

# Samba / OpenLDAP

## Ein Erfahrungsbericht



Digicomp Academy – OpenTuesday, 4. April 2006  
Beni Schoedler, PHZ Luzern

# Themen

Zu meiner Person

Die PHZ Luzern

Vorgeschichte + Entwicklung

Heutige Infrastruktur im Überblick

Samba / OpenLDAP basierte Server

OpenLDAP nutzende Dienste / Angebote

Print-Accounting

Backup / Restore

Verwaltung LDAP Directory

Zukünftige Projekte

Weitere Features von Samba 3

Wichtigste Einschränkungen

Fazit

# Zu meiner Person

Beni Schoedler

Dipl Masch Ing ETH, Leiter Technik PHZ Luzern

1996 Erste Linuxerfahrungen

1996-1998 Assistententätigkeit an ETH (Perl Progr)

1998-2000 TD Luzern

1999-2004 Aufbau ICT Infrastruktur PZM Luzern

2002-2004 ICT Projekte BKD, Verantwortlich für  
Linuxserver (Proxy, DNS, etc) Mittel- und Berufsschulen  
Kt. Luzern (BKD)

2003-heute Leiter ICT Technik PHZ Luzern

# Die PHZ Luzern

Grösste Teilschule der Pädagogischen Hochschule Zentralschweiz

Drei Standorte Luzern, Schwyz und Zug + Direktion

Teil des Campusnetzwerks Zentralschweiz (FHZ, UNILU, ZHB, PHZ)

Teilt Gebäude und Infrastruktur mit dem Pädagogischen Ausbildungszentrum Musegg (Lehrerseminar und Kurzzeitgymnasium)

Gemeinsame ICT Infrastruktur unter dem Namen MuseggNet

# Vorgeschichte

1999

## **PZM Luzern (Lehrerseminar)**

650 Studierende, 200 Lehrpersonen, ICT Support durch  
Lehrperson

ca 40 Windows 95 PCs in 3 Zimmern

1 NT Server ohne Funktion

10base2 Netzwerk

Internetzugang via ISDN & Wingate Proxy

# Schulverwaltung

## Strikte Trennung Verwaltungs- und Schulnetz

1999: Novellserver, ca 8 Clients, Netzwerkdrucker

2000: Windows 2000 Server, 10 Clients, Netzwerkdrucker

2005: Windows 2000 Server, 30 Clients, Netzwerkdrucker

2006: Trennung Verwaltung PZM & PHZ Luzern

PZM: weiterhin Windows 2000 Server

PHZ: Integration in MuseggNet, eigener Server

# Entwicklung

1999

## PZM Luzern (Lehrerseminar + Kurzzeitgymnasium)

700 Studierende, 200 Lehrpersonen

ICT Support durch Lehrperson und **1 Student (10%)**

Ersatz der Schüler-Computer (ca 40 Stück)

Windows 98 Clients

10base2 + 100baseT Netzwerk

1 PC als File- und Printserver mit Samba

1 Login für alle, 1 Share auf dem Server

1 Netzwerkdrucker

# Entwicklung

2000

PZM Luzern (Lehrerseminar + Kurzzeitgymnasium)  
750 Studierende, 200 Lehrpersonen  
ICT Support durch Lehrperson und **2 Studenten (20-30%)**

Zusätzlicher Computerraum mit 12 PCs und Netzwerkdrucker  
Computer für Lehrer (ca 10 PCs), lokale Drucker  
100baseT Netzwerk  
Serverraum  
Neuer Fileserver (Linux Samba, DHCP, DNS)  
Persönliche Konti für Lehrer und Schüler  
Internetzugang via Mietleitung (256kBit/s)  
Linuxproxy (Squid)

# Entwicklung

2001

PZM Luzern (Lehrerseminar + Kurzzeitgymnasium)  
750 Studierende, 200 Lehrpersonen  
ICT Support durch Lehrperson und **2 Studenten (40-60%)**

Umfassende ICT Projekte durch BKD

- Beschaffung zusätzlicher Computer für Fachschaften und Lehrerzimmer
- E-Mail Adressen für Lehrpersonen

Erster Mailserver (qmail) für ICT, Maillisten & Studis; SMTP

Neue Clientimages

# Entwicklung

2002

PZM Luzern (Lehrerseminar + Kurzzeitgymnasium)  
750 Studierende, 200 Lehrpersonen  
ICT Support: **60% + 1 Student 20%**

Erster Mailserver (qmail) für ICT, Maillisten & Studis; SMTP  
Zusätzliche Server (appl, www, DNS)  
Aufstockung Informatikzimmer von 12 auf 25 Computer  
ICT Website  
Umfassendere Betreuung (Workshops, Dokumentationen etc)  
Erste Planung ICT PHZ

- Notebooks für alle
- 850 Studierende, 150 Doz, 50 MA

# Entwicklung

2003

PZM Luzern + **PHZ Luzern (Start im Herbst)**  
**1000** Studierende, 300 Lehrpersonen, 20 MA  
**ICT Technik + Support: 200% + 70% Organisation/Pädagogik**

Aufbau Wireless LAN

Vernetzung neuer Räumlichkeiten

Einführung eines Mailclusters für Studierende (qmail-ldap)

Ersatz fast aller Computer + Zusatzbeschaffung (ca 140)

Planung neuer Infrastruktur (Netzwerk, Server)

Beschaffung Hardware

# Entwicklung

2004

PZM Luzern + PHZ Luzern

1250 Studierende, 300 Lehrpersonen, 20 MA

ICT Technik + Support: **250%** + 70% Organisation/Pädagogik

## Umsetzung neuer Infrastruktur

L3 Netzwerk

Ausbau WLAN

Ablösung des bisherigen Sambaservers durch neue Server (5)

Neue Firewalls (2)

