Samba-Workshop

Ziele

- SMB Grundlagen

- Komponenten kennenlernen

- verschiedenen Passwort-Datenbanken anbinden

- Anbindung an andere Systeme

Ablauf

- Dauer: rund eine Stunde

- bei Bedarf mit einer Pause

- Diskussion und Fragen erwünscht

Manuel Schneider

- Fachinformatiker (Systemintegration)

- andere Betriebssysteme:

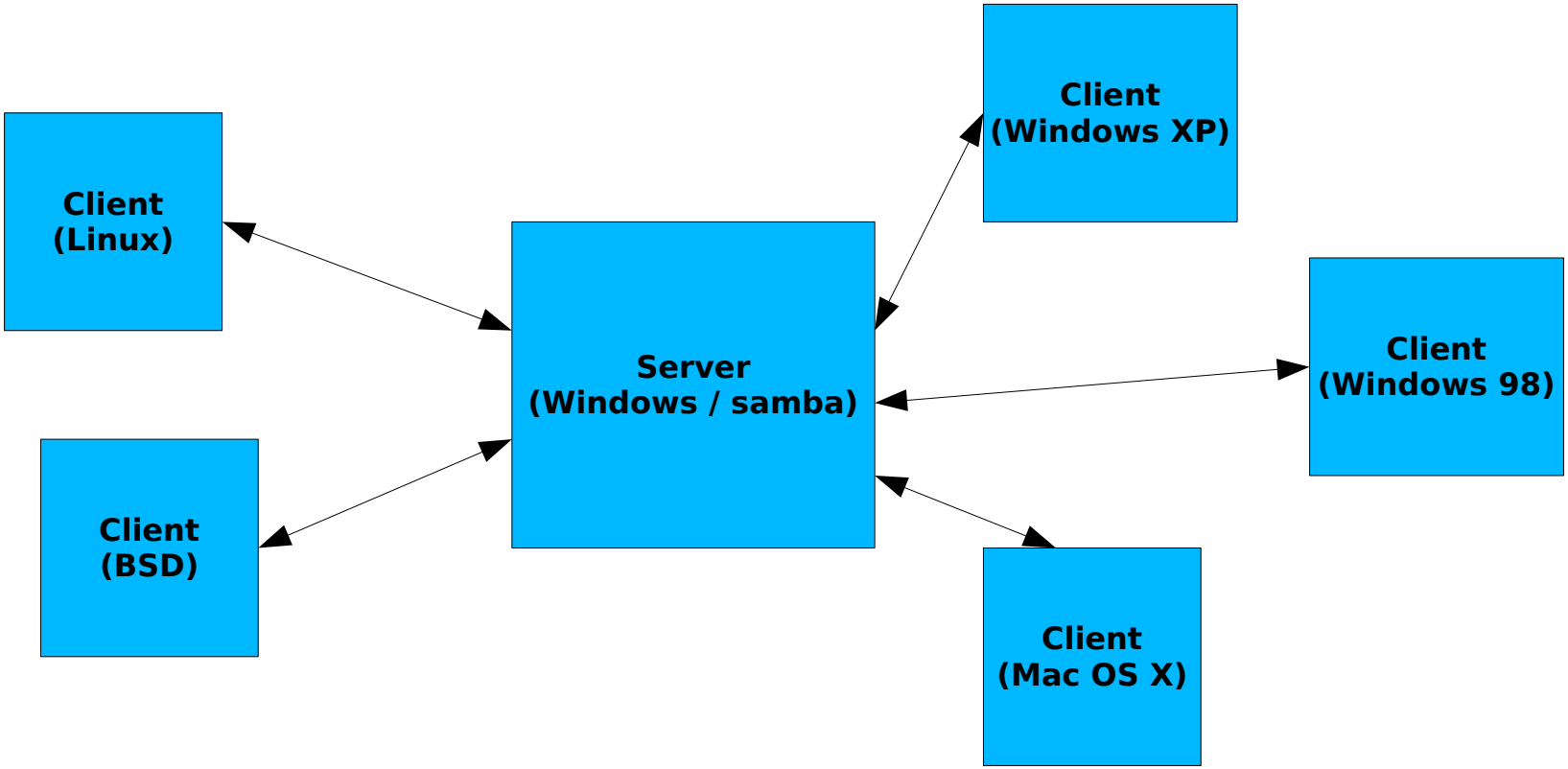
- FreeBSD

- Solaris

- Mac OS X / OpenDarwin

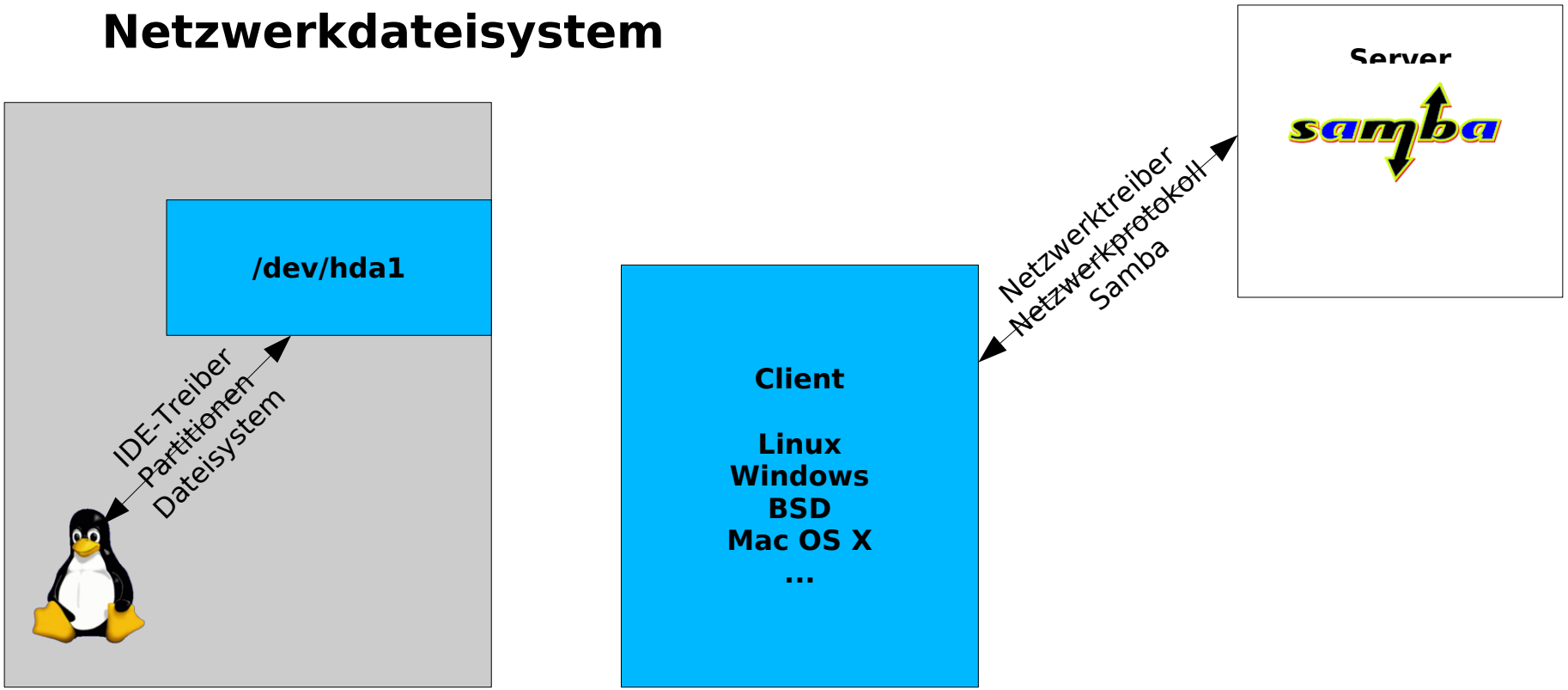
Grundlagen

die Verbindung zwischen Windows und UNIX



Grundlagen

Netzwerkdateisystem



Grundlagen

Begriffe:

