



# Directory Serving Solutions using OpenLDAP

Michael Maclsaac  
Mon. Feb. 28, 2005  
Session 9207  
SHARE, Anaheim, CA



# Outline

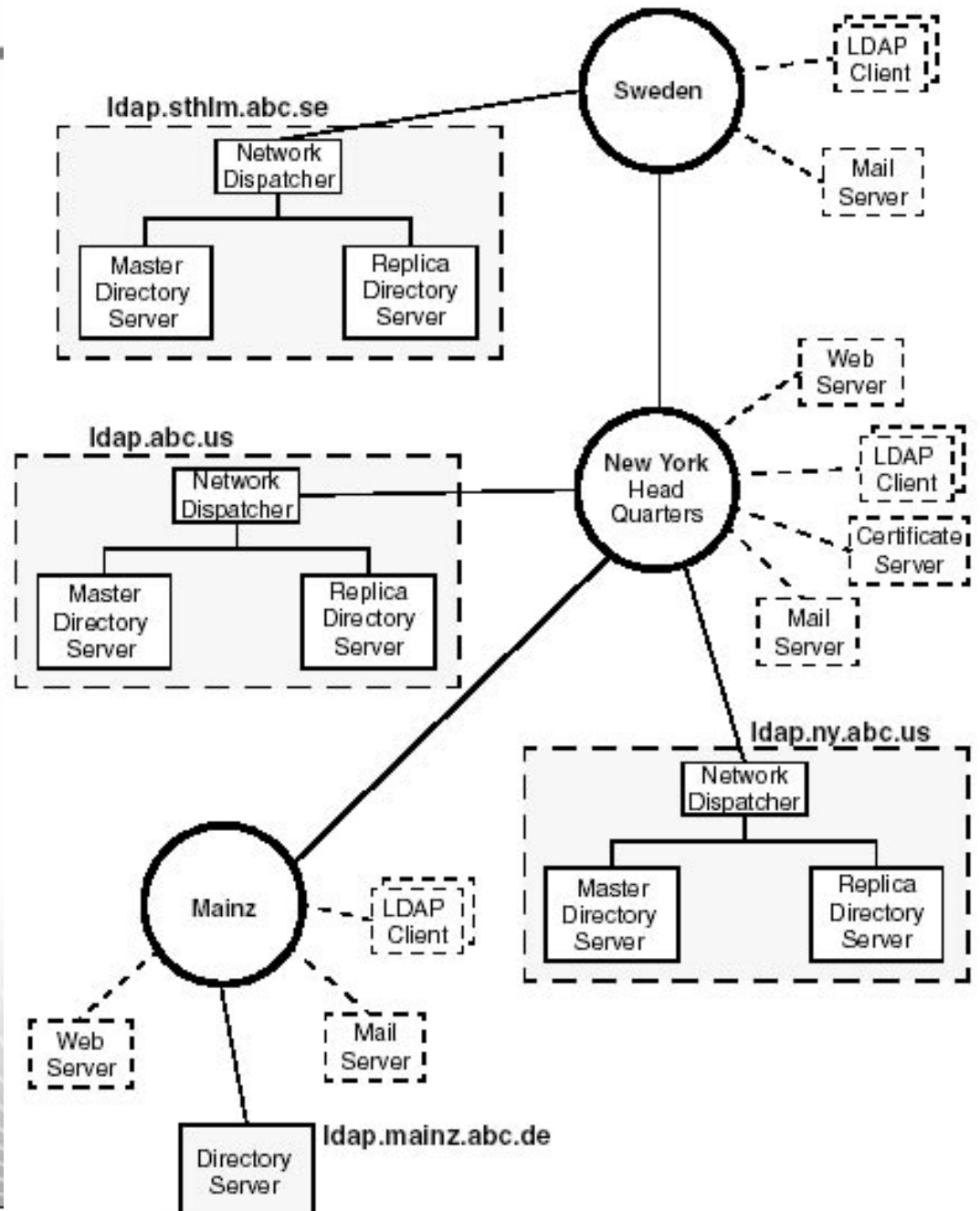


- ▶ Introductions
- ▶ Overview of LDAP
- ▶ SuSE SLES-9 install an LDAP client/server
- ▶ Maintaining LDAP server/data
- ▶ LDAP GUIs/browsers
- ▶ LDAP client-only install
- ▶ LDAP master/slave configuration (replication)
- ▶ Documentation and resources

# Overview - complex LDAP solution



LDAP can become a complex solution - Example of a more sophisticated LDAP architecture:



# Overview

- What is LDAP?
  - ▶ Lightweight Directory Access Protocol
  - ▶ A network *protocol* for accessing information in a directory
  - ▶ Hierarchical data reflecting political, geographic or organizational boundaries
  - ▶ Based on the "heavyweight" X.500 standard - used OSI and is probably over-engineered
  - ▶ A system designed for reading more than writing
- How can LDAP be used?
  - ▶ Personnel information lookup
  - ▶ Centralized login - User authentication, Password maintenance
  - ▶ Centralized home directories - automount and NFS
  - ▶ e-mail system
  - ▶ File, Print, Centralized Windows login - Samba

# Overview - What are some LDAP clients?



- Linux Idap\* commands:
  - Idapadd, Idapdelete, Idapsearch, Idapcompare, Idapmodify, Idappasswd, etc.
- Linux library via nsswitch, PAM
  - /lib/libnss\_ldap.so.2
  - /lib/security/pam\_ldap.so
- GUIs/LDAP browsers
  - gq - included with SLES distro  
<http://biot.com/gq/>
  - LDAP Account Manager (LAM)  
<http://sourceforge.net/projects/lam/>
  - Directory Administrator  
<http://diradmin.open-it.org/index.php>
- e-mail clients:
  - Outlook, OS X Mail, Eudora, Netscape/Mozilla, QuickMail Pro, Mulberry, etc.
- Samba
- Custom Perl, C or dynamicWeb apps with LDAP back-ends

# Overview - LDAP terms

- Commonly used LDAP terms
  - ▶ Suffix, base or root - the base of the local tree
    - Country/Organization-based - e.g. "c=us, o=acme"
    - DNS-based - e.g.. dc=ibm, dc=com
  - ▶ DN - distinguished name - refers to an entry unambiguously
    - uid=ldapuser,ou=People,dc=poklcc,dc=ibm,dc=com
  - ▶ RDN - relative distinguished name
  - ▶ OU - organizational unit
  - ▶ CN - common name
  - ▶ DIT - Directory Information Tree - the hierarchical data
  - ▶ LDIF - LDAP Interchange Format - flat text
  - ▶ Schema - definition of objects, metadata
    - Object Class
    - Super Class and inheritance - "top" is the super-est class
    - Auxiliary Class - cannot stand on its own like a "structural" class
    - Attribute Type
    - Attribute Definitions

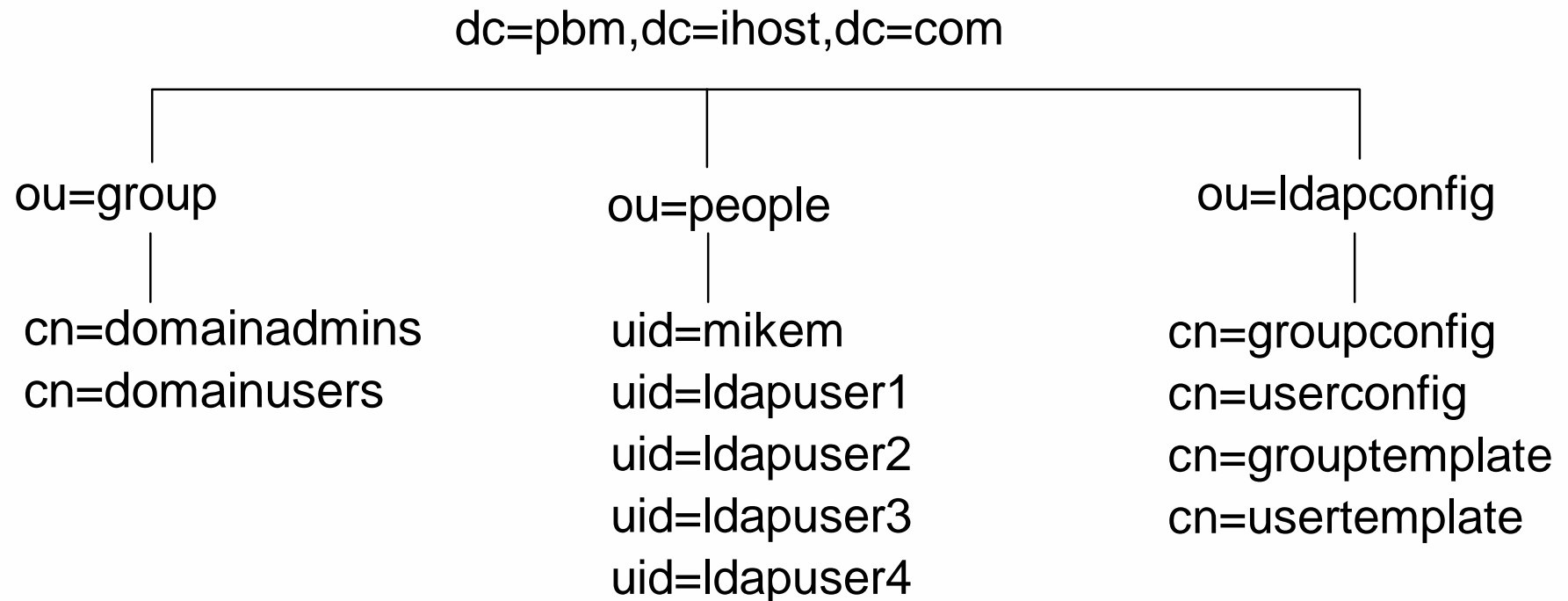
# Overview - LDAP implementations



- IBM Tivoli Directory Server (ITDS)
  - free trial:
    - <http://www-106.ibm.com/developerworks/offers/linux-speed-start/download-z.html>
  - click on **Downloads**
- Microsoft Active Directory (AD) - considered proprietary:
  - Active Directory requires API developers to perform external application integration that a pure LDAP server would handle.
  - Active Directory has limited schema support within directory structures.
- Novell eDirectory (shipped with OES?)
  - Formerly Novell Directory Services (NDS)
  - Available on Linux (but still not on s390?)
  - Excellent user interface that abstracts LDAP into users and groups
- OpenLDAP
  - Based on original University of Michigan LDAP implementation
  - Included standard with SuSE SLES and Red Hat RHEL
- Sun ONE (Open Networking Environment)
  - Formerly Netscape iPlanet

