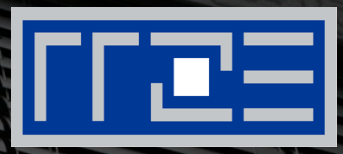
REGIONALES RECHENZENTRUM ERLANGEN [RRZE]

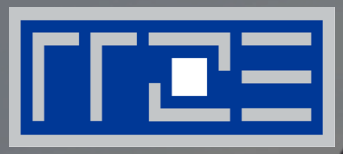


Benutzerverwaltung - LDAP

Systemausbildung - Grundlagen und Aspekte von Betriebssystemen und System-nahen Diensten, 22.07.2020

FRIEDRICH-ALEXANDER UNIVERSITÄT ERLANGEN-NÜRNBERG

AGENDA



- Einführung
- LDAP-Grundlagen
- LDAP-Formate
- Implementierungen und Werkzeuge
- Ausblick

EINFÜHRUNG

- Was ist LDAP?
- Was ist ein Verzeichnisdienst?
- Wie ist LDAP entstanden?
- Warum LDAP?

Was ist LDAP?

- **L**ightweight **D**irectory **A**ccess **P**rotocol
- Protokollstandard zur Abfrage und Modifikation von Informationen eines Verzeichnisdienstes (Directory)
- leichtgewichtige Implementierung des DAP-Protokolls (X.500)
- Aktuelle Version LDAP v3 in RFC 2251 spezifiziert
- Oberbegriff für Implementierungen und Technologien, die eine LDAP Schnittstelle anbieten

Was ist ein Verzeichnisdienst?

- Eigenschaften:
  - hierarchisch
  - zentral
  - optimiert für lesenden Zugriff
- Anwendung:
  - Authentifizierung
  - zentrale Benutzerverwaltung
- Beispiele:
  - OpenLDAP - Sun Directory Server - Apache DS
  - Microsoft Active Directory
  - DNS

Wie ist LDAP entstanden?

- Entwicklung in den frühen 90er an der University of Michigan
- Wurzeln im sehr komplexen X.500 Standard
  - DAP Protokoll
  - eigener Netzwerkstack
- LDAP als leichtgewichtige Alternative des DAP Protokolls
  - reduzierter Funktionsumfang - einfachere Implementierung
  - nutzt den verbreiteten TCP/IP-Stack
- Durch diese Merkmale fand LDAP bereits in den 90er Jahren eine breite Anwendungsbasis

Warum LDAP?

- hohe Interoperabilität
  - Zugriff mittels einheitlichem LDAP Protokoll, ermöglicht (theoretische) Unabhängigkeit von zugrundeliegender Datenhaltung
  - Spezifikation von Datenstrukturen in Schemas erhöht die Nutzbarkeit der gespeicherten Daten durch verschiedenste Client-Anwendungen
    - Authentifizierung - Samba, PAM, Radius, …
    - E-Mail Verzeichnis - Thunderbird, Outlook, …

- hierarchische Datenhaltung/-zugriff
  - wird als Nachschlage-Verzeichnis verstanden
  - passt oft besser zur Wirklichkeit der Einordnung von Personen in einer Organisationsstruktur

LDAP-GRUNDLAGEN

- LDAP v3
- Logisches Modell
- DIB, Einträge, Attribute
- Namensräume, Hierarchien
- Operationen
- Zugriffssicherung

