RECHENZENTRUM der
UNIVERSITÄT MANNHEIM

Konzeption und Umbau der Mail-Infrastruktur an der Universität Mannheim

Dipl.-Wirtsch.-Inf. Matthias Merz

Dienstag, 20.03.2007

Agenda

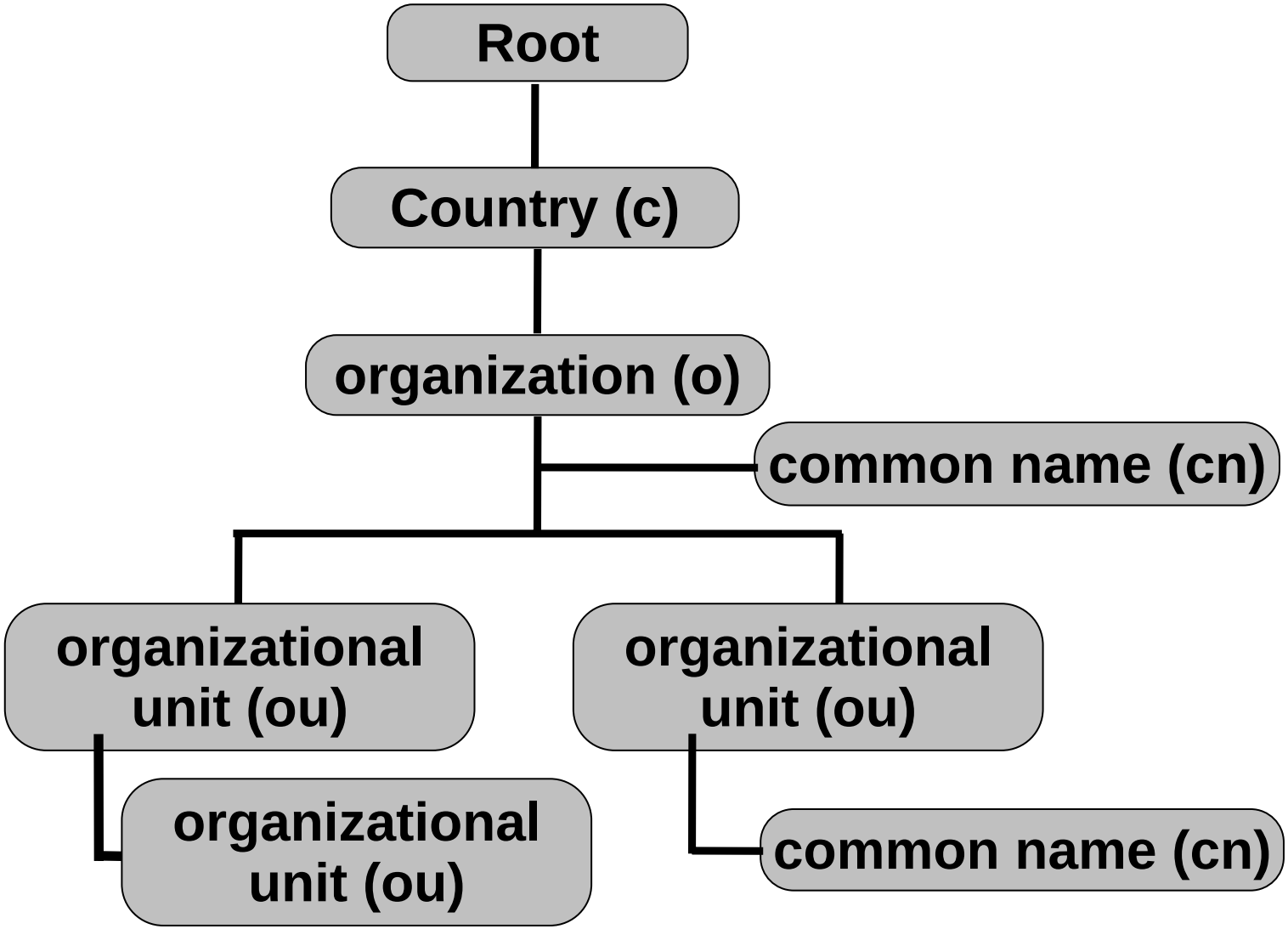
1. Einrichtung eines zentralen LDAP-Servers
2. Der neue Web-Mailer Horde
3. Migration der Mitarbeiter-Mailboxen

