LDAP

Lightweight Directory Access Protokoll

Desanka Bogicevic 1121621

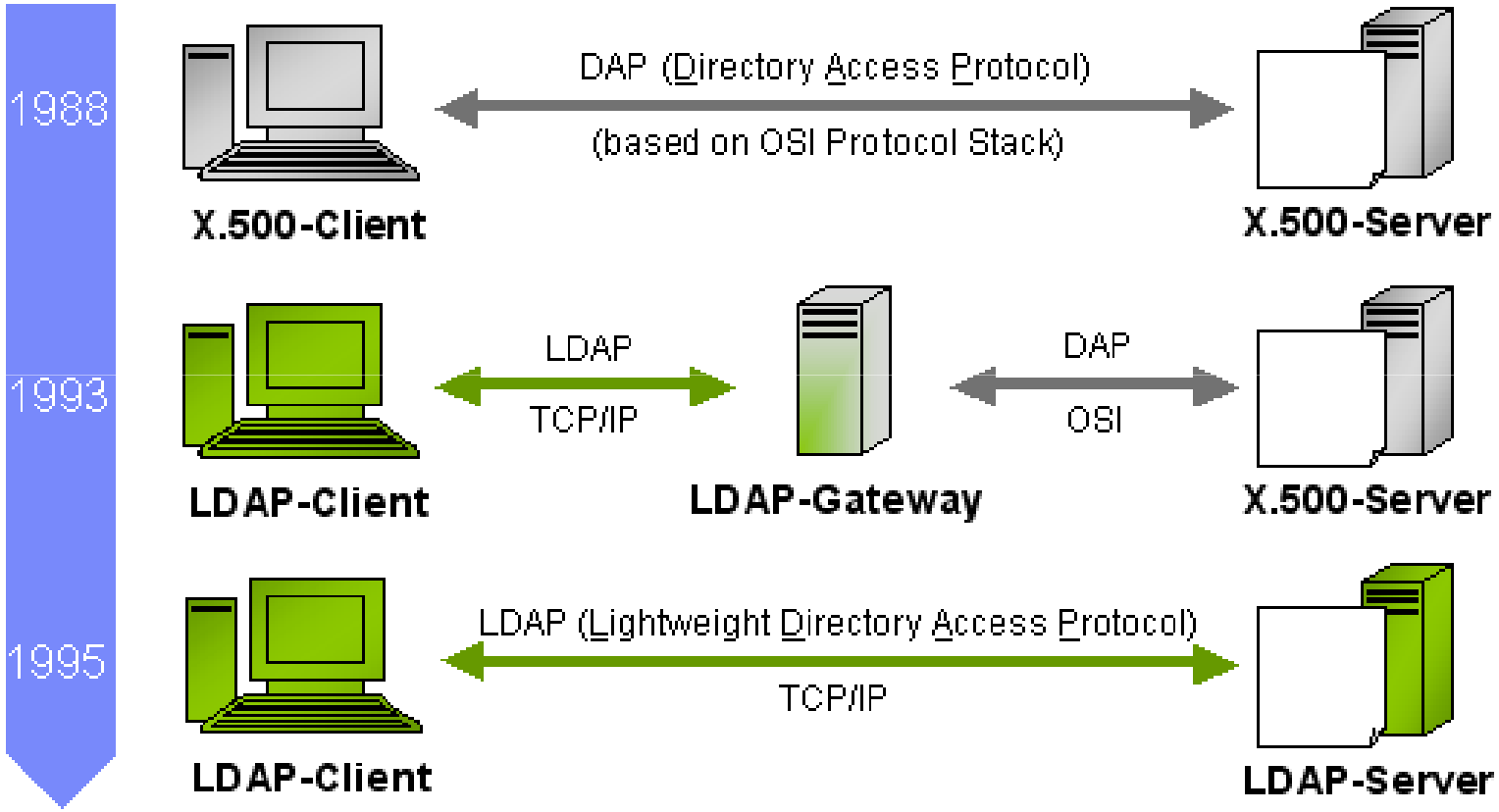
Michael Wenig 1220567

Rupert Eisl 1220225

LDAP

- Was ist LDAP?
- Was sind Verzeichnisdienste?
- Was ist ein Verzeichnis?