LDAP v3

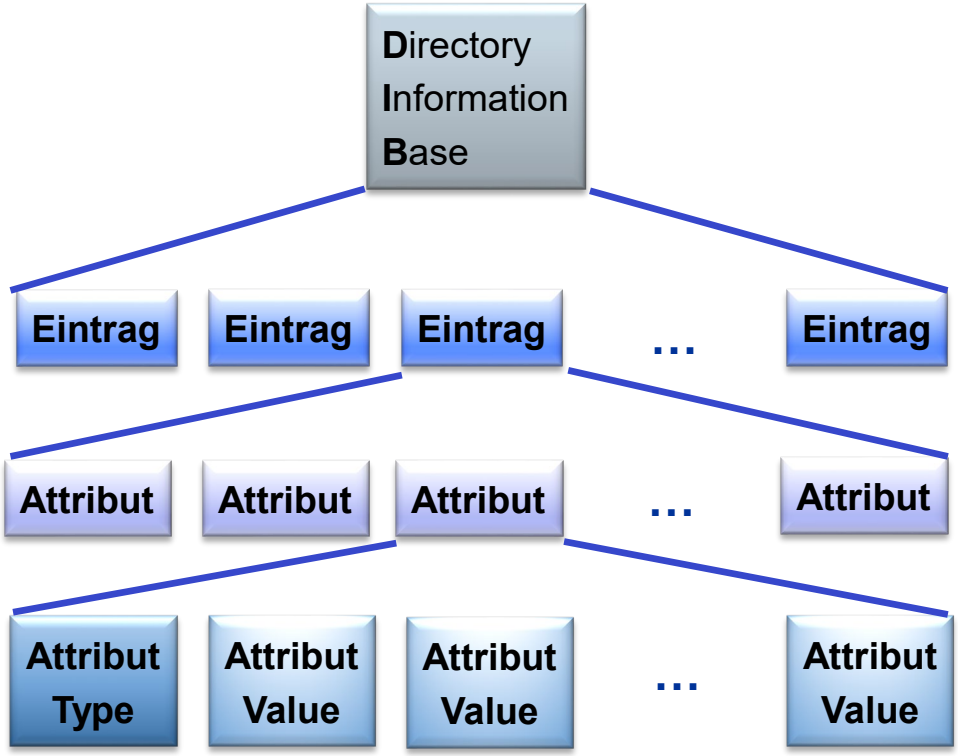
- Dez. 1997 von der IETF als Proposed Internet Standard bestätigt
- Verbesserungen gegenüber LDAP v2
  - Globalisierungssupport: Unicode für die interne Repräsentierung - Zeichen aller Weltsprachen können benutzt werden
  - Referrals: Verweismechanismus der es Servern erlaubt auf Queries mit Referenzierungen auf anderen Servern zu antworten
  - Sicherheit: Simple Authentication and Security Layer (SASL) vs. Transport Layer Security (TLS)
  - Erweiterbarkeit: Möglichkeit die existierenden Operationen zu erweitern (Extensions und Controls)
  - Offenlegen von Informationen die Kommunikationsrelevant sind (z.B. Protokoll Version)

LDAP Architektur - Logisches Model

- Information Model: Struktur und Art der Informationen die in einen LDAP-Directory gespeichert werden können
- Naming Model: Organisation und Adressierung dieser Informationen
- Functional Model: Definiert welche Operationen auf den Informationen möglich sind
- Security Model: Schutz der Informationen vor nicht autorisiertem Zugriff

Information Model: DIB, Einträge, Attribute,.. (1)

- Gesamtmenge der Informationen in einen LDAP: **D**irectory **I**nformation **B**ase (DIB)



Information Model: DIB, Einträge, Attribute,.. (2)

- Einträge:
  - Menge von Informationen über ein einzelnes Objekt (z.B. Person)
  - eindeutig über Ihre **D**istinguished **N**ames (DNs) adressierbar
  - setzen sich aus einer Menge von Attributen zusammen
- Attribute:
  - können vorgeschrieben oder optional sein (required vs. optional)
  - jedes Attribut hat einen Attributtyp
  - können einen oder mehreren Werten haben (single vs. multivalued)
  - Attributtyp wir über die Syntax festgelegt (z.B. string bzw. number)
  - Definition kann auch Informationen wie Vergleichsoperationen gehandhabt werden beinhalten (z.B. case-sensitive vs. case-insensitive)

