

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



„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

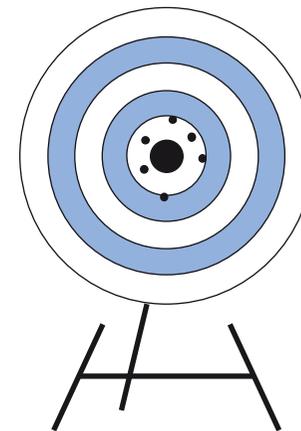
Ausgangssituation



Eine Beispielfirma...

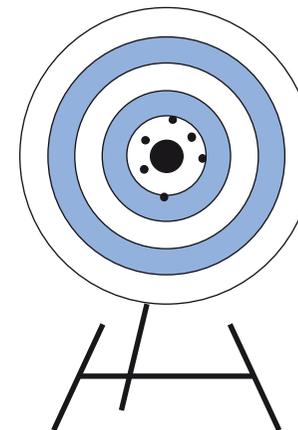
„Killbill Inc.“

- 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



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, Endgeräteerkennung
 - Endgeräteregistrierung, Zugriffsrechte
 - Email-Adressen für Fax-to-Mail-Mapping
- „Killbill Inc. Homepage“ -> Webserver
 - Zugriffsrechte für geschützte Bereiche



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.

Agenda

- Motivation
- Ausgangssituation

LDAP Grundlagen

- GOsa²

LDAP Grundlagen



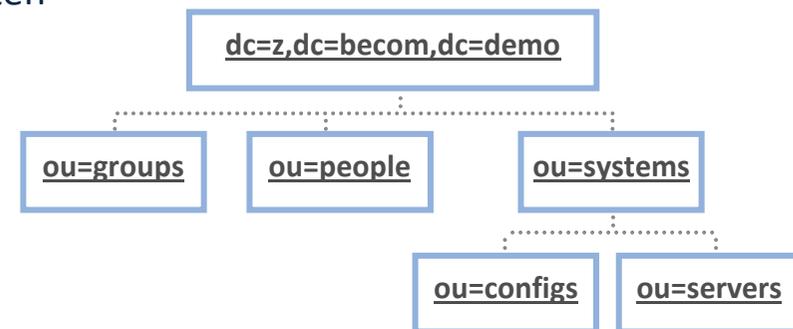
Exkurs: LDAP Grundlagen

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 Hierarchie
- 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.)

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.