- **Freigabe / Share: Verzeichnis auf welches zugegriffen werden kann**

- **Workgroup: Gemeinsames SMB-Netzwerk**

- **Domäne: Geschlossenes SMB-Netzwerk**

Grundlagen

samba <-> SMB

- SMB: Protokoll zum Dateiaustausch (und vielem mehr)

- samba: SMB-Server für UNIX

- smbfs: Kernelmodul zum Zugriff auf Freigaben ("Treiber")

- smbclient: Werkzeuge zum Zugriff auf SMB-Netzwerke

SMB-Komponenten:

- SMB (Server Message Block) - Dateiaustausch

- NMB - Namensauflösung via NetBios

- WINS (Windows Name Service) - Namensauflösung

- Active Directory - Benutzer- und Passwortverwaltung

Benutzer- und Passwortverwaltung:

- **PAM**
- **smbpasswd**
- **LDAP**
- **Kerberos**
- **MySQL**

Das SMB-Protokoll:

- jeder Rechner meldet sich per Broadcast

- beteiligte Rechner führen Listen (Browser)

- Wahl eines Masterbrowsers

- Namensauflösung NMBD / WINS vs. DNS

Die SMB-Architektur:

- SMB als Workgroup-Server

- SMB als Domain-Controller (primär - PDC)

- SMB als Domain-Controller (Backup - BDC)

- SMB als Domain-Member-Server

smb.conf

```
[Global]
  workgroup = EXAMPLE
  netbios name = server
  interfaces = eth0
  printcap name = cups
  printing = cups
  load printers = yes
  encrypt passwords = yes

[homes]
  valid users = %S
  writeable yes
  browseable = no

[cdrom]
  path = /mnt/cdrom

[public]
  path = /mnt/data
  writeable = yes
```

SMB als Workgroup-Server:

- SMB führt eine eigene Benutzerdatenbank

- Berechtigungen bzgl. User oder Freigaben

- jeder Rechner im Netzwerk ist gleichberechtigt

SMB als Domain-Controller (primär - PDC):

- der Server ist der "Chef" im Netzwerk

- der PDC verwaltet zentral alle Benutzer für alle Clients

- Berechtigung auf Benutzerebene

- üblicherweise Masterbrowser

SMB als Domain-Controller (Backup - BDC):

- erhält Benutzerdatenbank von seinem PDC

- verhält sich wie ein PDC

SMB als Domain-Member-Server:

- arbeitet wie ein Workgroup-Server

- Berechtigungen auf Benutzerebene

- keine besondere Rolle in der Domäne

Active Directory

Funktionen:

