



IBM eServer™ iSeries™

Session: 420034

Configuring and Using the IBM Directory Server (LDAP)

Beth L. Hoffman

© Copyright IBM Corporation, 2003. 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.

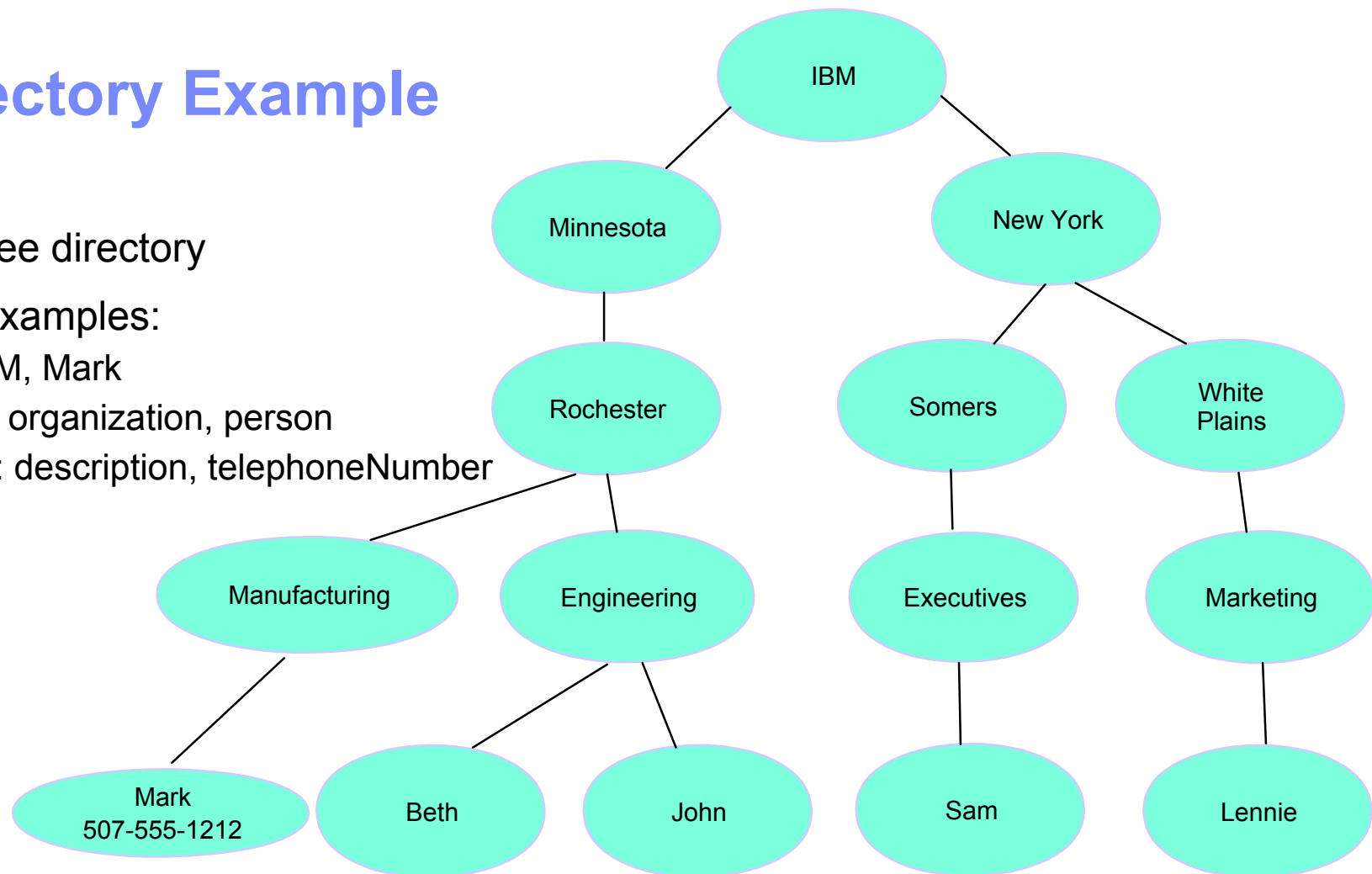
Agenda

- Concepts
 - ▶ Advanced directory concepts and terminology
 - ▶ Authentication
- Configuration
 - ▶ Configure the server the first time
 - ▶ Ongoing configuration
 - ▶ Manage the server
 - ▶ Control access
 - ▶ Configure publishing
- Client Tools
 - ▶ Accessing the directory
 - ▶ Managing schema
- References

Directory Concepts & Terminology

Basic Directory Example

- IBM employee directory
- Entry data examples:
 - ▶ Name: IBM, Mark
 - ▶ Structure: organization, person
 - ▶ Attributes: description, telephoneNumber



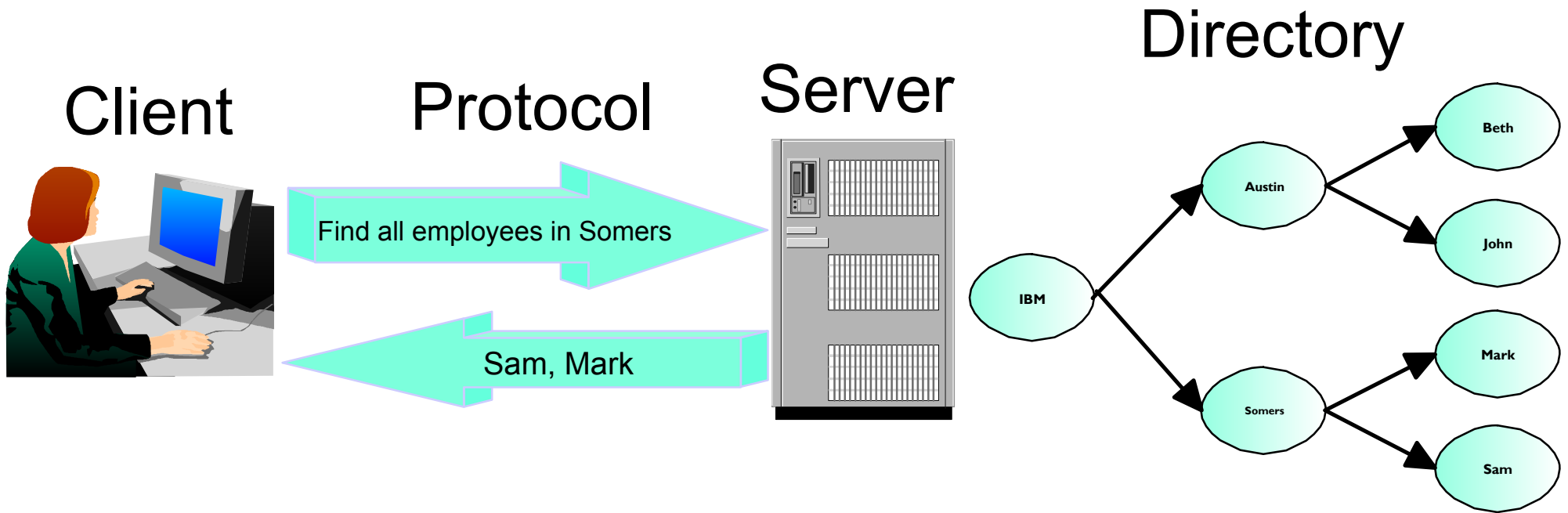
Concept: Directory Hierarchy

- Entries are arranged in a hierarchical structure that reflects political, geographic, or organizational boundaries.
 - ▶ Entries that represent countries appear at the top of the hierarchy. Entries representing states occupy the second level down in the hierarchy. The entries below that can then represent people, organizational units, printers, documents, or other items.
 - ▶ Example: `cn=beth,ou=marketing,o=ibm,c=us`
- You are not limited to the traditional hierarchy when structuring your directory. The domain component structure, for example, is gaining popularity. With this structure, entries are composed of the parts of TCP/IP domain names.
 - ▶ Example: `dc=ibm,dc=com`

LDAP Terminology: LDAP

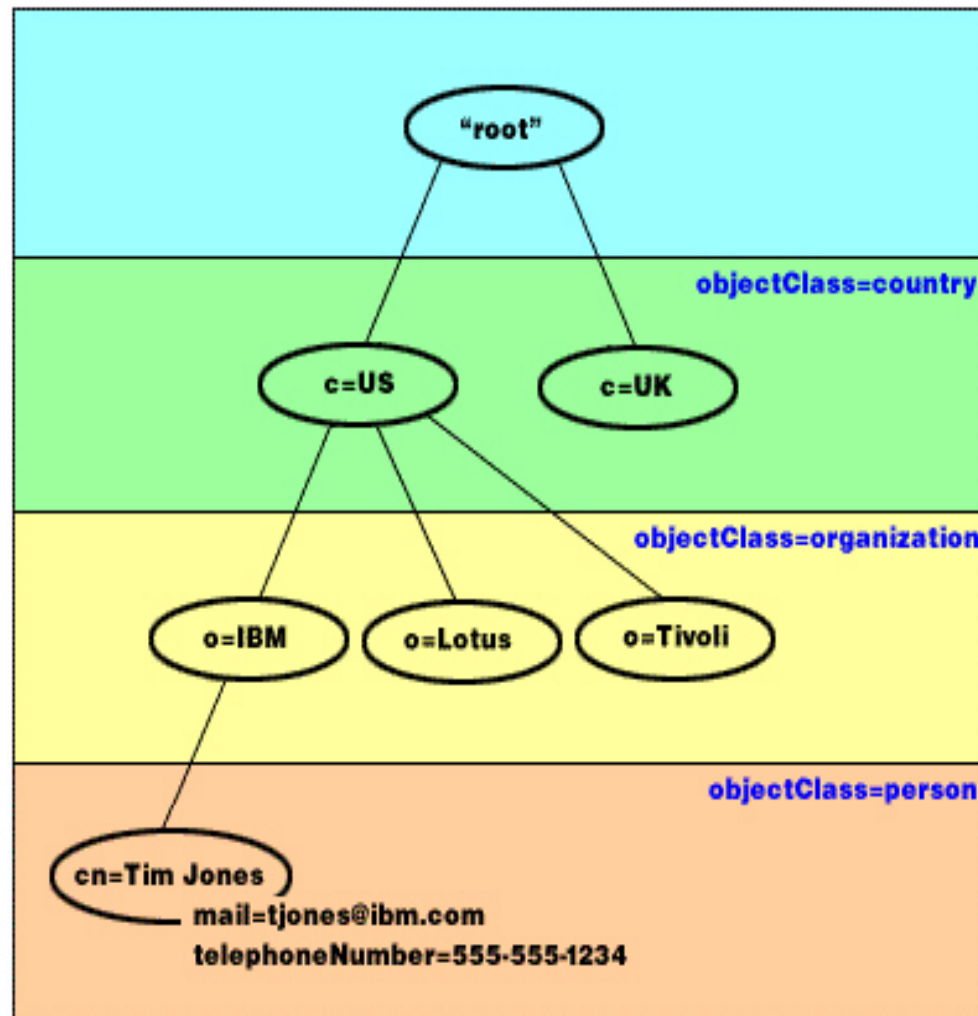
- Lightweight Directory Access Protocol
- A directory service protocol that runs over TCP/IP
- LDAP client, protocol, and server
- Protocol defines interfaces between a client and a server for requesting/returning data

LDAP Example



Terminology Picture

- Future LDAP terms will refer back to this example



LDAP Terminology: Entry

- The LDAP directory model is based on a hierarchy of entries.
 - ▶ The hierarchy is also referred to as a DIT (Directory Information Tree).
 - ▶ Entries are also referred to as objects.
- Each entry consists of one or more attributes such as a name and a type.
- Examples:
 - ▶ Each circle in the picture is an entry.
 - ▶ US is an entry of type country. US is the name of the entry.
 - ▶ Tim Jones is an entry of type person. Tim Jones is the name of the entry.

LDAP Terminology: ObjectClass

- Each entry has a special attribute called objectClass.
- An objectClass controls which attributes are required and allowed in an entry.
- The values of the objectClass attribute determine the schema rules the entry must obey.
- Example:
 - ▶ country, organization, and person are object classes
 - ▶ Other examples are organizational person which is a subtype of person.

LDAP Terminology: Attributes

- Each entry consists of one or more attributes.
- The type of data stored in attribute values can be:
 - ▶ DirectoryString, Binary (ex. JPEG photo), Integer, Boolean
- Each entry also has operational attributes (automatically maintained):
 - ▶ CreatorsName
 - ▶ CreateTimestamp
 - ▶ modifiersName
 - ▶ modifyTimestamp
- Example:
 - ▶ mail and telephoneNumber are attributes.
 - ▶ Some other possible attributes include fax, title, sn (for surname), and jpegPhoto.

LDAP Terminology: DNs

- LDAP refers to entries with Distinguished Names (DNs).
- Distinguished names consist of the name of the entry itself as well as the names, in order from bottom to top, of the objects above it in the directory.
- Each entry has at least one attribute that is used to name the entry. This naming attribute is called the Relative Distinguished Name (RDN) of the entry.
- The entry above a given RDN is called its parent Distinguished Name.
 - ▶ Examples:
 - the complete DN for the entry Tim Jones is cn=Tim Jones, o=IBM, c=US
 - the RDN of the entry is cn=Tim Jones
 - the parent DN for cn=Tim Jones is o=IBM, c=US

LDAP Terminology: Suffix

- A suffix defines a "namespace" that the LDAP server recognizes.
- Suffixes are the highest level distinguished names in the server configuration.
- The server can access all objects in the directory that are below the specified suffix in the directory hierarchy.
- An LDAP server can serve many suffixes or namespaces.
- The suffix "o=ibm,c=us" tells the server that DNs that end in "o=ibm,c=us" are in this server's namespace.
- DNs that do not fall within the defined suffixes are not handled by the server.
 - ▶ The server will return "no such object" or will redirect the client to another server that might handle that namespace (referral).
- Example:
 - ▶ The suffix o=ibm, c=us must be specified in the server configuration in order for the server to respond to client queries regarding Tim Jones.

LDAP Terminology: Schema

- Each directory has a schema.
- A schema is a set of rules that determine the structure and contents of the directory.
- Use IBM Directory Management Tool (DMT) to edit schema files.
- Default schema files are in /QIBM/ProdData/OS400/DirSrv. Copy to UserData to update.
- Schema includes:
 - ▶ objectclasses
 - ▶ attributetypes
 - ▶ ibmattributetypes
 - ▶ matchingrules

Example Schema

- objectclasses=(2.5.6.2 NAME 'country' DESC 'Defines entries that represent countries.' SUP top MUST c MAY (description \$ searchGuide))
- objectclasses=(2.5.6.4 NAME 'organization' DESC 'Defines entries that represent organizations. An organization is generally assumed to be a large, relatively static grouping within a larger corporation or enterprise.' SUP top MUST o MAY (businessCategory \$ description \$ destinationIndicator \$ facsimileTelephoneNumber \$ internationalSDNNumber \$ I \$ physicalDeliveryOfficeName \$ postalAddress \$ postalCode \$ postOfficeBox \$ preferredDeliveryMethod \$ registeredAddress \$ searchGuide \$ seeAlso \$ st \$ street \$ telephoneNumber \$ teletexTerminalIdentifier \$ telexNumber \$ userPassword \$ x121Address))
- objectclasses=(2.5.6.6 NAME 'person' DESC 'Defines entries that generically represent people.' SUP top MUST (cn \$ sn) MAY (description \$ jpegPhoto \$ seeAlso \$ telephoneNumber \$ title \$ userPassword))
- objectclasses=(2.5.6.7 NAME 'organizationalPerson' DESC 'Defines entries for people employed by or associated with an organization.' SUP person MAY (destinationIndicator \$ facsimileTelephoneNumber \$ internationalSDNNumber \$ I \$ ou \$ physicalDeliveryOfficeName \$ postalAddress \$ postalCode \$ postOfficeBox \$ preferredDeliveryMethod \$ registeredAddress \$ st \$ street \$ teletexTerminalIdentifier \$ telexNumber \$ title \$ x121Address))
- attributetypes=(2.5.4.20 NAME 'telephoneNumber' DESC 'Telephone number.' EQUALITY 2.5.13.20 SUBSTR 2.5.13.21 SYNTAX 1.3.6.1.4.1.1466.115.121.1.50)

Authentication

LDAP Authentication

- Each LDAP client must authenticate to the LDAP server.
- The process of authenticating is called a "bind" operation.
- If no bind is performed, the client is treated as "anonymous".
- There are 4 ways to provide a client identity.

Authentication Choices

1. Provide user name and password

- ▶ Also called a "simple bind"
- ▶ Example: Administrator - has access to all objects and attributes. The DN (cn=admin is the default on iSeries) and password are part of the server configuration.
- ▶ **A. DN with password**
 - Client's identity is a DN (an entry in the directory) which contains a userpassword attribute. Server verifies the password.
 - dn: cn=John Smith,cn=users,o=acme,c=us
objectclass: inetorgperson
userpassword: secret
- ▶ **B. DN with UID**
 - The entry has no userpassword attribute. The entry has a UID attribute which is the same as an OS/400 user profile. 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
- ▶ **C. Projected user and password**
 - DN is an OS/400 user profile. It does not map to a user entry in the directory.
 - All OS/400 user profiles are always available using LDAP.
 - The LDAP server verifies the user is an OS/400 user profile and the passwords match.
 - os400-profile=JSMITH,cn=accounts,os400-sys=SystemA.acme.com

Authentication Choices (cont.)

2. Provide a Kerberos ticket

- ▶ Uses SASL (Simple Security and Authentication Layer) bind
- ▶ 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

3. Provide Digital Client Certificate

- ▶ Another form of SASL bind
- ▶ Uses SSL/TLS
- ▶ The client identity is the DN from the certificate used to establish the connection.
- ▶ This is optionally a DN of an object in the directory.

