becom einfach. mehr. wissen.

Konsolidiertes Systemmanagement mit z/VM LDAP und GOsa²

24. VM/VSE IT-Leiter Kolloquium, Bad Wörishofen

26. November 2009, Dresden

Simon Fischer

Agenda

Motivation

- Ausgangssituation
- LDAP Grundlagen
- GOsa²

Motivation

becom einfach. mehr. wissen.

Motivation

„LDAP…. endlich! …

- LDAP Server für z/VM
- LDAP Client für z/VSE

… Und nun?“

- Erste Anwendungsbeispiele:
  - Zentrales Management der Linux-User
  - Authentifizierung der z/VSE User im z/VM LDAP bzw. OpenLDAP-Server (Mapping-File erforderlich)

„Der Anfang ist die Hälfte des Ganzen.“ Aristoteles

Agenda

- Motivation

Ausgangssituation

- LDAP Grundlagen
- GOsa²

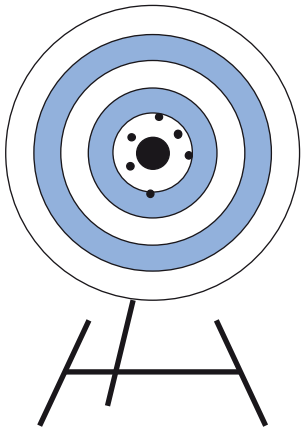
Ausgangssituation

becom einfach. mehr. wissen.

Eine Beispielfirma…

„Killbill Inc.“

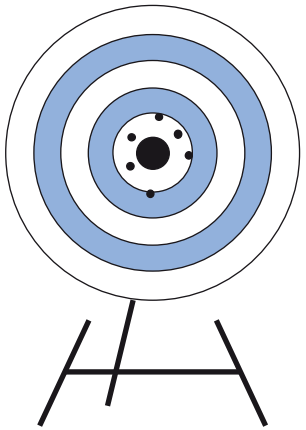
- Netzwerk: DNS/DHCP, Proxy
- Zentrale Authentifizierung und Autorisierung
- Windows und Linux Arbeitsplatzrechner
- Samba Datei- und Druckdienste
- Groupware/Adressbuch
- Kommunikation VoIP-Telefonie und Fax
- „Killbill Inc. Homepage“ -> Webserver



becom einfach. mehr. wissen.

Redundante Konfigurations- und Anwendungsdaten

- Netzwerk: DNS/DHCP, Proxy
  - Netzwerkstruktur
  - IP<->DNS Mapping
  - Authentifizierung
  - Zugriffsrechte
- Zentrale Authentifizierung und Autorisierung
  - Benutzeraccounts
  - Zugriffsrechte
  - Umgebungsspezifische Pflichtattribute
- Windows und Linux Workstations
  - Hardwareausstattung
  - Systemkonfiguration (IP-Adresse, etc.)
  - Softwareausstattung
- Datei- und Druckdienste (z.B. Samba)
  - Freigabe- bzw. Druckername
  - Konfigurationsattribute
  - Zugriffsrechte
- Groupware/Adressbuch
  - Personendaten (Name, Adresse, Telefonnummer, Email-Adressen)
  - Gruppenstrukturen
- Kommunikation: VoIP-Telefonie und Fax
  - Telefonnummer, Endgerätekennung
  - Endgeräteregistrierung, Zugriffsrechte
  - Email-Adressen für Fax-to-Mail-Mapping
- „Killbill Inc. Homepage“ -> Webserver
  - Zugriffsrechte für geschützte Bereiche



becom einfach. mehr. wissen.

Problemstellung

Die Herausforderung:

- Wie können die unterschiedlichen Systeme und Services verwaltet werden ?
- Wie kann Komplexität minimiert werden ?
- Wie können multiple Speicherorte für Daten (Email-Adresse, Telefonnummer, Passwörter etc.) vermieden werden ?
- Wie kann Self-Service und Delegation für Nutzer abgebildet werden?

Ein Lösungsansatz:

- Erstellung und Nutzung eines zentralen unternehmensweiten Informationsspeichers!

Pragmatische Variation:

- Bestmögliche Integration der unternehmensweiten Datenquellen und Nutzung eines zentralen Managementwerkzeuges.

becom einfach. mehr. wissen.

Agenda

- Motivation
- Ausgangssituation

LDAP Grundlagen

- GOsa²

LDAP Grundlagen

becom einfach. mehr. wissen.

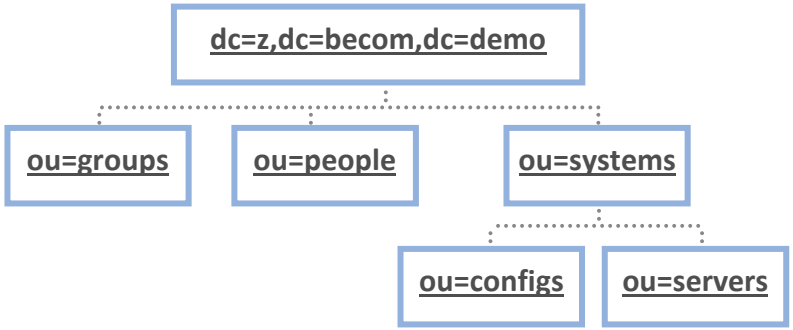
Exkurs: LDAP Grundlagen

LDAP: Lightweight Directory Access Protocol

- Ursprünglich „nur“ ein leichtgewichtiges Zugriffsprotokoll für Verzeichnisdienste (X.500)
- Verwendung des Begriffs als Kurzform für einen LDAP-kompatiblen Verzeichnis(dienst).

„LDAP“ Verzeichnisdienste – typische Basiseigenschaften

- Optimiert für lesenden Zugriff
- Datenorganisation in baumartiger Hierachie
- Objektorientiertes Datenmodell
- Verteilte Datenhaltung
  (unterschiedliche Server für Teilbäume)



„Bereitstellung eines Single Point of Administration“

- Keine integrierte „Single Sign On“ Funktionalität – nur „Single Point of Authentication“
- *aber:* i.d.R. sinnvolle Grundlage für „Single Sign On“ Technologien (Kerberos, etc.)

becom einfach. mehr. wissen.