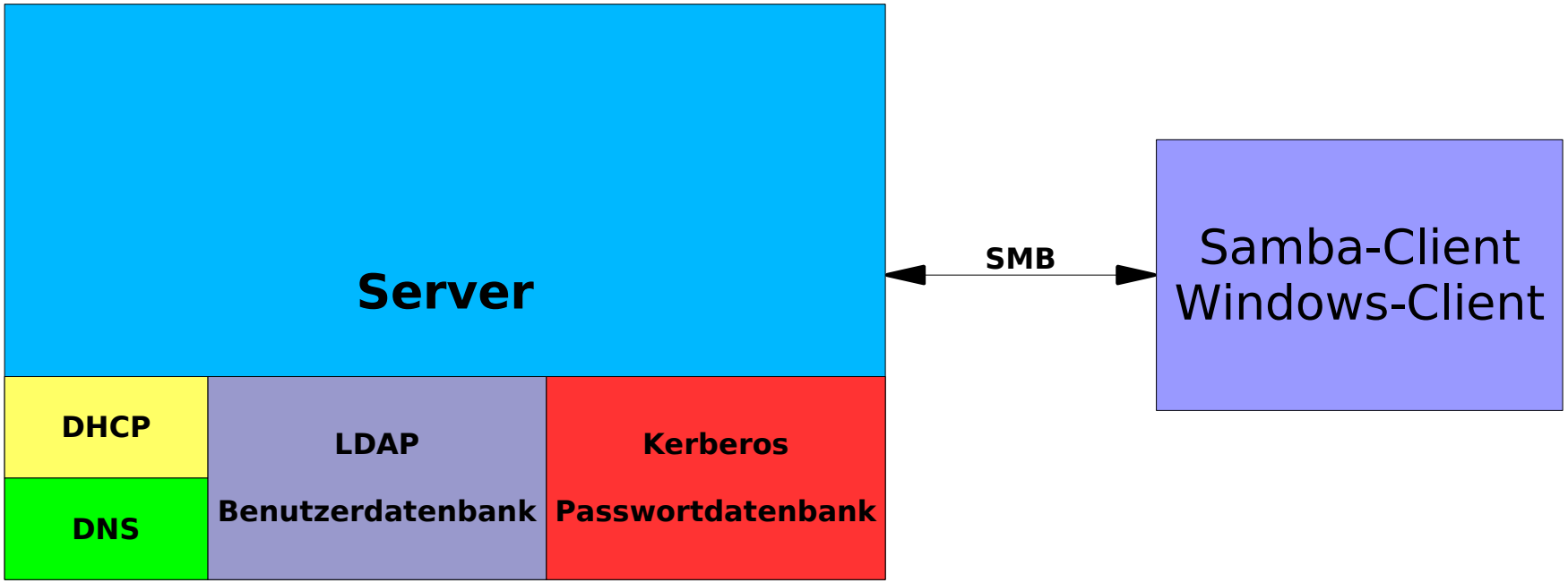
- zentrale Benutzerverwaltung

- zentrale Passwortverwaltung (Single Sign On)

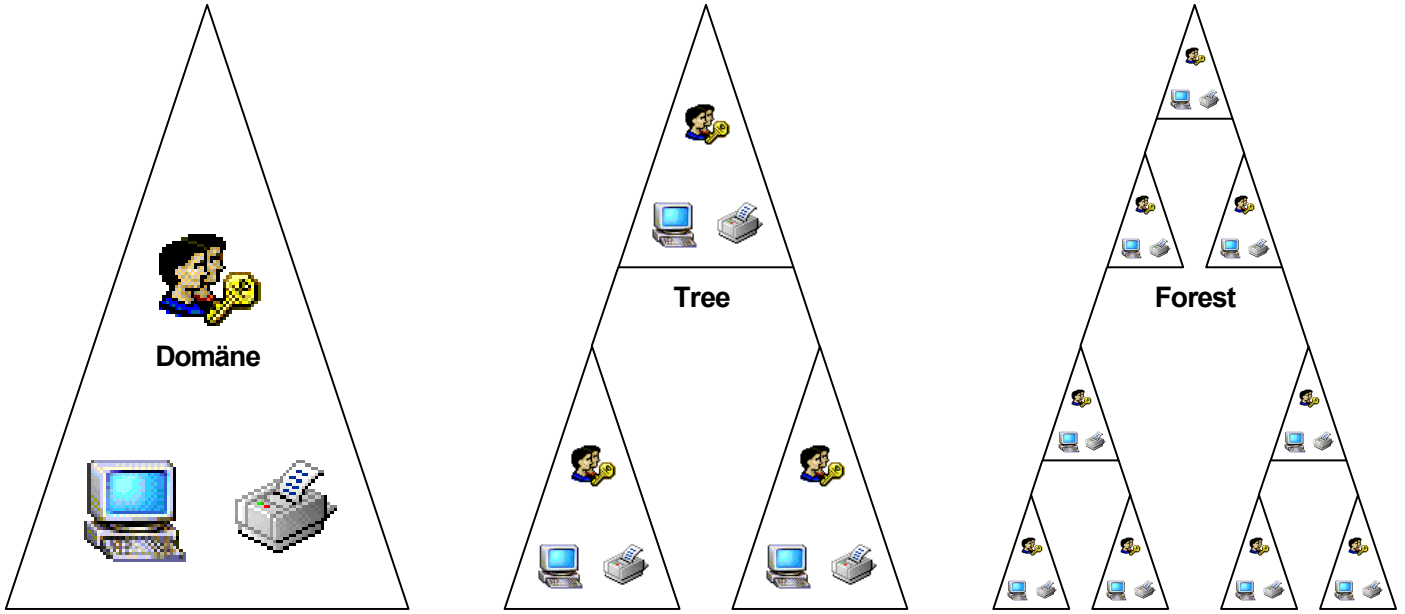
- benötigt für PDC und BDC

- benötigt ausserdem DNS und DHCP

Active Directory



Active Directory



Active Directory

Anbindung an Samba:

