Kurs-Dokumentation

Zentrum für Informatik ZFI AG

LDAP (LDAP)

http://www.zfi.ch/LDAP

Weitere Infos finden Sie unter www.zfi.ch oder via Adresse:

Zentrum für Informatik ZFI AG
Zentralsekretariat
Rütistrasse 28
CH-8952 Zürich-Schlieren
Telefon: 044 732 40 00
Telefax: 041 530 31 68

Zürich, Basel, Bern, ZÃ¼rich, Schweiz

Titel	**LDAP**
Untertitel	**LDAP**
Einleitung	**LDAP basiert auf dem Client/Server-Modell und kommt bei sogenannten Verzeichnisdiensten (engl. directories bzw. directory services) zum Einsatz. Es beschreibt die Kommunikation zwischen dem sogenannten LDAP-Client und dem Verzeichnis (Directory Server). Aus einem solchen Verzeichnis können objektbezogene Daten, z. B. Personendaten, Rechnerkonfigurationen etc. ausgelesen werden. Die Kommunikation erfolgt auf Basis von Abfragen. Das Verzeichnis kann beispielsweise ein Adressbuch enthalten: In seinem E-Mail-Client stösst ein Nutzer die Aktion Suche die Mailadresse von Joe User an. Der E-Mail-Client formuliert eine LDAP-Abfrage an das Verzeichnis, das die Adressinformationen bereitstellt. Das Verzeichnis formuliert die Antwort und übermittelt sie an den Client:joe.user@example.org. Mittlerweile hat sich im administrativen Sprachgebrauch eingebürgert, dass man von einem LDAP-Server spricht. Damit meint man einen Directory-Server, dessen Datenstruktur der LDAP-Spezifikation entspricht und der über das LDAPv3-Protokoll Daten austauschen kann. Das Protokoll bietet alle Funktionen, die für eine solche Kommunikation notwendig sind: Anmeldung am Server (sogenannte bind), die Suchabfrage (Suche mir bitte alle Informationen zum Benutzer mit dem Namen "Joe User") und die Modifikation der Daten (Ändere das Passwort beim Benutzer Joe Cool). Neuere Implementierungen, die über RFC 2251 hinausgehen und Gegenstand für eine mögliche Erweiterung des Protokolls sind, berücksichtigen die Replikation der Daten zwischen verschiedenen Verzeichnissen. LDAP wurde an der Universität von Michigan (UMich) entwickelt und 1993 erstmals im RFC 1487 vorgeschlagen. Gleichzeitig stellte die UMich die erste Serverimplementierung vor, die heute als "UMich-LDAP" bekannt ist. Das LDAP ist eine vereinfachte Alternative zum Directory Access Protocol (DAP), welches als Teil des X.500-Standard spezifiziert ist. Der X.500-Standard ist sehr umfangreich und setzt auf einem vollständigen ISO/OSI-Stack auf, was die Implementierung schwierig und hardwareintensiv machte. LDAP wurde mit dem Ziel entwickelt, Verzeichnisdienste einfacher und somit populärer zu machen. LDAP setzt auf einem TCP/IP-Stack auf und implementiert nur eine Auswahl der DAP-Funktionen und Datentypen. Dadurch liess sich LDAP auch auf Arbeitsplatzrechnern der frühen Neunzigerjahre implementieren und gewann eine breite Anwendungsbasis. LDAP kommt heutzutage in vielen Bereichen zum Einsatz, z. B.:- Adressbuch (z. B. Apple Adressbuch, IBM Lotus Notes, Microsoft Outlook, Mozilla Thunderbird, Novell Evolution, OpenOffice.org Serienbrieferstellung, Ritlabs The Bat!)- Benutzerverwaltung (z. B. Apple Open Directory, POSIX Accounts, Microsoft Active Directory Service)- Authentifizierung (z. B. PAM)- Verwaltung von Benutzerdaten für SMTP- POP- und IMAP-Server, sowie Antispam-Software (z. B. postfix, qmail, exim, Lotus Domino, sendmail, Cyrus, Courier, SpamAssassin und Amavisd)**
Ihr Nutzen	**Der Kurs befähigt die Teilnehmenden, Verzeichnisdienste mit LDAP richtig zu planen, zu konfigurieren, einzusetzen und zu unterhalten.**
Vorausetzungen	**Gute Informatik-Kenntnisse, Erfahrung in der Administration von Server-Betriebssystemen.**

Teilnehmerkreis	**System-Administratoren, welche LDAP nutzen wollen.**
Unterlagen	**ZFI Kursunterlagen**
Folgekurse	
Inhalt	**- Einführung in LDAP** **- Verzeichnisdienste** **- Von X.500 zu LDAP** **- LDAP v3** **- LDAP in der Netzwerkadministration** **- Das X.500-Datenmodell** **- Objekte** **- Attribute** **- Verzeichniseinträge** **- Vererbung** **- Klassenzugehörigkeit** **- Vererbung** **- Klassenzugehörigkeit und Polymorphie** **- Standardisierung von Attributen und Objektklassen** **- Typen von Objektklassen: structural, auxiliary und abstract** **- Der Verzeichnisbaum** **- Aliase** **- Distinguished Name und Relative Distinguished Name** **- "Relative" namen** **- Zusammengesetzter RDN** **- Vom RDN zum DN** **- Kodierung von RDN** **- Das funktionale Modell** **- Die LDAP-Session** **- Messages und Operationen** **- Controls und Extented Operations** **- Partitionierung** **- Naming Context** **- Referrals und Continuations** **- LDAP-Proxying: Serverseitige Auflösung von Referrals** **- LDAP-URL und Search Filters** **- Beispiele für LDAP-URLs** **- Sonderzeichen in URLs** **- Suche im Verzeichnis** **- Sicherheit** **- Autorisierung und Authentifizierung**