Einführung von Samba3 und OpenLDAP

# Entwicklung

2005

PZM Luzern + PHZ Luzern

**1400** Studierende, 350 Lehrpersonen, 50 MA

ICT Technik + Support: **310%** + **100%** Leitung/Pädagogik

Weitere Standorte

Verdoppelung WLAN

Weitere Dienste

Neue Diskbackup-Lösung

# Entwicklung

2006

PZM Luzern + PHZ Luzern

**1500** Studierende, 350 Lehrpersonen, 50 MA

ICT Technik+Support: **310%** + **100%** Leitung/Pädagogik + 40%  
Sekretariat

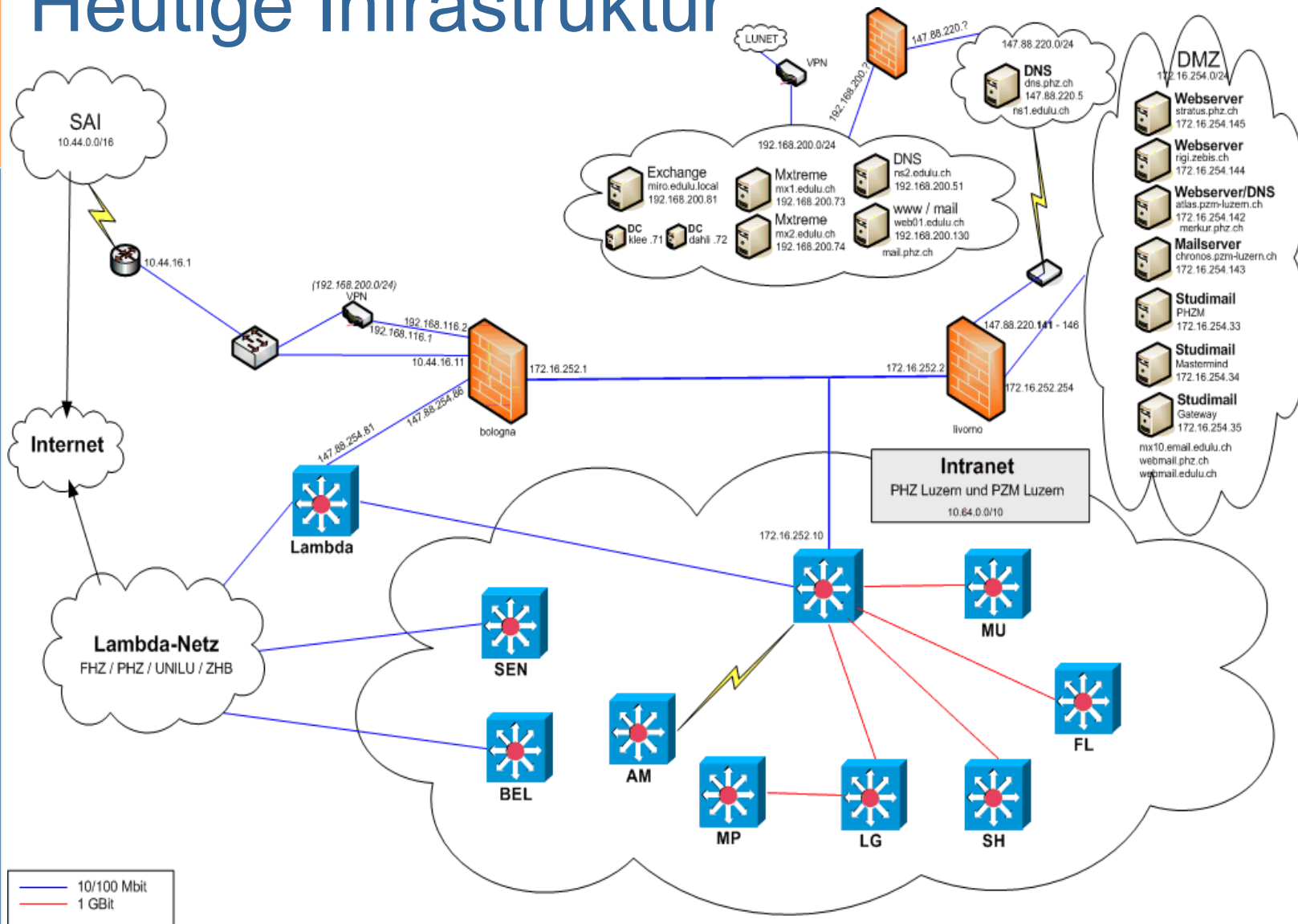
Netzwerküberarbeitung (LAN + WLAN)

Integration weiterer Standorte und Dienststellen

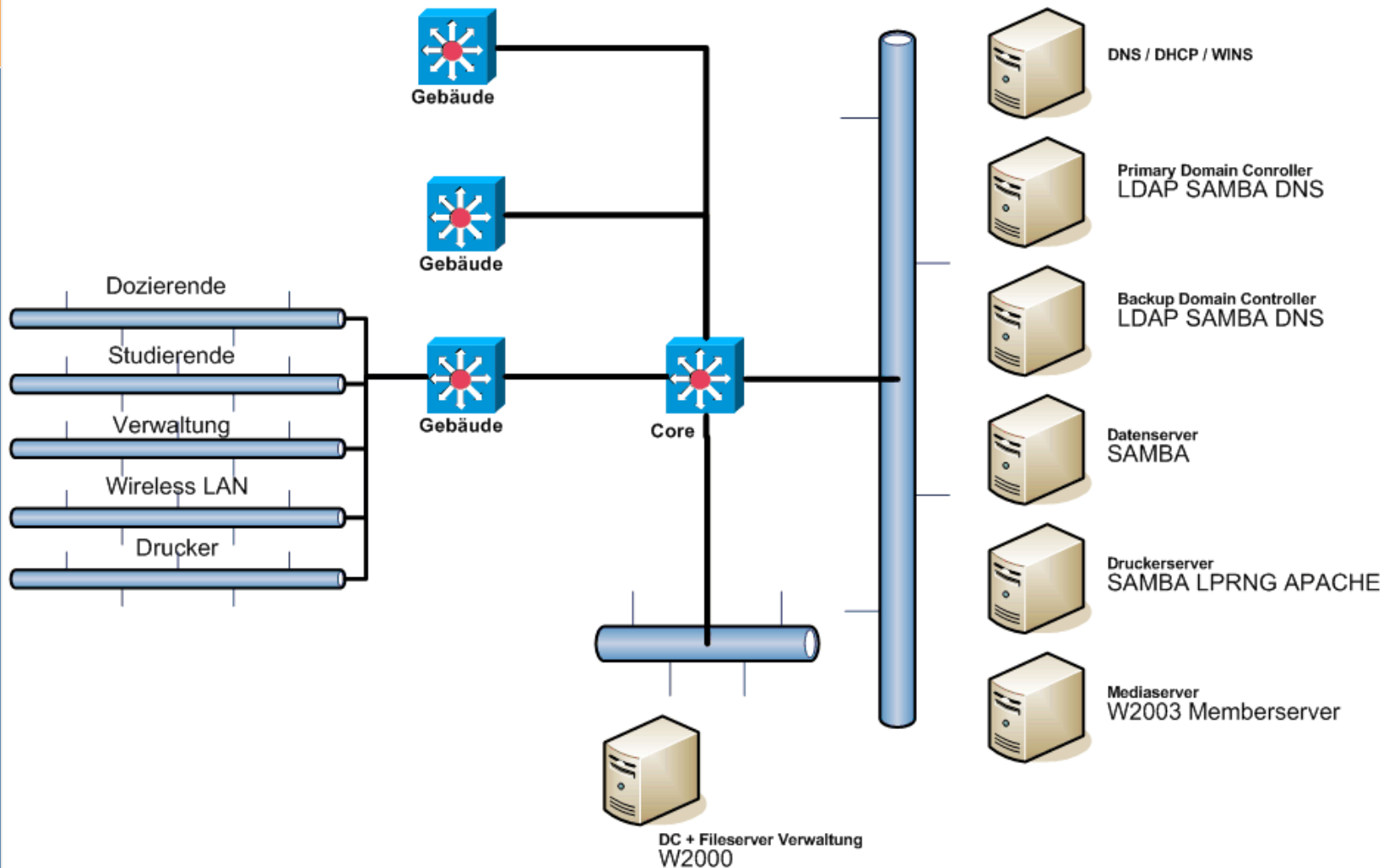
Redesign Websites

Daily business...