Geschichte



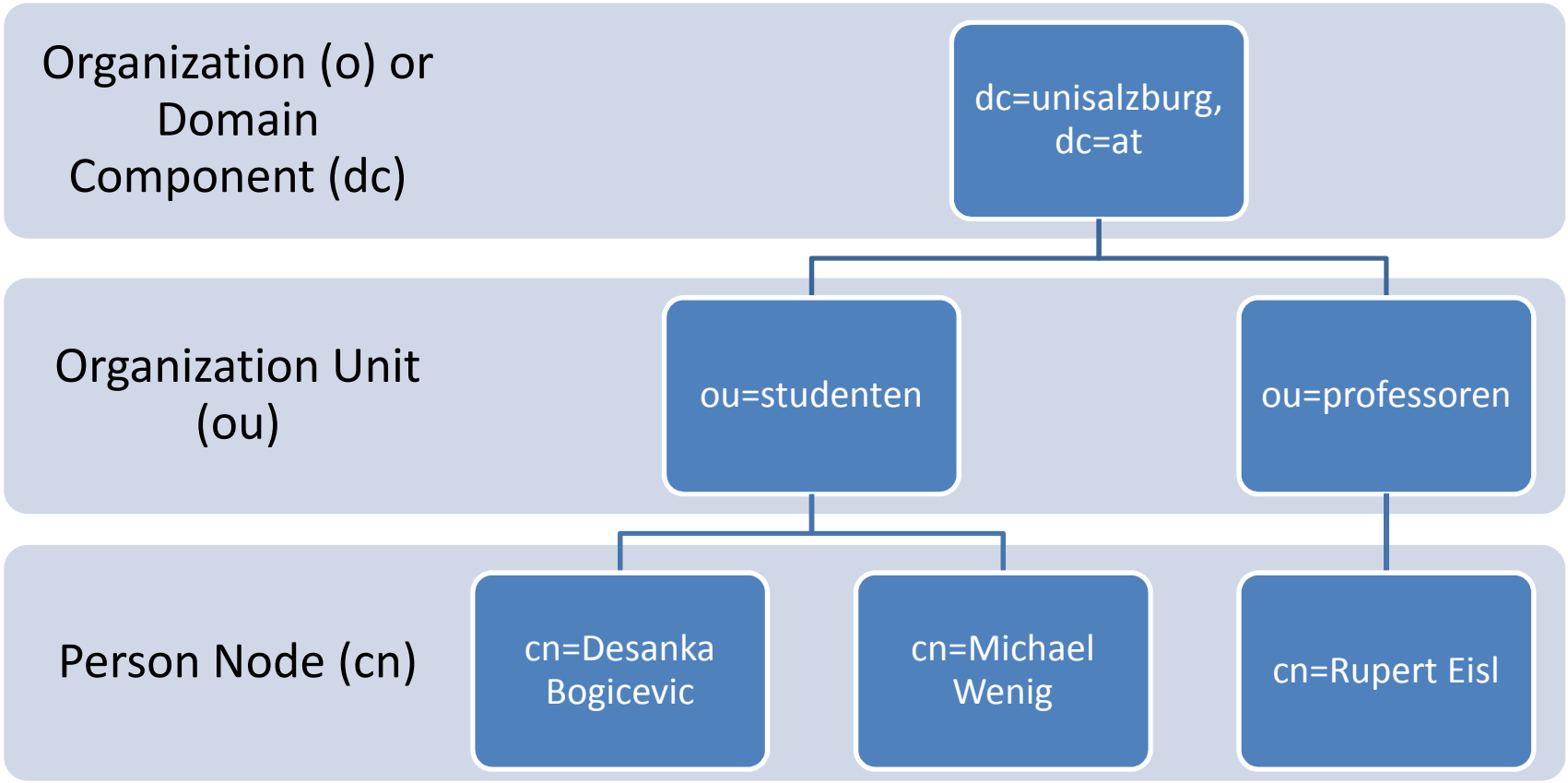
http://directory.apache.org/apacheds/basic-ug/1.2-some-background.html

Vorteile von LDAP

im Vergleich zur relationalen SQL Datenbank

- Optimiert auf Lesen
- Erweiterte Suchfunktionen
- Erweiterbare Datenstrukturen
- Standardkompatibilität
- Verteilte Daten