Einsatzszenarien

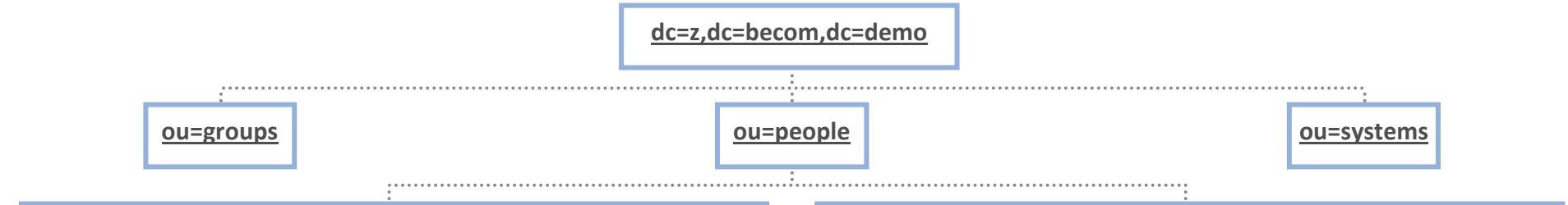
- Abbildung von Organisationsstrukturen und Netzwerken
  - Speicherung von Daten über Personen bzw. Benutzer und Personen-/Benutzergruppen
- Verwaltung von IT-Ressourcen
  - Server
  - Clients
  - Drucker
  - Dienste und Anwendungen
    - »z.B. Konfigurationsattribute
  - etc.
- „Single Point of Authentication“ 

Etablierte „Vorbilder“:

- Novell Netware (NDS/eDirectory)
- Microsoft Active Directory
- (IBM Lotus Domino/Notes)

becom einfach. mehr. wissen.

LDAP-Objekte



cn=Cajus Pollmeier	
ObjectClasses:	
top	gosaAccount
person	
organizationalPerson	
inetOrgPerson	
Attributes:	
cn	Cajus Pollmeier
uid	cajus
givenname	Cajus
sn	Pollmeier
telephonenumber	…….
l	München
st	Deutschland
userpassword	{crypt} ……
sambalmpassword	……..
sambantpassword	……..
u.s.w.	

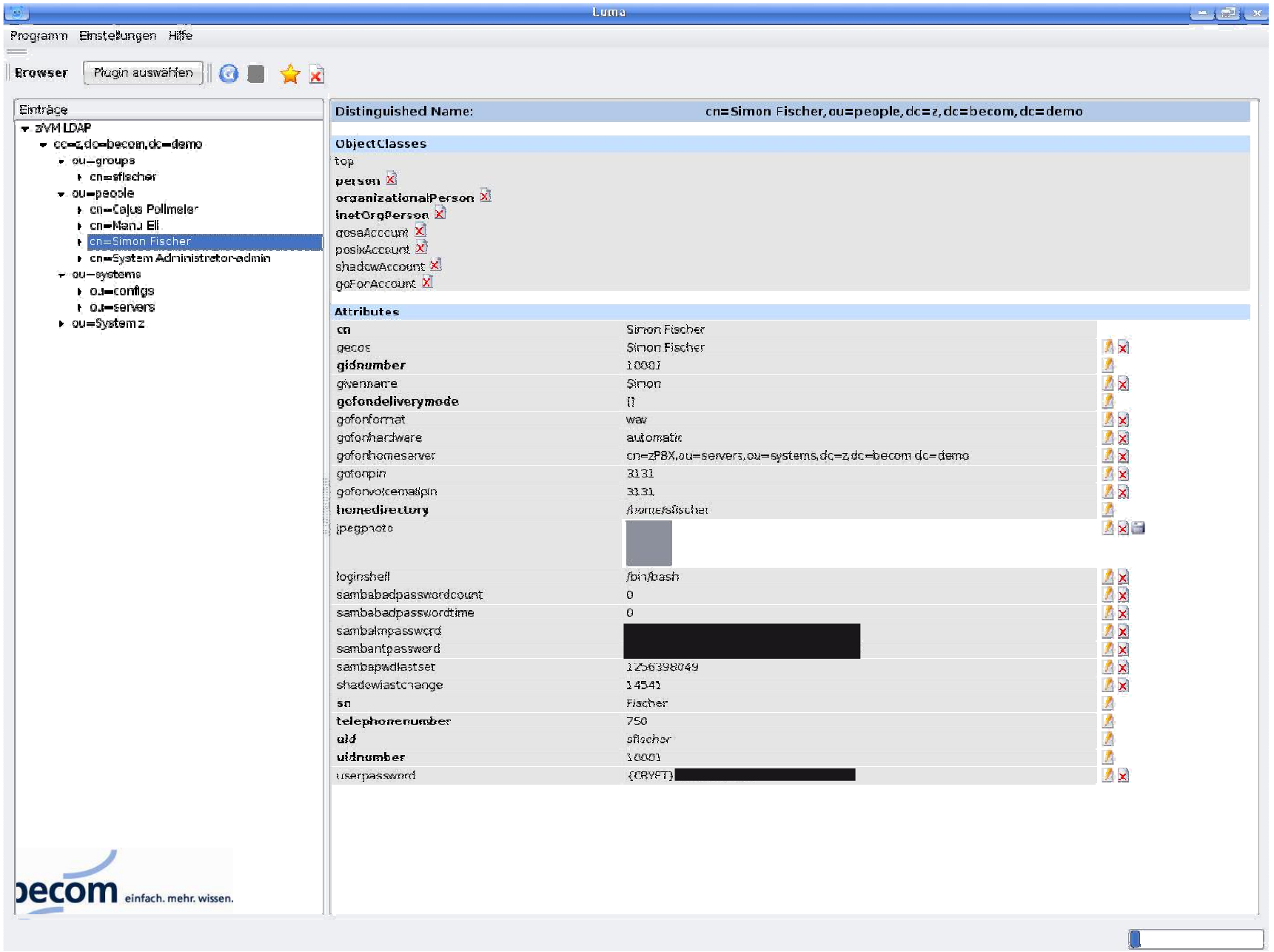
Distinguished Name: „cn=Cajus Pollmeier,ou=people,dc=z,dc=becom,dc=demo“

cn=Simon Fischer	
ObjectClasses:	
top	posixAccount
person	shadowAccount
organizationalPerson	gosaAccount
inetOrgPerson	goFonAccount
Attributes:	
cn	Simon Fischer
gecos:	Simon Fischer
uid	sfischer
gidnumber	10001
uidnumber	10001
givenname	Simon
sn	Fischer
homedirectory	/home/sfischer
loginshell	/bin/bash
telephonenumber	720
userpassword	{crypt} ……
sambalmpassword	……..
sambantpassword	……..
gofonformat	wav
gofonhomeserver	cn=zPBX,ou=servers,ou=systems,dc=z,…..
gofonpin	1313
u.s.w.	

