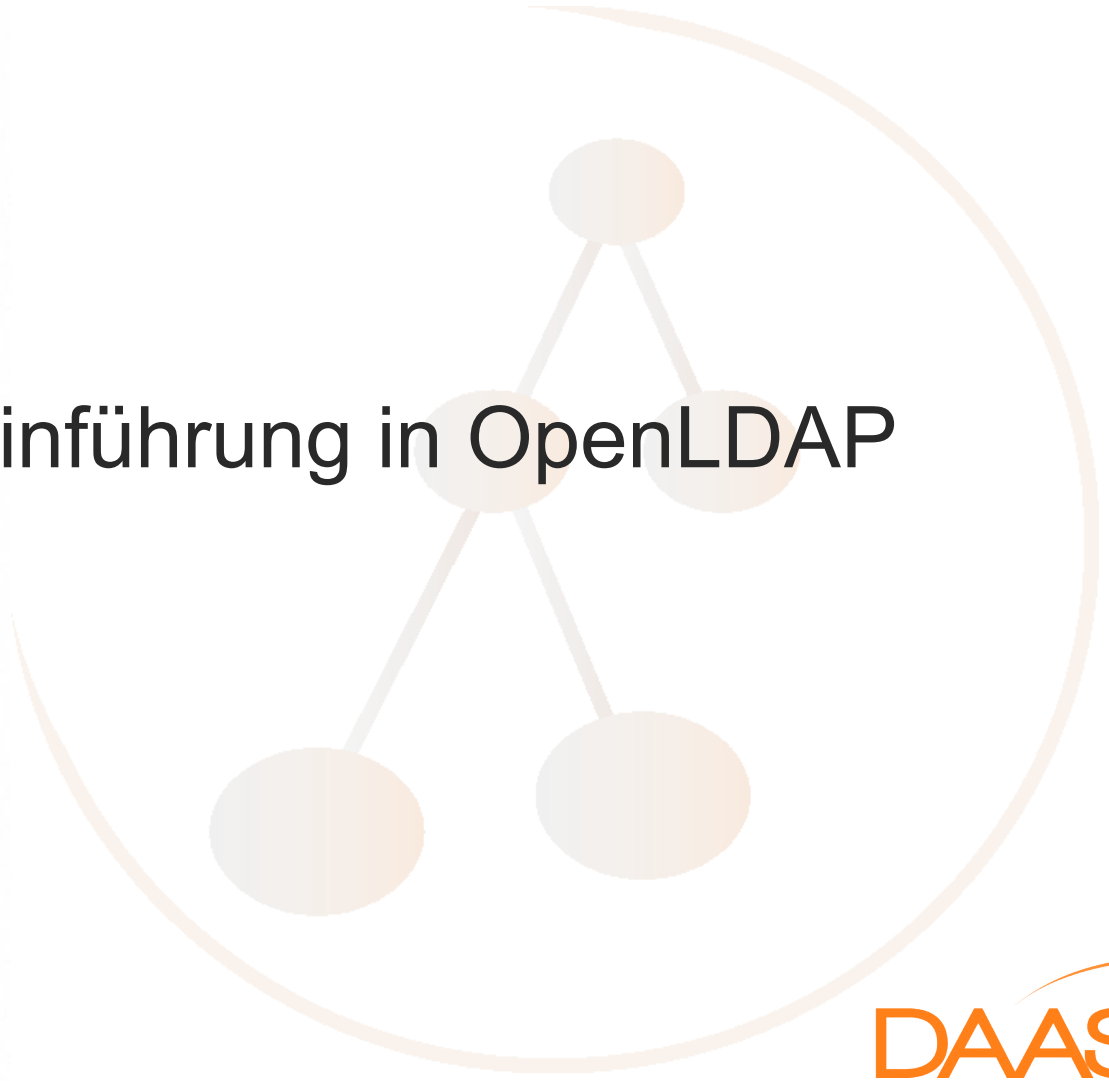
OpenLDAP

Autor Peter Gietz,
DAASI International GmbH

© 2015 DAASI International GmbH

Einführung in OpenLDAP



DAASI International

© 2015 DAASI International GmbH

Technologie

- Referenz-Implementierung des RFC [TODO]
- Impelentiert in C
- Aktuelle Version 2.4.40
- Speichert Daten in verschiedenen Backends
  - BDB / HDB (Berkeley)
  - MDB (Memory Mapped)
  - Text-Dateien (LDIF)
- Konfiguration
  - Datei
  - LDIF (cn=config)