# Overview - DIT example

## Example of a Directory Information Tree (DIT)





# Overview: Security

- Security levels in LDAP
  - ▶ Anonymous
  - ▶ Simple authentication - clear text
  - ▶ Simple authentication over SSL/TLS - encrypted over the wire
    - Set up by default with SLES-9 install
  - ▶ Simple Authentication and Security Layer (SASL) - supports
    - Kerberos system
    - MD-5 hashing algorithm
    - SHA-1 hashing algorithm

# Overview: Replication and referrals



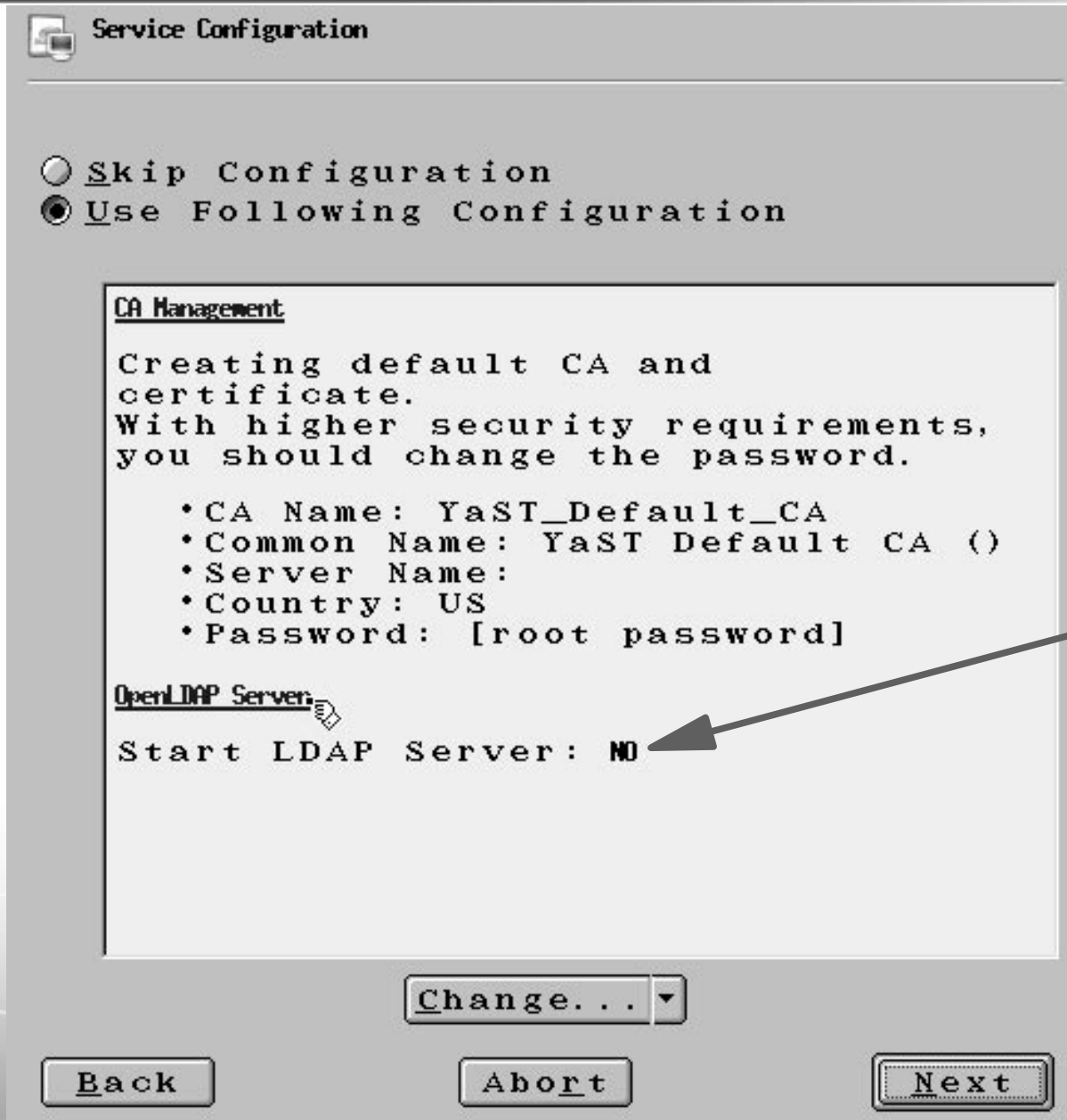
- Replication
  - ▶ Duplicating the data in a server
  - ▶ Not a standard
    - LDAP Duplication Update Protocol (LDUP) is an IETF working group, but is it dead?
    - LDAP Content Synchronization (or LDAP Sync)
    - OpenLDAP uses slurpd
    - ITDS uses its own mechanism
- Referrals in a distributed database
  - ▶ Distributes the data in a server - no data duplication
  - ▶ Uses the referral object class and the "ref" attribute

# Set up LDAP on SLES-9

- OpenLDAP can be set up during SLES-9 installation
  - ▶ Advantages
    - LDAP "jump start" - server running out of the box
    - Easier configuration - you don't have to be a Linux/LDAP hacker
    - No initial LDIF file to configure
    - Works with YaST using a user/group paradigm
  - ▶ Disadvantages
    - Bugs/features
    - Often impossible to go back:



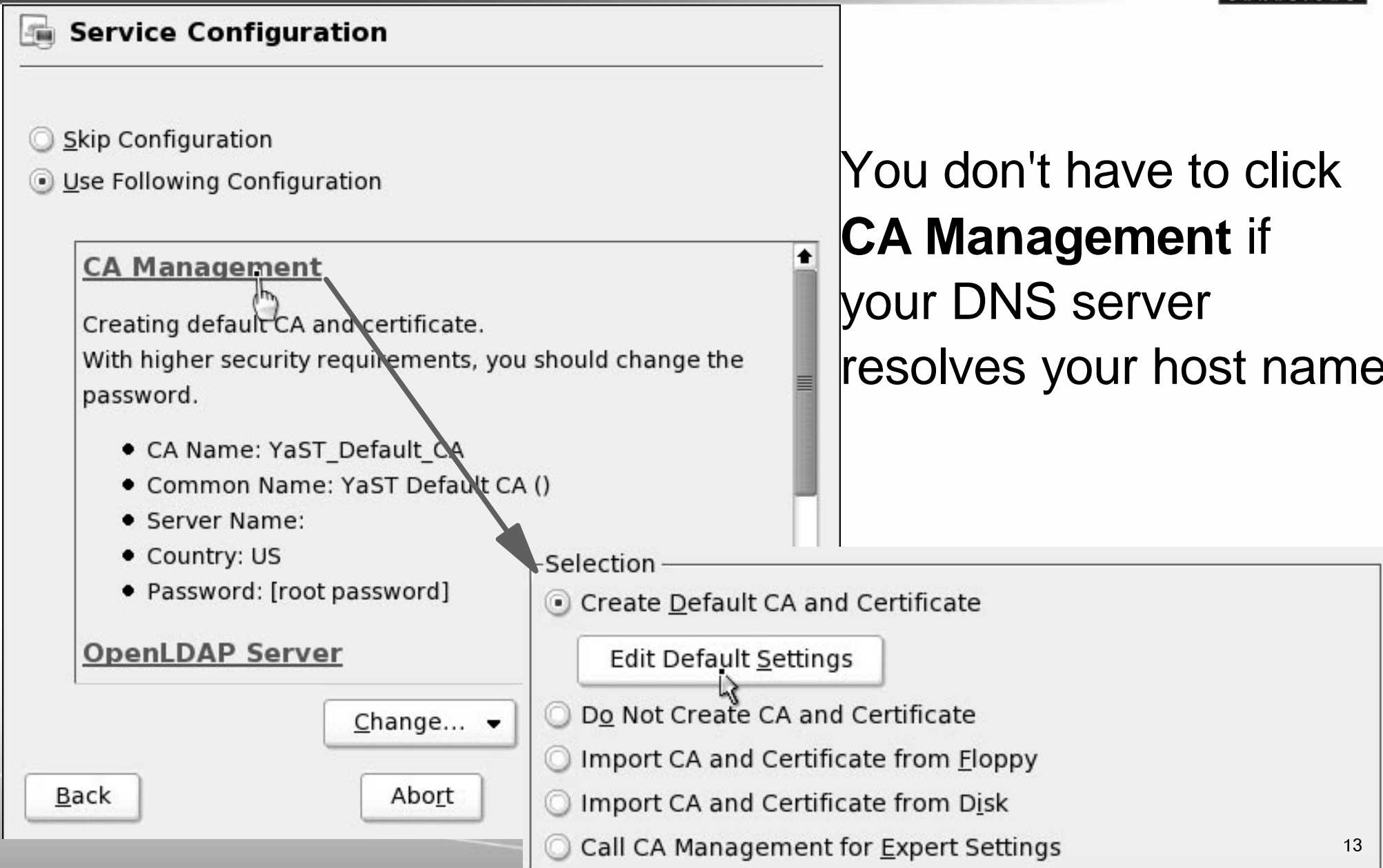
# Set up LDAP on SLES-9



SLES-9 install now allows LDAP to be set up: see [cd1/docu/en/manual.pdf](http://cd1/docu/en/manual.pdf) section 8.1

Default is NO with minimal install

# Set up LDAP on SLES-9 (cont'd)



**Service Configuration**

Skip Configuration  
 Use Following Configuration

**CA Management**

Creating default CA and certificate.  
With higher security requirements, you should change the password.