Configuring the LDAP Server - the first time

iSeries Navigator: Directory

Environment: My Connections | Rchasyxm: TCP/IP | 3 minutes old

Server Name	Status	Description
DLFM	Stopped	Datalinks File Server
Virtual Private Networking	Stopped	Virtual private networking
ASFTomcat	Started	ASFTomcat server
Triggered Cache Manager	Stopped	Triggered cache manager
FTP	Started	FTP
LPD	Started	LPD
POP	Stopped	POP
Remote Execution	Stopped	Remote execution
SMTP	Started	SMTP
TELNET	Started	TELNET
HTTP Administration	Started	HTTP administration
Directory	Not configured	Directory

My Tasks

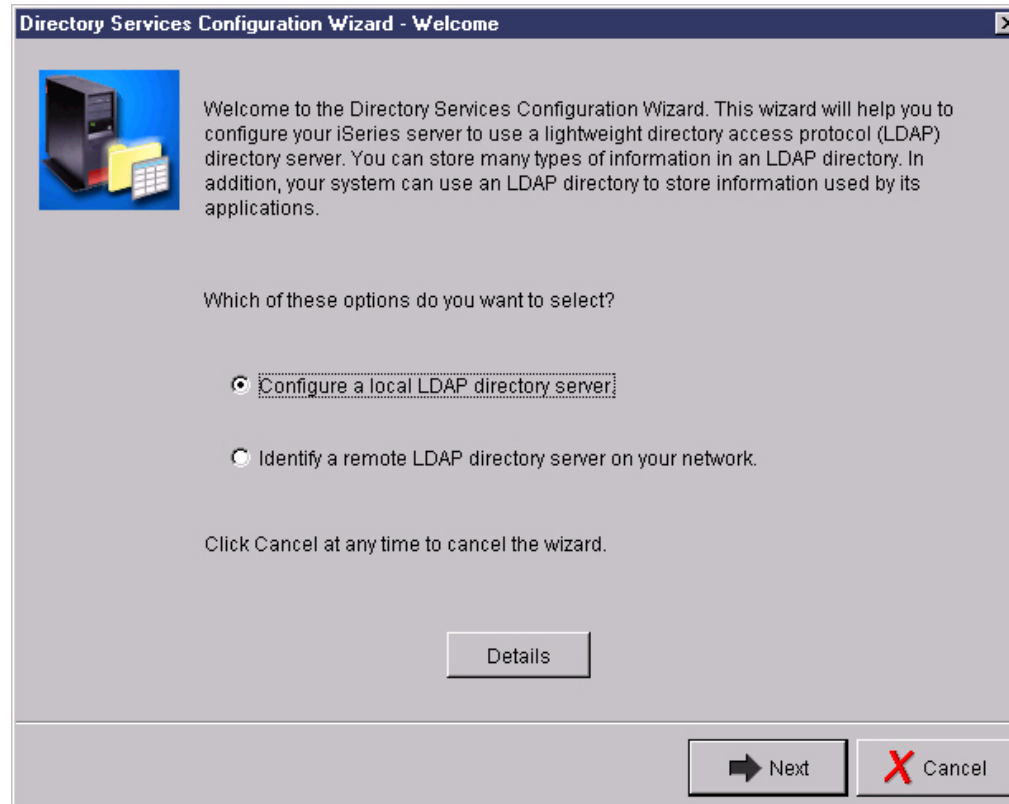
- Add a connection
- Install additional components

Server Configuration tasks

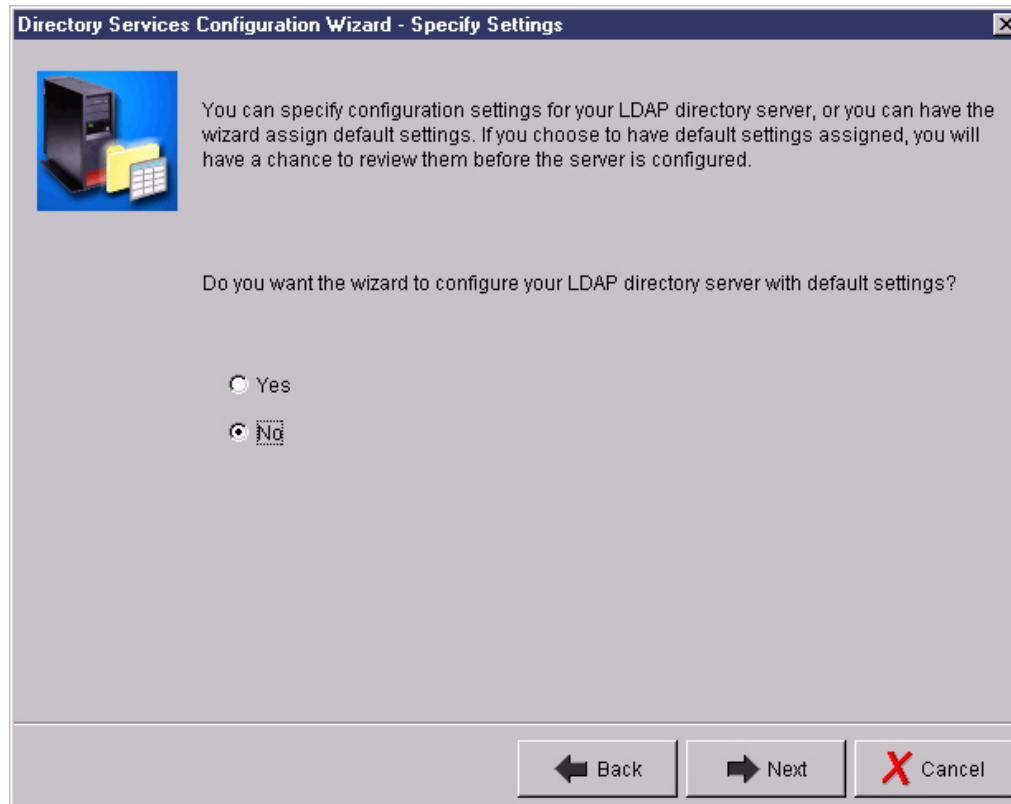
- Configure subsystems for server jobs
- Create a new DNS Name Server
- Configure system as DHCP server
- Configure system as Directory server
- Help for related tasks

18 - 29 of 29 objects

Configure local or remote




Use the defaults



Select the administrator name and password

Directory Services Configuration Wizard - Specify Administrator DN



The directory server administrator has unrestricted access to all directory entries on the server.

What do you want the distinguished name (DN) and password to be for the administrator of this directory?

Administrator Distinguished Name

System-generated

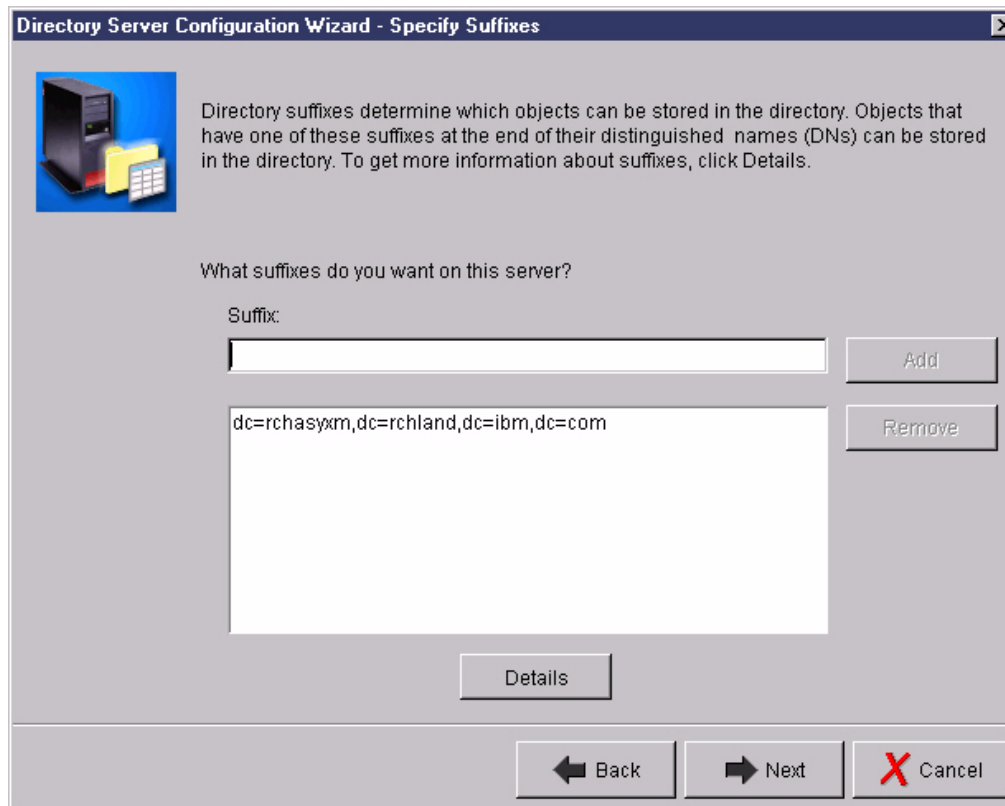
Select this option when you do not need to know the Administrator DN or password because only the system will use the directory.

Administrator DN:

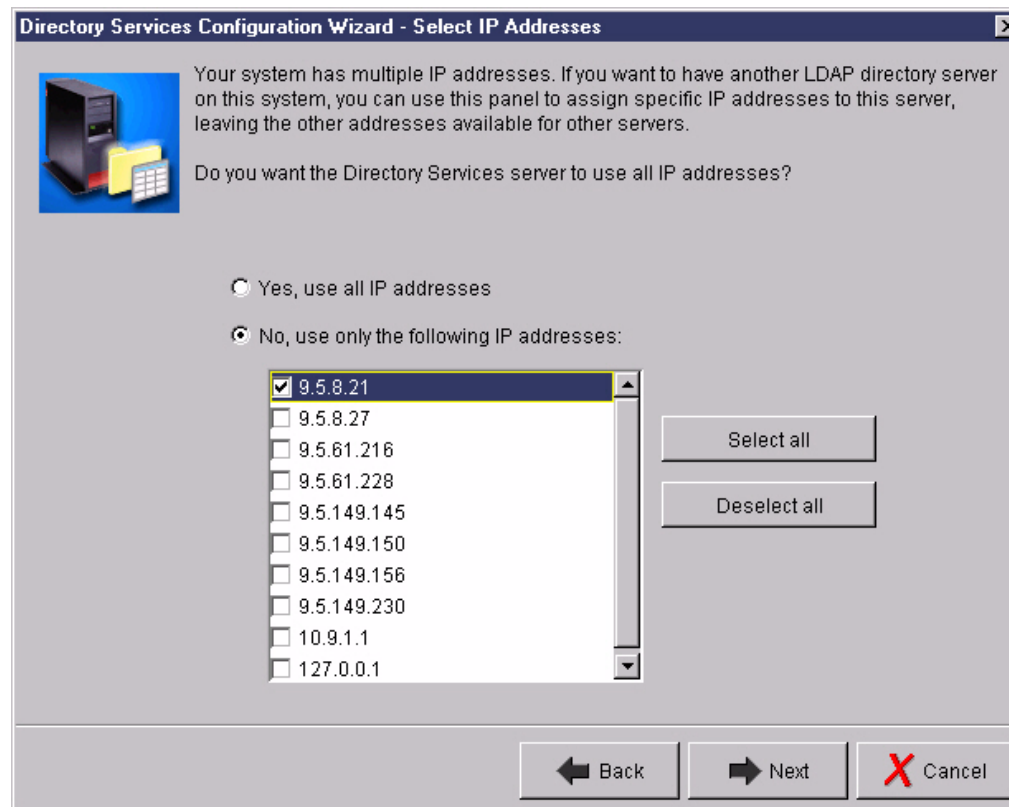
Password:

Confirm password:

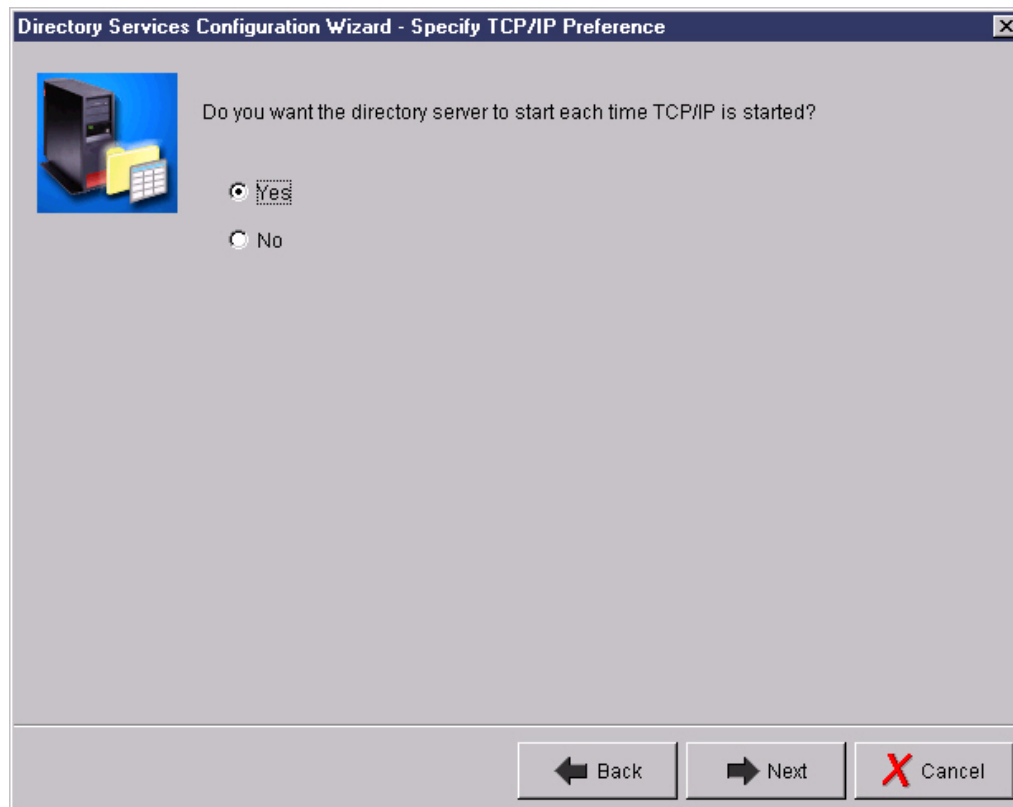
Add a suffix



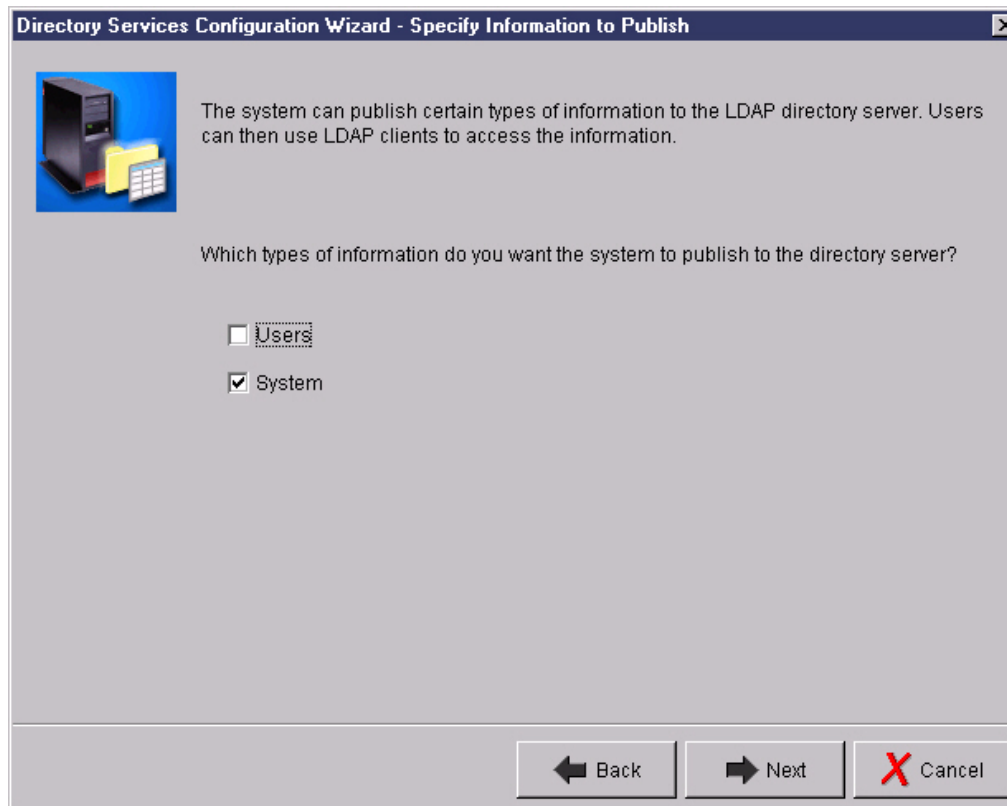
Select the IP addresses



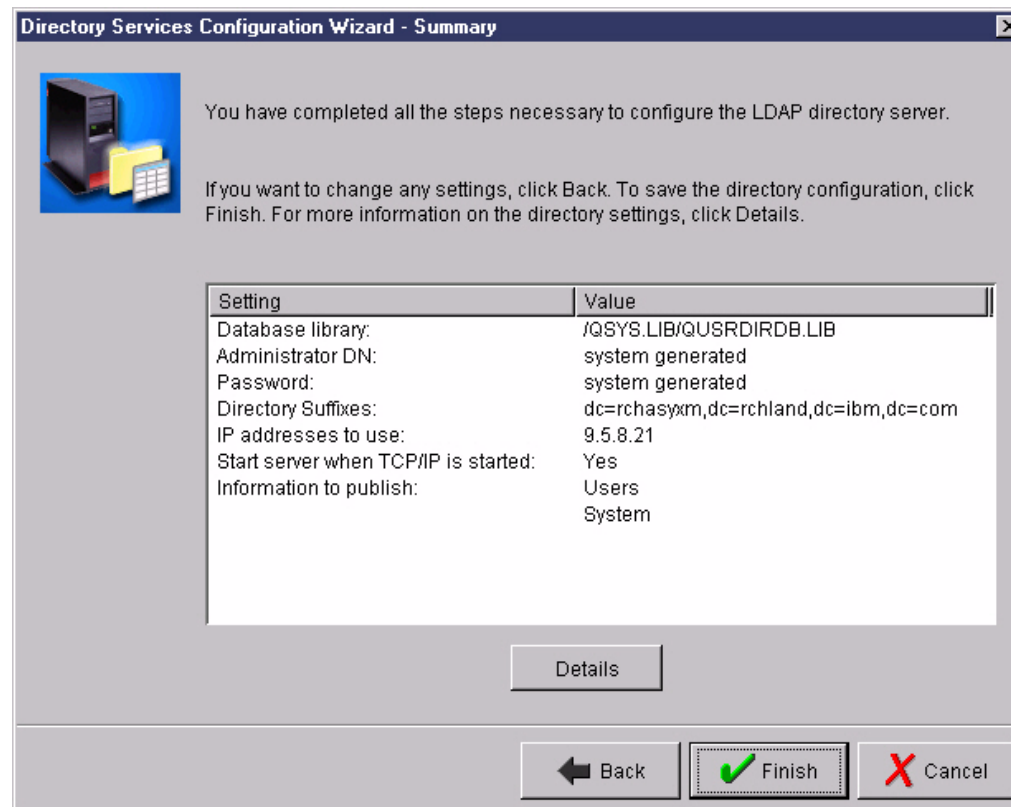
Autostart the server



Publish user and system information



Final summary



Final summary - Details

Directory Services Configuration Wizard - Summary

This panel summarizes the following configuration settings that you have chosen for your LDAP directory server:

Disk pool	The disk pool that contains the library that stores the LDAP directory's database files. This field is only displayed if your system has more than one disk pool.
Database library	The database library that contains your LDAP directory's information. This field is only displayed if you configure your LDAP directory with default settings.
Administrator DN	The distinguished name (DN) that has unrestricted access to the entire directory. If you selected System-generated , the administrator DN is not displayed, because only the server uses it.
Password	The password that is used by the Administrator DN.
Directory Suffixes	Lists the directory's suffixes, which determine which objects in the directory that this LDAP directory server can access.
Start server when TCP/IP is started	Indicates whether the LDAP directory server is automatically started each time that TCP/IP starts on your system.
Information to publish	Specifies the types of information that your system will automatically publish to the LDAP directory. Note: this field is not displayed if publishing was configured prior to running the wizard.
Publishing DN	The suffix that will be used as the starting point when OS/400 publishes information to the directory. Note: this field is not displayed if publishing was configured prior to running the wizard.

