Verzeichnisbasiertes Benutzer- und Systemmanagement mit LDAP und Gosa

Dipl.-Inform. Holger Burbach
GONICUS GmbH
Arnsberg/Bonn

http://www.GONICUS.de
info@GONICUS.de

Agenda

- Über GONICUS
- Einführung in LDAP
- Integrationsmöglichkeiten
- Administrations-Front-Ends

GONICUS* GmbH

- Unabhängiger Open-Source-Dienstleister
- Langjährige Erfahrung mit LINUX auf dem Desktop
- Spezialist in Migration und Integration von LINUX in heterogenen Umgebungen
- Consulting, Implementation, Support und Training

*Königspinguin: (lat.) Aptenodytes-Pata**gonicus**

GONICUS GmbH

- Hauptsitz in Arnsberg
  (Niederlassungen in Berlin und Bonn)
- 15 Mitarbeiter
- Technisches und betriebswirtschaftliches Know-how
- Internationale Projekterfahrung*

*unter anderem: USA, China, Italien und Frankreich

Kurze Einführung in LDAP

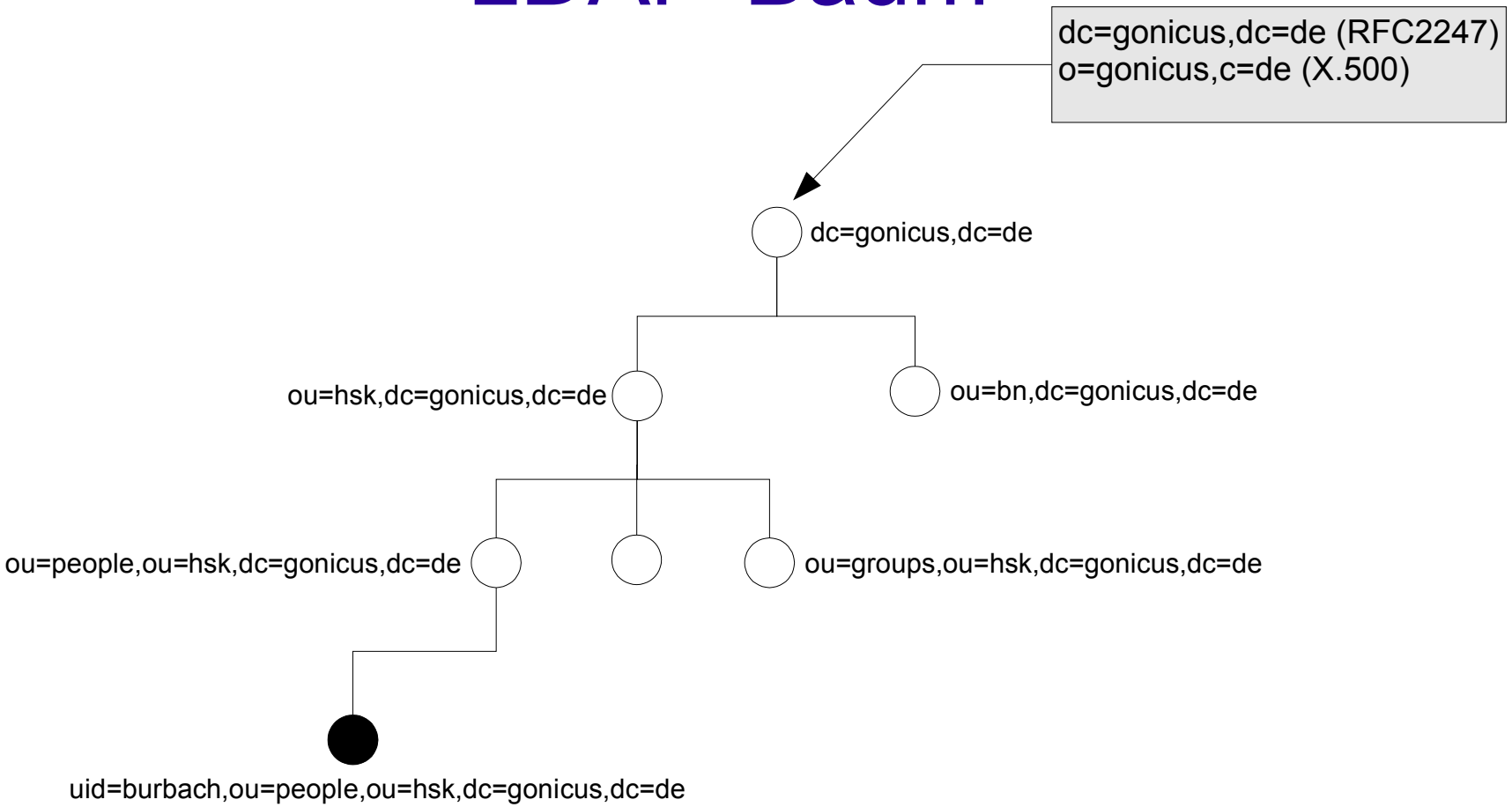
Was ist LDAP?

