

OpenLDAP

Autor Peter Gietz,
DAASI International GmbH

Einführung in OpenLDAP

Technologie

- Referenz-Implementierung des RFC [TODO]
- Implementiert 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)

Vorteile

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

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

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

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

Konfiguration über cn=config

The screenshot shows the Apache Directory Studio interface. The title bar reads "LDAP - olcDatabase={1}mdb,cn=config - Playground cn=config - Apache Directory Studio". The menu bar includes "Datei", "Bearbeiten", "Navigieren", "LDAP", "Fenster", and "Hilfe". The toolbar contains various icons for file operations and navigation. The "LDAP Browser" pane on the left shows a tree view of the LDAP directory structure. The selected entry is "olcDatabase={1}mdb (2)", which is expanded to show sub-entries: "olcOverlay={0}accesslog", "olcOverlay={1}syncprov", and "olcDatabase={2}mdb". The search field at the bottom left contains "uid" and "fd1000". The right pane displays the details for the selected entry, showing the DN "olcDatabase={1}mdb,cn=config" and a table of attributes.

Attributbeschreibung	Wert
objectClass	olcDatabaseConfig (strukturiert)
objectClass	olcMdbConfig (strukturell)
olcDatabase	{1}mdb
olcDbDirectory	/var/lib/openldap-playground
olcAccess	{0}to dn.base="" by * read
olcAccess	{1}to dn.sub="cn=subschema" by * read
olcAccess	{2}to attrs=userPassword filter="(description=deactivated)" by peername.regex="192\.\d{1,3}\.\d{1,3}\.\d{1,3}" by * break

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 )
```

Aufbau einer Objektklasse im Schema

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

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>]]+

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

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

Vielen Dank für Ihre Aufmerksamkeit.

DAASI International GmbH

www.daasi.de

Telefon: 07071 4071090

E-Mail: info@daasi.de

