



Wir optimieren Ihren Business Prozess

**H**IGH **V**ALUE **C**ONSULTING AG  
Hauptstrasse 77  
4147 Aesch

T: +41 61 751 72 78

F: +41 61 751 72 79

Mail: [info@hvc.ch](mailto:info@hvc.ch)

# Identity & Access Management

Open Source

- In der elektronischen Welt gilt es, den Produktionsfaktor Information sowohl gezielt zu nutzen als auch vor Missbrauch zu schützen. Die Informations- und Kommunikationssicherheit spielt vor diesem Hintergrund eine zentrale Rolle. Innerhalb der gesamten Architektur, insbesondere innerhalb der Sicherheitskette, ist Identity und Access Management ein Glied von höchstem operationellem wie auch strategischem Stellenwert und bildet die Grundlage, auf der durchgängige, nachhaltig wirksame Prozesse erst möglich werden.
- Interne und externe Personen, die an den Geschäftsabläufen beteiligt sind, müssen sich zweifelsfrei identifizieren lassen. Es ist sicherzustellen, welche Personen auf welche Ressourcen zu welchem Zeitpunkt und mit welchen Rechten zugreifen dürfen.
- Die Grundlage dazu bildet eine übergreifende, einheitliche und automatisierte Userverwaltung unter Einbezug betroffener Ressourcen wie Verzeichnisse und Applikationen.

# Warum Identity & Access Management?

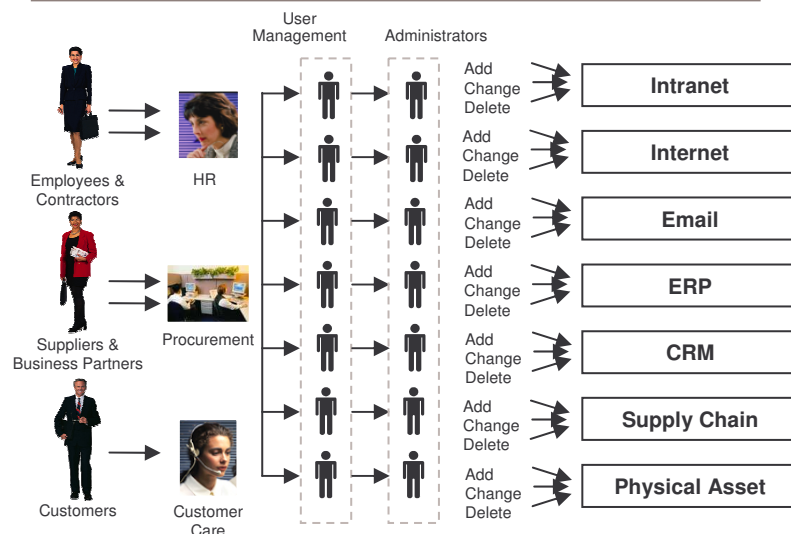
## Die Herausforderung

- Unterschiedliche User mit Zugriff auf Unternehmensapplikationen und Daten, wie Business Partner, Kunden, Lieferanten usw.
- Immer mehr Applikationen – mit “mission critical” Funktionalität – innerhalb und ausserhalb der vier Wände der Unternehmung
- Verschiedene User-Klassen mit unterschiedlichen Security- und Kontroll-Anforderungen
- Jede Informationsquelle hat eigene Security- und Kontroll-Mechanismen
- Applikationen alleine bieten nicht länger umfassenden Schutz
- **Wie behält man die Kontrolle?**

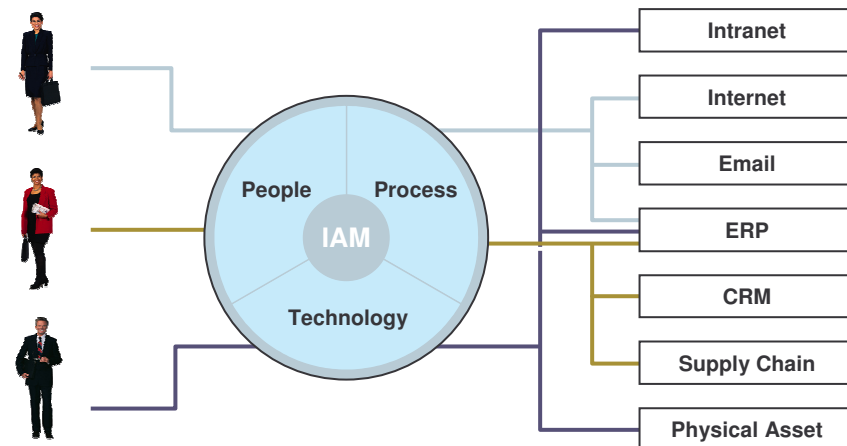
## Die Lösung

- Ausrichtung der Organisation, Prozesse und Technologie mittels Integration von Identity & Access Management (IAM) Services
- Individualisierte Security und Zugriffsrechte basierend auf einer Identität oder Rolle
- Integration von “Best Practice” Lösungen

