LDAP Demystified

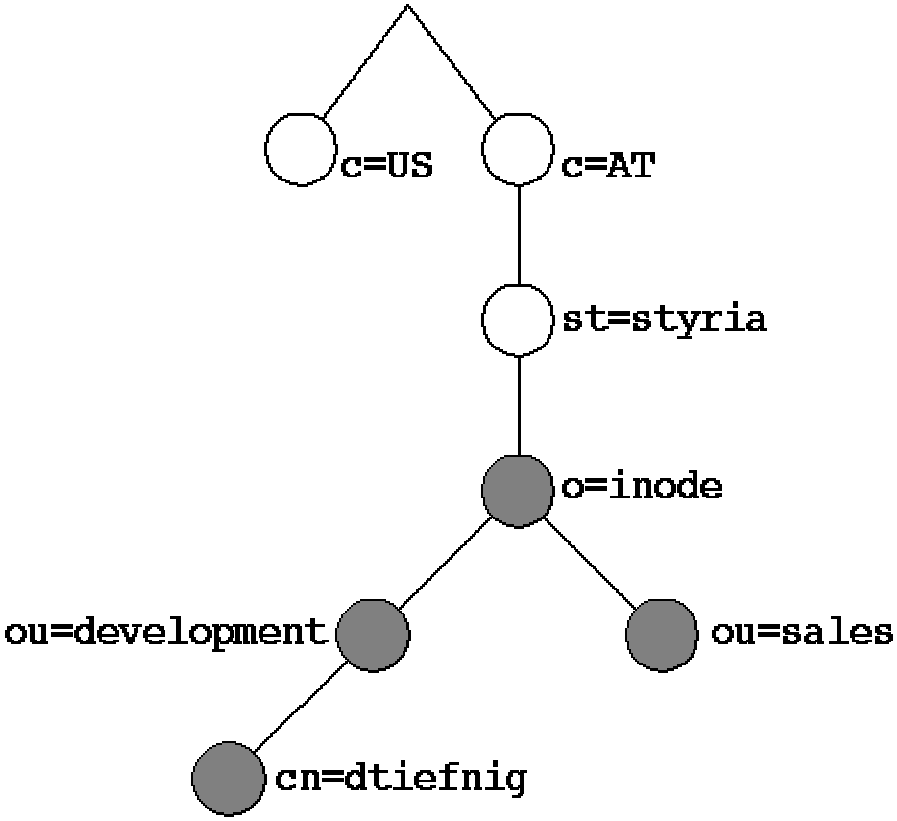
Daniel Tiefnig

25. April 2003

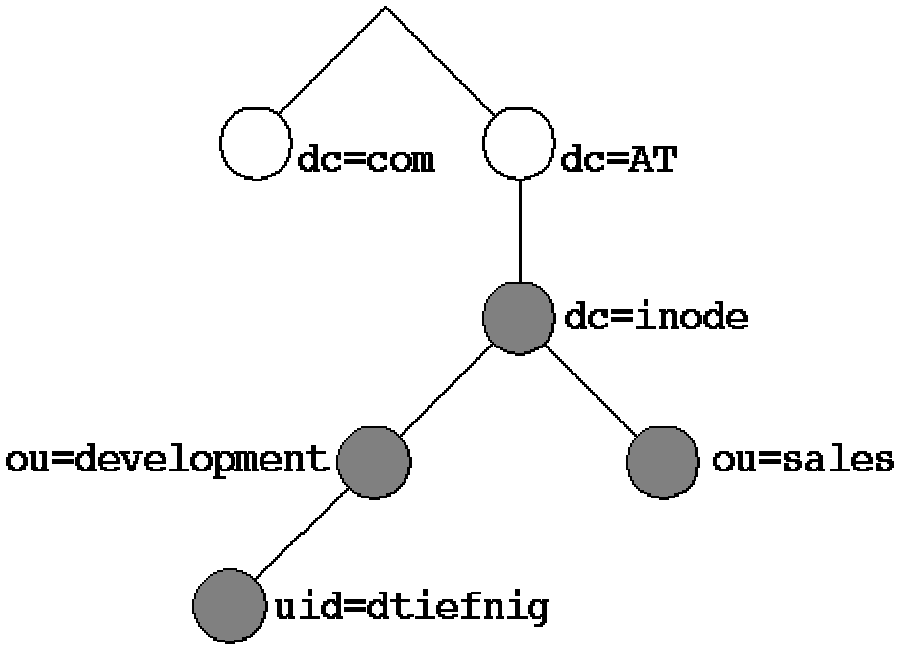
– Typeset by FoilTEX –

Was ist LDAP

- Was ist ein Verzeichnisdienst
  - X.500, DAP
  - LDAPv2
  - LDAPv3
- Was kann in einem Verzeichnis gespeichert werden
- Wie wird die Information gespeichert



