Session: 420033

What Can LDAP Do For Me?

IBM eserver iSeries

John McMeeking

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.

IBM eserver. For the next generation of e-business.

Agenda

- What is LDAP?
- Why Use LDAP?
- IBM and iSeries Directory Offerings

What is LDAP?

LDAP in a Nutshell

- LDAP - Lightweight Directory Access Protocol
- de-facto Internet (TCP/IP based) wire protocol for accessing and updating directory information
- "V3" defined in IETF RFCs 2251-2256, 2829, 2830
- New RFCs all the time (e.g. RFC 2849 - LDIF format)
- Protocol defines interfaces between a client and a server for requesting and returning information

LDAP in a Nutshell

- Simple and interoperable APIs

- Core schema enables common data access

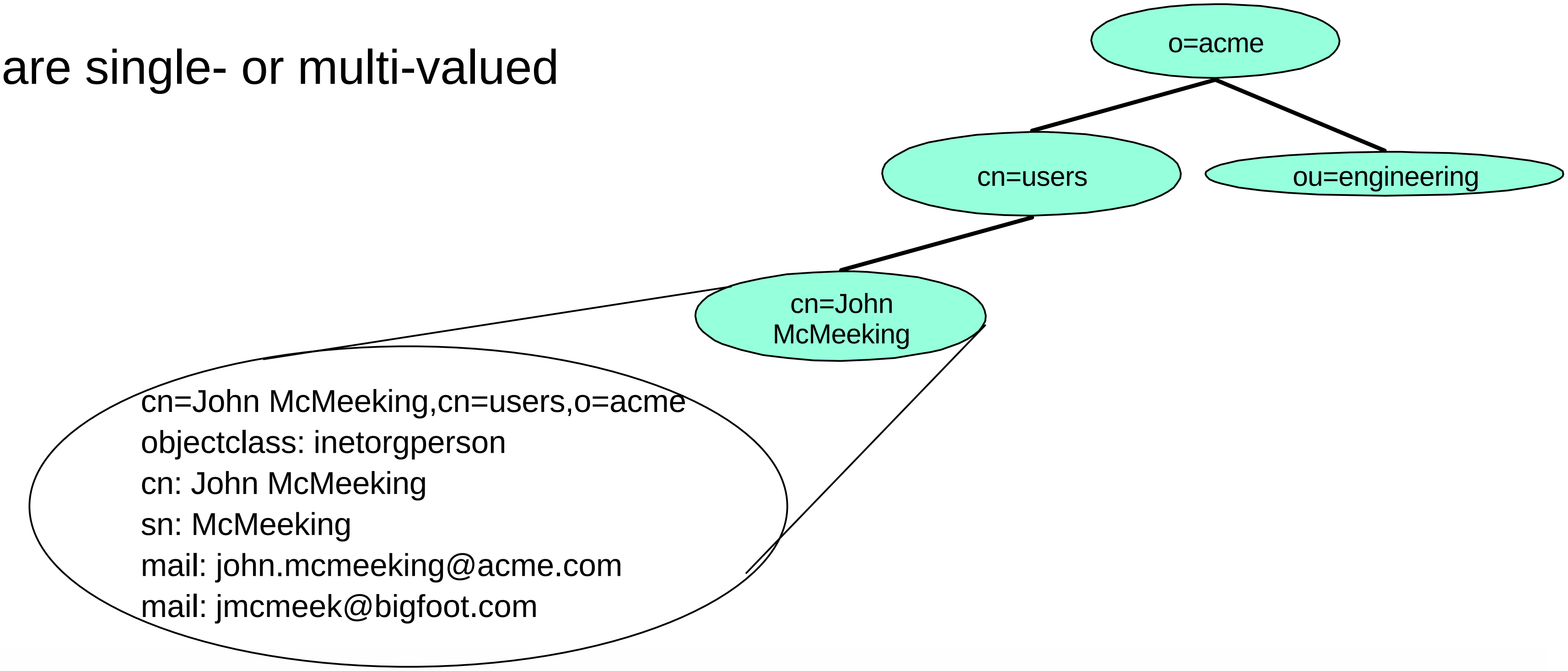
- Integrated into many products:
  - Most e-mail clients: MS Exchange, MS Outlook, Netscape, Notes, ...
  - Public key infrastructure
  - Network components and more coming

- Server vendors include:
  - Netscape/iPlanet Directory Server, Microsoft Active Directory, Novell e-Directory, IBM Directory Server (formerly SecureWay Directory)
  - Virtual directory and meta-directory products also available

Directory Information Model

- An LDAP Directory is formed by a hierarchy of "entries"