- CA Name: YaST\_Default\_CA
- Common Name: YaST Default CA ()
- Server Name:
- Country: US
- Password: [root password]

**OpenLDAP Server**

Change... ▼

Back Abort

**Selection**

Create Default CA and Certificate

Edit Default Settings

Do Not Create CA and Certificate

Import CA and Certificate from Floppy

Import CA and Certificate from Disk

Call CA Management for Expert Settings

You don't have to click **CA Management** if your DNS server resolves your host name!

# Set up LDAP on SLES-9 (cont'd)



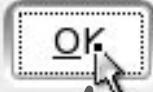
**Edit Default Settings**

<b>CA Name:</b> <input type="text" value="MyCertificateAuthority"/>	<b>Common Name:</b> <input type="text" value="pbc4533.pbm.ihost.com"/>
<b>Server Name:</b> <input type="text" value="pbc4533"/>	<b>Country:</b> <input type="text" value="USA"/>
<b>Organization:</b> <input type="text" value="IBM"/>	<b>Organizational Unit:</b> <input type="text" value="zNTC"/>
<b>Locality:</b> <input type="text" value="Poughkeepsie"/>	<b>State:</b> <input type="text" value="NY"/>
<b>Password:</b> <input type="password" value="*****"/>	<b>Confirm Password:</b> <input type="password" value="*****"/>

Common name must be == DNS name

# Set up LDAP on SLES-9 (cont'd)

Changing anything in this dialog disables the automatic generation of base DN, root DN, and LDAP password.



Ignore this warning

Uncheck "Append Base DN" and type out both Base DN and Root DN (bug as LTC bugzilla 10847)

## Configuration

### OpenLDAP Server Settings

Enable Server  Disable Server

Base DN

dc=pbm,dc=ihost,dc=com

Root DN

cn=Administrator,dc=pbm,dc=ihost,dc=com

Append Base DN

LDAP Password

\*\*\*\*\*

Validate Password

\*\*\*\*\*

Encryption

SSHA

Activate StartTLS with Common Server Certificate

Register at an SLP Daemon

Back

Abort

Next

# Set up LDAP on SLES-9 (cont'd)



**LDAP Client Configuration**

User Authentication

Do Not Use LDAP

Use LDAP

LDAP client

LDAP base DN

dc=pbm,dc=ihost,dc=com

Addresses of LDAP Servers

localhost

LDAP TLS/SSL

LDAP Version 2

Start Automounter

Advanced Configuration...

Back      Abort      Next

Take defaults



# Set up LDAP on SLES-9 (cont'd)

 **User Authentication Method**

---

Authentication Method

NIS

LDAP

Local (/etc/passwd)

Take  
defaults

# Set up LDAP on SLES-9 (cont'd)

 **Add a New LDAP User**

User Data

First Name	Last Name
<input type="text" value="Mike"/>	<input type="text" value="MacIsaac"/>
User Login	<input type="button" value="Suggestion"/>
<input type="text" value="mikem"/>	
Password	
<input type="password" value="*****"/>	
Verify Password:	
<input type="password" value="*****"/>	
<input type="checkbox"/> Receive System Mail	<input type="button" value="Password Settings..."/>
<input type="checkbox"/> Auto Login	<input type="button" value="Details..."/>

Take defaults,  
Avoid other panels

For Samba,  
skip this and  
add users  
later

# Set up LDAP on SLES-9 (cont'd)

## ▶ Login to your new LDAP server

- Check that LDAP is running:

```
# rcldap status
```

```
Checking for service ldap:
```

running

- Check the contents of the LDAP server

```
# ldapsearch -x | grep uid=mikem
```

```
dn: uid=mikem,ou=people,dc=pbm,dc=ihost,dc=com
```

- Check the Name Service Switch

```
# grep ldap /etc/nsswitch.conf
```

```
passwd_compat: ldap
```

```
group_compat: ldap
```

```
# id mikem
```

```
uid=1000(mikem) gid=100(users) groups=100(users)
```

- Check PAM

```
# grep ldap /etc/pam.d/* /etc/security/*
```

```
/etc/security/pam_unix2.conf:auth: use_ldap
```

```
/etc/security/pam_unix2.conf:account: use_ldap
```

```
/etc/security/pam_unix2.conf:password: use_ldap
```

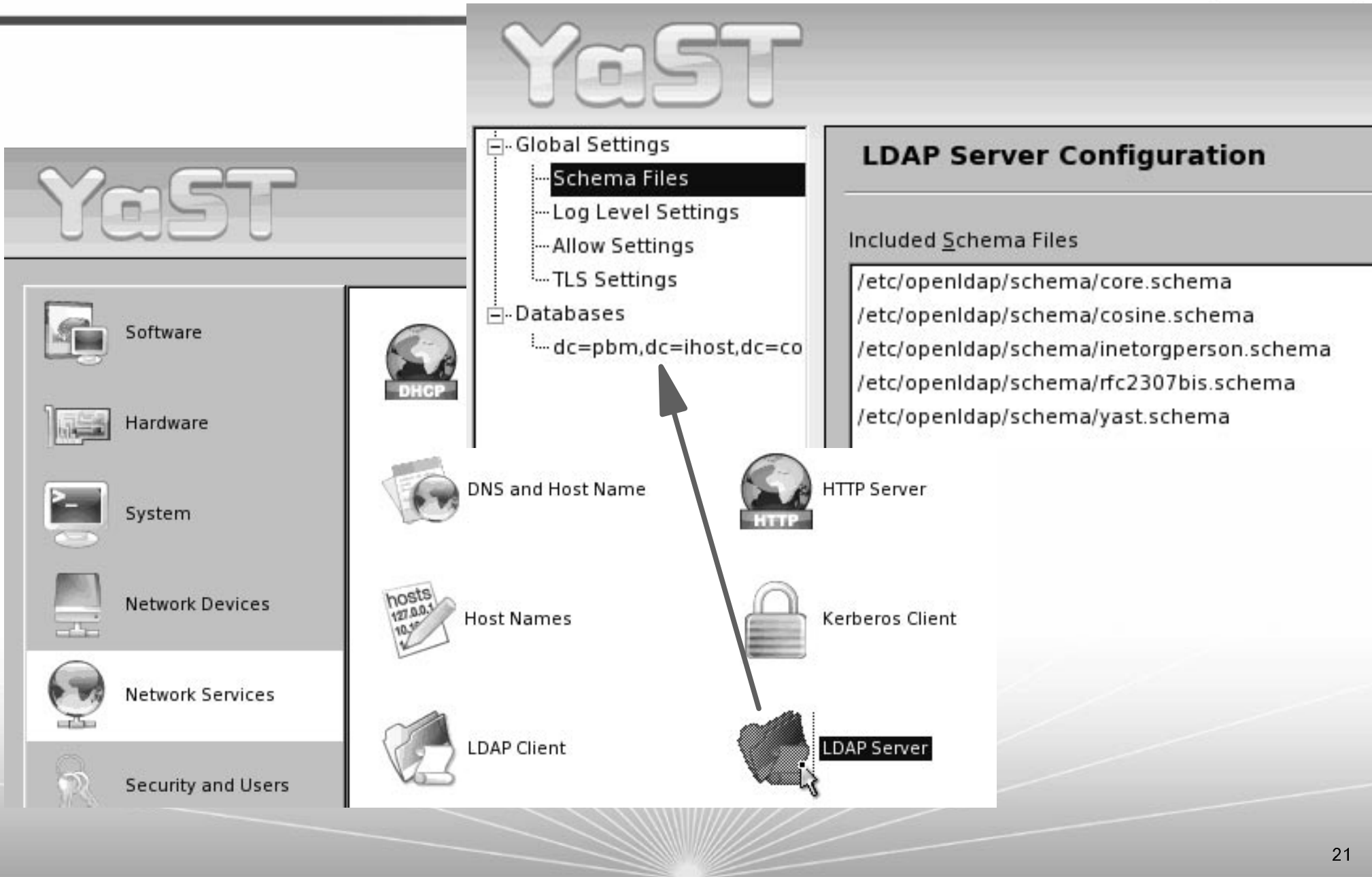
# Set up LDAP on SLES-9 (cont'd)