Note that unless have previously associated a digital certificate with the Directory Services server application, connections to your LDAP directory server are initially not secure. See the iSeries 400 Information Center for information on securing your LDAP server with secure sockets layer (SSL).

To save the directory configuration, click **Finish**. To change any settings, click **Back**.

Configuring the Server

After initial configuration

The screenshot shows the iSeries Navigator interface. The main window displays a table of server configurations for the 'Rchasyxm: TCP/IP' environment. The 'Directory' service is selected, and a context menu is open over it, showing options like Start, Stop, Server Jobs, Tools, Reconfigure, Authority, ACL Groups, Reconnect, Status, and Properties. The 'Tools' option is expanded, showing 'Import File' and 'Export File'.

Server Name	Status	Description
DLFM	Stopped	Datalinks File Server
Virtual Private Networking	Stopped	Virtual private networking
ASFTomcat	Started	ASFTomcat server
Triggered Cache Manager	Stopped	Triggered cache manager
FTP	Started	FTP
LPD	Started	LPD
POP	Stopped	POP
Remote Execution	Stopped	Remote execution
SMTP	Started	SMTP
TELNET	Started	TELNET
HTTP Administration	Started	HTTP administration
Directory	Stopped	Directory

Server Configuration tasks:

- Configure subsystems for server jobs
- Create a new DNS Name Server
- Configure system as DHCP server
- Configure system as Directory
- Help for related tasks

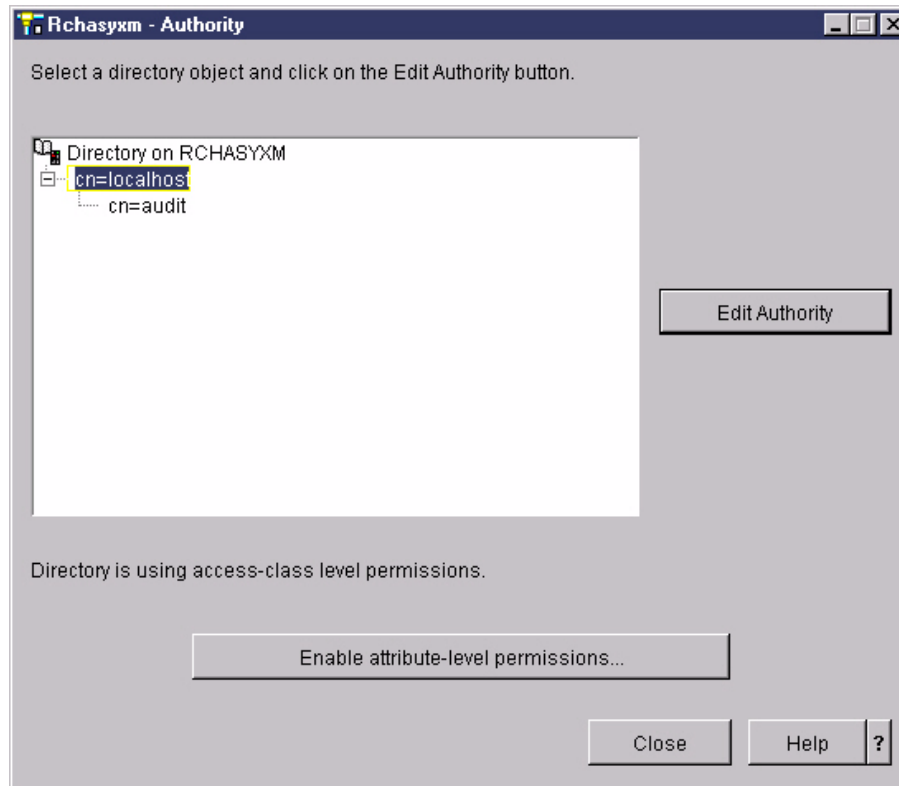
Context Menu:

- Start
- Stop
- Server Jobs
- Tools
 - Import File
 - Export File
- Reconfigure
- Authority
- ACL Groups
- Reconnect
- Status
- Properties

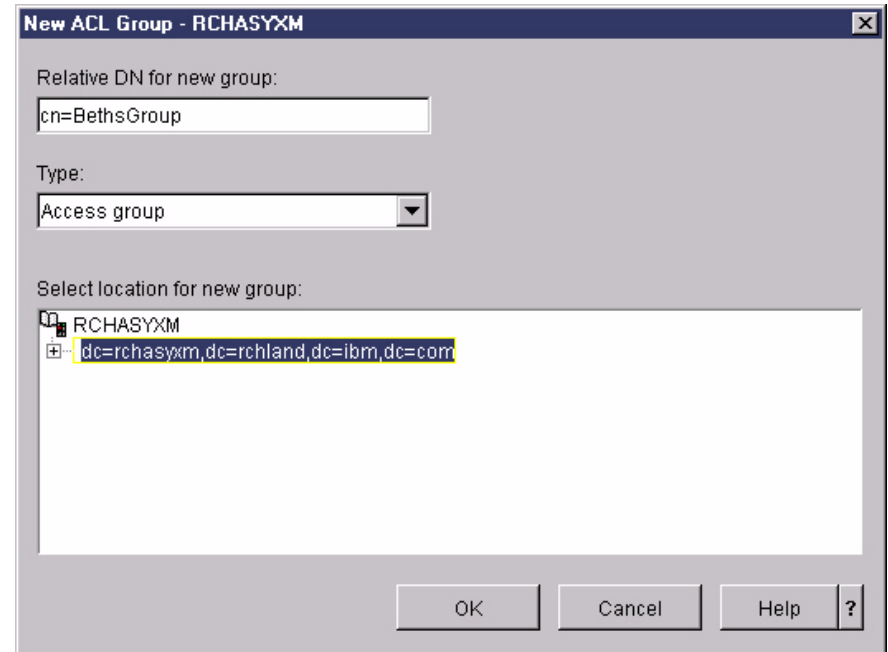
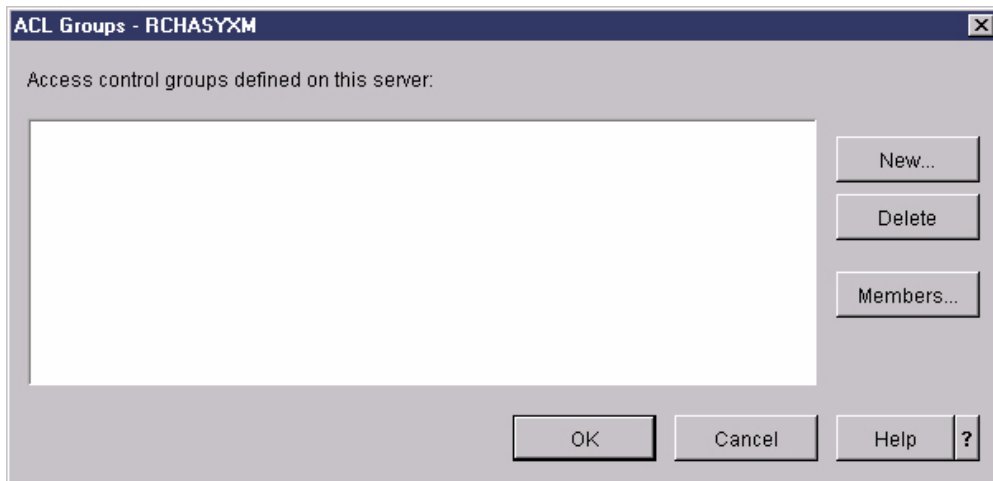
Configuring the Server

- **Reconfigure**
 - ▶ Use configuration wizard to replace current configuration.
- **Authority**
 - ▶ Controlling access to subtrees, data entries, and attributes.
- **ACL Groups**
 - ▶ Create/update groups and group membership.
- **Properties**
 - ▶ Changing the LDAP administrator password.
 - ▶ Creating new suffixes.
 - ▶ Selecting the ports.

Authority



ACL Groups



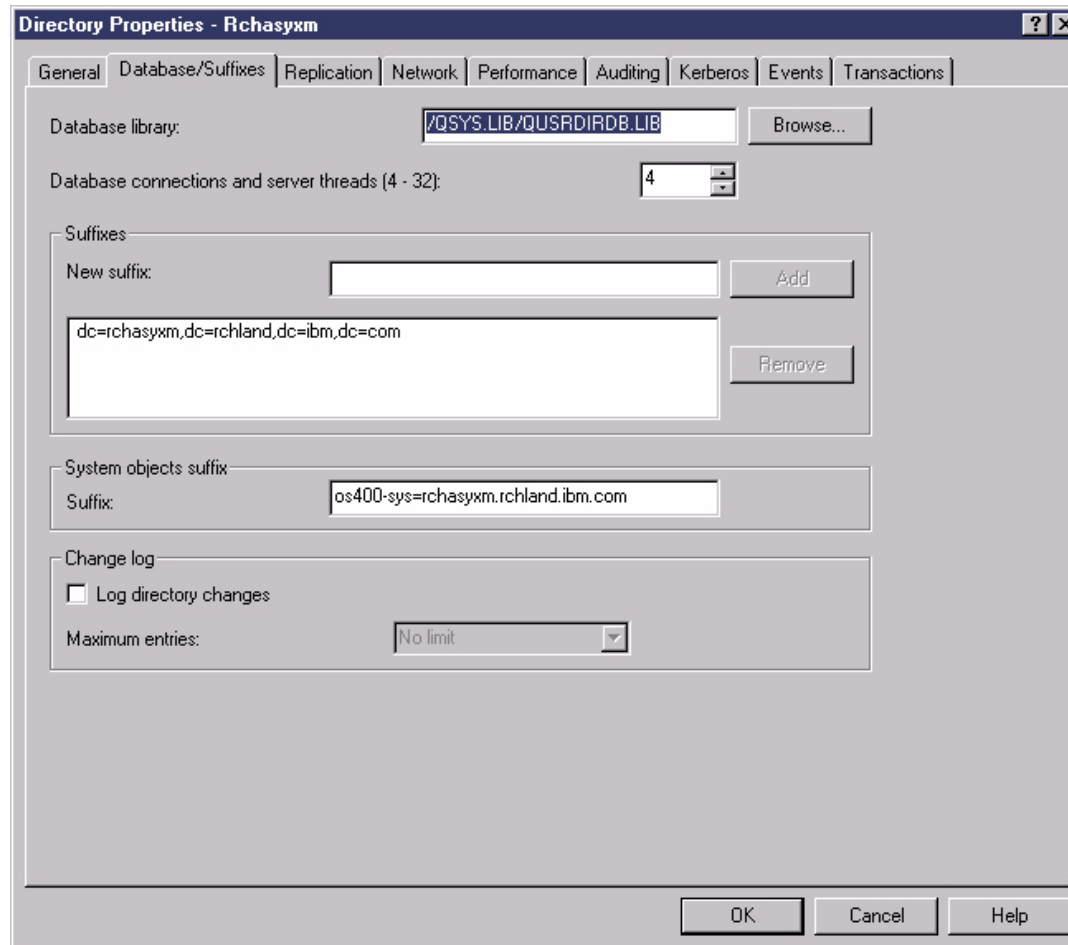
Properties: General

The screenshot shows the 'Directory Properties - Rchasyxm' dialog box with the 'General' tab selected. The dialog has several tabs: General, Database/Suffixes, Replication, Network, Performance, Auditing, Kerberos, Events, and Transactions. The 'General' tab contains the following settings:

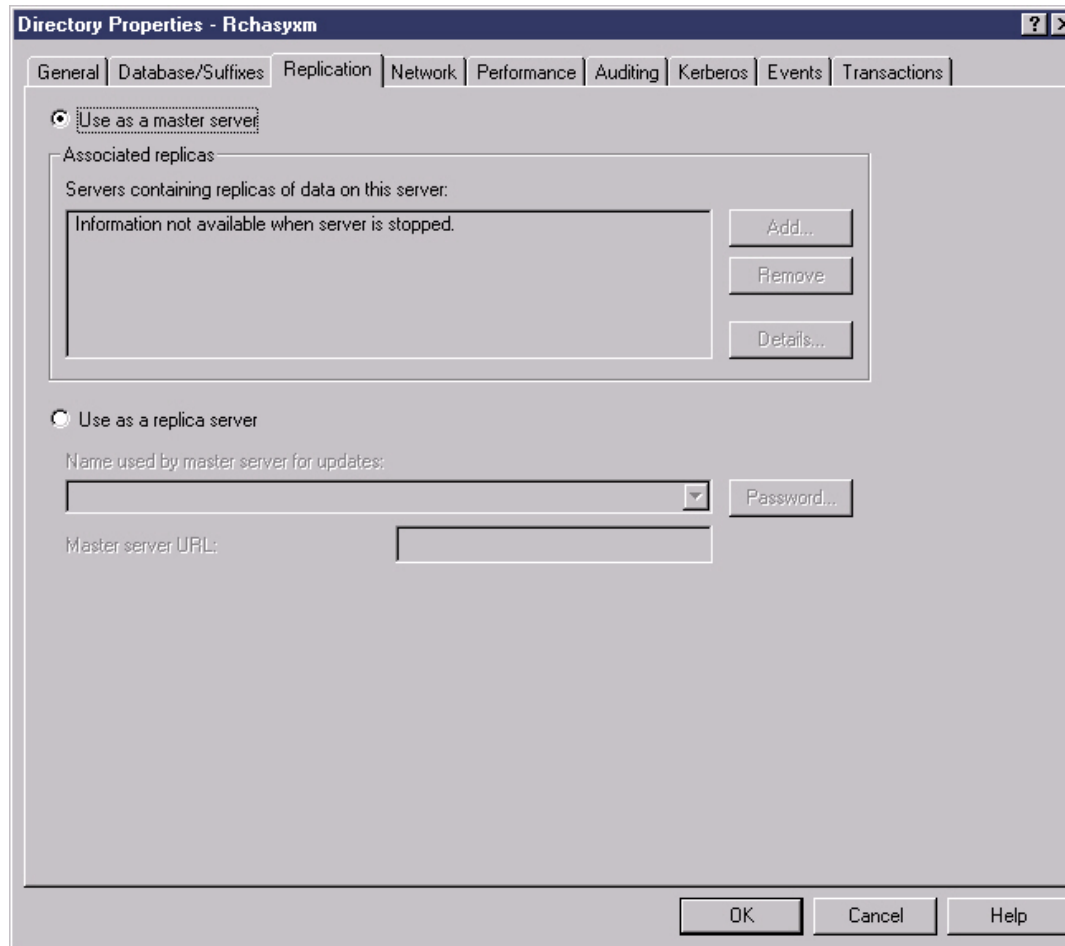
- LDAP protocol version: 3
- Start server when TCP/IP is started
- Allow directory updates
- Schema checking: V3 (lenient)
- Administrator information:
 - Administrator name: cn=admin
 - Grant administrator access to authorized users:
- Referrals: (empty list with buttons: Move Up, Move Down, Add, Edit, Remove)

At the bottom of the dialog are buttons for OK, Cancel, and Help.

