

# Windows Active Directory

## Sicherheitstage WS 2005/2006

Hergen Harnisch

`harnisch@rrzn.uni-hannover.de`

30.11.2005

1. Einführung / Nutzerdatenbank
2. Active Directory
3. Alternativen zu Active Directory
4. Anhang: Literatur, Sicherheitstipps zu 2003

## Nutzerverzeichnis in Form einer Liste

- Keine Anordnung / Abhängigkeit zwischen Einträgen
- Zusammenfassungen durch Gruppen (ebenfalls Liste)

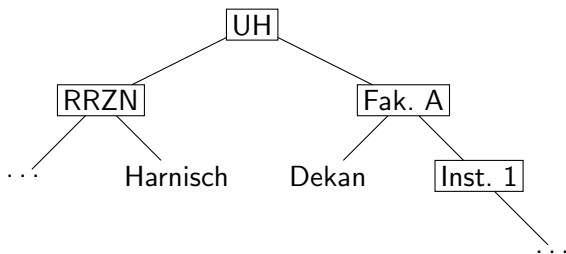
## Findet Anwendung bei

- Windows NT 4.0 Domäne
- lokale Benutzer unter Windows
- /etc/passwd & /etc/groups unter Unix
- Novell-Bindery (bis Netware 3.12)

## Vor-/Nachteile:

- einfach zu verstehen und zu implementieren
- skaliert nicht: unübersichtlich, keine Delegation

## Beispiel



Nutzerverzeichnis in Form eines Baumes

## Nutzerverzeichnis in Form eines Baumes

- hierarchische Anordnung und Abhängigkeit
- Abbildung einer (streng hierarchischen) Organisationsstruktur
- natürliche Zusammenfassungen nach Teilbäumen, zusätzlich Gruppen
- Vererbung von Rechten und Eigenschaften möglich
- Attribute, z.B. Rechte am Baum im Baum selbst abgelegt

## Findet Anwendung bei

- Windows Active Directory (ab Windows 2000)
- unter Unix z.B. mit LDAP
- Novell: NDS / eDirectory (seit Netware 4)
- Zertifikatsverwaltung: X.500

1. Einführung / Nutzerdatenbank
2. Active Directory
3. Alternativen zu Active Directory
4. Anhang: Literatur, Sicherheitstipps zu 2003

Ein Active Directory ist mehr als ein einfacher Baum:  
„Sammlung von Bäumen von Bäumen“.

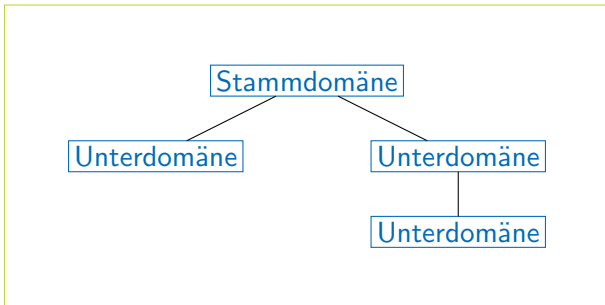
Absteigend im Sinne von „umfasst“:

- Gesamtstruktur
- Struktur
- Domäne
- Organisationseinheit
- Objekt:  
Benutzer, Computer, ...



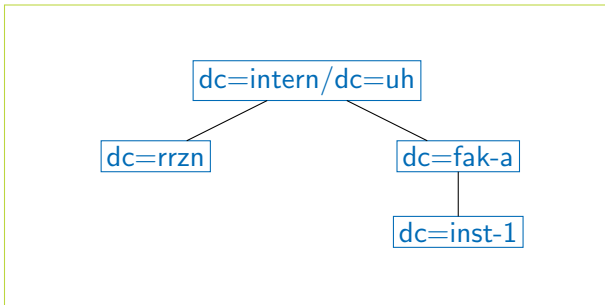
## Struktur (Baum, *tree*)

- ein Baum von Domänen, Wurzel heißt Strukturstammdomäne
- automatisch Vertrauensstellung zur übergeordneten Domäne
- gemeinsamer Namensraum (s.u. DNS)



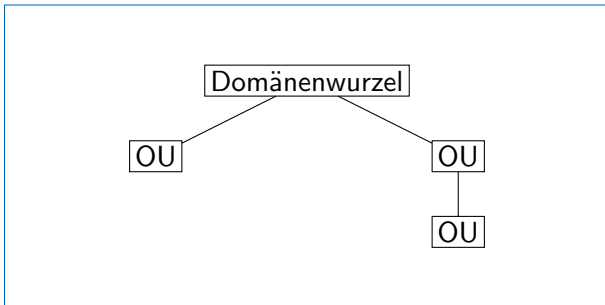
Struktur (Baum, *tree*)