Struktur von Verzeichnissen

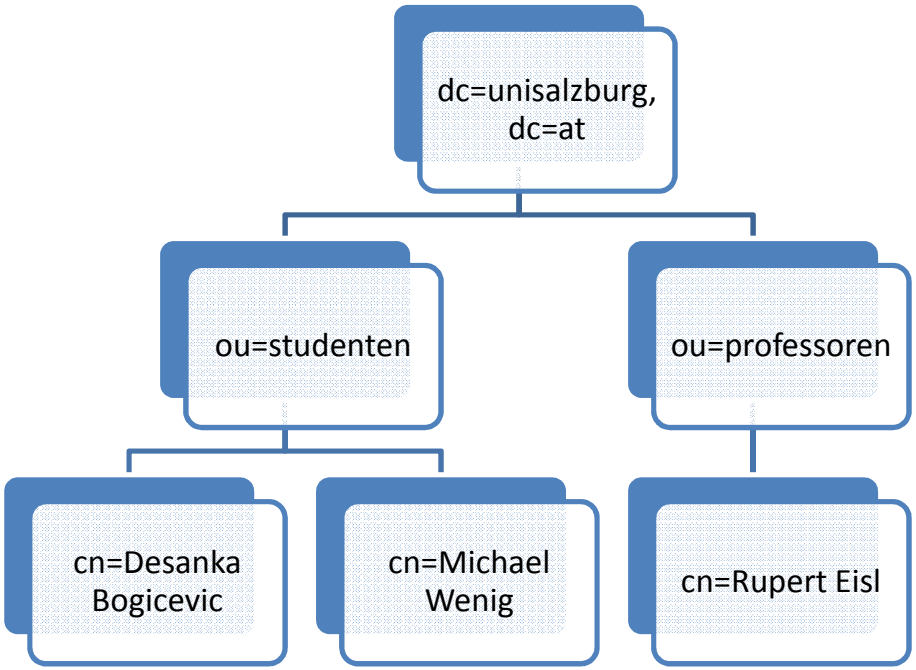


Namen

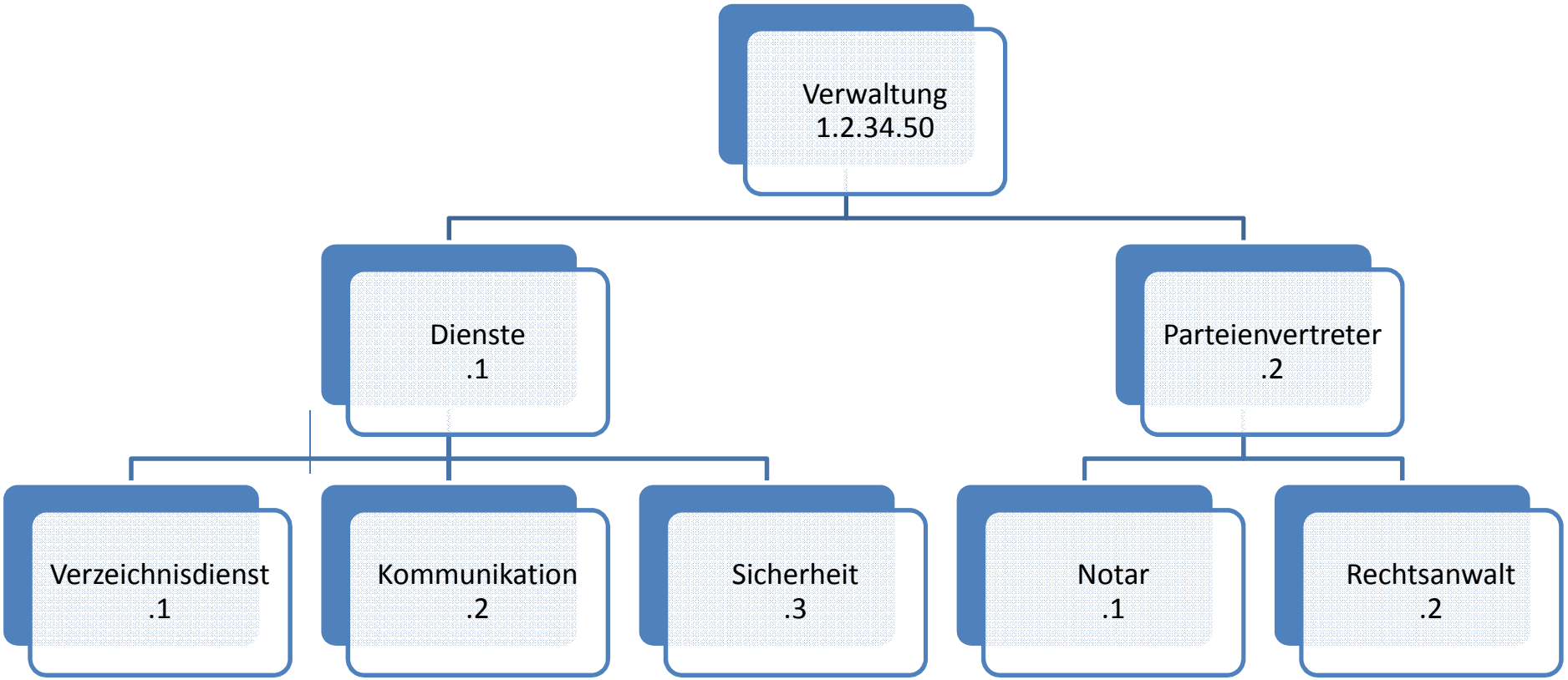
- **RDN:**
  cn=Rupert Eisl

  - **DN:**

  cn=Rupert Eisl,
  ou=professoren,
  dc=unisalzburg, dc=at



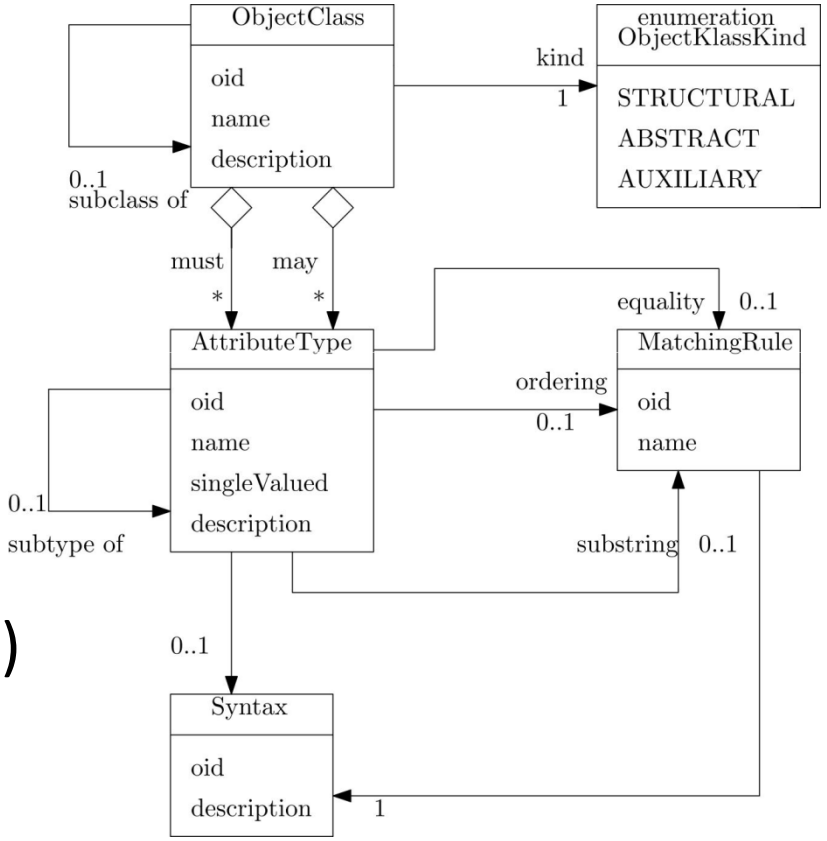
OIDs (Object Identifiers)



Das Schema

- Speicherung von Daten in einem Verzeichnis in Form von Einträgen
- Schema eines Verzeichnisses legt fest, wie gültige Einträge aufgebaut sind
- LDAP-Schema besteht aus folgenden Bestandteilen:

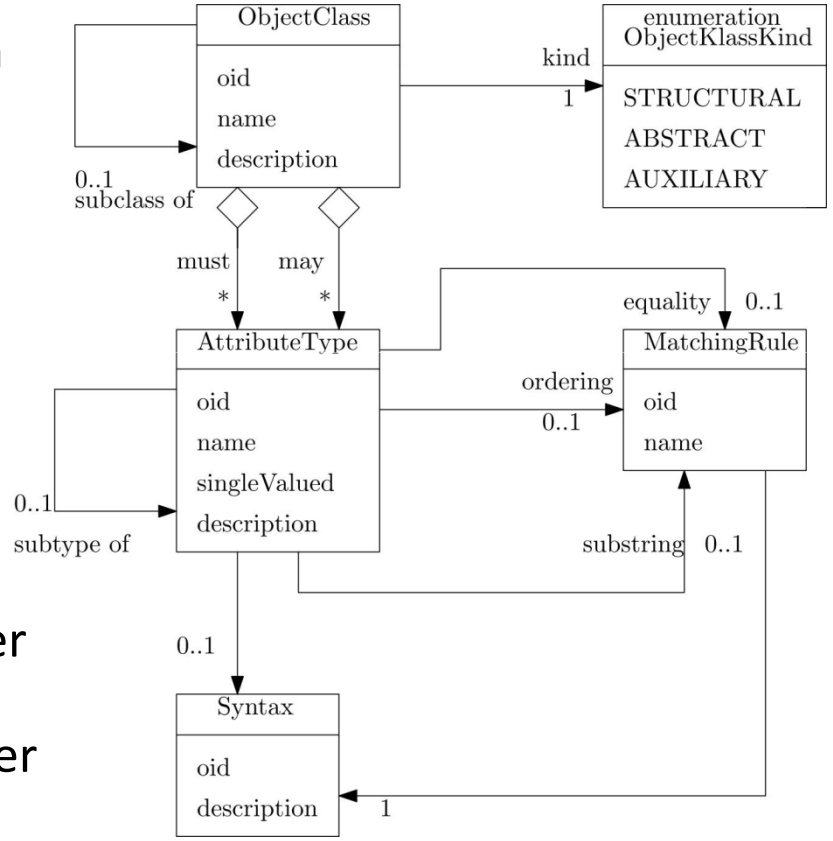
a) Attribute (Attributes)
b) Objektklassen(Object Classes)
c) Syntaxregeln(Syntaxes)
d) Vergleichsregeln(Matching Rules)



Attribute

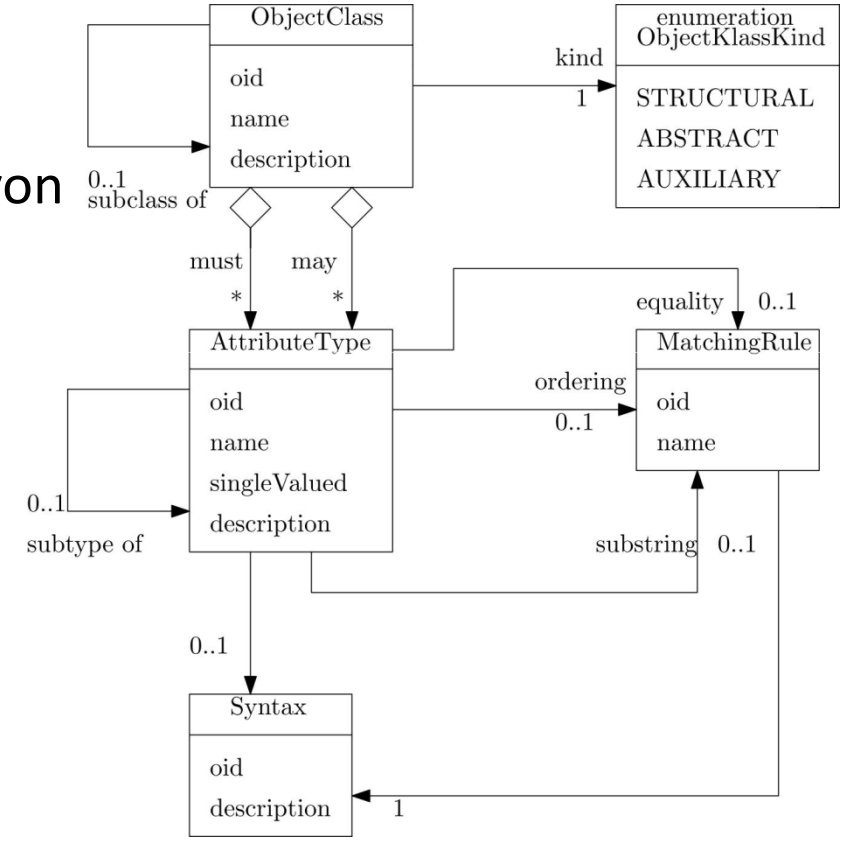
- Bildung von Einträgen in einem Verzeichnis aus Paaren von Attributen und Werten
- Beschreibung der erlaubten Eigenschaften von Einträgen
- Jedes Attribut besitzt Name und OID
- Weitere Informationen, z.B. Beschreibung des Attributes

- Betriebsattribute: für interne Verwaltungszwecke
- Beispiel: Zeitpunkt des Anlegens u. Der letzten Änderung eines Eintrags
- Werden normalerweise nur vom Server angelegt



Objektklassen

- Legen benötigte(<<must>>) und erlaubte (<<may>) Attribute eines Verzeichnis-Eintrags fest
- Jede Objektklasse im Schema ist von anderer Objektklasse abgeleitet
- Ausnahme: Oberklasse top
- Jeder Eintrag vom Typ einer Unterklasse ist auch Typ der Oberklasse!
- --> Kann erlaubte Attribute des Obertyps implementieren
- --> Muss benötigte Attribute des Obertyps implementieren
- Objektklassen können weiter unterteilt werden