- Zugriffskontrolle im LDAP
- Athentifizierung
- SASL
- Der Strong Bind

- Transport Layer Security

- Schema
- Schema Discovery
- Allgemeiner Aufbau eines Schemas
- Eigene Schemas entwerfen
- Referenzierung von Objekten durch Name oder OID
- Der Object Identifier (OID)
- Der eigene OID
- Attribute Types definieren
- Object Classes definieren
- Spezielle Attribute für den Serverbetrieb

- Das LDIF-Format
- Was ist OpenLDAP?
- OpenLDAP installieren und konfigurieren
- OpenLDAP installieren
- Die Kompilation
- Die Overlays
- Die unterschiedlichen Backends
- Die Konfiguration

- Überlegungen zur Struktur des Verzeichnisbaumes
- Eine Basiskonfiguration
- Was bewirkt die Indexkonfiguration?
- Das Backend cn=config
- Einrichten der Database

- Die Serverfunktionen und -operationen
- Die Client-Tools
- Simple Paged Results Control
- Dynamic Directory Services extended Operation
- Proxy-Autorisierung-Control
- All Operational Attributes extended Operation

- Methoden der Authentifizierung und Autorisierung

- Cyrus-SASL
- Cyrus-SASL kompilieren
- Verwendung der SASL-Mechanismen

- Verwendung von EXTERNAL-Mechanismen

- Die Log-Backends
- Accesslog
- Auditlog

- Aspekt der Zugriffs- und Transportsicherheit
- Schutz vor unberechtigten Zugriffen
- Berechtigungskontrolle durch ACL
- Regeln für Was-Funktion
- Regeln für Wer-Funktion
- Regeln für den Security Strength Factor
- Die zu vergebenden Rechte
- Anwendungsbeispiele für diverse Regelsätze

- Regelsätze mittels Sets definieren
- Berechtigungskontrolle ducrh ACI
- Zugangskontrolle durch TCP-Wrapper
- Berechtigungskontrolle durch Overlays
- Transportsicherheit
- X.509-Zertifikate erstellen
- OpenLDAP mit TLS-Operationen kofigurieren

- Verteilte Systeme
- Verweise yuf andere Einträge
- Verweise auf andere Server
- Einbinden mehrerer Datenbasen
- Replikationen von gesamten Verzeichnissen und Teilbäumen
- Replikationen durch slurpd

- Replikationen durch Synchronisation
- Synchronisierte Replikation einrichten

- Proxy-, Meta- und Virtual Server
- LDAP Backend
- Meta Backend
- SQL Backend
- Directory mit subordinate SQL Backend

- Lösungsansätze mit Overlays
- Dynamische Einträge erstellen, darstekken und verwalten
- Konsolidierte Attributdarstellung
- Passwort-Regeln und Kontrolle

- Die Administration
- Die SLAPD-Tools
- Die regelmässige Datensicherung
- Die Indexdatenbanken pflegen

- Die Berkeley DB-Werkzeuege
- Alte Logdateien entfernen
- Database reparieren
- Ist die Cachegrösse ausreichend?
- Die Datei DB_CONFIG

- Tools zur Administration eines Directory
- web2ldap
- JXplorer

- Ausgewählte Anwendungen
- Die zentrale Mailadministration
- Sendmail
- Postfix-Mailrouting mit LDAP
- Mailrelaying mit SASL-Authentifizierung

- Cyrus-Imap
- OpenLDAP als Backend für BIND

- LDAP-APIs und SDKs
- APIs und SDKs im Überblick

- libldap
- libldap-Clients konfigurieren
- libldap-Code mit dem GCC kompilieren
- Eine LDAP-Sitzung mit der libldap
- Eine einfache libldap-Anwendung
- Speichervefreiung

- Asynchrone Operationen und Timeouts
- Listings

- Perl und Net:: LDAP
- Net:: LDAP
- Installation von Net:: LDAP
- Eine LDAP-Sitzung mit Net:: LDAP
- Asynchrone Operationen und cellbacks
- Timeout

- Java und das JNDI
- Das JNDI
- Namens- und Verzeinisdienste
- JNDI-Dokumentation

- Eine JNDI-Anwendung
- Contexts
- Der Initial Context
- Erzeugung
- des Context
- Bind
- LDAP-Suche
- Das Suchergebnis
- unbind

- Listing

- Die Directory Service Markup Language
- LDIF oder DSML?
- Darstellung von Verzeichnisdaten
- DSMLv1: Statistische Verzeichnisdaten in XML-Verpackung
- Verzeichnisdaten in DSMLv1
- Schemadaten in DSMLv1

- DSML mit net::LDAP erzeugen
- Ein Schema-Dokument in DSML
- Ein Suchergebnis nach DSML wandeln

- DSMLv2: Requests und Responses in XML-Verpackung

Beitrag	**Der Teilnehmerbeitrag versteht sich rein netto. Das ZFI ist (gemäss MwSt-Gesetz) nicht Mehrwertsteuerpflichtig und erhebt somit keine MwSt. Bei länger als einen Monat dauernden Lehrgängen ist die Zahlung des Teilnehmerbeitrages in mehreren Raten möglich (pro rata temporis).**