Distinguished Name: „cn=Simon Fischer,ou=people,dc=z,dc=becom,dc=demo“

becom einfach. mehr. wissen.

LDAP Werkzeuge: Browser/Editor - LUMA



Agenda

- Motivation
  - Ausgangssituation
  - LDAP Grundlagen

GOsa²

becom einfach. mehr. wissen.

GOsa² - Hintergrund

Hintergrund:

- Linux (nsswitch) unterstützt eine zentrale Verwaltung von Benutzern in einem LDAP-Verzeichnisdienst
- Linux (pam) unterstützt eine zentrale Authentifizierung und Autorisierung durch einen LDAP-Verzeichnisdienst
- eine Reihe von weitverbreiteteten OpenSource Softwarelösungen unterstützt eine zentrale Verwaltung von Konfigurationsattributen oder Anwendungsdaten bzw. eine zentrale Authentifizierung und Autorisierung innerhalb eines LDAP-Verzeichnisdienstes
  - samba
  - postfix
  - squid
  - pureftpd
  - dns, dhcp
  - ...
- die Administration eines LDAP-Verzeichnisdienstes mittels CLI oder generischen LDAP-Tools ist ineffektiv!

Was ist GOsa?

- GOsa² bietet eine intuitive, rollenbasierte Administrationsoberfläche für die effiziente Verwaltung und Steuerung komplexer IT-Umgebungen.
- GOsa² beinhaltet im Kern eine zentrale Verwaltung von Personen, Gruppen und IT-Systemen und unterstützt eine Vielzahl von Anwendungsdiensten.
- Durch den modularen Aufbau können komfortabel weitere Funktionalitäten ergänzt werden.
- GOsa² ist „Free Software“

- Details:
  - Tool für die Verwaltung eines unternehmensorientierten Anwendungsszenarios eines LDAP Verzeichnisdienstes
  - Entwicklung in 2001 begonnen (GONICUS GmbH)
  - OpenSource, GPL
  - die Weiterentwicklung wird gefördert durch die GONICUS GmbH
  - Keine „Pro“-Version verfügbar, aber mit Enterprise-Features ausgestattet.
  - Web-Basierte PHP5-Applikation mit validem W3C und CSS
  - In 10 Sprachen lokalisiert

http://www.gosa-project.org/

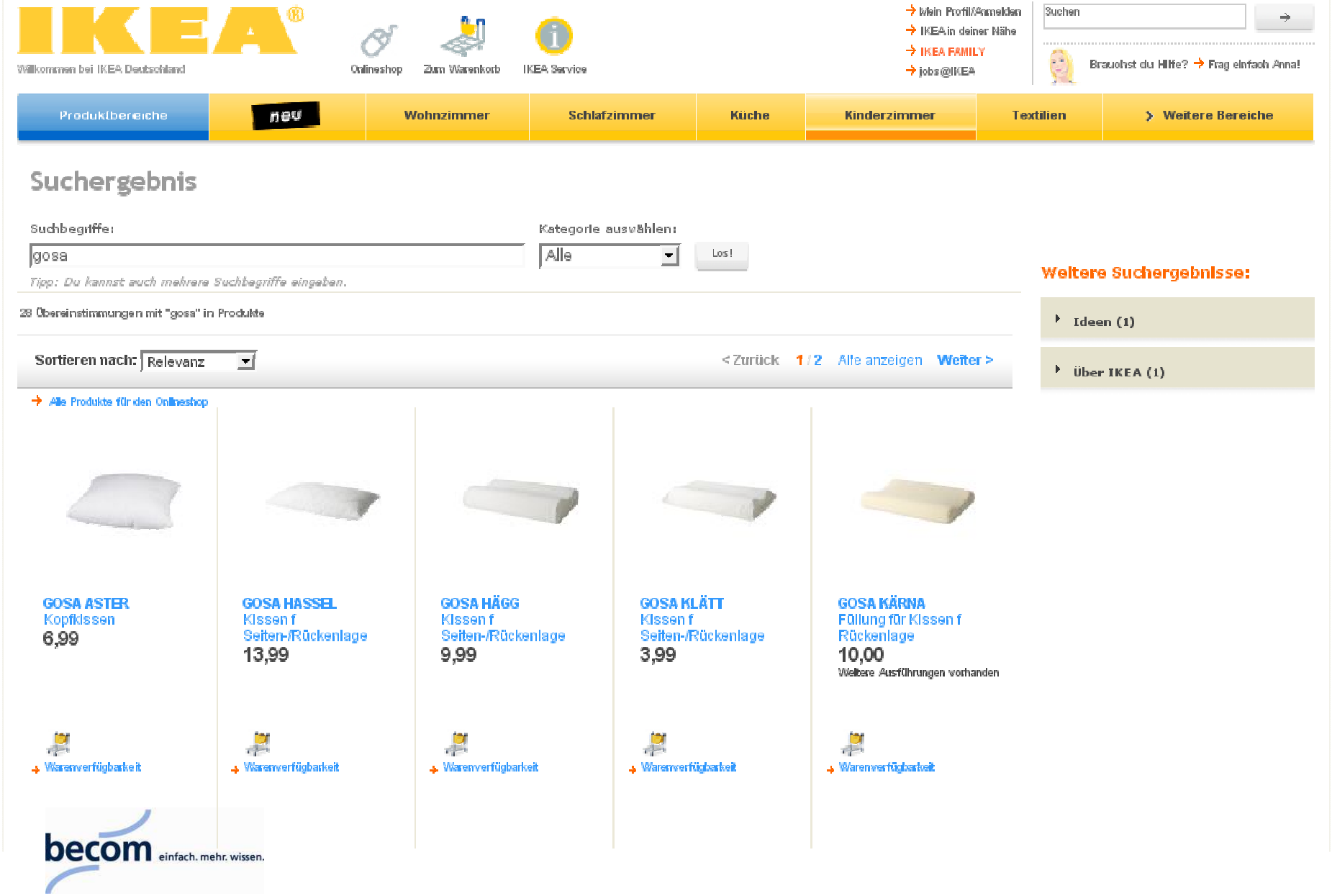
GONICUS

becom einfach. mehr. wissen.