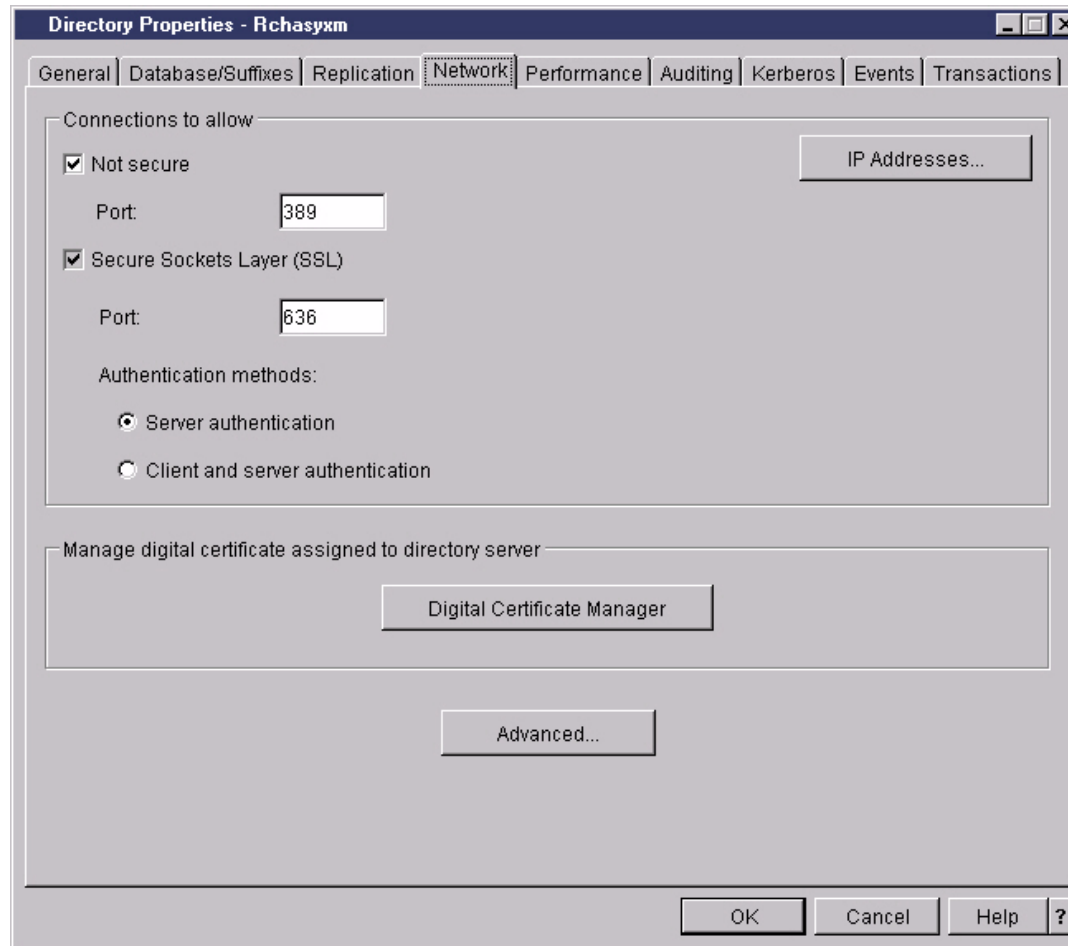
Properties: Database/Suffixes



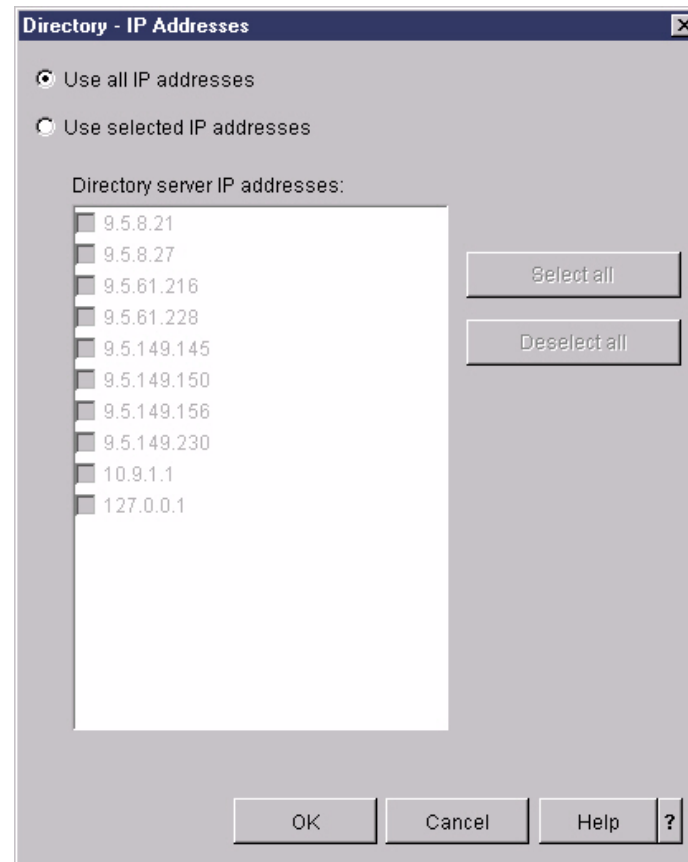
Properties: Replication



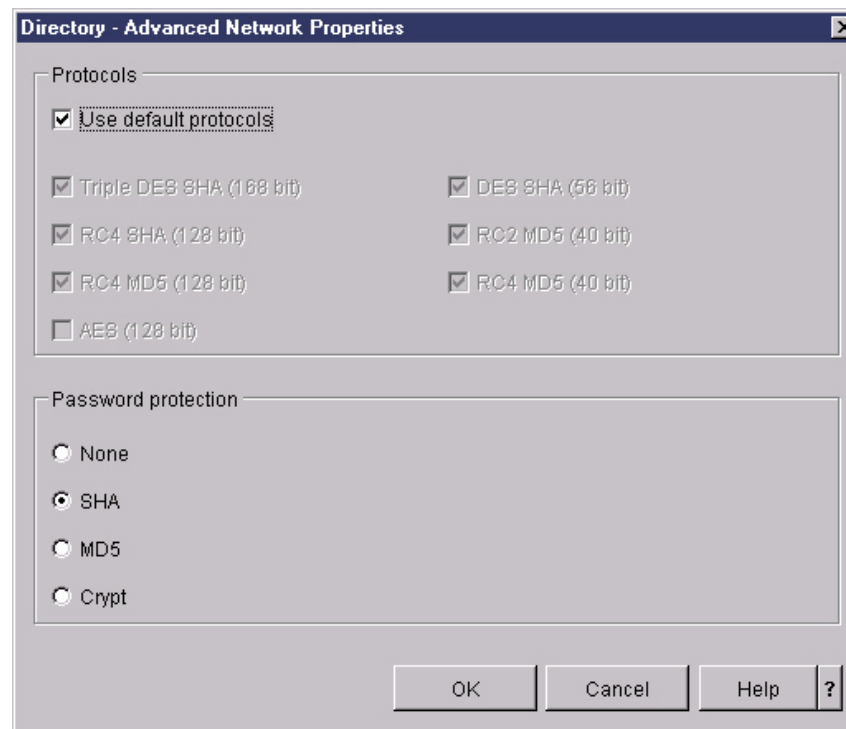
Properties: Network



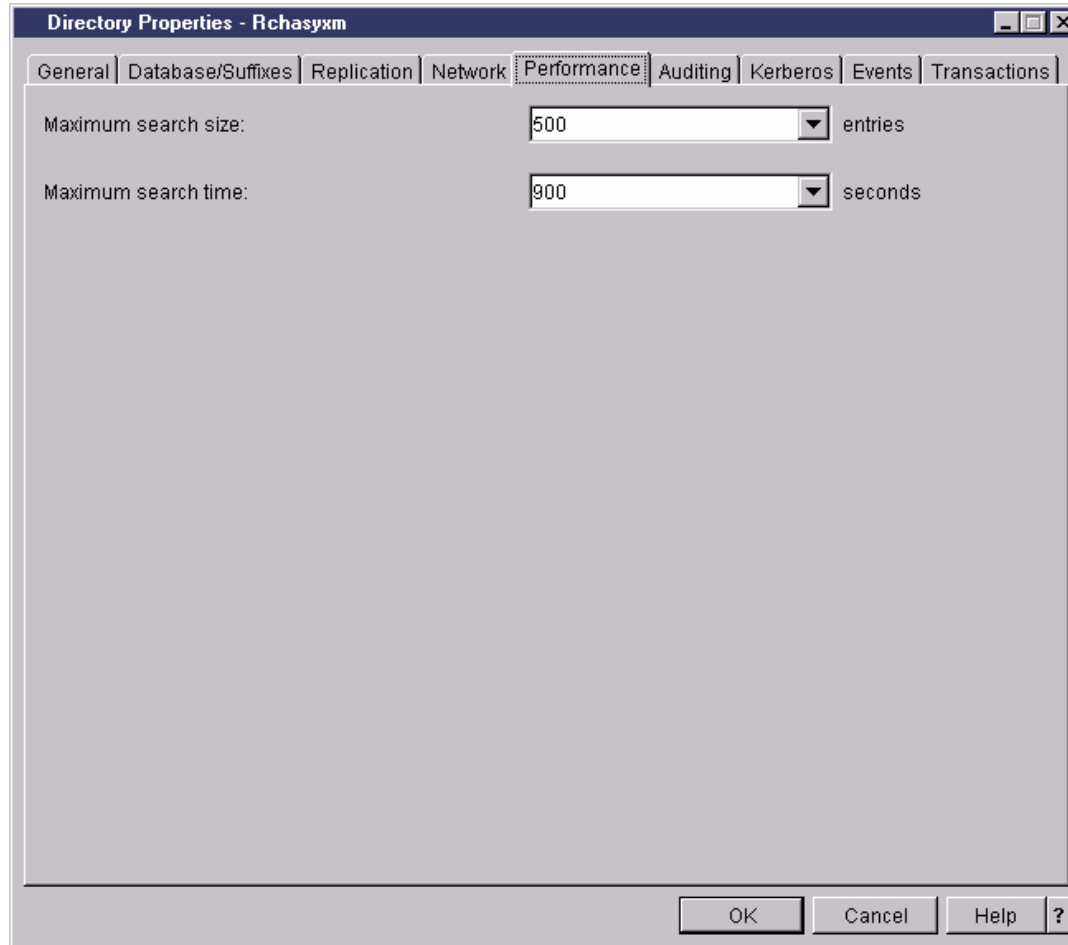
Properties: Network->IP Addresses



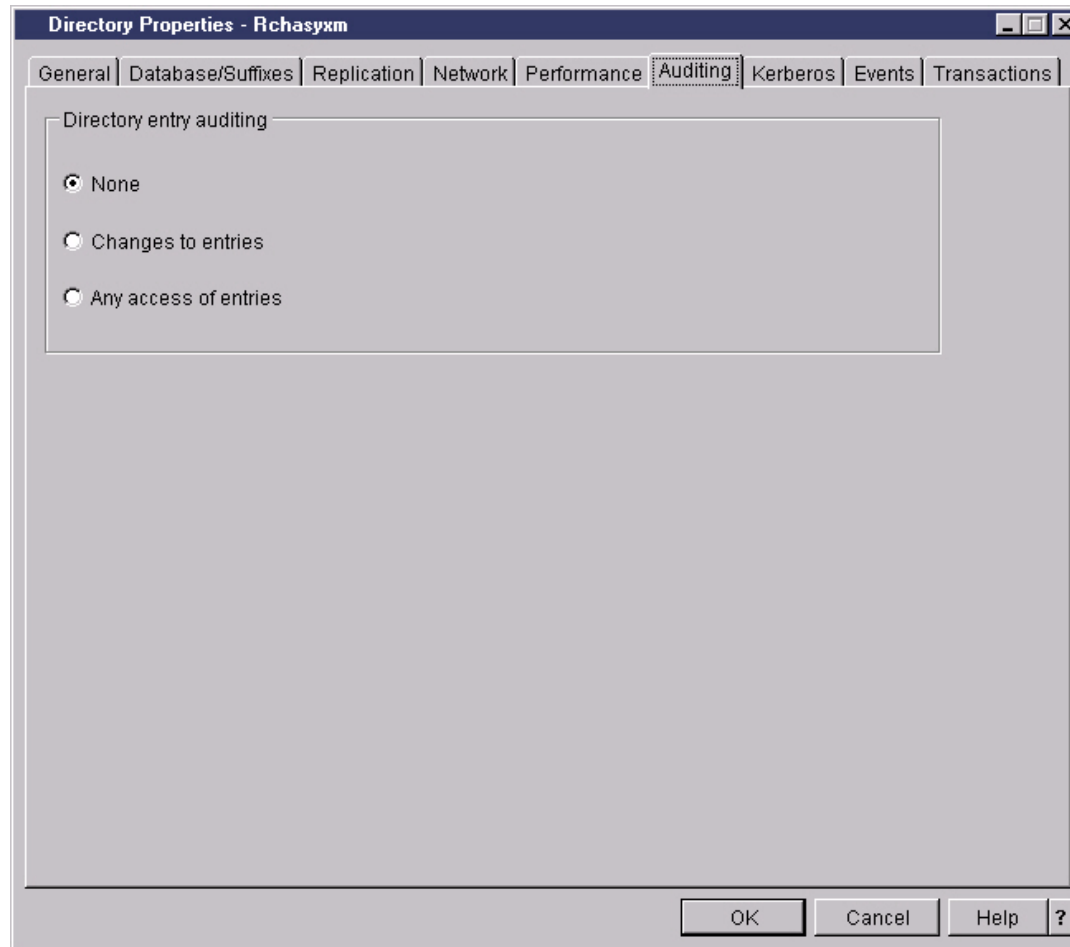
Properties: Network->Advanced



Properties: Performance



Properties: Auditing



Properties: Kerberos

Directory Properties - Rchasyxm

General Database/Suffixes Replication Network Performance Auditing **Kerberos** Events Transactions

Enable Kerberos authentication

Kerberos key tab file:

DN to use for connections

Search directory for DN with Kerberos attribute

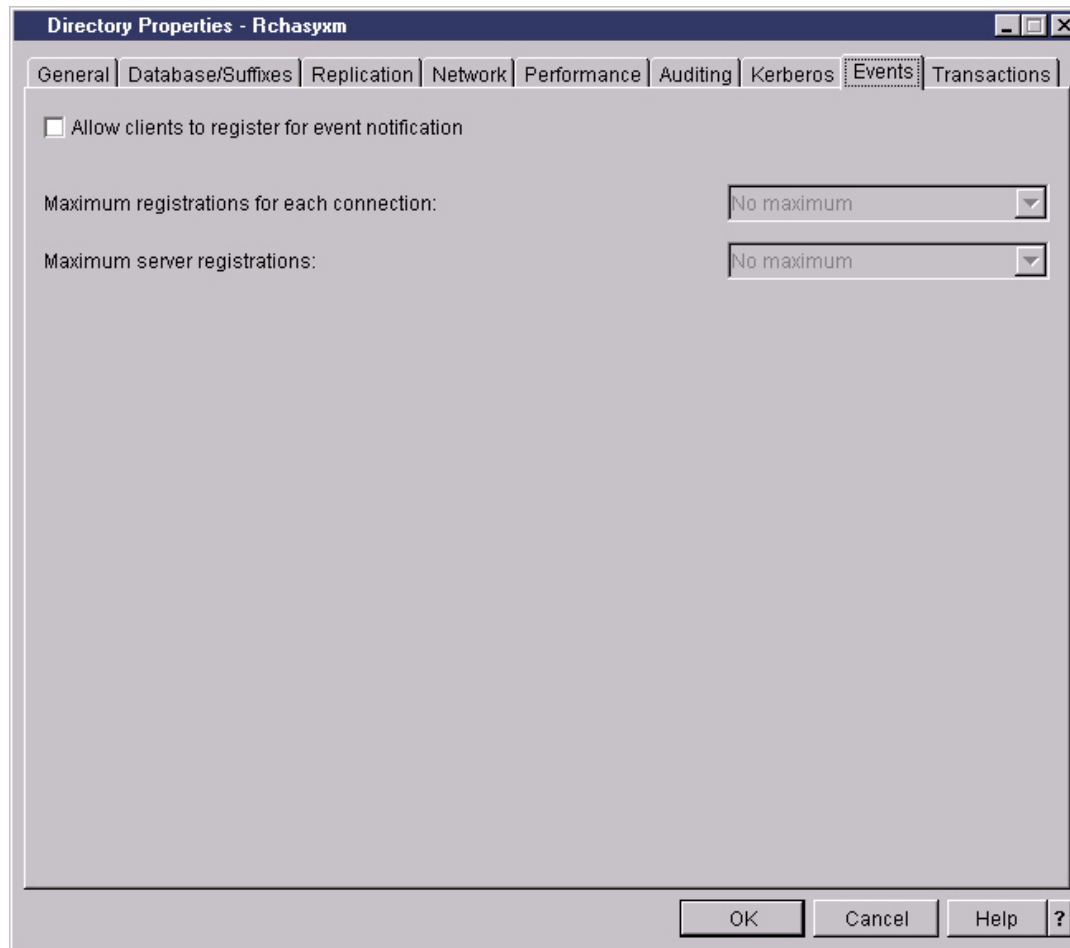
Create DN from Kerberos ID

Kerberos Administrator ID

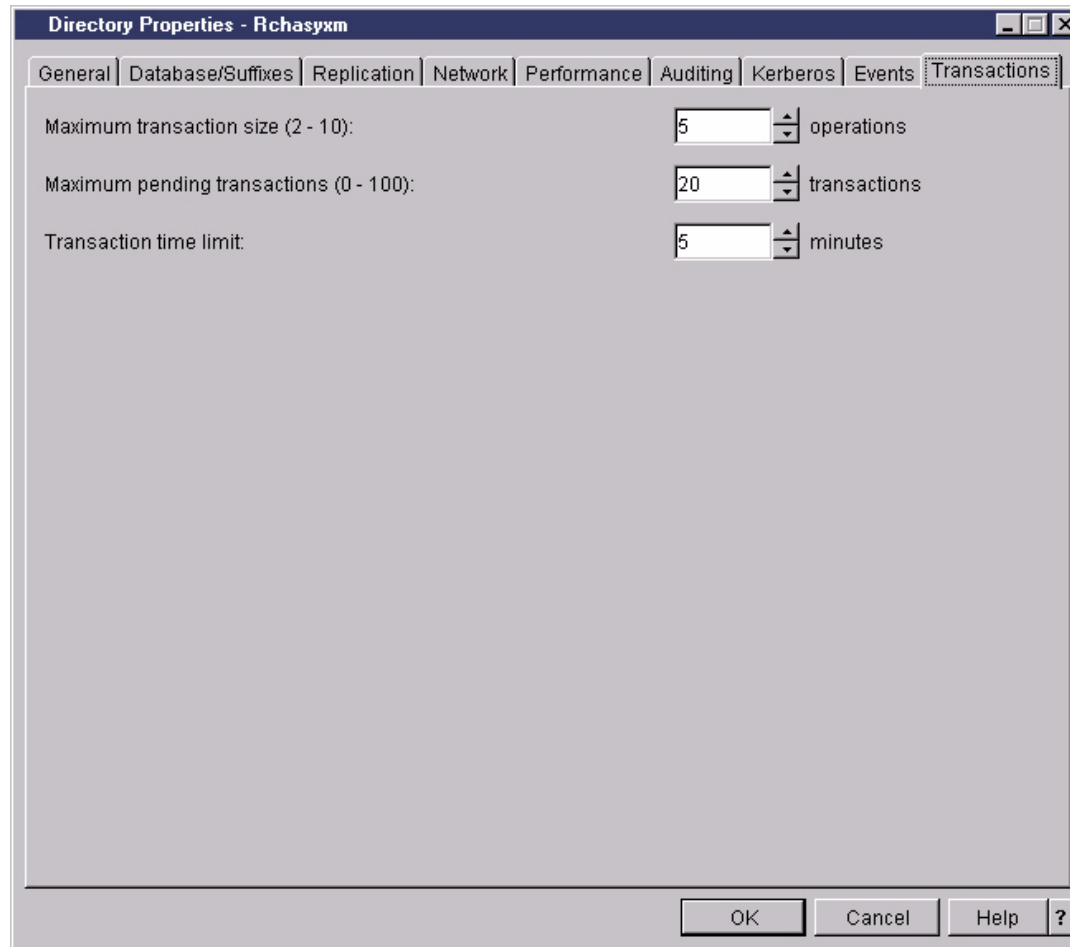
Name:

Realm:

Properties: Events



Properties: Transactions



Managing the Server

After initial configuration

The screenshot shows the iSeries Navigator interface. The main window displays a tree view on the left and a table of server configurations on the right. The table lists various services and their status. A context menu is open over the 'Directory' service, showing options like Start, Stop, Server Jobs, Tools, Reconfigure, Authority, ACL Groups, Reconnect, Status, and Properties. The 'Tools' option is expanded, showing 'Import File' and 'Export File'.

