LUGS-Treff @ 24.08.2006

Mario Iseli
<admin@marioiseli.com>

What is a directory?

(Where did i put that damn username?)

- Your business partners, friends, coworkers.
- Do you know all their E-Mail addresses?
- How many lines does your /etc/hosts contain?
- How do you share this information?
- Imagine a world without DNS!

What is a directory?

(Where did i put that damn username?)

- DNS stores all Hosts in a distributed, hierarchical databse
- LDAP can store all your contacts
- LDAP can be distributed
- LDAP is extendable
- LDAP has a nice structure
- LDAP can be easily integrated into applications

Mario Iseli
<admin@marioiseli.com>

What is a directory?

(Where did i put that damn username?)

- Sense of distribution (geographic, organisational, security reasons)
- Sense of centrality (laziness of administrators, one change fixes all)
- Reasons why OpenLDAP is a good solution (open standard, supported by most software, PAM+NSS, easy to administrate)

Mario Iseli
<admin@marioiseli.com>

LDAP – The protocol

- RFC 2251-2256 Core set of RFCs
- RFC 2829 Authentication
- RFC 2830 TLS extensions
- RFC 3377 Technical specification

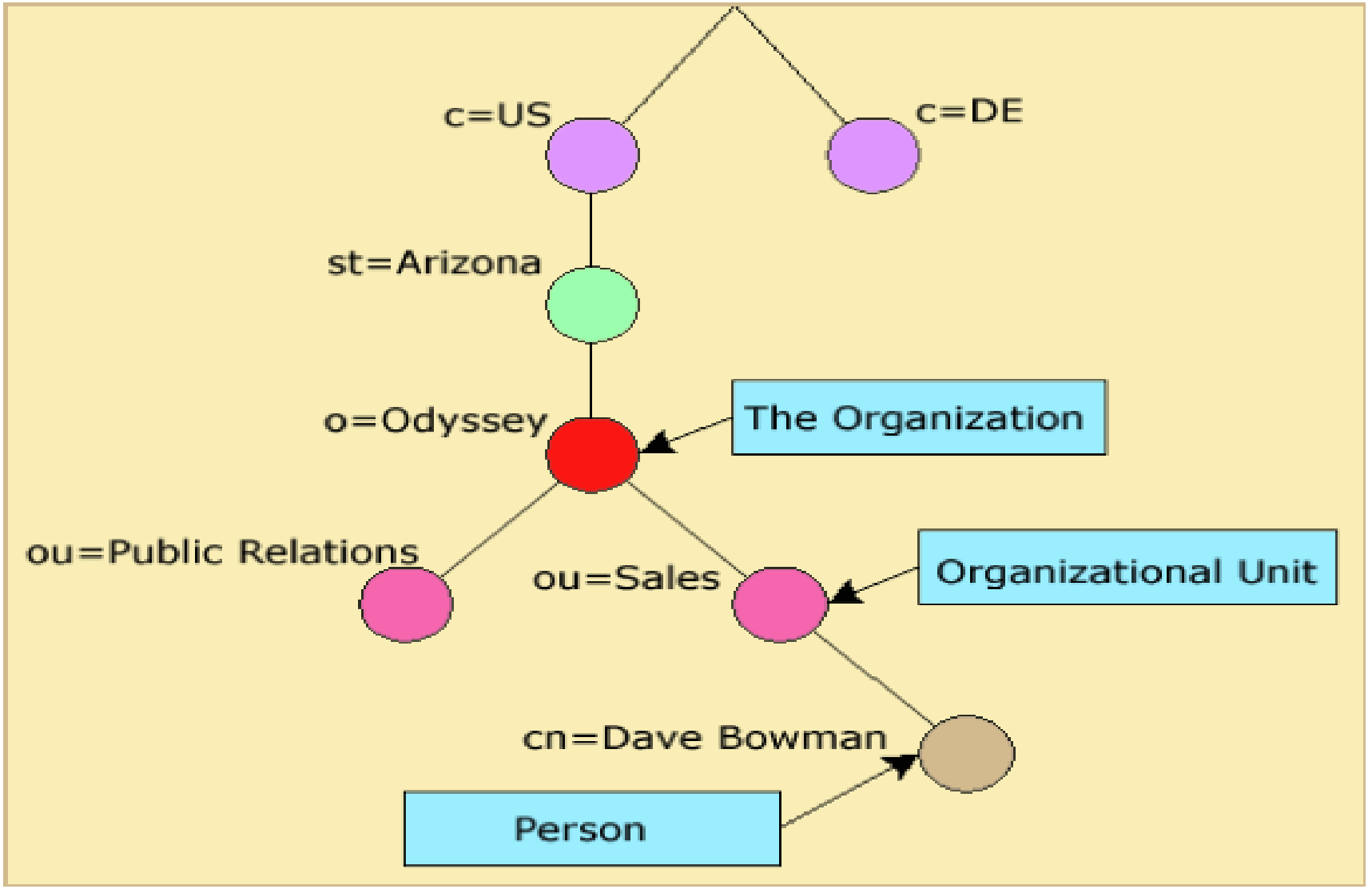
Mario Iseli
<admin@marioiseli.com>

LDAP – the protocol

- LDAP – LIGHTWEIGHT????
- X.500 – Heavyweight!
- 9 core operations
- Easier API

Mario Iseli
<admin@marioiseli.com>

LDAP – the protocol



Mario Iseli
<admin@marioiseli.com>

LDIF – LDAP interchange format

```
#LDIF example for ou=people,dc=marioiseli,dc=com
dn: ou=people,dc=marioiseli,dc=com