# Heutige Infrastruktur



# Heutige Infrastruktur



# Heutige Infrastruktur

## **Samba / OpenLDAP basierte Server**

(Domaincontroller, Fileserver, Printserver, Webserver)

## **OpenLDAP nutzende Dienste / Angebote**

## **Print-Accounting**

## **Backup / Restore**

# Samba / OpenLDAP basierte Server

## Warum OpenLDAP als Account-Datenbank?

- Bedürfnis beliebige Informationen abzulegen
- Viele Dienste haben eine LDAP Schnittstelle
- Elegante Art mehrere Domaincontroller einzusetzen
- Memberserver können einfach eingebunden werden

> **Skalierbarkeit und Flexibilität**

# OpenLDAP Account Datenbank

## smbpasswd

Username

UID

LM Password Hash

NT Password Hash

Account Flags

Last Change Time

## ldapsam

sambaLMPassword

sambaNTPassword

sambaPwdLastSet

sambaPwdCanChange

sambaPwdMustChange

sambaKickoffTime

sambaAcctFlags

sambaUserWorkstation

sambaHomeDrive

sambaLogonScript

sambaProfilePath

sambaHomePath

sambaSID

sambaPrimaryGroupSID

sambaDomainName

sambaLogonTime

sambaLogoffTime

# OpenLDAP Account Datenbank

```
dn: uid=beni,ou=Mitarbeiter,ou=People,o=museggnet,c=ch
objectClass: posixAccount
objectClass: sambaSamAccount
cn: Schoedler Beni
sn: Schoedler
givenName: Beni
gecos: Schoedler Beni
displayName: Schoedler Beni
uid: beni
uidNumber: 5079
gidNumber: 1016
homeDirectory: /home/b/beni
loginShell: /bin/bash
sambaHomeDrive: P:
sambaSID: S-1-5-21-xxx-11158
sambaPrimaryGroupSID: S-1-5-21-xxx-3033
sambaHomePath: \\files\beni
sambaAcctFlags: [U]
sambaPwdMustChange: 2147483647
sambaPwdCanChange: 1104758339
sambaLMPassword: xxxxxxxxxxxx
sambaNTPassword: xxxxxxxxxxxx
sambaPwdLastSet: 1104759939
userPassword: xxxxxxxxxxxx
```

# OpenLDAP Account Datenbank

## Flexibilität durch eigene Schemas

```
dn: uid=beni,ou=Mitarbeiter,ou=People,o=museggnet,c=ch
objectClass: museggnetUser
description: --
mail: beni.schoedler@phz.ch
affiliation: PLU
affiliation: PZM
museggnetAccountStatus: active
museggnetUserType: MAV
museggnetEcoOpenID: 1234
museggnetEventoID: 12345
museggnetToken: bs
museggnetMailAddress: beni.schoedler@phz.ch
museggnetMailAddress: beni.schoedler@edulu.ch
museggnetBlackBoardLogin: phzlu_a_beni
museggnetStatusChangedDate: 2006-03-23
initialPassword: xxxxxxxxx
...
```

# UIDs in MS Windows und Linux

Unix/Linux arbeitet mit UIDs, Windows mit SIDs

Samba verlangt für alle Konten eine lokale UID

UIDs und SIDs werden im LDAP Verzeichnis verwaltet

pam\_ldap und nss\_ldap werden für die UNIX  
Benutzerauflösung und Anmeldung verwendet.

```
dn: uid=beni,ou=Mitarbeiter,ou=People,o=museggnet,c=ch
objectClass: posixAccount
objectClass: sambaSamAccount
gecos: Schoedler Beni
uid: beni
uidNumber: 5079
gidNumber: 1016
homeDirectory: /home/b/beni
loginShell: /bin/bash
sambaSID: S-1-5-21-xxx-11158
sambaPrimaryGroupSID: S-1-5-21-xxx-3033
```

# nss\_ldap und pam\_ldap

## /etc/ldap.conf

```
base o=museggnet,c=ch
uri ldap://torino.museggnet.ch ldap://venezia.museggnet.ch
ldap_version 3
scope sub
pam_filter objectclass=posixAccount
pam_login_attribute uid
pam_member_attribute memberuid
nss_base_passwd o=museggnet,c=ch?sub
nss_base_shadow o=museggnet,c=ch?sub
nss_base_group ou=Groups,o=museggnet,c=ch?sub
```