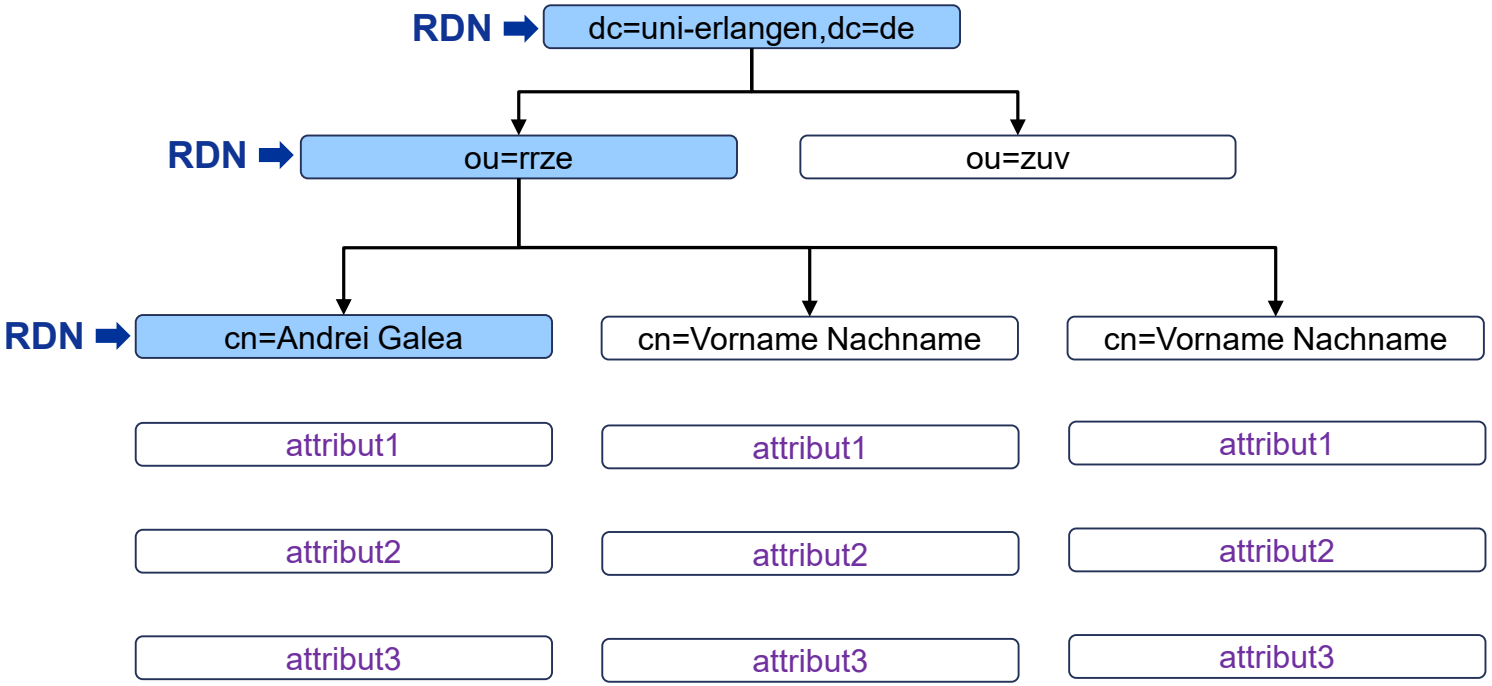
Information Model: DIB, Einträge, Attribute,.. (3)

- Objektklassen
  - jeder Eintrag beschreibt ein Objekt ist also eine Instanz einer Objektklasse
  - jede Objektklasse hat eine Eindeutige ID (OID)
  - Objektklasse beinhaltet Liste der vorgeschriebenen (mandatory) bzw. optionalen (optional) Attribute
  - Objektklassen nach RFC 2252
    - Abstrakt (ableiten anderer Objektklassen)
    - Strukturell (jeder Eintrag muss mindestens zu einer Objektklasse diesen Typs gehören)
    - Auxiliär (Hilfsobjektklassen)
  - Objektklassen werden in Schema des LDAP-Servers abgelegt

Naming Model: Namensräume, Hierarchien,.. (1)

- DIT (**D**irectory **I**nformation **T**ree) besteht aus den DNs der LDAP-Einträge
- DN (**D**istinguished **N**ame) identifiziert jedes Objekt eindeutig und beschreibt seine Position in der Hierarchie
- setzt sich aus einzelnen RDNs (**R**elative **D**istinguished **N**ames) zusammen

Naming Model: Namensräume, Hierarchien,.. (2)



dn: cn=Andrei Galea,ou=rrze, dc=uni-erlangen,dc=de

Functional Model: Operationen (1)

