

Network Services, VU 2.0

LDAP

Dipl.-Ing. Johann Oberleiter
Institute for Information Systems, Distributed
Systems Group

Directory

- Goal: help people find things
- Online: help also computer find things
 - Dynamic (Update)
 - Flexible Content & Organization
 - Can be made Secure
 - Can be personalized
 - Information inside the directory
 - Info delivered to users

Lightweight Directory Access Protocol

- Standardized Directory Access Protocol
- Supports
 - Centrally manage users, groups, devices, and other data
 - Single Sign-On
 - Reduces need to implement proprietary user and group management database
 - Reduces need for separate application-specific directories
 - Avoids tying exclusively to a single vendor and/or OS

LDAP Protocol

- Not simple string-based
 - Simplified version of Basic Encoding Rules (BER)
- Operations in 3 categories
 - Interrogation operations
 - Update operations
 - Authentication and control operations
- Lightweight
 - More efficient than "heavyweight" X.500 Directory Access Protocol (DAP)

LDAP Information Model

- Types of data and basic units that can be stored
- Basic unit is the entry
 - Collection of information about an object
 - Consists of a set of attributes
- Each attribute
 - Type
 - One or more values
 - May have constraints on type and length
- Information Model describes entries

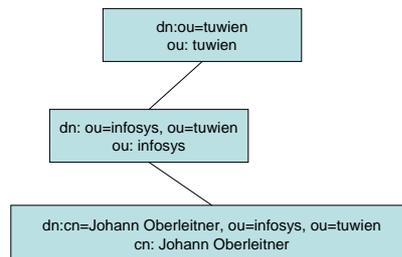
Information Model - Sample

cn: (common name)	Johann Oberleitner
sn: (sur name)	Oberleitner
telephonenumber:	+43 1 58801 58400
mail:	johann.oberleitner@infosys.tuwien.ac.at

LDAP Naming Model

- How data in directory is structured
 - How entries can be accessed
- Similar to file system
 - Every node contains data in LDAP directory
 - Any node can be a container
 - Backward relative to filenames
 - DN (distinguished name) refers to an entry
 - Within DN, leftmost component is RDN (relative DN)
- Aliases
 - One entry points to a completely different entry
 - Allows structures not strictly hierarchical

LDAP Naming Model



LDAP Functional Model

- Operations possible on the directory with LDAP
- Interrogation operations
 - Search
 - Parameters may restrict search scope, time limit, size limit, search filter
 - Search filter: (sn=K*), (sn>=O), logical operators
 - Compare
 - Whether a particular entry contains a particular attribute

LDAP Functional Model / 2

- Update operations
 - Add
 - Parent must exist, new entry must conform to schema in effect, no entry exists with same DN
 - Delete
 - Entry must exist
 - No children
 - Modify
 - Entry must exist
 - All attribute modifications must succeed
 - Result must obey schema in effect
 - Modify (DN) = rename
 - Entry renamed must exist
 - New name must not already exist

LDAP Functional Model / 3

- Authentication and Control operations
 - Bind
 - Client authenticates to directory
 - Unbind
 - Discards authentication information
 - Abandon
 - Takes message ID of LDAP operation
 - Client sends abandon if no longer interested in results

Active Directory

- Microsoft's Directory Service
- API
 - ADSI (Active Directory Services API)
 - Supports LDAP and other servers
 - One of Microsoft's most important tools in Server business
- Compatible with LDAPv3
 - Unfortunately interpretations are possible