Überblick

Meta-Directory

Ronny John, HRZ Darmstadt

Übersicht

1. Historie
2. NDS
3. Anwendungen
4. Leitgedanken und Ziele
5. Verzeichnis-Struktur
6. Rechteregeln
7. Schluss: Fragen und Diskussion

Historie

- 1997:
  - Umstellung der NetWare Server von Version 3.12 auf 4.11
  - Einführung des Verzeichnisdienstes NDS als Ersatz für die NetWare Bindery
- 1998:
  - Authentifizierung der Modempoolbenutzer über RADIUS - NDS
- 2001:
  - Update auf NW 5.1 und NDS 8.0
  - LDAP-Schnittstelle
- 2002:
  - 2 neue Server im Cluster für hohe Verfügbarkeit und Performanz (NW 6.0, eDirectory 8.7.1)

Historie

- 2003:
  - Intensive Nutzung der LDAP-Schnittstelle
  - Stabiler, wartungsarmer Betrieb

NDS

Novell Directory Services (NDS):

- Verzeichnisdienst von Novell
- Ursprünglich nur für NetWare verfügbar
- An X.500 angelehnt
- Neue Versionen als „eDirectory“ auch für Windows, Linux, Solaris, AIX
- Sehr flexibel und hoch skalierbar
- Viele Überwachungs- und Trace-Möglichkeiten
- Connectoren für Drittanbieter – DirXML
- SDKs für viele Programmiersprachen (LDAP Class Libraries for Java – JLDAP) verfügbar

NDS

Schnittstellen:

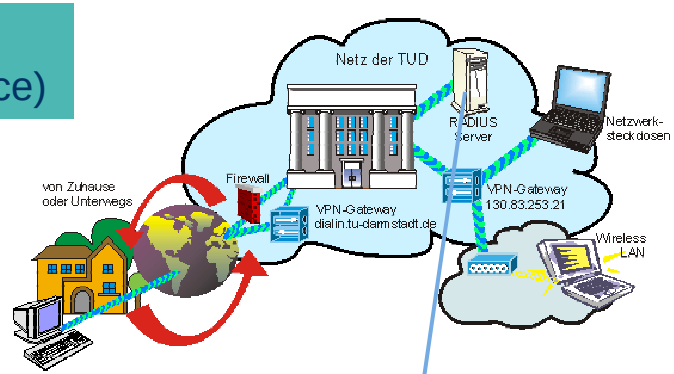
- Proprietär - „Client32“ (NDAP over NCP)
- LDAP v3 (auch SSL, TLS)
- RADIUS
- Service Location Protocol (SLP)
- DSML, UDDI, ...

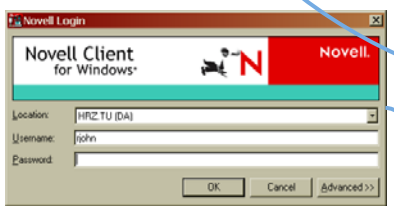
Anwendungen

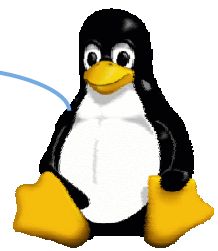
HORDE-IMP

DWI
(Web-Interface)

Studenten-
verwaltung







ldap_pam

NetWare

NDAP | LDAP | RADIUS

Verzeichnis

Anwendungen

NDAP:

- NetWare OS:
  - Ressourcen, Konfiguration
  - User-Management, Rechte-Management
- Client32:
  - Login und Desktopverwaltung (Roaming Profile)
  - Zugriff auf alle Verzeichnisdaten
    - „Bordmittel“: NWAdmin, ConsoleOne, NLIST
    - 3-Anbieter: JRB-Utilities
- Mercury: MTA im NDS-Modus

Anwendungen

LDAP (1):

- Authentifizierungsinstanz
  - Linux (ldap_pam)
  - Webseiten (Apache → htaccess)
- Repository
  - DWI (Suchen und Anzeigen von Daten)
  - Postfix (Mailalias, Forward)
  - Horde/IMP (Benutzerspezifische Einstellungen)

