Session: 420034

Getting My LDAP Server Up and Running

IBM @server iSeries

John McMeeking

8 Copyright IBM Corporation, 2002. All Rights Reserved.
This publication may refer to products that are not currently available in your country. IBM makes no commitment to make available any products referred to herein.

Agenda

- Basic concepts
- Configuring the server
- Managing the server
- Configuring publishing
- Tools for accessing the directory
- References

Basic Concepts

LDAP Concepts

- Concept Review:
  - Directory Information Tree - directory entries are organized in a hierarchical structure
    - entries have a distinguished name (DN) made up of the entry's name (RDN) in combination with its ancestor entries -- "cn=John McMeeking, cn=users, o=acme, c=us"
  - Data Model - object consists of a set of attribute values
    - objectclass - defines the set of required and allowed attributes for an entry
    - attribute - has a defined syntax (directory string, boolean, etc.) and matching behavior
  - Directory accessed via a standard protocol (LDAP -- Lightweight Directory Access Protocol) defined by various Internet RFCs
    - protocol defines operations for searching the directory, as well as adding, modifying, deleting and moving entries
  - Widely available client APIs: C API defined by draft RFC, the Java Naming and Directory Interface (JNDI) LDAP service provider, others

LDAP Concepts - Suffixes

- What is a suffix (aka naming context)?
  - Used by many server implementations to define the "namespace" that the server recognizes
  - "o=ibm,c=us", "dc=ibm,dc=com", "o=acme,c=au", "cn=John Smith,cn=users,o=ibm,c=us" are all valid DNs.
  - The suffix "o=ibm,c=us" tells the server that DNs that end in "o=ibm,c=us" are in this server's namespace -- a given DN in this namespace might not refer to an existing entry, but... DNs that do not fall within the defined suffixes are not handled by the server. The server will return "no such object" or a redirect the client to another server that might handle that namespace (a "referral").

LDAP Concepts - Authentication

- Each client has an authenticated identity established through a "bind" operation. If no bind is performed, the client is treated as "anonymous".

- "Simple" bind
  - Anonymous - no authentication done or provided a null/empty DN at bind time
  - DN and password - client's identity is the DN provided at bind time. Server verifies the password. This is also called a "simple bind".
  - Administrator - has access to all objects and attributes. The DN (cn=administrator is the default on iSeries) and password are part of the server configuration
  - DN can be the name of an object with a userPassword attribute

```
dn: cn=John Smith,cn=users,o=acme,c=us
objectclass: inetorgperson
userpassword: secret
```

  - DN can also be an entry with a UID attribute the same as an OS/400 user profile and no userPassword. Server calls OS/400 to see if password is valid for that user profile.

```
dn: cn=John Smith,cn=users,o=acme,c=us
objectclass: inetorgperson
uid: JSMITH  <== JSMITH must be a user profile on the same system
```

LDAP Concepts - Authentication

- SASL (Simple Security and Authentication Layer) binds:
  - Kerberos (GSSAPI) - authentication via a Kerberos ticket. This is used in Windows 2000 and other environments.
    - LDAP server can be configured to generate a DN based on the Kerberos principal name: ibm-kn=jsmith@acme.com
    - Or server can be configured to search for an object that has an altSecurityIdentities attribute matching the Kerberos principal:

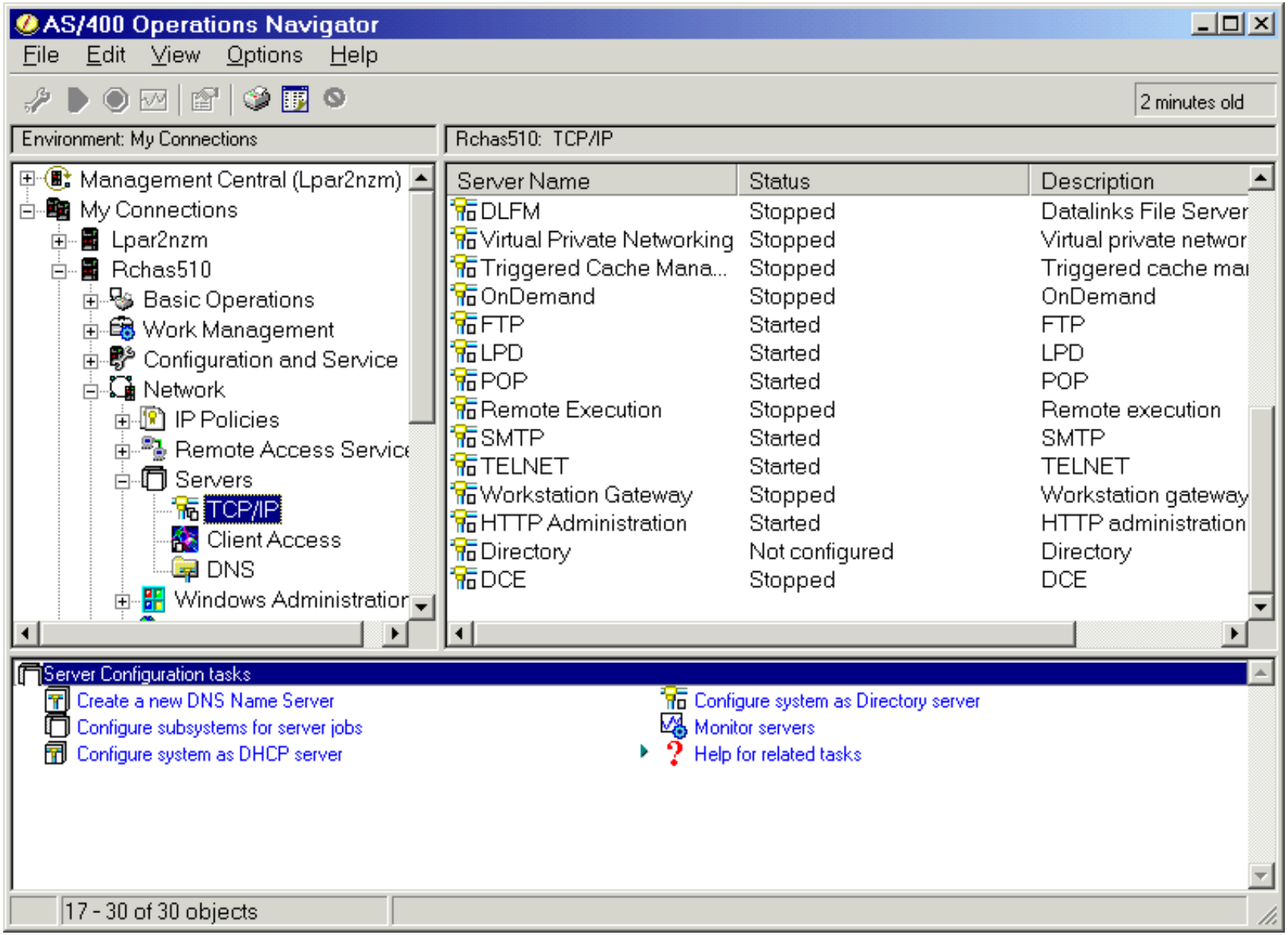
```
dn: cn=John Smith,cn=users,o=acme,c=us
objectclass: inetorgperson
objectclass: ibm-securityIdentities
altsecurityidentities: kerberos:jsmith@acme.com
...
```

    - The above would result in a client with the identity cn=John Smith,cn=users,o=acme,c=us
  - EXTERNAL using SSL/TLS - identity is the subject DN from the certificate used to establish the connection.
    - This can (but need not) be the DN of an object in the directory.

Configuring the LDAP Server

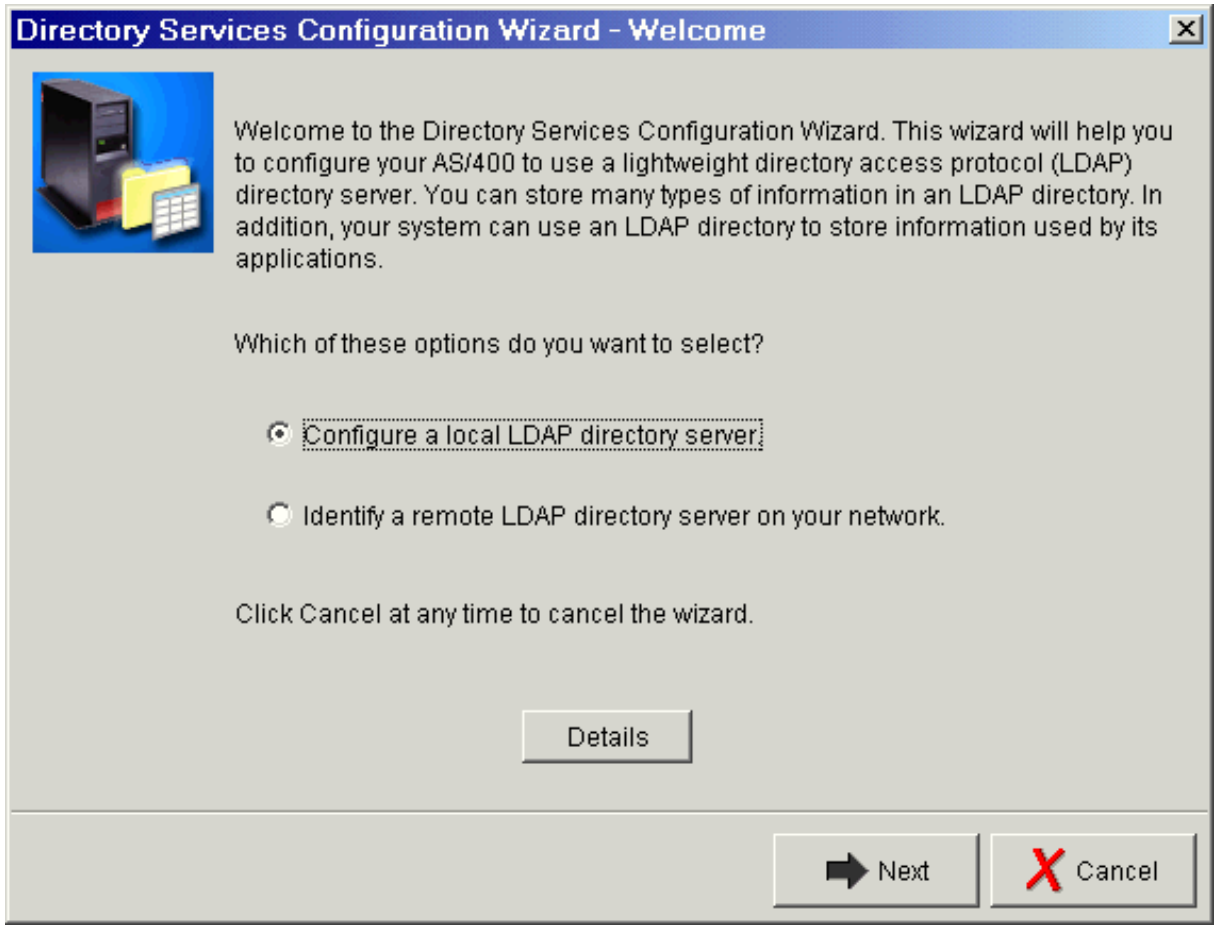
Configuring the LDAP server

IBM @server iSeries



IBM @server. For the next generation of e-business.

Configuration Wizard Welcome Panel

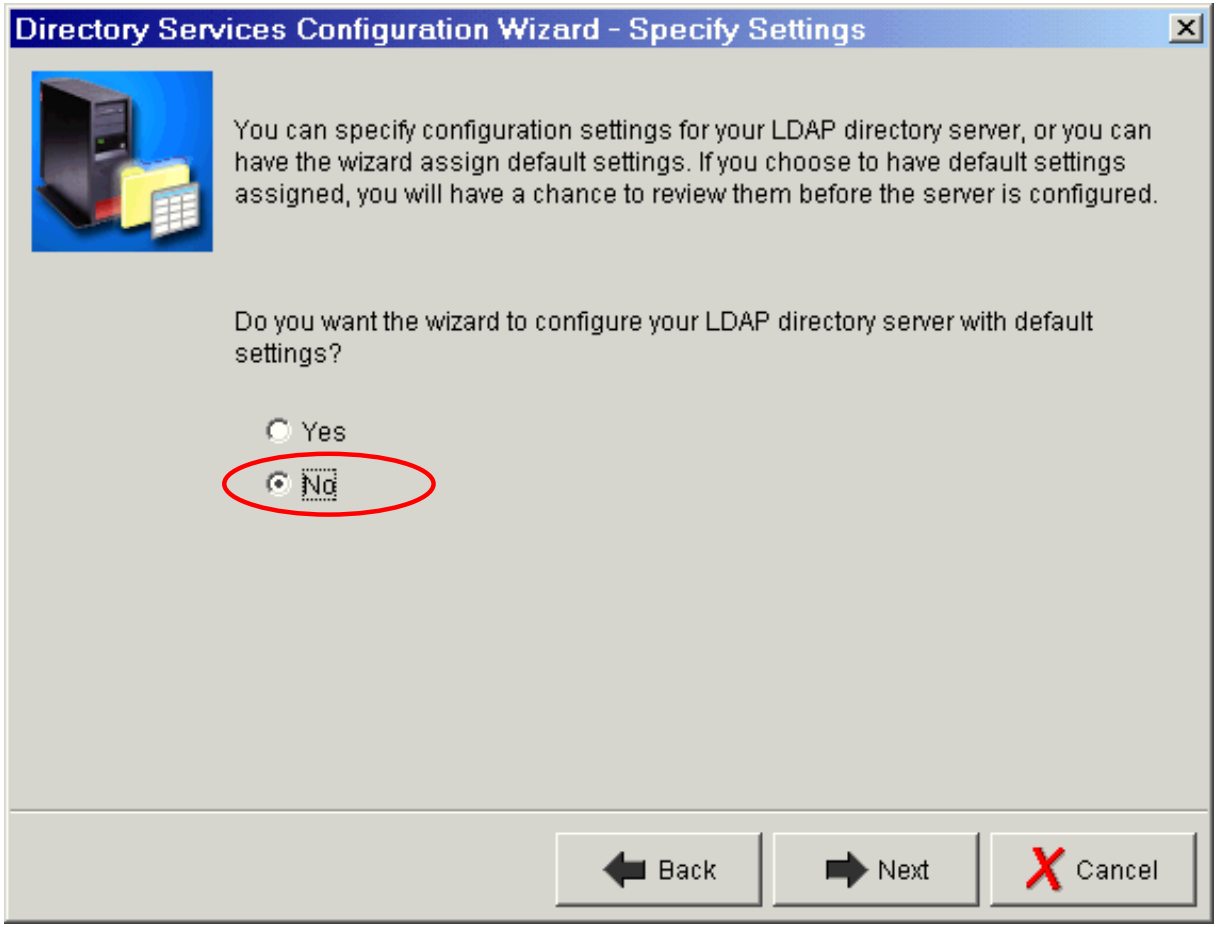


Before you start - new server

- Do you want to configure a local server (this machine)? You'll need:
  - administrator dn and password
  - suffix to add to the server (you can change this later). There are two common naming conventions:
    - organization name (o=acme, c=us) from X.500 standards
    - domain naming (rchas510.acme.com becomes dc=rchas510,dc=acme,dc=com)
- Underlying database will be in library QURDIRDB
- Server will use default port (389), and will use SSL if a certificate has been assigned to the QIBM_GLD_DIRSRV_SERVER server application

Configuration Wizard - Use defaults?