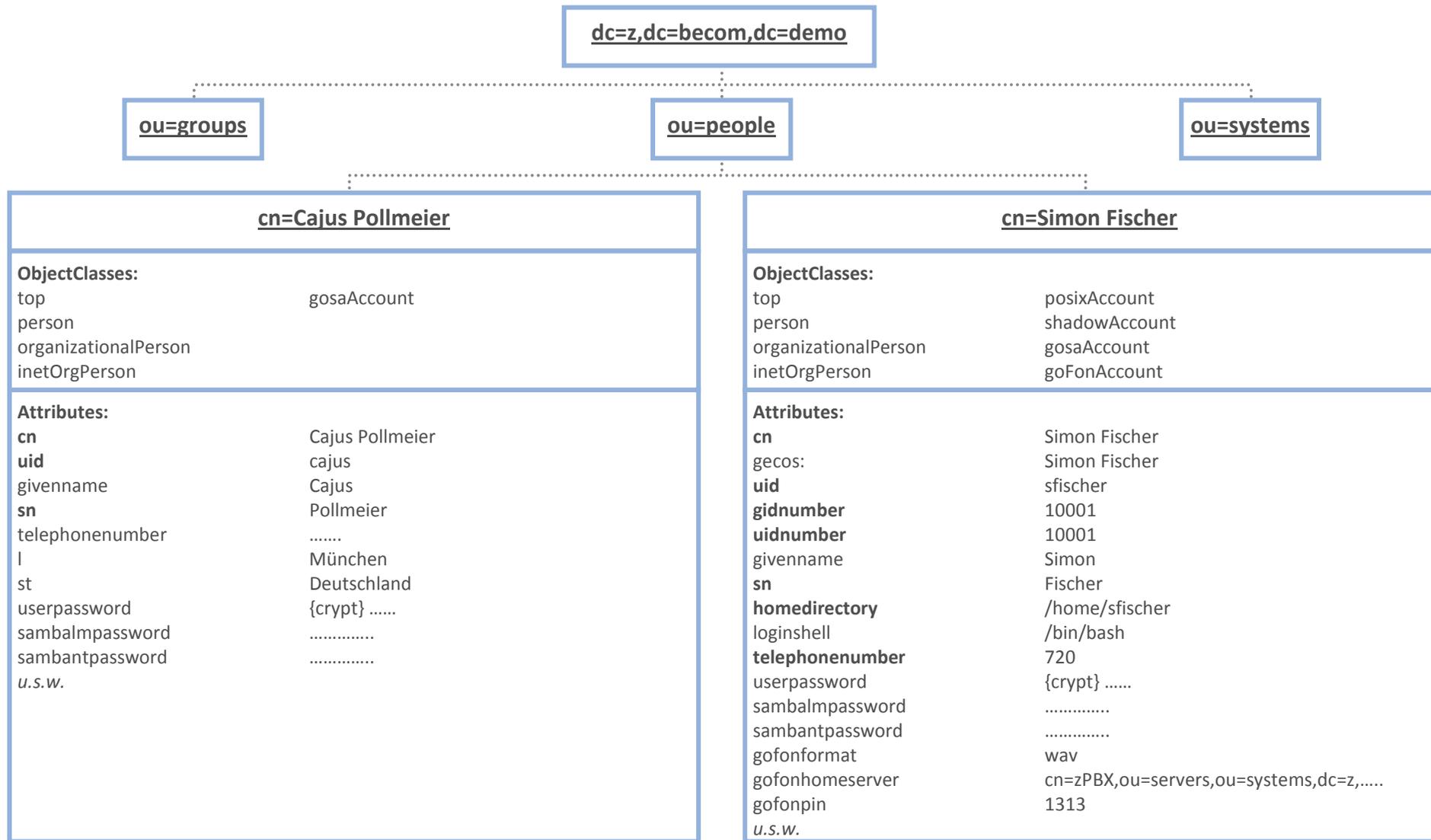
- „Single Point of Authentication“ 

Etablierte „Vorbilder“:

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



LDAP-Objekte



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

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

LDAP Werkzeuge: Browser/Editor - LUMA

The screenshot displays the LUMA LDAP browser/editor interface. The window title is "Luma". The menu bar includes "Programm", "Einstellungen", and "Hilfe". Below the menu bar is a "Browser" section with a "Plugin auswählen" button and several icons. The main interface is divided into three panes:

- Einträge (Entries):** A tree view showing the LDAP hierarchy. The selected entry is "cn=Simon Fischer" under "ou=people".
- Distinguished Name:** A text field containing "cn=Simon Fischer,ou=people,dc=z,dc=becom,dc=demo".
- ObjectClasses:** A list of object classes associated with the entry: top, person, organizationalPerson, inetOrgPerson, gosaAccount, posixAccount, shadowAccount, and goForAccount.
- Attributes:** A table listing various attributes and their values. Each attribute has a small icon to its right.

Attribute	Value
cn	Simon Fischer
gecos	Simon Fischer
gidnumber	10001
givenname	Simon
gofondeliverymode	()
gofonformat	wav
gofonhardware	automatic
gofonhomeserver	cn=zPBX,ou=servers,ou=systems,dc=z,dc=becom,dc=demo
gofonpin	3131
gofonvoicemailpin	3131
homedirectory	/home/sfischer
jpegphoto	[Redacted]
loginshell	/bin/bash
sambabadpasswordcount	0
sambabadpasswordtime	0
sambalmpassword	[Redacted]
sambantpassword	[Redacted]
sambapwlastset	1256398049
shadowlastchange	14541
sn	Fischer
telephonenumber	750
uid	sfischer
uidnumber	10001
userpassword	{CRYPT} [Redacted]

The Beacom logo is visible in the bottom left corner with the tagline "einfach. mehr. wissen."

Agenda

- Motivation
- Ausgangssituation
- LDAP Grundlagen

GOsa²

GOsa²



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 weitverbreiteten 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

Was soll GOsa nicht sein?

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



GOsa² ist kein Kopfkissen !