## /etc/nsswitch.conf

```
passwd:      files ldap
shadow:     files ldap
group:      files ldap
```

# nss\_ldap und pam\_ldap

## /etc/pam.d/system-auth

```

auth          required      pam_env.so
auth          sufficient   pam_unix.so likeauth nullok
auth         sufficient   pam_ldap.so use_first_pass
auth          required      pam_deny.so

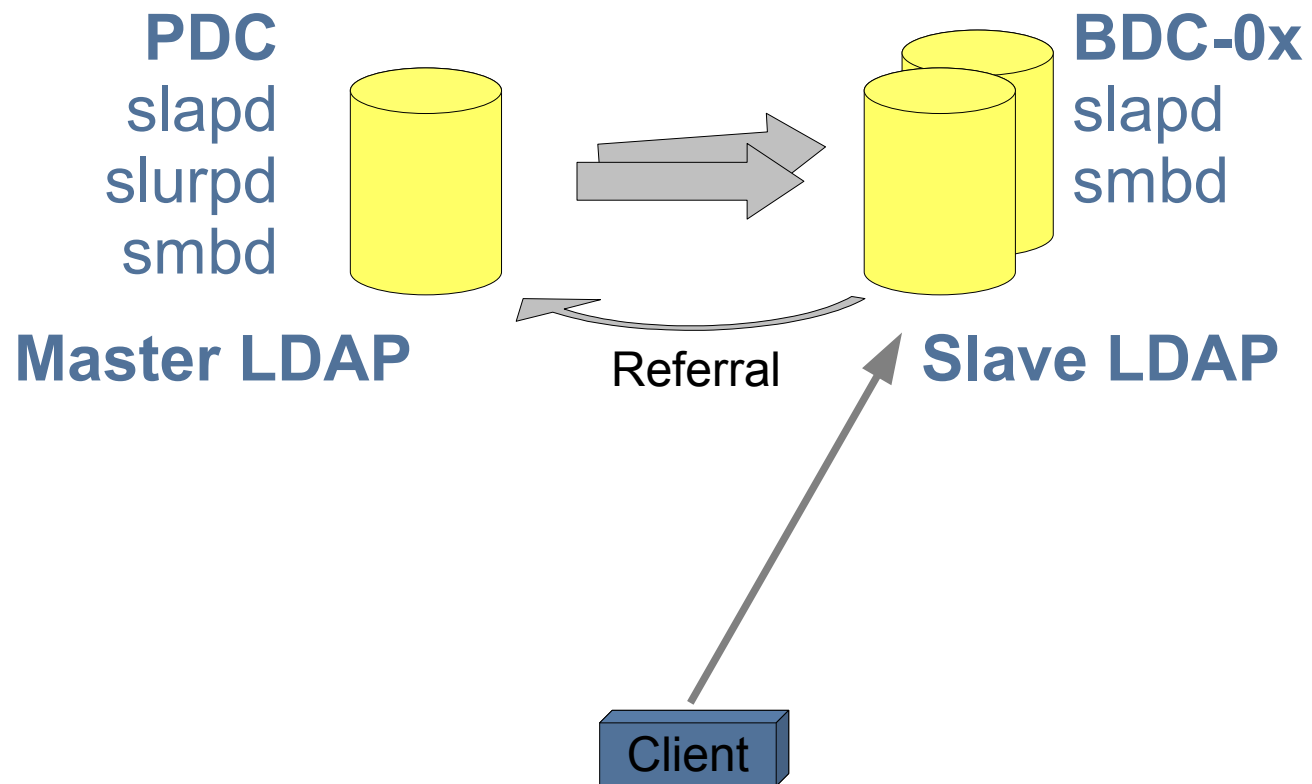
account     sufficient   pam_ldap.so
account       sufficient   pam_unix.so
account       required      pam_deny.so

password      required      pam_cracklib.so difok=2 minlen=8 dcredit=2
ocredit=2    retry=3
password      sufficient   pam_unix.so nullok md5 shadow use_authtok
password    sufficient   pam_ldap.so use_authtok
password      required      pam_deny.so

session       required      pam_limits.so
session       required      pam_unix.so
session       optional     pam_ldap.so

```

# Primary & Backup Domain Control



# Primary & Backup Domain Control

## Master LDAP

```
# master slurp replication config
replica          uri=ldap://venezia.museggnet.ch
binddn="cn=replica,ou=DSA,o=museggnet,c=ch"
bindmethod=simple
credentials="xxxxx"
repllogfile      /etc/openldap/replica/repllog
```

## Slave LDAP

```
# slave slurp replication config
updatedn         "cn=replica,ou=DSA,o=museggnet,c=ch"
updateref        ldap://torino.museggnet.ch
```

# Primary & Backup Domain Control

## Primary Domain Controller: Master LDAP

```
[global]
workgroup = MUSEGGNET
netbios name = PDC
server string = Domain Controller
security=user

domain logons = yes
domain master = yes
preferred master = yes
local master = yes
os level = 65
passdb backend = ldapsam:ldap://torino.museggnet.ch
ldap suffix = o=museggnet,c=ch
ldap user suffix = ou=People
ldap group suffix = ou=Groups
ldap machine suffix = ou=Computers
ldap filter = (&(uid=%u)(objectClass=*))
ldap admin dn = "cn=samba,ou=DSA,o=museggnet,c=ch"
```

# Primary & Backup Domain Control

## Backup Domain Controller: Slave LDAP

```
[global]
workgroup = MUSEGGNET
netbios name = BDC-MU1
server string = Domain Controller
security=user

domain logons = yes
domain master = no
preferred master = no
local master = no
os level = 1
passdb backend = ldapsam:ldap://venezia.museggnet.ch
ldap suffix = o=museggnet,c=ch
ldap user suffix = ou=People
ldap group suffix = ou=Groups
ldap machine suffix = ou=Computers
ldap filter = (&(uid=%u)(objectClass=*))
ldap admin dn = "cn=samba,ou=DSA,o=museggnet,c=ch"
```

# Domain-Memberserver

## z.B. der Fileserver

```
[global]
workgroup = MUSEGGNET
netbios name = FILES
server string = Schulserver
security=DOMAIN
domain logons = no
domain master = no
preferred master = no
local master = no
os level = 1
password server = *
# password server = torino
```

## Server der Domäne hinzufügen

```
# net rpc join -Ubeni
Password:
Joined domain MUSEGGNET.
```

# Lokale Einstellungen auf Servern

Home - Directories auf Fileservern

Quotas auf Fileservern

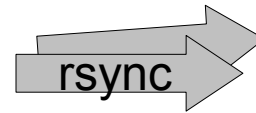
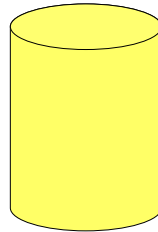
Print-Accounting auf Printserver

- > Automatische Einrichtung beim ersten Login
- > Abfrage von Informationen aus Verzeichnis
- > root preexec

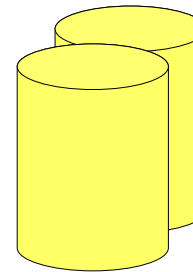
```
[homes]  
root preexec = /root/bin/makehomedir %u
```

# Logonskripte

**PDC**  
smbd



**BDC-0x**  
smbd



**\\pdc\netlogon**

**\\bdc-0x\netlogon**

Authentifizierung am  
nächstgelegenen DC (BDC)  
`\\%LOGONSERVER%\netlogon`



# Logonskripte



```
C:\ MUSEGGNET Logon Script

Willkommen im MUSEGGNET      Fritz le Pücher      3.4.2006, 15:20:57

Umgebung einrichten

* Netzlaufwerke verbinden...
  \\files\daten auf Q:      [OK]
  \\files\public auf R:    [OK]
  \\mm\sw-allg$ auf U:     [OK]

* Netzwerkdrucker verbinden...
  \\printer\lg403-lj5000    [OK]
  \\printer\lg500-lj4300    [OK]
  \\printer\lg500-ph8200    [OK]

* Standarddrucker setzen...
  \\printer\lg403-lj5000    [OK]

Kontoinformationen fritz

* Fileserver Speicherbelegung:
  Daten: 8 MB (max 98 MB)
  Files: 408 (max 10000)

* Druck-Credits:
  Kontostand: CHF 4.10

ICT PZM & PHZ Luzern: http://ict.luzern.phz.ch / support@ict.luzern.phz.ch
```