Don't take default configuration. You'll want to know the password.

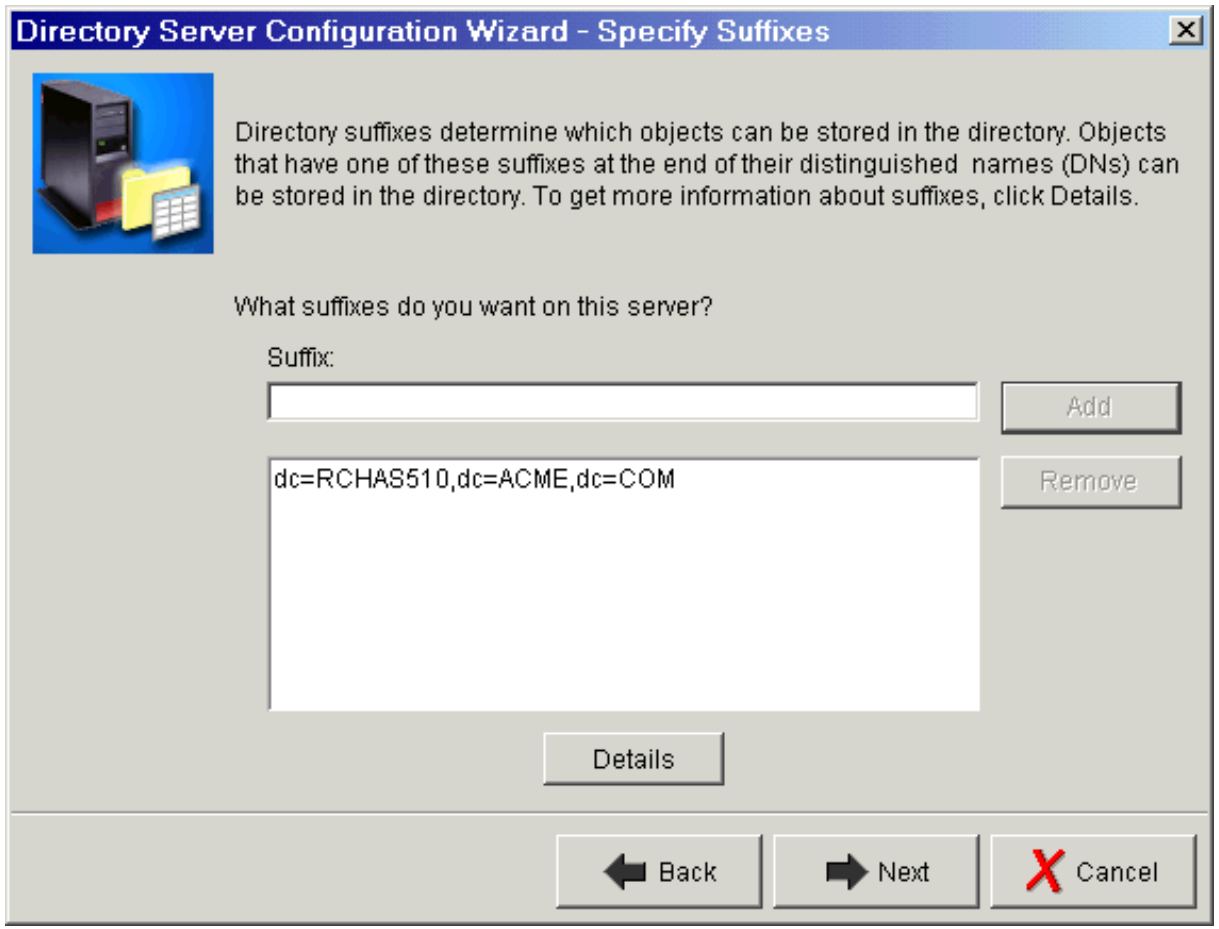


Configuration Wizard - Administrator

Uncheck 'System-generated' so you can enter a password - unless you want a random password known only to the server.

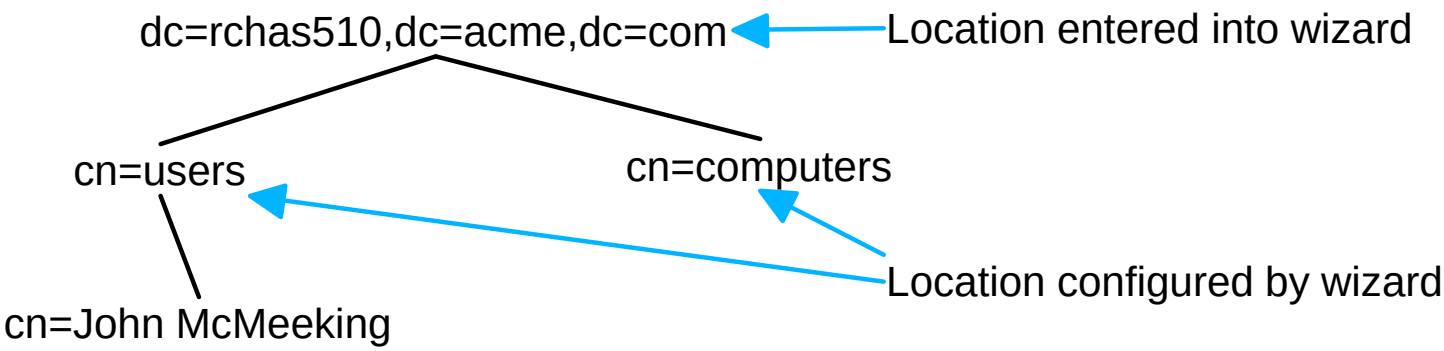
Configuration Wizard - Suffixes

Use the generated suffix or create your own.



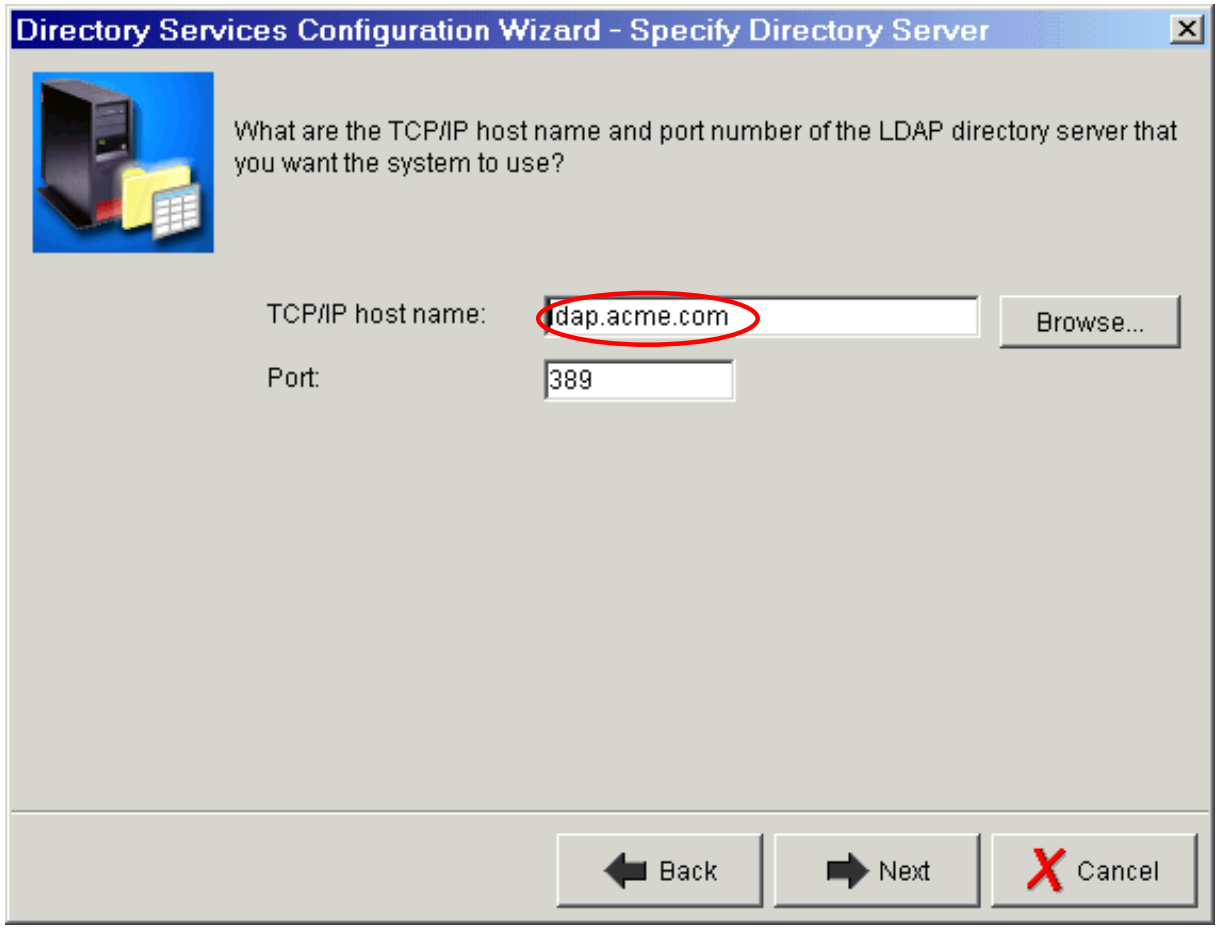
Before you start - Publishing

- Publishing to a local or remote (elsewhere in your network) server
  - May want to publish users from SDD or publish basic system info
  - Server name, port, etc.
  - Location in the directory to publish information

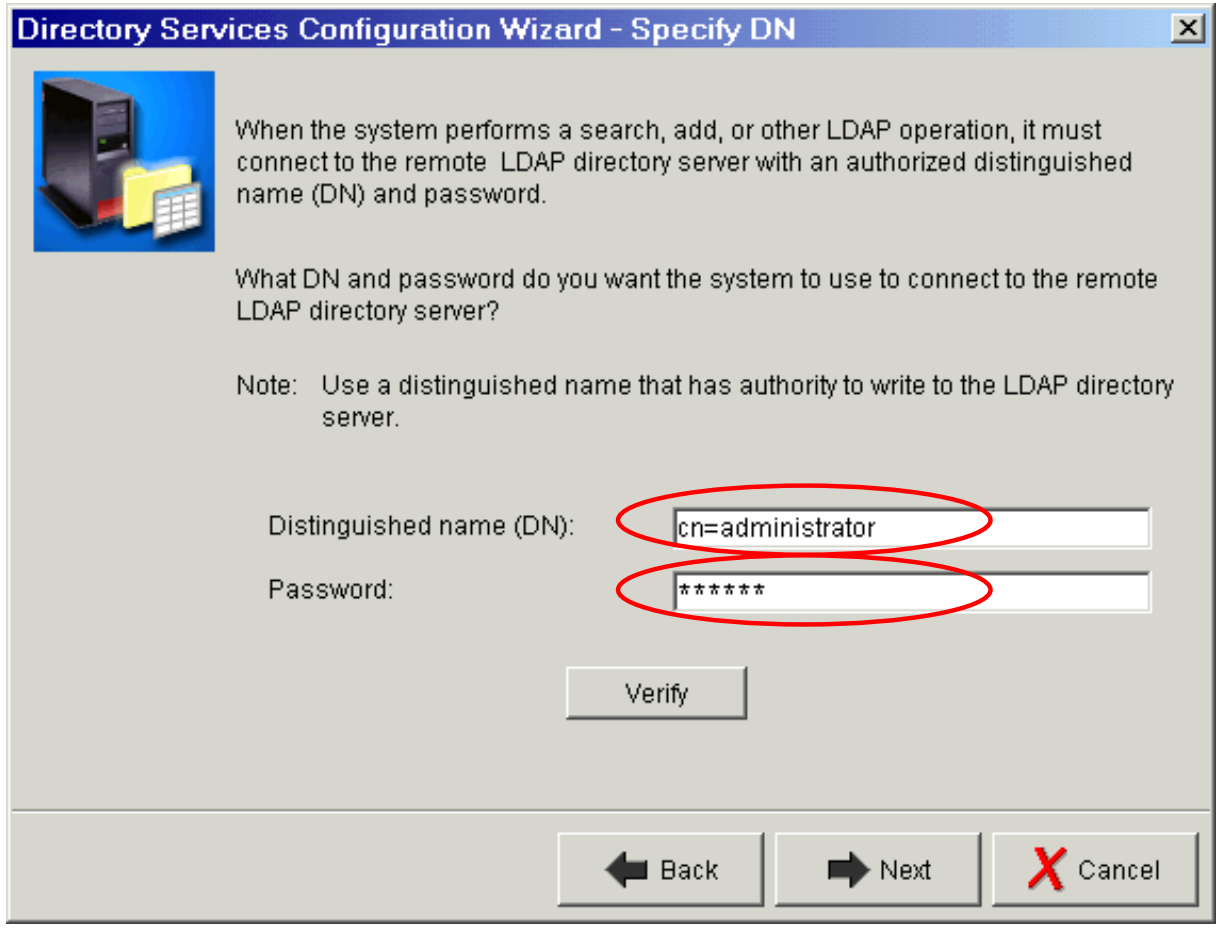


  - Credentials for someone authorized to create/delete/change entries in selected location
    - Could be administrator (cn=administrator), but you might want to create other identities and give them authority