Willkommen bei IKEA Deutschland



Online shop



Zum Warenkorb



IKEA Service

→ Mein Profil/Anmelden

→ IKEA in deiner Nähe

→ IKEA FAMILY

→ jobs@IKEA

Suchen



Brauchst du Hilfe? → Frag einfach Anna!

Produktbereiche

NEU

Wohnzimmer

Schlafzimmer

Küche

Kinderzimmer

Textilien

→ Weitere Bereiche

Suchergebnis

Suchbegriffe:

gosa

Kategorie auswählen:

Alle

Los!

Tipp: Du kannst auch mehrere Suchbegriffe eingeben.

29 Übereinstimmungen mit "gosa" in Produkte

Sortieren nach: Relevanz

< Zurück 1 / 2 Alle anzeigen Weiter >

→ Alle Produkte für den Online shop



GOSA ASTER
Kopfkissen
6,99

→ Warenverfügbarkeit



GOSA HASSEL
Kissen f
Seiten-/Rückenlage
13,99

→ Warenverfügbarkeit



GOSA HÄGG
Kissen f
Seiten-/Rückenlage
9,99

→ Warenverfügbarkeit



GOSA KLÄTT
Kissen f
Seiten-/Rückenlage
3,99

→ Warenverfügbarkeit



GOSA KÄRNA
Füllung für Kissen f
Rückenlage
10,00
Weitere Ausführungen vorhanden

→ Warenverfügbarkeit



Weitere Suchergebnisse:

▶ Ideen (1)

▶ über IKEA (1)

Anmeldefenster

Nutzen Sie Ihren Benutzernamen und Ihr Passwort, um sich an der Verwaltung des Standorts anzumelden.

Warnung: Die Sitzung ist nicht verschlüsselt!



GOsa² Administrator Ansicht

 [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-Eerichte
- Systemprotokolle
- Verteilungs-Status



Willkommen Simon Fischer!

Dies ist das GOsa Hauptmenü. Wählen Sie die gewünschte Option aus dem Menü links oder durch die Auswahl eines Piktogrammes unten. Alle Änderungen werden direkt in den LDAP-Server Ihres Unternehmens eingefügt.

Benutzen Sie 'Abmelden' oben links, um die Arbeit mit GOsa zu beenden und 'Hauptmenü', um wieder in diese Ansicht zurückzugelangen.

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-Eerichte	 Systemprotokolle	 Verteilungs-Status
--	--	--	--	--

© 2002-2009 Das GOsa Team, GOsa gosa.org

becom einfach. mehr. wissen.

GOsa² Benutzeransicht – „User Self Service“

 [Hauptmenü](#) [Hilfe](#) [Abmelden](#) Angemeldet: **manu**

Mein Konto

- Allgemein
- UNIX
- Umgebung
- Mail
- Samba
- Netatalk
- Telefon

Administration

- Benutzer

Zusätzliches

- Adressbuch

 **Willkommen Manu!!!**

Dies ist das GOsa Hauptmenü. Wählen Sie die gewünschte Option aus dem Menü links oder durch die Auswahl eines Piktogrammes unten. Alle Änderungen werden direkt in den LDAP-Server Ihres Unternehmens eingepflegt.

Benutzen Sie 'Abmelden' oben links, um die Arbeit mit GOsa zu beenden und 'Hauptmenü', um wieder in diese Ansicht zurückzugelangen.

Mein Konto

 Allgemein

 UNIX

 Umgebung

 Mail

 Samba

 Netatalk

 Telefon

Administration

 Benutzer

Zusätzliches

 Adressbuch

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)



Stammdaten



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

cr=Manu Eil,ou=people,dc=z.dc=becom,dc=demo

Allgemein | Unix | Umgebung | Mail | Samba | Netatalk | Konnektivität | Telefon | Zugriffsregeln | Referenzen

Persönliche Informationen



Bild ändern...