Was soll GOsa nicht sein?

- YALE : Yet Another LDAP Editor, wie z.B.
  - PHPldapadmin
  - Web2LDAP
  - ldapvi
  - LUMA
  - GQ
  - Apache Directory Studio
- Keine Alternative zu Webmin
- *Und, ebenfalls wichtig.....*

GOsa² ist kein Kopfkissen !



GOsa² Start

becom einfach. mehr. wissen.

GOsa² Administrator Ansicht

becom einfach. mehr. wissen.

GOsa² Benutzeransicht – „User Self Service“

becom einfach. mehr. wissen.

GOsa² Basisfunktionalität

GOsa² - Personenbezogenes Systemdatenmanagement

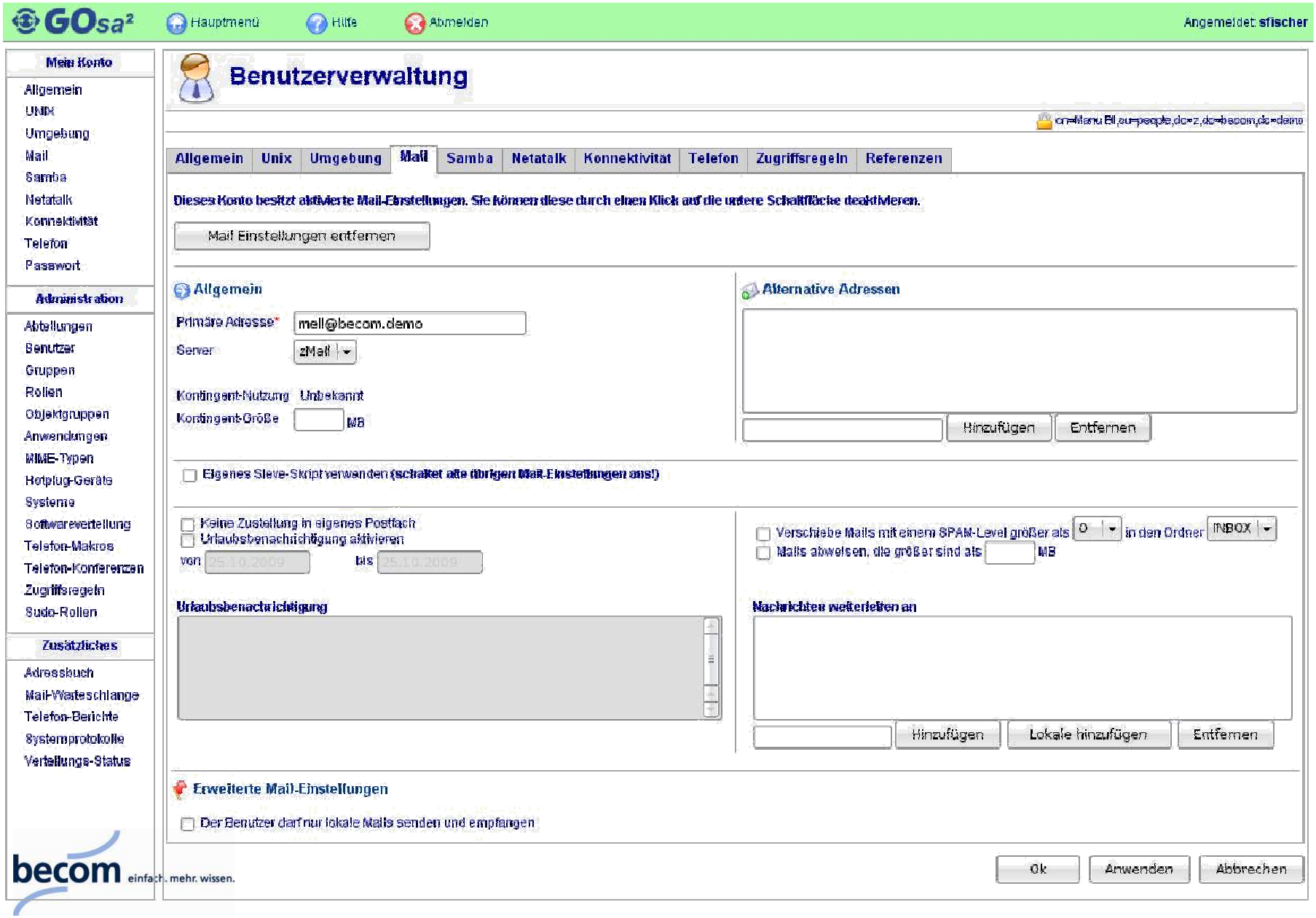
- Personenstammdaten
- Email-Einstellungen
- Unix Benutzeraccount (Posix)
- Samba Benutzeraccount
- Netatalk Benutzeraccount
- Konnektivität (Squid Proxy, pureFTPd)
- Telefon (Asterisk)
- [Arbeits-]Umgebung (GOto „Slean Clients“ – Desktop Virtualisierung)

becom einfach. mehr. wissen.