Configuration Wizard - Publishing



Configuration Wizard - Publishing



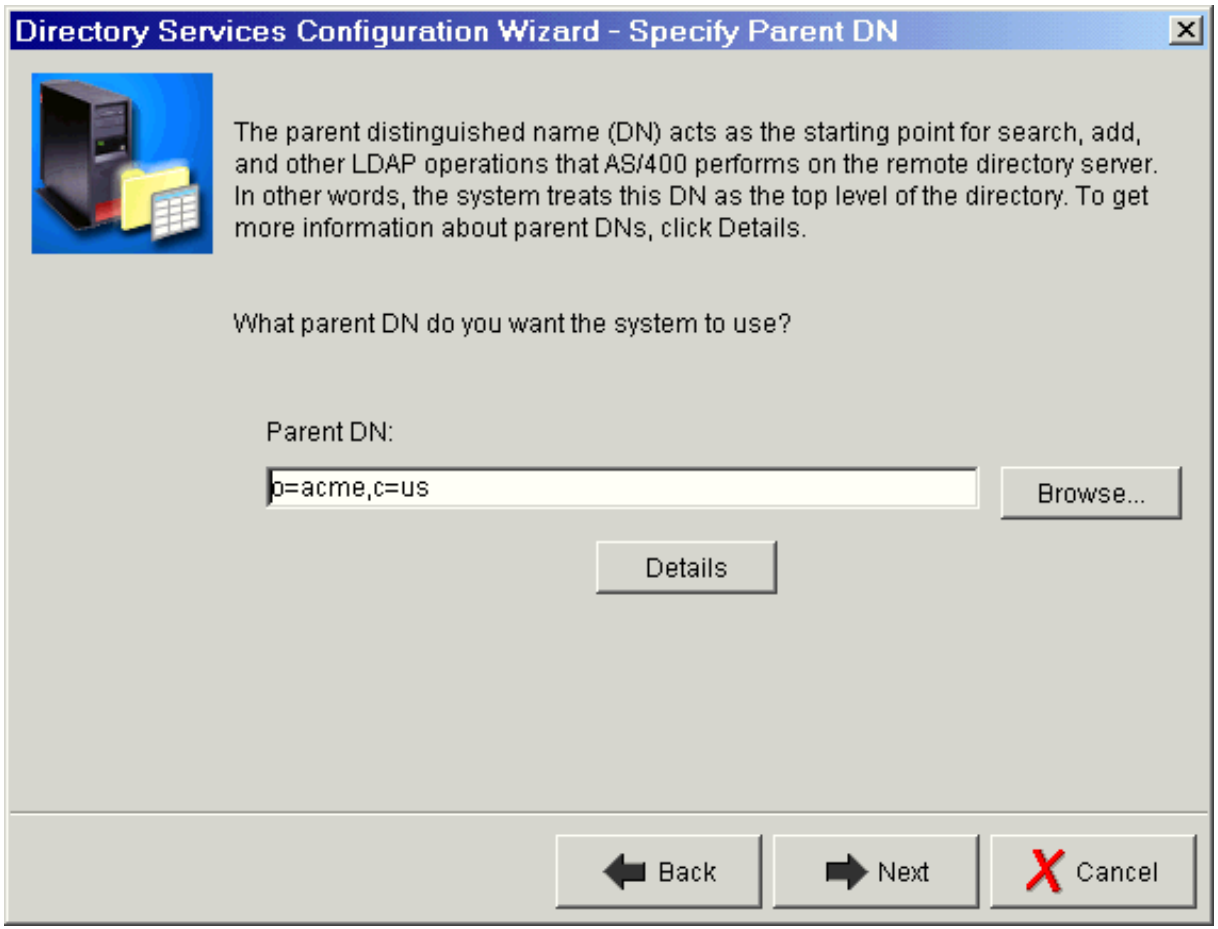
Configuration Wizard - Publishing

Wizard will configure agents to use parent DNs beneath this suffix:

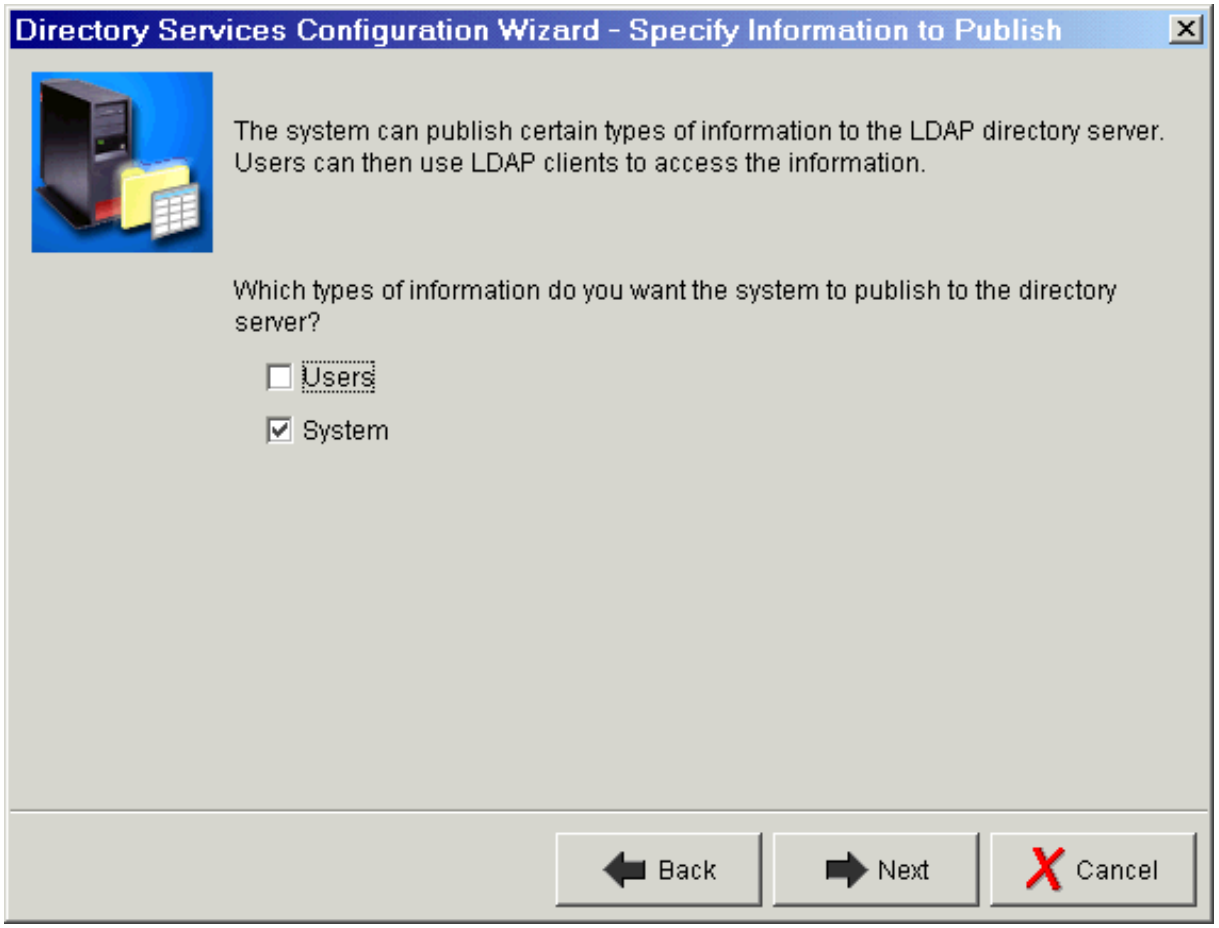
"cn=users," + configured parent DN

"cn=computers," + configured parent DN

These entries will be created by the publishing engine if they do not exist.

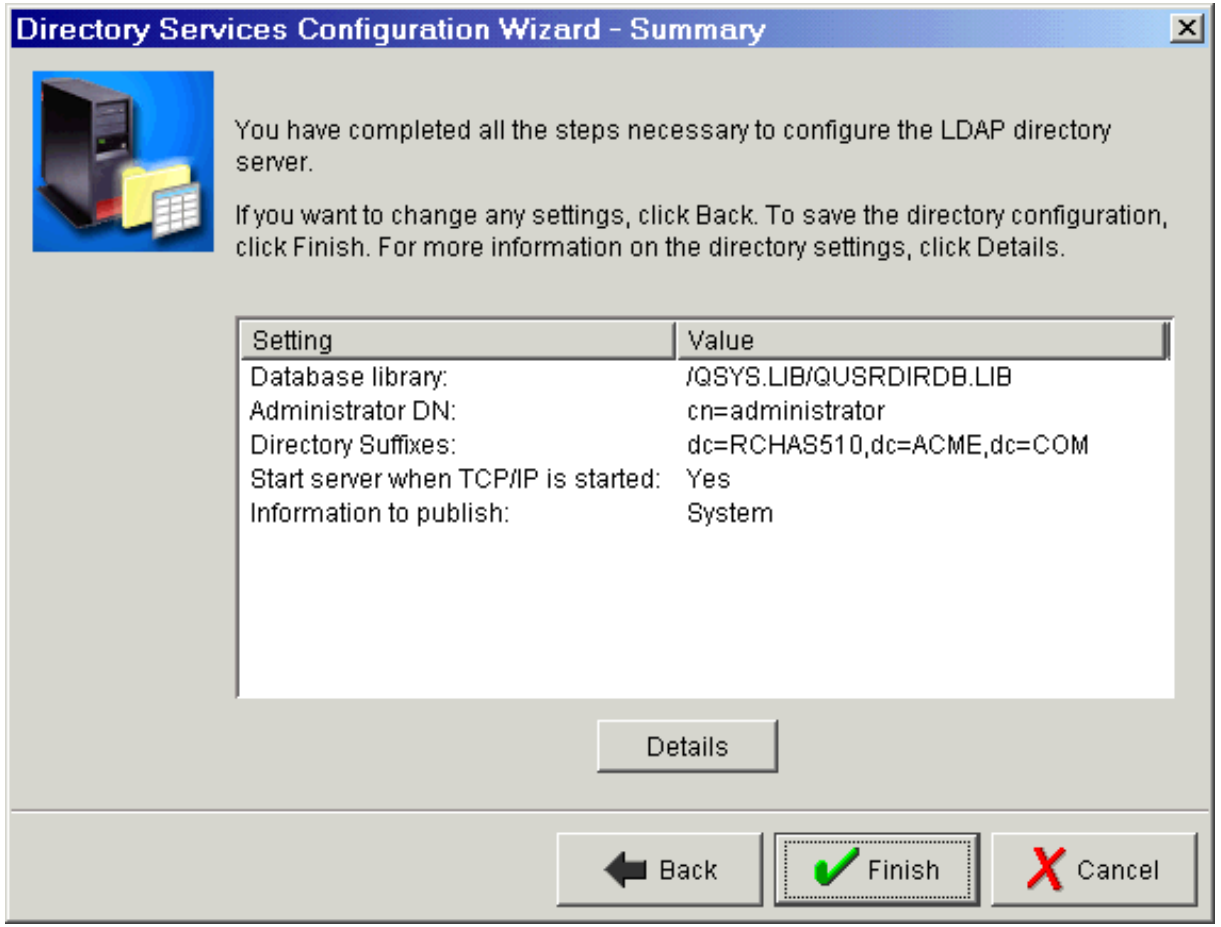


Configuration Wizard - Publishing



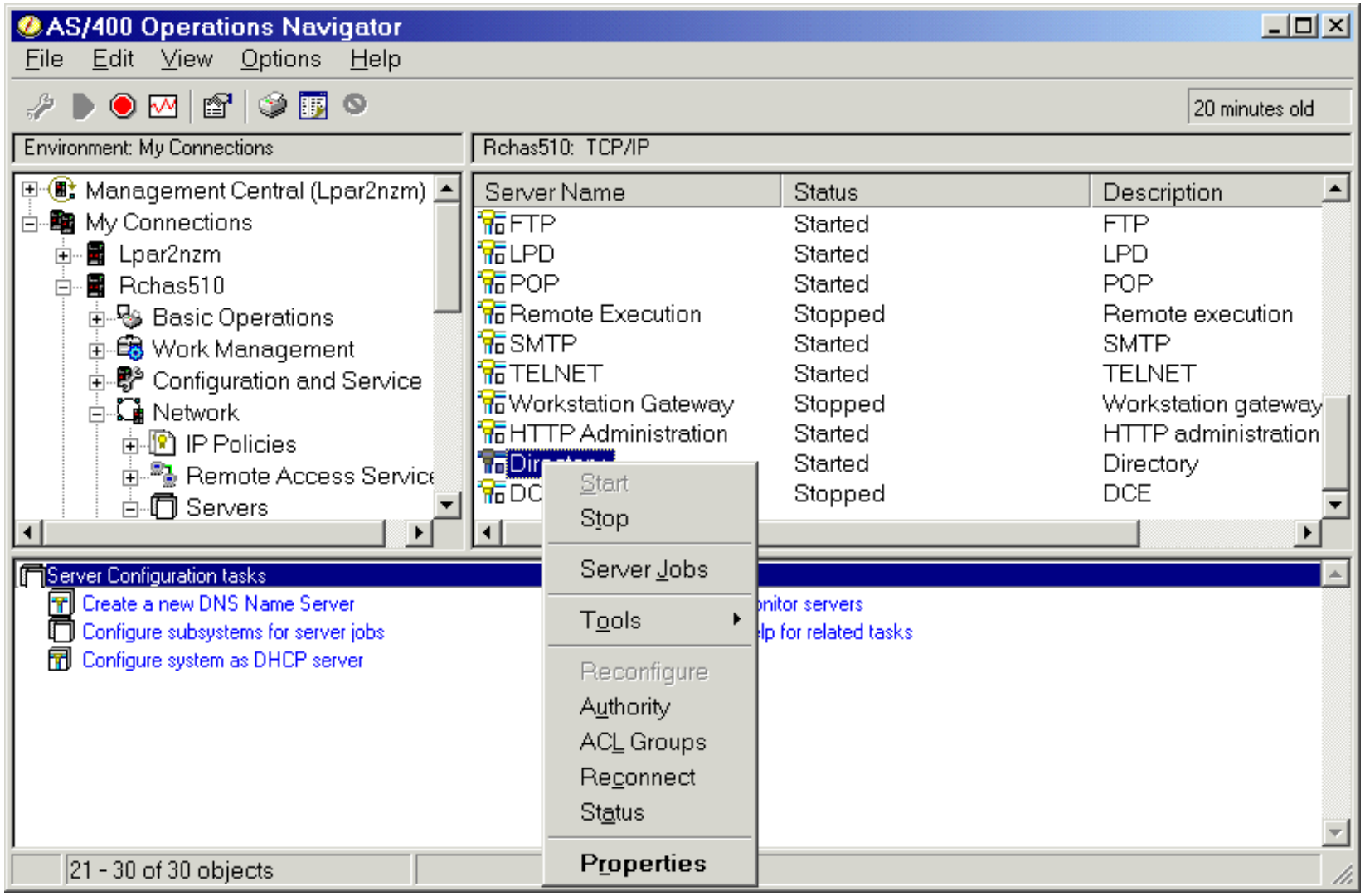
Configuration Wizard - Summary

Wizard will create server and/or publishing configuration and start the server



Managing the Directory Server

Managing the server with Operations Navigator



Managing the server with Operations Navigator

- Start and stop server, monitor status
- Import/export data to/from directory
- Manage access to directory data, including group management
- Server configuration, including:
  - Database and suffixes
  - Network (SSL, ports)
  - Kerberos
  - Administrative limits associated with various features:
    - Searches, transactions, event notification

