Einführung in Verzeichnisdienste

Übersicht

1. Entstehung (Historie)
2. Grundlagen, Charakteristika
3. Produktübersicht (Anbieter)

Historie

- 1988: OSI X.500 Directory Services
  - Weltweiter *white pages service* für Fax, Telefon, E-Mail
  - *name service* für OSI-Anwendungen
- 1997: light directory access protocol (LDAP)
  - University of Michigan
  - Entwicklung eines „leichten“, einfachen Protokolls für den Zugang zu Verzeichnisdaten
  - Erster LDAP-Server

Grundlagen

- Was ist ein Verzeichnis?
  - Eine strukturierte Auflistung von Informationen in einer bestimmten Reihenfolge → Telefonbuch (*white pages*)
- Welche Daten kann man im Verzeichnis erfassen?
  - Alle... ☺
    - Bevorzugt statische Daten
    - engl. *Repository* = Lager, Magazin, Depot
  - Inhalt eines Verzeichnisses:
    - Gestaltung nach eigenen Definitionen und Wünschen
    - Kombinationen von verschiedenen Arten / Typen von Informationen (Objekten) interessant

Grundlagen

- Was bietet ein Verzeichnis**dienst**?
  - Einfache Möglichkeit seine Daten zu speichern, zu organisieren und zu suchen.
  - Suchen nach Informationen aufgrund bestimmter Eigenschaften eines Objektes (Bsp: yellow *pages*)
  - Technisch:
    - Speicherung von Informationen über ein Netzwerk sowie dessen verfügbaren Ressourcen (Benutzerkonten, Server, Drucker, etc)
    - Bereitstellung dieser Informationen für Benutzer, Anwendungen und Geräte
    - Beispiel: Namensauflösung - DNS → Abbildung von Rechnernamen auf IP-Adresse

Grundlagen

- Aufbau eines Verzeichnisses:
  - Struktur:
    - Hierarchische Gliederung in Form eines Baumes
    - Zweige (= Container) beinhalten Objekte
    - Objekte sind Sammelbehälter für Eigenschaften
    - In den Eigenschaften stehen die Informationen
  - Schema:
    - Definition von Attributsklassen → Vorgabe von Wertebereichen
    - Definition von Objektklassen → Organisation definierter Attribute

Grundlagen

- Aufbau eines Verzeichnisses (Forts.):
  - Adressierung von Objekten:
    - Eindeutige Namen innerhalb eines Containers:
      relative distinguished name (RDN)
      → Beispiel: *cn=john (john)*
    - Global eindeutige Namen durch Hinzufügen des Container-Namens zum RDN:
      distinguished name (DN)
      → Beispiel: *cn=john,ou=hrz,o=tu (.john.hrz.tu)*

