

Kurs: OpenLDAP (Verzeichnisdienst-Server)

© T. Birnthal, OSTC GmbH (www.ostc.de)

(Version 1.2 vom 29.8.2005)

Dauer: 2-3 Tage

Motivation: LDAP-basierte Verzeichnisdienste gewinnen nicht nur unter Linux/UNIX, sondern auch in heterogenen Netzen an Bedeutung. LDAP ermöglicht flexiblen, sicheren, effizienten, redundanten und skalierbaren Zugriff auf Benutzer- und Ressourcen-Informationen. OpenLDAP ist eine freie Implementierung eines LDAP-Servers mit Schnittstellen zu vielen Clients.

Ziel: Dieser Kurs gibt auf der Basis von OpenLDAP einen Überblick über LDAP, die dahinterstehenden Modelle und Abstraktionen und den Entwurf von LDAP-basierten Verzeichnisdiensten. Es werden die Installation und Konfiguration von OpenLDAP auf Linux, die Authentisierung von Linux- und Windows-Clients gegenüber LDAP, LDAP-Sicherheit und die Anbindung von Programmen wie z.B. Apache, Squid, Postfix, Sendmail, Cyrus-IMAP, Courier-IMAP, Samba und Mail-Clients betrachtet.

Inhalt:

- Übersicht Verzeichnisdienste / Directory Services
 - Was ist ein Directory Service?
 - Lokale/globale Verzeichnisse
 - Zentralisierte, replizierte und verteilte Verzeichnisse
 - Verzeichnis-Sicherheit
 - Sinnvoller Einsatz von Verzeichnissen
- LDAP Historie und Standards
 - OSI versus TCP/IP
 - Der LDAP-Vorgänger X.500
 - LDAP versus DAP

- RFCs
- Unterschiede zwischen LDAPv2 und LDAPv3
- OpenLDAP im Vergleich zu anderen LDAP-Implementationen
- LDAP Konzepte und Architektur
 - Aufbau der Directory-Struktur
 - Aufbau einer LDAP-Nachricht
 - (Relative) Distinguished Name Syntax
 - Objekte und deren Attribute
 - DIT (“Directory Information Tree”)
 - Objektklassen und Vererbung
 - OIDs (Object Identifier)
 - Schema
 - Suffixe und Referrals
 - Aliase
- LDIF-Format
- OpenLDAP-Sicherheit
 - Authentifizierung, Autorisierung und Verschlüsselung
 - Der “Strong Bind”
 - SASL und TLS
- OpenLDAP-Installation und -Konfiguration
 - Server-Installation- und -Konfiguration
 - Auswahl von Standard-Schemata
 - Schema-Anpassung und -Erweiterung
 - Grafische und nichtgrafische Tools
 - Zugriffskontrolle und Logging
 - Verteilung/Weiterleitung
 - Replikation
 - Failover
- Anwendungsbeispiele
 - Benutzer-Authentifizierung (OpenLDAP als NIS-Alternative)

- Übersicht LDAP-API
 - Zugriff über Shell (Kommandozeile)
 - Zugriff über Perl
 - Zugriff über PHP
- Zukunft von LDAP/OpenLDAP

Schulungsunterlagen:

- Skript
- Lösungsblätter zu allen Übungen
- Zusammenfassung der wichtigsten Linux/UNIX-Befehle
- Zusammenfassung der wichtigsten Vi-Befehle

Voraussetzungen:

- Muss: Allgemeine Computer-Kenntnisse (Tastatur, Maus, Grafische Oberfläche, Editor)
- Muss: Linux-Grundlagen
- Muss: Linux-Administrationskenntnisse
- Muss: Netzwerkkennnisse
- Muss: Arbeiten auf der Kommandozeile (analog MS-DOS)

Abgrenzung:

- Verbindung von OpenLDAP und Active Directory wird nicht behandelt