Nachname*
Vorname*
Kennung*
Titel
Akademischer Titel
Geburtsdatum
Geschlecht
Bevorzugte Sprache
Basis

Adresse
Privat-Telefon
Homepage
Passwort-Speicherung
Zertifikate
Anmeldung beschränken
IP oder Netzwerk + -

Angabe zur Organisationseinheit

Organisation
Abteilung
Abteilungs-Nr.
Angestellten-Nr.
Anstellungsart
Zimmer-Nr.
Telefon
Mobiltelefon
Pager
Fax

Ort
Land
Adresse

Ok

Anwenden

Abbrechen

Email-Einstellungen



Hauptmenü

Hilfe

Abmelden

Angemeldet: sfischer

Mein Konto

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

Administration

- Abteilungen
- Benutzer
- Gruppen
- Rollen
- Objektgruppen
- Anwendungen
- RIME-Typen
- Hotplug-Geräte
- Systeme
- Softwareverteilung
- Telefon-Makros
- Telefon-Konferenzen
- Zugriffsregeln
- Sudo-Rollen

Zusätzliches

- Adressbuch
- Mail-Warteschlange
- Telefon-Berichte
- Systemprotokolle
- Verteilungs-Status



Benutzerverwaltung

icon@konu.BI.cuppeople.de z, dc=becom, dc=demo

- Allgemein
- Unix
- Umgebung
- Mail**
- Samba
- Netatalk
- Konnektivität
- Telefon
- Zugriffsregeln
- Referenzen

Dieses Konto besitzt aktivierte Mail-Einstellungen. Sie können diese durch einen Klick auf die untere Schaltfläche deaktivieren.

Mail-Einstellungen entfernen

Allgemein

Primäre Adresse*

Server

Kontingent-Nutzung

Kontingent-Größe MB

Eigenes Sieve-Skript verwenden (schaltet alle übrigen Mail-Einstellungen aus!)

Keine Zustellung in eigenes Postfach

Urlaubsbenachrichtigung aktivieren

von bis

Urlaubsbenachrichtigung

Alternative Adressen

Hinzufügen

Entfernen

Verschiebe Mails mit einem SPAM-Level größer als in den Ordner

Mails ablehnen, die größer sind als MB

Nachrichten weiterleiten an

Hinzufügen

Lokale hinzufügen

Entfernen

Erweiterte Mail-Einstellungen

Der Benutzer darf nur lokale Mails senden und empfangen

Ok

Anwenden

Abbrechen

Unix Benutzeraccount (Posix)

  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

cr=Manu Ell,ou=people,dc=z,dc=becom,dc=demo

Allgemein Unix Umgebung Mail Samba Netatalk Konnektivität Telefon Zugriffsregeln Referenzen

Dieses Konto besitzt aktivierte POSIX-Erweiterungen. Um sie zu deaktivieren, müssen Sie zunächst die Samba / Umgebung Einstellungen entfernen!

POSIX-Einstellungen entfernen

Allgemein

Basisverzeichnis*

Shell

Primäre Gruppe

Status aktiv, Passwort kann nicht geändert werden

Erzwingen UID/GID UID GID

Gruppenmitgliedschaft

HinzufügenEntfernen

SSH-Schlüssel

Öffentliche Schlüssel bearbeiten...

System-Vertrauen

Vertrauens-Modus

HinzufügenEntfernen

Konto

- Der Benutzer muss beim ersten Anmelden sein Passwort ändern
- Passwort kann bis zu Tage nach der letzten Änderung nicht geändert werden
- Der Benutzer muß sein Passwort nach Tagen ändern
- Passwort läuft ab am
- Konto nach Tagen nach Ablauf ohne Aktivität deaktivieren
- Benutzer Tage vor dem Ablauf des Passwortes warnen

OkAnwendenAbbrechen

 betriebl. Status
ein Fach, mehr Wissen.

Samba Benutzeraccount



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
Softwareverwaltung
Telefon-Makros
Telefon-Konferenzen
Zugriffsregeln
Sudo-Rollen

Zusätzliches

Adressbuch
Mail-Warteschlange
Telefon-Berichte
Systemprotokolle
Verteilungs-Status



einfach. mehr. wissen.



Benutzerverwaltung

cn=filianu.EB,ou=people,dcsz,dc=hscom,dc=danc

Allgemein Unix Umgebung Mail **Samba** Netatalk Konnektivität Telefon Zugriffsregeln Referenzen

Dieses Konto besitzt aktivierte Samba-Einstellungen. Sie können diese durch einen Klick auf die untere Schaltfläche deaktivieren.