# MSDFS – MS Distributed Filesystem

Notebooks nicht in Domäne  
(Zu) viele Server können verwirren  
Laufwerksbuchstaben sparen

- > Transparente Verbindungen mit msdfs
- > Unterstützt von W95 bis XP

```
[global]
    host msdfs = yes

[homes]
    msdfs root = yes

# ls -l ~beni
lrwxrwxrwx 1 root root 19 Oct 31 21:16 homepage -> msdfs:palermo\beni
```

# LDAP nutzende Dienste / Angebote

**SSH Authentifizierung (via PAM)**

**HTTP Authentifizierung (TWiki, Print-Accounting)**

**FTP Authentifizierung (auf dem Webserver)**

**Adressbuch**

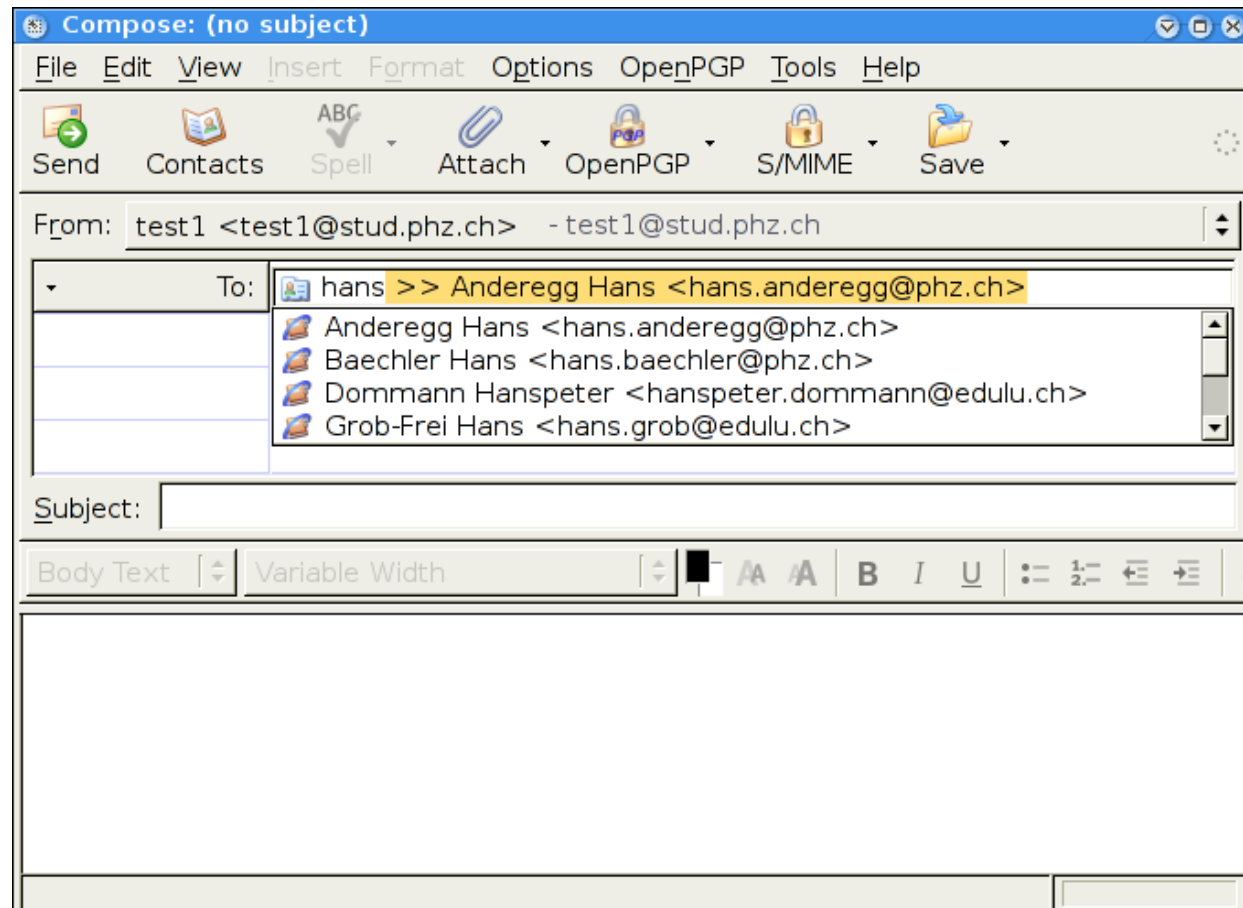
**Studi-E-Mail: Accounts in OpenLDAP DB**

# HTTP Authentifizierung

[http://www.rudedog.org/auth\\_ldap/](http://www.rudedog.org/auth_ldap/)

```
<VirtualHost *>
  [...]
  AuthLDAPCacheSize 0
  <Directory "/data/httpd/sites/doc/htdocs">
    AllowOverride All
    Order allow,deny
    Allow from all
    AuthName "Whatever"
    AuthType basic
    AuthLDAPAuthoritative on
    AuthLDAPUrl ldap://torino.museggnet.ch/o=museggnet,c=ch?uid
    AuthLDAPGroupAttribute memberuid
    AuthLDAPGroupAttributeIsDN off
    require group cn=ict,ou=Abteilung,ou=groups,o=museggnet,c=ch
```

# Adressbuch



# Print-Accounting

**Drucken nicht gratis**

**Kredit- und Debitsystem**

**Accounting wird automatisch eingerichtet**

**Keine virtuellen Spooler; Pagecounter der Drucker werden abgefragt > nur wirklich gedruckte Seiten werden verrechnet.**