## Das Problem

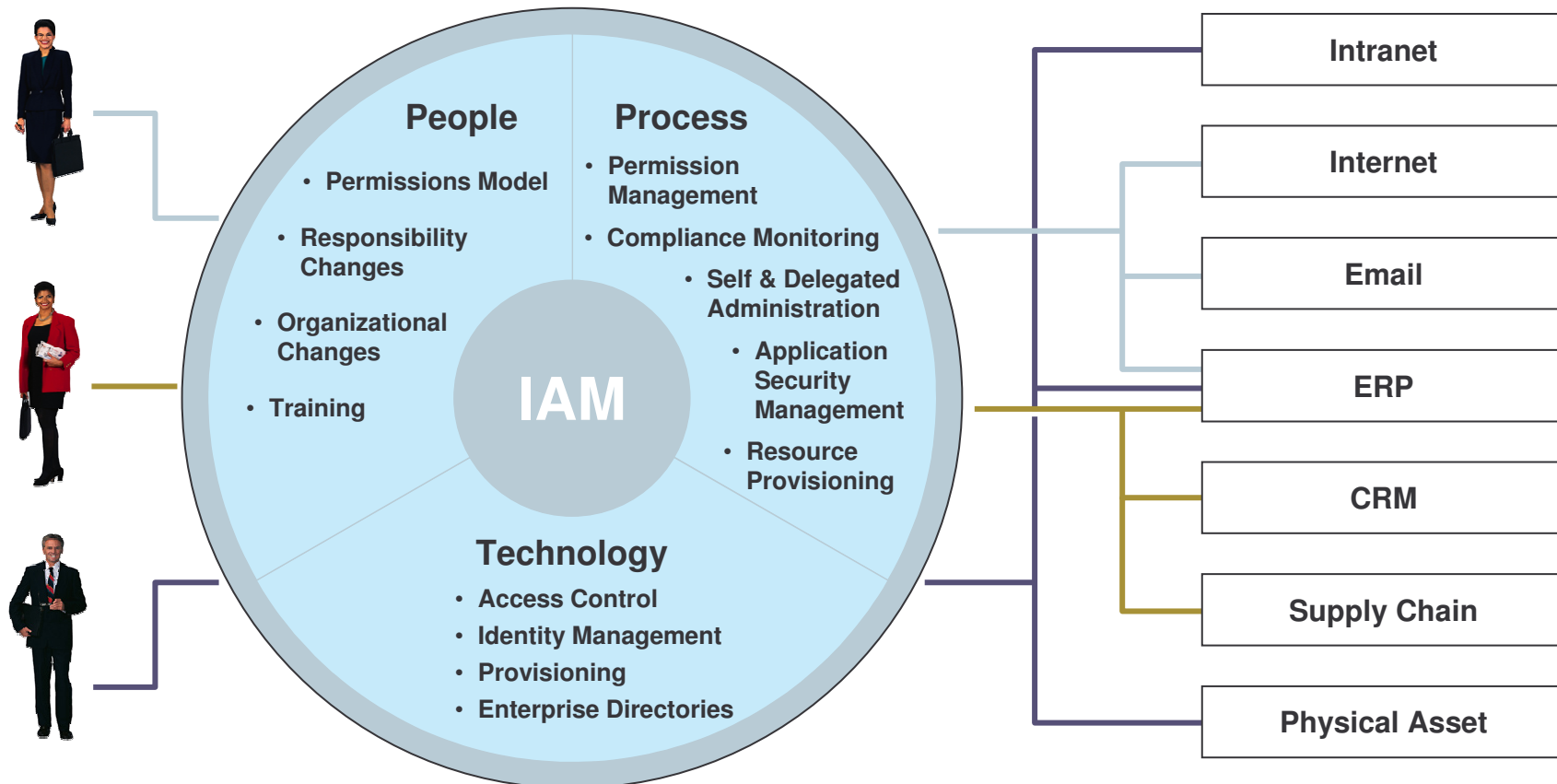


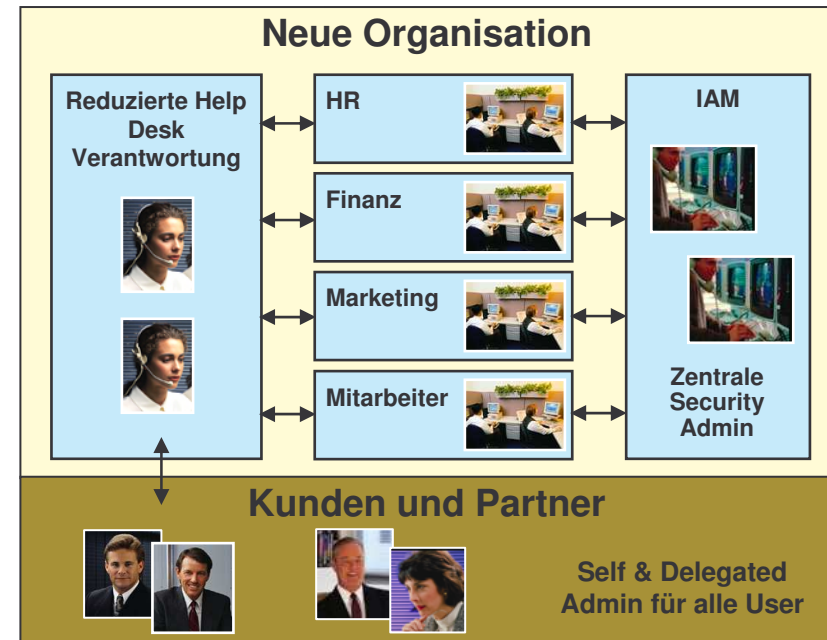
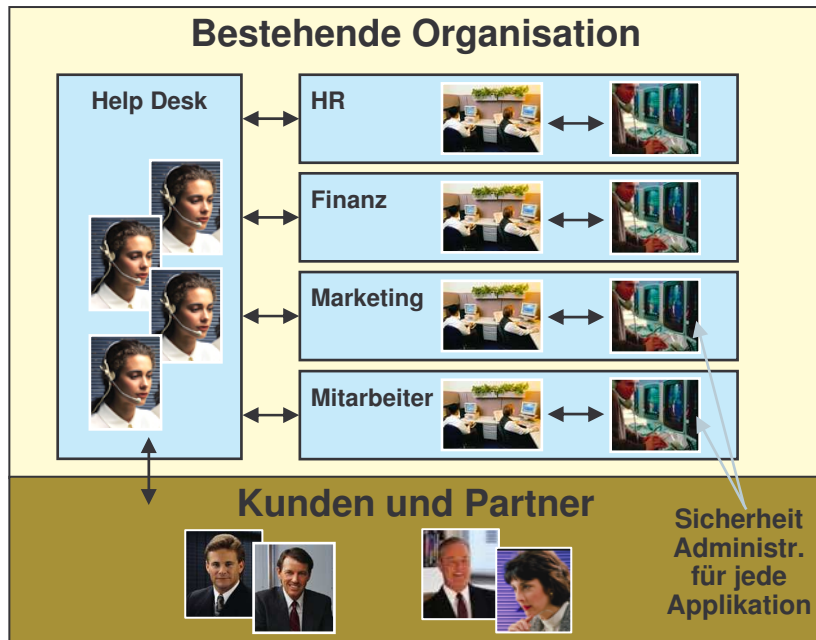
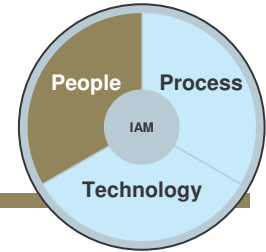
## Die Antwort



# Das IAM-Referenzmodell

Die technische Implementation IAM ist nur ein Teil einer Lösung. Das Verständnis für die Natur eines Transformationsprozesses und die Ausrichtung der Lösung auf die Personen in der Organisation, ist der Schlüssel für den Erfolg einer IAM Lösung.





## Berechtigungen

- Definiert organisatorische Rollen, Bezeichnungen und Berechtigungsmodell
- Mappt diese zu den entsprechenden Access-Levels und Ressourcen

## Verantwortung

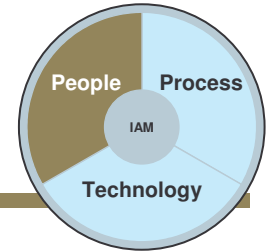
- Verschiebt die Verantwortung der User-Administration vom Help Desk zum End User, durch Delegation von Tasks zum End User
- Verschiebt die Verantwortung für Verwaltung der Zugriffskontrolle von der IT zu den Ressource-Verantwortlichen
- Neue Verantwortung für die Security-Administration für das Verwalten des Workflow und der Rollen

## Organisation

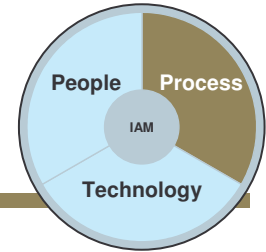
- Reduktion im Help Desk und neuer Verantwortungsbereich bei den verbleibenden Help Desk Ressourcen
- Neue zentrale Security-Administration durch den Support der IAM Infrastruktur

## Training

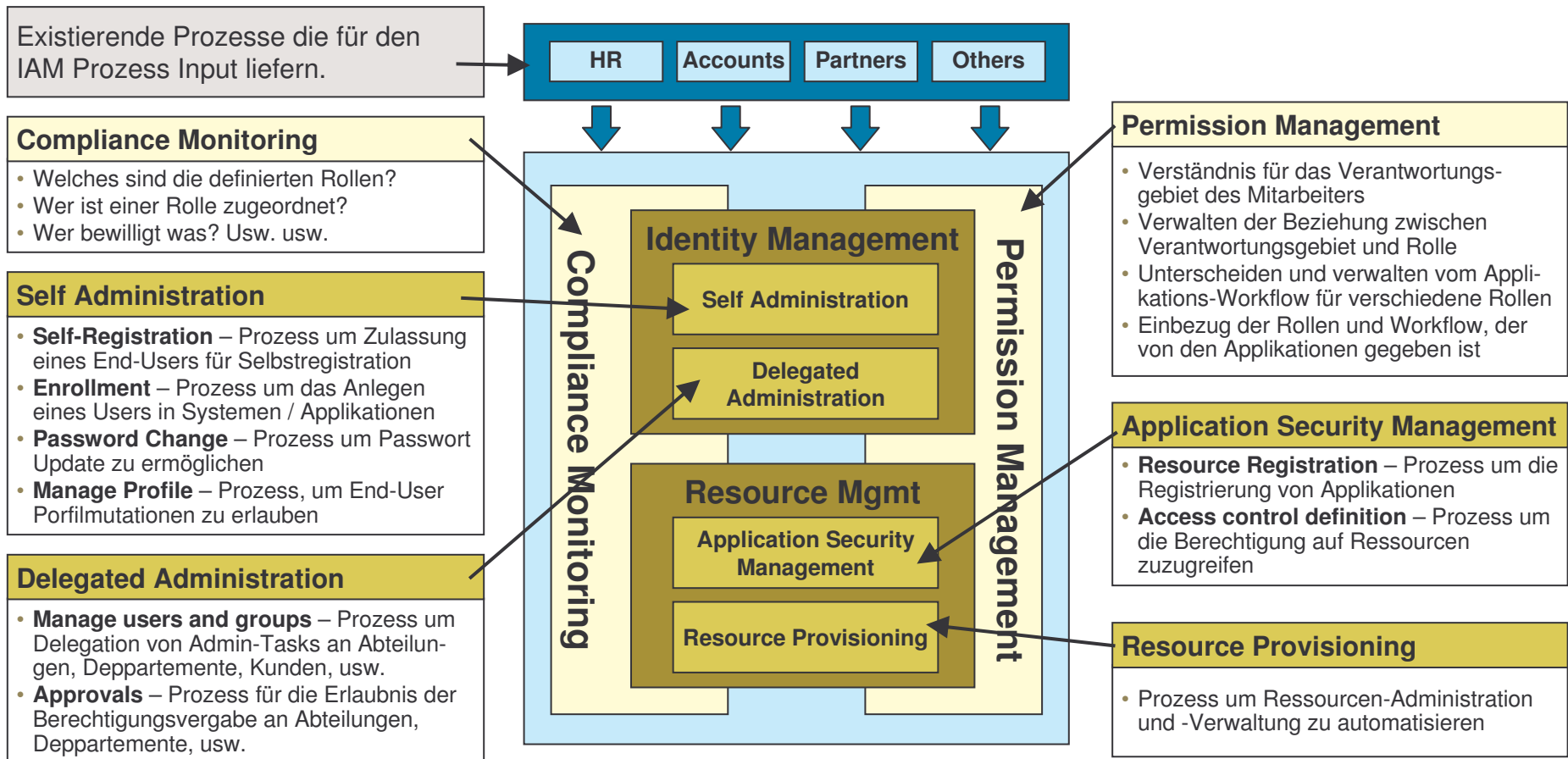
- Benötigt Training für die Security-Administration um die IAM Infrastruktur supporten zu können
- Benötigt Training für die User um ihre eigenes Profil, Passwort und Registration zu verwalten
- Benötigt Training für delegierte Administratoren um User und Gruppen im Interface zuweisen zu können.