Anwendungen

LDAP (2):

- Verwalten
  - DWI (Ändern von Daten)
  - Studentenverwaltung (Abgleich der Daten mit Verwaltung)
  - LINUX Account-Management
  - Abrechnungen

Anwendungen

RADIUS:

- Authentifizierungsinstanz
  - ISDN- und Modempool
    - UNI@Home, DFN@Home
  - VPN
    - W-LAN
    - „offene Laptopdose“ in den PC-Pools
    - Extern (DSL, Internet Service Provider)
  - News-Server
  - SMTP-Relay

Leitgedanken und Ziele

Zentrale Benutzerdatenbank:

- Bisher: Getrennte Benutzerdaten- und verwaltung für einzelne Dienste und Plattformen
- Neu: Nur eine Benutzerdatenbank, in der alle Benutzer verwaltet werden können
  - Nur ein Benutzername und ein Passwort für die Dienste des HRZ notwendig
  - Einfaches Management → Verwaltungstools setzen immer auf die gleichen Schnittstellen auf
  - Einsparung von Kosten und Personal → Nur eine Datenbasis pflegen (Betrieb, Backup, etc.)
  - Aufbau von Verknüpfungen und Beziehung zwischen einzelnen Benutzer möglich

Leitgedanken und Ziele

Universitätsweites Repository:

- Automatische Erfassung aller Studierenden und Übergang in Alumni-Bereich

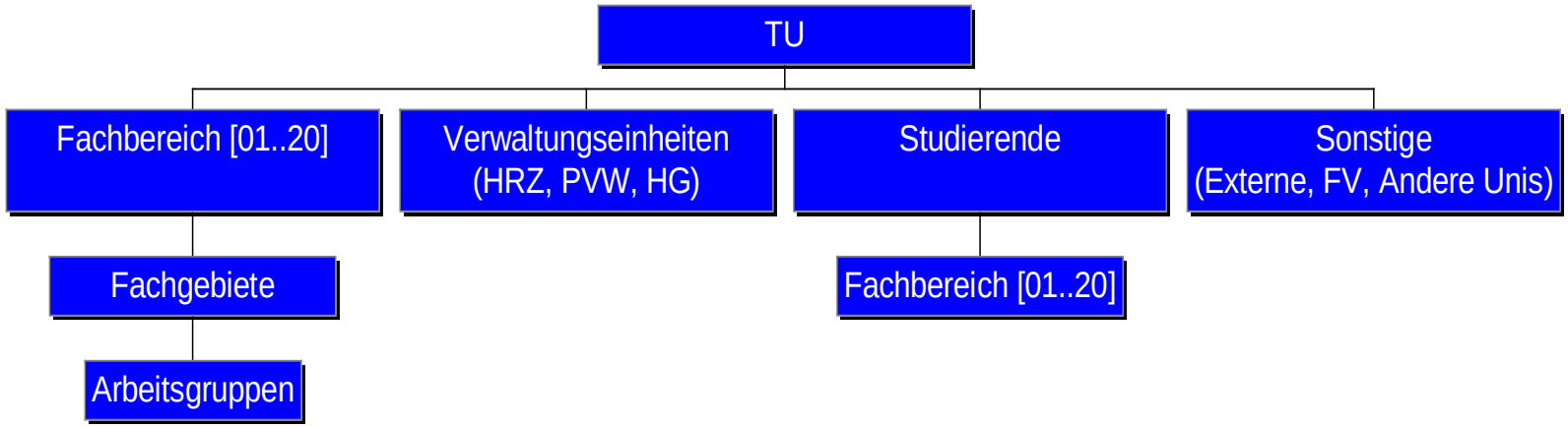
- *Bereitstellung von Benutzerinformationen (Adressen, Telefon) sowie Information über die Institutionen der TUD (Tätigkeit, Profil, etc.)*
- *Erfassung aller Mitarbeiter*
- *Kopplung mit Telefonanlagen-Verzeichnis (?)*
- *Schlüsselverzeichnis (Zertifikate von Servern und Benutzern)*

