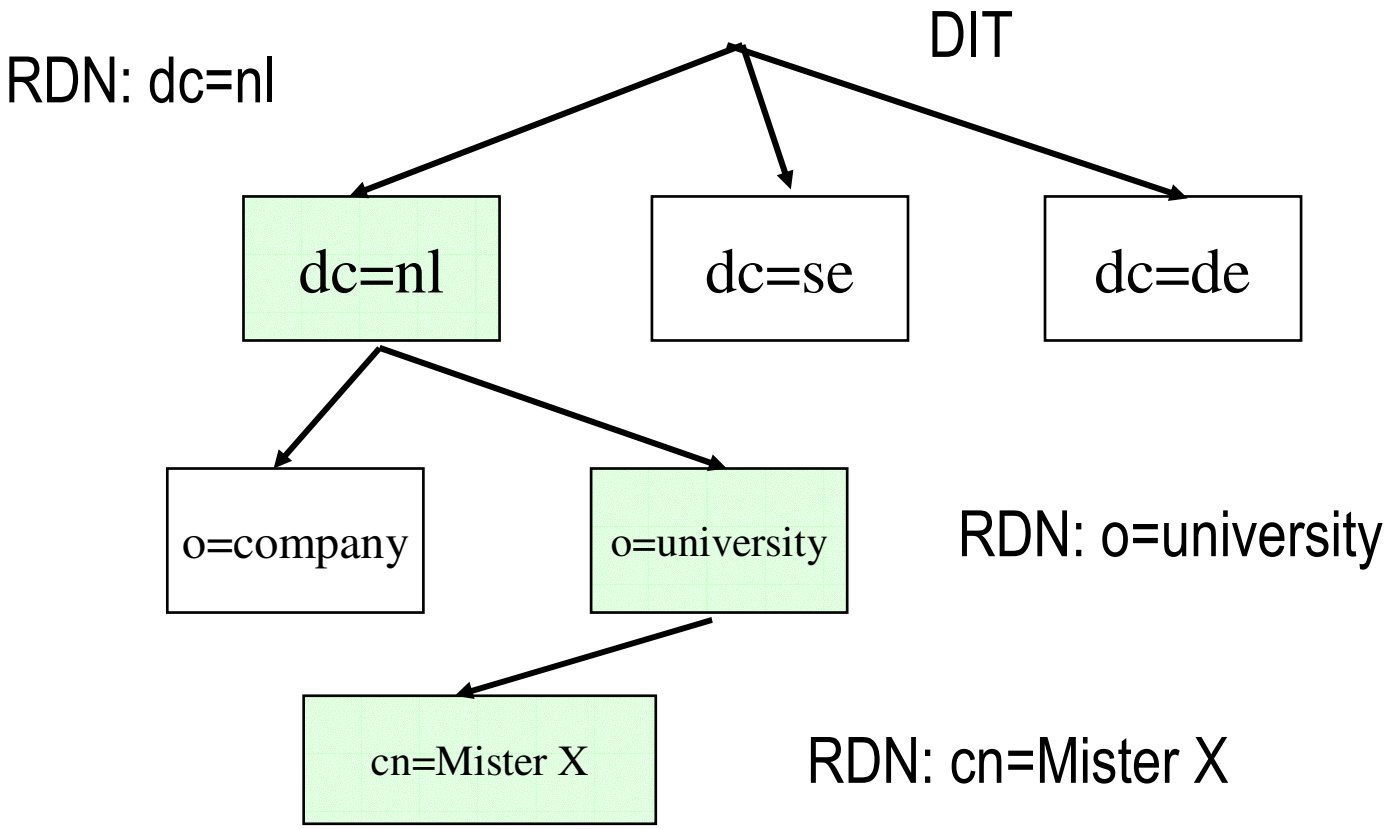
- Man kann Schemas selbst definieren und einfach verwenden
- Zur globalen Nutzung können sie standardisiert (IETF) oder registriert werden