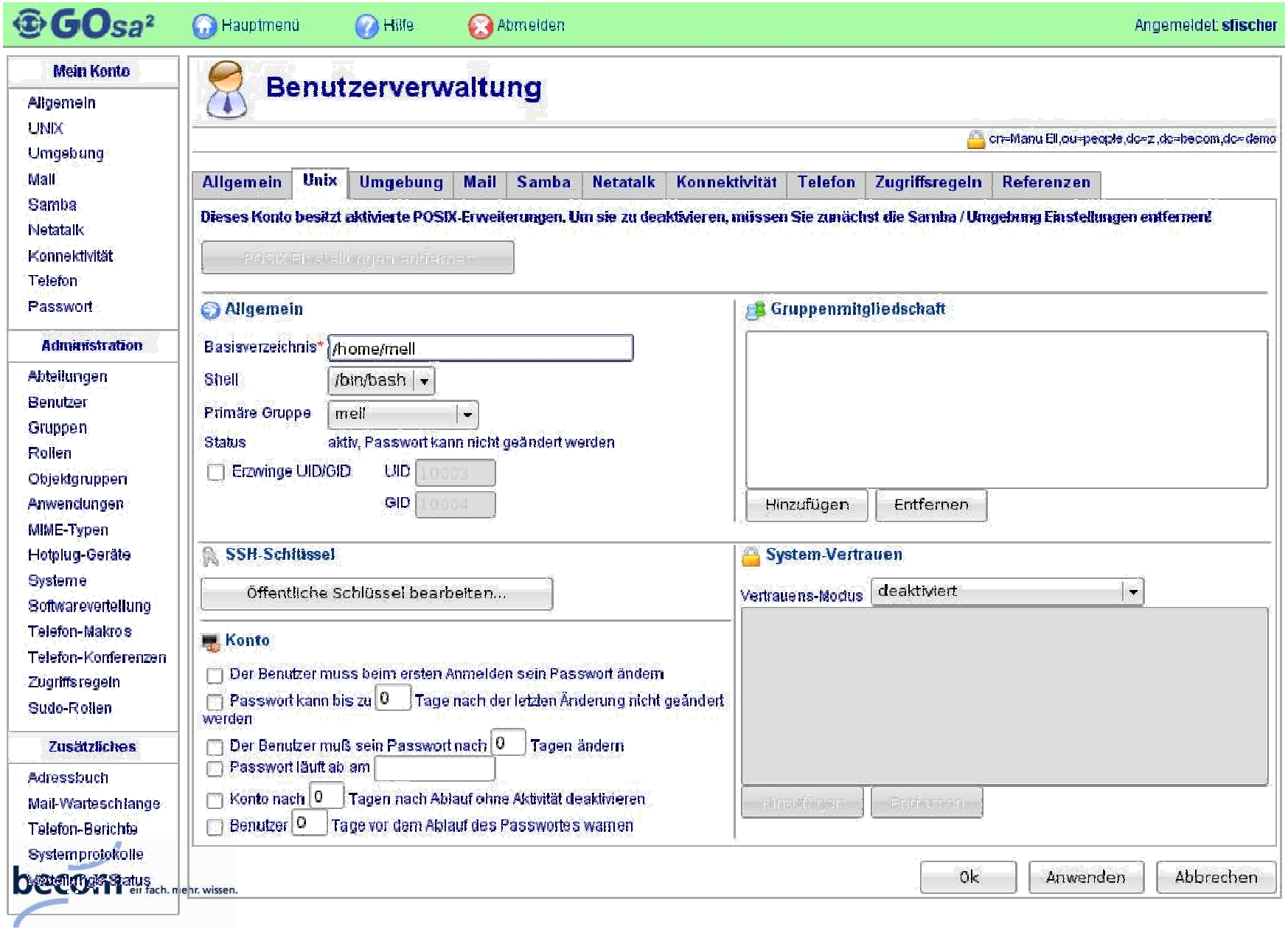
Stammdaten


GOsa²
Hauptmenü
Hilfe
Abmelden
Angemeldet: sfischer
Mein Konto
Allgemein
UNIX
Umgebung
Mail
Samba
Netatalk
Konnektivität
Telefon
Passwort
Administration
Abteilungen
Benutzer
Gruppen
Rollen
Objektgruppen
Anwendungen
MIME-Typen
Hotplug-Geräte
Systeme
Softwareverteilung
Telefon-Makros
Telefon-Konferenzen
Zugriffsregeln
Sudo-Rollen
Zusätzliches
Adressbuch
Mail-Warteschlange
Telefon-Berichte
Systemprotokolle
Benutzerverwaltung
cn=Manu Ell,ou=people,dc=z,dc=becom,dc=demo
Allgemein
Unix
Umgebung
Mail
Samba
Netatalk
Konnektivität
Telefon
Zugriffsregeln
Referenzen
Persönliche Informationen
Bild ändern...
Nachname*
Ell
Vorname*
Manu
Kennung*
mell
Titel
Akademischer Titel
Geburtsdatum
01.01.1981
Geschlecht
männlich
Bevorzugte Sprache
Deutsch (Deutsch)
Basis
/
Adresse
Privat-Telefon
Homepage
Passwort-Speicherung
crypt/standard-des
Zertifikate
Anmeldung beschränken
IP oder Netzwerk
Angabe zur Organisationseinheit
Organisation
Abteilung
Abteilungs-Nr.
Angestellten-Nr.
Anstellungsart
Zimmer-Nr.
0815
Telefon
0123443210
Mobiltelefon
0432112340
Pager
Fax
01234432109
Ort
Automatización
Land
Spanien
Adresse
Camino de la automatización 0815
Ok
Anwenden
Abbrechen

