Michael Flachsel

Active Directory

Allgemeiner Aufbau & Struktur an der TUB

6. Juni 2007

Agenda

- Motivation
- Grundlagen
- TU-Windows Konzept
- Vorhandene Umgebung

Warum Active Directory

Inhalt
Motivation
Grundlagen
Konzept
Umgebung

Ca. 2000

Ca. 6000*

- Einheitliches Management
- Einheitliche Benutzerverwaltung
- Einheitliche Softwareverteilung

- Anbindung an bestehende Systeme

*Quelle: NOC Recherche nach gemeldeten Typen

Was ist das AD I

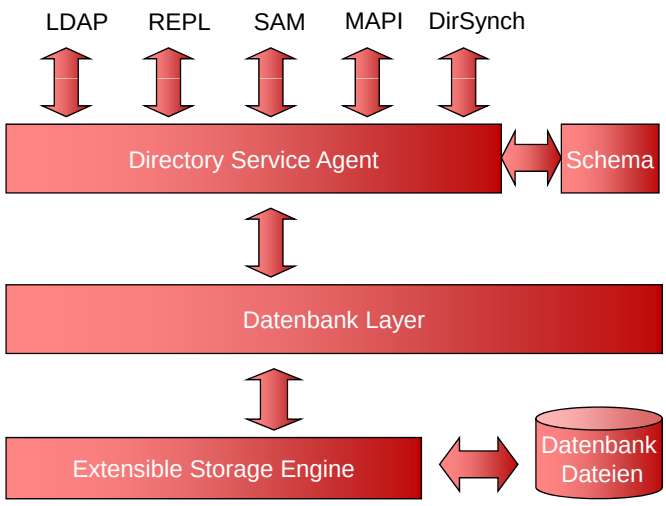
Inhalt
Motivation
Grundlagen
Konzept
Umgebung

- Verzeichnisdienst abgeleitet von X.500
- Angeordnet in Baum-Struktur
- enthält alle Informationen über
  - Netzwerk
  - Anwender
  - Computer
  - Applikationen
- In Datenbank, die
  - Erweiterbar
  - schnell Recherchierbar
  - verteilt
  - mit offenen Schnittstellen (LDAP, KRB)

Was ist das AD II

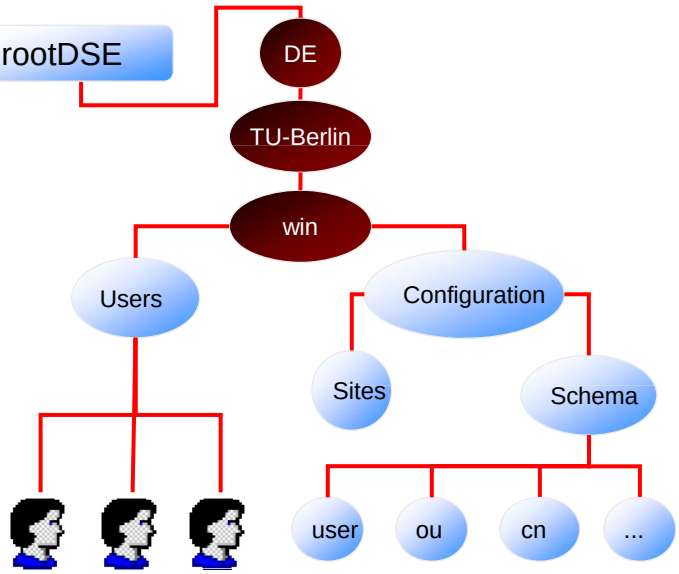
- Besteht aus mehreren Komponenten
  - Verzeichnis
  - Schema
  - Replikation
  - Global Catalog
  - Sicherheitskonzept

Interner Aufbau I



Interner Aufbau II

Inhalt
Motivation
Grundlagen
Konzept
Umgebung



Multi Master

Inhalt
Motivation
Grundlagen
Konzept
Umgebung

- Das AD arbeitet nach dem Multi Master Prinzip mit loser Konsistenz und Konvergenz:
  - Da an jedem Domänencontroller Änderungen stattfinden können (Multi Master), wird eine Konsistenz zum Zeitpunkt X nicht garantiert. (Lose Konsistenz)
  - Nach einer gegebenen Zeit ist garantiert, dass durch Replikation alle Domänencontroller identische Inhalte haben (Konvergenz)