Server Name	Status	Description
DLFM	Stopped	Datalinks File Server
Virtual Private Networking	Stopped	Virtual private networking
ASFTomcat	Started	ASFTomcat server
Triggered Cache Manager	Stopped	Triggered cache manager
FTP	Started	FTP
LPD	Started	LPD
POP	Stopped	POP
Remote Execution	Stopped	Remote execution
SMTP	Started	SMTP
TELNET	Started	TELNET
HTTP Administration	Started	HTTP administration
Directory	Stopped	Directory

Server Configuration tasks:

- Configure subsystems for server jobs
- Create a new DNS Name Server
- Configure system as DHCP server
- Configure system as Directory
- Help for related tasks

Context Menu Options:

- Start
- Stop
- Server Jobs
- Tools
 - Import File
 - Export File
- Reconfigure
- Authority
- ACL Groups
- Reconnect
- Status
- Properties

Managing the server with iSeries Navigator

- **Start**
 - ▶ Starts the server when it is stopped.
- **Stop**
 - ▶ Stops the server when it is running.
- **Server Jobs**
 - ▶ Opens another window showing the status of the jobs running on the iSeries.
- **Tools->Import File**
 - ▶ Imports data into the directory from an LDIF file.
- **Tools->Export File**
 - ▶ Exports data from the directory into an LDIF file.
- **Reconnect**
 - ▶ Allows an administrator to reauthenticate to the server.
- **Status**
 - ▶ Shows information about server activity since last started.

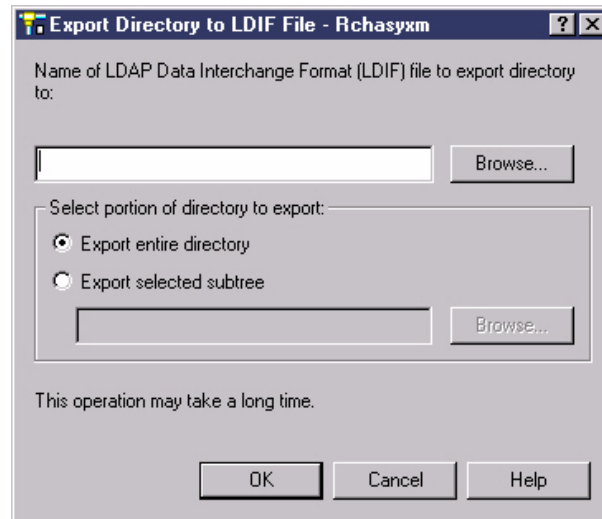
Server Jobs

Status: Active jobs

Job Name	Current User	Detailed Status	Server	Run Priority	Thread Count
Qdirsv		Completed - Printer output available	Directory	0	0
Qdirsv	Qdirsv	Waiting for signal	Directory	50	10
Qdirsv		Completed - Printer output available	Directory	0	0

1 - 3 of 3 objects

Tools->Export File



Status: Summary

Connect to Directory Server

Directory server: RCHASYXM

Distinguished name:

Password:
 Use system password

Use secure connection

OK Cancel Help ?

Directory Server Status - Rchasyxm

0 minutes old

Summary | Connections

Status:	Started at Feb 18, 2003 1:45:55 PM
Current number of threads:	1
Requests:	7
Requests completed:	7
Event registrations:	0
Notifications sent:	0

Refresh Now Timed Refresh...

OK Cancel Help ?

Status: Connections

0 minutes old

Summary **Connections**

Connections: 1

Active connections: 1

Blocked on read: 0

Blocked on write: 0

Distinguished Name	Connect Time	Completed Requests	Active Requests	Blocked
CN=ADMIN	Feb 18, 2003 1:48:05 PM	12	1	

Refresh Now Timed Refresh...

OK Cancel Help ?

Controlling Access

Ownership

- Each object in your directory has one or more owners.
- Object owners have the power to delete the object.
- Owners and the server administrator are the only users that can change the ownership properties and the access control list (ACL) attributes of an object.
- Ownership of objects can be either inherited or explicit.
 - ▶ Explicitly set up ownership for a specific object.
 - ▶ Specify that objects inherit their owners from objects higher up in the directory hierarchy.
- You can also specify that an object owns itself.
 - ▶ Specify a special DN `cn=this` in the list of object owners.
 - ▶ Example: if object `cn=A` has owner `cn=this`, then any user will have owner access to the `cn=A` object if he connects to the server as `cn=A`.

LDAP ACLs and Groups

- ACLs control who may add and delete directory objects.
- ACLs control who may read, write, search, and compare directory attributes.
- ACLs can be either inherited or explicit.
 - ▶ Explicitly set up an ACL for a specific object.
 - ▶ Specify that objects inherit ACLs from objects higher up in the directory hierarchy.
- ACL groups can simplify granting authority if the same set of users requires access to the same set of objects.
- ACL groups allow you to grant access to specific groups of users rather than granting authority on an individual basis.

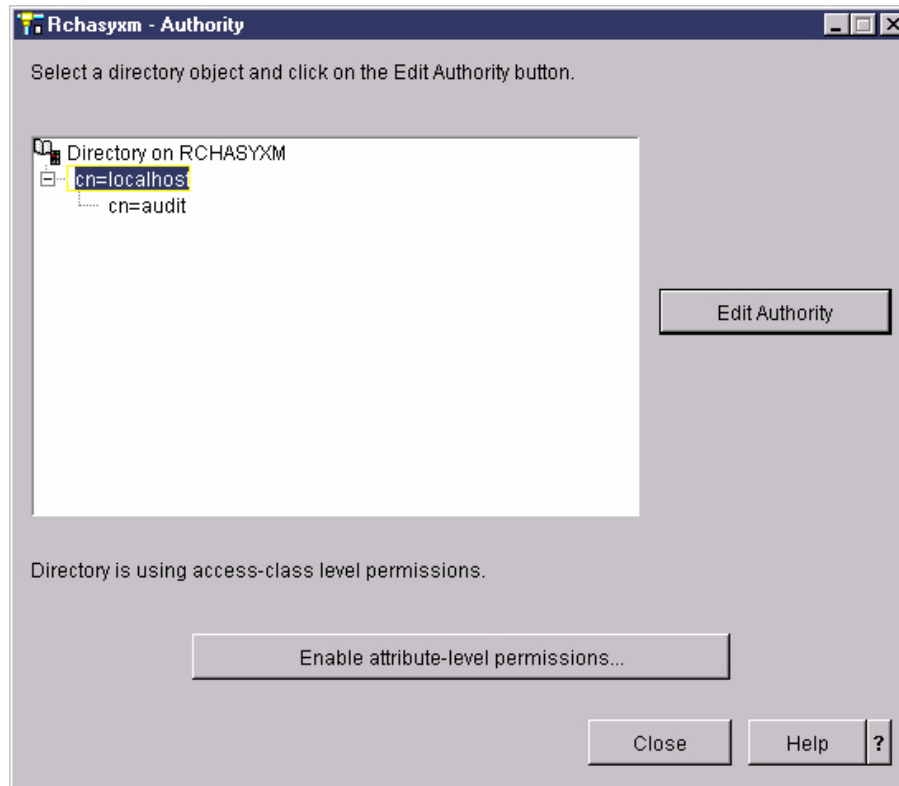
Controlling Access: General

- You can manage access to directory data from iSeries 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

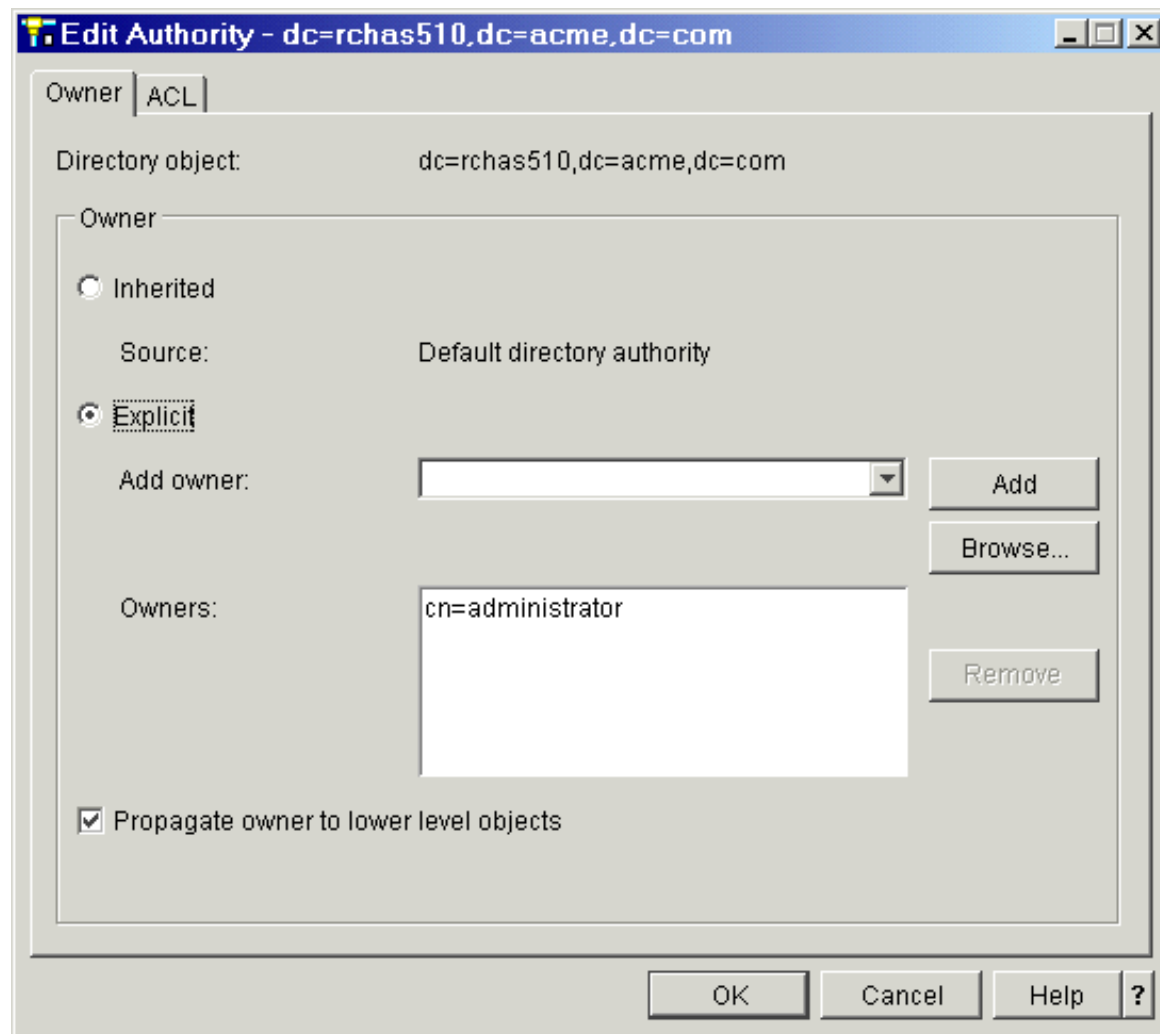
Controlling Access: General

- 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

Authority



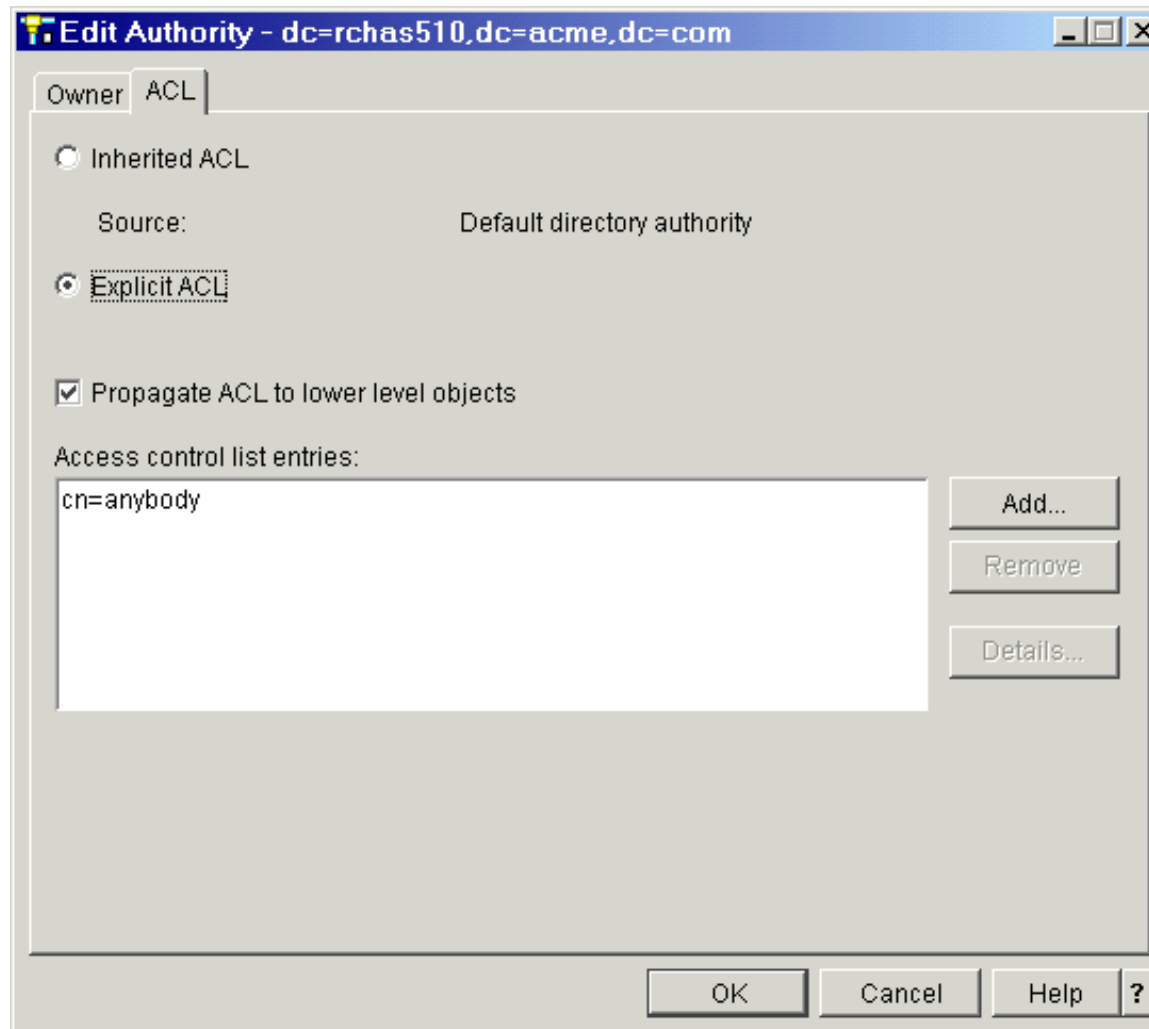
Controlling Access: Owner



Controlling Access: ACLs

- 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

Controlling Access: ACLs



Controlling Access: ACLs

Add ACL Entry

Object | Attributes

Directory object: dc=rchas510,dc=acme,dc=com

User: cn=John McMeeking,cn=users,dc=ac Browse...

Object permissions:

Add: Unspecified

Delete: Unspecified

Controlling Access: ACLs

Add ACL Entry [X]

Object: **Attributes**

Directory object: dc=rchas510,dc=acme,dc=com

User: cn=John McMeeking,cn=users,dc=acme,...