- ein Baum von Domänen, Wurzel heißt Strukturstammdomäne
- automatisch Vertrauensstellung zur übergeordneten Domäne
- gemeinsamer Namensraum (s.u. DNS)



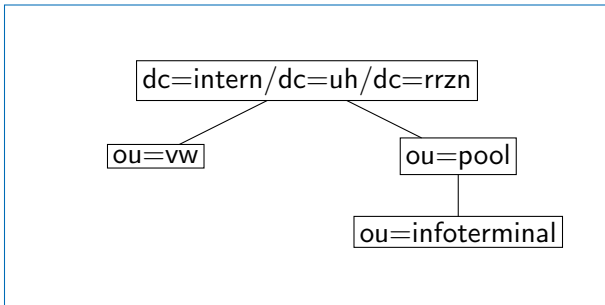
## Domäne (*domain*)

- abgeschlossenes Verzeichnis von Objekten der Domäne
- ein Baum aus Organisationseinheiten und Objekten
- ein Domänenname (s.u. DNS)



## Domäne (*domain*)

- abgeschlossenes Verzeichnis von Objekten der Domäne
- ein Baum aus Organisationseinheiten und Objekten
- ein Domänenname (s.u. DNS)



## Organisationseinheit (*OU, organizational unit*)

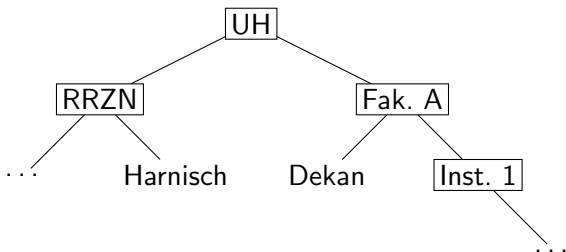
- Untercontainer einer Domäne (Knoten im Baum/Unterbaum)
- kann OU, Objekt (Benutzer, Computer, ...) enthalten

## Benutzer, Gruppe, Computer, Drucker (Objekt)

- Nicht unterteilbar, kleinste Einheit (Blätter im Baum)
- steht für eine Netzwerkressource

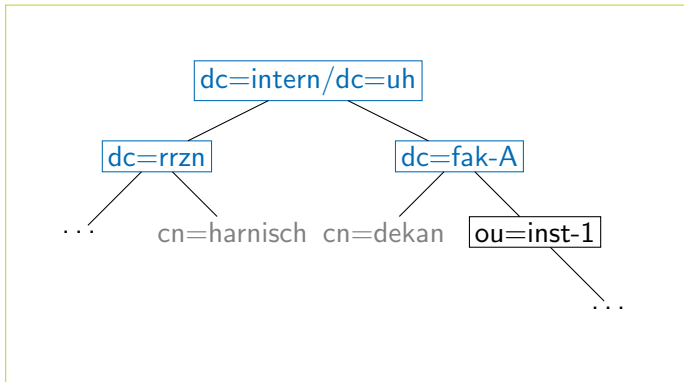
# Active Directory: Aufbau

## Beispiel



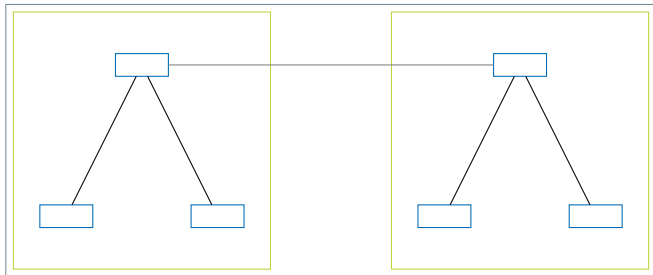
# Active Directory: Aufbau

## Beispiel



## Gesamtstruktur (Wald, *forest*)

- AD besteht immer aus 1 Gesamtstruktur
- Gesamtstruktur ist Liste von Strukturen
- keine Struktur bevorzugt, keine gemeinsame Wurzel



- häufig gleich der Struktur

## Gesamtstruktur

### Gesamtstruktur = Struktur

- einfachster Ansatz
- zentraler Eingriff in Unterdomänen durch Strukturstammdomäne, z.B. auch Richtlinien
- schwächster Domänencontroller bestimmt Gesamtsicherheit