- Das LDAP-Protokoll definiert folgende Operationen an Einträge:
  - Search: Suche nach Einträgen anhand bestimmter Kriterien (Filter)
  - Add: Hinzufügen von Einträgen
  - Delete: Löschen von Einträgen
  - Modify: Ändern von Einträgen
  - Modify DN: Verschieben (Umziehen) der Einträge
  - Compare: Vergleich von Einträgen
  - Bind: Client Authentifiziert sich am LDAP-Server
  - Unbind: Verbindung wird abgebaut

Functional Model: Operationen (2)

- Jede Operation bis auf Unbind liefert ein Operation Result bestehend aus:
  - ResultCode z.B. 0: Success, 1: Operation Errors…
  - Eine DN (optional)
  - Ein Meldung (optional)
  - Eine Menge von Referrals (optional)
- Eine Such-Operation liefert nach erfolgreicher Ausführung die gefundenen Einträge

Security Model: Zugriffsschutz

- Im LDAP-Protokoll wird auch bestimmt wie Informationen zwischen Client und Server ausgetauscht werden
- Grundsätzlicher Ablauf:
  - Bind: Verbindungsaufbau mit optionaler Authentifizierung ggf. verschlüsselte Verbindung
  - Ausführen von Operationen auf dem LDAP-Server
  - Unbind: Session schließen

LDAP-FORMATE

- LDAP Data Interchange Format
- Schemas

LDAP Data Interchange Format (LDIF) (1)

- ASCII-basierendes Format zur Darstellung von Informationen eines LDAP-Verzeichnises
- LDIF ist als Austauschformat zwischen heterogenen LDAP-Verzeichnisse spezifiziert
- LDIF Format ist durch seine rein textuelle Darstellung leicht interpretierbar
- LDIF Formate
  - LDIF Content: Stellt Einträge und ihre Attribute dar
  - LDIF Change: Beschreibt Operationen an Einträgen und ihre Attribute

LDAP Data Interchange Format (LDIF) (2)

```
dn: ou=rrze, dc=uni-erlangen, dc=de
objectclass: organizationalunit
ou: rrze
locality: Erlangen
description: Regionales RechenZentrum
telephonenumber: 09131-8528326

dn: cn=Andrei Galea, ou=rrze, dc=uni-erlangen, dc=de
objectclass: person
objectclass: inetorgperson
cn: Andrei Galea
sn: Galea
givenname: Andrei
mail: andrei.galea@fau.de
locality: Erlangen
```

LDAP Data Interchange Format (LDIF) (3)

```
dn: cn=Andrei Galea, ou=rrze, dc=uni-erlangen, dc=de
changetype: modify
add: telephonenumber
telephonenumber: 09131-27029
-
replace: mail
mail: andrei.galea@rrze.fau.de
-
delete: locality

dn: cn=Vorname Nachname, ou=rrze, dc=uni-erlangen, dc=de
changetype: add
objectclass: person
objectclass: inetorgperson
cn: Vorname Nachname
sn: Nachname
givenname: Vorname
mail: vorname.nachname@fau.de
locality: Erlangen
```

LDAP Schemas (1)

- Definieren alle möglichen Typen von Einträgen (Objektklassen) und deren Attribute
- Schema Definitionen werden in Dateien gespeichert
- LDAP-Server haben eine oder mehrere Schemas auf denen zurückgegriffen werden kann
- Vordefinierte Schemas:
  - nis.schema
  - openldap.schema
  - inetorgperson.schema

LDAP Schemas (2)

```
attributetype( 2.16.840.1.113730.3.1.241
   NAME 'displayName'
   DESC 'RFC2798: preferred name to be used when displaying
entries'
   EQUALITY caseIgnoreMatch
   SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
   SINGLE-VALUE ))

objectclass( 2.16.840.1.113730.3.2.2
   NAME 'inetOrgPerson'
   DESC 'RFC2798: Internet Organizational Person'
   SUP organizationalPerson
   STRUCTURAL
   MUST ( cn )
   MAY ( audio $ businessCategory $ carLicense $ departmentNumber$
    displayName $ employeeNumber $ employeeType $ givenName $ ..))
```