objectClass: organizationalUnit
ou: people
telephoneNumber: +41 79 573 12 31
description: In this OU are my address book entries, note that I don't need a “\”
      as in most UNIX config files when I use more than one line.
```

Some words about objectClasses

- every entry must have at least one!
- can have more than one
- the OID (registered by IANA)
- can be defined as you want (schema)
- Structural / Auxiliary / Abstract

```
objectclass ( 1.3.6.1.1.1.1.13 NAME 'automount' SUP top STRUCTURAL
        DESC 'An entry in an automounter map'
        MUST ( cn $ automountInformation $ objectclass )
        MAY ( description ) )
```

referral – the objectClass

```
# ou=accounts,dc=marioiseli,dc=com is on ldap2
dn: ou=people,dc=marioiseli,dc=com
objectClass: referral
ref: ldap://ldap2.local/ou=people,dc=marioiseli,dc=com
```

Authentication on LDAP

- Anonymous (empty user and passwd)
- Simple authentication
- SSL/TLS
- SASL
- userPassword -> {CRYPT}, {MD5}, {SHA}, {SSHA}

Mario Iseli
<admin@marioiseli.com>

Authentication on LDAP

- Supported SASL-AUTH-Mechanisms:
  - ANONYMOUS
  - CRAM-MD5
  - DIGEST-MD5
  - GSSAPI
  - KERBEROS_V4
  - LOGIN
  - PLAIN
  - SCRAM-MD5

SSL/TLS with OpenLDAP

- TLSCipherSuite (see ciphers(1))
- TLSCertificateFile
- TLSCertificateKeyFile

Mario Iseli
<admin@marioiseli.com>

Database-Backends

- “database” parameter in slapd.conf
  - bdb (Berkeley DB 4)
  - ldbm (GNU Database Manager / Sleepycat)
  - passwd (as argument a filename)
  - shell (for doing some experiments?)