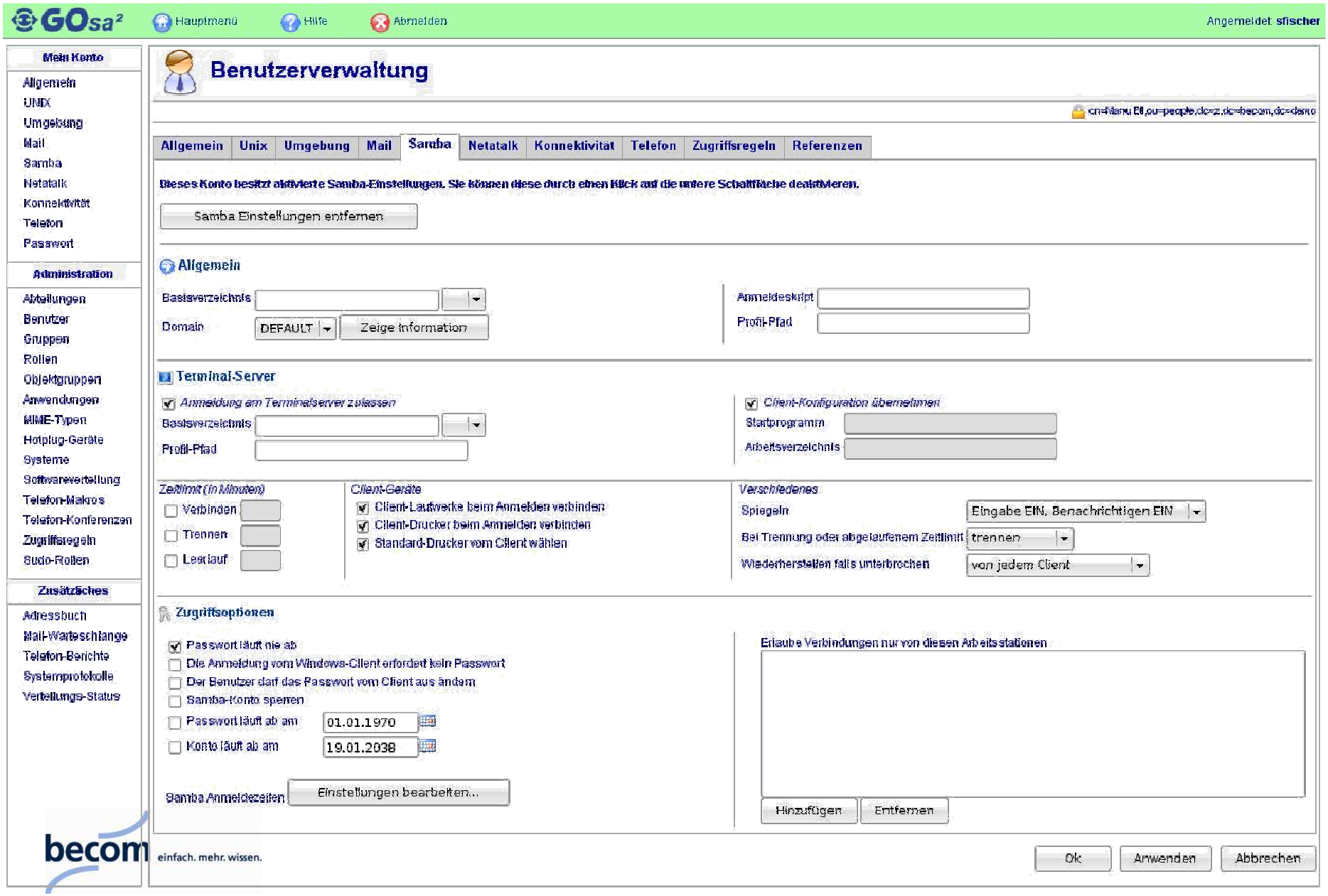
Email-Einstellungen



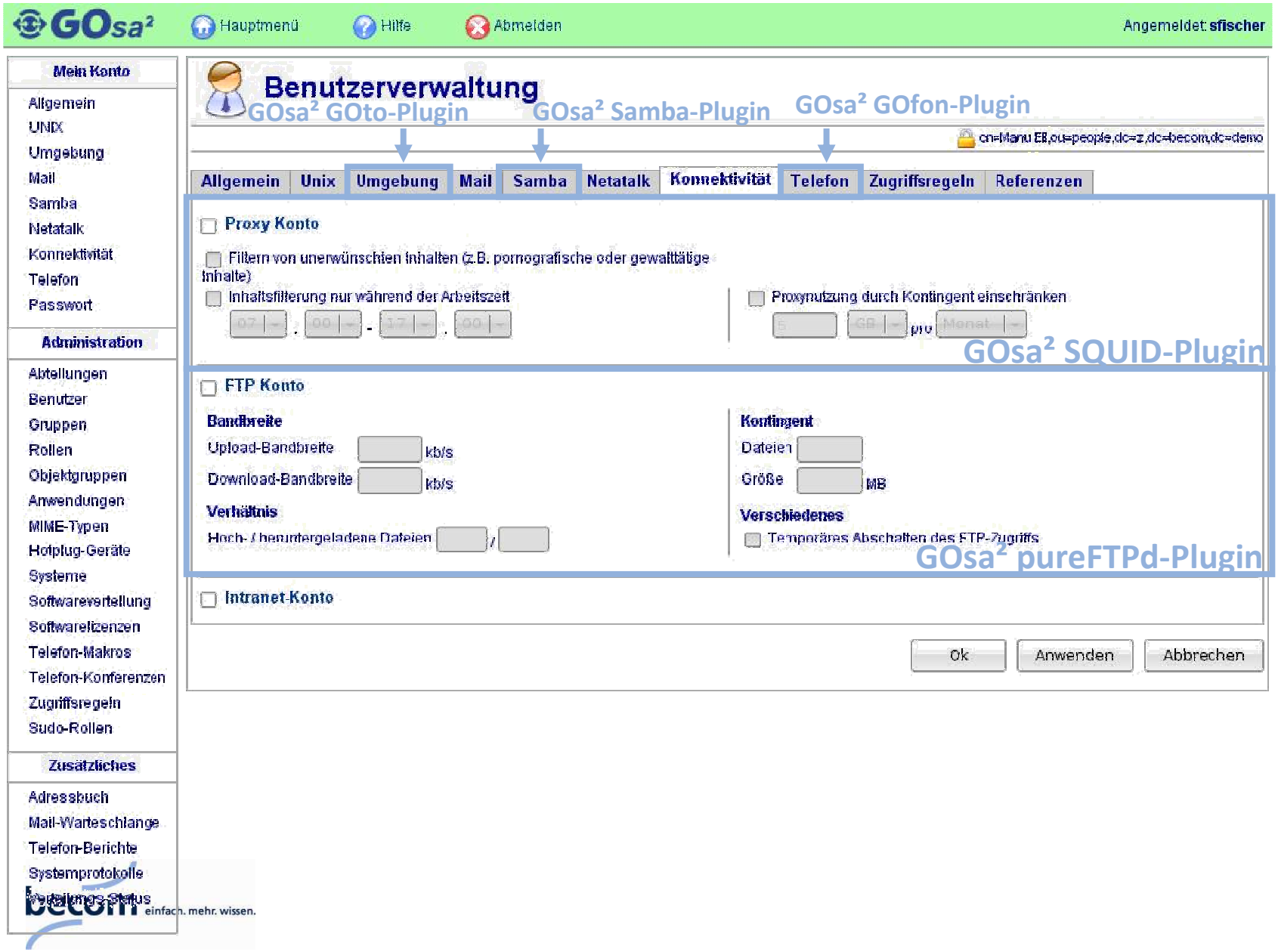
Unix Benutzeraccount (Posix)