- Try to login via SSH as a new LDAP user ==> Error: Access Denied
  - Workaround - simply have to reboot one time or just restart sshd (Bugzilla 10846 - fixed in SP1)
- Try to get the ID of an LDAP user

```
# id mikem
uid=1000(mikem) gid=100(users) groups=100(users)
```
- Look at the LDAP data files

```
# ls /var/lib/ldap
DB_CONFIG      __db.004      gidNumber.bdb  objectClass.bdb
__db.001        __db.005      givenName.bdb  sn.bdb
__db.002        cn.bdb        id2entry.bdb   uid.bdb
__db.003        dn2id.bdb     log.0000000001 uidNumber.bdb
```
- Also note there are two files /etc/ldap.conf and /etc/openldap/ldap.conf

# Maintaining LDAP server/data



The image shows a screenshot of the YaST (Yast) configuration tool. The main window is titled "YaST" and displays a tree view of configuration categories. The "Global Settings" category is expanded, showing sub-items: "Schema Files", "Log Level Settings", "Allow Settings", and "TLS Settings". The "Databases" category is also expanded, showing "dc=pbm,dc=ihost,dc=co". A mouse cursor is pointing at the "LDAP Server" icon in the bottom right corner of the main window. To the right of the main window, a panel titled "LDAP Server Configuration" is visible, showing a list of "Included Schema Files":

- /etc/openldap/schema/core.schema
- /etc/openldap/schema/cosine.schema
- /etc/openldap/schema/inetorgperson.schema
- /etc/openldap/schema/rfc2307bis.schema
- /etc/openldap/schema/yast.schema

The left sidebar of the YaST window contains several icons and labels: Software, Hardware, System, Network Devices, Network Services, and Security and Users. The bottom right corner of the main window features several icons: DHCP, DNS and Host Name, Host Names, LDAP Client, HTTP Server, Kerberos Client, and LDAP Server. An arrow points from the "LDAP Server" icon to the "Schema Files" item in the tree view.

# YaST

## Maintaining LDAP server/data



- Software
- Hardware
- System
- Network Devices
- Network Services
- Security and Users
- Misc



CA Management



Edit and create groups



Edit and create users



Firewall

YaST2@linpoc3

## YaST

Linux is a **multiuser system**. Several different users can be logged in the system at the same time. To avoid confusion, each user must have a unique identity if they want to use Linux. Furthermore, every user at least belongs to one group.

In this dialog, get information about existing **Users**.

To shift to the group

### User and Group Administration

Users    Groups   Filter: Custom

Login	Name	UID	Groups
mikem	Mike MacIsaac	1000	
ldapuser1	LDAP User	1001	

# Maintaining LDAP server/data (cont'd)

The screenshot shows a 'Module Configuration' window with a list of configuration modules. The 'userconfiguration' module is selected, and its configuration details are displayed in a table below. The table has two columns: 'Name' and 'Value'. The 'cn' entry is highlighted.

Name	Value
cn	userconfiguration
susedefaultbase	ou=people,dc=pbm,dc=ihost,dc=com
susedefaulttemplate	cn=usertemplate,ou=ldapconfig,dc=pbm,dc=ihost,dc=com
susemapattribute	
susemaxpasswordlength	8
susemaxuniqueid	60000
suseminpasswordlength	5
suseminuniqueid	1000
susenextuniqueid	1001
susepasswordhash	CRYPT
susesearchfilter	objectclass=posixaccount
suseskeldir	/etc/skel

Buttons at the bottom of the window include: Edit, Configure Template, Back, Abort, and Next.

# LDAP GUIs and Browsers

## ■ LDAP GUI and browsers

### ▶ gq

GQ is a GTK-based LDAP client that is an LDAP browser, an LDAP V3 Schema browser, and template builder and more.

### ▶ LDAPbrowser

The LDAP Browser/Editor provides a user-friendly Windows Explorer-like interface to LDAP directories with tightly integrated browsing and editing capabilities. It is entirely written in Java with the help of the JFC (SwingSet) and JNDI class libraries. It connects to LDAP v2 and v3 servers.

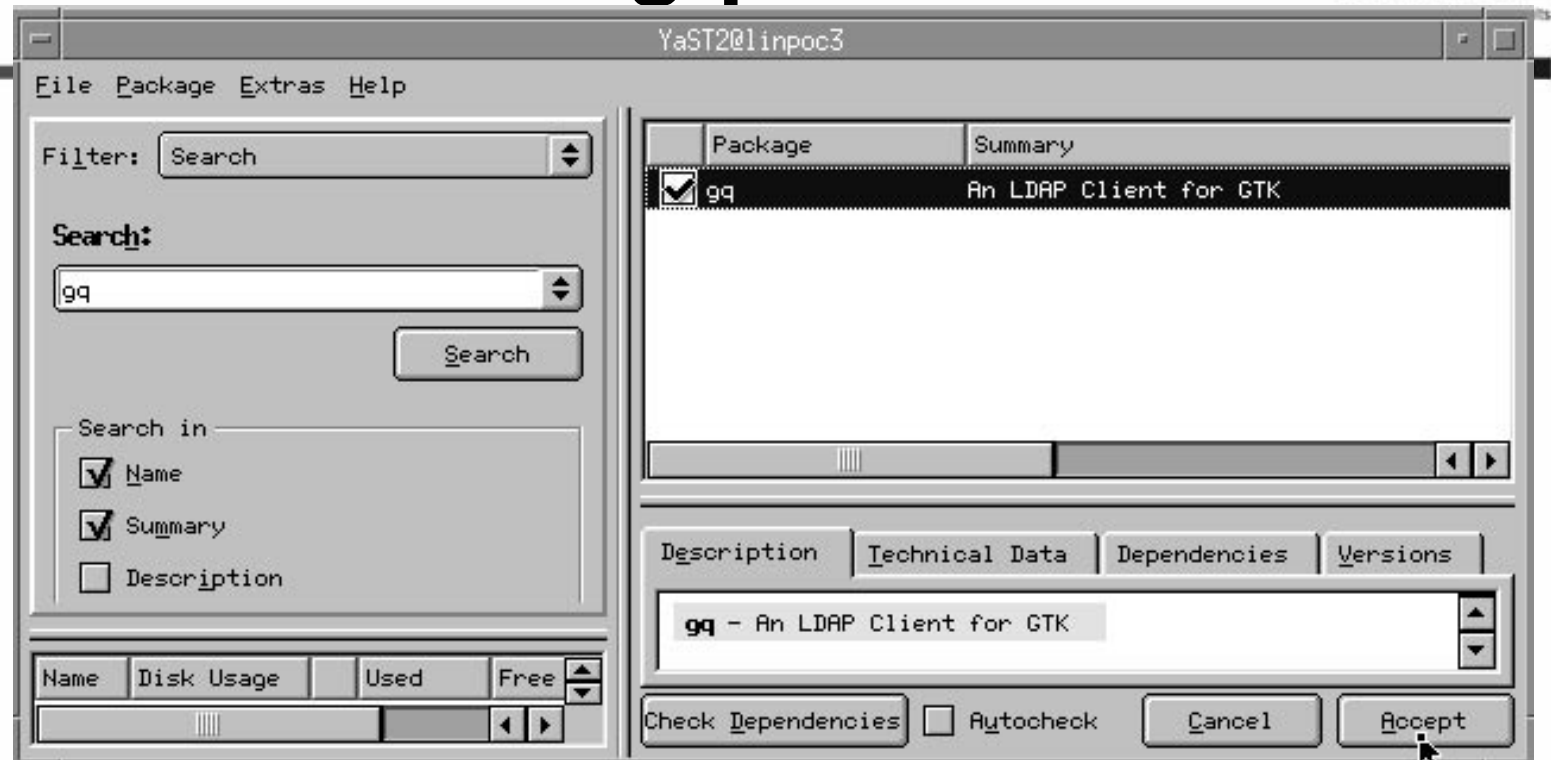
### ▶ LDAP Account Manager

LDAP Account Manager (LAM) is a Web front end for managing accounts stored in an OpenLDAP server. It integrates with Samba well.



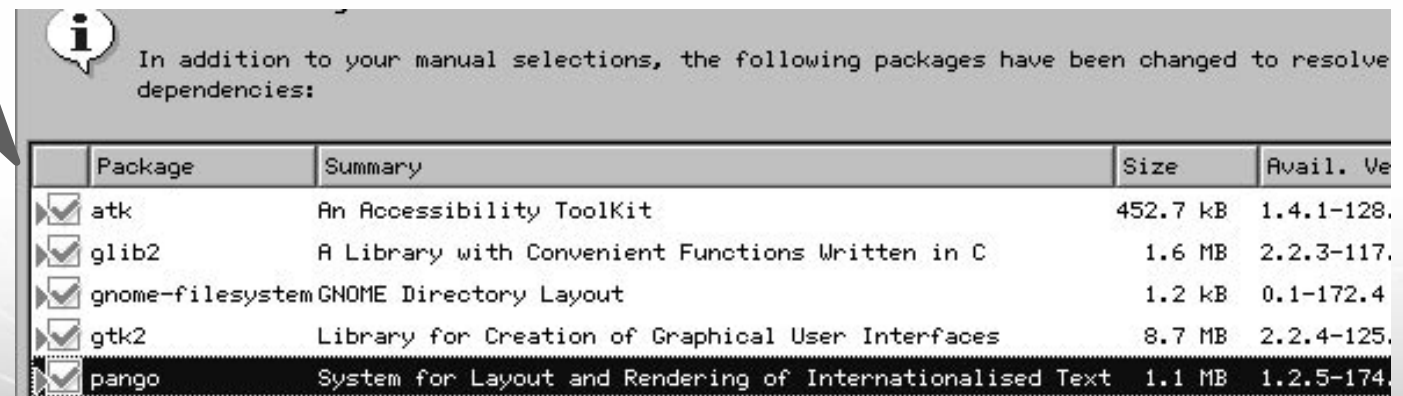
# LDAP GUI - gq

1.) For minimal install: add gq via yast2 to resolve dependencies:

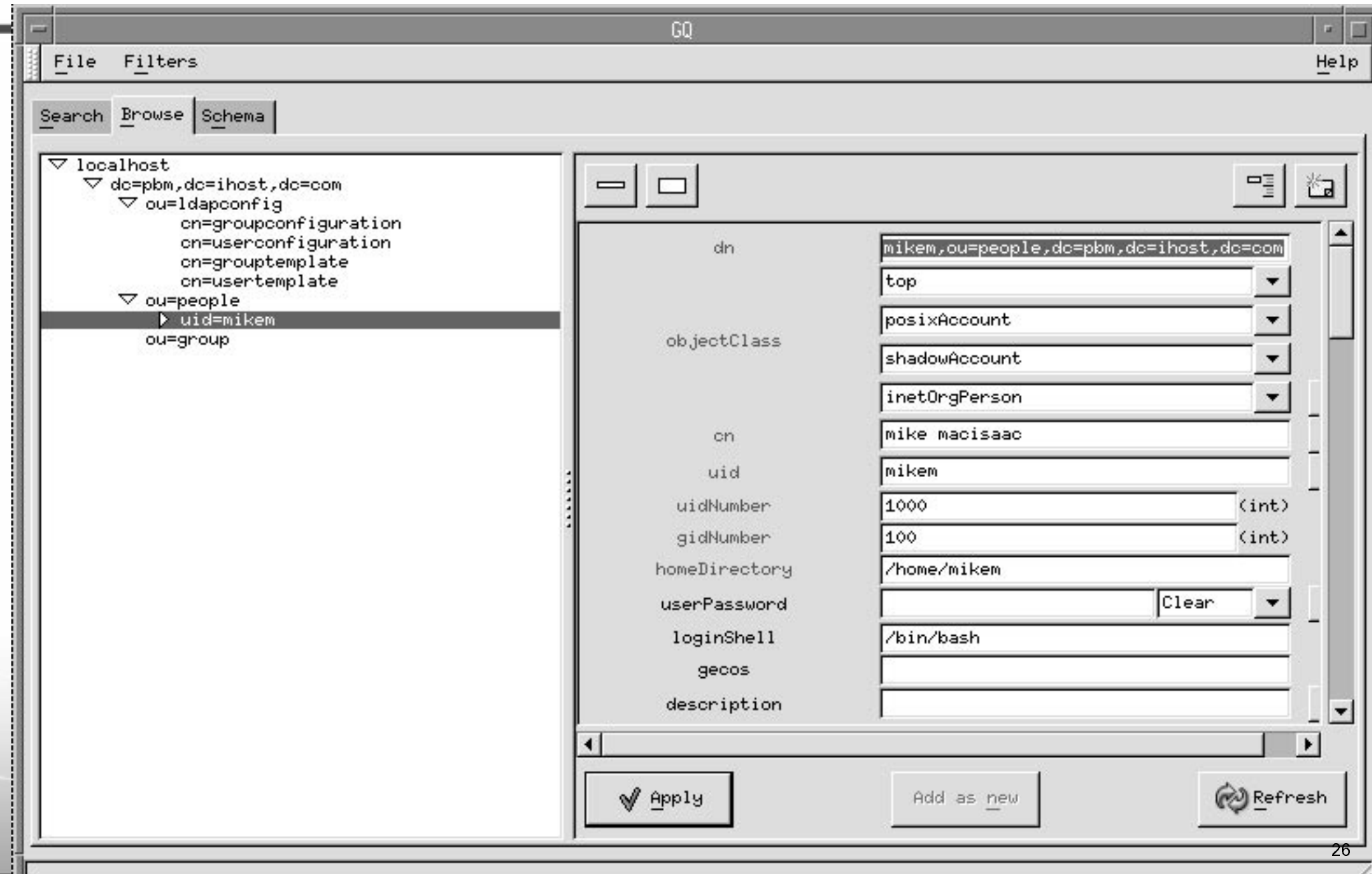


2.) Run gq (X or VNC):

```
# cd /opt/gnome/bin/
# ./gq &
```



# LDAP GUI - gq (cont'd)

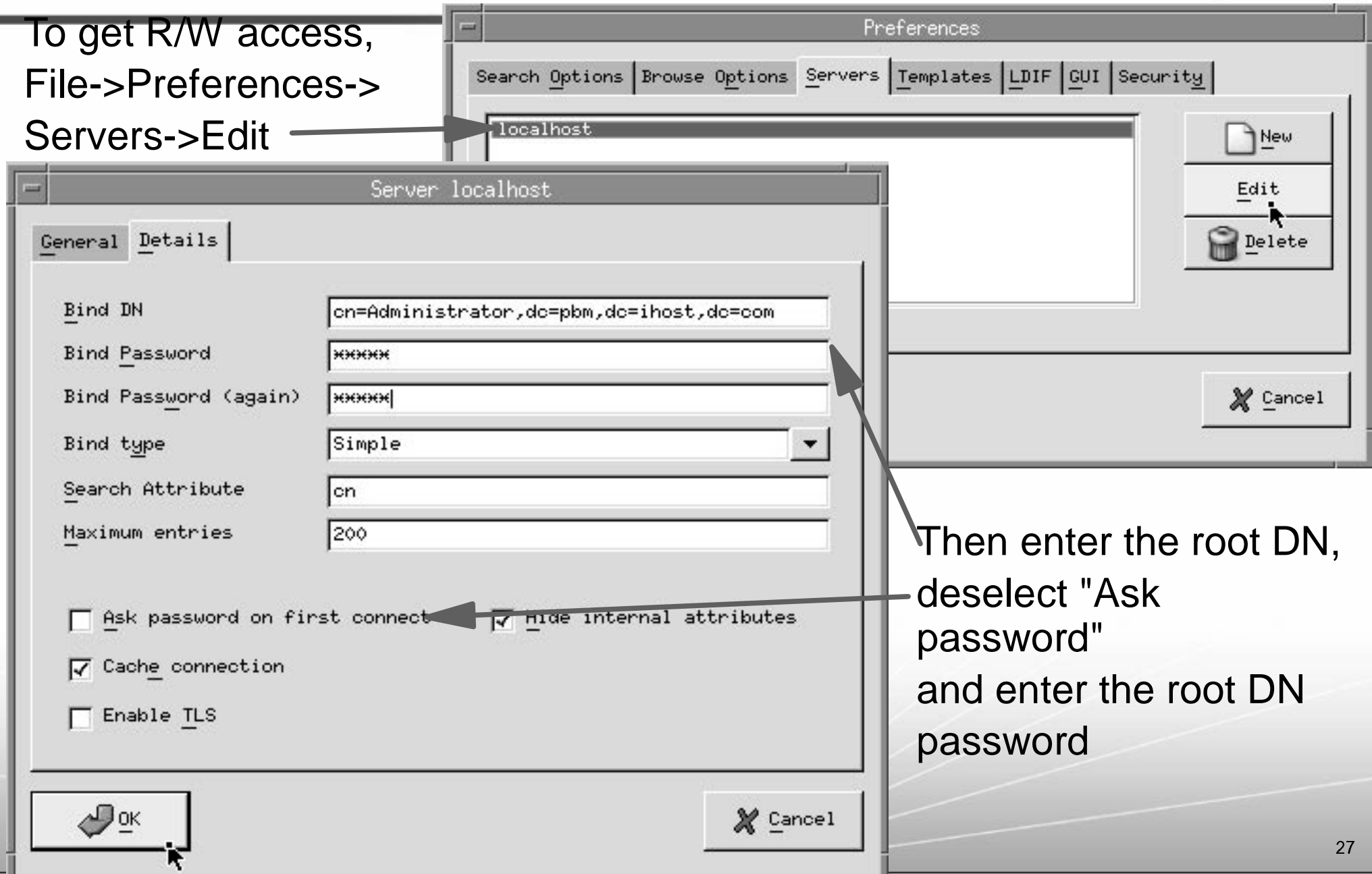


The screenshot shows the 'gq' LDAP GUI window. The left pane displays a tree view of the LDAP hierarchy, with 'localhost' expanded to show 'dc=pbm,dc=ihost,dc=com' and 'ou=people'. The 'uid=mikem' entry is selected. The right pane shows the configuration form for this entry, with fields for 'dn', 'objectClass', 'cn', 'uid', 'uidNumber', 'gidNumber', 'homeDirectory', 'userPassword', 'loginShell', 'gecos', and 'description'. The 'Apply' button is checked.

Attribute	Value
dn	mikem,ou=people,dc=pbm,dc=ihost,dc=com
objectClass	posixAccount shadowAccount inetOrgPerson
cn	mike macisaac
uid	mikem
uidNumber	1000 (int)
gidNumber	100 (int)
homeDirectory	/home/mikem
userPassword	[Redacted] Clear
loginShell	/bin/bash
gecos	
description	

# LDAP GUI - gq R/W access

To get R/W access,  
File->Preferences->  
Servers->Edit



The image shows two overlapping windows from the LDAP GUI. The background window is titled "Preferences" and has tabs for "Search Options", "Browse Options", "Servers", "Templates", "LDIF", "GUI", and "Security". The "Servers" tab is active, showing a list with "localhost" selected. To the right of the list are buttons for "New", "Edit", and "Delete". The "Edit" button is highlighted with a mouse cursor. Below these buttons is a "Cancel" button.