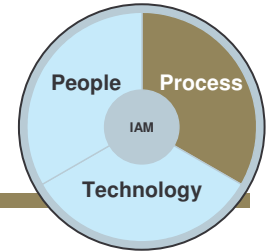


- ✓ Abbildung von Hierarchien, Funktionen und Aufgaben
- ✓ Schemaerweiterungen für diverse Parameter u. Attribute
- ✓ Mapping zu Access-Levels und Ressourcen
- ✓ Rollen
  - ✓ Managed Roles
  - ✓ Filtered Roles
  - ✓ Nested Roles

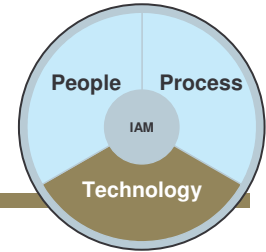


**IAM Lösungen transformieren den bestehenden Business Prozess für das Verwalten der User und Ressourcen. Wo immer möglich, werden manuelle Prozesse automatisiert und ICT Prozesse vereinfacht oder an das Business Owner delegiert.**

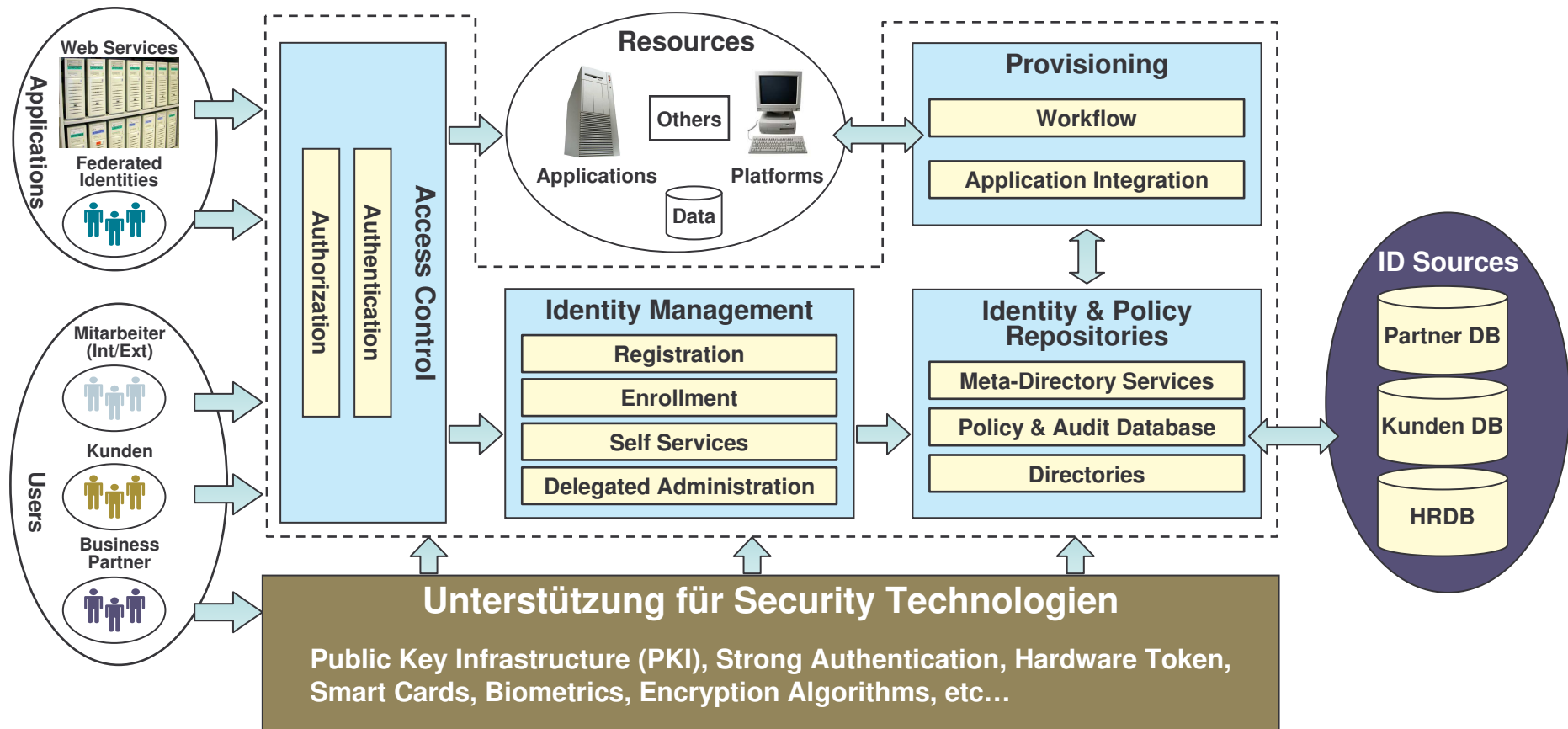


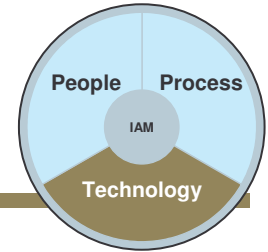


- ✓ Compliance Monitoring ⇒ Virtual Views
- ✓ Self Administration ⇒ GUI, Console
  - ✓ Self-Registration, Entrollement, Password-Change
- ✓ Delegated Administration ⇒ GUI, Console
  - ✓ Manage users an Groups, Approvals
- ✓ Permission Management ⇒ GUI, Console
  - ✓ Role based access (z.B. auch Printing)
- ✓ Application Security Management ⇒ DSML-GW
  - ✓ Ressource Registration, Access Contorl Definition
- ✓ Ressource Provisioning
  - ⇒ Win Sync
  - ⇒ DSML GW
  - ⇒ Plugins



Die Schlüsseltechnologien für IAM sind Identity Management, Access Control, Provisioning und Directories. Integriert bilden diese Technologien eine Plattform die End to End IAM Lösungen erst ermöglichen.





- ✓ Access Control
- ✓ Identity Management
- ✓ Identity & Policy Repository
- ✓ Provisioning

- ⇒ LDAP / RHDS
- ⇒ Java GUI/Console
- ⇒ RHDS
- ⇒ Win Sync
- ⇒ DSML GW
- ⇒ Plug-in / API's














































Provisioning ist auf wenige Standard-Konnektoren limitiert!



- 4-Way Mult-Master Replication
- Attribute encryption
- Chaining and Referrals
- Data Interoperability Plugins
- High Performance Logging
- Access Control Mechanism
- Language Handling
- Multiple Databases
- Online configuration and management
- Password Policy and Account Lockout

- Resource-limits by bind DN
- Roles and Class of Services
- SASL – Simple Authentication and Security Layer
- Server Side Sorting
- SSL / TLS
- Virtual Views

- Prozessausrichtung
- Release-Zyklen
- Administrationsschnittstellen
- Replikationsfunktion
- Performance
- Skalierbarkeit
- ACL's
- Interoperabilität

# Vendor Matrix

	Vendor Quality	Identity Mgmt.	Access Control	Provisioning	Directory	Release Mgmt	Security	Related Techn.
OpenLDAP								
RHDS								
Novell								
SUN								
Siemens								
Microsoft								

Unterstützung: Sehr hoch:  hoch:  mittel:  tief:  sehr tief: 

## I&AM mit Open Source Software

**H**IGH **V**ALUE **C**ONSULTING AG  
Hauptstrasse 77  
4147 Aesch

T: +41 61 751 72 78

F: +41 61 751 72 79

Mail: [info@hvc.ch](mailto:info@hvc.ch)

# Was ist die Funktion des Directory Servers?

- 1. Nur** Userverwaltung (Passwort hosting)?
  - Login von einer *Art Client* (zB. *Windows, Mac, Linux..*)
- 2. Zentrale** Identitätsverwaltung?
  - Verschiedenste Clients **und** Services (zB. Datenbank, Proxy, Druckerzuweisung, ..)