**Statusabfrage durch User**

**Gutschriften durch Sekretariate**

**Reports**

# Print-Accounting

Drucksystem PZM und PHZ Luzern - Mozilla Firefox

File Bearbeiten Ansicht Gehe Lesezeichen Extras Hilfe

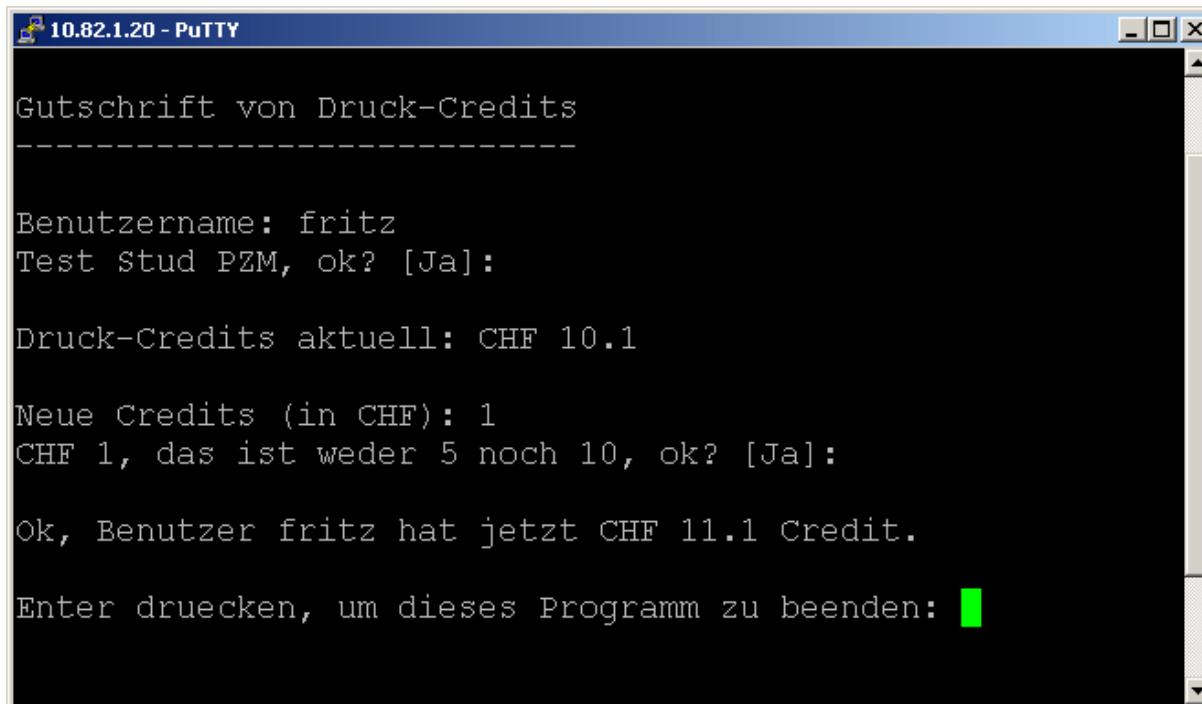
## Ihr Druck-Konto

Benutzername: **fritz** (Test Stud PZM)  
Kontostand: **Fr 10.10**

Datum	Zeit	Aktion	Betrag	Infos
1970-01-01	03:16:27	Saldo	5.00	-11-18T16:59:00Z initial credits
2005-11-18	18:04:53	Ausdruck	-0.10	pages 1 printer lg500-lj4300
2005-12-15	16:24:44	Ausdruck	-0.20	pages 2 printer lg500-lj4300
2005-12-15	16:25:26	Ausdruck	-0.10	pages 1 printer lg500-lj4300
2005-12-15	16:26:07	Ausdruck	-0.10	pages 1 printer lg500-lj4300
2005-12-19	16:21:17	Ausdruck	-0.10	pages 1 printer lg403-lj5000
2006-01-04	17:17:58	Ausdruck	-0.10	pages 1 printer fl100-lj2300
2006-01-13	17:21:33	Ausdruck	-0.10	pages 1 printer lg403-lj5000
2006-02-23	09:04:06	Ausdruck	0.00	printer lg403-lj5000 job 15009 acct: start 29712 pages 0 bytes 1148
2006-02-23	10:10:48	Ausdruck	-0.10	printer lg403-lj5000 job 16136 acct: start 29714 pages 1 bytes 74204
2006-04-03	15:33:24	Gutschrift	1.00	bought new credits
2006-04-03	15:33:46	Gutschrift	5.00	bought new credits

**Tech info** for support personnel: acct fritz balance 1010 limit 0

# Print-Accounting



```
10.82.1.20 - PuTTY
Gutschrift von Druck-Credits
-----
Benutzername: fritz
Test Stud PZM, ok? [Ja]:
Druck-Credits aktuell: CHF 10.1
Neue Credits (in CHF): 1
CHF 1, das ist weder 5 noch 10, ok? [Ja]:
Ok, Benutzer fritz hat jetzt CHF 11.1 Credit.
Enter druecken, um dieses Programm zu beenden: █
```

# Backup und Restore

## OpenLDAP Backup

### Periodische DB Sicherung

```
ldapsearch -x -W -h localhost -b "c=CH" -D "cn=admin,..." \  
            "(objectclass=*)" > backup.ldif
```

## OpenLDAP Restore

slapd stoppen

Datenbank-Files löschen

slapd starten

Daten einlesen

```
ldapadd -h localhost -x -W -c -D "cn=admin,..." -f backup.ldif
```

# Backup und Restore

## Linux Backup

### Fullbackup mit rsync auf Diskserver

```
rsync -avz -e ssh quellserver:/ .  
rsync -avz -e ssh -exclude-from=lost+found -exclude-from=/proc/ \  
quellserver:/ .
```

# Backup und Restore

## Linux Restore

Gerät von CD booten (z.B. Knoppix)

Disks partitionieren und formatieren

Mountpoints erzeugen, Disks mounten

Backup mit rsync vom Diskserver holen

Chrooten

Evtl Kernel neu kompilieren (bei geänderter Hardware)