LDAP-Namensraummodell: DIT, DN u. RDN

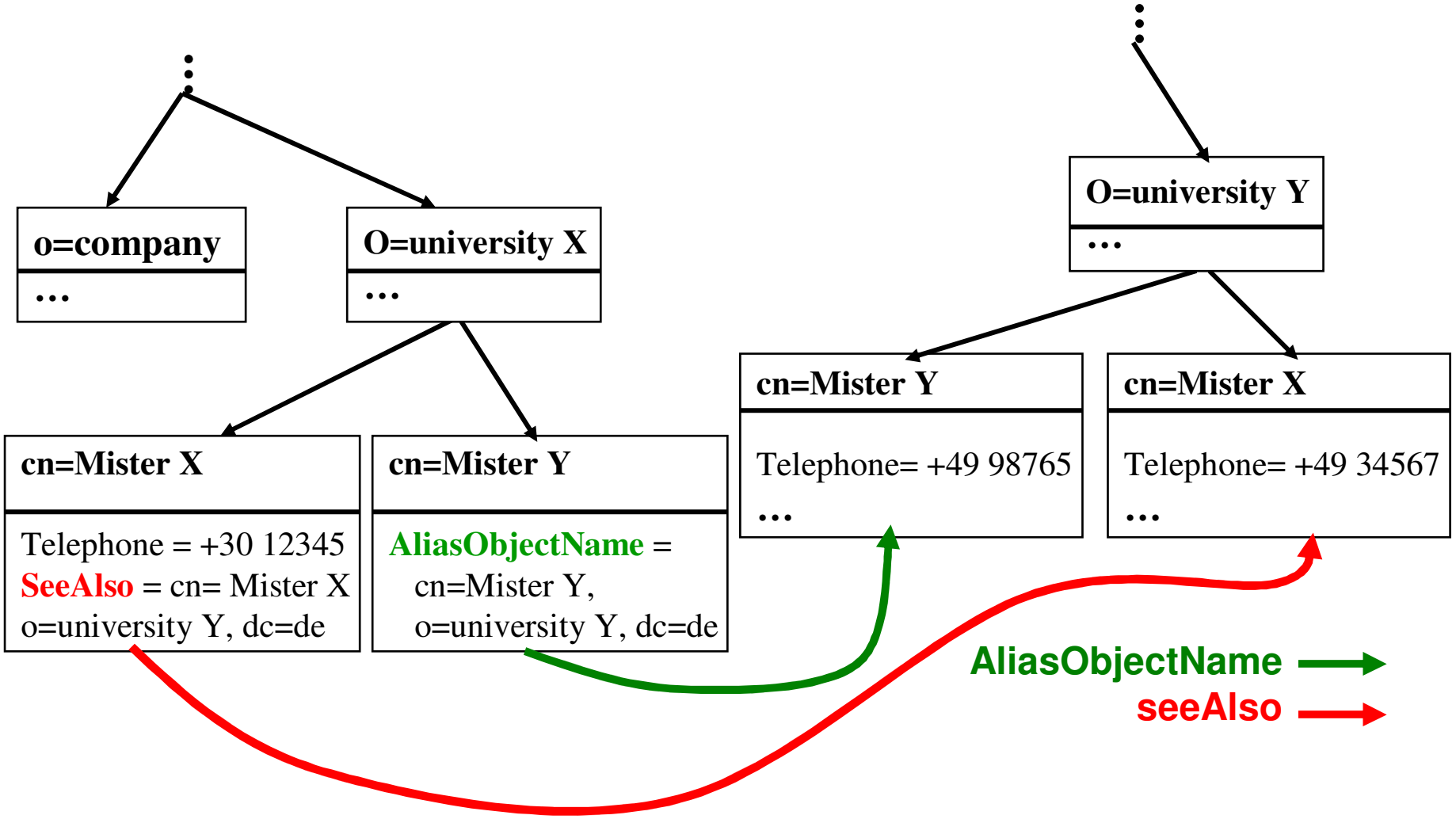
- Objekte sind Baumknoten:
  Directory Information Tree (DIT)
  - Jeder Knoten hat 0 bis n Kinderknoten
  - Jeder Konten hat genau 1 Elternknoten

- Jeder Eintrag hat in seiner Hierarchieebene einen eindeutigen Namen: Relativ Distinguished Name (RDN)
- Alle RDNs von Objekt bis Wurzel ergeben den Distinguished Name (DN)

