OpenLDAP, adieu?
Ein LDAP Server in Java:
ApacheDS Reality Check

Stefan Zörner

Enterprise ARCHITEKTUR KONFERENZ 2007
APPLICATION LIFECYCLE & BUSINESS PROCESS MANAGEMENT

oose. Innovative Informatik

Zusammenfassung.

Short Talk: OpenLDAP, adieu? Ein LDAP Server in Java: ApacheDS Reality Check

Das Apache Directory Projekt entwickelt einen Verzeichnisdienst in 100 % purem Java. Ergebnis: ApacheDS – der erste Open Source Server, der die LDAP-Zertifizierung der Open Group erfolgreich absolviert hat. Konkurrenz für OpenLDAP und Co.? Committer Stefan Zörner gibt einen kurzen Überblick über die Projektziele, den Server selbst sowie dessen Eigenschaften und Fähigkeiten. Wo macht sein Einsatz Sinn?

Verzeichnisdienste, LDAP

Verzeichnisse, Verzeichnisdienste

- spezielle Datenspeicher, die Einträge mit relevanten Eigenschaften in einer Baumstruktur speichern
- optimiert auf Lese- und Suchoperationen, auf Kosten der Performance beim Schreiben

Lightweight Directory Access Protocol

- Standardisierter, TCP/IP-basierter Zugriff auf Verzeichnisdienste (Client/Server-Prinzip)
- hohe Verbreitung, Clients und Server unterschiedlicher Anbieter sind sehr gut austauschbar

Klassische Einsatzgebiete.

- Unternehmensweite Speicherung von …
  - Netzwerkressourcen (Rechner, Drucker, …)
  - Benutzern, inkl.
    - Kontaktdaten (Telefonbuch)
    - Organisationsstruktur (Berichtswege)
    - Kennwörtern (inkl. Forcierung von Richtlinien)
  - Benutzergruppen
- Realisierung von Verteilungsaspekten (Repliken)
- Zentrale Datenbasis Authentifizierung / Autorisierung

Typen von LDAP-Clients.

Applikationen für Endanwender

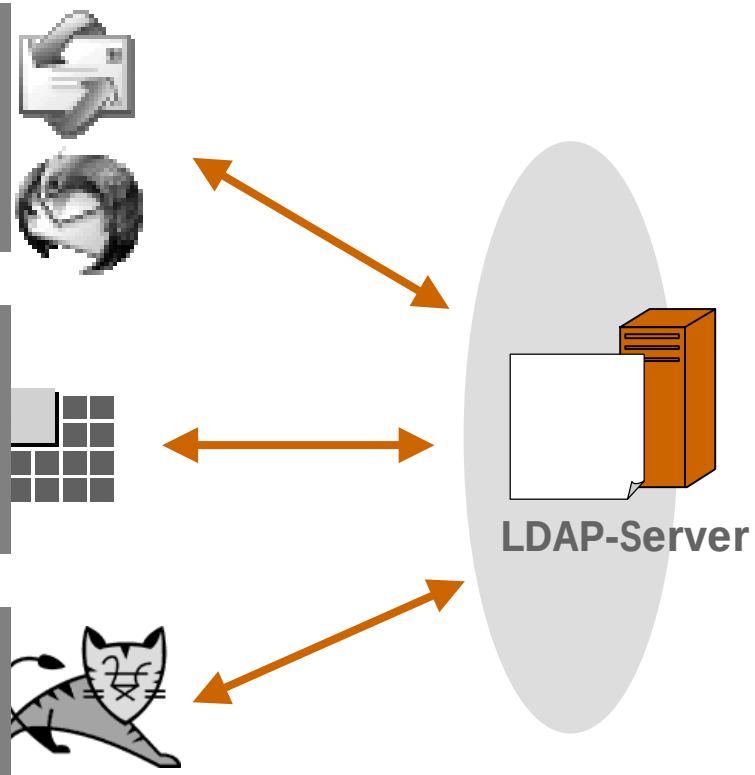
z.B. Mailclients (Outlook, Thunderbird, ...)
LDAP in der Regel vor Benutzer „versteckt“

Anwendungen für Spezialisten / Administratoren

Herstellerspezifische oder –unabhängige Werkzeuge, LDAP ist unmittelbar „erlebbar“

Serverlösungen, die Verzeichnisse integrieren

z.B. Mailserver, Webserver, ...
LDAP-Kenntnisse zur Konfiguration erforderlich



LDAP-Implementierungen.