- plattformunabhängiges Protokoll zwecks Kommunikation mit einem LDAP-Server
- Abkömmling des X.500 OSI Directory Access Protocol

Was ist ein Verzeichnis?

- ein Verzeichnis ist eine hierarchische Sammlung von Objekten und deren Attributen.
- es ist keine Datenbank, denn Objekte können verschiedene und unterschiedlich viele Attribute besitzen.

LDAP-Baum



LDAP-Objekte und ihre Attribute

dn: uid=burbach,ou=people,dc=gonicus,dc=de ← **Distinguished Name (dn)**
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: account
objectClass: posixAccount
objectClass: top
uid: burbach
cn: Holger Burbach
givenName: Holger
sn: Burbach
mail: holger.burbach@gonicus.de
userPassword:: efksaodf223KDwekwdpsowwd
loginShell: /bin/bash
uidNumber: 500
gidNumber: 100
homeDirectory: /home/burbach
gecos: Holger Burbach

Objektklassen

Attribute

Werte

LDAP Schemata

OID

Name (Alias für OID)

```
objectclass ( 2.5.6.6 NAME 'person' SUP top
        MUST ( sn $ cn )
        MAY ( userPassword $ telephoneNumber $ seeAlso $ description ) )
```

Pflicht-Attribute

Erlaubte bzw. optionale Attribute

```
attributetype ( 2.5.4.41 NAME 'sn'
        EQUALITY caseIgnoreMatch
        SUBSTR caseIgnoreSubstringsMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{32768} )

attributetype ( 2.5.4.20 NAME 'telephoneNumber'
        EQUALITY telephoneNumberMatch
        SUBSTR telephoneNumberSubstringsMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.50{32} )
```

LDAP-Integration

Beispiele für Integrations-Möglichkeiten

- Personendaten
- Benutzer- und Gruppen-Accounts (Posix)
- Windows-Accounts (Samba 2 + 3)
- Mail-Accounts (Postfix + Cyrus)

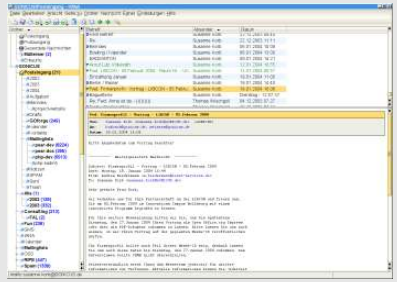
Personendaten

Personendaten:

- sn
- cn
- department
- Telefon-Nummer
- Fax-Nummer
- Adressen
- etc.