Samba Einstellungen entfernen

Allgemein

Basisverzeichnis
Domain

Anmeldeskript
Profil-Pfad

Terminal-Server

Anmeldung am Terminalserver zulassen

Client-Konfiguration übernehmen

Basisverzeichnis
Profil-Pfad

Startprogramm
Arbeitsverzeichnis

Zeitlimit (in Minuten)

Verbinden
 Trennen
 Leerlauf

Client-Geräte

Client-Laufwerke beim Anmelden verbinden
 Client-Drucker beim Anmelden verbinden
 Standard-Drucker vom Client wählen

Verschiedenes

Spiegeln
Bei Trennung oder abgelaufenem Zeitlimit
Wiederherstellen falls unterbrochen

Zugriffsoptionen

Passwort läuft nie ab
 Die Anmeldung vom Windows-Client erfordert kein Passwort
 Der Benutzer darf das Passwort vom Client aus ändern
 Samba-Konto sperren
 Passwort läuft ab am
 Konto läuft ab am

Samba Anmeldezeiten

Erlaube Verbindungen nur von diesen Arbeitsstationen:

GOsa² Plugin Konzept

The screenshot displays the GOsa² web interface for user management. At the top, there is a navigation bar with the GOsa² logo, a main menu (Hauptmenü), help (Hilfe), and logout (Abmelden) options. The user is logged in as 'sfischer'. The main content area is titled 'Benutzerverwaltung' and shows a tree view of plugins: GOsa² GOto-Plugin, GOsa² Samba-Plugin, and GOsa² GOfon-Plugin. Below this, there are tabs for 'Allgemein', 'Unix', 'Umgebung', 'Mail', 'Samba', 'Netatalk', 'Konnektivität', 'Telefon', 'Zugriffsregeln', and 'Referenzen'. The 'Umgebung' tab is active, showing settings for 'Proxy Konto', 'FTP Konto', and 'Intranet-Konto'. The 'Proxy Konto' section includes options for content filtering and proxy usage. The 'FTP Konto' section includes settings for bandwidth, ratio, and quotas. The 'Intranet-Konto' section is currently empty. At the bottom right, there are 'Ok', 'Anwenden', and 'Abbrechen' buttons. A blue box highlights the 'Umgebung' tab and its associated settings, with a label 'GOsa² SQUID-Plugin'. Another blue box highlights the 'FTP Konto' section, with a label 'GOsa² pureFTPd-Plugin'. The left sidebar contains a navigation menu with categories like 'Mein Konto', 'Administration', and 'Zusätzliches'. The bottom left corner features the 'becom' logo and the tagline 'einfach. mehr. wissen.'

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-openexchange
- 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



Die Grenzen von LDAP.....

Anwendungen und Dienste ohne LDAP-Unterstützung

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

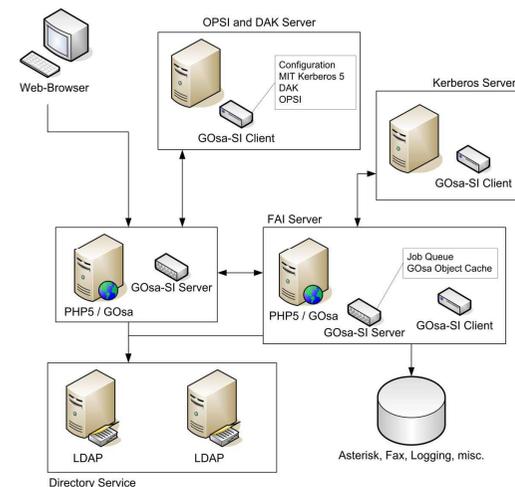
Integration von aktuellen „Bewegungs- bzw. Zustandsdaten“ in die zentrale GOsa² Managementoberfläche

- Systemmeldungen (syslog)
- Monitoring (nagios)

Integration von administrativen Workflows zur Reduktion von manuellen Administrationstätigkeiten