RECHENZENTRUM der
UNIVERSITÄT MANNHEIM

Einrichtung eines zentralen LDAP-Servers

LDAP

- Lightweight Directory Access Protocol
- Verzeichnisdienst mit baumartiger Datenstruktur
- Aktuelle Protokollversion: LDAPv3
- Basiert auf TCP/IP und ist optimiert für lesende Zugriffe
- Der Directory Information Tree (DIT) besteht aus Containerobjekten und Blattobjekten
- Containerobjekte sind:
  - Country (c)
  - Organization (o)
  - Organizational unit (ou)
- Blattobjekte: common name (cn)


Root
Country (c)
organization (o)
common name (cn)
organizational unit (ou)
organizational unit (ou)
organizational unit (ou)
common name (cn)

LDAP

Ziel:

- Etablierung einer zentralen Authentifizierungsinstanz
  - ermöglicht Anbindung unterschiedlicher Mail-Box Server
  - kann hierzu u. a. den Benutzerstatus (Student, Mitarbeiter, etc.) berücksichtigen
- Bereitstellung von Lookup-Services:
  - Verifikation von E-Mail Adressen (Reduzierung von Spam-Mails)
  - Zuordnung generischer und „echter“ E-Mail Adressen
- Zukünftig Anbindung weiterer Dienste
  - compute-Server (HPC)
  - dotlrn
  - Webserver (Webmaster)

LDAP

- Objekte in LDAP werden durch Objektklassen (LDAP Schema) spezifiziert – diese bestimmen über welche Attribute ein Objekt verfügt
- Abhängig von der jeweiligen Objektklasse existieren Pflicht- und optionale Attribute
- Der LDAP-Server an der Universität Mannheim nutzt folgende Objektklassen:
  - **`inetOrgPerson`** (Mitarbeiter in einer Organisation)
  - **`posixAccount`** (Benutzerkennung)
  - **`inetLocalMailRecipient`** (E-Mail Adressen)
  - **`uniMannheim`**

LDAP-Schema

- inetOrgPerson
  - **cn=Vorname Nachname**
  - **sn=Nachname**
  - **givenName=Vorname**
  - **ou=Fakultät_or_Einrichtung**

- posixAccount
  - **uid=RUM_Kennung**
  - **uidNumber=RUM_kennung_nummer**
  - **gidNumber=RUM_group_number**
  - **homeDir=users/fakul/uid**
  - **userPassword={SHA}xxxxxxxxxxxxx**

LDAP-Schema

- inetLocalMailRecipient
  - **mailLocalAddress=generische@mail_adresse**
  - **mailRoutingAddress=zieladresse@zb_staffmail**

- uniMannheim
  - **accountStatus=active inactive locked deleted**
  - **creationDateADMD=Datum**
  - **lastOpcodeADMD=Datum**
  - **modificationDateADMD=Datum**
  - **passwordChangeADMD=Datum**
  - **userRole=compute_webmaster_etc**
  - **userType=student staff extern absolventum**

LDAP-Directory Information Tree

Aufbau des Directory Information Tree:

- **dc=uni-mannheim,dc=de**
  - **ou=users**
    - **uid=merz**
      - **…**
      - **…**
      - **…**

(**dc** = Domain Component, entspricht dem Internet-Domainnamen)

Beispiel

```
dn: uid=merz,ou=users,dc=uni-mannheim,dc=de
uid: merz
cn: Matthias Merz
userPassword: {SHA} xxxxxxxxxxxxxxxxxxxxxx
uidNumber: xxxxx
gidNumber: xxxxx
creationDateADMD: 19951020085456+0100
mailRoutingAddress: merz@staff.mail.uni-mannheim.de
mailLocalAddress: matthias.merz@rz.uni-mannheim.de
mailLocalAddress: merz@rz.uni-mannheim.de
mailLocalAddress: support@ipacs-benchmark.org
accountStatus: active
userType: staff
```

LDAP

Herausforderungen beim Aufbau des LDAP-Servers:

- Planungsphase:
  - Welche Daten müssen in welcher Form vorgehalten werden?
- Daten kommen aus unterschiedlichen Quellen:
  - ADMD: Informationen über Kennungen
  - Benutzerdatenbank: Generische und echte Mail-Adressen
- ADMD:
  - Skript-Plugin mit LDAP-Schnittstelle
  - Kontinuierliches Update des LDAP-Servers

LDAP

Herausforderungen beim Aufbau des LDAP-Servers (Fortsetzung):

- Benutzerdatenbank:
  - Keine direkte LDAP-Schnittstelle
  - Export der Tabellen als Textfiles, diese werden in den LDAP eingelesen
  - Problem:
    - Große Anzahl an Datensätzen, kann nicht jedes mal importiert werden
    - Wie kann man Änderungen feststellen, wenn in dem Export hierzu keine Informationen enthalten sind?
  - Lösung:
    - Zum Feststellen von Änderungen müssen mit komplexen Skripten und dem Vorhalten unterschiedlicher Export-Versionen aufwändig Diffs-Files erzeugt werden.
    - Diese werden stündlich per Cronjob in den LDAP importiert