Kommerzielle Server (kleine Auswahl):

- Microsoft Active Directory
- Sun Java System Directory Server
- IBM Tivoli Directory Server
- Novell eDirectory

Open Source (Auswahl):

- OpenLDAP
- Fedora Directory Server
- OpenDS
- Apache Directory Server

Was ist ApacheDS ?

- LDAPv3-Server, 100% in Java realisiert
- Standalone betreibbar (z.B. Windows Service)
- alternativ: als einbettbare Komponente
- Kerberos KDC
- Weitere Protokolle werden unterstützt (z.B. NTP)

➔ **http://directory.apache.org**

Besondere Stärken.

Apache Directory Server:

- 100% in Java realisiert
- Open Source, Apache Software License
- Einbettbar („embeddable“)
- Erweiterbar
- Standard-kompatibel

Einbettbar.

Server-Kern ist Java-Komponente

- Core realisiert als JNDI-Provider, über Standard-Schnittstelle programmatisch ansprechbar (in JVM)
- Komplette Konfiguration kann programmatisch erfolgen
- Auch embedded Version kann z.B. mit Netzwerk starten

Bereits erfolgreich eingebettet z.B. in

- JBoss
- Apache Geronimo
- WebSphere Application Server (als Custom User Registry)
- Servlet 2.4 Web Application

Erweiterbar.

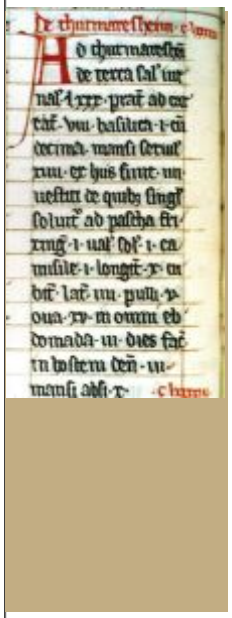
Realisiert in reinem Java, konfigurierbar mit Spring

- Attraktive Plattform für Java-Entwickler
- Verwendung üblicher Frameworks und Technologien (ab ApacheDS 1.5: Java 5 SE)

Eine Architektur, offen für Erweiterungen

- Eigene Partitionen zur Datenspeicherung
- Interceptoren, um den Server um beliebige Funktionalität zu erweitern
- Custom Schemata für eigene Objektklassen, Attribute usw.

Standardkonform (1).



Kernfunktionalität orientiert sich an Industrienormen

- Implementierung der LDAPv3 relevanten RFCs, u.a. RFC 4510 („LDAP: Technical Specification Road Map“)
- Wichtige Schemata out-of-the Box, z.B. X.500 Core (person, ou, …), inetOrgPerson, Java-Objekte
- Gängige Security-Features, z.B. LDAPS, SASL (ab ApacheDS 1.5)

Standardkonform (2).

ApacheDS hält LDAP-Zertifizierung der Open Group

- September 2006: ApacheDS 1.0 ist erster Open Source Server mit „LDAP Certified“-Stempel
- Hintergrund: Spende der Open Group (Bereitstellung der Test Suite, Unterstützung beim Zertifizierungsprozess)
- Auflage: Jeder Release von ApacheDS 1.0 muss Compliance-Tests erfolgreich durchlaufen
- Plan: ApacheDS 1.5 ebenfalls offiziell zertifizieren lassen

THE Open GROUP
Making standards work®

➔ http://www.opengroup.org

Wie fange ich an?

Herunterladen + Installieren

- http://directory.apache.org
- Native Installer verfügbar für
  - Linux, Windows, MacOS, Solaris

Alternative: Selber bauen

- Subversion, Maven 2

Basic User‘s Guide

- „Getting started with ApacheDS“
- Gedacht primär für ApacheDS- und LDAP-Neulinge

Mögliche Einsatzgebiete.