The foreground window is titled "Server localhost" and has two tabs: "General" and "Details". The "General" tab is active. It contains the following fields and options:

- Bind DN: `cn=Administrator,dc=pbm,dc=ihost,dc=com`
- Bind Password: `xxxxxx`
- Bind Password (again): `xxxxxx`
- Bind type: Simple (dropdown menu)
- Search Attribute: `cn`
- Maximum entries: `200`
- Ask password on first connect
- Hide internal attributes
- Cache connection
- Enable TLS

At the bottom of the "Server localhost" window are "OK" and "Cancel" buttons. A mouse cursor is pointing at the "OK" button.

Text annotations with arrows point to the "Edit" button in the "Preferences" window and the "Ask password on first connect" checkbox in the "Server localhost" window.

Then enter the root DN,  
deselect "Ask  
password"  
and enter the root DN  
password

# LDAP GUI - gq R/W access (cont'd)

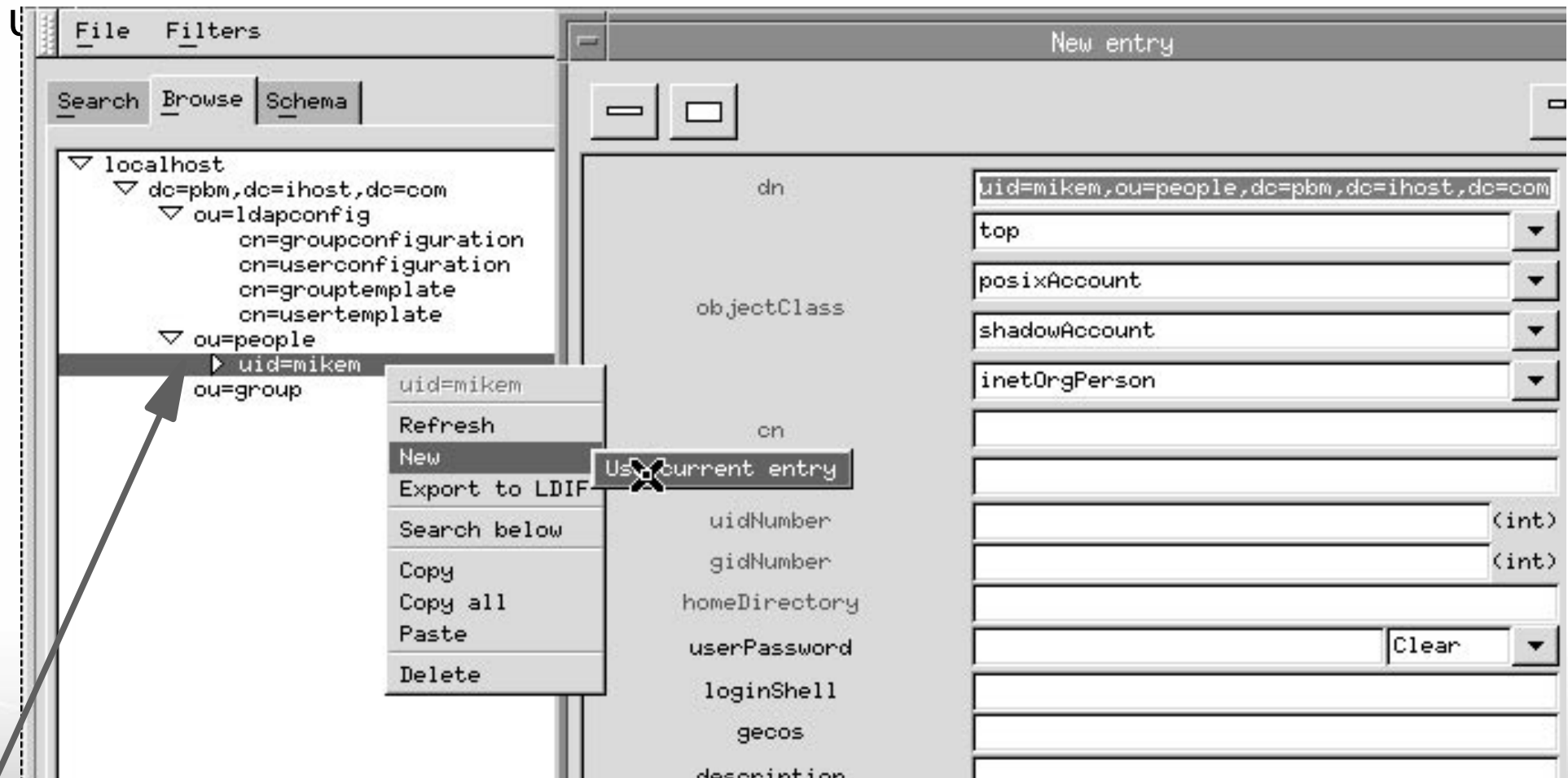


Setting these values results in this being added to `~root/.gq`:

```
<ldapserver>
  <name>localhost</name>
  <ldaphost>localhost</ldaphost>
  <ldappport>389</ldappport>
  <binddn>cn=Administrator,dc=pbm,dc=ihost,dc=com</binddn>
  <bindpw>MTIzNDU=</bindpw>
  <pw-encoding>Base64</pw-encoding>
  <search-attribute>cn</search-attribute>
  <ask-pw>False</ask-pw>
</ldapserver>
```