Adressbücher

- Mozilla, kmail



LDIF-Export

- IVBB X.500

Posix-Benutzer- und Gruppenaccounts

posixAccount:
- cn
- uid
- uidNumber
- gidNumber
- homeDirectory
- userPassword
- loginShell
- gecos
- description

posixGroup:
- cn
- gidNumber
- memberUid

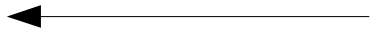
PAM,
libnssldap

Benutzer-authentifizierung auf UNIX-Systemen
- **/etc/pam.d/***
- **/etc/libnss-ldap.conf**

Windows-Accounts

sambaAccount:

- uid
- uidNumber
- lmPasswort
- ntPasswort
- homeDrive
- profilePath
- rid
- primaryGroupID
- ...



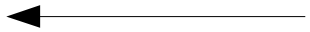
Emulieren eines PDC für Windows-Systeme durch Samba-Server mit LDAP-Anbindung

samba

www.samba.org

Mail-Accounts

mailAccount:
- mail
- mailAlternateAddress
- vMailBox
- mailHost
- mailTarget



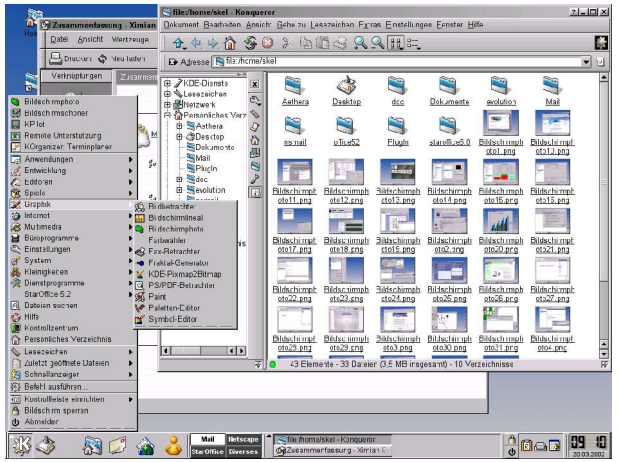
Postfix
- SMTP
- SpamAssassin

Cyrus IMAP
- IMAP, POP3

LINUX ThinClients

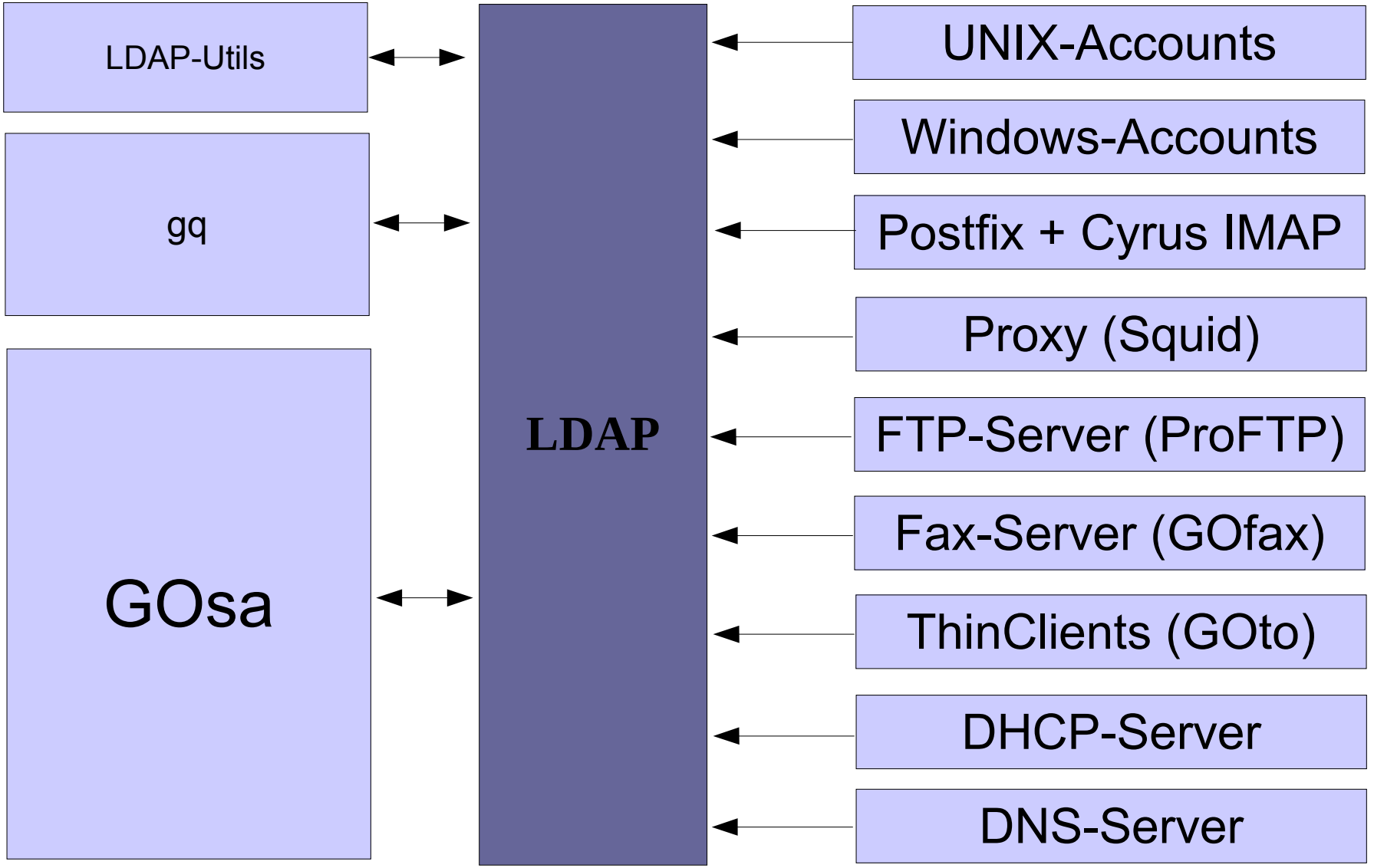
GOto*-Konzept

- Booten des Linux-Kernels per PXE / TFTP
- Betriebssystem (/) via NFS
- Konfiguration via LDAP / GOsa*
- Unterstützung lokaler Peripherie (Drucker, Scanner, Digitale Kameras, etc.)
- X-Window-Login auf OTS-Cluster mit Load-Balancing
- Geringe Hardware-Anforderungen (z.B. Siemens Netterms: P166, 64MB)