IMPLEMENTIERUNGEN UND TOOLS

- OpenLDAP
- LDAP Command Line Tools
- LDAP Suchfilter
- Apache Directory Studio

OpenLDAP (1)

- Heutzutage am weitesten verbreitete LDAP-Implementierung
- Aktuelle Version: 2.4
- Projekt wurde 1998 von Kurt Zeilenga gestartet
- Freie Software unter OpenLDAP Public License
- Auf folgenden Plattformen verfügbar:
  - Mac OS X
  - Unix, GNU-Linux
  - BSD Derivate
  - Microsoft Windows
- Bestandteil vieler aktuellen Linux-Distributionen z.B. Ubuntu

OpenLDAP (2)

- Bestandteile:
  - slapd - LDAP Daemon
  - backends - Datenspeicherung und -zugriff z.B. Oracle Berkeley DB
  - overlays - Verhalten der backends modifizieren
  - libraries - Bereitstellung des LDAP-Protokolls
  - syncrepl - Replikation

LDAP Command Line Tools (1)

- Kommandozeilen Tools zum Managen eines LDAP-Servers
- In vielen Linux-Distributionen standardmäßig verfügbar
- Bestandteile:
  - ldapbind: Authentifizieren
  - ldapadd: Einträge hinzufügen
  - ldapmodify: Einträge ändern
  - ldapsearch: Einträge suchen
  - ldapdelete: Blatt-Einträge löschen
  - ldapmoddn: RDN eines Eintrags ändern

LDAP Command Line Tools (2)

```
ldapsearch -h myhost -p 389 -b "ou=rrze,dc=uni-erlangen,dc=de"
           "(uid=admin)" cn sn givenname

ldapsearch -h myhost -p 389 -b "dc=uni-erlangen,dc=de"
           "(&(uid=admin*)(locality=Erlangen))" *
```

LDAP Suchfilter

Relationale LDAP-Operatoren	
=	Werte müssen übereinstimmen
>=	größer gleich
<=	kleiner gleich