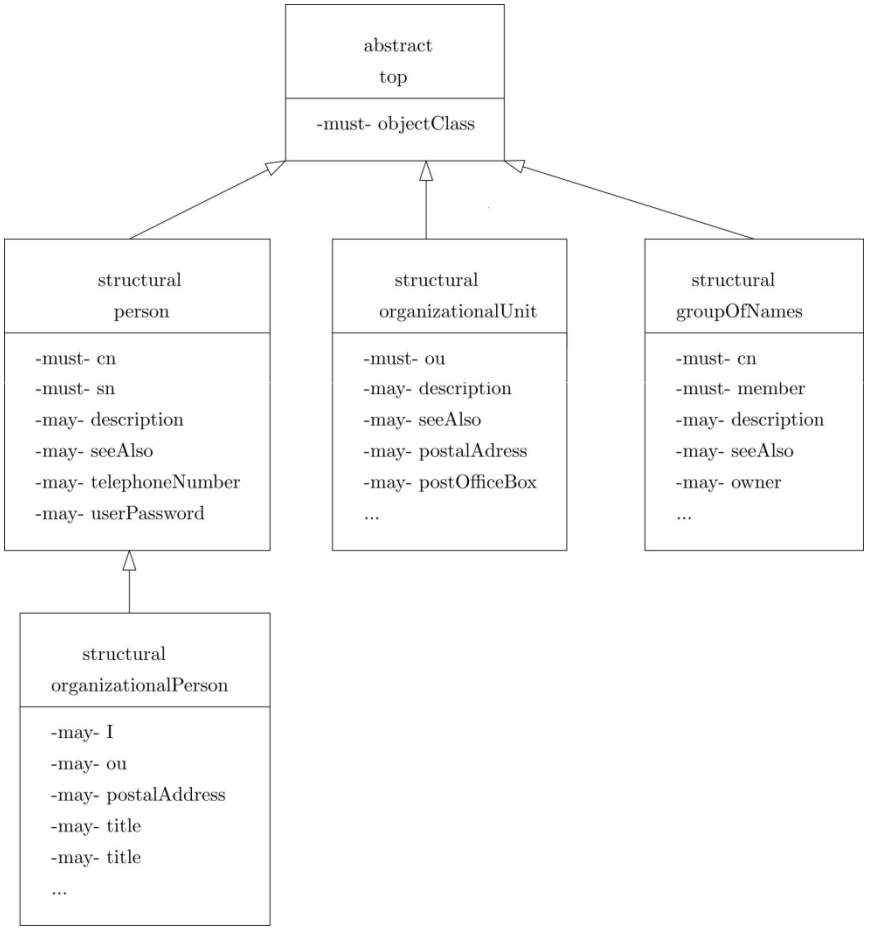


Objektklassen Unterteilung

- Es gibt drei Arten von Objektklassen:

a. Abstrakte Klassen
b. Strukturelle Klassen
c. Hilfsklassen

- Einträge können nicht aus abstrakten Klassen gebildet werden
- Andere Klassen werden von abstrakten Klassen abgeleitet
- Strukturelle Klassen dienen zur Erzeugung konkreter Einträge
- Hilfsklassen werden als "Schnittstelle" für unterschiedliche Objektklassen verwendet

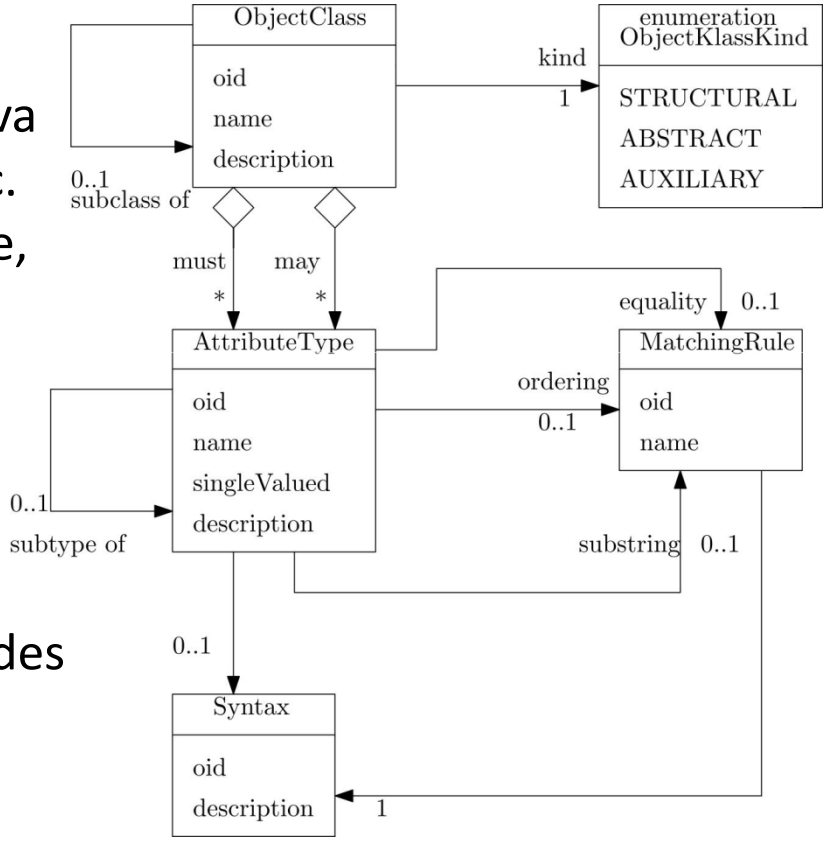


Syntaxregeln

- Syntax legt fest, welche Werte ein Attribut annehmen darf
- Analogie: Regeln für Datentypen in Java
- Beispiel: Regeln für Strings, Zahlen etc.
- Spezifische Syntaxregeln für Zertifikate, Telefonnummern usw.
- Standardmäßig besitzt jedes Attribut eine Syntax
- Sinn von Syntaxregeln:

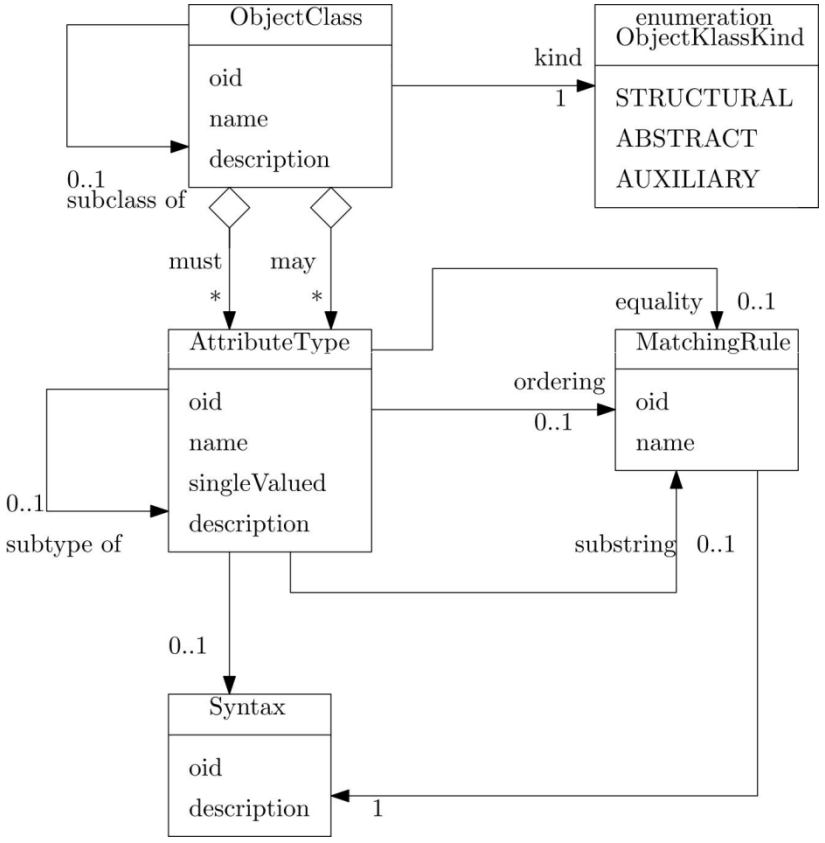
a. Client erfährt, welche Werte er bei Anfrage erwarten kann

b. Regeln wichtig bei Vergleichsregeln des Schemas



Vergleichsregeln

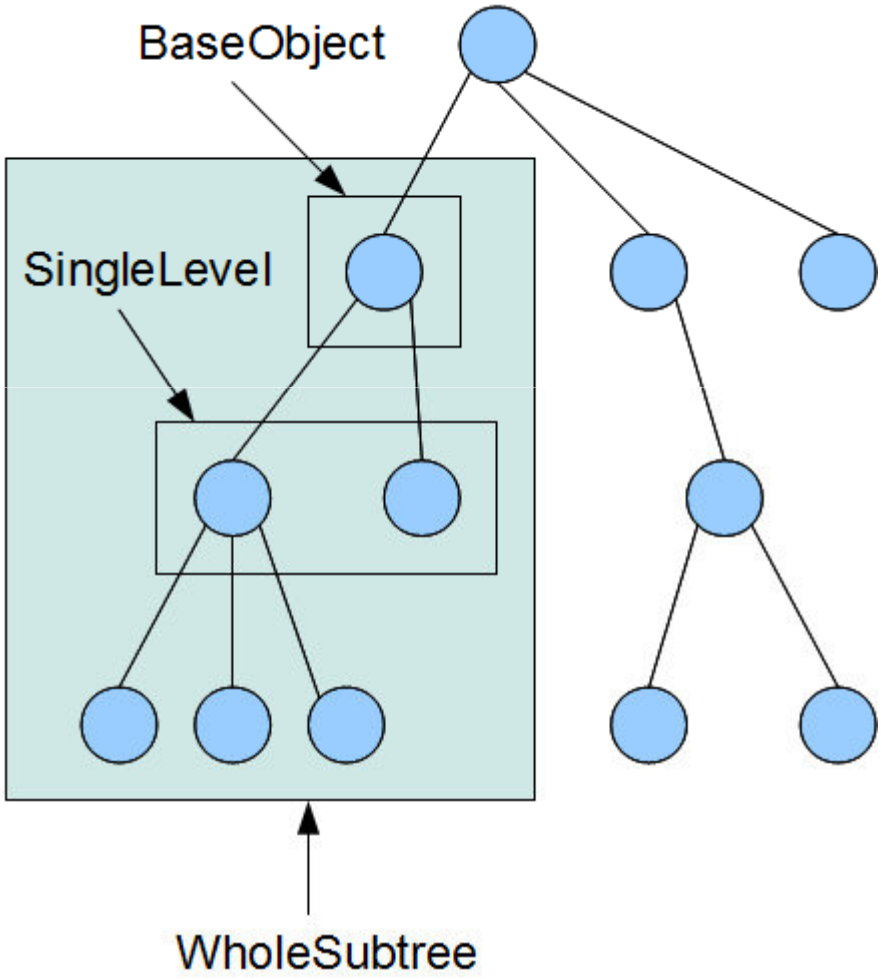
- Vergleichsregeln legen fest, wie Attribute verglichen werden
- Drei Kategorien: equality, ordering und substring
- Equality: Sind zwei Attribute gleich?
- Ordering: Ist ein Attribut größer/kleiner als das andere?
- Substring: Ist ein Attributwert Teilstring eines anderen Attributwerts?
- Sinn von Vergleichsregeln: Attributvergleiche können trotz gleicher Syntax unterschiedlich interpretiert werden
- Beispiel: Personennamen und Passwörter
- --> Unterscheidung Groß-/Kleinschreibung bei Passwörtern zwingend erforderlich!
- Aber: nicht unbedingt bei Personennamen