Samba Benutzeraccount

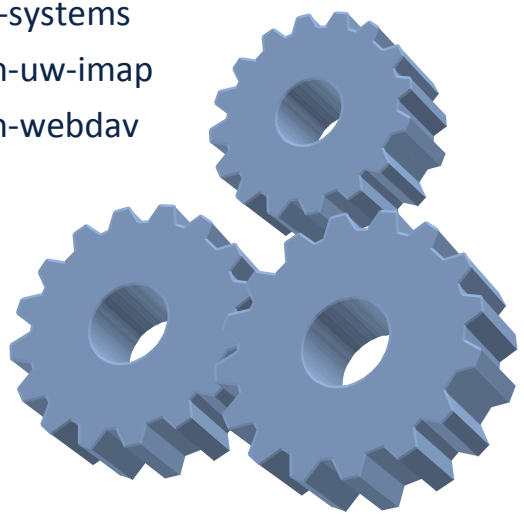


GOsa² Plugin Konzept



GOsa² Plugins (Debian Pakete)

- i gosa
- i gosa-plugin-addressbook
- i A gosa-plugin-connectivity
- i gosa-plugin-dhcp
- i gosa-plugin-dns
- i gosa-plugin-fai
- p gosa-plugin-gofax
- i gosa-plugin-gofon
- i A gosa-plugin-goto
- p gosa-plugin-kolab
- p gosa-plugin-ldapmanager
- i gosa-plugin-log
- i gosa-plugin-mail
- p gosa-plugin-mit-krb5
- p gosa-plugin-nagios
- i gosa-plugin-netatalk
- p gosa-plugin-opengroupware
- p gosa-plugin-openxchange
- i gosa-plugin-opsi
- p gosa-plugin-phpgw
- p gosa-plugin-phpscheduleit
- p gosa-plugin-pptp
- i gosa-plugin-pureftpd
- i gosa-plugin-rolemanagement
- i gosa-plugin-samba
- p gosa-plugin-scalix
- i gosa-plugin-squid
- i gosa-plugin-ssh
- i gosa-plugin-sudo
- i gosa-plugin-systems
- p gosa-plugin-uw-imap
- p gosa-plugin-webdav



becom einfach. mehr. wissen.

Die Grenzen von LDAP…..

Anwendungen und Dienste ohne LDAP-Unterstützung

- Konfiguration über Textdateien
- Speicherung von Anwendungs- und Konfigurationsdaten in relationalen Datenbanken

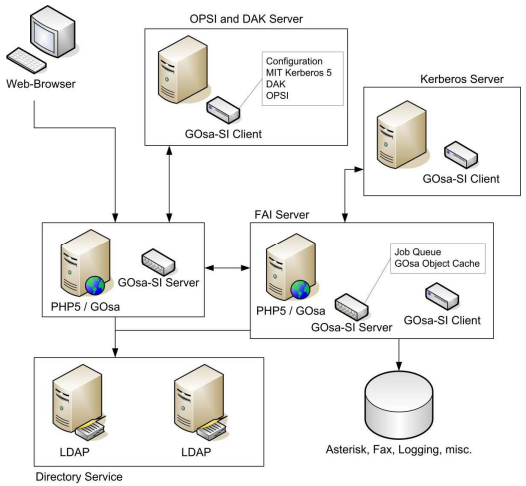
Integration von aktuellen „Bewegungs- bzw. Zustandsdaten“ in die zentrale GOsa² Managementoberfläche

- Systemmeldungen (syslog)
- Monitoring (nagios)

Integration von administrativen Workflows zur Reduktion von manuellen Administrationstätigkeiten

- Systemdeployment
- Softwareverteilung
- Patchverteilung

…der Anfang der GOsa² Systemarchitektur!



becom einfach. mehr. wissen.

Desktopmanagement für heterogene Umgebungen

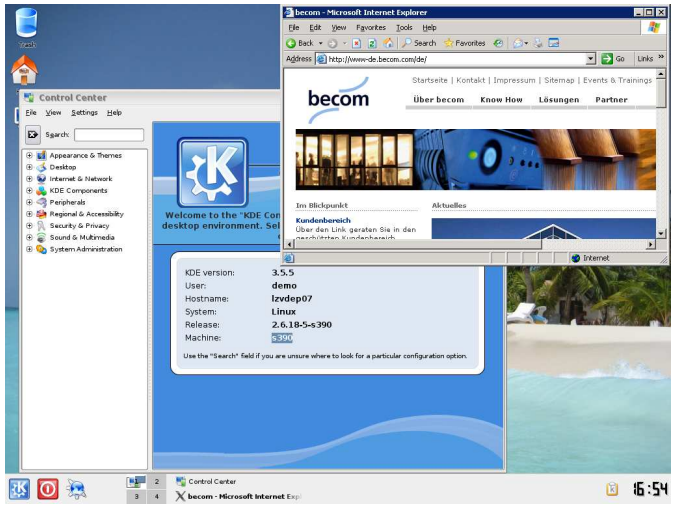
- Zentrales (kaskadierbares) Management von
  - Hardware („Thin“ & „Fat“)
  - linuxbasierten Virtual Desktops (GOto)
  - Linux „Fat Clients“ (Systemdeployment mit FAI)
  - Windows Desktops (OPSI)

- Release- & Patchmanagement (DAK)

- „historisch gewachsener“ Fokus auf Clientumgebungen
- äquivalent anwendbar für Serversysteme

LiMux
Die IT-Evolution

GONICUS



becom einfach. mehr. wissen.