## 1. *Nur* Userverwaltung (Passwort hosting)?

- Einfacher Setup  
Geringe Anforderungen an den Funktionsumfang der Software, ist mit jeglicher Art Software möglich (Perl basierte Directory Server)
- Einfaches Directory Design  
Flaches Design: nur User und Gruppen, keine Verzweigung der User in Suborganisationen
- Einfache Funktionalitäten/Useridentitäten  
Useridentität beinhaltet nicht viel mehr als:
  - Name
  - Vorname
  - UID
  - Passwort

## 1. *Nur* Userverwaltung (Passwort hosting)?

- Ad-Hoc Definition und (kleinere) Veränderung ist jederzeit möglich
- Bei kleiner Userzahl und Funktionalität einfach zu handhaben/administrieren
- Gleiche Bedeutung jedes Users (Ausnahme: Administrator/en)
- Zusatzfunktionen sind nur schwer im Nachhinein implementierbar
- Kann nur schwer erweiterte Funktionalitäten übernehmen (Spaghetticode-Gefahr)

## 2. Zentrale Identitätsverwaltung?

- Komplizierteres Setup mit Synchronisations Funktionalität
- Verschachteltes Directory Design  
Einzelne Departments werden als Substrukturen aufgebaut.  
Beinhaltet auch Setup von Computern, Druckern, Servern....
- Verschiedenste Clients **und** Services (zB. Datenbank, Proxy..)  
Verschiedene Anforderungen an Inhalt der übergebenen Daten.  
Es werden einzelne Teile der Identität ausgewertet
- Komplexe Useridentität  
Beinhaltet auch Autorisierungsinformationen
  - Position
  - Abteilung
  - Aufgabe/Projektzugehörigkeit

## 2. Zentrale Identitätsverwaltung?

- Abklärung der Funktionalitäts- und auch Firmenstruktur
- Directory Design von entscheidender Bedeutung für Performance und Nutzen
- Bei steigender Funktionalität, Bedeutung und Firmengrösse auch Abbildung der Geschäftsprozesse
  - Web Portal (Firmenangehörige, Kunden, Guests)
  - ID basierter Ressourcenzugriff (Datenbanken, Formulare, Programme, Kalender)
  - Abrechnung (Zeit/Projekt) via ID
  - Zutrittsverwaltung aufgrund der ID

## Was gibt es

1. OpenLDAP: Der erste OpenSource Directory Server.
2. Fedora Directory Server: Neues OpenSource Projekt (vorher closed Source)
3. ApacheDS: Neues Projekt der Apache Foundation
4. Kleinere Projekte, zum Teil Perl basierte Server

## **OpenLDAP: Der erste OpenSource Directory Server**

- Erstes Projekt, das eine Userverwaltung mit LDAP Funktionalität nachgebildet hat. (Authentifizierung)
- Im Laufe der Zeit Ausbau zu einem Directory Server.
- Synchronisationsfähigkeit nur von/zu einem LDAP Server (nativ), via Hilfstools (Samba, Perl,...) auch erweiterte Möglichkeiten
- Master-Slave Replikation
- Kein eigenes Administrationstool, nur via Kommandozeilentools
- Nicht voll RFC konform

## OpenLDAP:

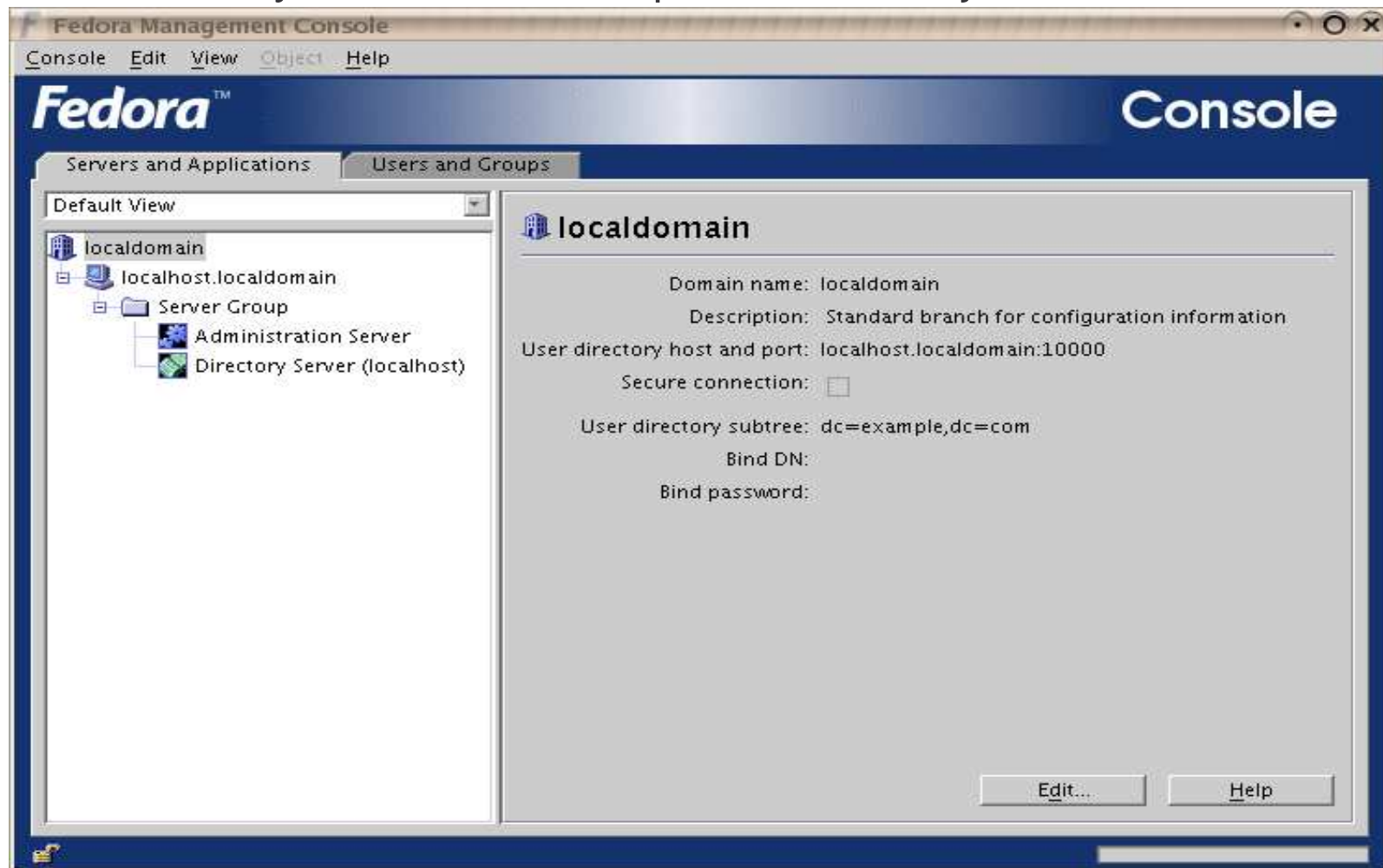
- Setup nur via Konfigurationsfile
- ***acl*** Definitionen im Konfigurationsfile (Accessrechte!)

```
access to dn.subtree="dc=example,dc=com" attr=homePhone
  by self write
  by dn.children=dc=example,dc=com" search
  by peername=IP:10\..+ read
access to dn.subtree="dc=example,dc=com"
  by self write
  by dn.children="dc=example,dc=com" search
  by anonymous auth
```

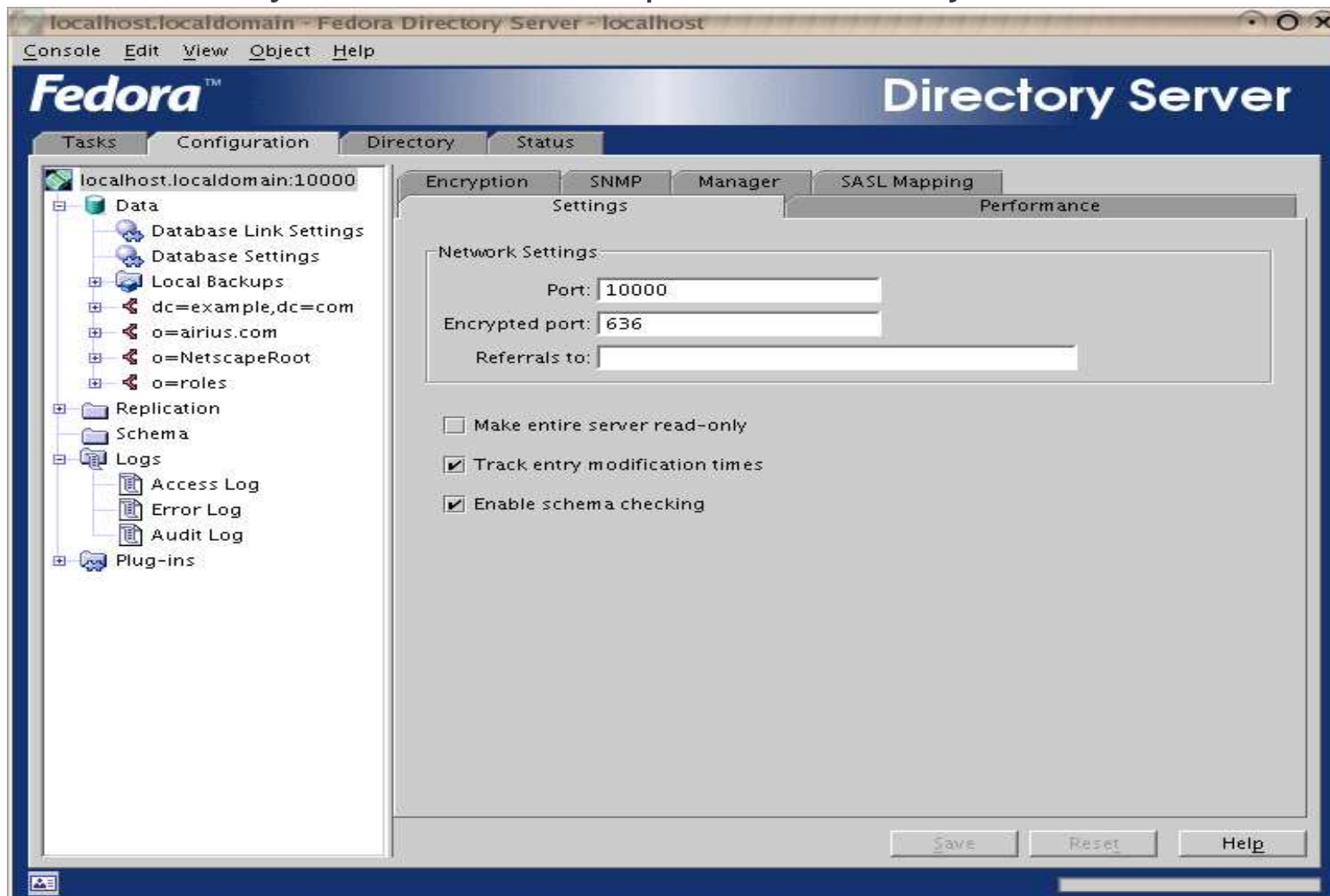
## Fedora Directory Server: Neues OpenSource Projekt