Objekte im AD

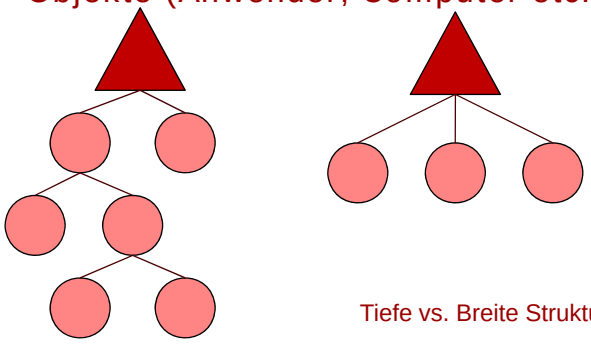
- Das AD enthält Objekte
- Jedes Objekt ist von einer Objektklasse abgeleitet, die seine Attribute definiert
- Hierarchisch gegliedert durch Container
- Ansprechbar über eindeutigen Pfad
- Zugriffe durch ACL für jedes Objekt einstellbar
- Beispiel:
  - Anwender
  - Computer
  - Drucker
  - Freigaben

Strukturen

- Die logische Struktur des AD bilden
  - Domänen
  - Organizational Units (OUs)
  - Tree
  - Forest
- Die Domäne bildet eine Sicherheitsgrenze des Active Directory
  - Skalierbar (>1 Mio. Objekte)
  - Ist Container für Objekte oder weitere Container
  - Muss mit einem gültigen DNS Namen benannt werden
  - Entspricht NT4 Domäne für Downlevel Clients

Domänen strukturieren

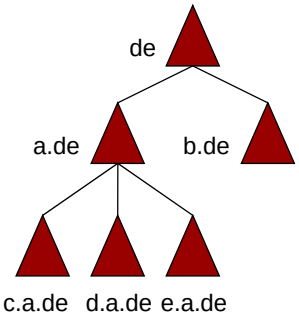
- Durch den Einsatz von Organizational Units (OUs) kann innerhalb einer Domäne eine Hierarchie aufgebaut werden
- OUs sind die primären Container für Objekte (Anwender, Computer etc.)



Tiefe vs. Breite Struktur

Tree

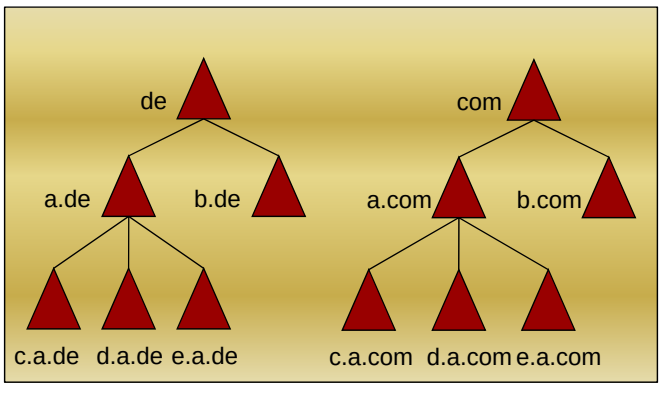
- Ein Tree ist eine Zusammenfassung von Domänen
- Alle Domänen müssen dem gleichen DNS Namespace angehören
- Alle Domänen besitzen das gleiche Schema des Active Directories



Forest I

- Ein Forest verbindet mehrere Trees
- Äussere Grenze des Schemas
- Vorteile
  - Trees mit unterschiedlichen DNS Namespaces können administrativ verbunden werden
  - Über den GC kann im gesamten Forest gesucht werden
- Mehrere Forests sind nur nötig, falls:
  - Verschiedene Schemata notwendig sind
  - Mindestens eine Domäne völlig unabhängig sein muss
  - Adminstration muss autonom sein

Forest II



FSMO Rollen

- Forest
  - Schema-Master
    - Enthält das Schema
    - Änderungen können nur hier vorgenommen werden
  - Domain-Name-Master
    - Enthält die Liste aller zum Forest gehörenden Domänen
- Domain
  - RID-Pool-Master
    - Verwaltet für SID nötige RID (Relative ID)
  - PDC Emulator
    - Für NT4 kompatiblen (Mixed-Mode) Modus nötig
  - Infrastruktur Master
    - Prüft Konsistenz von Objekten (darf kein GC Server sein)