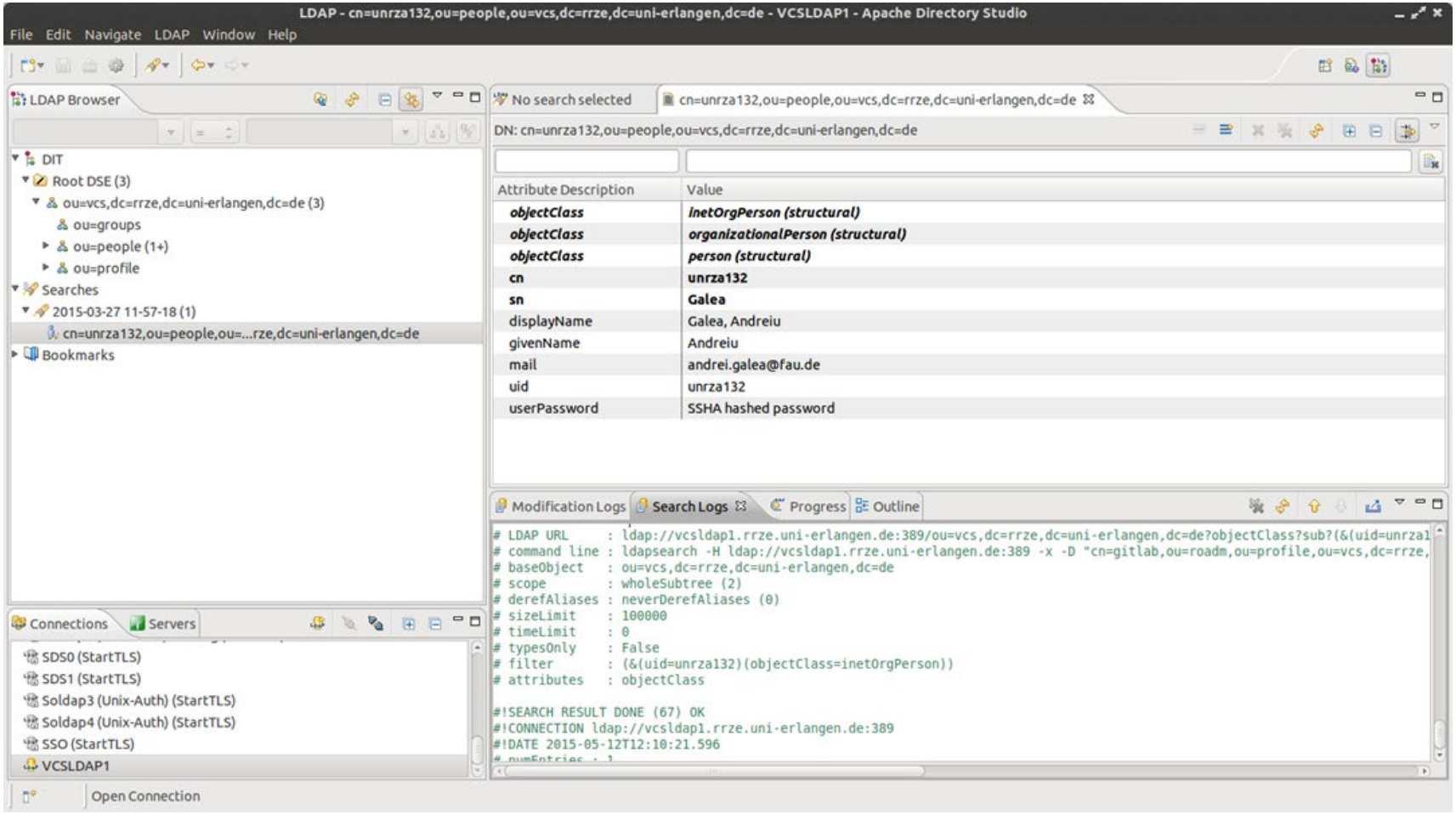
Logische LDAP-Operatoren	
!	logisches nicht (ungleich)
&	logisches und
|	logisches oder

```
(&(objectclass=inetorgperson)(sn=Galea))
(|(uid=admin)(uid=user))
(|(uid=user*)(uid=admin*))
(!(sn=Galea))
(objectclass=*)
```

Apache Directory Studio (1)

- Auf Eclipse basierender LDAP-Browser und Directory Client
- Aktuelle Version 1.5.3
- Features:
  - LDAP-Editor und Browser
  - Schema-Editor und Browser
  - LDIF-Editor
  - LDAP-Filter Editor
  - Managment von LDAP-Verbindungen
  - Multiplatform: support für Linux, Windows und Mac OSX

Apache Directory Studio (2)

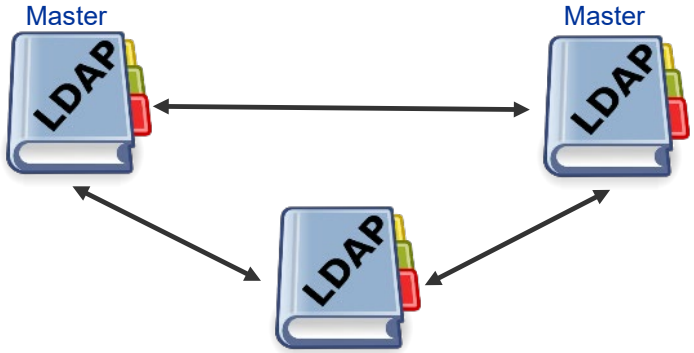


AUSBLICK

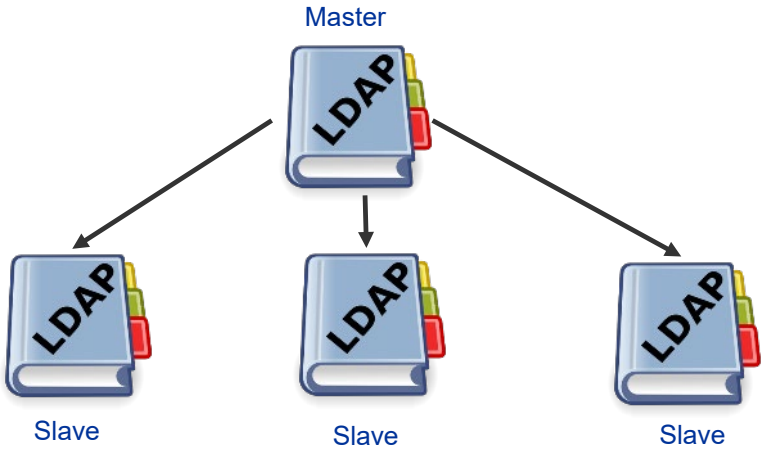
- Replikation
- Anwendung - PAM Authentifizierung