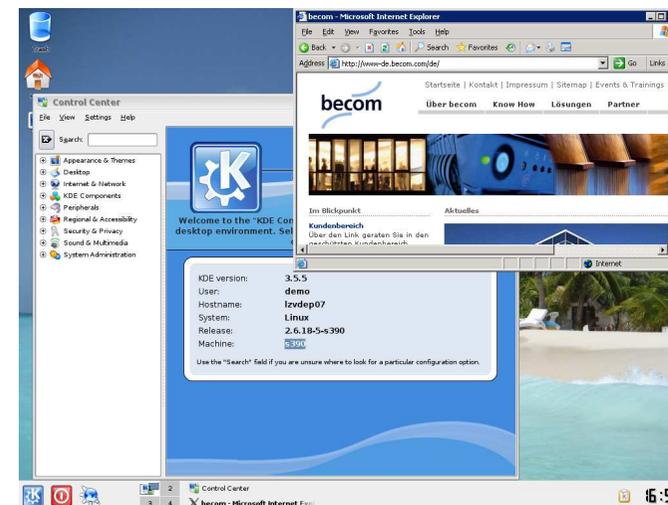
- Systemdeployment
- Softwareverteilung
- Patchverteilung

...der Anfang der GOsa² Systemarchitektur!



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



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
```

Roll-Out Techniken

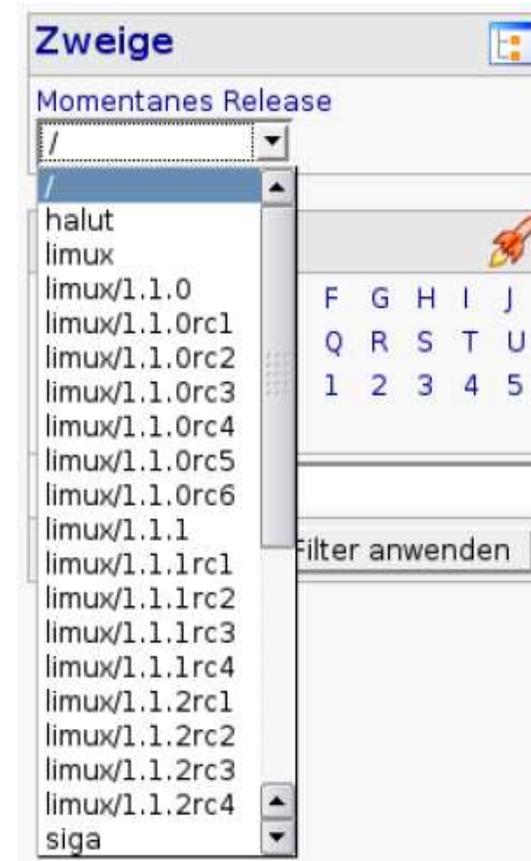
- c(ustom)tftpd für flexible Bereitstellung von PXE Bootfiles -> werden dynamisch aus LDAP generiert
- Gosa-si daemon -> Kommunikationsinfrastruktur zwischen Verteil- und Subverteilserversn sowie Clients
- Speicherung aller FAI-Attribute im LDAP

The screenshot shows a web interface with two main panels. The left panel, titled "Liste von zu verteilenden Klassen und Produkten", contains a table with columns for "Klassen-Name", "Klassen-Typen", and "Aktionen". The right panel, titled "Releases", includes a dropdown for "Momentanes Release" (set to "etch"), a list of actions like "Release erzeugen" and "Unveränderbares Release erzeugen", and a "Filter" section with a grid of letters and numbers, and a "Filter anwenden" button.

<input type="checkbox"/>	Klassen-Name	Klassen-Typen	Aktionen
<input type="checkbox"/>	BASE		
<input type="checkbox"/>	DEBIAN-Base		
<input type="checkbox"/>	DHCP-NETWORK		
<input type="checkbox"/>	DHCP-SERVER		
<input type="checkbox"/>	DNS-SERVER		
<input type="checkbox"/>	FAI-TEST		
<input type="checkbox"/>	FAI-TEST-SIMPLE		
<input type="checkbox"/>	FAISERVER		
<input type="checkbox"/>	FRANK		
<input type="checkbox"/>	FRANK-BASE		
<input type="checkbox"/>	FRANK-MESSE-DEMO		
<input type="checkbox"/>	FRANK-WORKSTATION		
<input type="checkbox"/>	GERMAN		
<input type="checkbox"/>	GONICUS-BASE		

Releaseverwaltung in GOsa²

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



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

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:

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

Fragen?



Wir sind für Sie da.

**Heute.
Morgen.
Und in Zukunft.**





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