Legend:

Unspecified Grant Deny

Attribute permissions:

Access Class	Read	Write	Search	Compare
Critical	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Normal	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Attribute specific permissions:

Attribute	Read	Write	Search	Compare
userPassword	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Add...
Remove

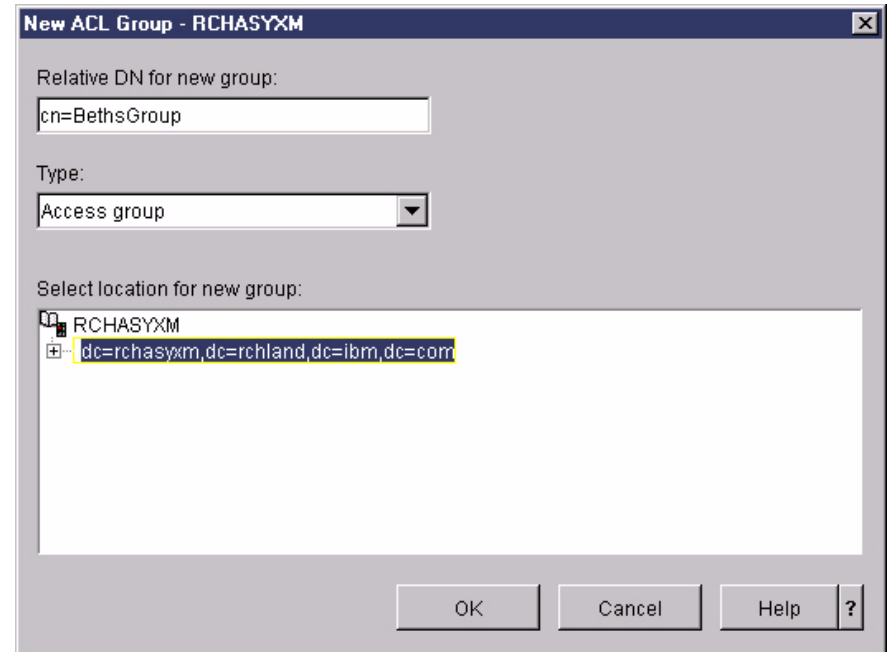
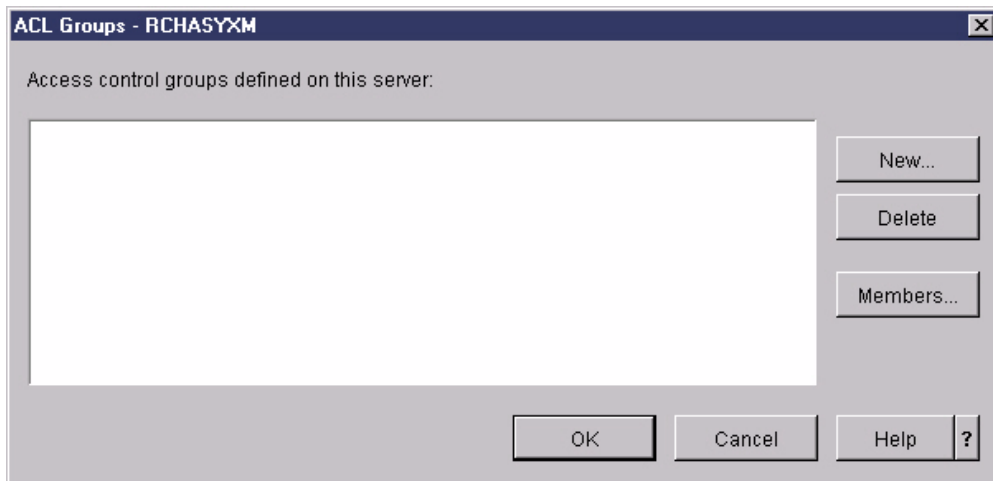
Grant All Deny All Clear All

OK Cancel Help ?

Controlling Access: Groups

- 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=jmcmeeek@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

ACL Groups



Controlling Access: ACLs

New ACL Group - RCHAS510

Group:

Common name:

Type: Access group

Member to add:

Members

- cn=John McMeeking,cn=users,dc=acme,dc=com
- cn=Marla Berg,cn=users,dc=acme,dc=com

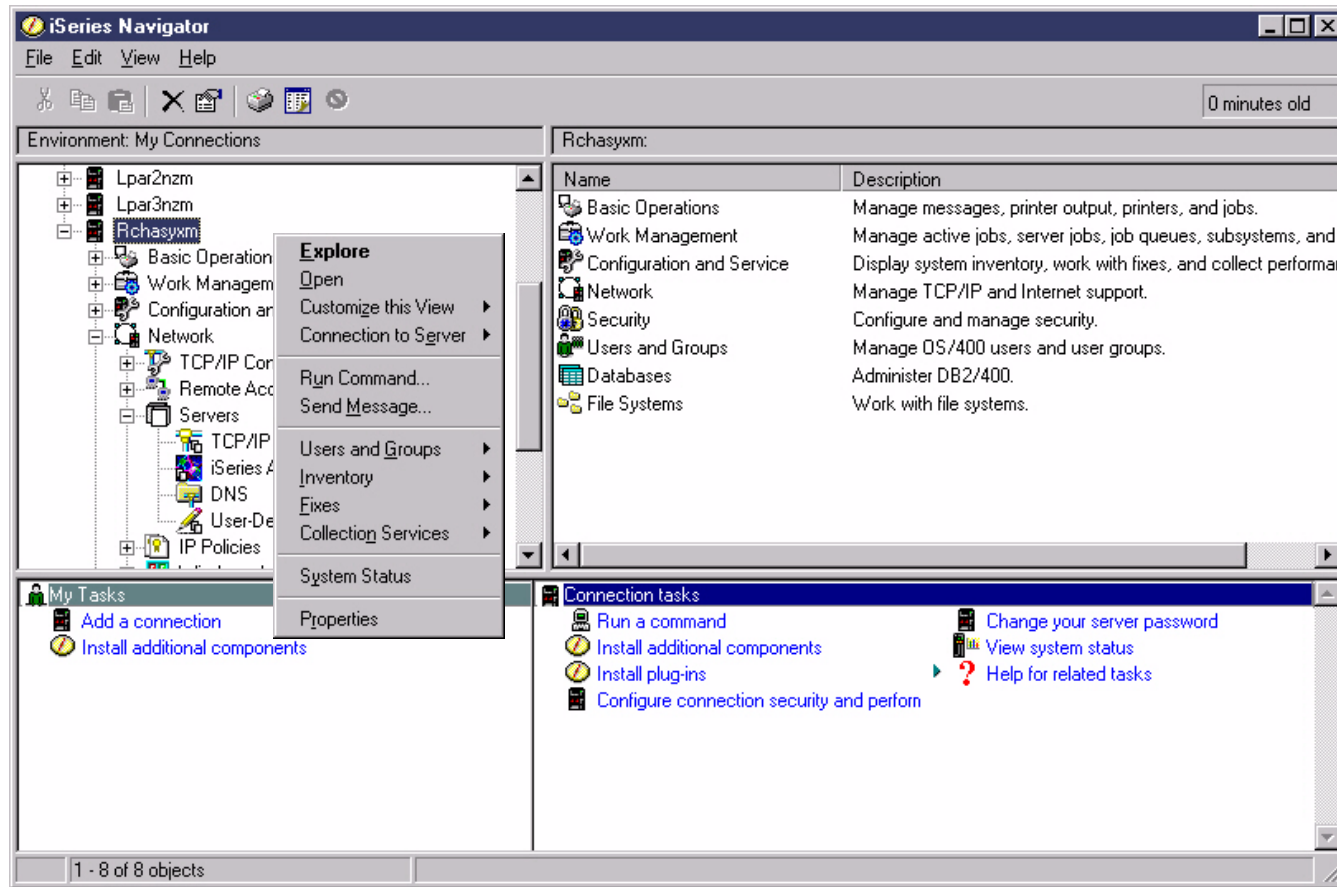
Directory:

- RCHAS510
 - dc=rchas510,dc=acme,dc=com

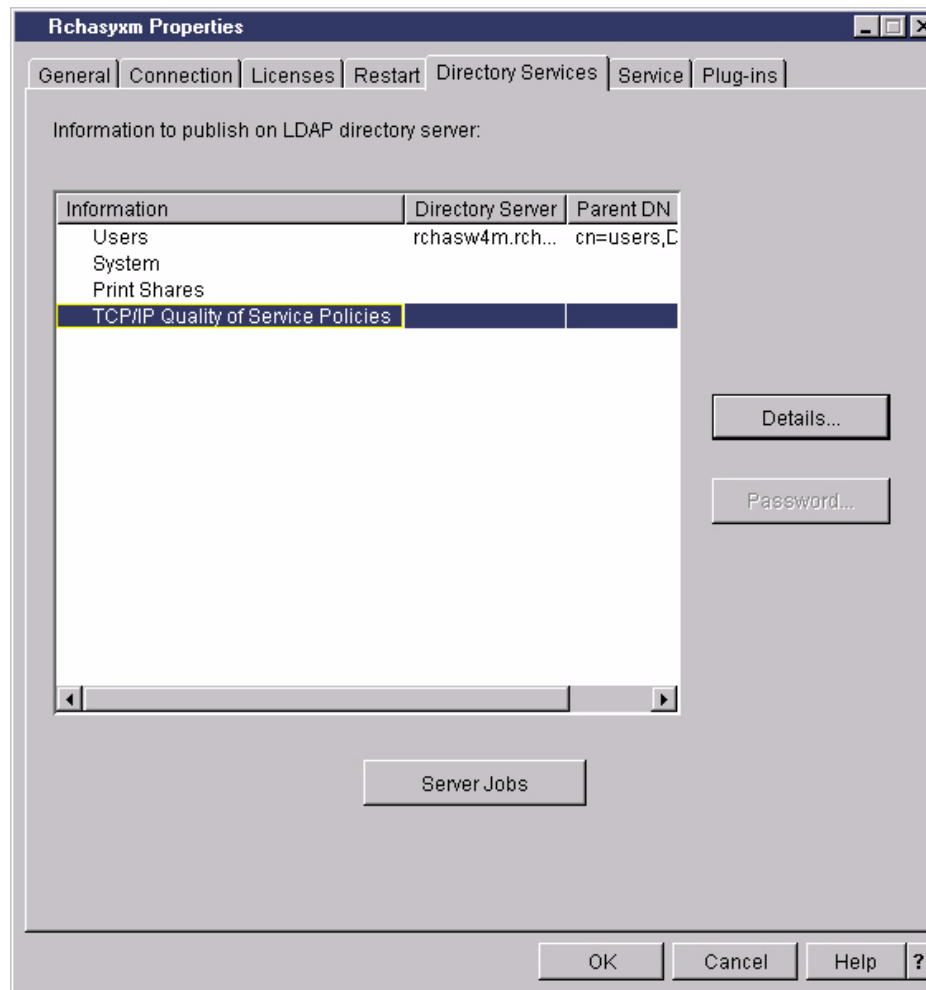
```
dn: cn=user administrators,dc=rchas510,dc=acme,dc=com
objectclass: accessgroup
objectclass: top
member: cn=John McMeeking,cn=users,dc=acme,dc=com
member: cn=Marla Berg,cn=users,dc=acme,dc=com
cn: user administrators
```

Publishing

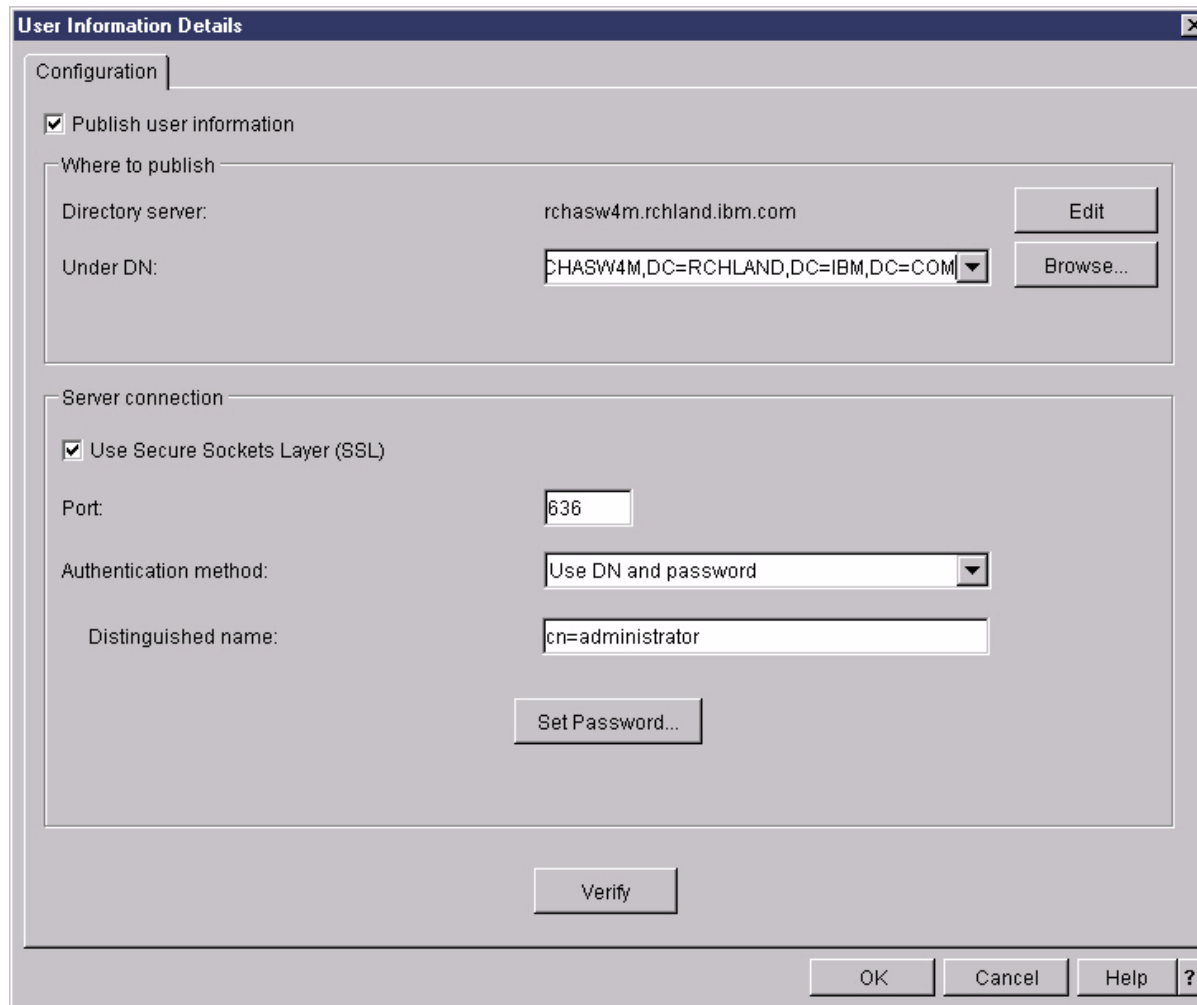
iSeries Navigator: Properties



Directory Services



User Information



The image shows a 'User Information Details' dialog box with a 'Configuration' tab. It is divided into two main sections: 'Where to publish' and 'Server connection'. The 'Where to publish' section includes a checked 'Publish user information' checkbox, a 'Where to publish' label, a 'Directory server' field with the value 'rchasw4m.rchland.ibm.com' and an 'Edit' button, and an 'Under DN' dropdown menu with the value 'CHASW4M,DC=RCHLAND,DC=IBM,DC=COM' and a 'Browse...' button. The 'Server connection' section includes a checked 'Use Secure Sockets Layer (SSL)' checkbox, a 'Port' field with the value '636', an 'Authentication method' dropdown menu with the value 'Use DN and password', and a 'Distinguished name' field with the value 'cn=administrator'. There is a 'Set Password...' button below the 'Distinguished name' field. At the bottom of the dialog is a 'Verify' button. The standard 'OK', 'Cancel', 'Help', and '?' buttons are located at the bottom right.

User Information Details

Configuration

Publish user information

Where to publish

Directory server: rchasw4m.rchland.ibm.com

Under DN: CHASW4M,DC=RCHLAND,DC=IBM,DC=COM

Server connection

Use Secure Sockets Layer (SSL)

Port: 636

Authentication method: Use DN and password

Distinguished name: cn=administrator

Example: Published User

```
C:\>ldapsearch -h myiseries -b "cn=users,dc=myiseries,dc=com" "(sn=hoffman)"
cn=Beth L Hoffman,cn=users,dc=myiseries,dc=com
objectclass=top
objectclass=person
objectclass=organizationalPerson
objectclass=inetOrgPerson
objectclass=publisher
objectclass=ePerson
cn=Beth L Hoffman
cn=Beth Hoffman
cn=BETHVH
sn=Hoffman
uid=BETHVH
givenname=Beth
description=BETHVH
title=OS/400 Directory Services
departmentnumber=G8RA
telephonenumber=(507)253-3627
roomnumber=J119
registeredaddress=3605 Highway 52 NW Rochester, MN 55901
mail=bethvh@US.IBM.COM
publishername=dc=MYISERIES,dc=COM
```


System Information - Configuration

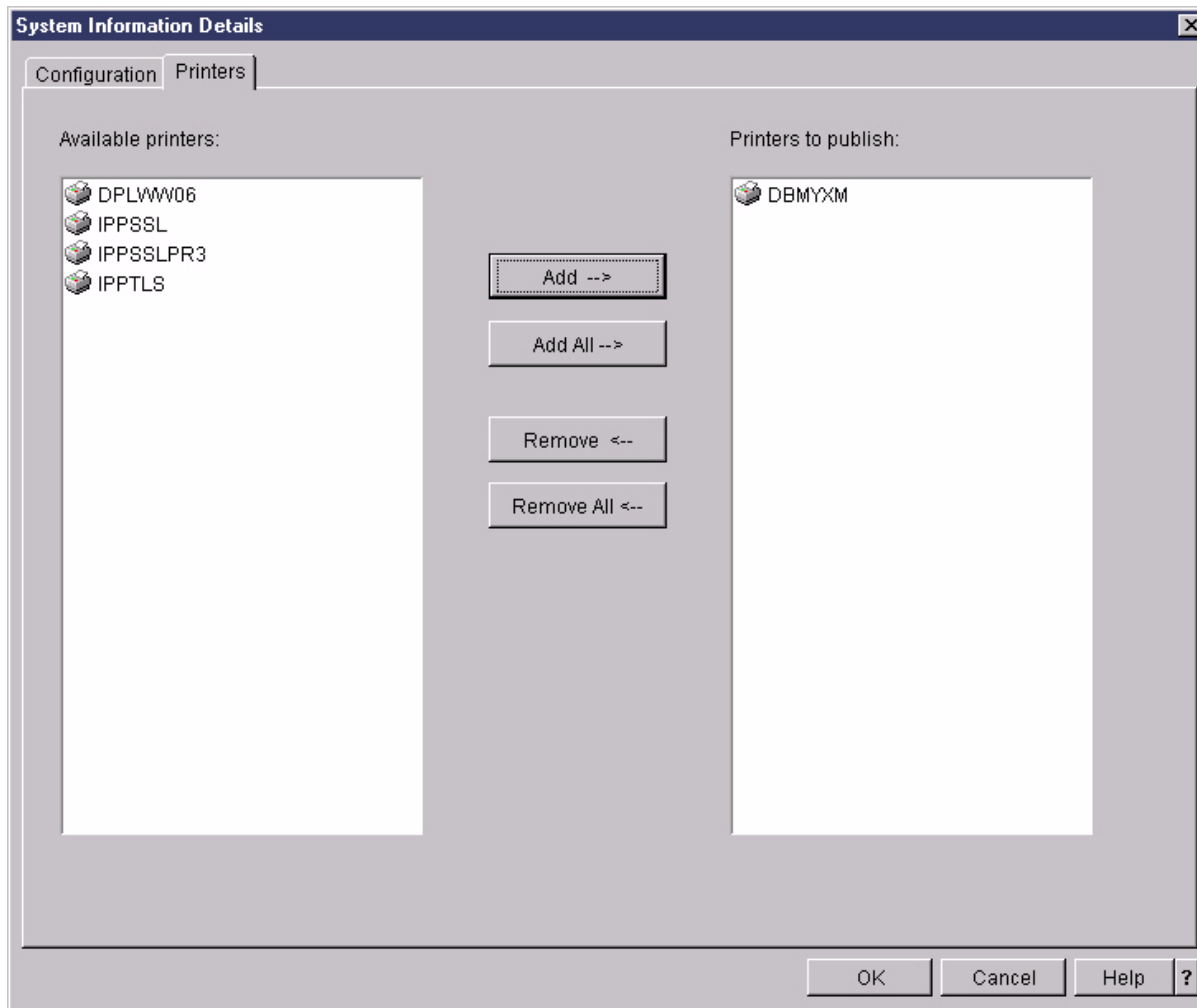
The screenshot shows a dialog box titled "System Information Details" with a close button (X) in the top right corner. It has two tabs: "Configuration" (selected) and "Printers".