# LDAP GUI - gq (cont'd)

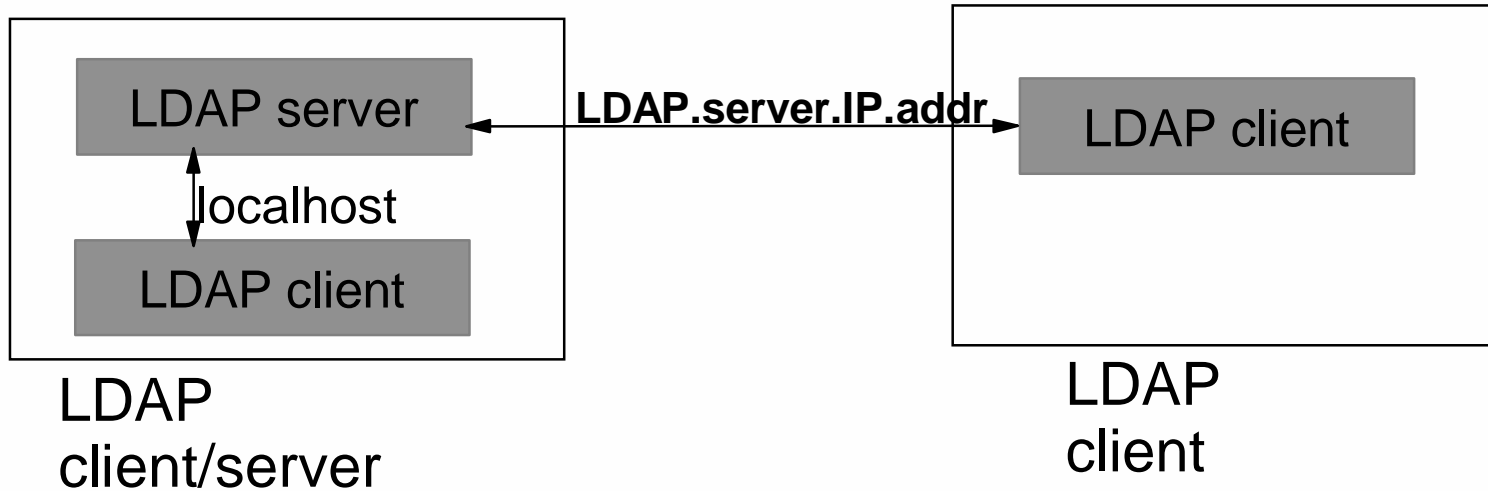
Adding a new



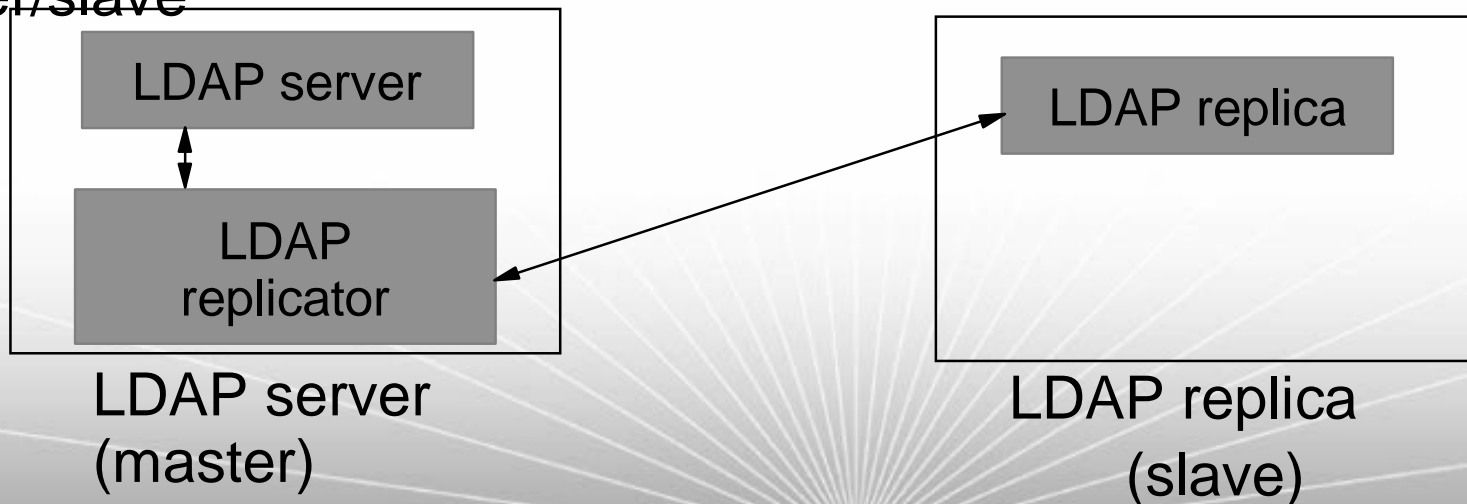
Right-click an existing user and select

# Beyond the basic LDAP client/server

LDAP client  
only

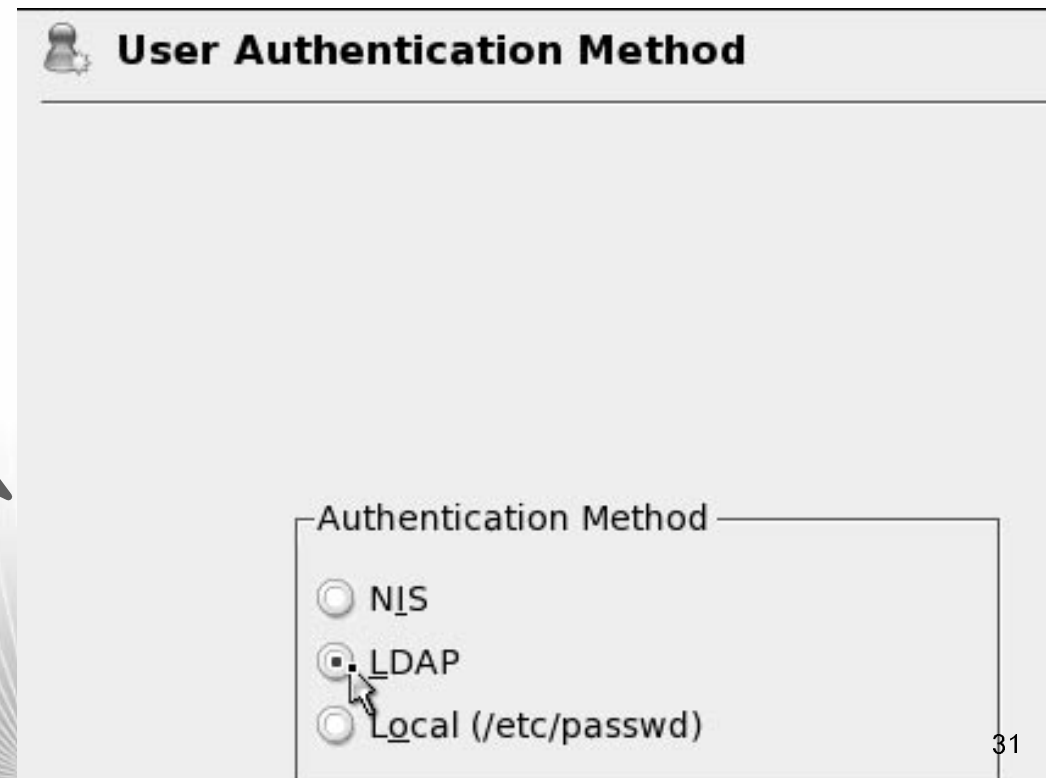
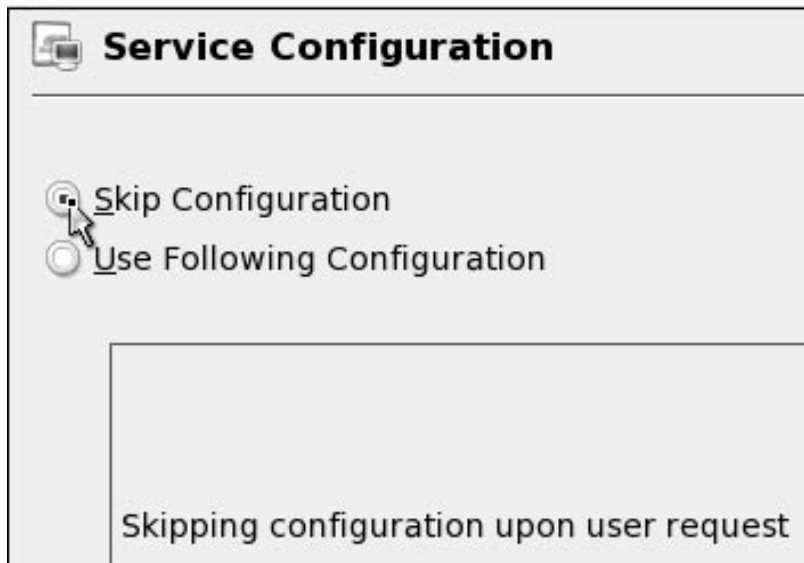


LDAP replication -  
master/slave

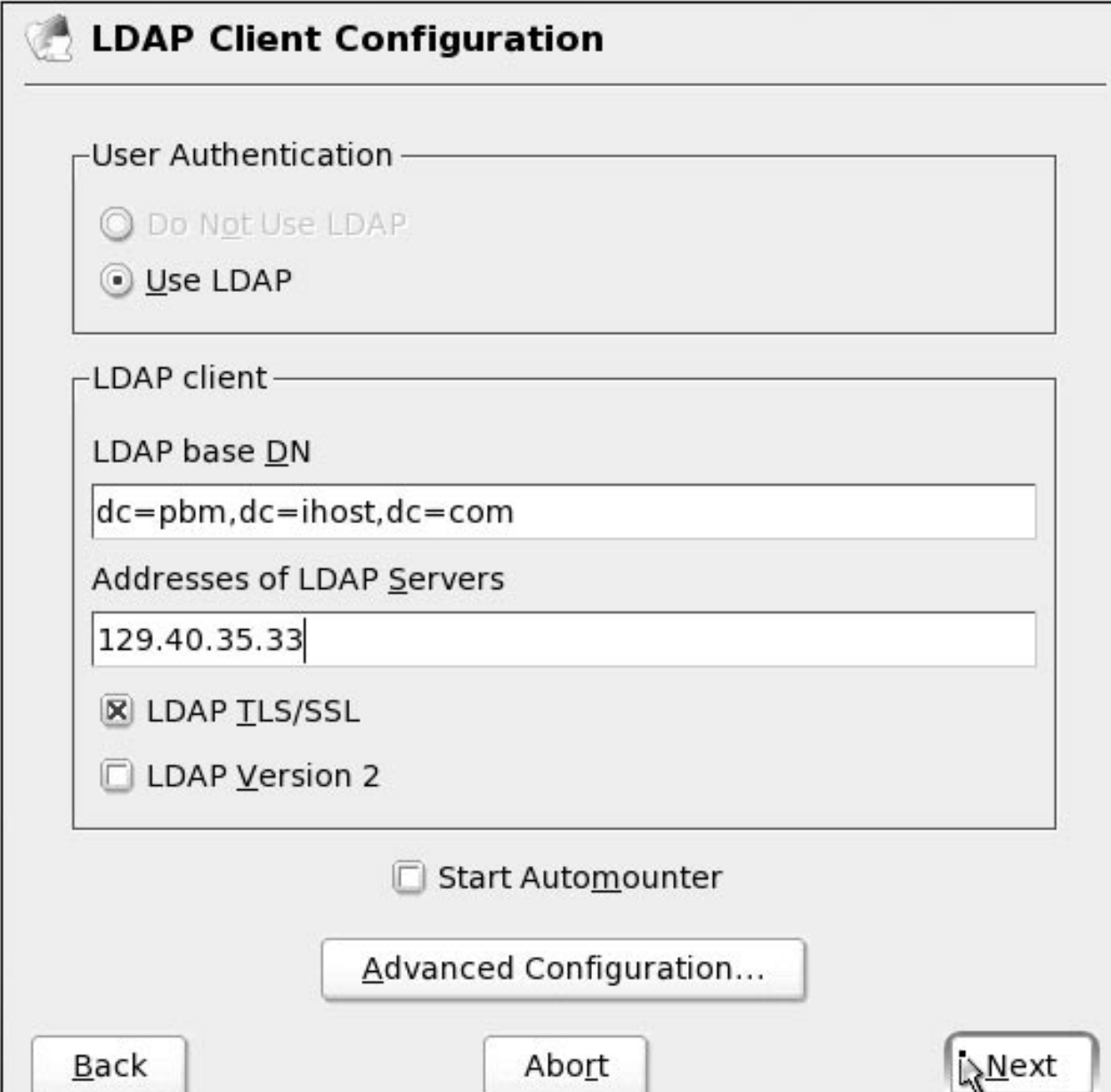


# LDAP client-only install

- ▶ Once you have an LDAP server, other penguins can use it
  - Install SLES-9 as before, but don't configure CA and LDAP



# LDAP client-only install (cont'd)

The image shows a screenshot of the 'LDAP Client Configuration' window. The window has a title bar with a small icon and the text 'LDAP Client Configuration'. Below the title bar, there are two main sections. The first section is 'User Authentication', which contains two radio buttons: 'Do Not Use LDAP' (unselected) and 'Use LDAP' (selected). The second section is 'LDAP client', which contains three text input fields: 'LDAP base DN' with the value 'dc=pbm,dc=ihost,dc=com', 'Addresses of LDAP Servers' with the value '129.40.35.33', and 'LDAP ILS/SSL' (checked) and 'LDAP Version 2' (unchecked). Below these sections, there is a checkbox for 'Start Automounter' which is unchecked. At the bottom of the window, there are three buttons: 'Back', 'Abort', and 'Next'. The 'Next' button has a mouse cursor over it.