Managing access to the directory

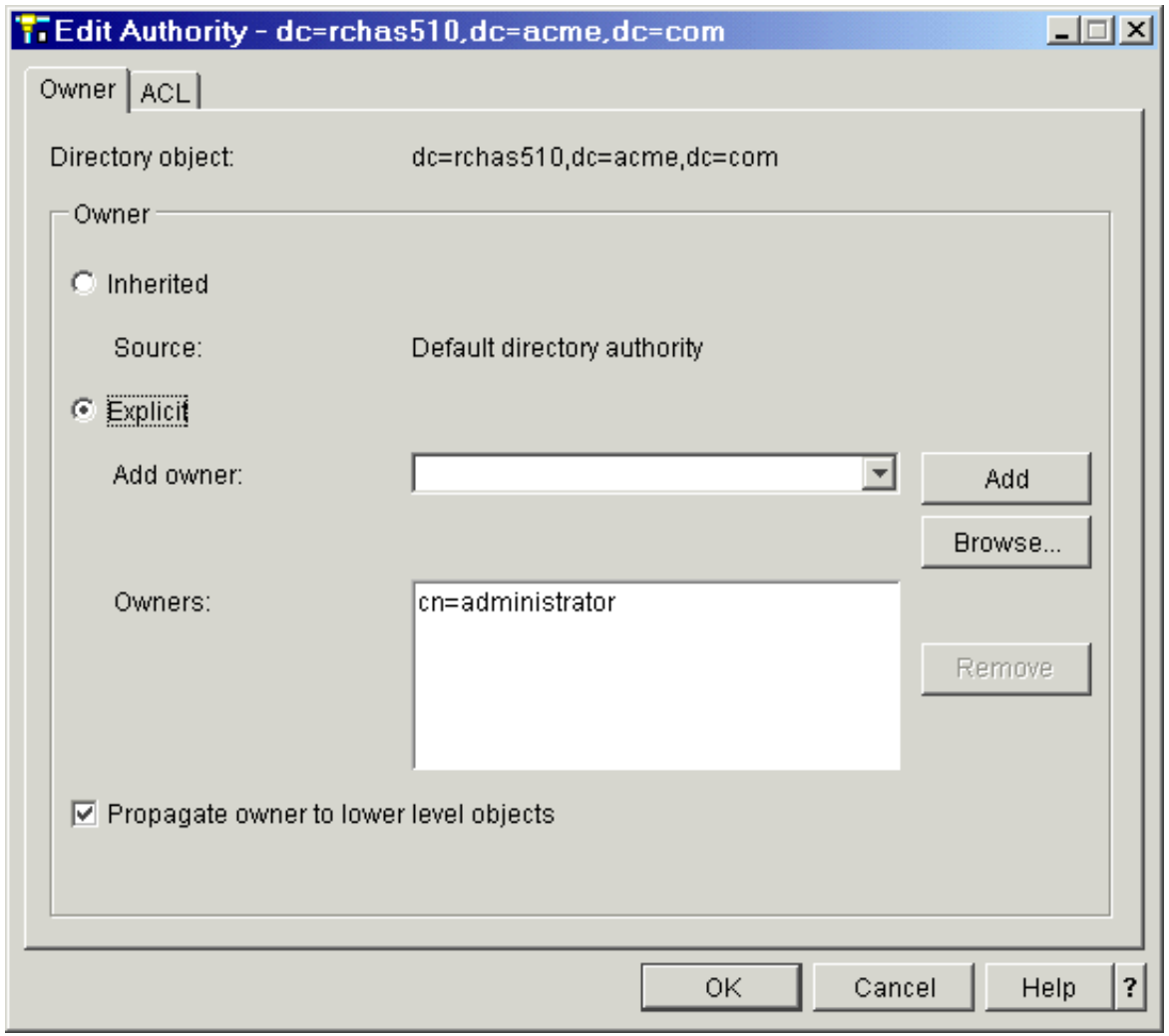
- You can manage access to directory data from Operations Navigator - or any LDAP application by modifying the proper attributes
- IBM specific - currently no standards define a LDAP access control model, but most vendors provide something
- Access defined in terms of:
  - subject: the authenticated identity of the client, determined at bind time
  - rights: the permissions granted to a subject or group
  - object: the entry being accessed
- IBM access control model defines owners and an access control list
  - Both can apply to a set of objects (a subtree) or a single entry

Managing access to the directory

- Special DNs that can be used
  - cn=anybody - all clients, including anonymous
  - cn=authenticated - everybody but anonymous
  - cn=this - client must be authenticated as the entry to which this applies
- Owner has complete access to the entry
  - Owner can be a group
  - Entries can inherit ownership

Managing access to the directory

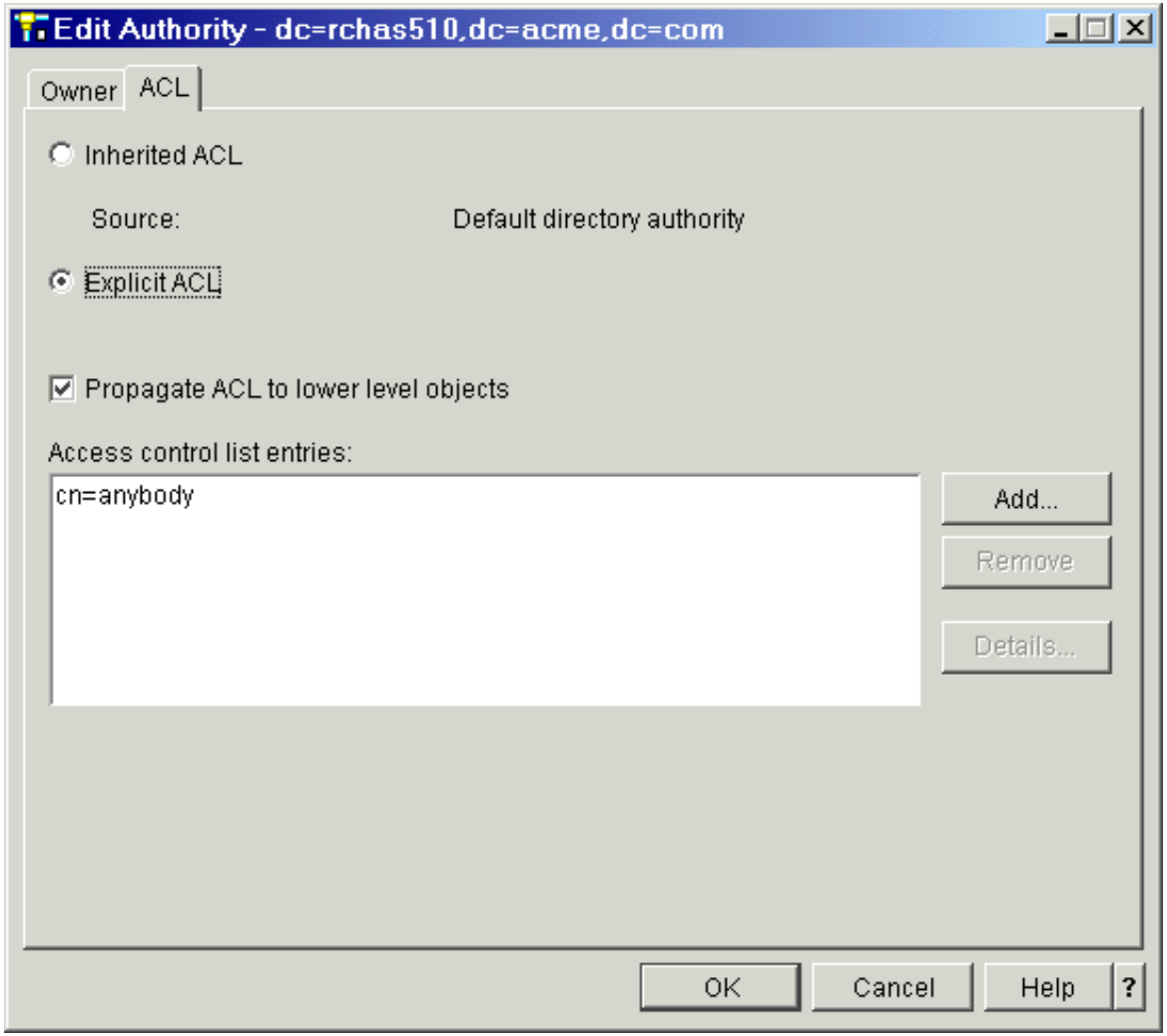
Entry Owner



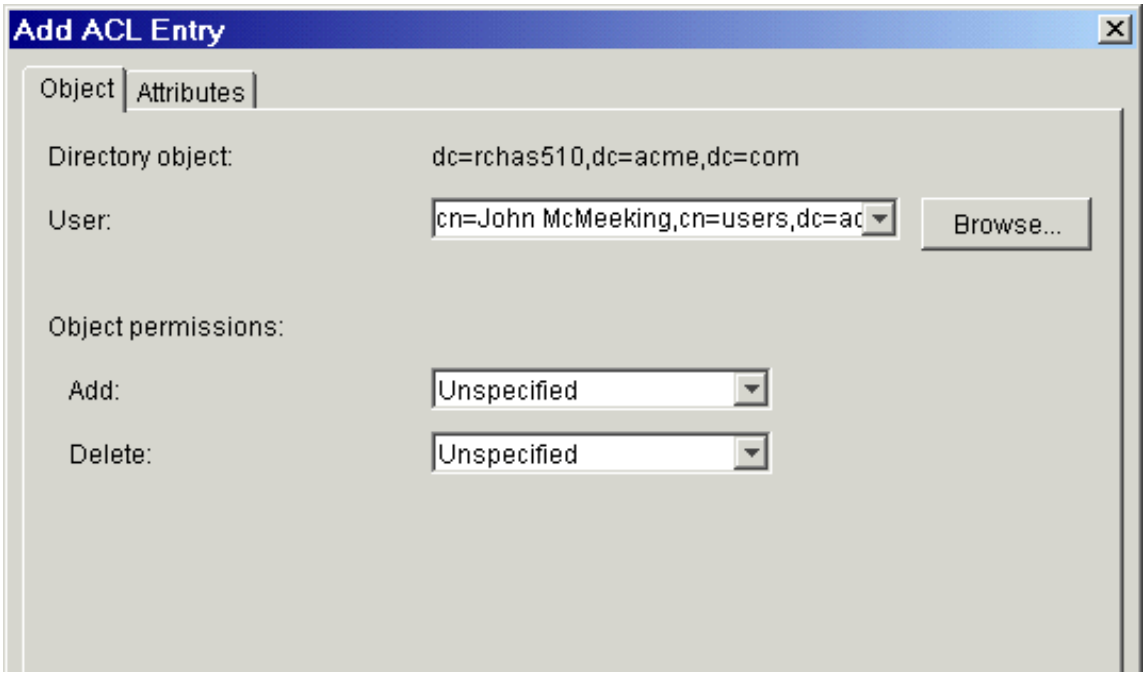
Managing access to the directory

- Access Control List grants permissions to others
  - attributes assigned to an "access-class"
    - NORMAL (cn, sn, telephoneNumber, ...)
    - SENSITIVE (homePhone, homeFax, ...)
    - CRITICAL (userPassword, userCertificate, ...)
  - grant write, read, search, compare permissions to attributes
  - grant add and delete permissions to objects that the ACL applies to
- V5R1 adds attribute level access control
  - grant or deny access to specific attributes