Leitgedanken und Ziele

Aktuell: Automatische Erfassung aller Studierenden:

- Mit der Einschreibung erhält jeder Studierende automatisch ein Benutzerkonto
- Freischaltung über Matrikelnummer und Einmalpasswort
  - Einmalpasswort wird mit Rückmeldeunterlagen verschickt
  - Web-basierte Freischaltung
- Struktur: User.[FB01..FB20].STUD.TU
  - Beispiel: *cn=john,ou=fb18,ou=stud,o=tu*
- Freischaltung von Diensten
- Mail-Adresse und Mail-Weiterleitung können web-basiert festgelegt werden
- Integriertes Guthaben(Druck)-konto mit 3 EURO Startguthaben

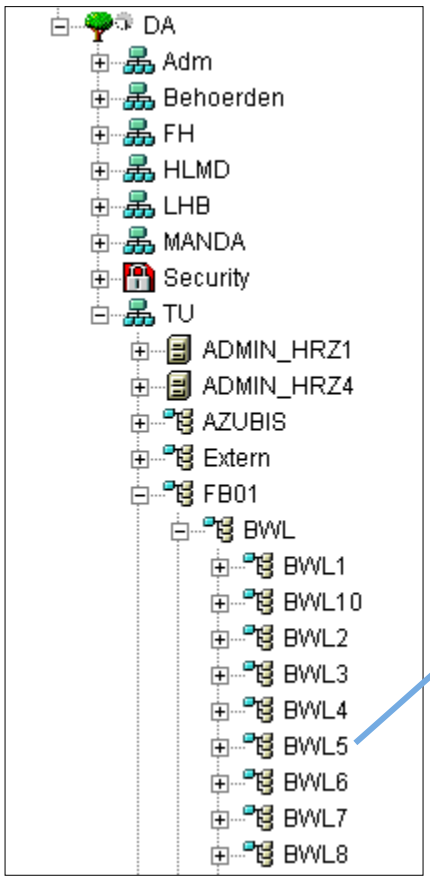
Verzeichnis-Struktur

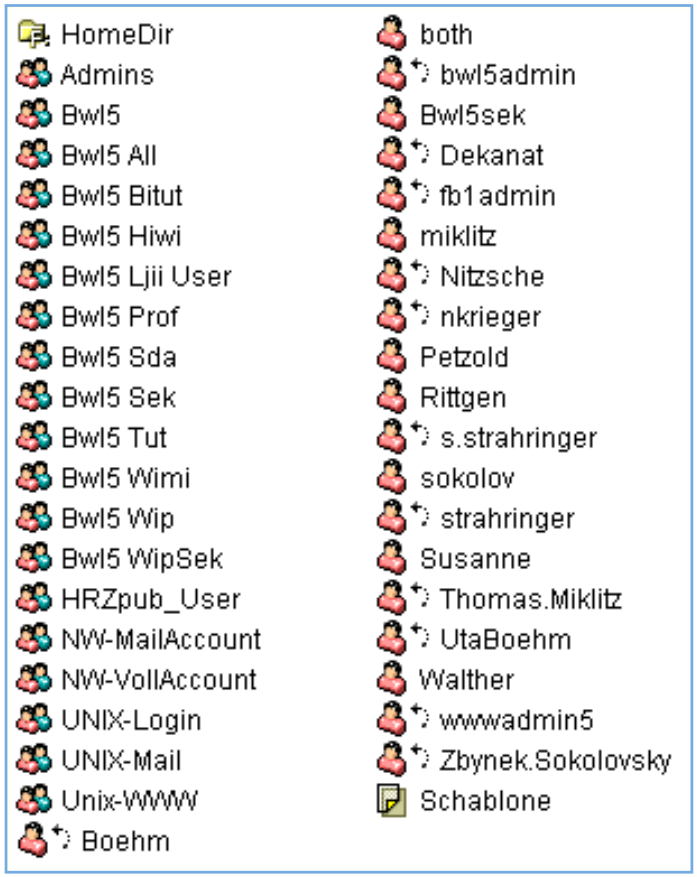


- Struktur nach Organisationen (Mitarbeiter)
- Struktur nach Funktionen (Studierende)