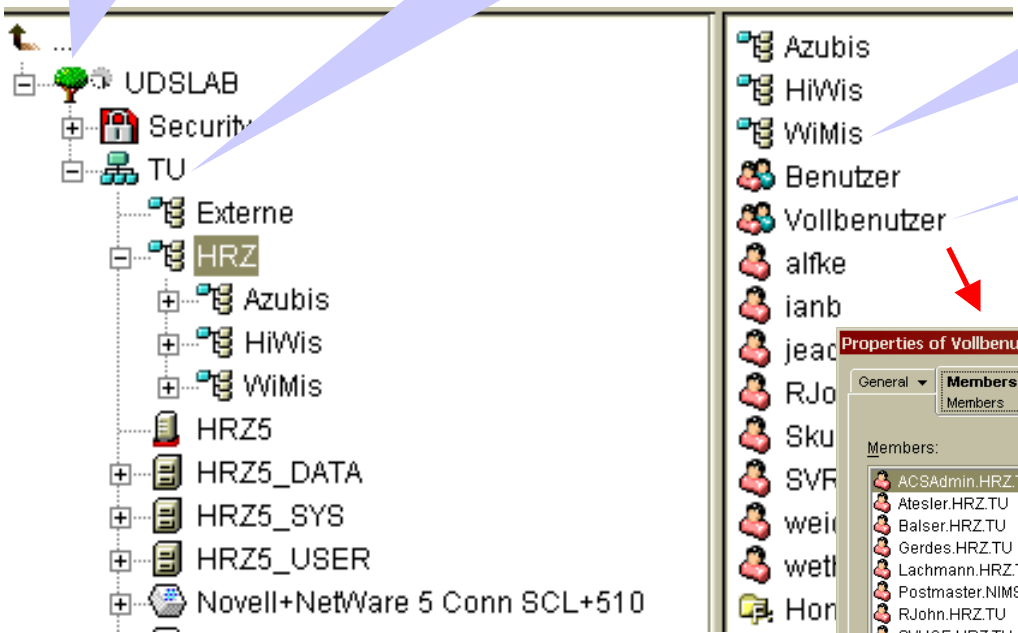
Grundlagen

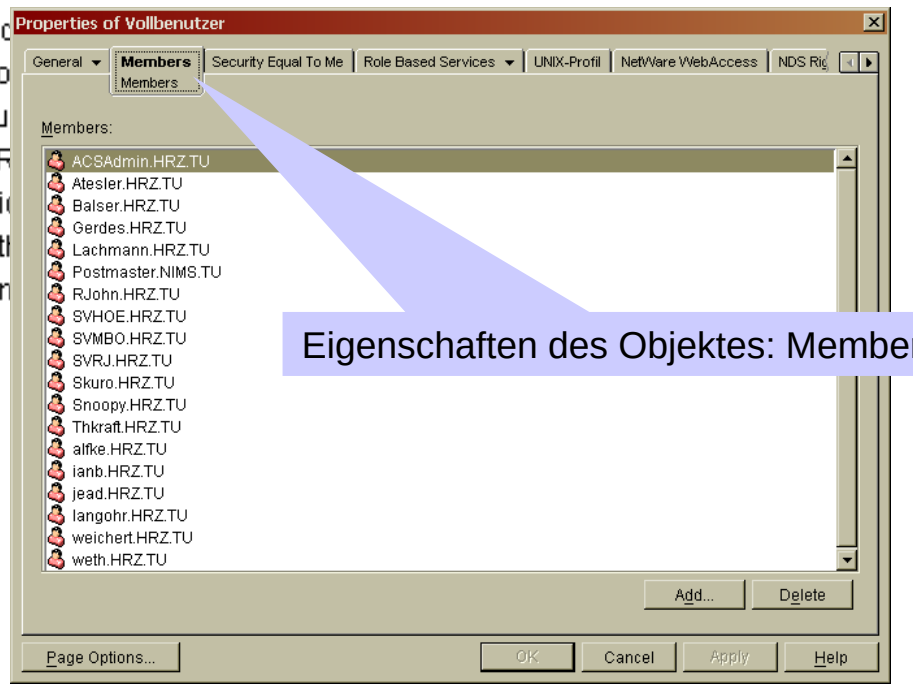
Wurzel: [Root]

Container: Organisation (O)

Container: Organisatorische Einheit (OU)

Objekt: Gruppe





Eigenschaften des Objektes: Members

[Public]
(Jeder, Anonymous)

Grundlagen

- Zugang zum Verzeichnis:
  - Zugangsprotokoll:
    - Suchen nach best. Kriterien (sog. Filter)
    - Lesen, Erstellen, Löschen, Modifizieren von Einzeldaten
  - Zugangskontrolle:
    - Mit Hilfe von *access control lists* (ACLs)
    - Was darf ich tun? → Vergleichen, Lesen, Schreiben, usw.
    - Auf welche Daten habe ich Zugriff? → ganzen Baum, Teilstrukturen, einzelne Attribute
  - Zugangsverfahren:
    - Klartext
    - Verschlüsselt:
      - Symmetrische und asymmetrische Verfahren

Grundlagen

- Charakteristik eines Verzeichnisdienstes
  - Optimiert auf Suchen und Lesen, weniger auf viele Schreiboperationen
  - I.d.R. keine Unterstützung von komplizierten Transaktionen → einfaches Zugangsprotokoll
  - Replizierung von Daten → Steigerung der Performance und Redundanz
  - Physikalische Partitionierung → Replizierung von Teilmengen über WAN
  - Unterschiedliche Authentifizierungsverfahren
  - Strukturierter Namensraum

Grundlagen

- Charakteristik eines Verzeichnisdienstes (Forts.)
  - Granulare Rechteregelung:

    → Ermöglicht Verteilung von administrativen Aufgaben
    - weltweites Telefonbuch: Jedes Land darf seine eigenen Nummer verwalten
    - Benutzerdatenbank: Administratoren in Fachgebieten können die Benutzerkonten ihrer Mitarbeiter oder Druckerwarteschlangen selber pflegen
    - Selbstadministration: Jeder Benutzer kann seine Adressdaten selber pflegen

Anbieter

- Allgemeine Entwicklung:
  - Wachsende Anzahl an Verzeichnisserver mit Anlehnung an X.500 oder LDAP
  - Proprietäre Datenbank oder Aufsatz auf bestehende Datenbankprodukte
  - Unterschiedlich starke Einbindung in eigene Betriebssysteme
  - Eigene Erweiterungen außerhalb des Standards

Anbieter

- Produkte:
  - Critical Path: CP Directory Server
  - Microsoft: Active Directory Service (ADS)
  - SUN: iPlanet Directory Server (vorher: NetScape DS)
  - IBM: SecureWay Directory
  - Novell: Novell Directory Service (NDS)
  - OpenLDAP: slapd, slurpd