**LDAP Client Configuration**

User Authentication

Do Not Use LDAP

Use LDAP

LDAP client

LDAP base DN

dc=pbm,dc=ihost,dc=com

Addresses of LDAP Servers

129.40.35.33

LDAP ILS/SSL

LDAP Version 2

Start Automounter

Advanced Configuration...

Back Abort Next



# LDAP client-only install (cont'd)

## ▶ Login as root and look at changes

– Look at ldap.conf file:

```
# tail -3 /etc/openldap/ldap.conf
TLS_REQCERT      allow
host             129.40.35.33
base             dc=pbm,dc=ihost,dc=com
```

– Query an LDAP user

```
# id mikem
uid=1000(mikem) gid=1000(domainusers) groups=1000(domainusers)
```

– Try to login:

```
login as: mikem
Password:
Access denied
```

- Should not happen (LTC bugzilla 10846) - reboot system and try again:

```
login as: mikem
Password:
Could not chdir to /home/mikem: No such file or directory
```

- Conclusion of bug report:

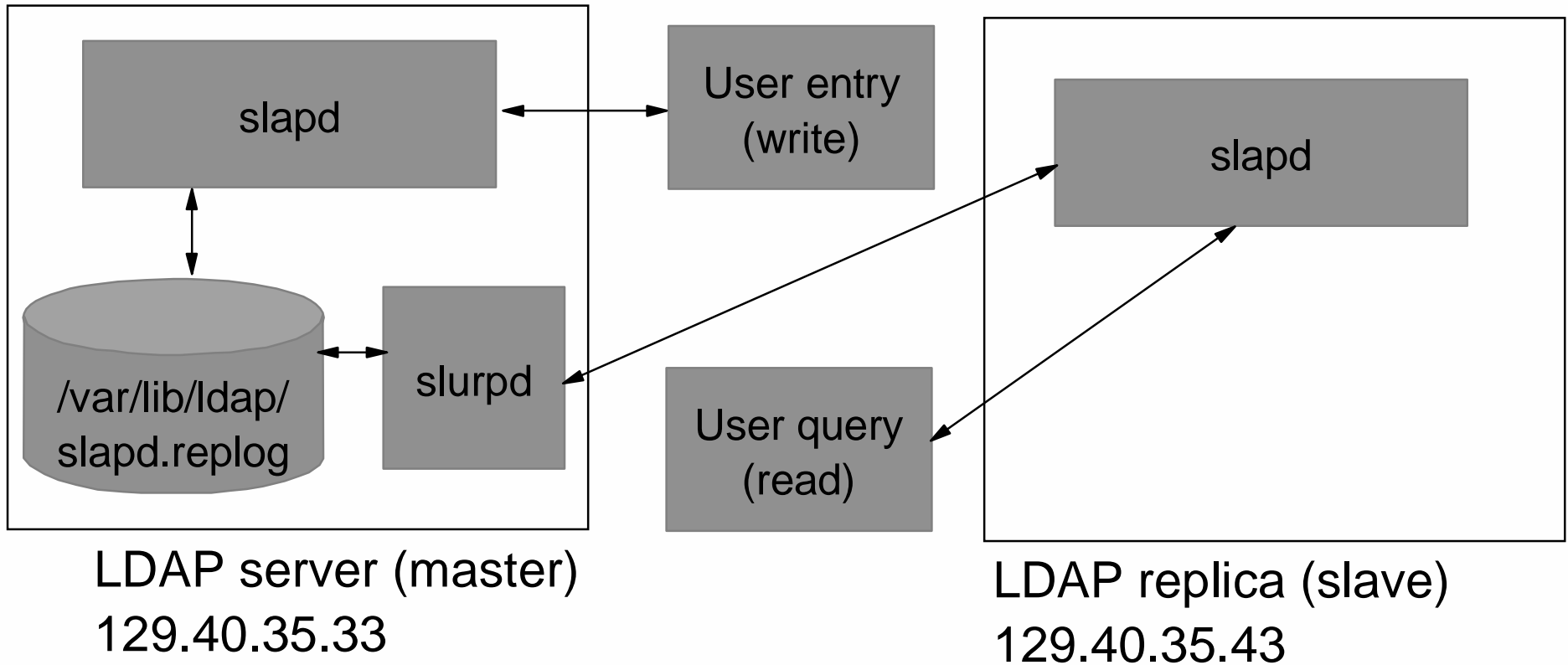
Because of low severity, I close it now. If you think it needs to be fixed for SLES9, reopen and reassign to rf.

Status	ASSIGNED	REJECTED
Resolution		WILL_NOT_FIX

# LDAP replication (master/slave)

- ▶ Replication cannot be setup at SLES-9 install time
- ▶ Steps involved for manual setup:
  - 1) Set up master server
    - a) Populate with data
    - b) Add a "replica" directive - point to the slave server
    - c) Add a "repllogfile" directive - the DB deltas to be replicated
  - 2) Set up a slave server
    - a) Add the common "suffix", "binddn" and "bindpw"
    - b) Add an "updatedn" directive - same as binddn
    - c) Add an "updateref" directive - point to the server
  - 3) Copy the master DB to the slave
    - a) Use **slapcat** on master to an LDIF file
    - b) Copy LDIF file to slave
    - c) Use **slapadd** on slave from LDIF file
  - 4) Restart master server
  - 5) Start slave server
  - 6) Start master replicator - slurpd

# LDAP replication (cont'd)



# DAP replication - master/slave (cont'd)



## ► Steps involved for manual setup (details):

### 1) Set up master server

```
# tail -5 /etc/openldap/slapd.conf
replica uri=ldap://129.40.35.43
  binddn="cn=Replicator,dc=pbm,dc=ihost,dc=com"
  bindmethod=simple
  credentials=12345
  tls=yes
repllogfile /var/lib/ldap/slapd.repllog
```

### 2) Set up a slave server

```
# tail -5 /etc/openldap/slapd.conf
suffix "dc=pbm,dc=ihost,dc=com"
rootdn "cn=Replicator,dc=pbm,dc=ihost,dc=com"
rootpw 12345
updatedn "cn=Replicator,dc=pbm,dc=ihost,dc=com"
updateref ldap://129.40.35.33
```

### 3) Copy the master DB to the slave (on master)

```
# cd /etc/openldap
# slapcat > slapcat.ldif
# scp slapcat.ldif 129.40.35.43:/etc/openldap
Password:
slapcat.ldif
```

100% 8630

8.4KB/s

00:00

# DAP replication - master/slave (cont'd)



3) Copy the master DB to the slave (on slave)

```
# cd /etc/openldap
# slapadd < slapcat.ldif
```

4) Restart master server

```
# rclldap start
Starting ldap-server
```

done

5) Start slave server

```
# rclldap start
Starting ldap-server
# chkconfig ldap on
```

done

6) Start master replicator - slurpd

```
# rclslurpd start
Starting slurpd
# chkconfig slurpd on
```

done

If a slave gets out of sync:

```
# rclldap stop
# rm /var/lib/ldap/*
# ftp> get new-fresh-copy-of-slapcat.ldif
# slapadd < slapcat.ldir
# rclldap start
```

# Resources

## ■ Books, papers

- IBM Redbook *Understanding LDAP*, SG24-4986, Heinz Johner, et al  
<http://www.redbooks.ibm.com/abstracts/sg244986.html>
- *OpenLDAP 2.1 Administrator's Guide*, OpenLDAP team  
<http://www.openldap.org/doc/admin21/>
- *Directory Services for Linux in comparison with Novell NDS and Microsoft Active Directory*, Norbert Klasen Master's Thesis  
<http://www.daasi.de/staff/norbert/thesis/>
- *LDAP System Administration*, Gerald Carter, O'Reilly, 2003  
<http://www.oreilly.com/catalog/ldapsa/index.html>

## ■ Web sites

- OpenLDAP  
<http://www.openldap.org/>
- PADL Software PDY Ltd.  
<http://www.padl.com/>
- web2ldap  
<http://www.web2ldap.de/>

# Questions?

- ▶ Are there any questions?

???

- ▶ This presentation (PDF, .prz) is on  
<ftp://9.57.26.222/>

# Birds of a Feather Advertisement

- **Linux Appliance BoF: Weds. at 6:00PM in room 207A** (session 0103)
- "The Linux on zSeries Appliance Cookbook: Featuring z/VM" will be discussed:
  - ▶ It is a draft redbook and associated tar file with EXECs and scripts
  - ▶ A goal is to approach the concept of "Linux appliances" on zSeries under z/VM
  - ▶ You can go "from LPAR to Linux cloning in two days" doing the following tasks:
    - Install and configure z/VM 5.1 from DVD
    - Install and configure a "golden image" Linux to be cloned from
    - Install and configure a "controller" Linux to clone, back up appliances, more
    - Create appliances such as Web server, LDAP server, File/print server, SNA server, 374x
    - Address z/VM and Linux backup, restore, service and monitoring requirements
- It is designed for people with mainframe/IT skills but not necessarily VM and Linux skills