- Sehr mächtiger Directory Server (vorher Netscape Directory Server) mit einer grossen Zahl an (native) plugins
- (native) Synchronisation zu LDAP Servern, NT Primary Domain Controller und AD. Mit Tools auch von anderen Diensten (Datenbank)
- Mehrfache (4) Master-Master Replikation
- Mehrfache kaskadierte Master-Slave/Hub Replikation
- Eigener Administrationsserver (lokal oder remote) und GUI Konsole
- RFC konform!

## Fedora Directory Server: Neues OpenSource Projekt



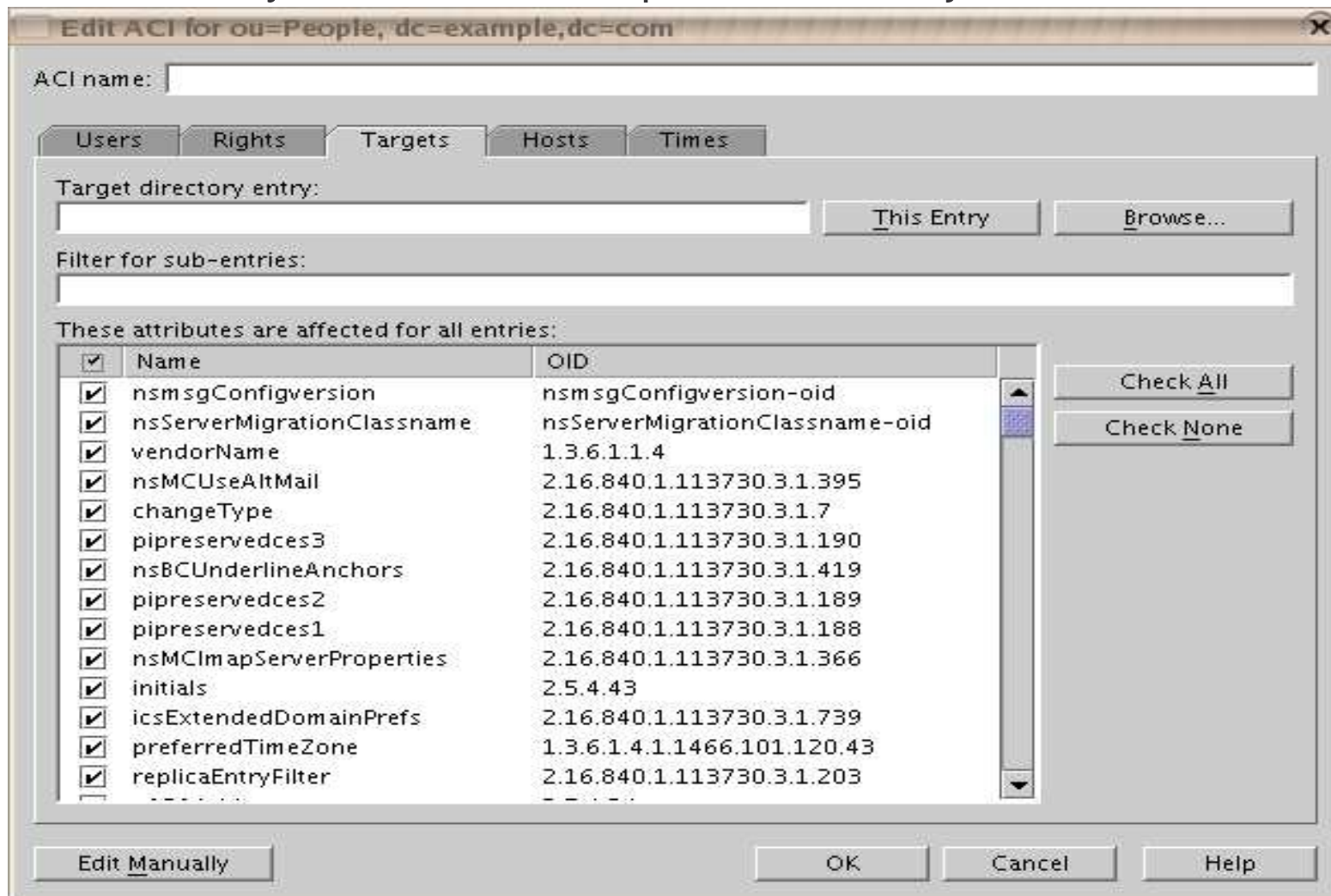
## Fedora Directory Server: Neues OpenSource Projekt



## Fedora Directory Server: Neues OpenSource Projekt




## Fedora Directory Server: Neues OpenSource Projekt



## Fedora Directory Server: Neues OpenSource Projekt

**Person Entry**

 **New Person - richm, People**

**\* Indicates a required field**

**Contact Information**

First Name:	<input type="text" value="Rich"/>	Common Name: *	<input type="text" value="Rich Megginson"/>
Last Name: *	<input type="text" value="Megginson"/>	E-Mail Address:	<input type="text" value="richm@example.com"/>
Password:	<input type="password" value="*****"/>	Repeat password to confirm:	<input type="password" value="*****"/>
Phone:	<input type="text" value="408 555 3141"/>	AIM ID:	<input type="text" value="richm"/>
Fax:	<input type="text"/>	User ID:	<input type="text" value="richm"/>
Pager:	<input type="text"/>	Mobile Phone:	<input type="text"/>

**Business and Location Information**

Business Category:	<input type="text"/>	Title:	<input type="text"/>
Organizational Unit:	<input type="text"/>	Manager:	<i>You must save this entry before you can edit these fields.</i>
Room Number:	<input type="text"/>	Admin.:	
Dept#:	<input type="text"/>	Emp#:	<input type="text"/>
Car License#:	<input type="text"/>		
Mailing Address:	<input style="width: 100%;" type="text"/>		

**Additional Information**

Description:	<input type="text"/>
See Also:	<i>You must save this entry before you can edit this field.</i>
URL:	<input type="text"/>

## Fedora Directory Server: Neues OpenSource Projekt

**Directory Server Org Chart**      Search for:       Go


**Welcome!**


To find a person in your corporate organization chart, enter their name in the search box above, then click "Go"


Below is a sample of an organization chart, with a description of the types of actions you can take

Thank you for using the Directory Server Org Chart!

[Prepare this page for printing](#)

▶ **Jeanne Grimley**  
VP Engineering  
Manager: ▶ Robert James 


├ ▶ Kenneth Lee 


▶ **Brian Bingham**   
Engineering Manager


├ ▶ Chris Felix  
└ ▶ Scott

**Chris Felix**  
Sr. Engineer

---

 [Email](#)

 [Phonebook](#)

 [Locator](#)

Total number of


Using the "Customize View" feature, you can display clickable icons next to names. (send Instant Message, etc.)