Traditioneller Verzeichnisbaum



"Internet" Verzeichnisbaum

Distinguished Names

cn=dtiefnig,ou=development,o=inode,st=styria,c=AT

uid=dtiefnig,ou=development,dc=inode,dc=at

LDIF - content

dn-spec = "dn:" FILL distinguishedName

attrval-spec = AttributeDescription value-spec

AttributeDescription = AttributeType [";" options]

value-spec = ":" (FILL (SAFE-STRING) /
":" FILL (BASE64-STRING) /
"<" FILL url)

dn: uid=dtiefnig,ou=development,dc=inode,dc=at
objectclass: person
objectclass: uidobject
uid: dtiefnig
cn: Daniel Tiefnig
sn: Tiefnig
userpassword: {crypt}c4jHzc08CN.ug

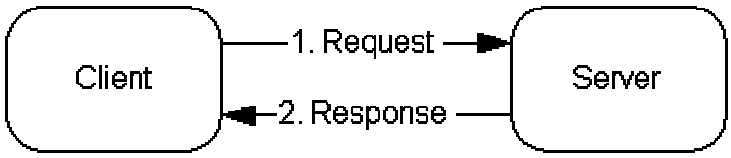
LDIF - changes

changerecord = "changetype:" FILL
(change-add / change-delete /
change-modify / change-moddn)

dn: uid=dtiefnig,ou=development,dc=inode,dc=at
changetype: modify
replace: userpassword
userpassword: {crypt}c4DqXPxcxUDNI
-
add: telephoneNumber
telephonenumber: 555-0161
telehonenumber: 555-1013

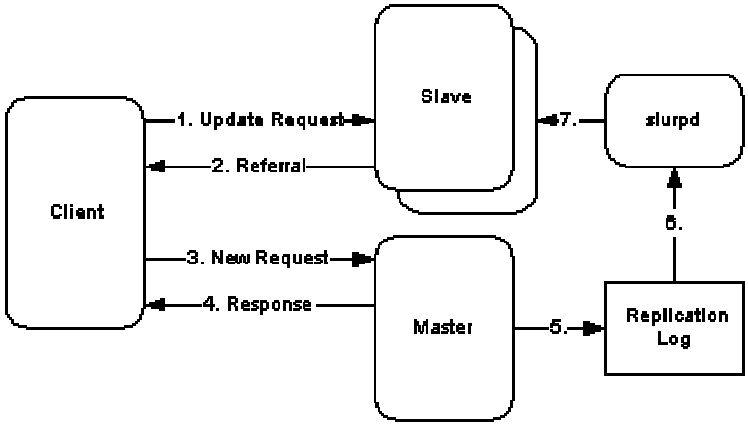
Konfigurationen

Einfaches Verzeichnis



Konfigurationen

Repliziertes Verzeichnis



Konfigurationen

Verteiltes Verzeichnis

OpenLDAP

- LDAPv3
- Simple Authentication and Security Layer (SASL)
- Transport Layer Security (TLS)
- TCP wrappers
- Access control
- Internationalisierung (Unicode)
- Modulare Schnittstelle
- Threads
- Replikation
- Einfache Konfiguration

slapd Konfiguration

Externe Konfigurationen
include <filename>

Access Control
access to <what>[by <who><accesslevel><control>]+

Datenbanken
database <type>
suffix <dn suffix>
rootdn <dn>
rootpw <password>
directory <directory>
index {<attrlist>— default} [pres,eq,approx,sub,none]

Schema Spezifikation

OpenLDAP 1.x:

objectclass person
    requires
        objectClass,
        cn
    allows
        sn,
        userPassword,
        telephoneNumber,
        seeAlso,
        description

OpenLDAP 2.x:

objectclass (2.5.6.6 NAME 'person'
    DESC 'RFC2256: a person'
    SUP top STRUCTURAL
    MUST (sn $ cn)
    MAY (userPassword $ telephoneNumber $
        seeAlso $ description))

attributetype (2.5.4.13 NAME 'description'
    DESC 'RFC2256: descriptive information'
    EQUALITY caseIgnoreMatch
    SUBSTR caseIgnoreSubstringsMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{1024})