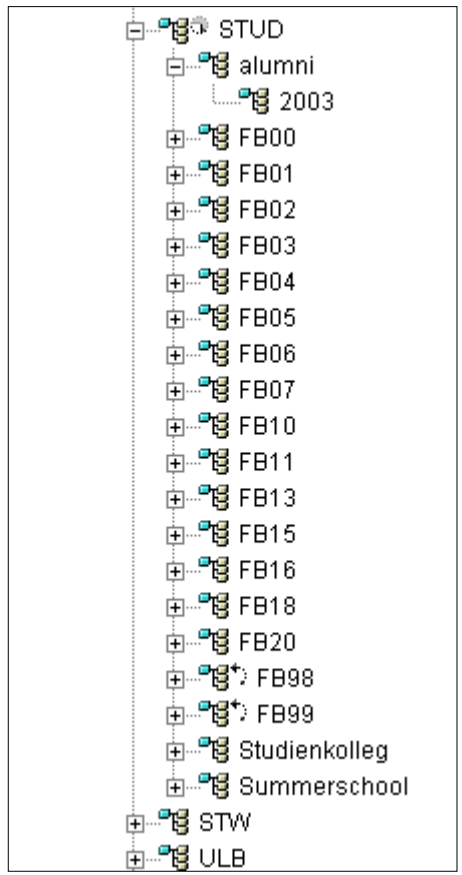
Verzeichnis-Struktur

Mitarbeiter





Studierende



Rechteregeln

Benutzer

- Unterscheidung: Studierende und Bedienstete

1. Studierende (Zentrale Entscheidung):
   - Darf alle seine Eigenschaften sehen
   - Darf einen festgelegten Teil seiner Eigenschaften direkt oder nur indirekt (multi-tier) ändern

2. Bedienstete
   - Darf alle seine Eigenschaften sehen
   - Darf nach Vorgabe des dez. Administrator seine Eigenschaften modifizieren

Rechteregeln

Benutzer

- Welche Daten sind sichtbar für andere Nutzer?
  - „restriktiver Ansatz“
    - Daten (Attribute) zu Beginn grundsätzlich nicht sichtbar
    - Explizites Freischalten von Daten durch den Anwender
  - Bündelung von semantisch ähnlichen Attributen
    - Kommunikation (Telefon, Fax)
    - Adressdaten (Anschrift)
  - 3 Kategorien von Nutzerkreisen
    - Persönlich
    - Campus
    - Weltweit

Rechteregeln

Dezentrale Administration von Teilstrukturen

- Selbständige Verwaltung der eigenen Benutzern (Bsp: Institut, Fachgebiet)
  a) Dez. Administrator erhält **Supervisor**-Recht auf den Untercontainer
  b) Eine Gruppe xxxx_Admins in dem Container erhält **Supervisor**-Recht auf den Untercontainer

- Bevorzugt: Verwendung einer Gruppe xxxx_Admins: Durch Hinzufügen von Benutzer zur Gruppe:
  - Realisierung einer Urlaubsvertretung
  - Nachfolger bei Weggang des vorherigen Admins

Zahlen und Fakten

- Verzeichnisdaten werden von 6 HRZ-Server repliziert
- Größe der Verzeichnisdatenbank: ~ 400 MByte
- 51.000 Objekte im Verzeichnis. Davon u.a.
  - 33.000 Benutzer
  - 3.200 Gruppen
  - 300 Organisatorische Einheiten
  - 9.500 Alias-Objekte
- Etwa 12.000 Authentifizierungsvorgänge pro Tag

Schluss

- Informationen und Kontakt:
  - Ronny John
    - Ronny.John@HRZ.TU-Darmstadt.De
    - 06151/16-4573
  - ds-admins@HRZ.TU-Darmstadt.De

Fragen und Diskussion...