Replikation

- Vorteile: Lastenverteilung und Ausfallsicherheit
- Typen:
  - Multimaster



  - Master-Slave:



Anwendung - PAM Authentifizierung

- **P**luggable **A**uthentication **M**odules (PAM)
- Programmierschnittschtelle (API) für Authentifizierungsdienste
- Weit unter Linux-Systemen verbreitet
- Beim RRZE für Linux-Server im Einsatz:
  - Modul PAM_SSS (SSSD - System Security Services Daemon)
    - Mehrere LDAP-Instanzen (Master-Slave Replication)
    - Hosts (Server) Authentifizieren Benutzer mit LDAP-Bind
    - Durch die Master-Slave Topologie ist Ausfallsicherheit und Lastenverteilung gewährleistet

ORGANISATORISCHES

- Die Vorträge im Überblick
- Andere Vortragsreihen des RRZE
- Ablageorte Vortragsfolien
- RRZE-Veranstaltungskalender / Mailingliste abonnieren
- Themenvorschläge & Anregungen

Weitere Vorträge zur „Systemausbildung“

13.05.2020 – Windows-Betriebssysteme
20.05.2020 – Systemüberwachung / Monitoring
27.05.2020 – Storage & Filesysteme
17.06.2020 – Virtualisierung
24.06.2020 – Backup / Archiv
01.07.2020 – IT-Sicherheit
08.07.2020 – High Performance Computing
15.07.2020 – Benutzerverwaltung: MS Active Directory
22.07.2020 – LDAP und Kerberos

Immer mittwochs
(ab 14:15 Uhr)
- online -

Details: www.rrze.fau.de/veranstaltungen/veranstaltungskalender/

Andere Vortragsreihen des RRZE

Campustreffen

- immer donnerstags ab 15 Uhr c.t.
- vermittelt Informationen zu den Dienstleistungen des RRZE
- befasst sich mit neuer Hard- & Software, Update-Verfahren sowie Lizenzfragen
- ermöglicht den Erfahrungsaustausch mit Spezialisten

Netzwerkausbildung „Praxis der Datenkommunikation“

- immer mittwochs in den Wintersemestern, ab 14 Uhr c.t.
- Vorlesungsreihe, die in die Grundlagen der Netztechnik einführt
- stellt die zahlreichen aktuellen Entwicklungen auf dem Gebiet der (universitären) Kommunikationssysteme dar

Vortragsfolien

Die Vortragsfolien werden nach der Veranstaltung auf der Webseite des RRZE abgelegt:

www.rrze.fau.de/ausbildung-schulung/veranstaltungsreihen/systemausbildung/

RRZE-Veranstaltungskalender & Mailinglisten

- Kalender abonnieren oder bookmarken
  - Alle Infos hierzu stehen auf der Webseite des RRZE unter: www.rrze.fau.de/veranstaltungen/veranstaltungskalender/
- Mailingliste abonnieren
  - Wöchentliche Terminhinweise werden zusätzlich an die Mailingliste RRZE-Aktuelles gesendet.
  - Auch diese Liste kann man abonnieren: https://lists.fau.de/mailman/listinfo/rrze-aktuelles

Themenvorschläge & Anregungen

Themenvorschläge und Anregungen nehmen wir gerne entgegen!

Bitte schreiben Sie uns einfach eine E-Mail an:
rrze-zentrale@fau.de (Betreff: Systemausbildung)

Vielen Dank für Ihre Aufmerksamkeit!

Regionales RechenZentrum Erlangen [RRZE]
Martensstraße 1, 91058 Erlangen
www.rrze.fau.de