Suchen in LDAP

- Ziel Suchanfrage: Auffinden von Einträgen, die bestimmte Kriterien erfüllen
- Suche benötigt zunächst DN des Eintrages, von dem aus die Suche erfolgen soll
- --> Suche im Teilbaum ab diesem Eintrag
- Ausmaß der durchsuchten Knoten wird durch Scope-Parameter eingeschränkt
- Drei mögliche Werte für Scope:

a. BaseObject: nur die Base selbst
b. SingleLevel: alle Kinder der Base
c. WholeSubtree: Durchsuchen des gesamten Teilbaums



Suchfilter

- Jede Suchanfrage benötigt sog. Filterausdruck
- Filterausdruck gibt Kriterium an, das auf Attributwerten basiert
- Erfassen aller Einträge, die das Kriterium erfüllen
- Filterausdruck besteht aus einer Komposition von Bedingungen und den boolschen Operatoren AND, OR und NOT
- Ausdruck in Präfix-Notation

!(a)
→ (!(a))

(x) & (y) & (z)
→ (& (x) (y) (z))

(!(x)) & ((y) | (z))
→ (& ((!a)) (| (b) (c))

Suchfilter Operatoren

Filter	Operator	Beispiel	Attribute
Vorhandensein	=*	(email=*)	Attribut kommt mindestens einmal vor
Gleichheit	=	(sn=Wenig)	Attribute hat exakt diesen Wert
Teil-String	=	(sn=We*)	Attribut passt auf das Muster
Ordnung	<=, >=	(sn>=W)	Attribut entspricht der Ordnung
Ähnlichkeit	~=	(sn~=Weinig)	Attribut ähnelt dem Argument

LDAP-Operationen

Name	Funktion
Bind	Beginn einer Sitzung
Unbind	Ende einer Sitzung
Search	Suche
Add	Einfügen eines Eintrags
Delete	Löschen eines Eintrags
Modify	Ändern von Attributen eines Eintrags
Modify DN	Umbenennen/Verschieben eines Eintrags
Compare	Test eines Attributwerts eines Eintrags
Abandon	Abbrechen einer Operation
Extended	Aufruf serverspezifischer Operationen

Server & Client

auf einem Linux Rechnersystem

Software & Installation

- Ubuntu 12.04 LTS
- OpenLDAP v2.4.38
  - ./configure
  - make depend
  - make
  - sudo make install
- Apache Directory Studio 2.0.0
  - Download & Execute

Server Konfiguration - slapd.config

- Include /usr/lo…..ap/schema/core.schema
  ….
  Include /usr/lo…..ap/schema/java.schema

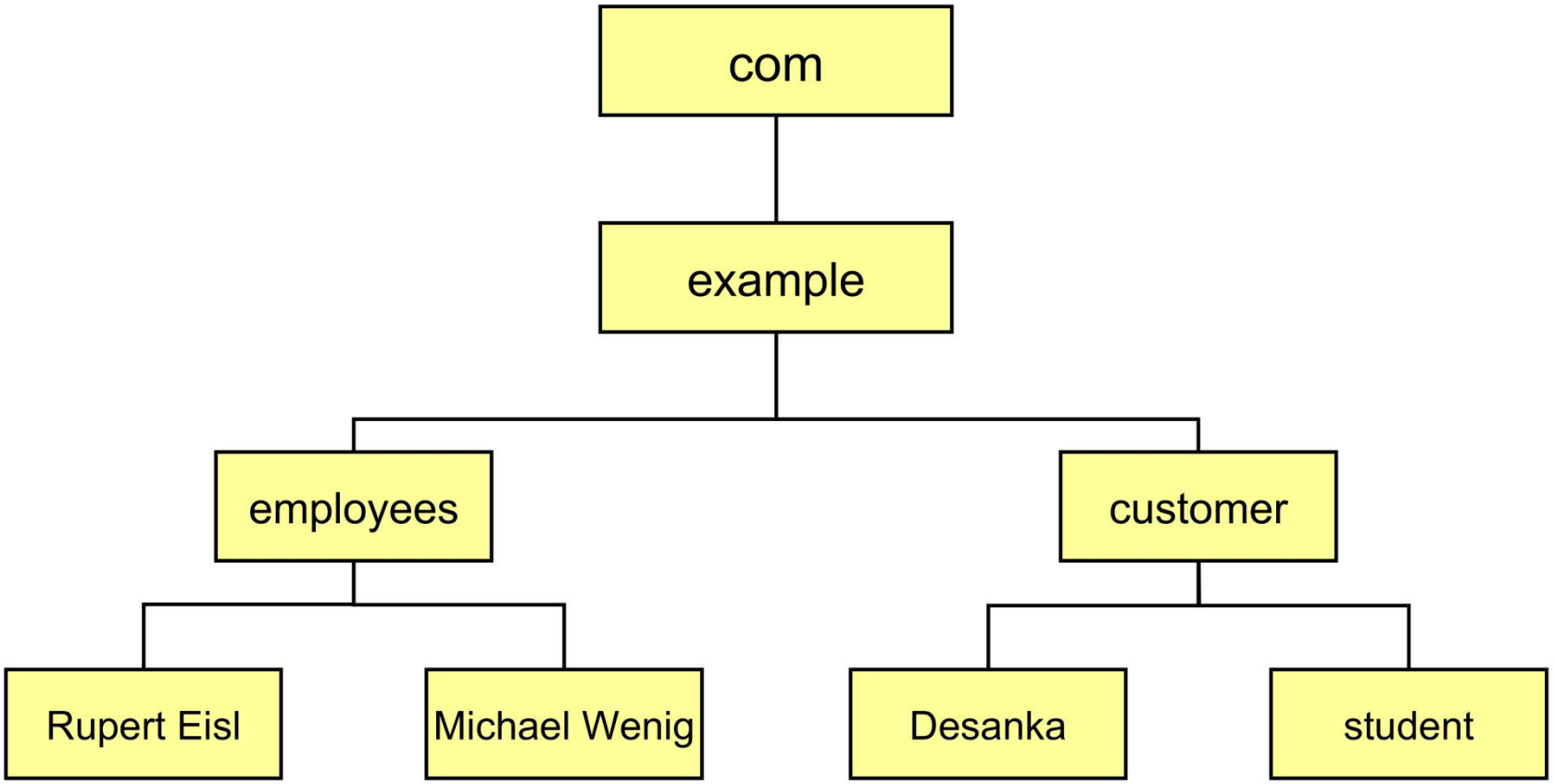
- Database bdb
  suffix "dc=example,dc=com"
  rootdn "cn=Manager,dc=example,dc=com"
  rootpw {SSHA}ObQkxj1JGPaaPNbByq6Wef3GZlrbWoGu