Hovering over the arrow next to a name displays more options and information.









































































































## Fedora Directory Server: Neues OpenSource Projekt

Directory Server Org Chart    Search for:     Go    [Customize](#)

[Prepare this page for printing](#)

➤ **Barry Parker** 

Manager: (no manager listed)

<div style="border: 1px solid gray; padding: 5px; margin-bottom: 10px;"> <p>➤ <b>Christoph Newport</b> </p> </div> <ul style="list-style-type: none"> <li>➤ Kelly Winters </li> <li>➤ Brad Walker </li> <li>➤ Brian Plante </li> <li>➤ Cecil Wallace </li> <li>➤ Emanuel Johnson </li> <li>➤ Gern Triplett </li> <li>➤ Harry Miller </li> <li>➤ Jeffrey Campaigne </li> <li>➤ John Falena </li> <li>➤ Kurt Jensen </li> <li>➤ Lee Ulrich </li> <li>➤ Marcus Langdon </li> <li>➤ Mike Lott </li> <li>➤ Peter Rigden </li> <li>➤ Randy Mills </li> <li>➤ Richard Bannister </li> <li>➤ Stephen Triplett </li> <li>➤ Sue Peterson </li> <li>➤ Tobias Pierce </li> <li>➤ Torrey Rigden </li> <li>➤ Alexander Lutz </li> <li>➤ Ashley Chassin </li> <li>➤ Barbara Hall </li> <li>➤ Barbara Jablonski </li> <li>➤ Benjamin Hall </li> <li>➤ Bjorn Talbot </li> </ul>	<div style="border: 1px solid gray; padding: 5px; margin-bottom: 10px;"> <p>➤ <b>David Miller</b> </p> </div> <ul style="list-style-type: none"> <li>➤ Sam Carter </li> <li>➤ Alexander Shelton </li> <li>➤ Benjamin Schneider </li> <li>➤ Bertram Rentz </li> <li>➤ Bjorn Free </li> <li>➤ Daniel Smith </li> <li>➤ David Thorud </li> <li>➤ Elba Kohler </li> <li>➤ Frank Albers </li> <li>➤ Janet Hunter </li> <li>➤ Laurel Campbell </li> <li>➤ Marcus Mcinnis </li> <li>➤ Paula Rose </li> <li>➤ Scott Lee </li> <li>➤ Stephen Carter </li> <li>➤ Sue Kelleher </li> <li>➤ Tim Labonte </li> <li>➤ Torrey Schneider </li> <li>➤ Ted Morris </li> <li>➤ Andrew Hel </li> <li>➤ Barbara Jensen </li> <li>➤ Chris Alexander </li> <li>➤ James Burrell </li> <li>➤ Jim Cruse </li> <li>➤ Jim Lange </li> <li>➤ Karen Carter </li> </ul>	<div style="border: 1px solid gray; padding: 5px; margin-bottom: 10px;"> <p>➤ <b>Erin Alexander</b> </p> </div> <ul style="list-style-type: none"> <li>➤ Andy Bergin </li> <li>➤ Anne-Louise Barnes </li> <li>➤ Dan Cope </li> <li>➤ Dan Lanoway </li> <li>➤ Eric Ward </li> <li>➤ James Lutz </li> <li>➤ Jon Bourke </li> <li>➤ Judy Rentz </li> <li>➤ Karl Cope </li> <li>➤ Lee Stockton </li> <li>➤ Matthew Vaughan </li> <li>➤ Morgan Jablonski </li> <li>➤ Pete Hunt </li> <li>➤ Peter Chassin </li> <li>➤ Richard Jensen </li> <li>➤ Tobias Cruse </li> <li>➤ Torrey Tully </li> <li>➤ Trent Couzens </li> <li>➤ John Walker </li> <li>➤ Andrew Langdon </li> <li>➤ Andy Walker </li> <li>➤ Barbara Francis </li> <li>➤ Bjorn Rigden </li> <li>➤ Cecil Harvey </li> <li>➤ David Rose </li> <li>➤ Emanuel Lott </li> </ul>	<div style="border: 1px solid gray; padding: 5px; margin-bottom: 10px;"> <p>➤ <b>Jeff Vedder</b> </p> </div> <ul style="list-style-type: none"> <li>➤ Chris Schmith </li> <li>➤ Alan Worrell </li> <li>➤ Allison Hunter </li> <li>➤ Andy Hall </li> <li>➤ Ashley Knutson </li> <li>➤ Bjorn Jensen </li> <li>➤ Dan Langdon </li> <li>➤ Dietrich Swain </li> <li>➤ Gern Tyler </li> <li>➤ Janet Lutz </li> <li>➤ Jeff Muffly </li> <li>➤ Jon Goldstein </li> <li>➤ Kelly Mcinnis </li> <li>➤ Matthew Reuter </li> <li>➤ Pete Worrell </li> <li>➤ Ted Jensen </li> <li>➤ Tobias Schmith </li> <li>➤ Wendy Lutz </li> <li>➤ Kirsten Vaughan </li> <li>➤ Alan White </li> <li>➤ Allison Jensen </li> <li>➤ Barbara Maddox </li> <li>➤ Daniel Ward </li> <li>➤ David Akers </li> <li>➤ Gern Jensen </li> <li>➤ Jody Jensen </li> </ul>
---	---	--	---

## ApacheDS: Neues Projekt der Apache Foundation

- Javabasiert, daher auf jeglichen Plattformen einsetzbar
- Einfacher Setup und Funktionalitäten
- Eher als reiner Autorisierungsserver (UID/Passwort) einsetzbar
- Nur LDAP Synchronisation
- Wird (abgewandelt) vom FDS für NT Synchronisation benutzt
- RFC konform ????

## Kleinere Projekte: zum Teil Perl basierte Server

- Einfachster Aufbau
- Langsam, weil interpretierende Sprachen (Perl)
- Nur LDAP Synchronisation
- Kommandozeilen orientiert
- RFC konform ????

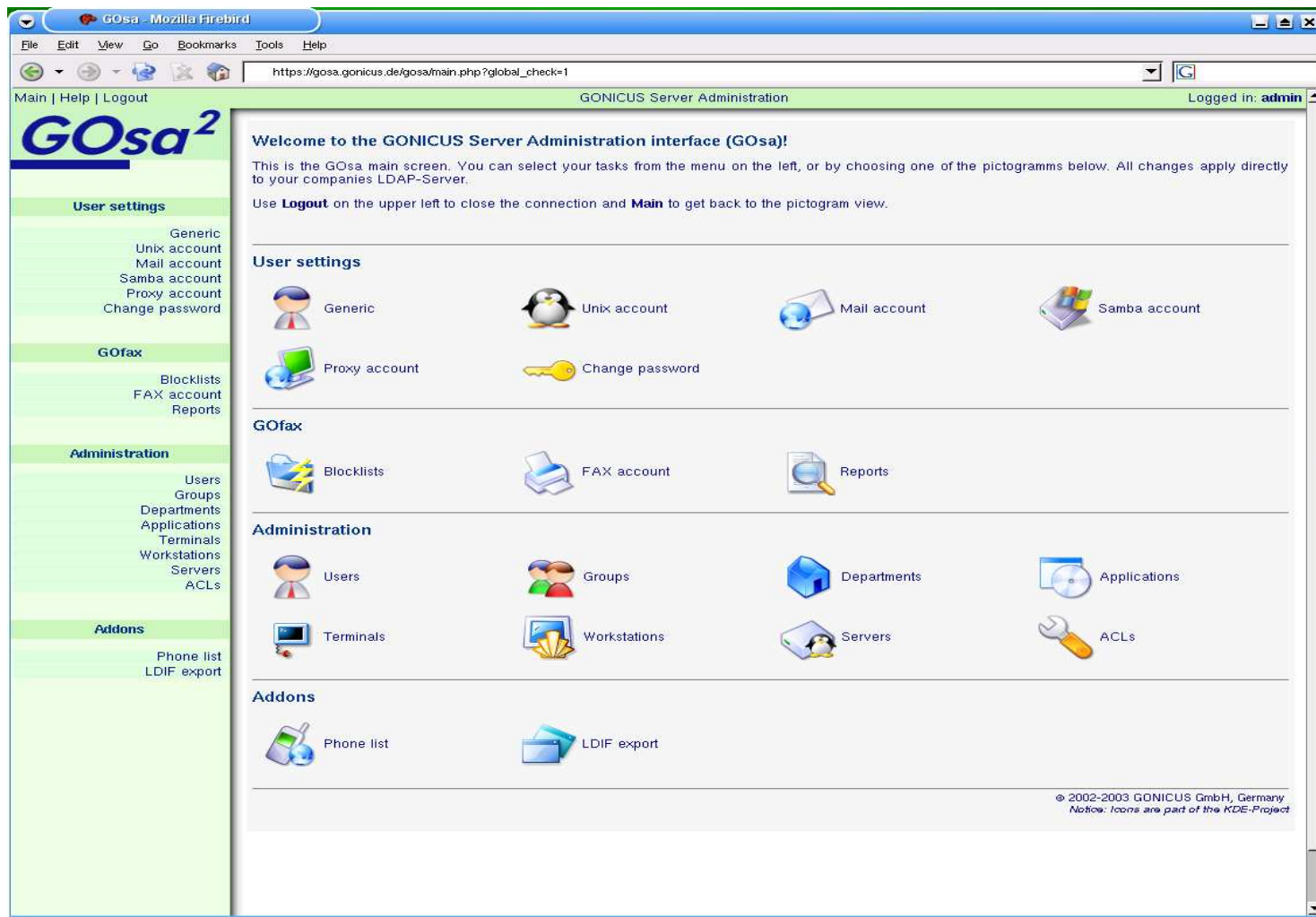
### Verschiedene Ausrichtung (Bedienung)

- Webbasiert: remote Tool, Oberfläche adaptierbar
- Lokal: schnelles (kompiliertes) Tool, Oberfläche fix
- Kommandozeile: kleine schnelle und mächtige Tools, lassen sich in eigene Scripte integrieren

## Grafische webbasierte Tools

- Gosa: mächtiges Allroundtool vom Debian Team. Entwickelt sich aber in letzter Zeit vom Directory Administrationstool zu einem LDAP basierten Server und Netzwerk Administrationstool (PHP4)
- LAM: Einfaches Tool um Accounts zu administrieren (PHP4)
- LDAP Client: Einfaches Tool um Accounts zu administrieren (kleinere Version des LAM - PHP4)
- Web2LDAP: Tool zur Account Administration (Python)

## Grafische webbasierte Tools Gosa



## Grafische webbasierte Tools Gosa

The screenshot shows the Gosa web interface in a Mozilla Firefox browser window. The page title is "Gosa - Mozilla Firefox" and the URL is "https://gosa.gonicus.de/gosa/main.php?plug=9". The user is logged in as "admin". The main content area is titled "User management - add/edit" and has tabs for "Generic", "Unix", "Mail", "Samba", "Proxy", and "Fax". The "Generic" tab is active, showing "Personal information" and "Organizational information" sections.