LDAP-Namensraummodell: Beispiel

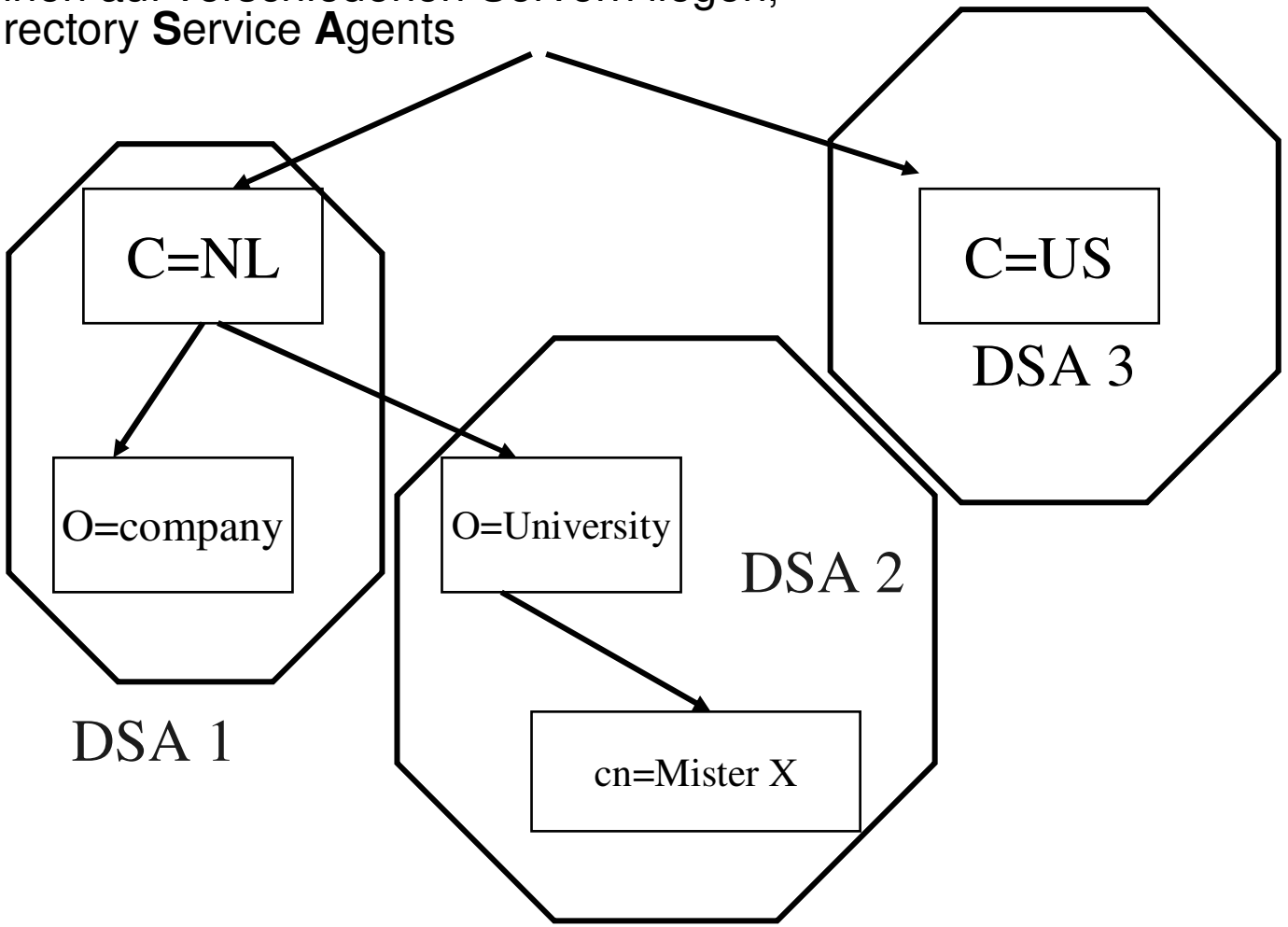


LDAP-Namensraummodell: DN als Zeiger



LDAP-Namensraummodell: Verteilung der Daten

Daten können auf verschiedenen Servern liegen,
sog **D**irectory **S**ervice **A**gents



Überblick

- Klassische Benutzerverwaltung
- OpenLDAP
  - Verzeichnisdienste
  - LDAP im Detail
  - Zugangskontrolle & Authentifizierung
  - Anwendung
  - Beurteilung