- winbind

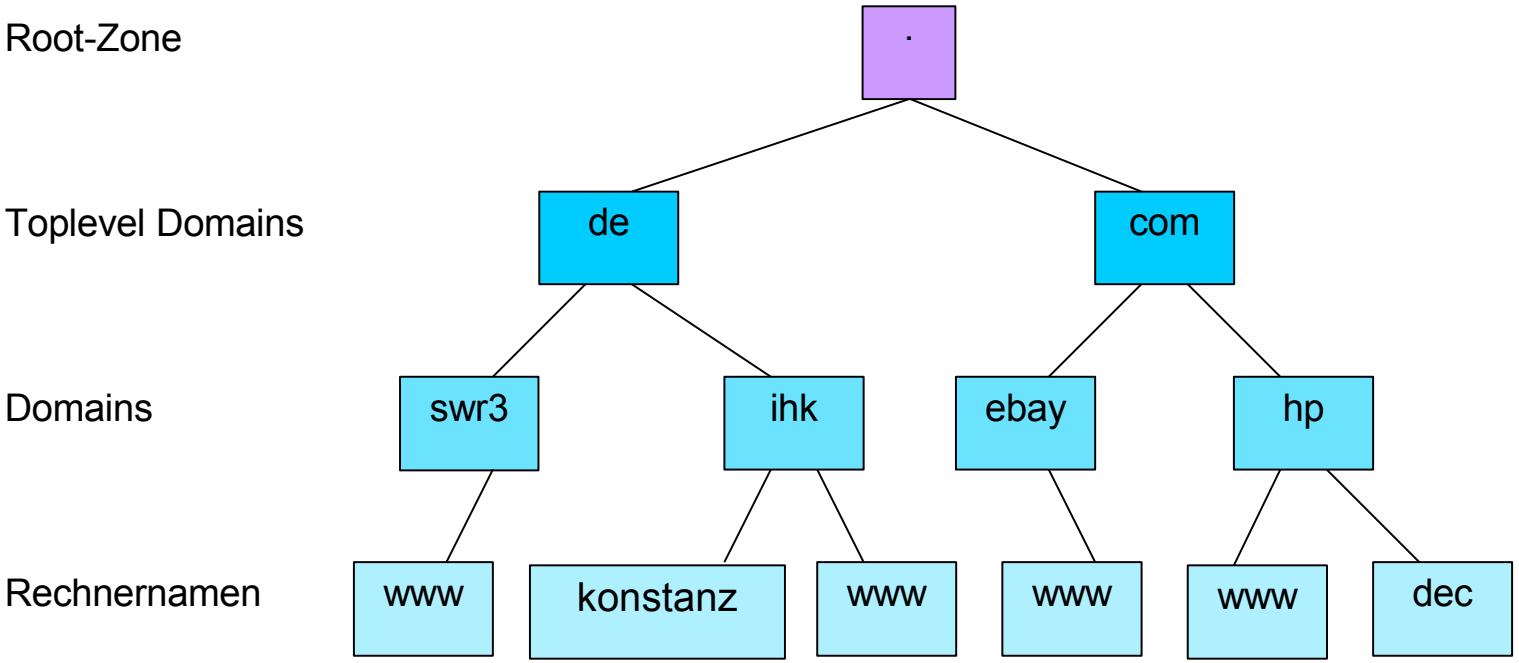
- dynamische Erzeugung von Home-Verzeichnissen