DAASI International

© 2015 DAASI International GmbH

Vorteile

- Sehr gute Performanz auch bei großen Datenmengen (Mehrere millionen Einträge)
- Einfaches Erstellen und Einbinden eigener Schema
- Vielzahl fertiger Overlays (Erweiterungen)
  - Referential integrety
  - MemberOf
  - AccessLog
- Eigene Erweiterungen (in C) möglich
- Protokollierung von Änderungen über Overlay AccessLog im Server
- Feingranulare ACLs

DAASI International

© 2015 DAASI International GmbH

Konfiguration

- Zwei Möglichkeiten: Datei und „cn=config“
- Globale Parameter:
  - Einbinden von Schema
  - Laden von Modulen (z.B. Overlays)
  - Konfiguration der Verbindungssicherheit
  - Globale ACLs
- Parameter pro Backend:
  - Manager-Account
  - Definieren der Attribute im Index
  - Konfiguration der geladenen Overlays
  - Replikation
  - Backend-ACLs

DAASI International

© 2015 DAASI International GmbH

Konfiguration über Datei

- Kontra
  - Statische Konfiguration → Erfordert Neustart bei Änderungen
  - Kann nicht auf andere Server repliziert werden
- Pro
  - Erlaubt Kommentare in der Konfiguration
  - Einfach mit einem Texteditor Änderbar
  - Im Besonderen sind Schema-Änderungen leicht möglich