LDAP-basiertes Systemverwaltungskonzept

Beispielhafter Prozess bei einem Systemneustart:

- PXE Boot einer „Spezialumgebung“ für initialen Systemstart:
  - automatische Hardwareerkennung
  - Kontakt zum LDAP-Server
  - Auswerten eines vorhandenen Systemprofils oder alternativ Neuregistrierung des Systems und Anstoßen eines Freigabeprozesses

- Ausführung der systemspezifischen Autokonfiguration auf Basis des Systemprofils:
  - mögliche Alternativen:
    - Netzwerkboot eines ThinClient-OS inklusive Remote Desktop Konnektivität (Nutzung von Thin Clients oder Recycling von „alten“ PC‘s)
    - Automatische lokale Betriebssysteminstallation gemäß Profilbeschreibung
      - Linux: FAI
      - Windows: OPSI

Hardwareverwaltung im LDAP

```
dn: cn=lt-
0070609,ou=workstations,ou=systems,dc=test,dc=de
macAddress: 00:11:5b:09:5e:8c
gotoSysStatus: new-system
gotoSndModule: snd_intel8x0
gotoXResolution: 1280x1024
ghSoundAdapter: Silicon Integrated AC'97 Sound
Controller
ghCpuType: GenuineIntel / Intel(R) Celeron(R) CPU
2.60GHz - 2600.102
gotoXKbModel: pc104
ghGfxAdapter: Silicon Integrated SiS 660
ghMemSize: 483728
gotoXMouseType: explorerps/2
ghUsbSupport: true
gotoXHsync: 30-83
gotoXDriver: sis
gotoXVsync: 55-75
gotoXMonitor: Acer AL1721
gotoHardwareChecksum: tMAwQMcSSneq7/RWGf99rwcn: lt-
0070609
gotoNtpServer: ltm-04.test.de
gotoLdapServer: 1:lts-101.clients.test.de
gotoBootKernel: linux-image-2.6.26-1-686
FAIclass: ACER-F1 TEST-CLIENT :etch
FAIdebianMirror: http://lts-
101.clients.test.de/debian
gotoXColordepth: 8
gotoXKbLayout: de
gotoXKbVariant: nodeadkeys
gotoXMouseport: /dev/input/mice
goFonHardware: automatic
objectClass: GOhard
objectClass: top
objectClass: gotoWorkstation
objectClass: FAIobject
gotoLastUser: mwagenbr
ipHostNumber: 192.168.128.100
gotoMode: active
ghIdeDev: WDC WD400EB-11JEF0
ghNetNic: Realtek RTL-8139/8139C/8139C+
gotoModules: ac97_bus
gotoModules: ata_generic
gotoModules: aufs
gotoModules: dock
gotoModules: exportfs
gotoModules: fan
gotoModules: ide_core
.........
gotoModules: thermal
gotoModules: thermal_sys
gotoModules: wmi
FAIstate: localboot
```

becom einfach. mehr. wissen.

Roll-Out Techniken

- c(ustom)tftpd für flexible Bereitstellung von PXE Bootfiles -> werden dynamisch aus LDAP generiert
- Gosa-si daemon -> Kommunikationsinfrastruktur zwischen Verteil- und Subverteilservern sowie Clients
- Speicherung aller FAI-Attribute im LDAP

becom einfach. mehr. wissen.

Releaseverwaltung in GOsa²

- Verwendung von Codenamen für Releases
- RCs, Unterversionen möglich
- Realisiert mit Debian Repository 'dak'

becom einfach. mehr. wissen.

GOsa² 2.6 Features – LDAP-basiert & „extended“

- Verwaltung von Subtrees
- Organisatorische und inetOrg Personen
- POSIX Benutzer und Gruppen
- Trust accounts und sudo
- Samba 3
- Objektgruppen
- GOto und FAI
- ACLs und logging
- **NEU:** MIT Kerberos 5 (policies, accounts, keys)
- **NEU:** OPSI – Integration für Roll-Out von Windows-PCs
- DNS
- ISC DHCP
- Asterisk VoIP
- GOfax + Hylafax
- Kolab 2 / OpenXchange / OpenGroupware
- Postfix / Cyrus / Sieve Verwaltung

becom einfach. mehr. wissen.

Resümee: z/VM LDAP Server & GOsa²

Ein erster Proof of Concept war erfolgreich! (Vgl. Screenshots)

- notwendige Schema-Erweiterungen für GOsa² für z/VM LDAP als LDIF-Datei erhältlich (simon.fischer@becom.com bzw. evtl. demnächst unter http://www.gosa-project.org)

aber

- LDAP ist nicht gleich LDAP
- und IBM wär nicht IBM, wenn nicht ein paar Kleinigkeiten ein kostenloses „Gehirnjogging“ beinhalten würden.
- notwendige „Workarounds“ für GOsa² erhältlich (cajus.pollmeier@gonicus.de bzw. evtl. demnächst unter http://www.gosa-project.org)

ToDo:

- **Ideeisieren:**
  - gosa-plugin-zvm bzw. gosa-plugin-zvse ?

Anregungen jederzeit willkommen!

becom einfach. mehr. wissen.

Fragen?

becom einfach. mehr. wissen.

Wir sind für Sie da.

Heute.
Morgen.
Und in Zukunft.

becom einfach. mehr. wissen.

becom Informationssysteme GmbH

Simon Fischer
Advisory Consultant

becom Informationssysteme GmbH
Konrad-Zuse-Straße 14
58239 Schwerte

Tel +49. 23 04. 931-720
Fax +49. 23 04. 931-401
Mobil +49. 15 22. 251 57 52

simon.fischer@becom.com
http://www.becom.com

becom informationssysteme GmbH
Konrad-Zuse-Str. 14
58239 Schwerte

becom einfach. mehr. wissen.