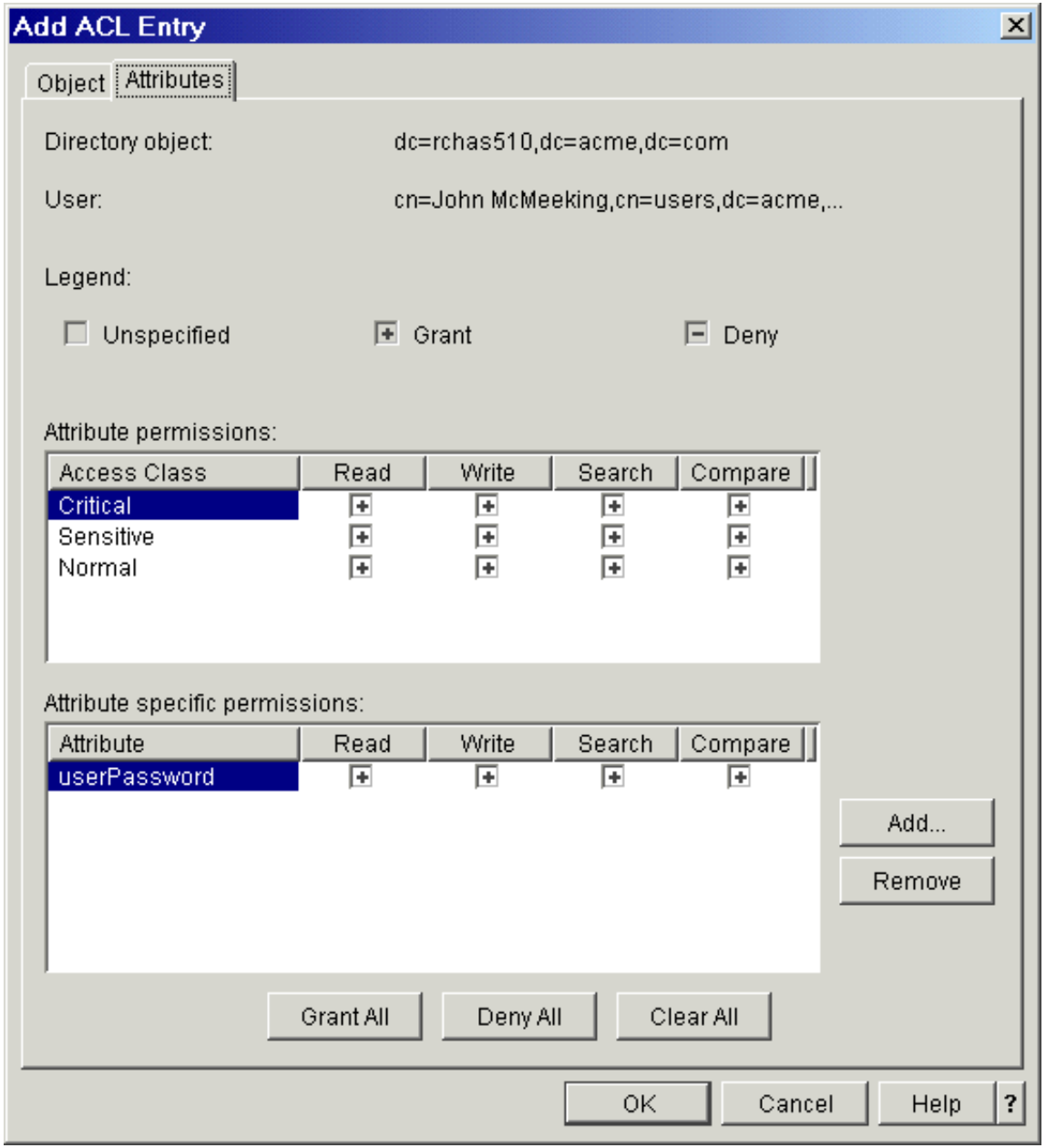
Managing access to the directory



Managing access to the directory



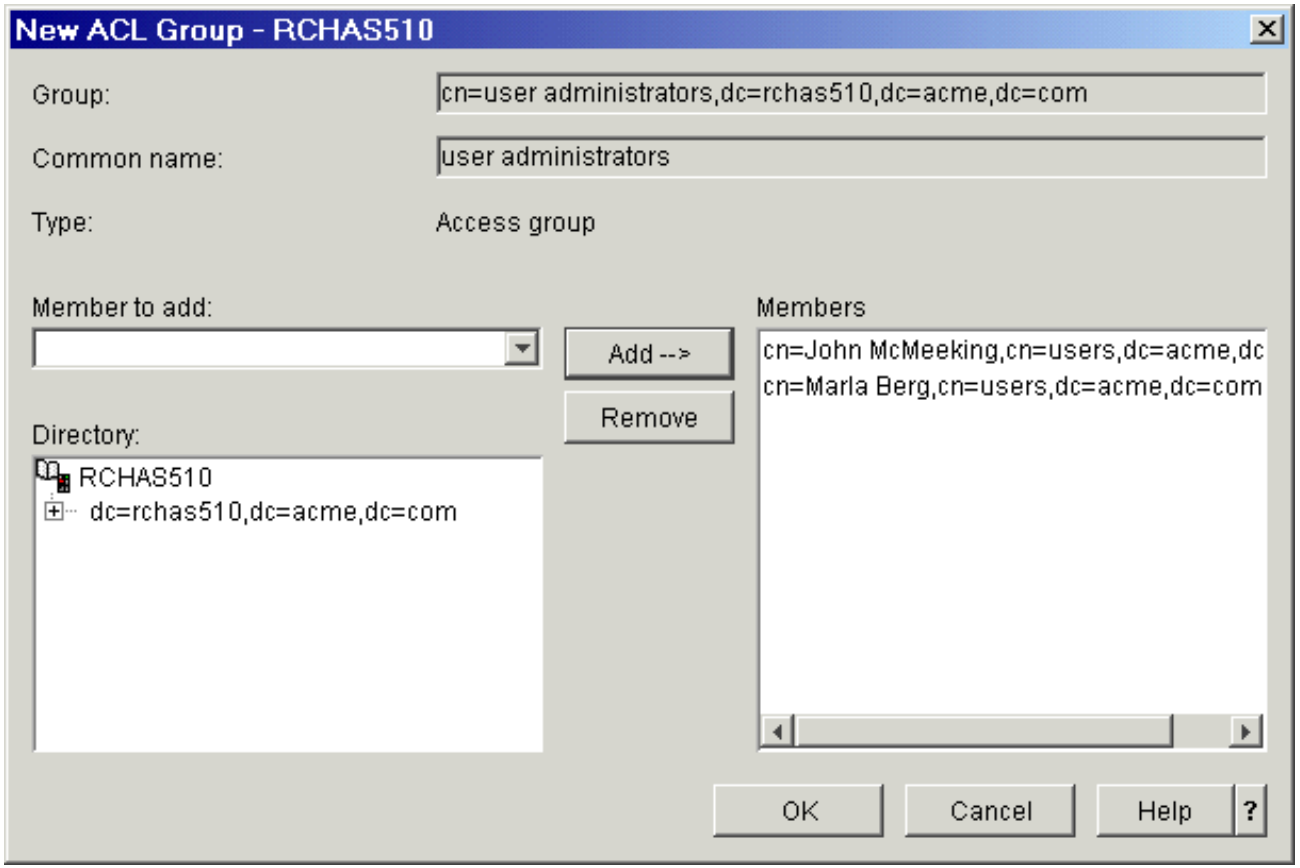
Managing access to the directory



Managing access to the directory

- Groups can be used as the "subject" for access control
  - Each of the "group" object classes defines membership via the "member" attribute
  - Member can be a LDAP entry or a pseudo-DN
    - Kerberos: ibm-kn=jmcmeek@acme.com
    - Digital Certificate: subject DN from certificate
  - Cannot nest groups for access control
- Initial release supported two "group" objectclasses that could be used in access control: accessgroup and accessrole.
- V5R1 also supports groupOfNames and groupOfUniqueNames
- You can manage groups via DMT, Operations Navigator (accessgroup and accessrole), or any LDAP client

Managing access to directory



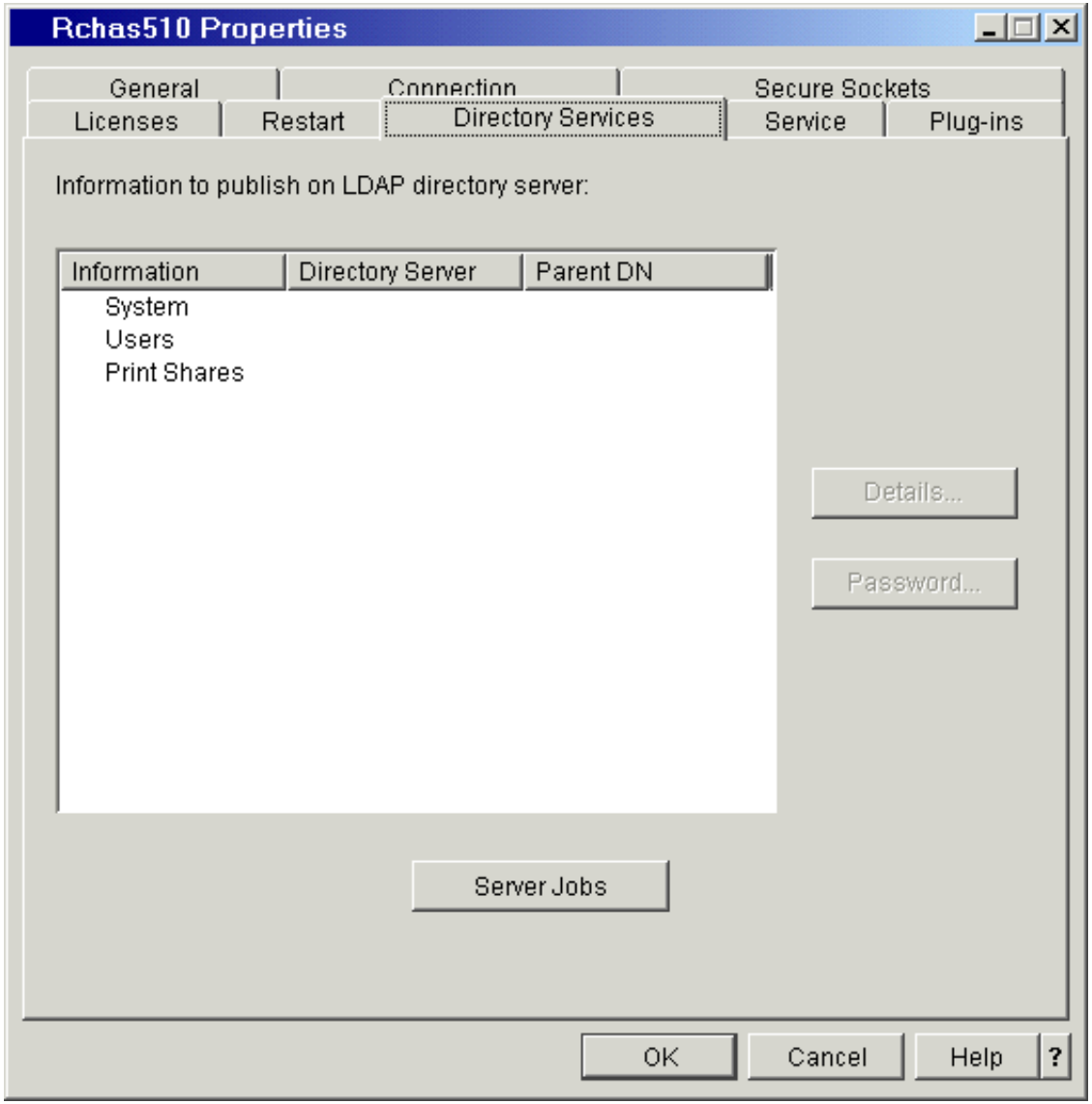
dn: cn=user administrators,dc=rchas510,dc=acme,dc=com
objectclass: accessgroup
objectclass: top
member: cn=John McMeeking,cn=users,dc=acme,dc=com
member: cn=Marla Berg,cn=users,dc=acme,dc=com
cn: user administrators

Configuring Publishing

Configuring Publishing

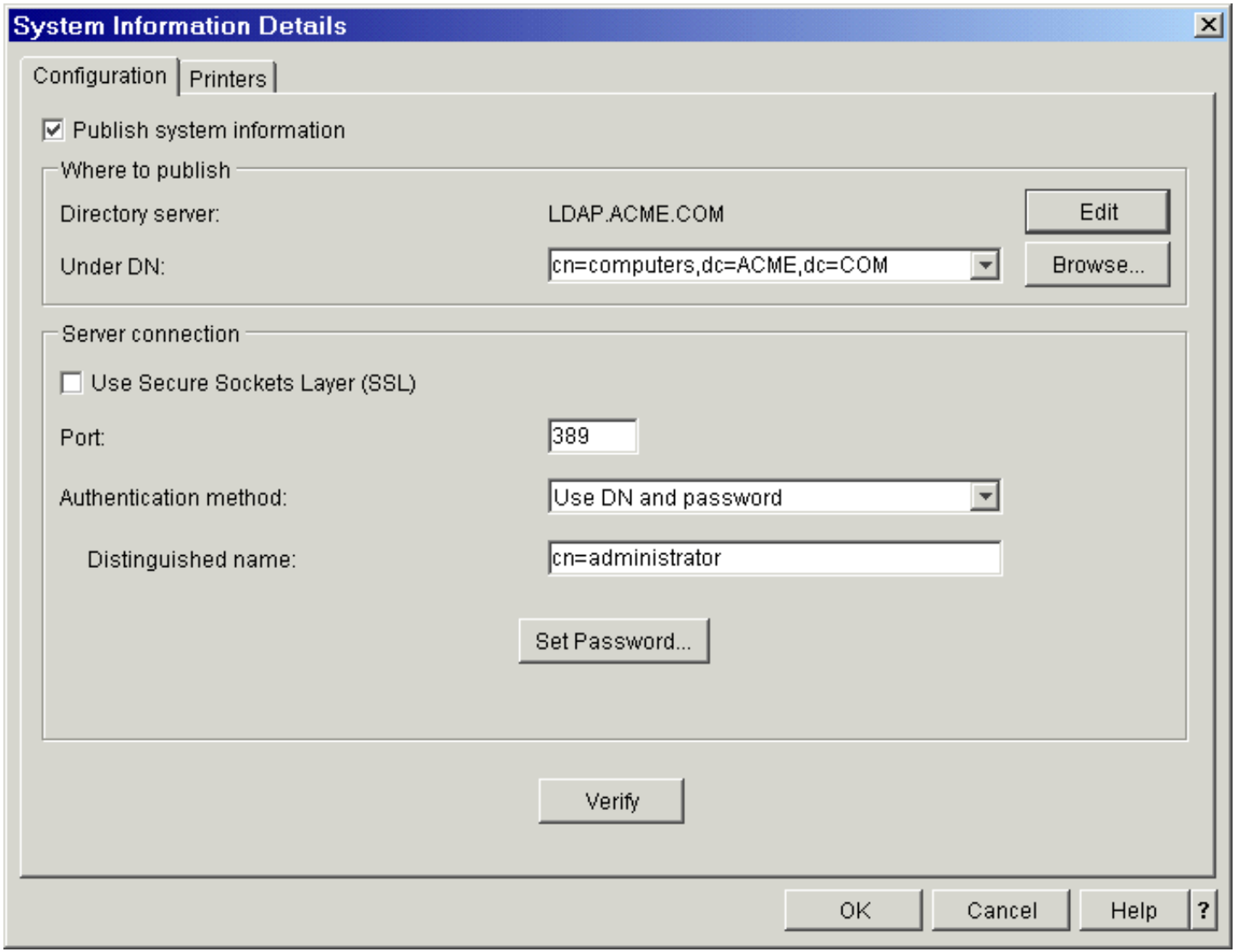
- Go to Properties for your system and select the Directory Services tab
  - Make sure you are connected first, or you cannot use this
- Manage configuration of publishing agents
  - System defined agents for users, system information, printer shares
  - Define your own agents via QgldChgDirSvrA API
- Users
  - SDD entries published to LDAP
- Computers
  - Basic system info published by OS/400
  - Management Central will publish detailed inventory (see Redbook "Management Central: A Smart Way to Manage AS/400 Systems" SG24-5407)
  - Can also publish information about OS/400 printers
- Printer Shares
  - Publish printer shares to Active Directory to use with Add Printer wizard

Configuring Publishing



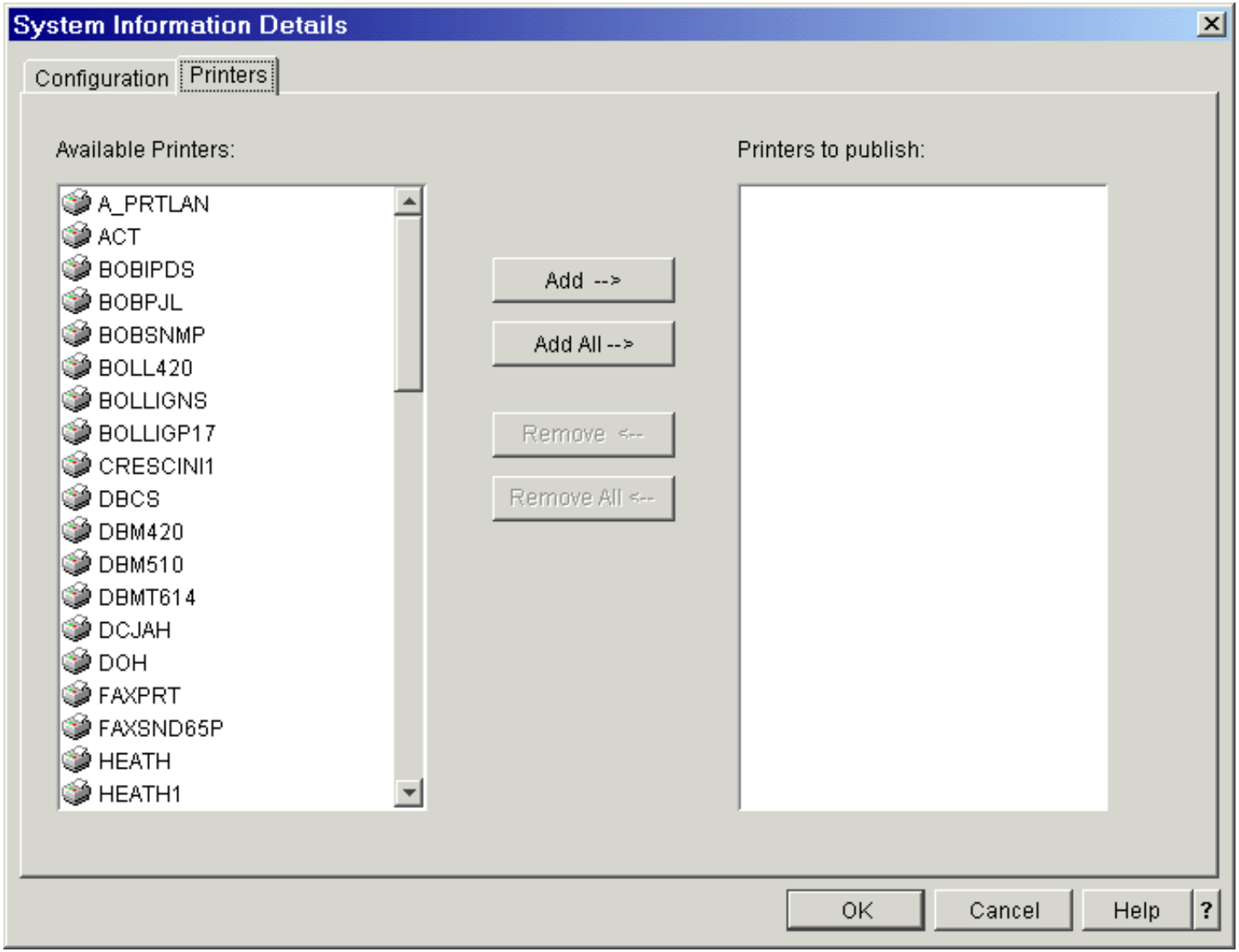
Configuring Publishing

- Example of the "System" information publishing configuration:



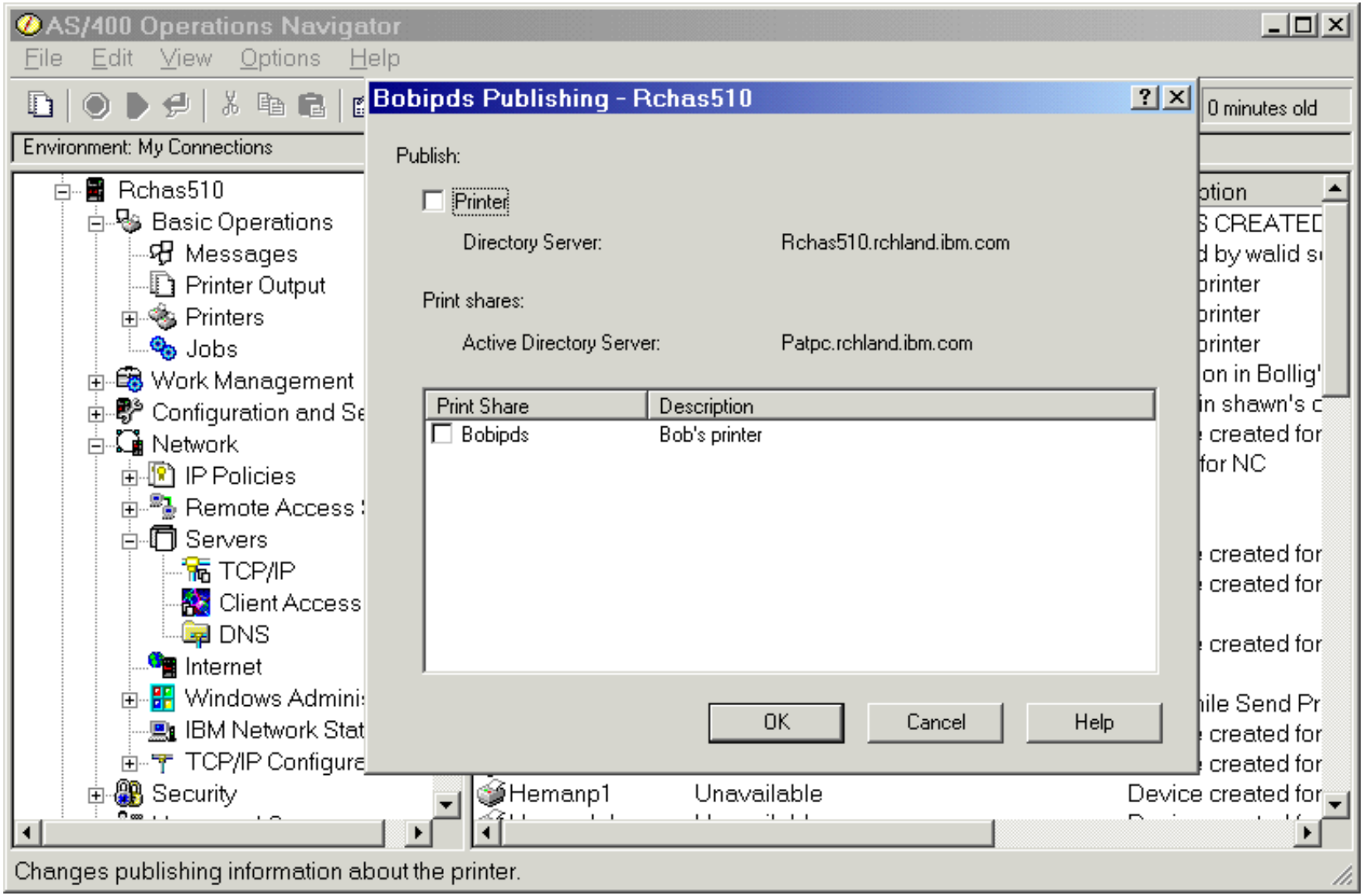
Configuring Publishingn

- Example of the "System" information publishing configuration:



Configuring Publishing

- Or you can select printers to publish from the Printers folder and AS/400 NetServer window



Configuring Publishing

- Sample published user:

```
C:\>ldapsearch -h lpar2nzm -b "cn=users,dc=lpar2nzm,dc=rchland,dc=ibm,dc=com"
   "(sn=mcmeeking)"
cn=John A McMeeking,cn=users,dc=lpar2nzm,dc=rchland,dc=ibm,dc=com
objectclass=top
objectclass=person
objectclass=organizationalPerson
objectclass=inetOrgPerson
objectclass=publisher
objectclass=ePerson
cn=John A McMeeking
cn=John McMeeking
cn=JAM
sn=McMeeking
uid=JAM
givenname=John
description=JAM
title=OS/400 Directory Services
departmentnumber=G8RA
telephonenumber=(507)253-4596
roomnumber=F115
registeredaddress=3605 Highway 52 N$Rochester, MN 55901
mail=jmcmeek@US.IBM.COM
publishername=dc=LPAR2NZM,dc=RCHLAND,dc=IBM,dc=COM
```

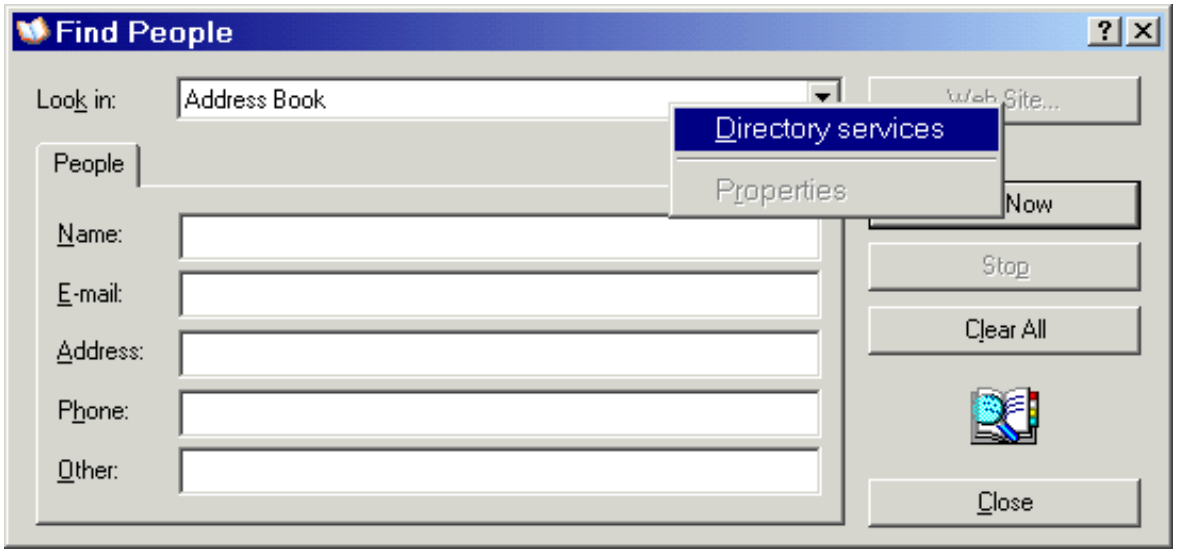
Tools for accessing the directory

Tools for accessing the directory

- Pointing your address book at an LDAP server
- IBM Directory Management Tool (DMT)
- Command line utilities
- Operations Navigator for management of access control
- Other tools
  - the Jarek Gawor LDAP Browser/Editor

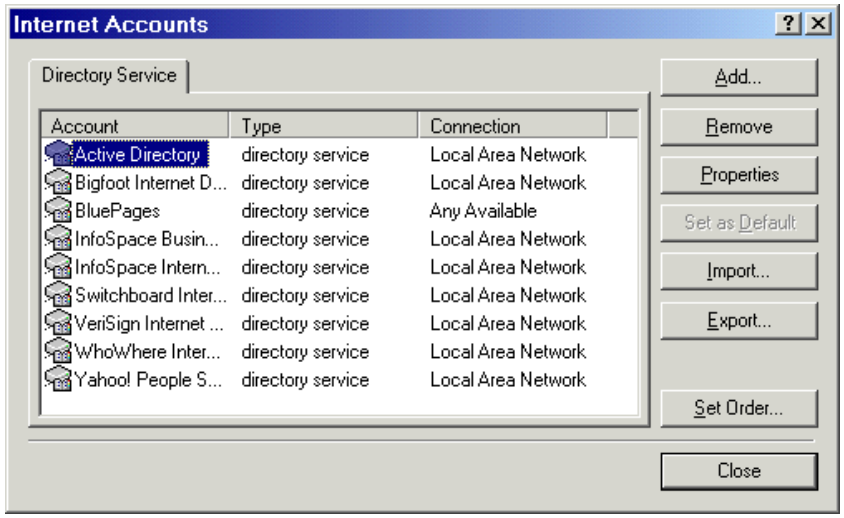
Pointing your address book at an LDAP server

- Accessing the LDAP server via Outlook Express (similar for other e-mail clients)
  - Launch 'Find People'
  - Right Click on "Look in:" to select "Directory services"



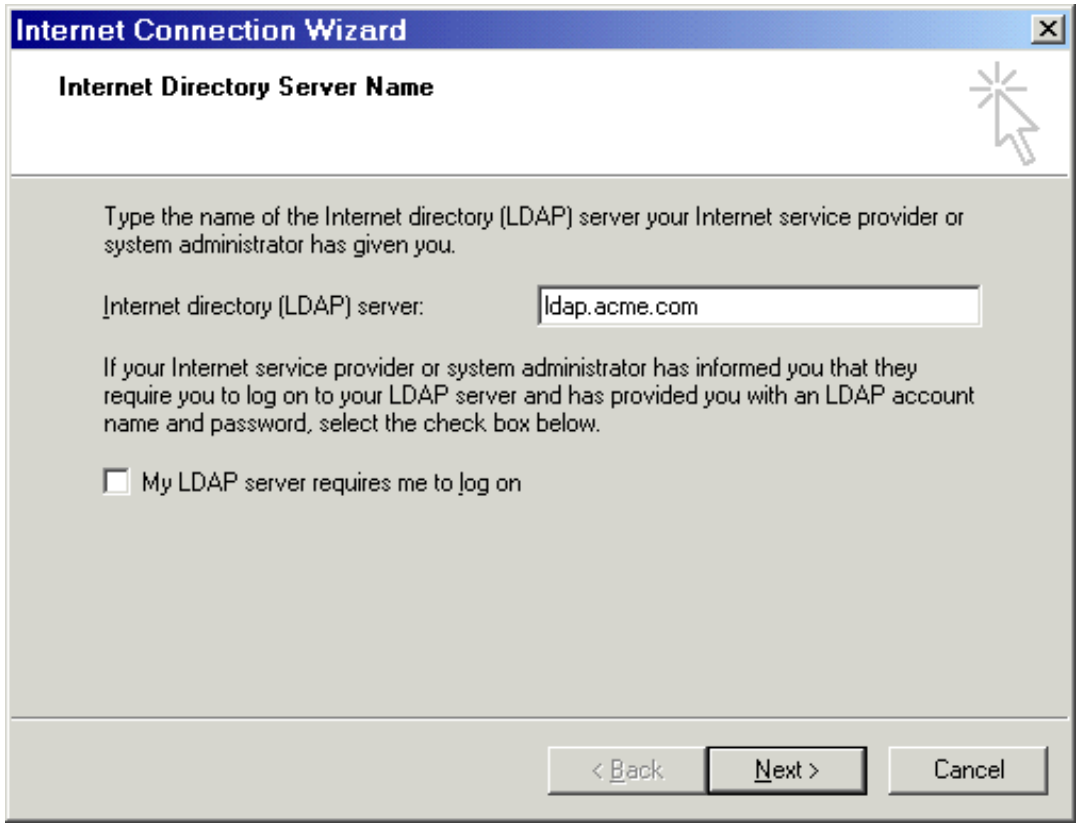
Address book setup

- Click "Add..." in Internet Accounts window



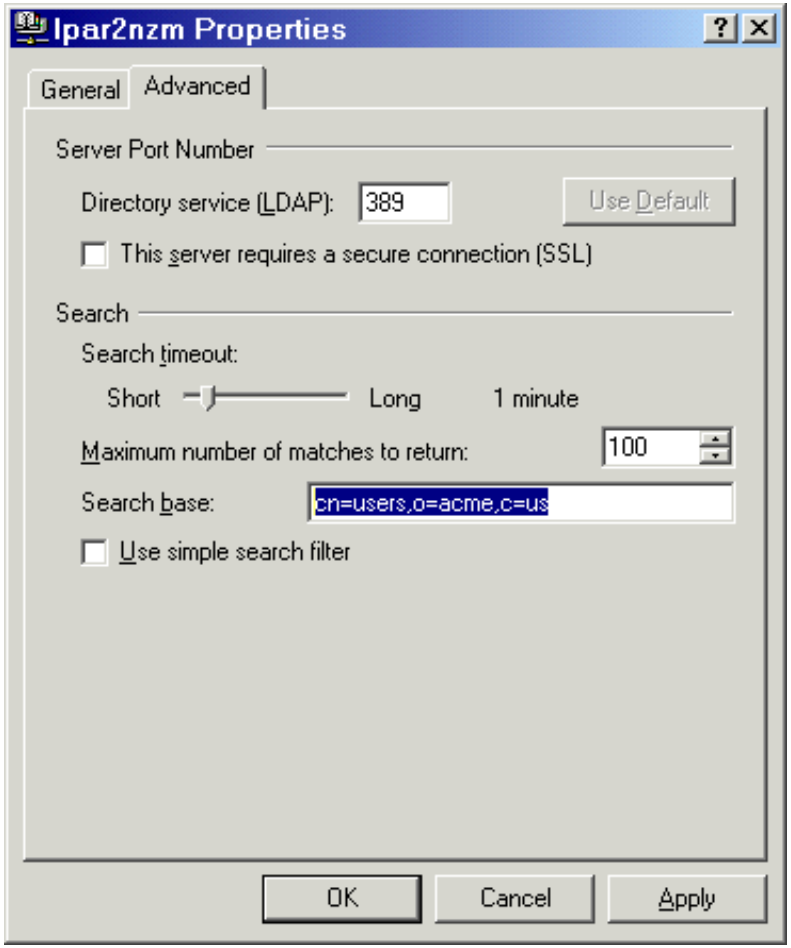
Address book setup

- Fill in Server name and continue to end of wizard



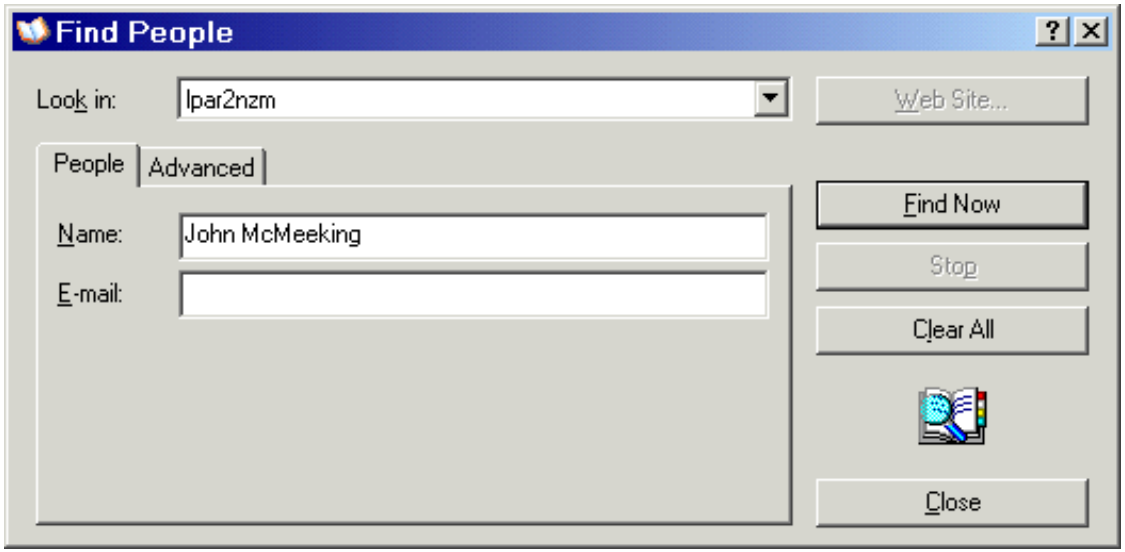
Address book setup

- After completing the wizard, select the server in the "Internet Accounts" window and click Properties. Go to advanced tab and fill in parent DN where users are published:



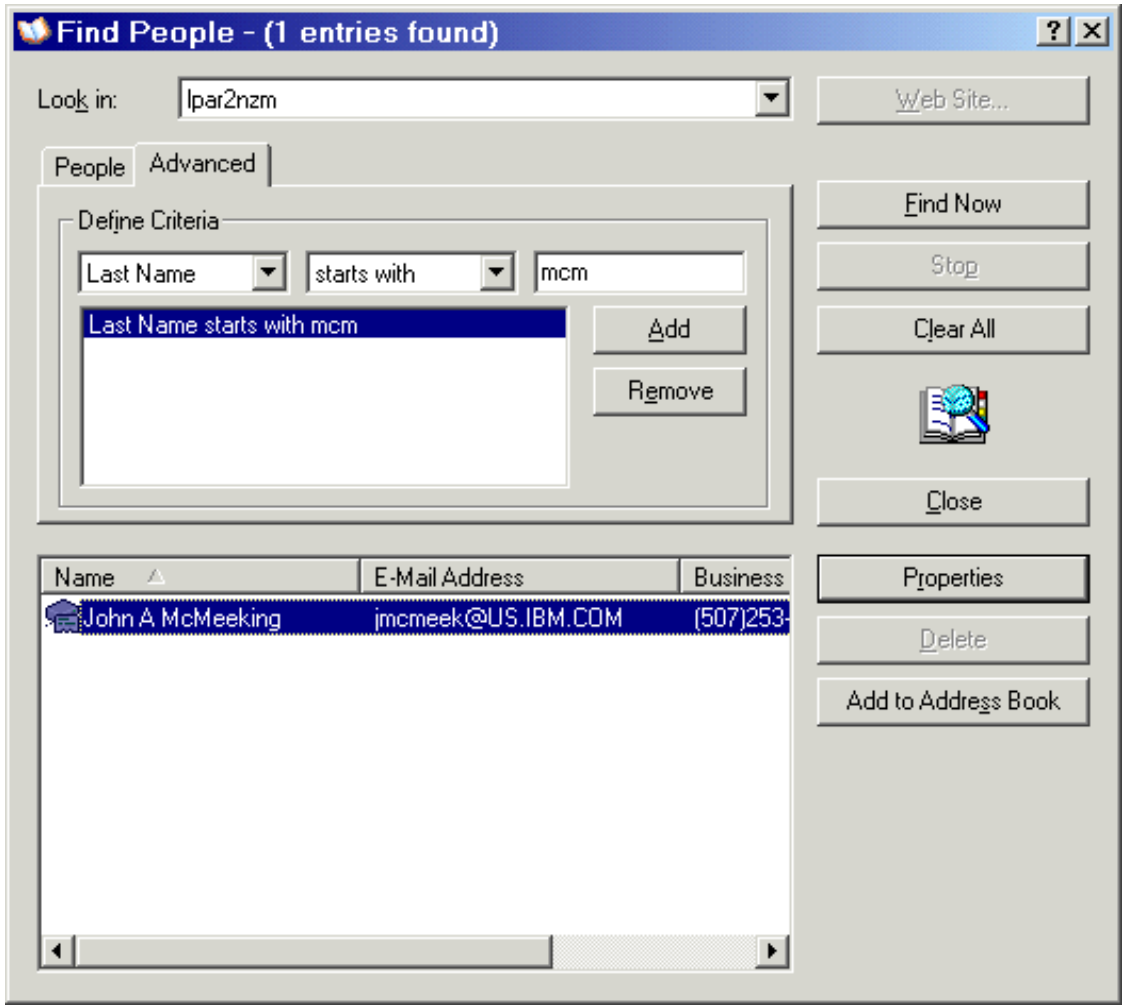
Address book setup

- Now look for someone in the directory:



Address book setup

- Or maybe try an advanced search:



Using DMT

IBM SecureWay Directory Management Tool

ldap://rchas510:389

- Introduction
- Server
  - Properties
  - Status
  - Administration
  - Rebind
- Schema
  - Refresh schema
  - Object classes
  - Attributes
  - Matching rules
  - Syntaxes
- Directory tree
  - Browse tree
  - Refresh tree
  - Search tree
    - Simple search
    - Advanced search
- Log file
  - View log file
  - Clear log file

Add server | Delete server | Exit

Introduction ?

Ready IBM

IBM SecureWay Directory Management Tool

IBM SecureWay Directory is a Lightweight Directory Access Protocol (LDAP) directory that runs as a stand-alone daemon. It uses a client/server model to provide LDAP clients access to the LDAP server.

This java client-based interface allows the administrator to maintain LDAP directories on multiple LDAP servers.

This interface supports the following functions:

- Displaying server properties and rebinding to the server
- Listing, adding, editing, and deleting schema attributes and object classes
- Listing, adding, editing, and deleting directory entries
- Modifying directory entry ACLs
- Searching the directory tree

At any time, you can select

? in the upper right corner to access help

Using DMT

- Install the IBM SecureWay Directory Client SDK
  - from your iSeries machine:
    /qibm/proddata/os400/dirsrv/usertools/windows/setup.exe
  - Or download from the IBM Directory web site:
    http://www.ibm.com/software/network/directory/downloads
- Default configuration of DMT attempts to connect to server running on "localhost" -- your PC

- Ignore this error and click "Add Server" on main window, OR...

Using DMT

- Or, edit C:\Program Files\IBM\LDAP\etc\dmt.conf, and uncomment/edit lines to look like:

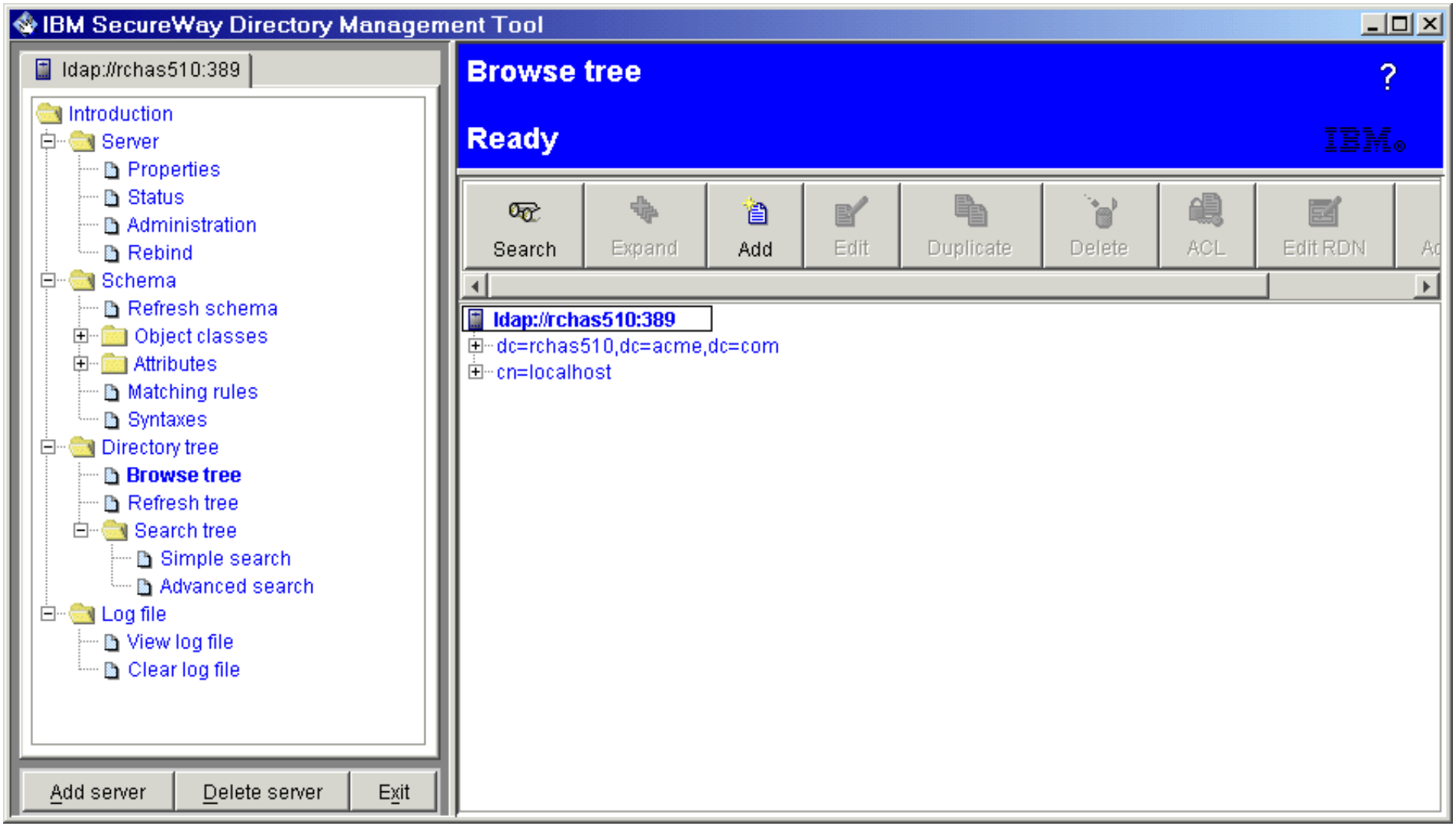
```
server1.url=ldap://rchas510.acme.com        << was localhost
server1.security.bindDN=cn=administrator    << was blank
server1.security.password=secret            << was blank
```

- Okay, I did that, but now I get:

- Your server has a suffix, but you haven't created any entries yet. Let's do that with DMT.

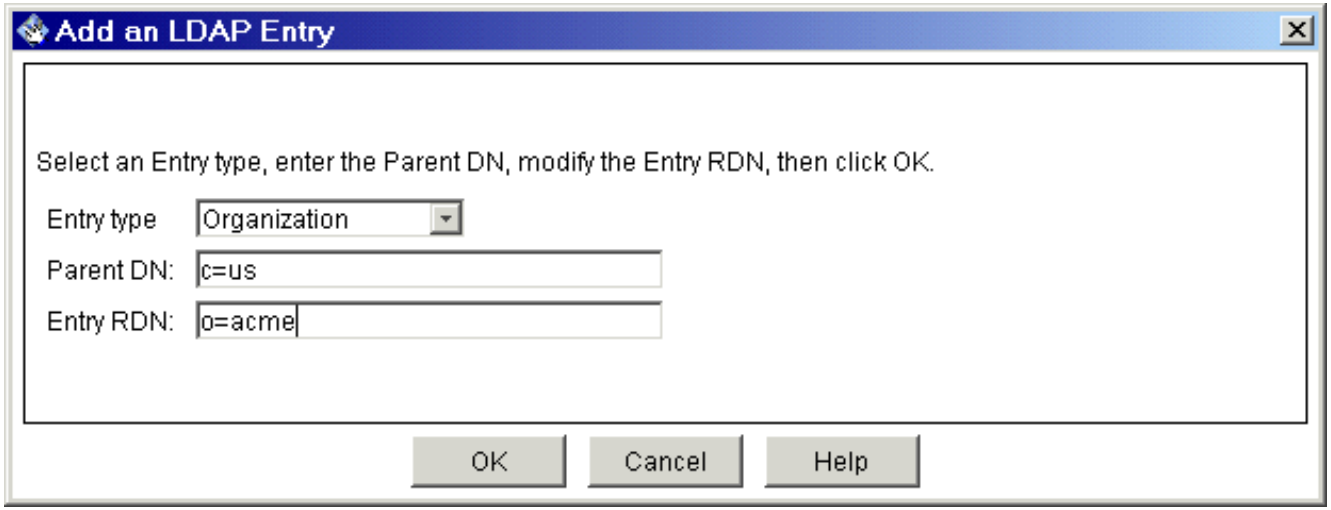
Using DMT - Create an entry

- Click "Browse tree", then the "Add" button



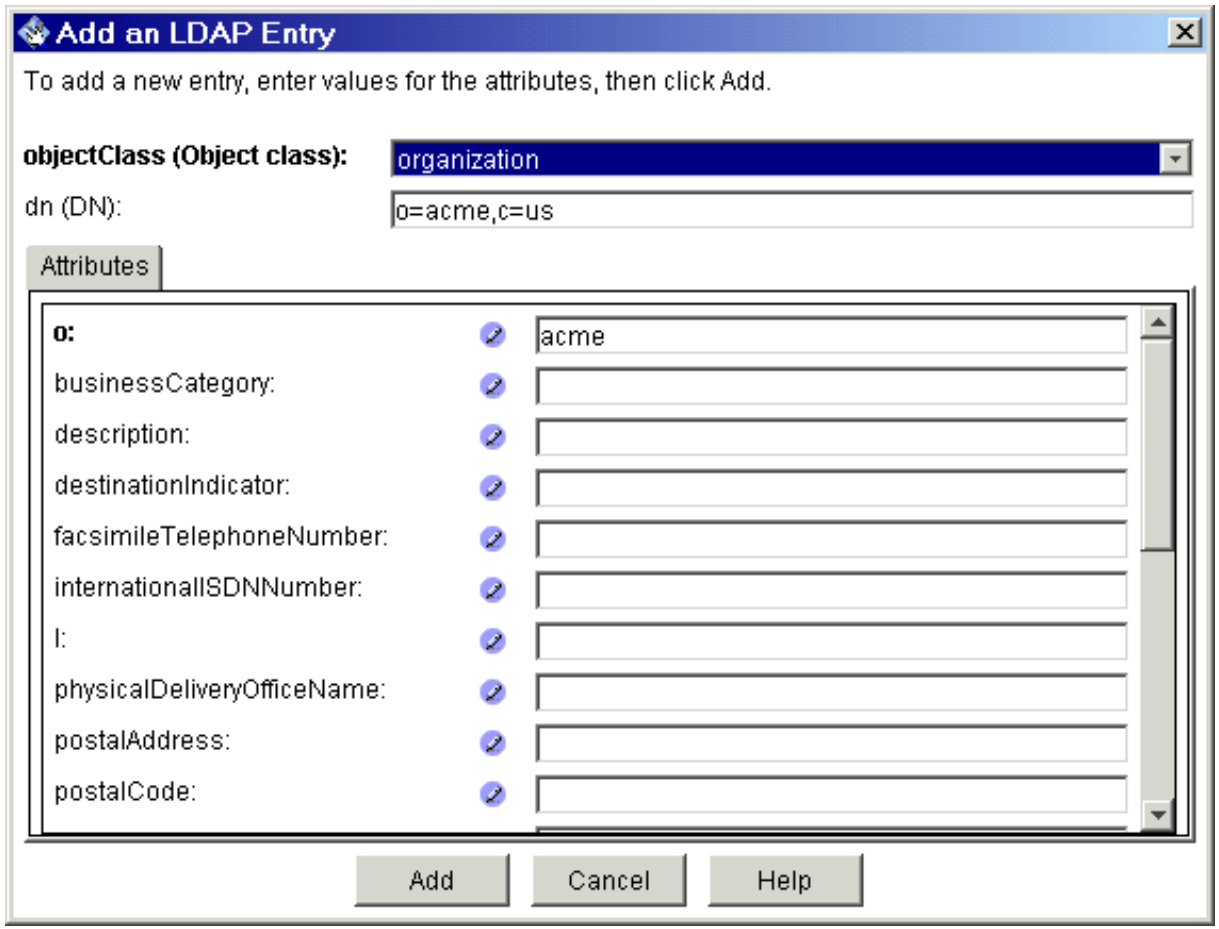
Using DMT - Create an entry

- Select the object class -- commonly used ones, like "organization", are listed in the dropdown, or chose "Other"
- Enter Parent DN (c=us) and entry DN (o=acme). Even though there is no c=us entry, DMT will combine these to get "o=acme,c=us"