- access to *
  by dn.exact="cn=Manager,dc=example,dc=com" write
  by * read

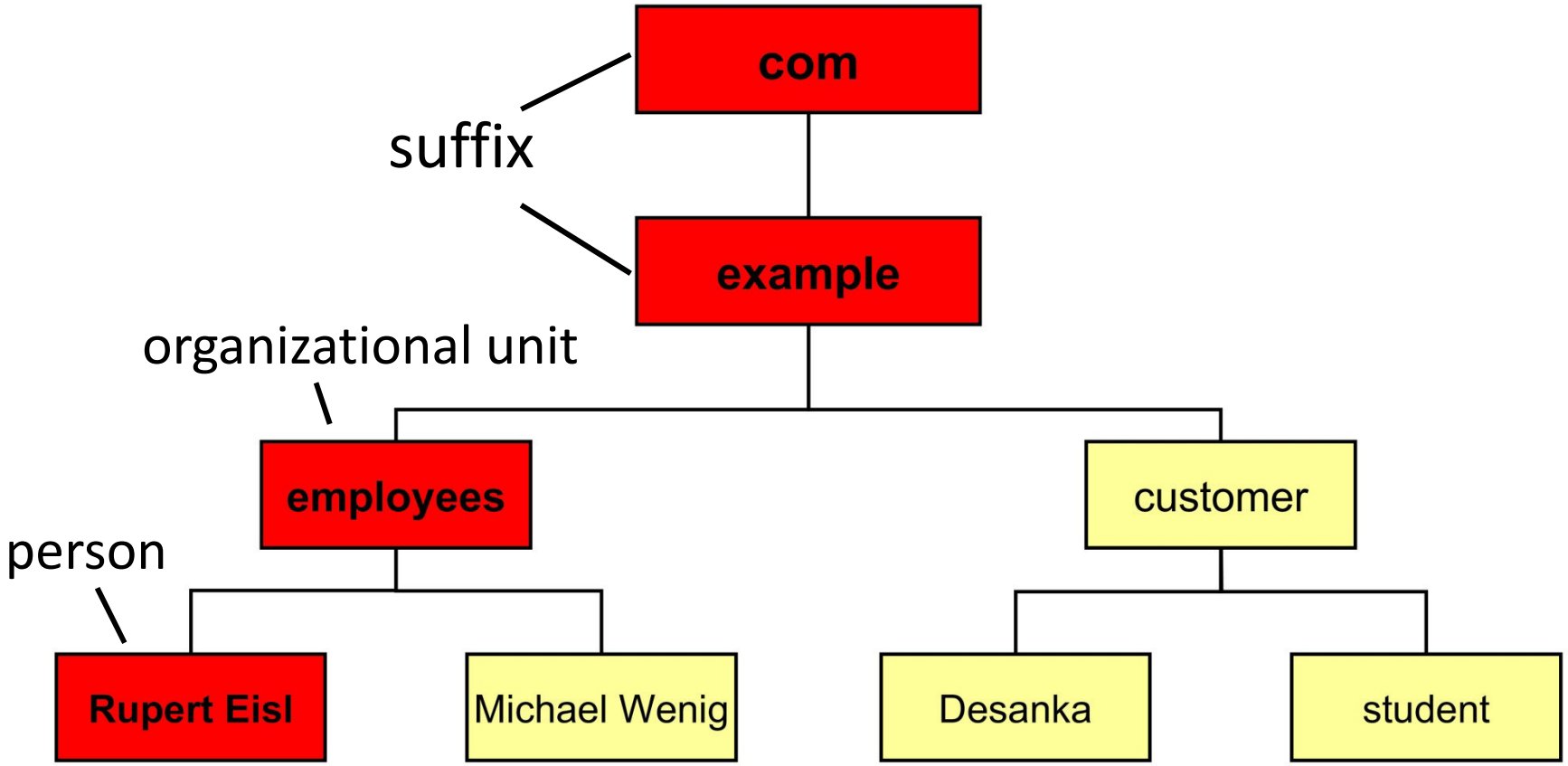
Server:

- Boot:
  - /usr/local/libexec/slapd
- Shutdown:
  - sudo kill -INT `cat /usr/local/var/run/slapd.pid`

Hierarchie


com
example
employees
customer
Rupert Eisl
Michael Wenig
Desanka
student

Hierarchie


com
suffix
example
organizational unit
employees
customer
person
Rupert Eisl
Michael Wenig
Desanka
student

VIDEO

Quellen

- Stefan Zörner: „LDAP für Java-Entwickler Einstieg und Integration“ entwickler.press, Frankfurt am Main 2013, 978-3-86802-094-6
- http://www.mitlinx.de
- http://www.galileocomputing.de
- http://www.bsi.bund.de
- http://www.ubuntu.com/
- https://www.virtualbox.org/
- http://directory.apache.org/studio/
- http://www.openldap.org/
- AVS Video Editor