AD an der TUB I

- Teil der AAI
- AD enthält Kopie aller Benutzer
- Gefüllt durch Import bestehender Daten aus LDAP Server
- Alphabetisch in OUs gruppiert nach Nachnamen
- Zugangsberechtigungen zu Ressourcen der jeweiligen Domain durch Gruppenmitgliedschaften
- Stammdatenänderung nur über Meta-Directory / Self-Care
- Änderung spez. Windowsattribute durch Berechtigungen an Objekt

AD an der TUB II

- Passwörter:
  - bei Import „zufällige“ Passwörter
  - später PW-Änderung über Webschnittstelle (Self-Care)
  - bei Anlegen weiterer, neuer Benutzer PW direkt gesetzt
- Computer:
  - Domaincomputer nur in den untergeordneten Domains
  - Aufnahme durch jeweilige Domain-Admins oder Enterprise-Admins

AD an der TUB III

- Schema:
  - Forestweit gültig
  - Erweiterungen:
    - Exchange 2003
    - R2
    - weitere Felder lt. LDAP Konzept
      - eduPerson
      - tubPerson
  - Verwaltung durch Schema-Admins
- Fileserver:
  - CIFS basierter Fileserver für Profildaten / Homes der Benutzer (später AFS)

AD an der TUB IV

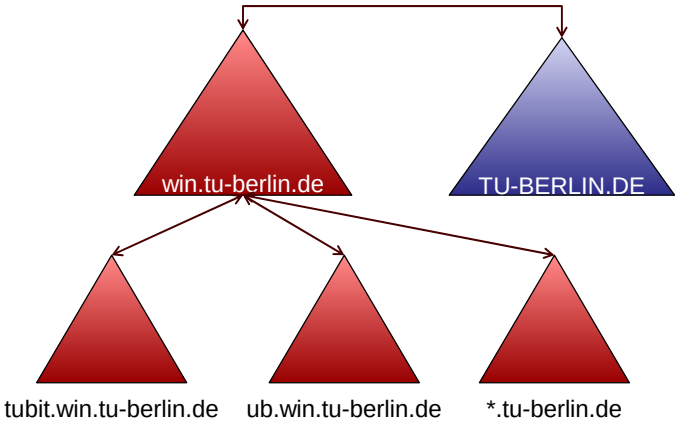
Inhalt
Motivation
Grundlagen
Konzept
Umgebung

- DNS:
  - Forward: *.win.tu-berlin über Windows DNS
  - Kein DDNS
  - Reverse: über NS von tu-berlin.de
- Exchange:
  - Server in *tubit.win.tu-berlin.de*
  - Cluster folgt später
- Weitere Dienste (im Aufbau):
  - WSUS
  - SW-Verteilung
  - ….

Logische Struktur

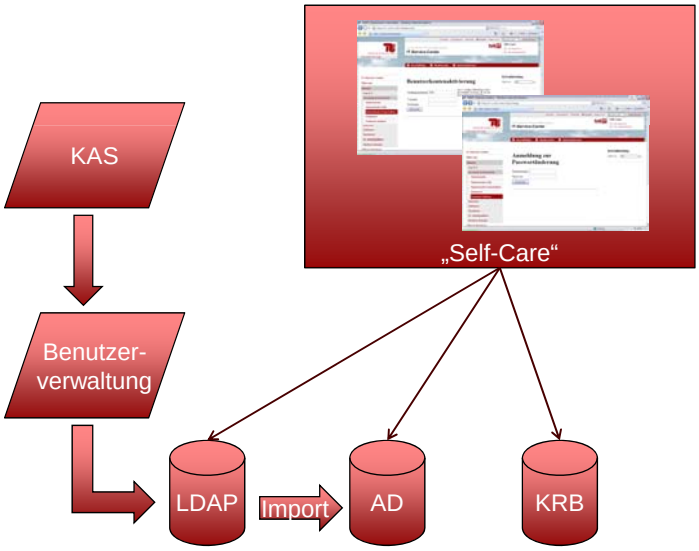
Inhalt
Motivation
Grundlagen
Konzept
Umgebung

- Single Forest, single Tree
- Cross-REALM-Trust zu TU-BERLIN.DE
- Ressource-Domain-Konzept