**Personal information**

Name*	Mustermann	Address	
Given name*	Hermann	Phone	
Login*	hermu	Homepage	
Personal title		Password storage	crypt
Academic title	Dr.	Certificates	<a href="#">Edit certificates...</a>
		Kerberos	<a href="#">Edit properties...</a>

Change picture... Base\* Testdepartment

**Organizational information**

Organization		Room No.		Location	
Department		Phone		State	
Department No.		Mobile		Address	
Employee No.		Pager			
Employee type		Fax			

Load defaults

Finish Cancel

## Grafische webbasierte Tools LAM

The screenshot displays the LDAP Account Manager (LAM) web interface. At the top, there is a navigation bar with a 'Tools' icon, the title 'LDAP Account Manager', and a 'Logout' button. Below the navigation bar, there are tabs for 'Tree view', 'Users', 'Groups', and 'Hosts'. The main content area is divided into a left sidebar and a main form area. The sidebar contains a 'Please select page:' section with buttons for 'Main', 'Personal', 'Unix', 'Samba 3', and 'Reset changes'. The main form area is titled 'Unix' and contains the following fields:

Field	Value
User name*	avogel
Common name*	Anja Vogel
UID number*	15428
Gecos	
Primary group*	admins
Additional groups	Edit groups
Home directory*	/home/avogel
Password	Change password
Set no password	<input checked="" type="checkbox"/>
Invalid password	<input type="checkbox"/>
Lock password	<input type="checkbox"/>
Login shell*	/bin/bash

\*required

## Grafische webbasierte Tools LAM



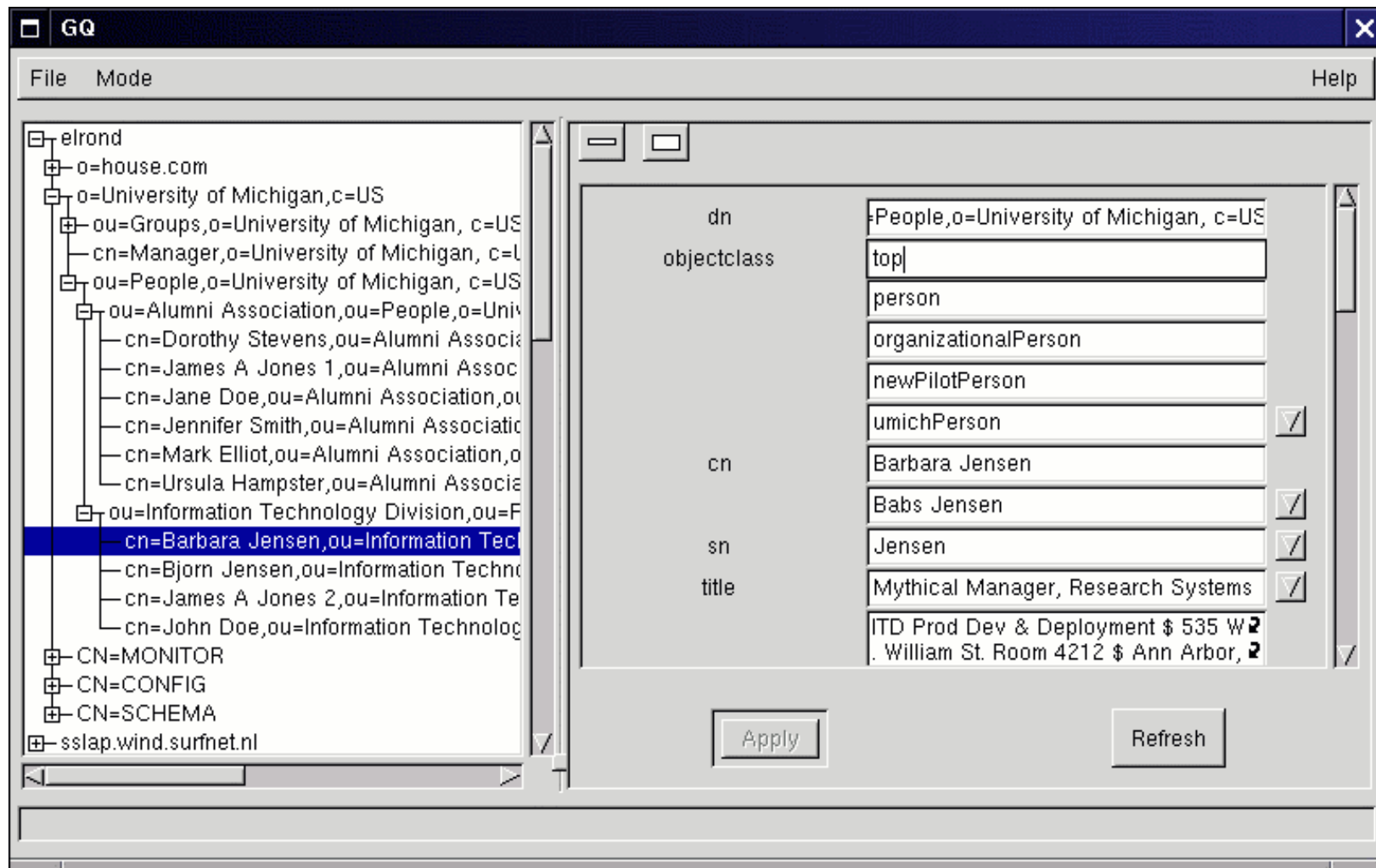
The screenshot shows the LDAP Account Manager web interface. At the top, there is a navigation bar with 'Tools', 'LDAP Account Manager', and 'Logout'. Below this, there are tabs for 'Tree view', 'Users', 'Groups', and 'Hosts'. The main content area displays a table of users with columns for User ID, First name, Last name, UID number, and GID number. A 'Filter' input field is present above the table. Below the table, there are buttons for 'New user' and 'Delete user(s)'. At the bottom, there is a 'PDF' section with a dropdown for 'PDF structure' and buttons for 'Create PDF for selected user(s)' and 'Create PDF for all users'.

		User ID	First name	Last name	UID number	GID number
<input type="checkbox"/>	Edit	avogel	Anja	Vogel	15428	10819
<input type="checkbox"/>	Edit	cbach	Claudia	Bach	15429	10819
<input type="checkbox"/>	Edit	ebaecker	Ernst	Bäcker	15430	10819
<input type="checkbox"/>	Edit	ehauser	Elke	Hauser	15431	10819
<input type="checkbox"/>	Edit	fmontag	Franz	Montag	15420	10815
<input type="checkbox"/>	Edit	hschuster	Heinz	Schuster	15427	10815
<input type="checkbox"/>	Edit	mfischer	Monika	Fischer	15425	11259
<input type="checkbox"/>	Edit	shuber	Sepp	Huber	15419	10815
<input type="checkbox"/>	Edit	thauser	Thomas	Hauser	15423	10815

## Grafische lokale Tools

- `gg`: lokaler LDAP Browser mit einfachen Account Administrationsmöglichkeiten (Gnome Toolkit)
- My LDAP klient: lokaler LDAP Browser mit einfachen Account Administrationsmöglichkeiten (KDE Toolkit)
- integrierte Tools in Linux Distributionen (Yast o.Ä.)