RECHENZENTRUM der
UNIVERSITÄT MANNHEIM

Der neue Web-Mailer Horde
(Version 3.1.3)

Horde

- Open-Source-Projekt (LGPL)
- Entwicklung
  - Begann 1998
  - Als Ein-Mann-Projekt gestartet (Chuck Hagenbuch)
  - Ausgangspunkt: IMP (Internet Messaging Program)
- Anwendungen:
  - E-Mail
  - Groupware
  - Entwicklungstools
- Ziel: Möglichst breite Unterstützung für eine Vielzahl an Backends

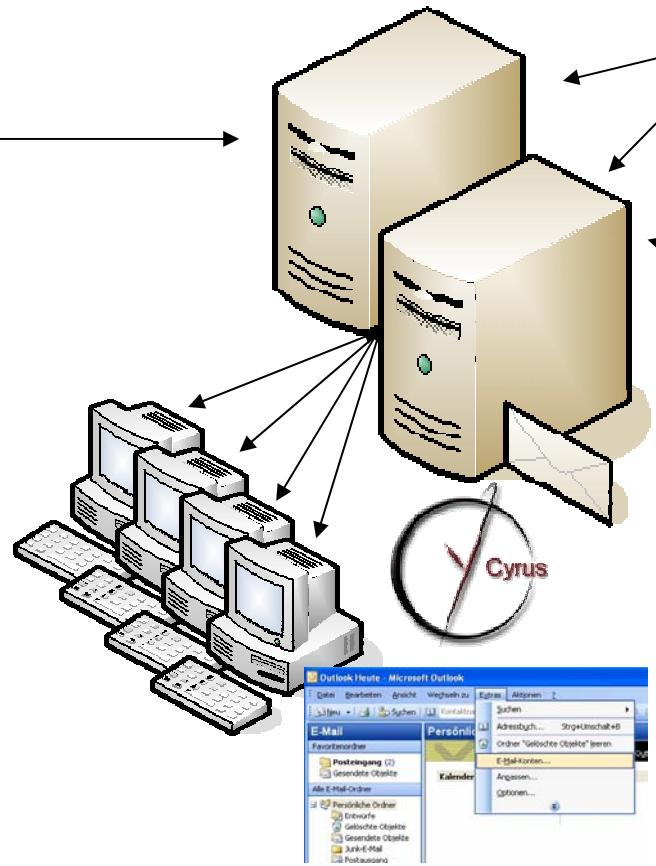
Die Horde-Architektur

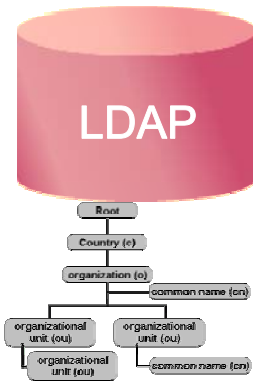
Horde bietet diverse Anwendungen in Form von Modulen:

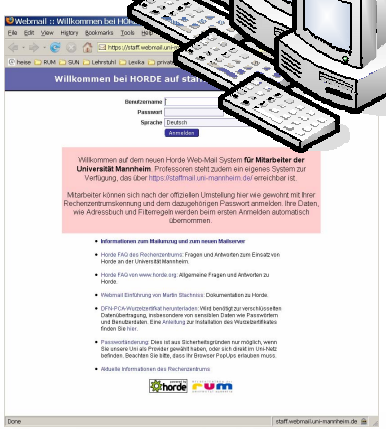
- E-Mail:
  - **Imp** ist der Horde Web-Mail Client
  - **Ingo** ist eine Anwendung zum Verwalten von Filterregeln
  - **Mimp** Mail-Client für Mobiltelefone und PDAs
- Groupware:
  - **Kronolith** ist eine Kalenderanwendung
  - **Mnemo** ist ein Notizbuch
  - **Nag** ist ein Taskmanager
  - **Gollem** ist ein Dateimanager (Zugriff auf das AFS)
  - **Trean** ist eine Anwendung zur Verwaltung von Bookmarks
  - **Turba** ist ein virtuelles Adressbuch mit Unterstützung für vCards
- Entwicklungstools:
  - **Chora** ist eine Anwendung zum Betrachten von CVS und Subversion Repositories

Horde an der Uni-Mannheim

staff.webmail.uni-mannheim.de staff.mail.uni-mannheim.de
students.webmail.uni-mannheim.de students.mail.uni-mannheim.de