### Gesamtstruktur $\neq$ Struktur

- meist bei späteren Zusammenschlüssen
- loser Verbund, Eigenständigkeit
- Domänencontroller der jeweils anderen Struktur wird nicht vertraut

⇒ *möglichst nur eine Struktur (=)*

## Struktur: unterteilen in Domänen oder OUs?

- jede Domäne benötigt mind. 1 Domänencontroller (DC), schwächster Domänencontroller bestimmt Gesamtsicherheit
- Domäne bietet mehr Eigenständigkeit als OU
- OU reicht für Delegation von Nutzer- und Richtlinien-Verwaltung
- Rechner an Domäne anzumelden, Standard bei Anmeldung
- (Anmelde-) Namen möglichst in Domäne eindeutig wählen
- Anwender sieht Domänen-Baum, nicht aber OU-Baum

⇒ *möglichst nur eine Domäne*

## Benennung von Objekten im AD

**DN** *distinguished name*, eindeutiger Name:  
wie bei X.500 vollständiger Pfad:  
dc=intern/dc=uh/dc=rrzn/cn=Hergen Harnisch

**RDN** *relative DN*:  
letzter Namensteil (meist Vor- & Zuname):  
Hergen Harnisch

**GUID** *global unique identifier*:  
interne 128Bit-Zahl, automatisch vergeben

→ **UPN** *user principal name*, Benutzerprinzipalname:  
Benutzeranmeldename & Domain in E-Mail-Syntax:  
harnisch@rrzn.uh.intern

- RDN muss nicht eindeutig sein
- i.Allg. RDN  $\neq$  Benutzeranmeldename,  
Benutzeranmeldename  $\neq$  Prä-2k-Name möglich

## Active Directory: Namen

## Beispiel für Namen beim Anlegen

Neues Objekt - Benutzer

Erstellen in: sht2005.intern/RRZN

Vorname: Hergen Initialen:

Nachname: Harnisch

Vollständiger Name: Hergen Harnisch

Benutzeranmeldename: harnisch @sht2005.intern

Benutzeranmeldename (Prä-Windows 2000): SHT2005\ harnisch

< Zurück Weiter > Abbrechen

Domäne OU

RDN

UPN

DN: dc=intern/dc=sht2005/ou=RRZN/cn=Hergen Harnisch

AD-Domänenname wird über DNS-Protokoll aufgelöst,  
über DNS-Subdomänen Suche des DC etc. (ersetzt WINS)

## Integration in bestehendes DNS

- lokalen AD-Domännamen  $\neq$  DNS-Namen wählen  
Vorschlag in UH: *Inst.Kürzel.intern*
- Windows-Server (meist DC)
  - als (alleiniger) DNS-Server für Windows-Clients
  - autorisierend für DNS-Zone mit AD-Domännamen
  - andere Anfragen an UH-DNS-Server weiterleiten

## Warnung

- ohne passendes DNS geht AD nicht
- DNS ist fundamental  $\implies$  Sicherheitsprobleme,  
falsche DNS-Konfiguration legt Internetzugriff lahm

## DNS-Subdomänen im AD

The screenshot shows the Windows DNS console window titled "dnsmgmt - [DNS\WINSERVH\Forward-Lookupzonen\sht2005.intern]". The left pane displays a tree view of the DNS hierarchy under "WINSERVH", with "Forward-Lookupzonen" expanded to show the "sht2005.intern" zone. The right pane shows the configuration for this zone, listing 9 entries in a table.

Name	Typ	Daten
_msdcs		
_sites		
_tcp		
_udp		
DomainDnsZones		
ForestDnsZones		
(identisch mit übergeordnete...)	Autoritätsursprung (SOA)	[23], win...
(identisch mit übergeordnete...)	Namenserver (NS)	winservh...
winservh	Host (A)	130.75....