Automatisierte Tests
- Embedded Server schnell gestartet/gestoppt
- vollständig programmatisch konfigurierbar

Entwicklungs- und Testumgebungen
- Schlanke Implementierung, standalone schnell gestartet
- Einbettbar in gängige Applikationsserver, und damit auch in gängige IDEs

Experimentierplattform für neue Features
- Solide Basis zur Implementierung neuer Funktionalität, z.B. neue Controls oder Extended Operations, in Java

Ausblick: Version 1.5

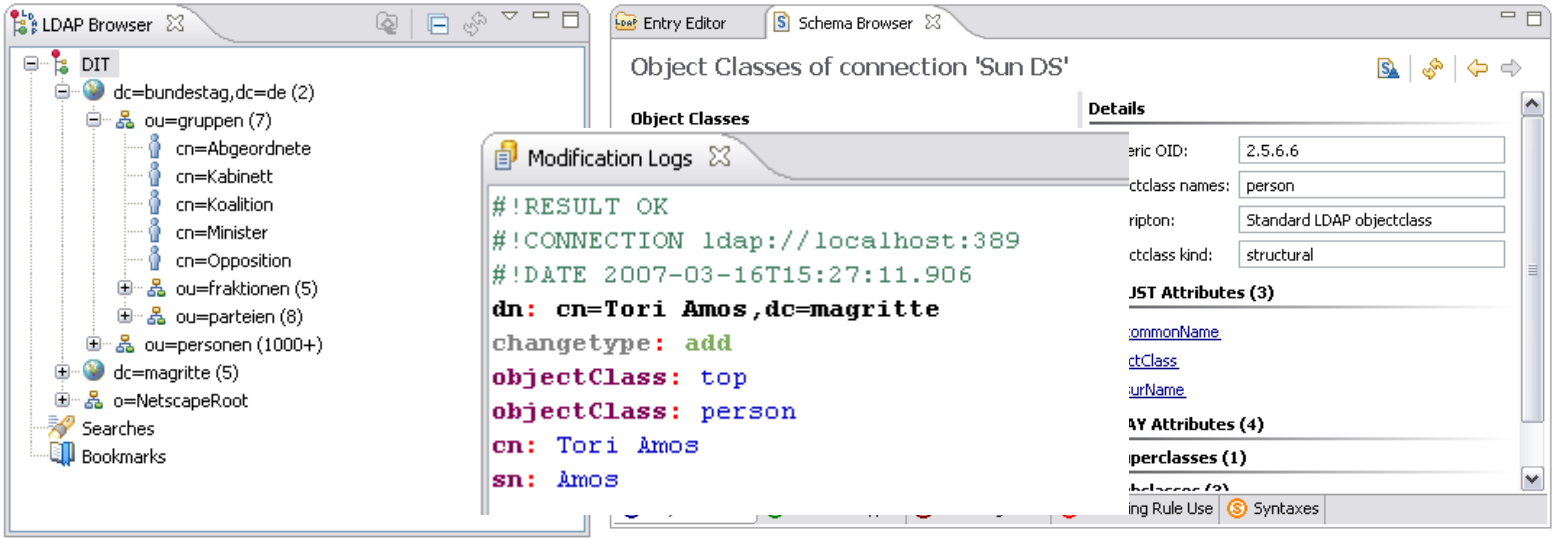
Wichtige Enterprise-Features, u.a.

- Dynamisches Schema
- Multimaster-Replikation
- SASL-Mechanismen
- Extended Operation StartTLS
- ...

➔ **http://directory.apache.org/apacheds/1.5/**

LDAP Studio.

- Eclipse-Plugins / RCP-Anwendung für LDAP
- Entry Editor, Schema Browser, LDIF-Editor …



➔ **http://directory.apache.org/ldapstudio/**

Ich bin gespannt auf Ihre Fragen!

Stefan Zörner

Stefan.Zoerner@oose.de :: szoerner@apache.org

Enterprise ARCHITEKTUR KONFERENZ 2007

APPLICATION LIFECYCLE & BUSINESS PROCESS MANAGEMENT

oose. Innovative Informatik