Configuration Tab:

- Publish system information
- Where to publish:**
 - Directory server: [Edit]
 - Under DN: [Text Field] [Browse...]
- Server connection:**
 - Use Secure Sockets Layer (SSL)
 - Port: [389]
 - Authentication method: [Use DN and password]
 - Distinguished name: [Text Field]
 - [Set Password...]
- [Verify]

At the bottom of the dialog are buttons for OK, Cancel, Help, and a question mark icon.

System Information - Printers



Print Shares - Configuration

Print Share Information Details [X]

Configuration | **Print Shares**

Publish print share information

Where to publish

Active Directory server: [Edit]

Under DN: [] [Browse...]

Server connection

Use Secure Sockets Layer (SSL)

Port: [389]

Authentication method: [Use DN and password]

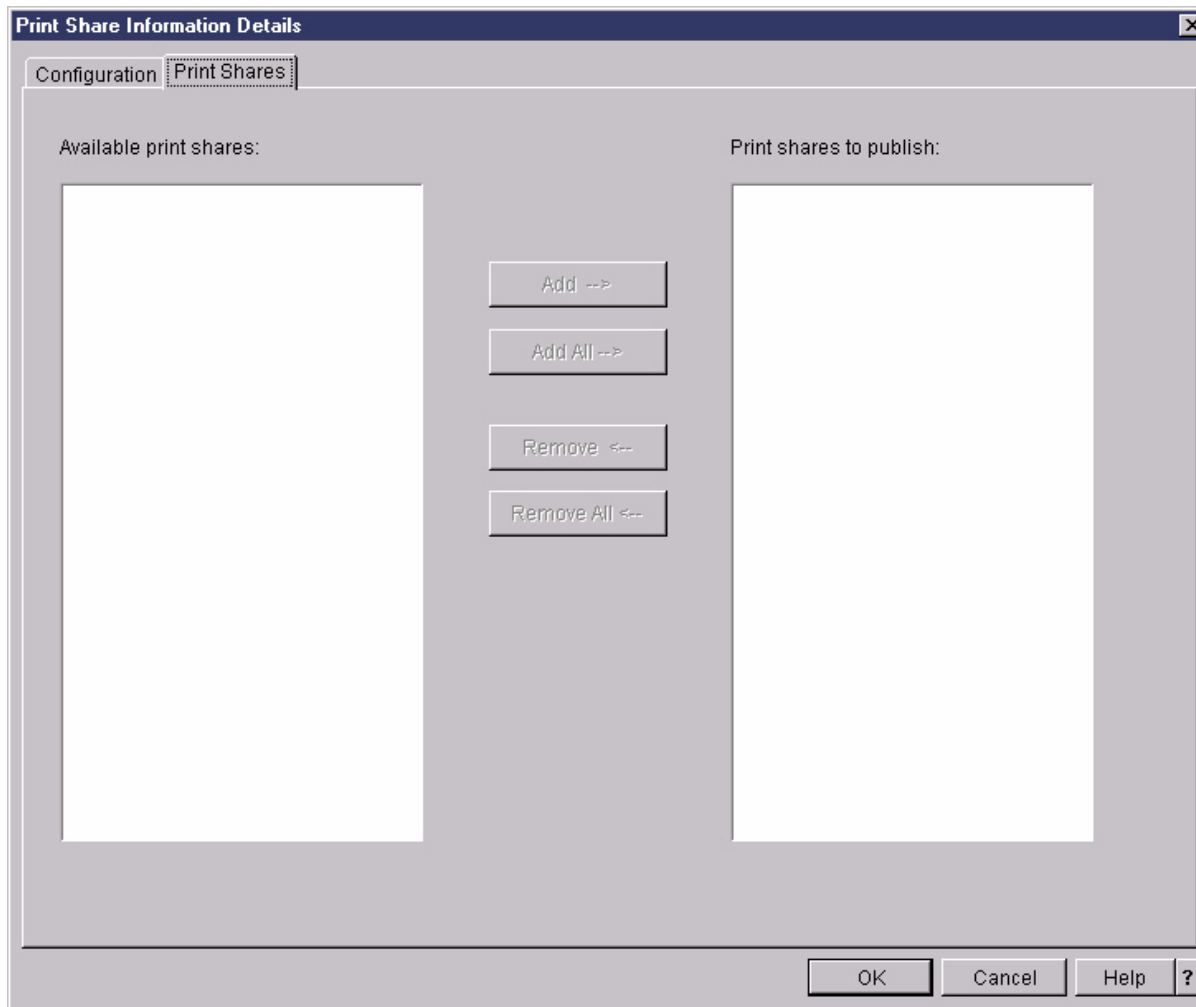
Distinguished name: []

[Set Password...]

[Verify]

[OK] [Cancel] [Help] [?]

Print Shares - Print Shares



TCP/IP QOS

TCP/IP Quality of Service Policy Information Details [X]

Configuration

Publish TCP/IP Quality of Service policy information

Where to publish

Directory server: Edit

Under DN: Browse...

Search...

Server connection

Use Secure Sockets Layer (SSL)

Port:

Authentication method:

Distinguished name:

Set Password...

Verify

OK Cancel Help ?

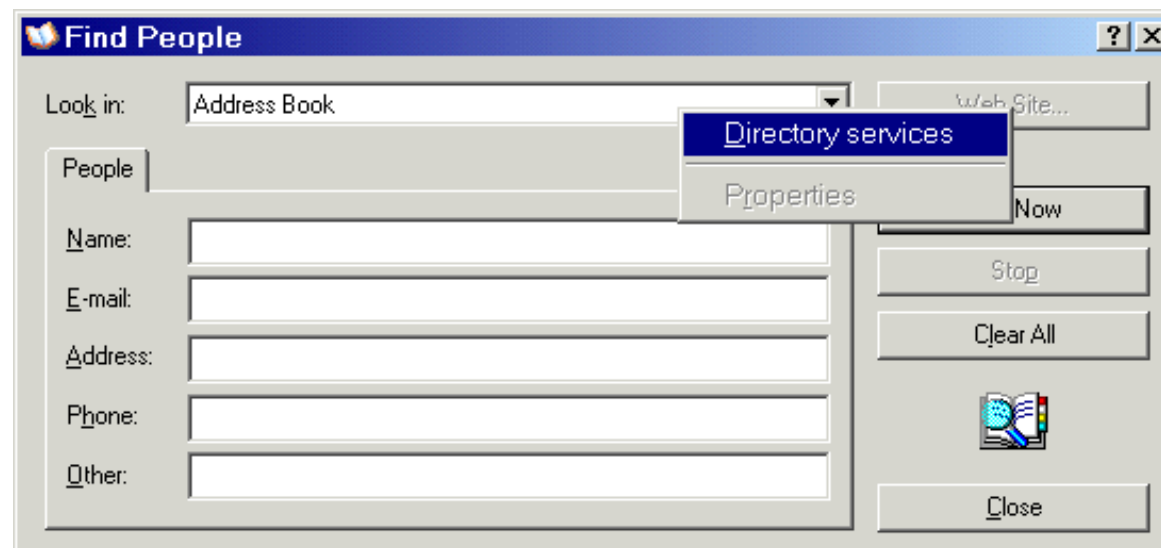
Tools for Accessing the Directory

Tools

- Pointing your address book at an LDAP server
- IBM Directory Management Tool (DMT)
- Command line utilities
- iSeries Navigator for management of access control
- Other tools

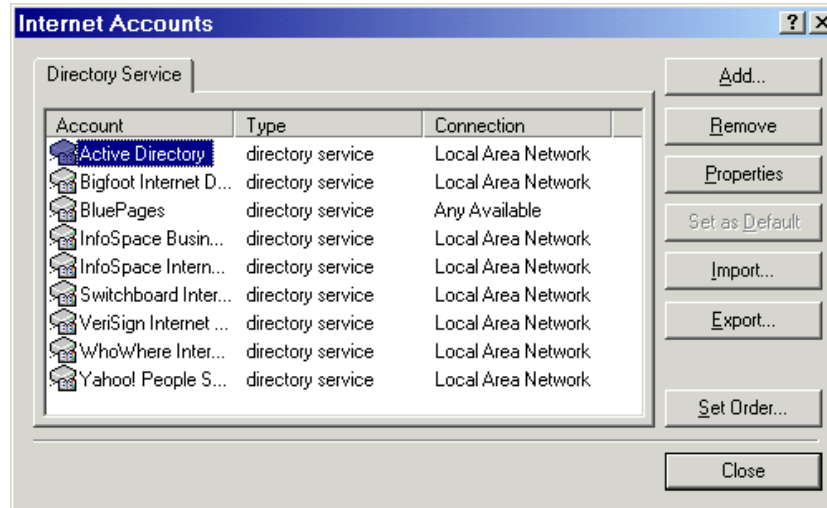
Pointing your address book at an LDAP server

- 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"



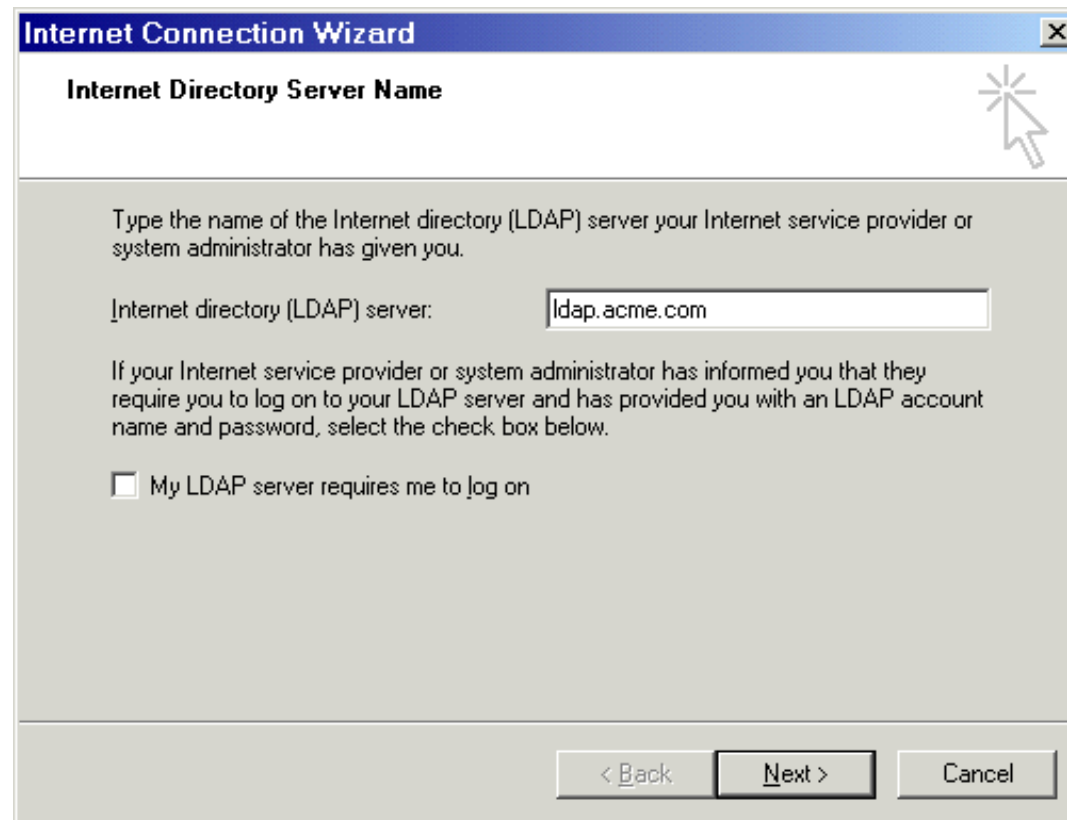
Address book setup

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



Address book setup

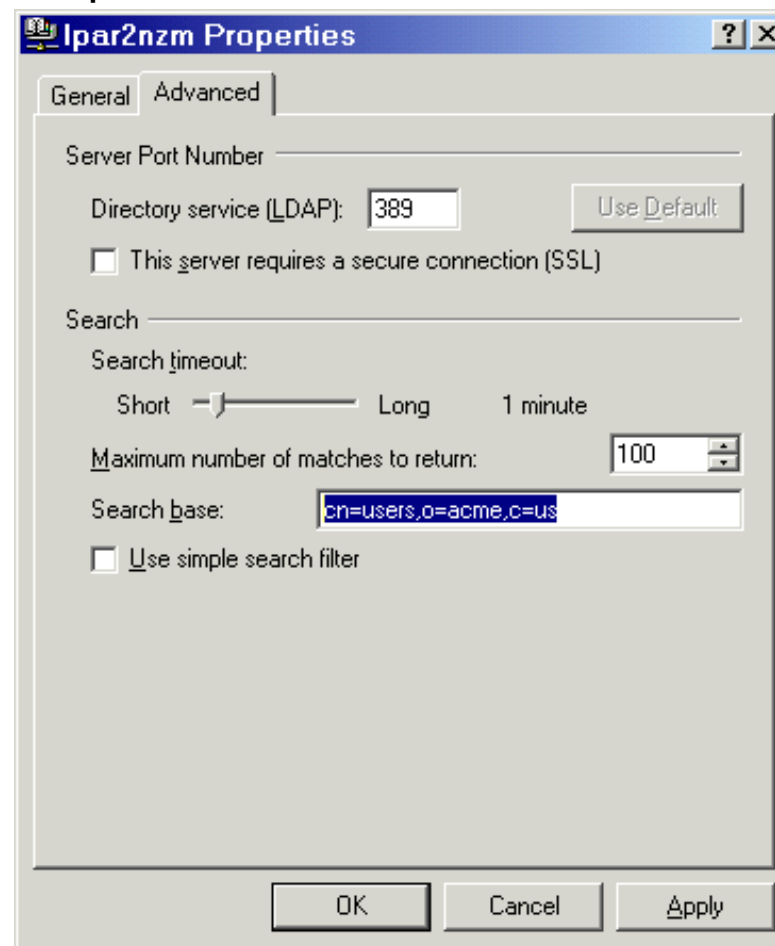
- Fill in Server name and continue to end of wizard



The screenshot shows a Windows-style dialog box titled "Internet Connection Wizard". The current step is "Internet Directory Server Name". The text inside the dialog reads: "Type the name of the Internet directory (LDAP) server your Internet service provider or system administrator has given you." Below this is a text input field labeled "Internet directory (LDAP) server:" containing the text "ldap.acme.com". Further down, there is a paragraph: "If your Internet service provider or system administrator has informed you that they require you to log on to your LDAP server and has provided you with an LDAP account name and password, select the check box below." Below this paragraph is a checkbox labeled "My LDAP server requires me to log on", which is currently unchecked. At the bottom of the dialog are three buttons: "< Back", "Next >", and "Cancel".

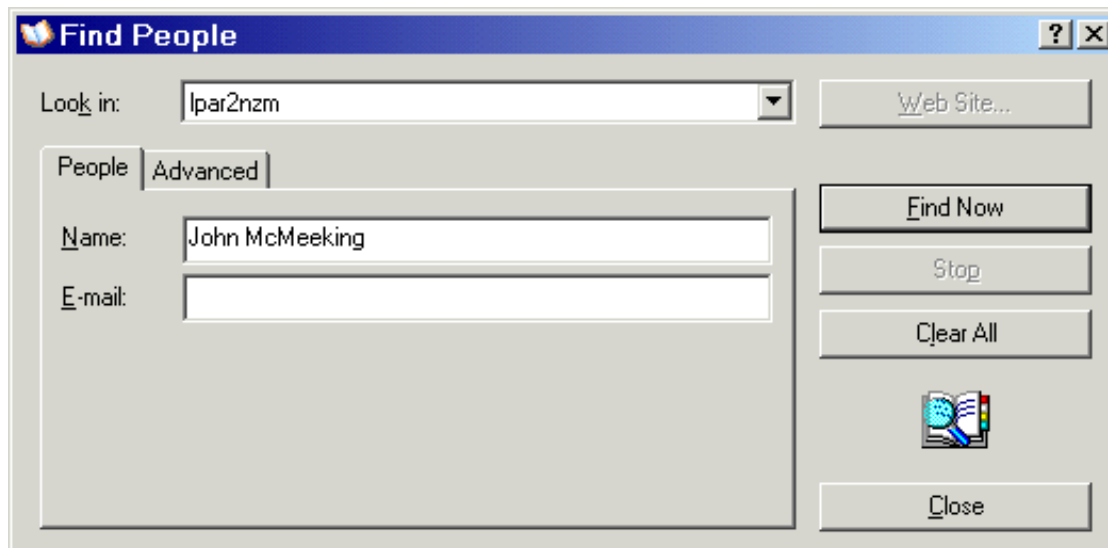
Address book setup

- 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:



Find People ? X

Look in: lpar2nzm Web Site...