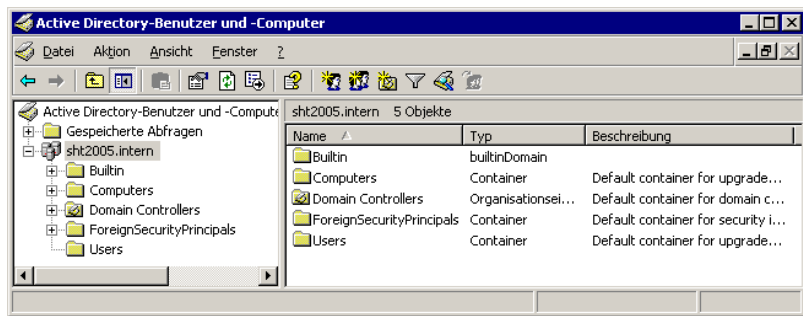
## DNS-Möglichkeiten

weitere, nicht zu empfehlende Möglichkeiten:

- AD-Domäne = DNS-Domäne mit extra bind-Server  
*Problem:* autorisierende für gleiche Zone, gegen rfc
- AD-Domäne = DNS-Domäne mit MS-DNS-Server  
*Problem:* häufige Zonen-Transfers wg. dynamischer DNS-Updates
- DNS mit bind verwaltet, akzeptiert dynamische Updates  
*Probleme:*
  - häufige Zonen-Transfers wg. dynamischer DNS-Updates
  - Sicherheitsproblem wg. Inkompatibilität von TSIG
  - entweder komplett dynamische Zone (Servereinträge änderbar),  
oder Subzones könnten sich ändern (nur \*-Subzones dyn.)

# Active Directory: Standard OUs

## automatisch generierte OUs



**D.C.** Domänencontroller der Domäne

**F.S.P.** Security-IDs vertrauter (anderer) Domänen

**Builtin** vordef. feste Gruppen für Netz-/VW-Aufgaben

**Comp.,Users** ... wenn nicht in anderer OU (z.B. bei Migration)

### 3 Arten von Gruppen

Gruppenbereich	Mitglieder (neben Benutzern)	Wirkung
universal	univ. & glob. Gruppen	AD
global	glob. Gruppen derselben Dom.	AD
lokal	univ. & glob. Gruppen, lok. Gruppen derselben Domäne	Domäne

- universale Gruppen vermeiden
- lokal heißt hier bzgl. Domäne,  $\neq$  lokal Arbeitsplatz
- Verfügbarkeit, Eigenschaften eingeschränkt bei gemischter Funktionsebene (s.u.)

## Empfehlung für Gruppenverwendung: A G DL P

Vorgehensweise:

1. Benutzer (*account*) in **g**lobale Gruppe
  2. globale Gruppe in **d**omänen-**l**okale Gruppe
  3. der lokalen Gruppe Rechte (*permissions*) geben
- *best practise* Empfehlung  
(u.a. gut für Domänenwechsel)
  - nur relevant bei mehr als einer Domäne

Es gibt 3 verschiedene (Domänen-) Funktionsebenen

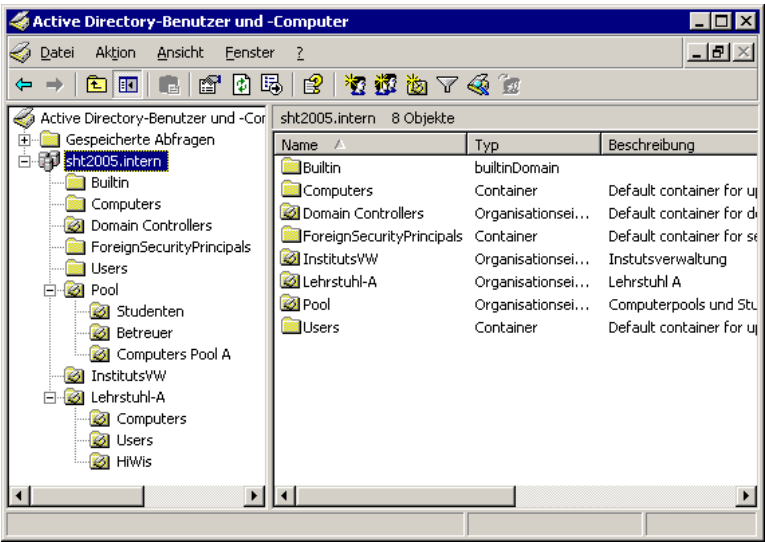
1. *Windows 2000 gemischt*  
Replikation mit NT4.0-DC möglich
2. *Windows 2000 pur*  
alle Server sind mind. Windows 2000
3. *Windows Server 2003*  
alle Server sind Windows Server 2003

... bezieht sich nur auf Domänencontroller, nicht Clients.