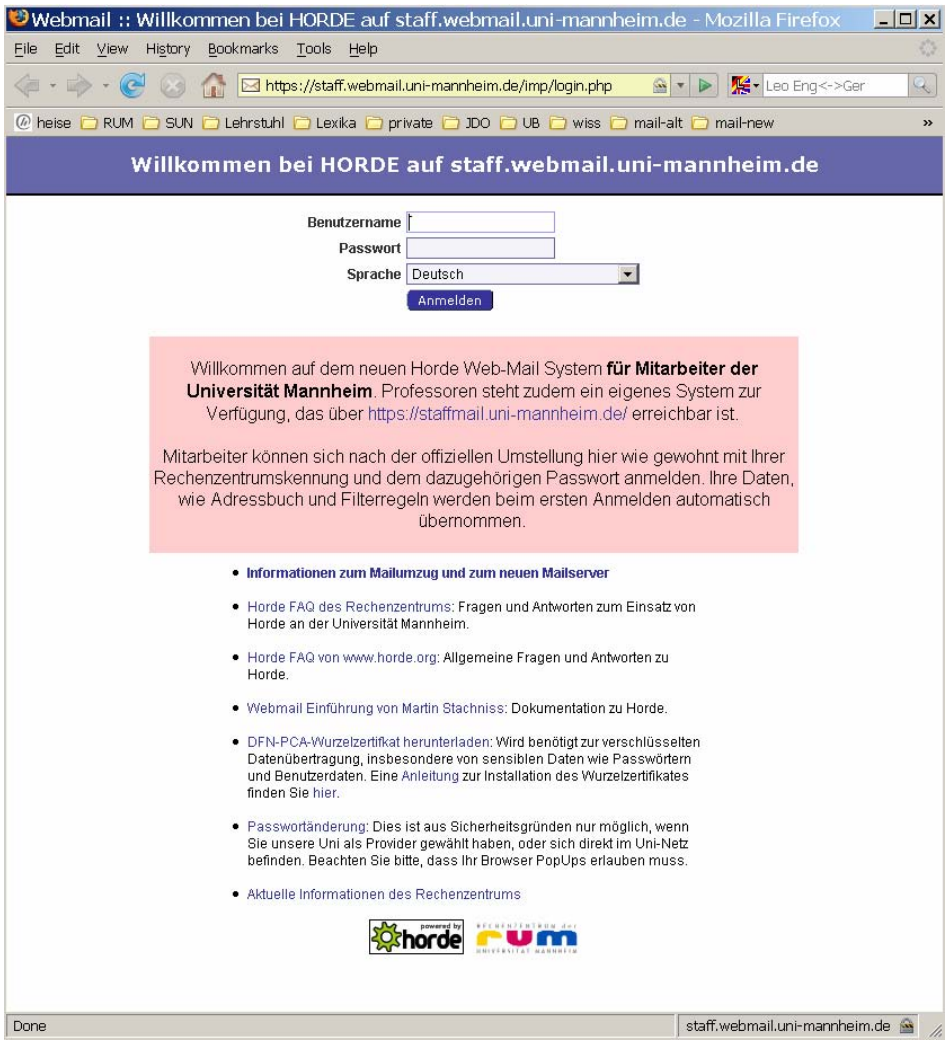


Horde an der Uni-Mannheim

- Derzeit drei Webmailer im Einsatz:
  - Web-Mail für Mitarbeiter der Universität soweit Umgezogen
  - Web-Mail für Studenten und nicht Mitarbeiter
  - Web-Mail für Professoren

- Neue Funktionen:
  - Filterregel flexibler einsetzbar (z. B. Spamfilter vor der Abwesenheitsnotiz)
  - Anzeige Speicherplatz-Kontingents (Quota)
  - AFS-Anbindung
  - Mail-Client für Mobiltelefone und PDAs (für Mitarbeiter)
    `https://staff.webmail.uni-mannheim.de/mimp/`
  - Umfangreichere Überwachungstools für Administratoren

Horde an der Uni-Mannheim



Kurze Live Demo

https://staff.webmail.uni-mannheim.de/

RECHENZENTRUM der
UNIVERSITÄT MANNHEIM

Migration der Mitarbeiter-Mailboxen

Migration der Mitarbeiter-Mailboxen

Einige Kennzahlen:

- Anzahl betroffener Kennungen: ca. 3.000
- Datenumfang: ca. 110 GB
- Quota für Mitarbeiter: 2 GB pro Kennung

Vorgehen:

1. Kennungen werden auf dem neuen Mail-Server angelegt
2. Änderung der MailRouting-Adresse: Mails werden zum neuen Rechner geleitet
3. Benutzer werden per E-Mail benachrichtigt („dies ist ihre letzte E-Mail auf diesem System“)
4. Forward wird im alten System gesetzt
5. Umzug der Mailboxen

Migration der Mitarbeiter-Mailboxen

Umstellungsablauf:

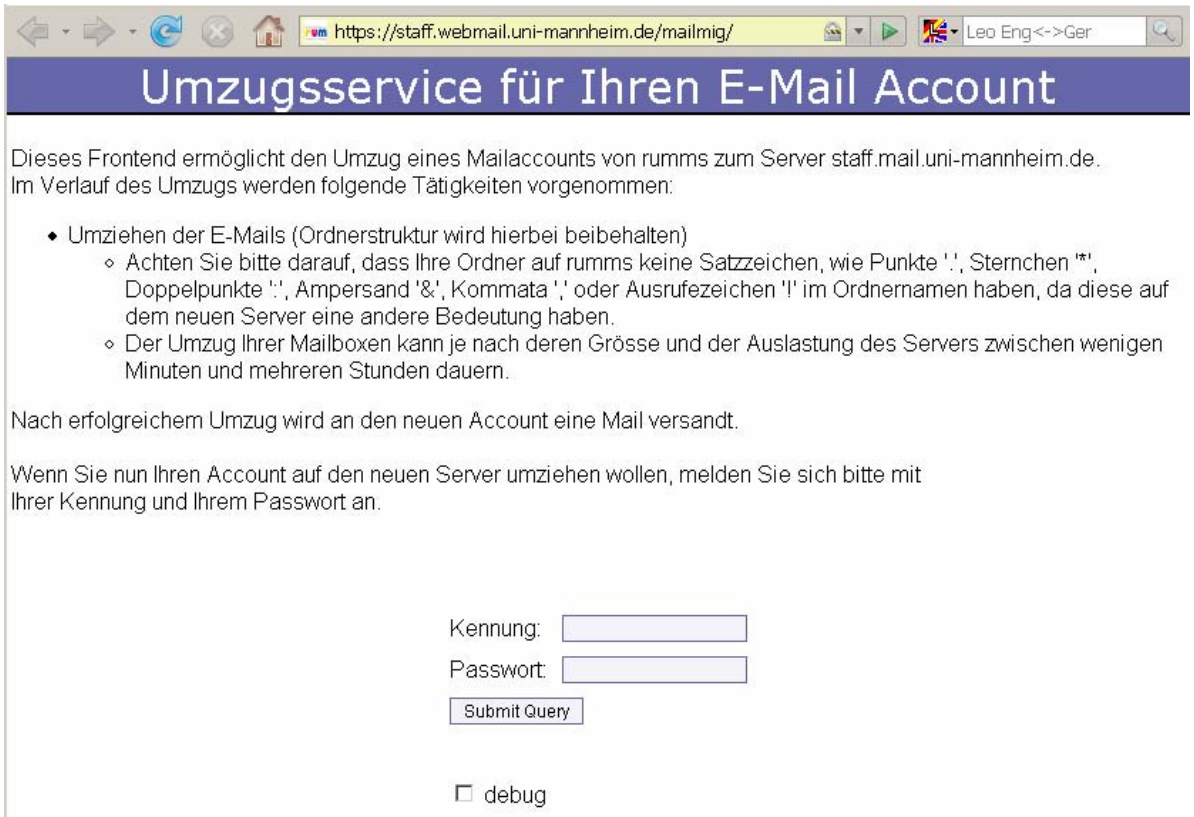
- Probe-Phase: Umstellung der Kennungen von Mitarbeitern des RUM
- Analyse: Was hat geklappt, was ging schief?
- Eigentliche Umstellungs-Phase

Migration der Mitarbeiter-Mailboxen

Anlegen der Mailboxen:

- Ein neuer Mitarbeiter wird im Infocenter registriert
- Die Informationen gelangen automatisch über den ADMD und speziellen Skripten auf den LDAP-Server
- Sobald diese Informationen auf dem LDAP-Server verfügbar sind, können auf den neuen Mail-Server Mails gelesen und empfangen werden
- Die Kennung wird hierbei automatisch angelegt
- Einmal am Tag werden für neue Kennungen Sieve-Skripte, Mailxbox-Directories und Quotas nachgetragen

Migration der Mitarbeiter-Mailboxen



Mailbox Umzugsservice:

- Benutzer melden sich mit Name und Passwort an
- Im Hintergrund werden Batchjobs gestartet
- Basieren auf dem Tool Imapsync, das die Mailboxen migriert

Danke für Eure Aufmerksamkeit!