## Grafische lokale Tools GQ

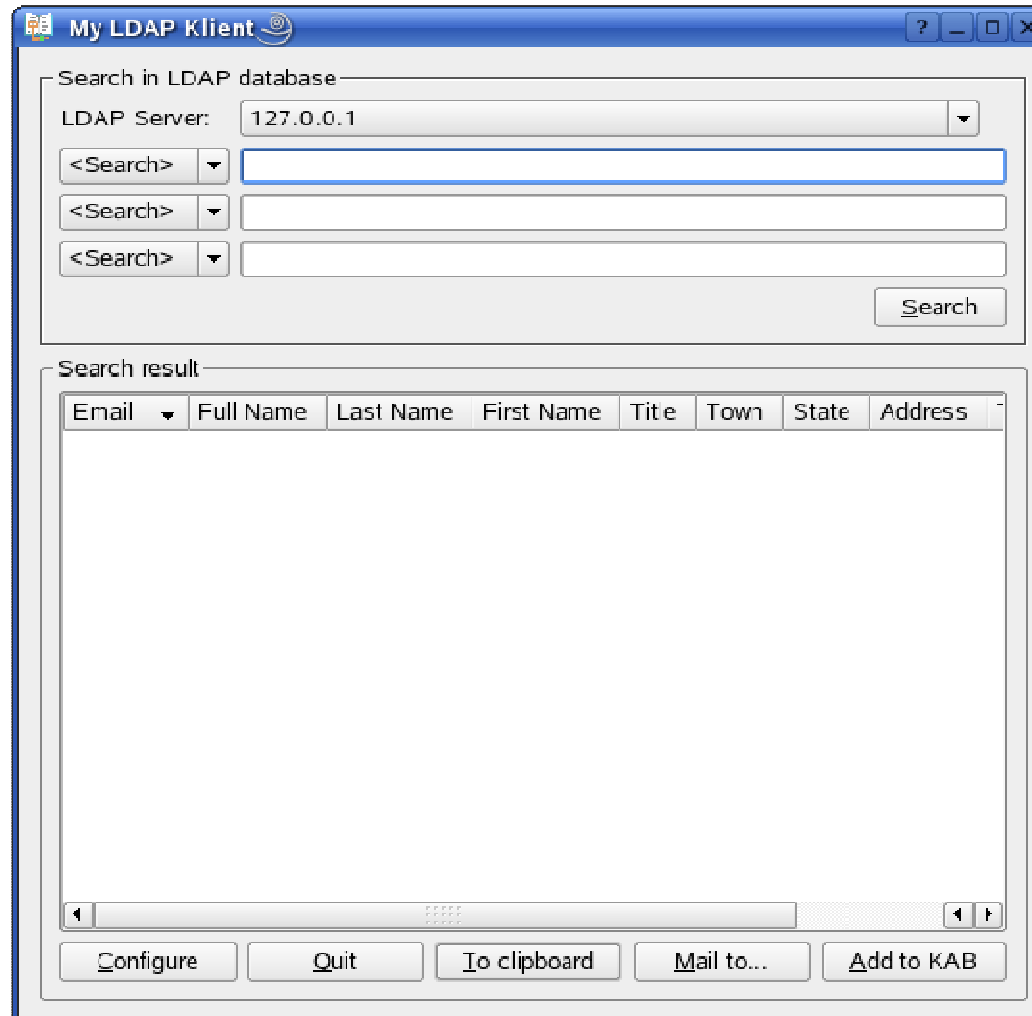


## Grafische lokale Tools GQ

The screenshot shows the GQ graphical tool interface. At the top, there is a menu bar with 'File', 'Mode', and 'Help'. Below the menu bar is a search area with a 'filter' dropdown set to '(sn=\*)', a search input field containing 'elrond UoffM', and a 'Find' button. The main area displays a table of LDAP search results with the following columns: DN, objectClass, cn, sn, and title. The table contains 11 entries. At the bottom of the window, a status bar indicates '11 entries found'.

DN	objectClass	cn	sn	title
cn=Barbara Jensen,ou=Information Technology	top person organizati	Barbara Jensen Babs	Jensen	Mythical Manager,
cn=Bjorn Jensen,ou=Information Technology	top person organizati	Bjorn Jensen Biiff Jer	Jensen	Director, Embedde
cn=Dorothy Stevens,ou=Alumni Association,ou=	top person organizati	Dorothy Stevens Dot	Stevens	Secretary, UM Alu
cn=James A Jones 1,ou=Alumni Association,c	top person organizati	James A Jones 1 Jar	Jones	Mad Cow Researc
cn=James A Jones 2,ou=Information Technolo	top person organizati	James A Jones 2 Jar	Doe	Senior Manager, Ir
cn=Jane Doe,ou=Alumni Association,ou=Peop	top person organizati	Jane Doe Jane Alver	Doe	Programmer Analys
cn=Jennifer Smith,ou=Alumni Association,ou=f	top person organizati	Jennifer Smith Jen Sr	Smith	Telemarketer, UM /
cn=John Doe,ou=Information Technology Divi	top person organizati	John Doe Jonathon C	Doe	System Administrat
cn=Manager,o=University of Michigan, c=US	top person quipuObje	Manager Directory M	Manager	
cn=Mark Elliot,ou=Alumni Association,ou=Peo	top person organizati	Mark Elliot Mark A El	Elliot	Director, UM Alumr
cn=Ursula Hampster,ou=Alumni Association,ou	top person organizati	Ursula Hampster	Hampster	Secretary, UM Alu

## Grafische lokale Tools My LDAP klient



### Kommandozeilen Tools

- Tool wie Idapmodify, Idapadd, Idapdelete lassen sich entweder von Hand oder per Script einsetzen
- Durch ihren einfachen (binäre) Aufbau kann man sie sehr schnell und ohne grosse Konfiguration einsetzen
- Lassen sich dann zu einer eigenen Weboberfläche einsetzen
- Perl bietet einige LDAP Bibliotheken mit direktem Directory Zugriff und darum lässt sich auch damit ein Administrations Tool aufbauen

## Wer soll darauf zugreifen? Und wie?

### 1. *Nur* Systemadministration?

- Begrenzte Anzahl zentraler Administratoren

### 2. Dezentral?

- Verschiedene Administrationsstufen, delegated administration

### 3. User?

- Selfdelegated Administration

# Wer soll darauf zugreifen? Und wie?

### 1. *Nur* Systemadministration? (Begrenzte Anzahl zentraler Administratoren)

- Geeignetes Tool kann nach Anforderungen (und Geschmack) des/der Administrator/en ausgesucht werden.
- Läuft lokal und bietet die gewünscht Komplexität/Mächtigkeit

## Administration

- gq lokal
- My LDAP klient
- LAM
- GOsa
- Fedora Administrationsserver und GUI

# Wer soll darauf zugreifen? Und wie?

## 2. Dezentral? (Verschiedene Administrationsstufen)

- Mehrere Tools.
- Abgestimmt in der Funktionalität auf den Aufgabenbereich des Bearbeiters (HR, Admin, Helpdesk, Superuser,...)
- Zuerst (!! ) Abklärung der Zuständigkeiten:
  - Wieviel darf derjenige sehen
  - Was darf er/sie verändern
  - Wer darf welche Werte initialisieren/hinzufügen

## Verschiedene Administration

- gq lokal
- My LDAP Klient
- LAM (Web)
- Web2LDAP (Web)
- Eigene Tools (Web, PHP/Perl, Kommandozeile)

# Wer soll darauf zugreifen? Und wie?

### 3. User? (Selfdelegated Administration)

- Meist geeignetes Webtool zur Selbstadministration
- Einfacher Aufbau und Zugriff, **aber abgesichert weil Sicherheitslücke!**
- Festlegen der Werte, welche ein User ändern darf
  - Passwort
  - privates Telefon
  - Mobiltelefon
  - vergessenes Passwort (via Kontrollfragen)
  - Eingabe von Kontrollantworten

## User Selbstadministration

- LAM (Web)
- Web2LDAP (Web)
- Eigene Tools (Web, PHP/Perl, Kommandozeile)

## Directories:

- OpenLDAP
- Fedora Directory Server
- ApacheDS

## Tools:

- Webbasiert (PHP): LDAP Admin, GOsa, LAM (LDAP Account Manager), Node
- Lokal (Gnome/KDE): qt, My LDAP klient
- Kommandozeile: Idapadd, Idapmigrate, Idapdelete und PERL Scripte

## IAM Projekt Planung

- Businessprozesse definieren
- Funktionsumfang festlegen
- Autoritäten (Zugriff / Änderung) planen
- Synchronisationsmöglichkeiten planen
- Pflichtenheft erarbeiten
- **Erst danach Auswahl von Directory und Tools!!!**

### Fall Kanton Solothurn:

- 2000 User
- schrittweise Ablösung einer NT Domäne
- Aufbau mehrerer Services, die auf den Directory Server zugreifen
- Mehrere Abteilungen mit verschiedenen Anforderungen
- Bereitstellung von Zusatzinformation für Clients und Applikationen
- Replikation über mehrere Standorte (Performance und Ausfallsicherheit)

- Durch die Synchronisationsmöglichkeiten mit dem NT PDC ist der FDS die erste Wahl (Killerkriterium). Ein vorheriger Versuch dieses durch die Kombination OpenLDAP/Samba abzubilden ist gescheitert.
- Weiter ist die 4 Wege Master-Master-Replikation des FDS ein weitere Grund gewesen. Dadurch konnte an mehreren Standorten (momentan 2) eine Masterreplika aufgestellt werden.
- Setup eines Administrationstools für die Administratoren entfällt durch das integrierte GUI (Adminkonsole)
- Für die Helpdeskmitarbeitete wurde der LAM ausgewählt, weil er ausreichende Funktionalitäten liefert und sich die Oberfläche (PHP) anpassen lässt.

## Wir optimieren Ihren Business Prozess

Weitere Fragen...

Rufen Sie uns an unter +41 61 751 72 78  
oder senden Sie uns eine E-Mail [info@hvc.ch](mailto:info@hvc.ch)