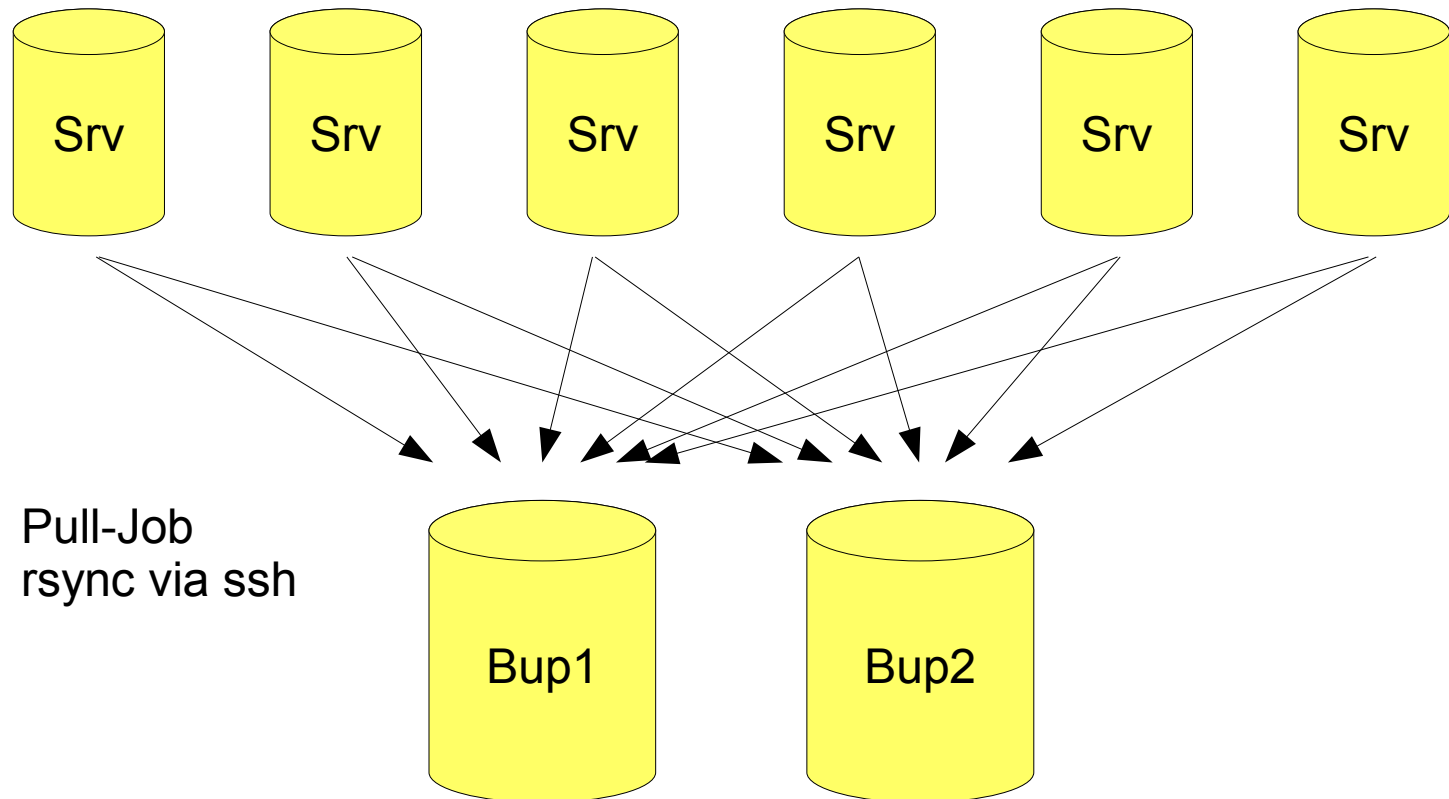
Bootloader (z.B. Grub) neu installieren

Exit und alle Disks unmounten

Neu starten

# Backup und Restore

## Diskbackup mit Dirvish



# Backup und Restore

## Diskbackup mit Dirvish

Sammlung von Perl-Skripten um rsync

Komplette Sicherung von Servern

1 Fullbackup dann inkrementelle Sicherungen

Stets Zugriff auf vollständige Daten durch  
ausgeklügeltes Hardlinking

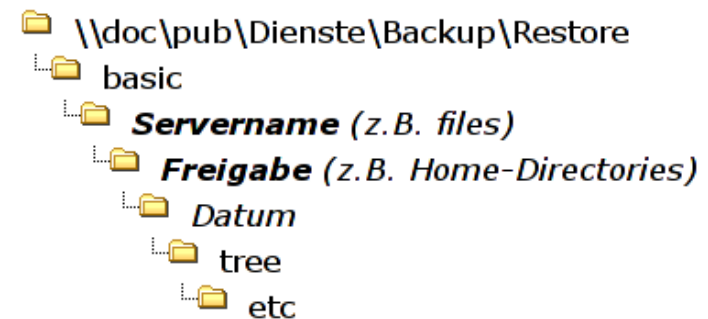
Automatisches Expiring

Weitere Informationen: <http://www.dirvish.com>

# Backup und Restore

## Diskbackup mit Dirvish

```
|-- milano  
|   |-- 2005-04-03-2300  
|       |-- tree  
|   |-- 2005-05-01-2300  
|       |-- tree  
|   |-- 2005-06-05-2300  
|       |-- tree  
|   |-- 2005-07-03-2300  
|       |-- tree  
|   |-- 2005-08-07-2300
```



# Verwaltung LDAP Directory

## Ein gewisses „Problem“

Viele Möglichkeiten: GUIs, Skripten

Meist keine „Out of the Box“ Lösung

Flexibilität ist hier ein „Nachteil“

Skripting funktioniert sehr gut

# Verwaltung LDAP Directory

## GUIs

GOSA (<http://gosa.gonicus.de>)

Ldap Account Manager LAM (<http://lam.sourceforge.net>)

phpLDAPadmin (<http://phpldapadmin.sourceforge.net>)

gq (<http://sourceforge.net/projects/gqclient>)

etc

# Gosa



**GOsa<sup>2</sup>** [Hauptmenü](#) [Hilfe](#) [Abmelden](#)

**Willkommen Beni Schoedler!**

Dies ist die Hauptseite von GOsa. Wählen Sie die gewünschte Option aus dem Menü links oder durch die Maus. Alle Änderungen werden direkt in den LDAP-Server Ihres Unternehmens eingepflegt.

Benutzen Sie **Abmelden** oben links, um die Arbeit mit GOsa zu beenden und **Hauptseite**, um wieder in die Hauptseite zu gelangen.

**Mein Konto**

- Allgemein
- UNIX
- Umgebung
- Mail
- Samba
- Konnektivität
- Fax
- Telefon
- Passwort

**Administration**

- Benutzer
- Gruppen
- Objektgruppen
- Abteilungen
- Anwendungen
- Systeme
- FAI
- Fax-Sperrlisten
- Telefon-Makros
- Telefon-Konferenzen