Authentifizierung

- Simple Bind: DN + Passwort
- Simple Bind + SSL: Verschlüsselte Session → DN + Passwort
- Alternative mit SASL (=Simple Authentification and Security Layer): Security Layer zwischen Protokol und der Verbindung

Zugangskontrolle

- Mit ACL (= Access Control List)
  - Nachteil: Zugriffsrechte stehen in der Serverkonfiguration

- Mit ACI (= Access Control Information)
  - Vorteile: Zugriffsrechte stehen in der Datenbank
  - Nachteile: nicht so flexibel, hoher Verwaltungsaufwand, noch experimentell

Anwendung: Login mit OpenLDAP

- Was man braucht:
  - `slap` : OpenLDAP Server
  - `libpam-ldap` : LDAP Modul für PAM
  - `ldap-utils` : Tools um Datenbank zu modifizieren
  - `gq` : zur grafischen Administration der Datenbank

Kann man unter Debian einfach mit

`apt-get install slap` ... installieren.

Anwendung: Login mit OpenLDAP

Konfiguration (1/2):

- /etc/ldap/slapd.conf: Serverkonfiguration
  - Name der Wurzel
  - Name und Passwort des Administrators

- /etc/ldap/ldap.conf : Zugriff-Infos für die Clienten-Seite
  - Rechnername oder IP des Servers
  - Wurzelobjekt, das als Basis für alle Suchaktionen verwendet wird

Anwendung: Login mit OpenLDAP

Konfiguration (2/2):

- /etc/pam.d/login : PAM Konfiguration für `login`
  - ersetzten des `pam_unix.so` Aufrufs gegen:

    ```
    auth requisite /lib/security/pam_ldpa.so
    ```

- /etc/pam_ldap.conf : Konfiguration des LDAP-PAM-Modules
  - Rechnername oder IP des Servers
  - Wurzelobjekt, das als Basis für alle Suchaktionen verwendet wird

Anwendung: Login mit OpenLDAP

- Einen Benutzer in die Datenbank eintragen:
  - Erstellen einer **L**DAP **D**irectory **I**nterchange **F**ormat (LDIF) Datei: sikamuel.ldif

```
dn: ou=user, dc=debian
ou: user
objectclass: organizationalUnit

dn: uid=sikamuel, ou=user, dc=debian
cn: Karl Müller
uid: sikamuel
uidNumber: 235
gidNumber: 100
homeDirectory: /usr/sikamuel/
userPassword: {CRYPT}kl1s4df3hklje5z87
beginShell: /bin/sh
objectclass: posixAccount
```

  - Import der Datei:
    ldapadd –D “cn=admin, dc=debian“ –w secret < sikamuel.ldif

Beurteilung

- Vorteile
  - Objektorientierte Datenmodulierung
  - Unabhängigkeit von Herstellern
  - Beliebige Skalierbarkeit
  - Ausfallsicherheit
  - Hohe Sicherheit
  - Anbindung über TCP/IP
  - Keine unnötige Redundanz

Beurteilung

- Nachteil
  - Schwierige Konsistenzhaltung
  - Unterstützung von ACIs noch experimentel

Literatur

- [1] Unix Benutzerverwaltung, Arnold Willemer
  http://www.willemer.de/informatik/unix/unsyuser.htm
- [2] Betriebssystem UNIX/Linux, Prof. Jürgen Plate
  http://www.fs.ei.tum.de/admin/howto/unix/
- [3] Linux: Installation, Konfiguration, Anwendung, Michael Kofler
  3. Auflage Addison-Wesley, 1998
- [4] LDAP Quellen: Wissen, Anleitungen, Artikel
  http://www.sendung.de/ldap/wissen/
- [5] LDAP – Überblick über das Chaos, Peter Wachtler, Linux-Magazin 09/1998
  http://www.linux-magazin.de/Artikel/ausgabe/1998/09/LDAP/ldap.html
- [6] Universalservice, Markus Jünemann, iX 8/1997
  http://www.heise.de/ix/artikel/1997/08/118/
- [7] OpenLDAP Documentation
  http://www.openldap.org/doc/
- [8] LDAP – Eine Einführung von Petra Haberer
  http://www.mitlinx.de/ldap/assets/LDAP.pdf
- [9] LDAP and OpenLDAP (on the Linux Platform), Adam Tauno Williams 2001
  ftp://kalamazoolinux.org/pub/pdf/ldapv3.pdf