- Hochstufen geht, runter nicht
- Windows Server 2003 anzustreben:  
größte Sicherheit
- *unabhängig davon*: auch Clients auf  $\geq 2000$ :  
NetBios, Wins vollständig deaktivierbar

## kleines Netz

- Globalstruktur = Struktur = Domäne
- vordefinierte OUs lassen, eigene dazu
- mit OUs strukturieren: Delegation, verschiedene Richtlinien  
→ *OUs hilfreich, nicht vor Anlegen zurückschrecken*
- separate Unter-OUs für Computer, Benutzer
- neben OUs auch Gruppen (für Verzeichnisrechte)



1. Einführung / Nutzerdatenbank
2. Active Directory
3. Alternativen zu Active Directory
4. Anhang: Literatur, Sicherheitstipps zu 2003

## Warum Alternativen?

- Komplexität
  - Schulungs- und Einarbeitungsaufwand
  - ohne grundlegendes Verständnis: Sicherheitsproblem
- heterogene Rechnerumgebung

## mögliche Alternativen

- Unix-Rechner mit Samba
- Novell-Netware
- nur lokale Windows-Nutzer
- (Ausblick: pGINA)

für Terminal-Server etc. bleibt Windows-Server (ohne AD)

- Nutzerverwaltung, File- und Printservices, ggf. mehr
- Gute Unterstützung der TCP/IP-Protokolle & Dienste und heterogener Umgebungen
- Open-Source: keine Anschaffungskosten, keine Client-Lizenzen
- verhält sich wie NT4.0-Domänencontroller
- Migration von NT4.0-Domäne möglich und gut dokumentiert, Übernahme von NT4-Usern mit Passwörtern möglich
- NT4-Richtlinien und serverbasierte Profile
- serverseitig dynamische Login-Skripte und Profile
- Nutzerverwaltung in DB (flach) oder LDAP (hierarchisch)
- ACL: Unix-ACL oder innerhalb von Samba als DB

## RRZN-Unterstützung

Herr Obendorf (Tel. 19078), Herr Froiep (Tel. 4721), Anleitung folgt

- Nutzerverwaltung, File- und Printservices
- offener gegenüber Linux, MacOSX (vgl. eDirectory)
- ausgereifter Verzeichnisdienst,  
OUs als Gruppen verwendbar (z.B. File-Rechte),  
CNs müssen nur je OU eindeutig sein
- ggf. extra Windows-Server nötig (z.B. Terminalserver)

- File- und Printservices
- Benutzerverwaltung wie in XP (flach), einfach
- nur lokal, sinnvoll bei nur einem (File-/Terminal-) Server;  
*quick & dirty*, skaliert nicht
- keine Domäne, daher keine zentralen Richtlinien
- Arbeitsgruppe statt Domäne
- ggf. keine Server- & Clientaccess-Lizenzen nötig

## portable GINA

GINA = **G**raphical **I**dentification a**N**d **A**uthentication

- ersetzt (von MS dokumentierten) Anmeldeprozess
- mögliche Anbindung u.a. an
  - Unix-PAM (Anbindung an „Unix-PAM-Server“)
  - LDAP
  - Pop3
  - NIS
- keine praktischen Erfahrungen, experimentell?

### Warnung

benötigt ausgiebige Tests vor Einsatz, derzeit abzuraten

<http://pgina.xpasystems.com/>

1. Einführung / Nutzerdatenbank
2. Active Directory
3. Alternativen zu Active Directory
4. Anhang: Literatur, Sicherheitstipps zu 2003

## zu Windows Server 2003 und AD

- RRZN-Handbuch Windows-Server 2003 Basis/Admin
- RRZN-Handbuch Windows-Server 2003 Migration
- Larisch, Active Directory Services, Galileo Press 2003
- Installationsleitfaden für W2K3 in der UH auf RRZN-Seite  
<http://www.rrzn.uni-hannover.de/1687.html>

## allgemein

- BMI: Migrationsleitfaden, Schriftenreihe KBSt Nr. 72  
<http://www.kbst.bund.de/Software/- ,223/Migration.htm>

## Samba

- Samba-Dokumentation auf <http://www.samba.org/>

## Installation

- offline installieren, möglichst SPs schon auf CD-Rom  
aktuelles CD-Image evt. durch *slipstreaming* herstellen
- mit aktiver Firewall (ab SP1) ans Netz, sofort Updates
- ...

## Betrieb

- Sicherheitskonfigurations-Assistent  
laufende Dienste & offene Ports anzeigen, prüfen  
ab SP1, als Windows-Komponente nachinstallieren  
vgl. GWDG-Nachrichten 07/2005
- Remote-Desktop nur mit SSL verwenden (ab SP1)  
vgl. GWDG-Nachrichten 11/2005
- ...