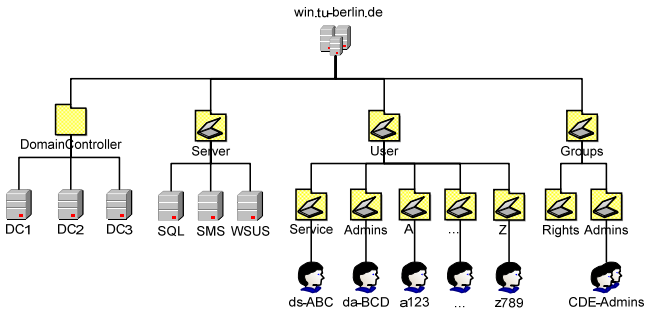
Integration des AD in tubIT

Inhalt
- Motivation
- Grundlagen
- Konzept
- Umgebung



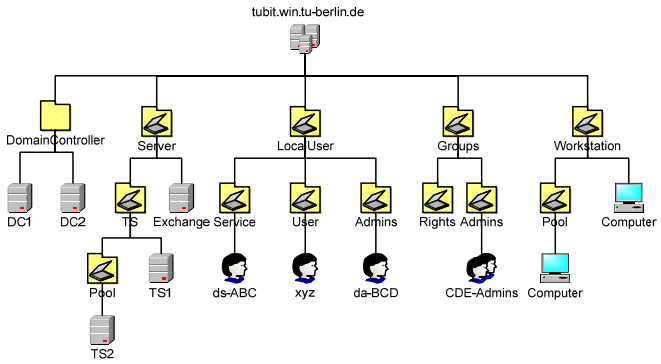
Struktur der Root-Domain

Inhalt
- Motivation
- Grundlagen
- Konzept
- Umgebung



Struktur der tubIT-Domain

Inhalt
Motivation
Grundlagen
Konzept
Umgebung



Vorhandene Umgebung

Inhalt
Motivation
Grundlagen
Konzept
Umgebung

- Domains vorhanden:
  - WIN
  - TUBIT
  - UB
- Domains geplant:
  - ZEMS
  - ZUV
- Weitere Strukturierung durch Domains für Fakultäten, danach OUs

Authentisierung / Autorisierung

Inhalt
Motivation
Grundlagen
Konzept
Umgebung

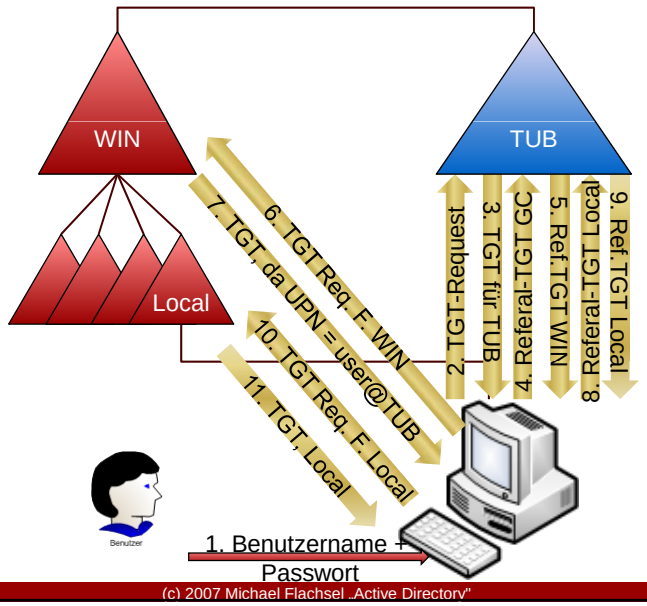
- Jedes Benutzerobjekt enthält Verweis auf KRB-Principal (altSecurityPrincipal)

  User1@win.tu-berlin.de <-> User1@TU-BERLIN.DE

- Die transitiven Trusts zwischen den Domains ermöglichen die Anmeldung
- Gruppenmitgliedschaften Global und Lokal regeln die Zugriffe
- „Loop-Back-Modus“ ermöglicht lokale GPOs an Computern, angewendet auf User

Anmeldeprozedur

Inhalt
Motivation
Grundlagen
Konzept
Umgebung



Nutzungsvoraussetzungen

- Organisatorisch:
  - Domain vorhanden (Fakultät / ZE) (oder hiermit aufgebaut)
  - 2 Administratoren benannt
  - tubIT-Nutzerkonto für alle „Betroffenen“
  - Migrationsszenario für bestehende Infrastrukturen
- Technisch:
  - Kein Hausnetz
  - Nur IPs aus 130.149.0.0, kein NAT
  - Installierte Patches / Hotfixes XP/2k3
    - KB 892090
    - KB 902336
  - Installiertes MIT Kerberos 4 Windows

ENDE

Fragen ?

Vielen Dank für die Aufmerksamkeit.