* GOto und GOsa sind Freie Software von GONICUS
http://oss.gonicus.de

Integrations- und Administrationsmöglichkeiten

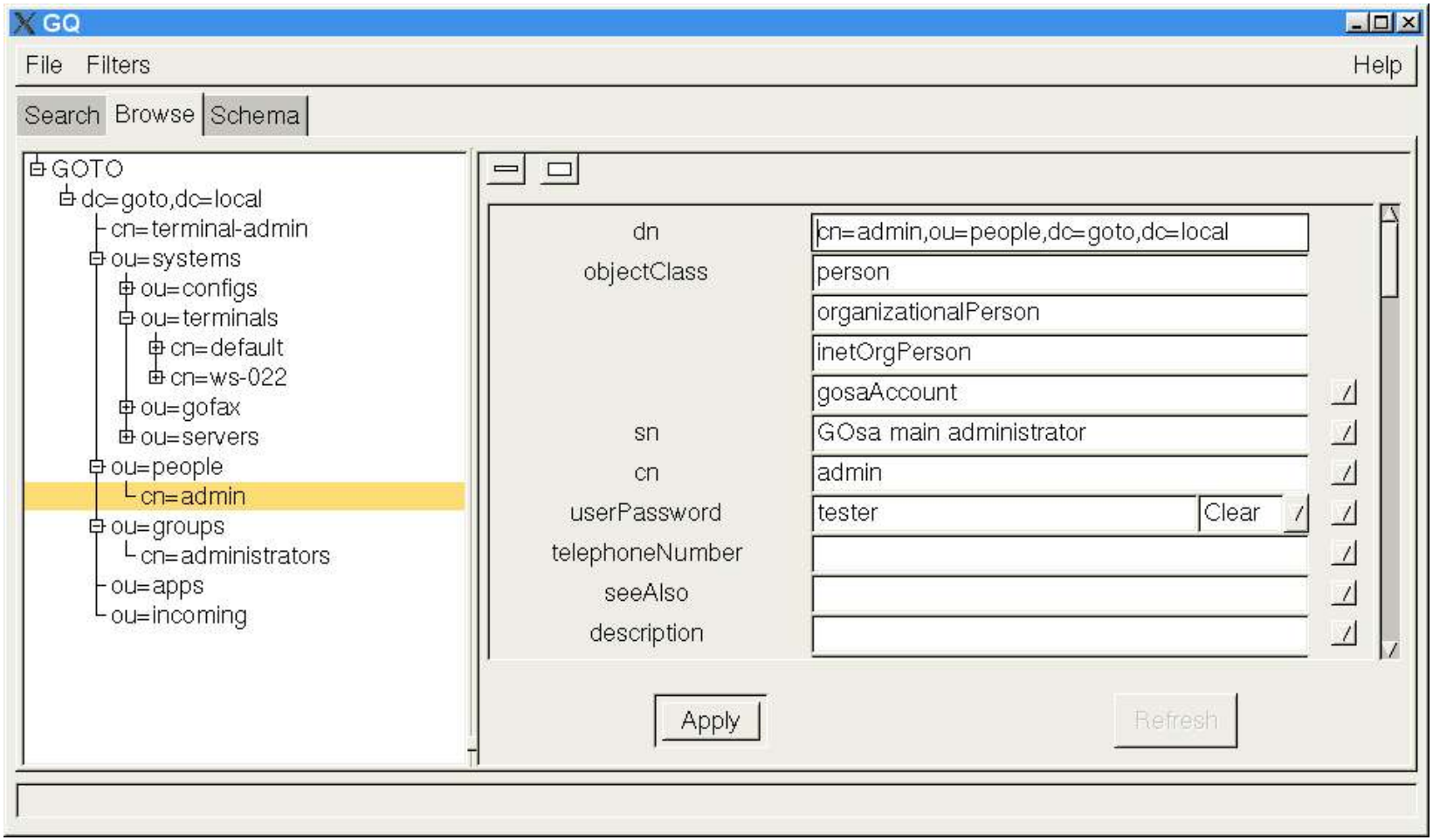


Administrationsmöglichkeit: LDAP-Utils

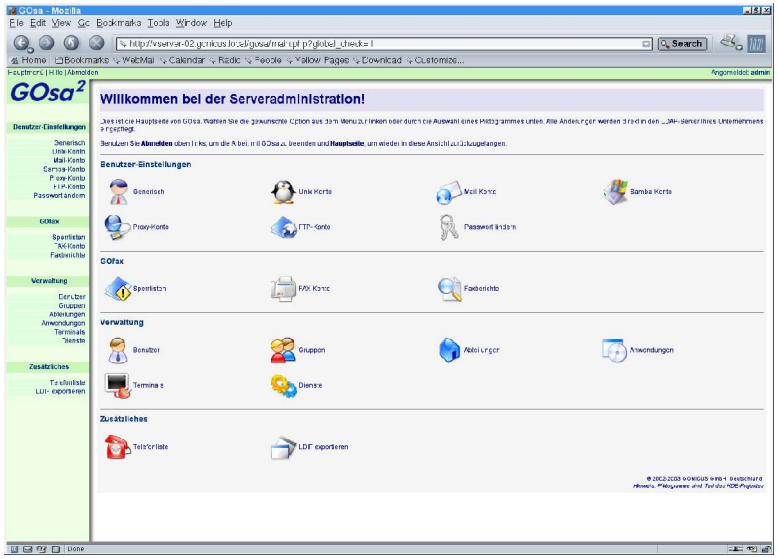

```
# ldapsearch -x -h localhost uid=burbach
dn: uid=burbach,ou=people,dc=gonicus,dc=de
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: account
objectClass: posixAccount
objectClass: top
uid: burbach
cn: Holger Burbach
givenName: Holger
sn: Burbach
mail: holger.burbach@gonicus.de
userPassword:: efksaodf223KDwekwdpsowwd
loginShell: /bin/bash
uidNumber: 500
gidNumber: 100
homeDirectory: /home/burbach
gecos: Holger Burbach
```