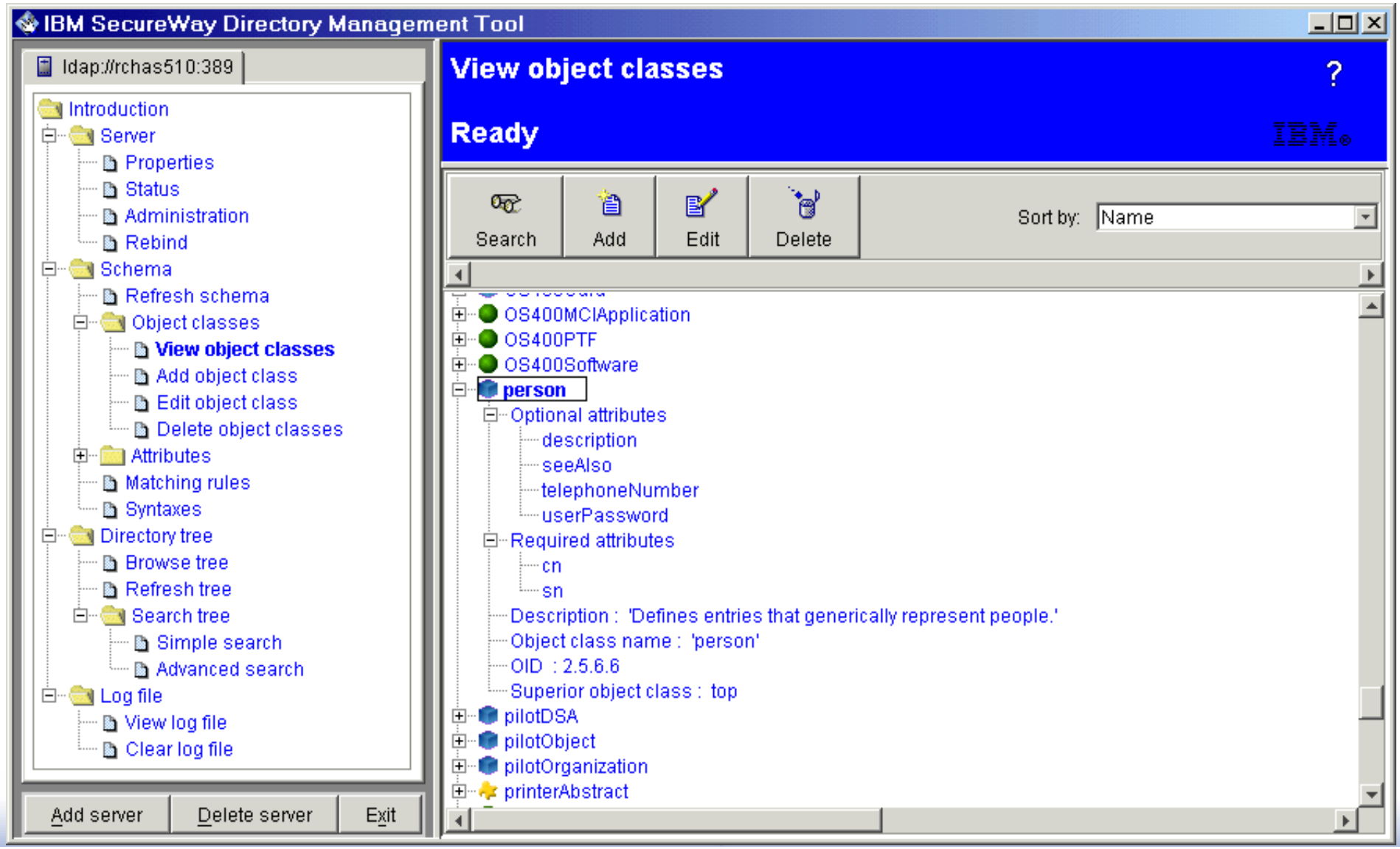
Using DMT - Create an entry

- Fill in any other information you might want to provide here, and click "Add"



Using DMT

- View or edit schema



QSHELL Utilities

- LDAP command line utilities can be invoked from QSH:
  - ldapadd, ldapmodify, ldapsearch, ldapdelete, ldapmodrdn
- Utilities accept input from standard input or from a file
- Search output can be redirected to a file
- Can be invoked from CL or a program

QSHELL Utilities

- ldapsearch examples

```
> ldapsearch -h rchas510 -D cn=administrator -w secret -b "DC=LPAR2NZM,DC=RCHLAND,DC=IBM,DC=C
    "(sn=mcmeek*)"
  cn=John A McMeeking,cn=users,dc=rchas510,dc=acme,dc=com
  objectclass=top
  objectclass=person
  objectclass=organizationalPerson
  objectclass=inetOrgPerson
  cn=John A McMeeking
  sn=McMeeking
  uid=JAM
  givenname=John
```

```
PGM
QSH         CMD('ldapsearch -h rchas510 -b "" -s base "(objectclass=*)" > rootdse.out')
ENDPGM
```

```
CALL QSYS/QGLDSEARCH PARM('-h' 'rchas510' '-b' '' '-s' 'base' '(objectclass=*)')
```

QSHELL Utilities

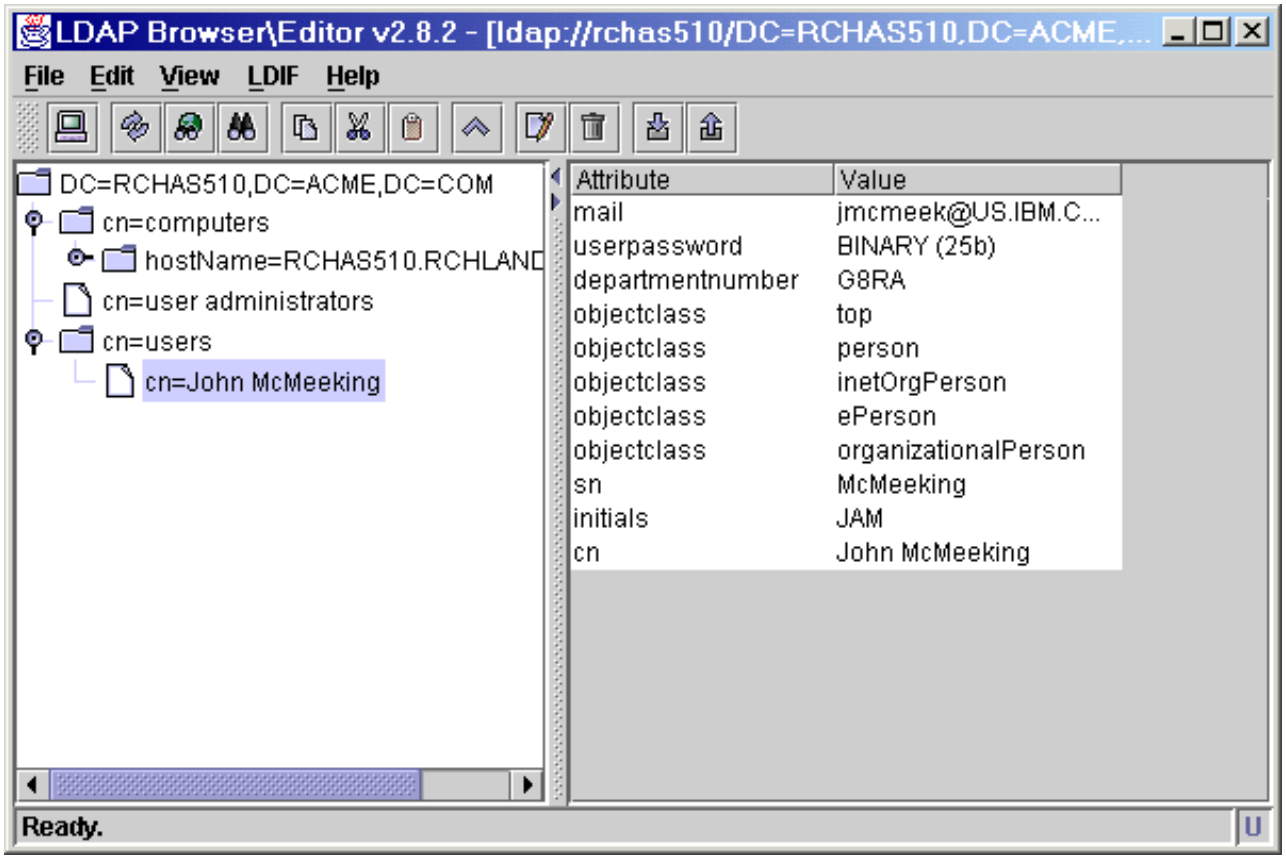
- ldapmodify examples
  - ldapmodify command can be used to add, modify, delete and rename entries via 'changetype' directive. See LDAP articles in Info Center for more information - particulary reference to RFC 2849

```
> ldapmodify -D cn=administrator -w secret -f mods.ldif

mods.ldif looks like:

dn: cn=john mcmeeking,cn=users,dc=acme,dc=com
changetype: modify
add: userpassword
userpassword: secret

dn: cn=mary jones,cn=users,dc=acme,dc=com
changetype: add
cn: mary jones
sn: jones
telephonenumber: 555.5555

dn: cn=paul smith,cn=users,dc=acme,dc=com
changetype: delete
```

Jarek Gawor's LDAP Browser/Editor

- LDAP edit/browser available from http://www.iit.edu/~gawojar/ldap/
  - Looks like it may now be licensed from Argonne National Laboratory. See http://www.techtransfer.anl.gov/software/ldapbrowser.html
- Features include:
  - Browsing, searching and editing of the DIT.
  - Entire trees and single entries can be exported to and imported from LDIF
  - Object templates are used for creating and adding new entries. The templates can be manually or automatically (from existing entries) created.
  - Attribute contents can be saved or loaded from a file.
  - Attribute viewers/editors

Jarek Gawor's LDAP Browser/Editor



References

For More Information

- iSeries LDAP home page at http://www.ibm.com/servers/eserver/iseries/ldap
- iSeries Information Center
  - Networking -> TCP/IP -> Directory Services (LDAP)
  - Programming -> CL and APIs -> APIs, look for Directory Services in APIs by category
- IBM Directory Server home page at http://www.ibm.com/software/network/directory/
- Redbooks (http://www.redbooks.ibm.com)
  - SG24-4986-00 Understanding LDAP
  - SG24-5110-00 LDAP Implementation Cookbook
  - SG24-6163-00 Using LDAP for Directory Integration: A Look at IBM SecureWay Directory, Active Directory, and Domino
  - SG24-6193-00 Implementation and Practical Use of LDAP on IBM eServer iSeries (draft Redbook available as a Redpiece)
- e-Directories Enterprise Software, Solutions, and Services by Daniel E. House, Timothy Hahn, Louis Mauget and Richard Daugherty. ISBN 0-201-70039-5. Published by Addison-Wesley Professional.

For More Information

- Programming:
  - The IBM SecureWay Directory Client SDK includes sample source code using the C APIs.
  - For Java programming using JNDI, refer to Sun's JNDI tutorial available at http://java.sun.com/products/jndi/docs.html, including the "Tips for LDAP Users" section

Trademarks and Disclaimers

8 IBM Corporation 1994-2002. All rights reserved.

References in this document to IBM products or services do not imply that IBM intends to make them available in every country.
The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both:

AS/400	IBM(logo)
AS/400e	iSeries
e (logo) business	OS/400
IBM	SecureWay

Lotus, Freelance Graphics, and Word Pro are registered trademarks of Lotus Development Corporation and/or IBM Corporation.
Domino is a trademark of Lotus Development Corporation and/or IBM Corporation.
C-bus is a trademark of Corollary, Inc. in the United States, other countries, or both.
Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.
Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.
ActionMedia, LANDesk, MMX, Pentium and ProShare are trademarks of Intel Corporation in the United States, other countries, or both.
UNIX is a registered trademark of The Open Group in the United States and other countries.
SET and the SET Logo are trademarks owned by SET Secure Electronic Transaction LLC.
Other company, product and service names may be trademarks or service marks of others.

Information is provided "AS IS" without warranty of any kind.

All customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer.

Information in this presentation concerning non-IBM products was obtained from a supplier of these products, published announcement material, or other publicly available sources and does not constitute an endorsement of such products by IBM. Sources for non-IBM list prices and performance numbers are taken from publicly available information, including vendor announcements and vendor worldwide homepages. IBM has not tested these products and cannot confirm the accuracy of performance, capability, or any other claims related to non-IBM products. Questions on the capability of non-IBM products should be addressed to the supplier of those products.

All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. Contact your local IBM office or IBM authorized reseller for the full text of the specific Statement of Direction.

Some information in this presentation addresses anticipated future capabilities. Such information is not intended as a definitive statement of a commitment to specific levels of performance, function or delivery schedules with respect to any future products. Such commitments are only made in IBM product announcements. The information is presented here to communicate IBM's current investment and development activities as a good faith effort to help with our customers' future planning.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements equivalent to the ratios stated here.

Photographs shown are of engineering prototypes. Changes may be incorporated in production models.