**Mein Konto**

- Allgemein
- UNIX
- Umgebung
- Mail
- Konnektivität
- Fax
- Telefon
- Passwort

**Administration**

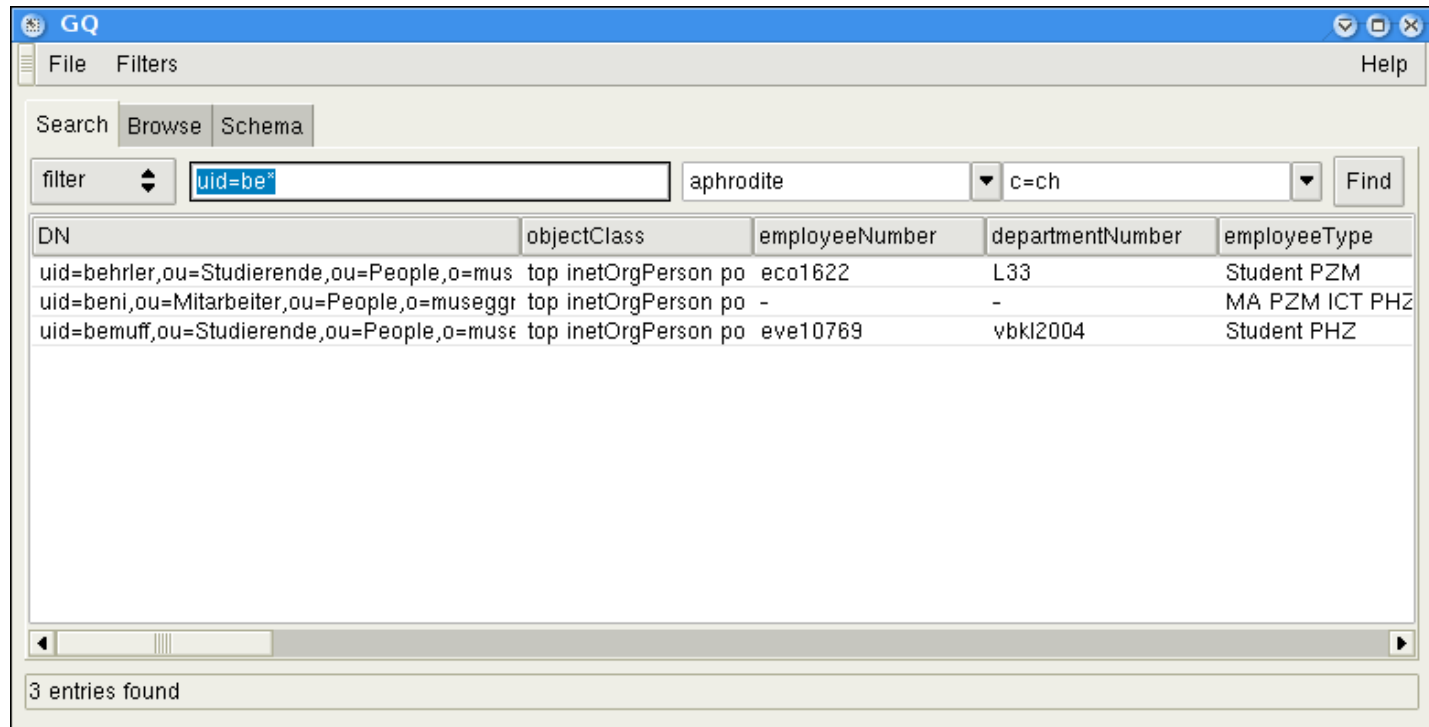
- Benutzer
- Gruppen
- Objektgruppen
- Abteilungen
- Systeme
- FAI
- Fax-Sperrlisten
- Telefon-Makros

# LDAP Account Manager LAM



The screenshot shows the LDAP Account Manager (LAM) web interface. At the top, there is a navigation bar with a "Spenden" link, a "Werkzeuge" link, and an "Abmelden" button. The main title "LDAP Account Manager" is prominently displayed. Below the title, there are navigation tabs for "Baumansicht", "Benutzer", "Gruppen", "Hosts", and "Samba-Domänen". The "Benutzer" tab is currently selected. On the left side, there is a sidebar with a "Bitte Seite wählen:" section containing buttons for "Allgemein", "Persönlich", "Unix", "Shadow", "Samba 3", and "Änderungen zurücksetzen". The "Allgemein" button is highlighted. The main content area shows the "Allgemein" configuration page for a user. It includes a "Suffix" dropdown menu with the value "ou=Mitarbeiter,ou=People,o=museggnet,c=ch", an "RDN-Bezeichner" dropdown menu with the value "uid", a "Profil laden" dropdown menu with the value "default" and a "Profil laden" button, and an "Account ändern" button. Each input field has a help icon (question mark) to its right.

gq



The screenshot shows the GQ LDAP client interface. The search filter is set to "uid=be\*", the search scope is "aphrodite", and the search base is "c=ch". The search results are displayed in a table with the following columns: DN, objectClass, employeeNumber, departmentNumber, and employeeType.

DN	objectClass	employeeNumber	departmentNumber	employeeType
uid=behrler,ou=Studierende,ou=People,o=mus	top inetOrgPerson po	eco1622	L33	Student PZM
uid=beni,ou=Mitarbeiter,ou=People,o=museggr	top inetOrgPerson po	-	-	MA PZM ICT PHZ
uid=bemuff,ou=Studierende,ou=People,o=muse	top inetOrgPerson po	eve10769	vbkl2004	Student PHZ

3 entries found

# Benutzererfassung PHZ Luzern

**Noch kein GUI > Anpassungen wären nötig**

**Erzeugen von Benutzern über LDIF Import**

- Mass-User-Creation
- Accountblätter drucken via OpenOffice

**Mutieren von Benutzern via `gq` oder neu über**

**Webinterface**

- Datenabfrage
- Kennwortänderungen
- Druck von Accountblättern

# Zukünftige Projekte

**Verbesserung Benutzerverwaltung**

**Zusammenführung Studimail + MuseggNet**

**Mailversand bei Ereignissen direkt an User**

**User-Identifizierung bei Internetaccess**

# Weitere Features von Samba3

Roaming-Profiles, Logon-Skripte per User

Automatischer Passwortverfall (Kennwort beim ersten Login ändern)

Automatischer Kontoverfall

# Wichtigste Einschränkungen

## OpenLDAP

- keine Master-Master Replikation

## Samba <> Windows 200x Server

- keine Group Policy Objekte
- WINS Server wird benötigt

## Installation

- nicht „Point and Click“

# Fazit

**Samba / OpenLDAP bietet eine sehr flexible, skalierbare, performante und stabile Plattform für Windows und UNIX/Linux.**

**Transparent für Benutzer und Clients**

**Installation erfordert gewisses Fachwissen**

**Backup und Restore sehr einfach möglich**

**Flexibilität kann Schwierigkeiten bei der Kontoverwaltung bringen**

# Weiterführende Informationen

<http://www.samba.org>

<http://www.openldap.org>

The official Samba-3; Prentice Hall, 0-13-145355-6

Samba3 by Example; Prentice Hall, 0-13-147221-6

Samba3 – Das offizielle Handbuch; Addison-Wesley, 3-8273-2152-2

Using Samba; O'Reilly, 2nd Edition, 0-596-00256-4

<http://www.idealx.org/prj/samba/smbldap-howto.en.html> z.Z. offline

LDAP System Administration; O'Reilly, 1-56592-491-6

LDAP/OpenLDAP; dpunkt.verlag, 3-89864-217-8

# Fragen?

PHZ Luzern - ICT  
Beni Schoedler  
[beni.schoedler@phz.ch](mailto:beni.schoedler@phz.ch)

Herzlichen Dank für Ihr Interesse  
und Ihre Aufmerksamkeit!