- kann als NSS und PAM-Modul genutzt werden

- erledigt die Anbindung über LDAP und Kerberos

LDAP

Hierarchisches System - Beispiel DNS



LDAP

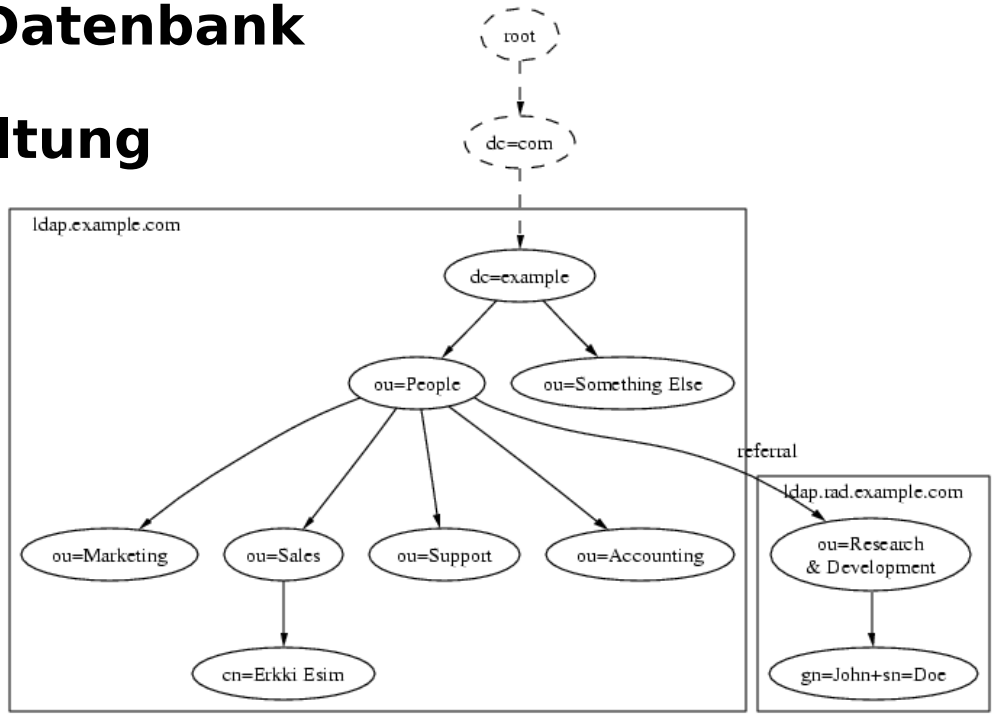
LDAP - objektorientierte Datenbank

- Zentrale Benutzerverwaltung

- SSO – Single Sign On

- Active Directory

- Globale Adressbücher



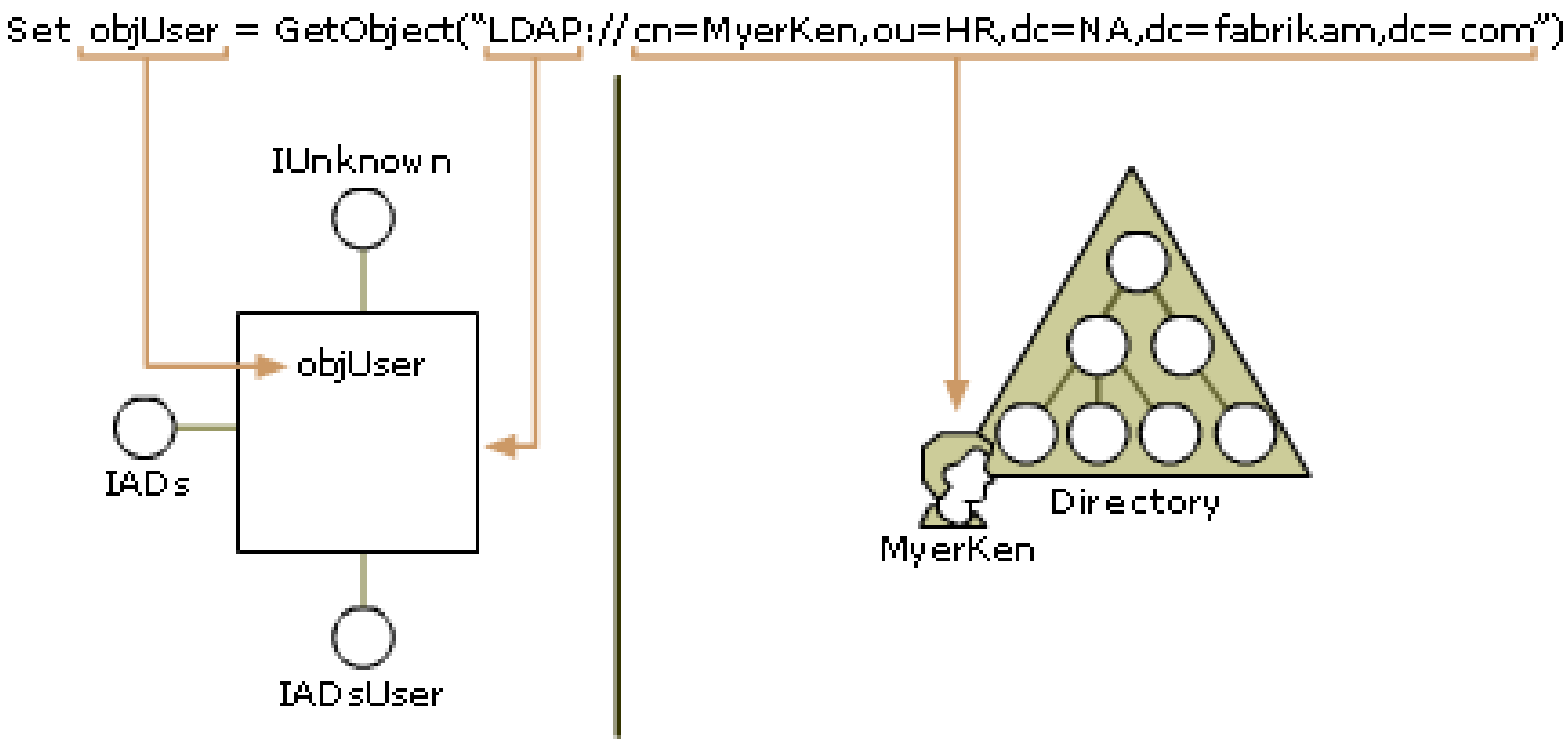
LDAP

Hierarchisches System - Beispiel DNS

- Root-Zone

- Delegationen

Active Directory



LDAP

```
dn: o=structure-net,c=de
objectclass: organization
objectclass: top
o: Structure Net
l: Hamburg
postalcode: 21033
streetadress: Billwiese 22

dn: ou=Sales, dc=structure-net, dc=de
objectclass: organizationalunit
ou: Sales
description: Verkauf
telephonenumber: 040-7654321
facsmiletelephonenumber: 040-7654321

dn: ou=Development, o=structure-net, c=de
objectclass: organizationalunit
ou: Development
description: Verkauf
telephonenumber: 040-7654321
facsmiletelephonenumber: 040-7654321

dn: ou=Support, o=structure-net, c=de
objectclass: organizationalunit
ou: Support
description: Verkauf
telephonenumber: 040-7654321
facsmiletelephonenumber: 040-7654321
```

LDAP

Authentifizierung

- pam_ldap / nss_ldap

- direkte Anbindung an samba ldap-backend

LDAP

Verwaltung

- phpldapadmin

- Kommando-Zeile (ldapadd, ldapsearch, ldapmodify...)

- gq

- Module für Perl, Ruby, Java...

Kerberos

Single Sign On

- Tickets

- Authentifizierung von Server, Clients und Diensten

- GSSAPI zum Austausch der Credentials

- pam_krb5

MySQL

relationale Datenbank

- pam_mysql / nss_mysql
- direkte Anbindung an samba mysql-backend
- auch PostgreSQL möglich

Abschluss

Literatur-Empfehlungen:

- samba für Unix/Linux-Administratoren
Volker Lendecke, dpunkt.verlag

- LDAP verstehen, OpenLDAP einsetzen
Dieter Klünter, Jochen Laser, dpunkt.verlag