ACL

access to *
by * read

access to attrs=userPassword
by self write
by * auth

access to dn=”uid=bla,ou=bla,dc=bla”
by dn=”cn=admin,dc=bla”

Mario Iseli
<admin@marioiseli.com>

ACL

- Levels:
  - write
  - read
  - search
  - compare
  - auth
  - non

Mario Iseli
<admin@marioiseli.com>

ACL

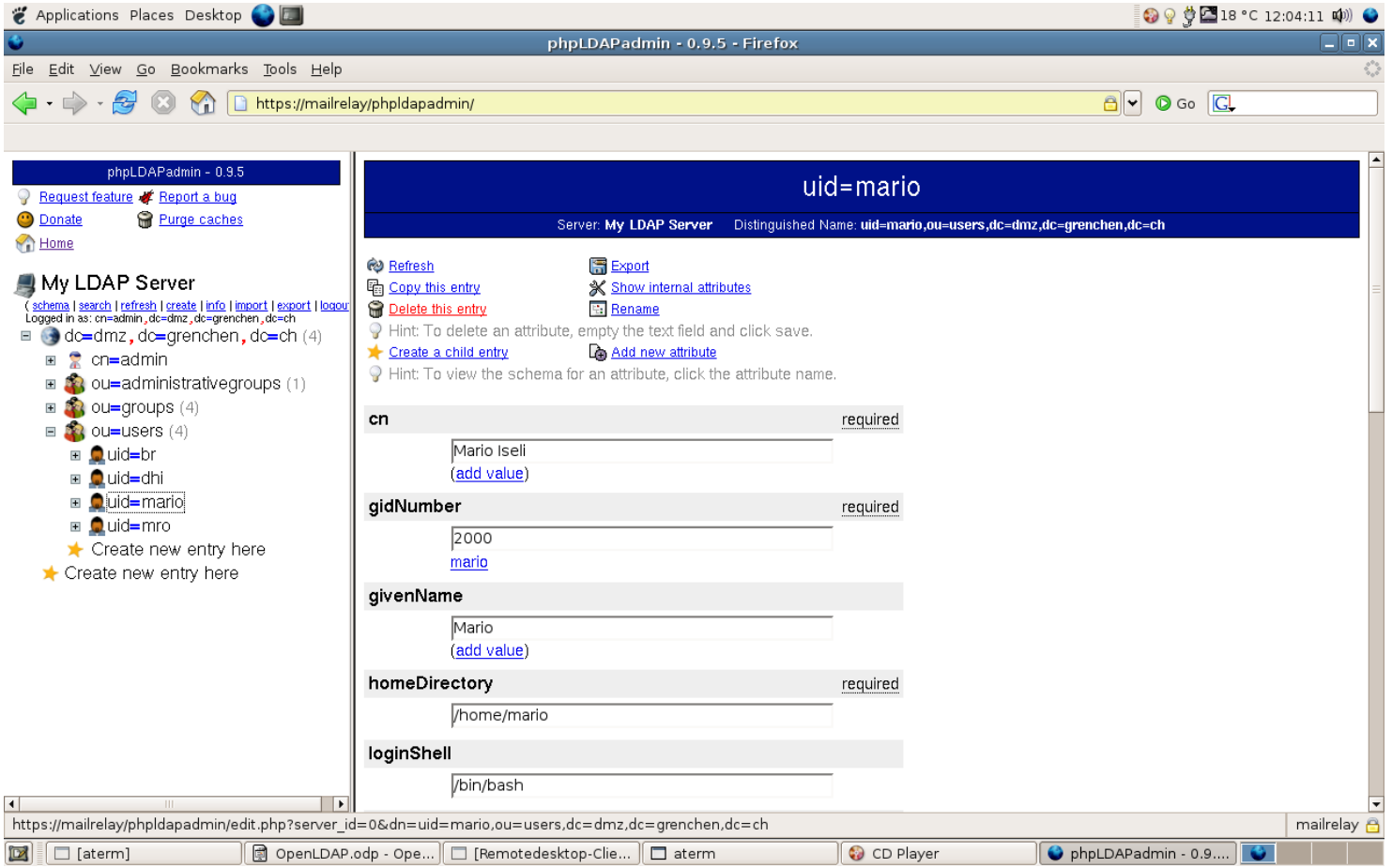
- Accessowners:
  - * (= Everybody)
  - self
  - anonymous
  - users
  - Regexps for DN's are possible