People Advanced

Name: John McMeeking

E-mail:

Find Now

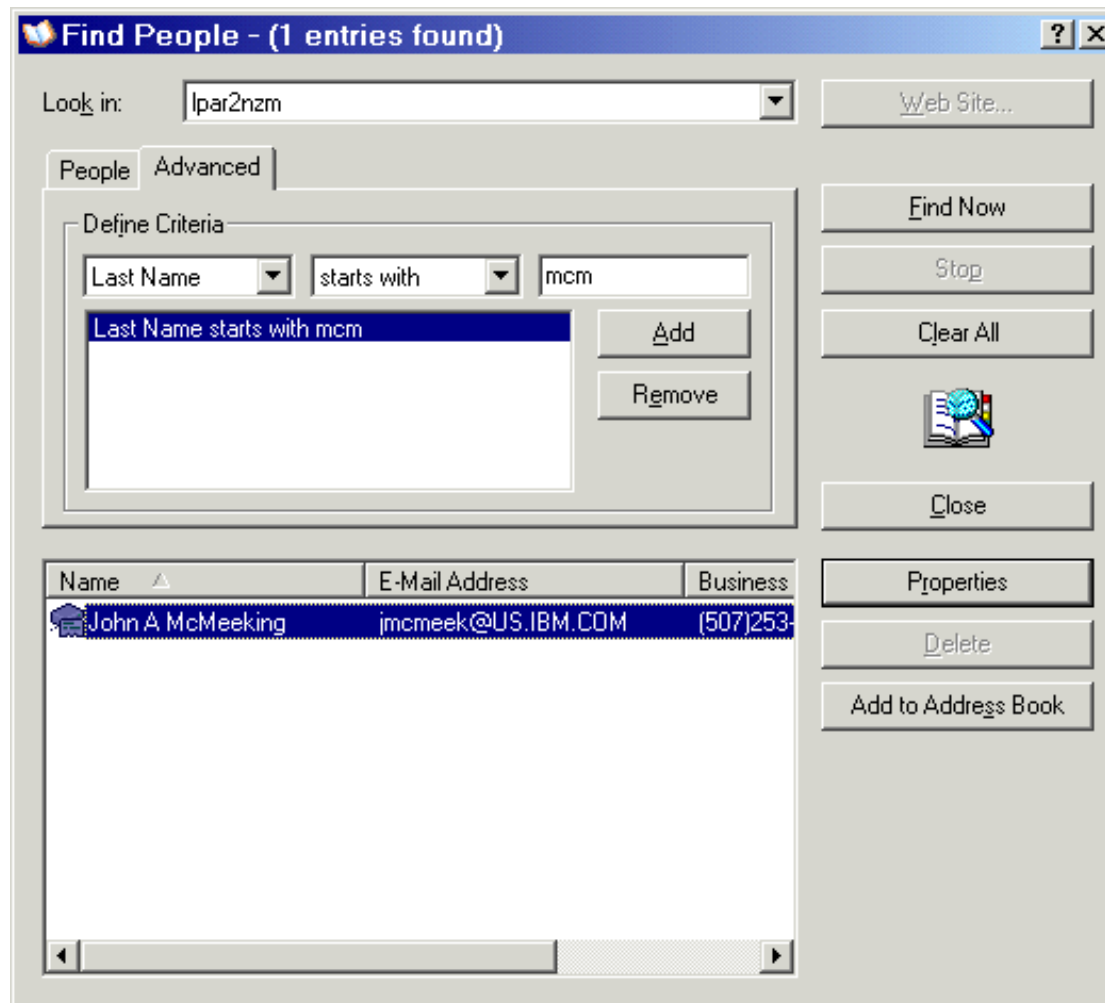
Stop

Clear All

Close

Address book setup

- Or maybe try an advanced search:



Using DMT

IBM SecureWay Directory Management Tool

ldap://rchas510:389

Introduction

Ready


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

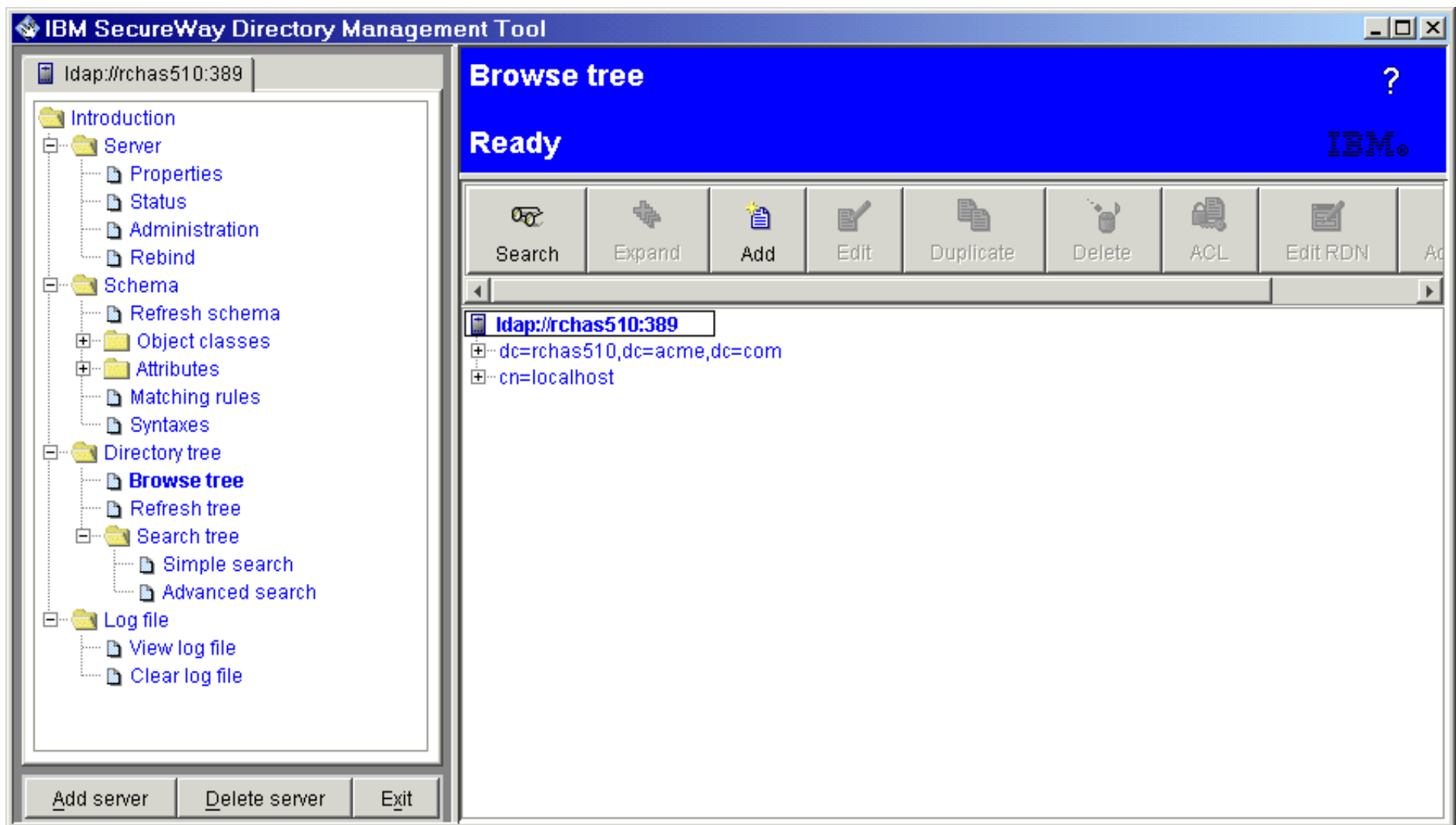
Buttons: Add server, Delete server, Exit

Using DMT

- Install the IBM 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>

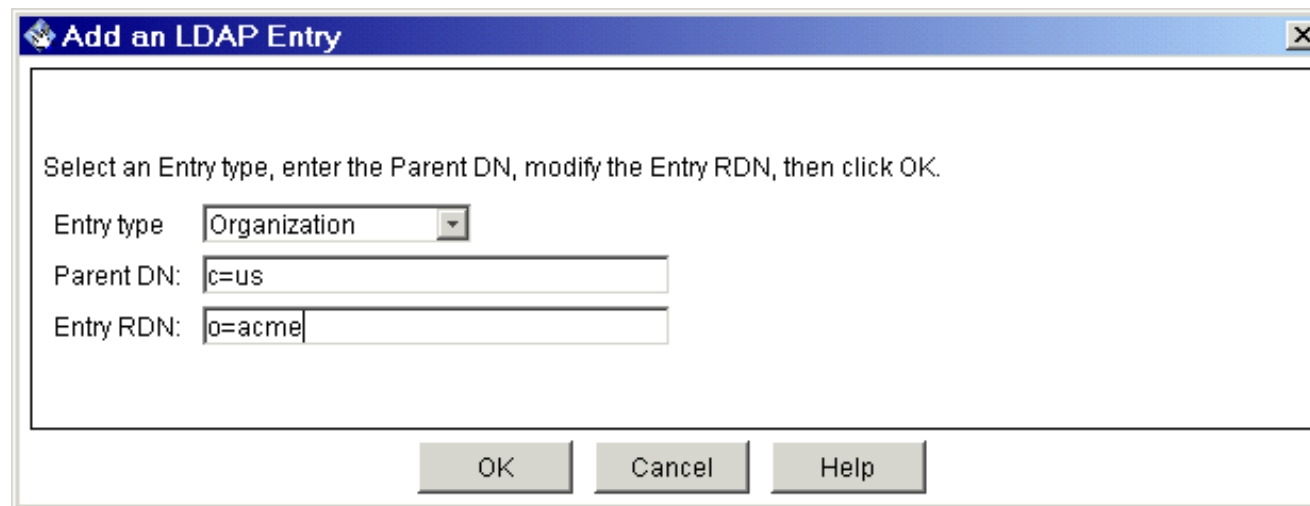
Using DMT - Create an entry

- 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"



Add an LDAP Entry

Select an Entry type, enter the Parent DN, modify the Entry RDN, then click OK.

Entry type:

Parent DN:

Entry RDN:

Using DMT - Create an entry

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

Add an LDAP Entry [X]

To add a new entry, enter values for the attributes, then click Add.

objectClass (Object class): organization

dn (DN): o=acme,c=us

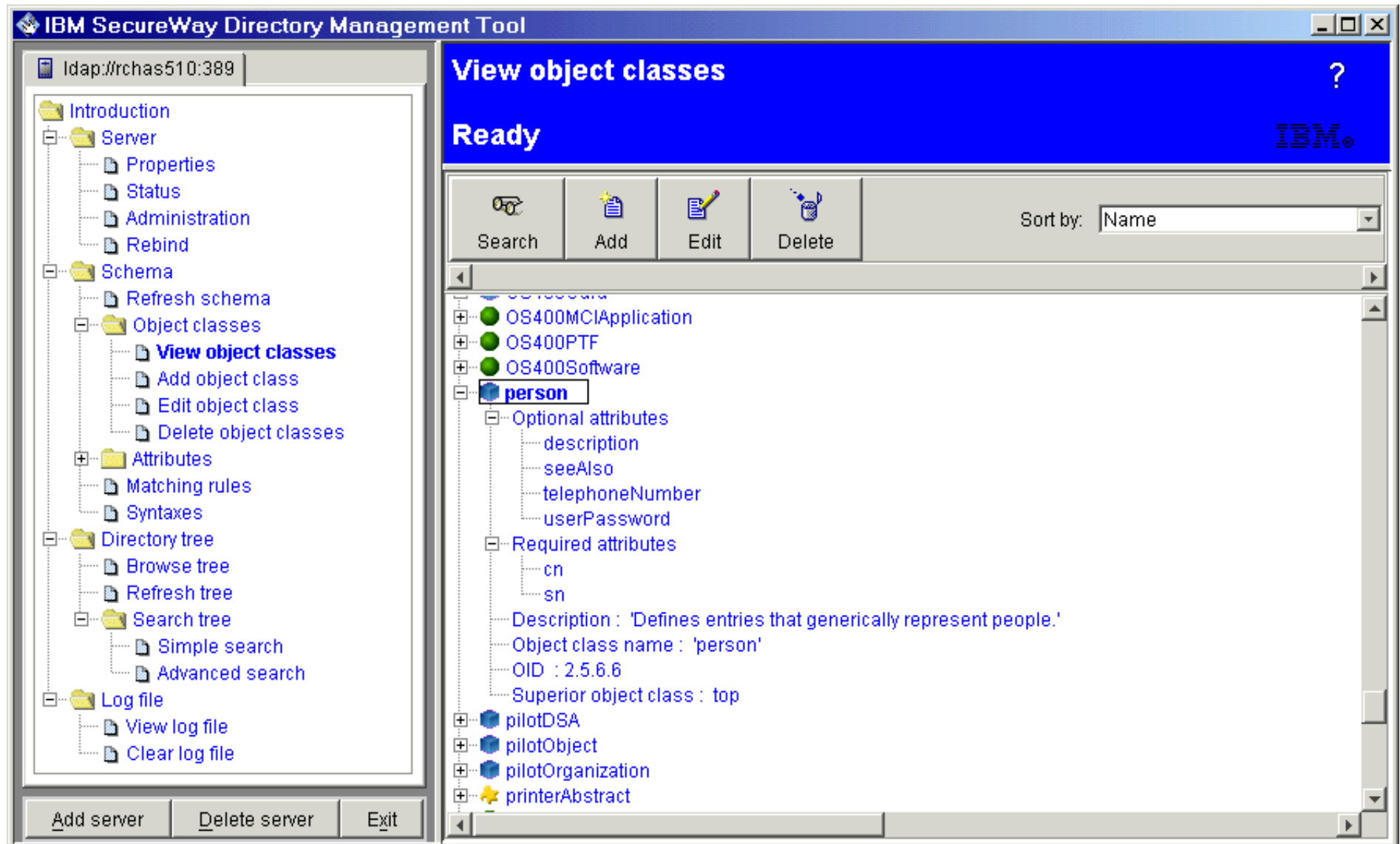
Attributes

o:	<input checked="" type="checkbox"/>	acme
businessCategory:	<input checked="" type="checkbox"/>	
description:	<input checked="" type="checkbox"/>	
destinationIndicator:	<input checked="" type="checkbox"/>	
facsimileTelephoneNumber:	<input checked="" type="checkbox"/>	
internationalISDNNumber:	<input checked="" type="checkbox"/>	
l:	<input checked="" type="checkbox"/>	
physicalDeliveryOfficeName:	<input checked="" type="checkbox"/>	
postalAddress:	<input checked="" type="checkbox"/>	
postalCode:	<input checked="" type="checkbox"/>	

Add Cancel Help

Using DMT

- View or edit schema



QSHLL Utilities

- LDAP command line utilities can be invoked from QSH:
 - ▶ Idapadd, Idapmodify, Idapsearch, Idapdelete, Idapmodrdn
- 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

QSHHELL Utilities

■ ldapsearch examples

```
> ldapsearch -h rchas510 -D cn=administrator -w secret -b "DC=LPAR2NZM,DC=RCHLAND,DC=IBM,DC=COM"
      "(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=*)')

LDIF Files

- LDIF is the LDAP data interchange format; an industry standard.
- Way to transfer directory data between LDAP servers; export from one, import into another.
- Simple text file format.
- Sequence of lines that describe either an entry or a set of changes to an entry.
- The order of entries in the file is important.
- To add an entry, the parent entry must first exist in the namespace.
- The specific format and contents of the LDIF file are determined by the schema.
- The servers used for export and import need to support the same part of the schema.

Example LDIF File

- Contents of mods.ldif:

```
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
```

QSHELL Utilities

- Idapmodify examples
 - ▶ Can be used to add, modify, delete and rename entries via 'changetype' directive.
 - ▶ Example using an LDIF file.

```
> Idapmodify -D cn=admin -w secret -f mods.ldif
```


Summary

- You've learned:
 - ▶ LDAP terminology and advanced concepts
 - ▶ Authentication methods
 - ▶ How to configure the server the first time using the wizard
 - ▶ How to start and stop the server
 - ▶ Access control and groups
 - ▶ How to publish information to the server
 - ▶ Examples of entries and LDIF files
 - ▶ GUI tools for accessing and managing the server
- What's next?
 - ▶ Gain hands on experience now
 - 440178: OPEN LAB: IBM Directory Server (LDAP)
 - ▶ Back at the office
 - Design a simple directory, configure your LDAP server and create your first directory
 - ▶ Read advanced information

LDAP Open Lab

- 430242: LAB: IBM Directory Server (LDAP)
 - ▶ Start and stop the server
 - ▶ Configure the server
 - ▶ Search entries in the directory
 - ▶ Create a suffix and add new directory entries
 - ▶ Work with directory data (delete/modify)
 - ▶ Import/export data using LDIF files
 - ▶ Use DMT
 - ▶ Work with the schema
 - ▶ Work with the changle log

- 440144: LAB: Using LDAP Authentication with Apache
 - ▶ Create an HTTP server
 - ▶ Configure HTTP server to connect to LDAP server
 - ▶ Protect a web page using LDAP authentication

For More Information

- iSeries LDAP home page: www.ibm.com/eservers/series/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: www.ibm.com/software/network/directory/
- Redbooks: 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)
- Java programming using JNDI, read Sun's JNDI tutorial section "Tips for LDAP Users": java.sun.com/products/jndi/docs.html
- "e-Directories Enterprise Software, Solutions, and Services. ISBN 0-201-70039-5. Published by Addison-Wesley Professional.

Appendix

- LDAP - Lightweight Directory Access Protocol
- RFC - Request for Comments
- LDIF - LDAP Data Interchange Format
- API - Application Programming Interface
- PKI - Public Key Infrastructure
- CRL - Certificate Revocation List
- EIM - Enterprise Identity Mapping
- SDD - System Distribution Directory
- QOS - Quality of Service

Trademarks and Disclaimers

© IBM Corporation 1994-2003. 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
AS/400e	IBM (logo)
eServer	iSeries
	OS/400

Lotus and SmartSuite are trademarks of Lotus Development Corporation and/or IBM Corporation in the United States, other countries, or both.

MMX, Pentium, and ProShare are trademarks or registered trademarks of Intel Corporation in the United States, other countries, or both.

Microsoft and Windows NT are registered trademarks of Microsoft Corporation 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.

SET and the SET Logo are trademarks owned by SET Secure Electronic Transaction LLC.

C-bus is a trademark of Corollary, Inc. in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product or 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.