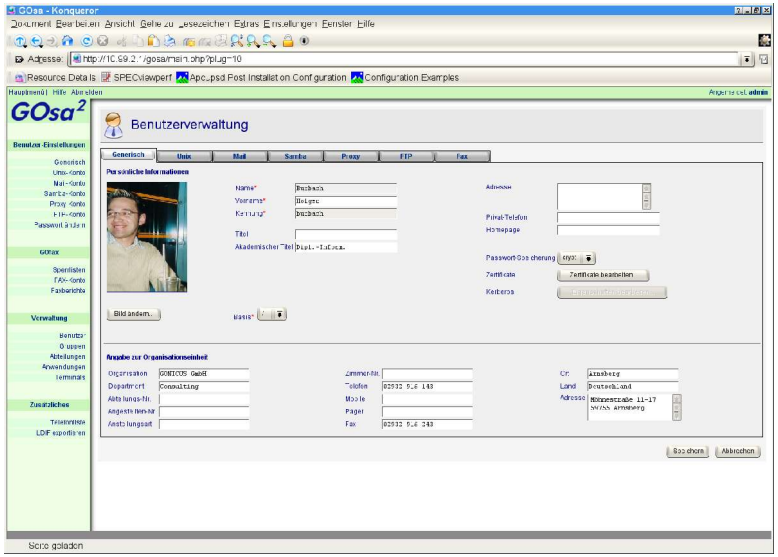
```
# ldapmodify -x -D“cn=ldapadmin,dc=gonicus,dc=de“ -W <<
EOF
dn: cn=Holger Burbach,ou=people,dc=gonicus,dc=de
changetype: modify
replace: userPassword
userPassword: secret
-
add: homePhone
homePhone: 0815-4711
-
delete: description
description: zu entfernen
-
EOF
```

Administrationsmöglichkeit: gq



Administrationsmöglichkeit: GOsa*





Administrations-Front-End GOsa*

- Komfortable Administration sämtlicher LDAP-Daten
- Implementiert in PHP
- Einfache Erweiterbarkeit
- Zuweisung von Administrationsrollen
- Internationalisiert (Englisch, Deutsch, Spanisch)

* GOsa ist Freie Software von GONICUS

http://oss.gonicus.de

GONICUS – Ein kompetenter Partner in Open-Source-Fragen für viele Unternehmen und Einrichtungen

SEVERIN
Henkel KG
IMMER EIN SICHERER HALT
Desch
Antriebstechnik
OBI
FAL
Bundesforschungsanstalt für Landwirtschaft
FerroTec
Stadtkrankenhaus Rüsselsheim
- HESSENKLINIK -
Nestlé
Good Food, Good Life
Fraport
Frankfurt Airport Services Worldwide
WAFFENSCHMIDT
Berndes
Made in Germany
Bundesministerium der Justiz
bremke hoerster
Bundesamt für Sicherheit in der Informationstechnik
Lufthansa
FREUNDE DER KUNSTHALLE
DENISON Hydraulics
Offset Druck Team
BASLER
HORST BASLER
dpa Deutsche Presse-Agentur GmbH