Administrate LDAP “the hard way”

- for i in `ls /usr/bin | grep ^ldap`; do man $i; done

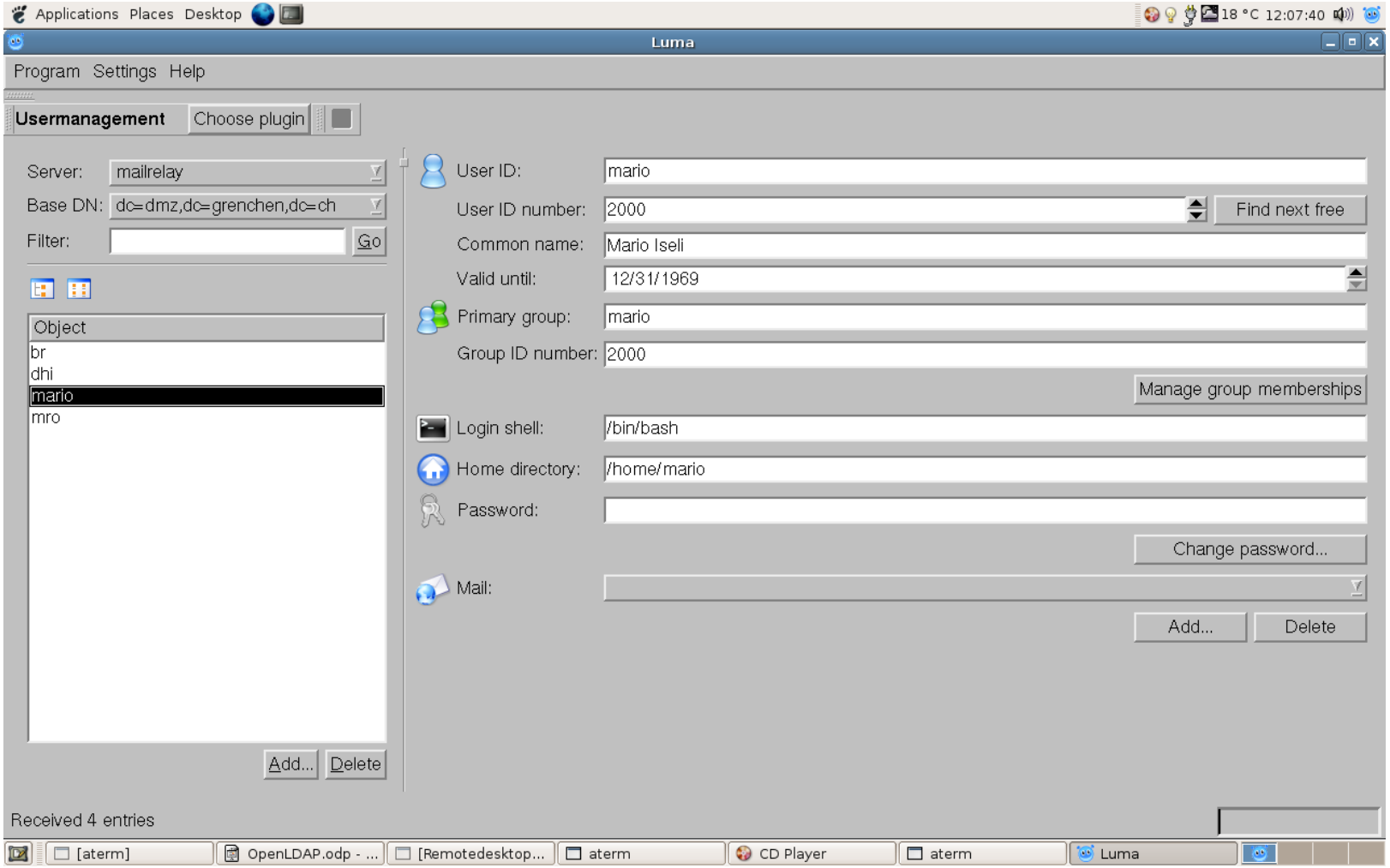
Mario Iseli
<admin@marioiseli.com>

... the easier way (phpldapadmin)