DAASI International

© 2015 DAASI International GmbH

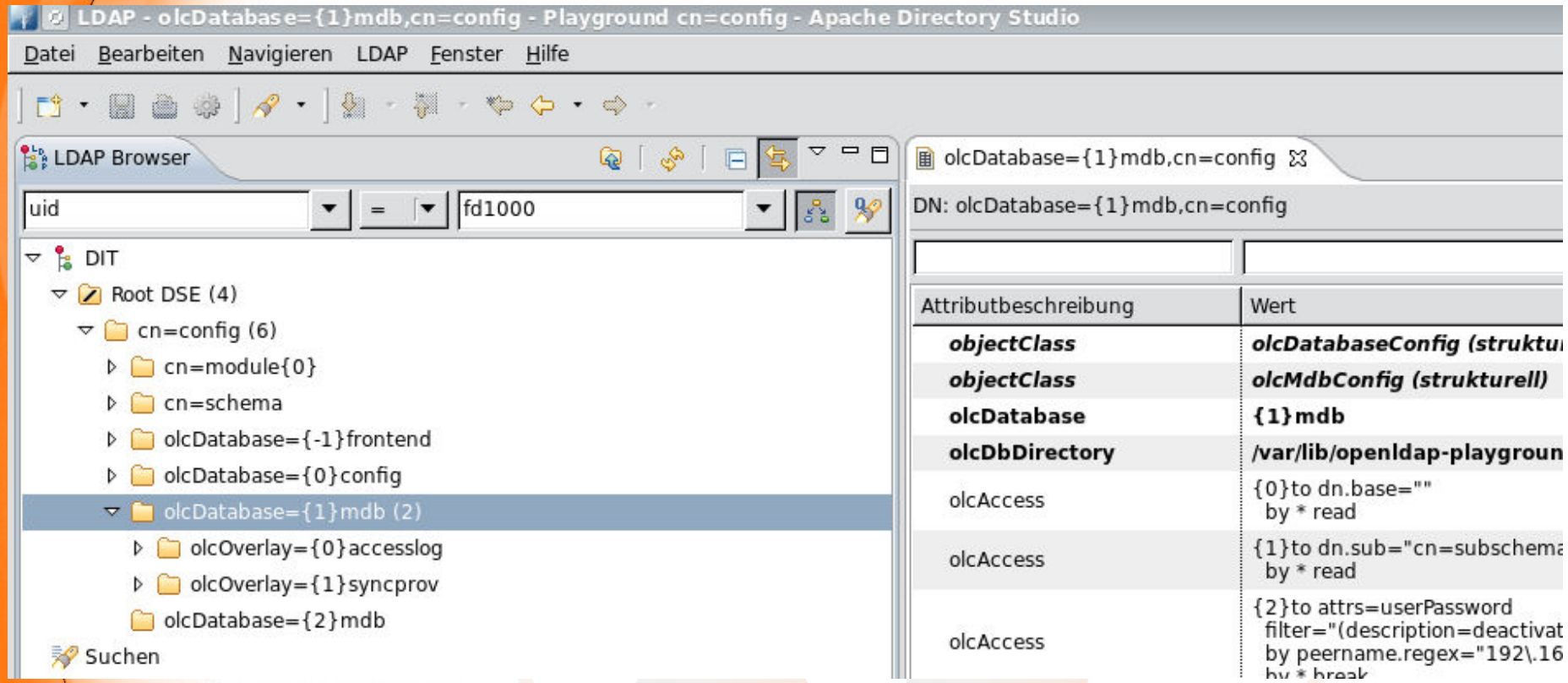
Konfiguration über cn=config

- Kontra
  - Keine Kommentare in der Konfiguration möglich
  - Umständliche Konfiguration über LDAP-Befehle
  - Unübersichtliche Darstellung
- Pro
  - Dynamische Konfiguration → Viele Einstellungen werden ohne Neustart übernommen (z.B. ACLs)
  - Replikation z.B. in Multi-Provider-Umgebung möglich

DAASI International

© 2015 DAASI International GmbH

Konfiguration über cn=config



© 2015 DAASI International GmbH

Aufbau eines Attributs im Schema

```
attributetype ( 2.16.840.1.113730.3.1.241
        NAME 'displayName'
        DESC '[...]'
        EQUALITY caseIgnoreMatch
        SUBSTR caseIgnoreSubstringsMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
        SINGLE-VALUE )
```

DAASI International

© 2015 DAASI International GmbH

Aufbau einer Objektklasse im Schema

```
objectclass ( 2.16.840.1.113730.3.2.2
    NAME 'inetOrgPerson'
    DESC '[...]'
    SUP organizationalPerson
    STRUCTURAL
    MAY ( [...] $ displayName $ […] )
    MUST () )
```

DAASI International

© 2015 DAASI International GmbH

Zugriffskontrolle (ACLs)

- Eine ACL besteht aus vier Teilen
  - <what> Für welchen Bereich ist die ACL gültig
  - <who> Für wen ist die ACL gültig
  - <access> Welche Rechte hat <who>
  - <control> Flags zur Kontrolle bei der Verarbeitung der nachfolgenden ACLs
- Eine ACL ist folgendermaßen aufgebaut:

  access to <what>

  [by <who> [<access>] [<control>]]+

DAASI International

© 2015 DAASI International GmbH

Diese Berechtigungen können vergeben werden

- 0: Keinerlei Zugriff
- d: Fehlermeldungen dürfen angezeigt werden
- x: Authentifizierung ist erlaubt
- c: Das Vergleichen von Attributen ist erlaubt
- s: Das Anwenden von Suchfiltern ist erlaubt
- r: Ein Lesezugriff wird gestattet
- w: Ein Schreibzugriff wird gestattet
- m: Gestattet Schreibzugriff auf operationale Attribute
- Kombinationen sind möglich, z.B. dxcs
- Reihenfolge der Angabe ist nicht relevant

DAASI International

© 2015 DAASI International GmbH

Berechtigungen können auf diese Bereiche vergeben werden

- * alle Daten
- dn.exact=<DN>: Der DN
- dn.regex=<regex>: Alle DNs, die auf den Regulären Ausdruck passen
- dn.base=<DN>: Der DN
- dn.one=<DN>: Alle direkten Untereinträge von DN
- dn.children=<DN>: Alle Untereinträge von DN
- dn.subtree=<DN>: Der DN und alle Untereinträge

DAASI International

© 2015 DAASI International GmbH

Vielen Dank für Ihre Aufmerksamkeit.

DAASI International GmbH

www.daasi.de

Telefon: 07071 4071090

E-Mail: info@daasi.de

© 2015 DAASI International GmbH