Mario Iseli
<admin@marioiseli.com>

luma



Mario Iseli
<admin@marioiseli.com>

slurpd (master)

```
replica         host=slave.local
                suffix=”dc=lugs,dc=ch”
                binddn=”cn=replica,dc=lugs,dc=ch”
                credentials=”Bla?”
                bindmethod=simple
                tls=yes
```


Mario Iseli
<admin@marioiseli.com>

slurpd (slave)

updatedn=”dc=lugs,dc=ch”
updateref=ldap://master.local

Mario Iseli
<admin@marioiseli.com>

ldap.conf

- host (if not specified nss_ldap will try to lookup over DNS with SRV records for ldap.tcp.<domain>.
- base (basedn where the search should begin)
- ldap_version
- binddn
- bindpw
- rootbinddn
- ssl
- scope (sub / one / base)
- uri

pam_ldap.conf

- pam_min_uid
- pam_max_uid
- pam_password (needs an encryption algorithm)

Mario Iseli
<admin@marioiseli.com>

nss_ldap.conf

- nss_base_group
- nss_base_hosts
- nss_base_rpc
- nss_base_netgroups

Mario Iseli
<admin@marioiseli.com>

Use nss and pam

- Add “ldap” to /etc/nsswitch.conf where needed
- For pam use “pam_ldap.so” in /etc/pam.d/*

netgroups

- objectClass: nisNetGroup
- cn: sysadmins
- nisNetgroupTriple: (selene.lugs.ch,-,-)
- memberNisNetGroup: techies
- userAccounts may also have a “host”

autofs

- ObjectClass: nisMap
- nisMapName: auto.home
- /home ldap:ldap.lugs.ch:nisMapName=auto.home,dc=lugs,dc=ch

Mario Iseli
<admin@marioiseli.com>

Apache mod_ldap

```
AuthType Basic
AuthName "For internal users only"
AuthLDAPUrl ldap://localhost:389/ou=users,dc=lugs,dc=ch?uid
require valid-user
```


Mario Iseli
<admin@marioiseli.com>

Samba

security = user
ldap admin dn = “cn=1337r00t,dc=lugs,dc=ch”
ldap server = localhost
ldap ssl = start_tls
ldap suffic = ou=samba,dc=lugs,dc=ch

-> smbpasswd -w CrYpTeDPaSsWoRd
-> objectClass: sambaAccount

Mario Iseli
<admin@marioiseli.com>

Addressbooks

- objectClass: inetOrgPerson
- Compatible with most MUA's (including M$ Outlook)

Storing DNS-Information in LDAP

```
zone "mydomain.de" {
        type master;
        database "ldap
ldap://127.0.0.1/ou=mydomain,ou=DNS,dc=lugs,dc=ch 172800";
};
```

You can find good schema files on the Internet which allow you to do almost everything with DNS!

Mario Iseli
<admin@marioiseli.com>

LDAP with OpenVPN

- Server: http://www.marioiseli.com/stuff/ldap.sh
- Client: add “auth-user-pass” to conf-file

Mario Iseli
<admin@marioiseli.com>

Resources

- http://www.rrze.uni-erlangen.de/dienste/arbeiten-rechnen/linux/how
- http://www.openldap.org/doc/admin23/
- “LDAP – System Administration” (ISBN: 1-56592-491-6)
- This presentation: http://www.marioiseli.com/stuff/OpenLDAP.pdf

Thanks to...

- The Debian Project (Software)
- Mathias Weyland (Inspiration and Book)
- Thierry Dussuet (Motivation)
- AIS Grenchen (Infrastructure)