- Each "entry" has:
  - a name (called a distinguished name)
  - a structure (called an "object class")
  - attributes
  - attributes are single- or multi-valued



cn=John McMeeking,cn=users,o=acme
objectclass: inetorgperson
cn: John McMeeking
sn: McMeeking
mail: john.mcmeeking@acme.com
mail: jmcmeek@bigfoot.com

Directory Information Model

- An Entry's "object class" defines
  - structure of an entry
  - attributes that MUST be present in an entry
  - attributes that MAY be present in an entry

```
( 2.5.6.6 NAME 'person'
  DESC 'Defines entries that generically represent people.'
  SUP top
  STRUCTURAL
  MUST ( cn $ sn )
  MAY ( userPassword $ telephoneNumber $ seeAlso $ description ) )
```

- An individual Entry in the directory can take on the form of multiple object classes
  - The attributes in the entry are the UNION of those defined for individual object classes

Directory Information Model

- Attributes are defined by their name, syntax, and matching rule(s)
  - Syntax refers to the type of data stored in attribute values
    - Examples: DirectoryString, Binary, Integer, Boolean
  - Matching Rules define how equality and ordering comparisons are performed on attribute values
    - Examples: caseIgnoreMatch, caseExactMatch, octetStringMatch

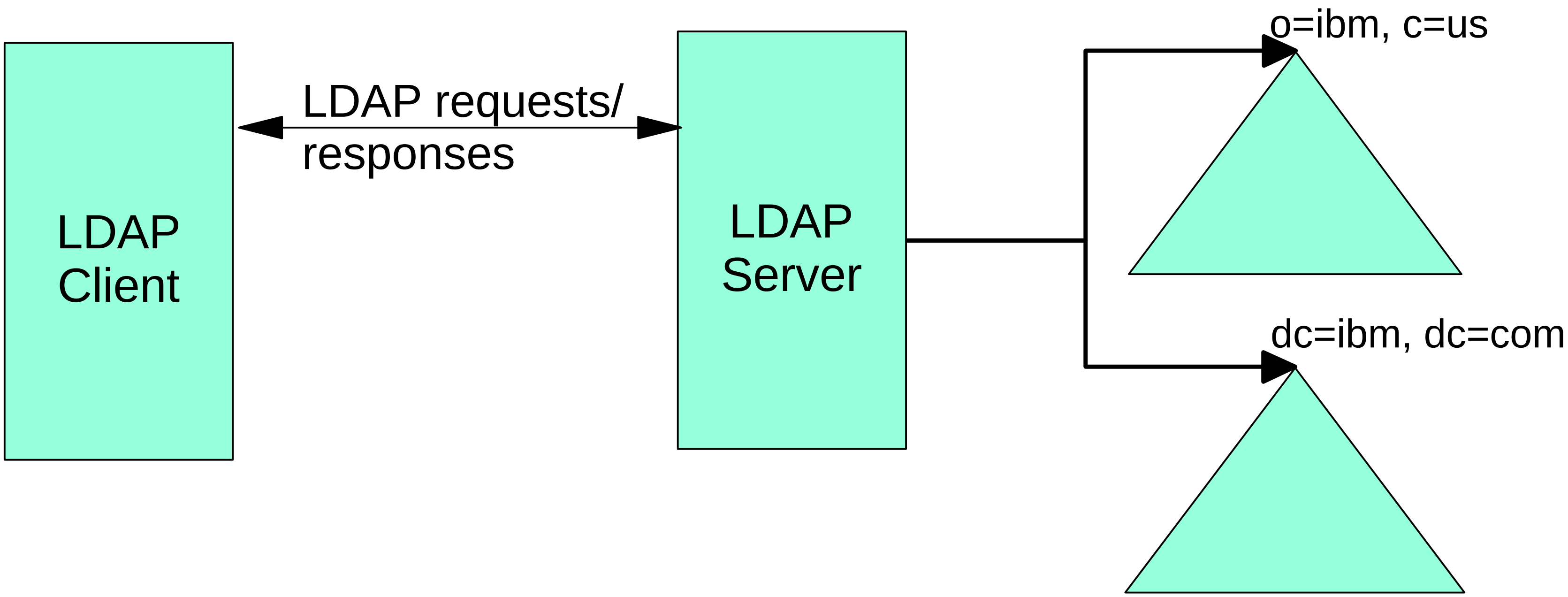
- Different attributes within an entry may be more "sensitive" than others within an entry
  - Example: cn (common name) vs. uid vs. userPassword
  - Within IBM servers, attributes are assigned to access classes (normal, sensitive, critical) with rights to data based on the access class
  - Many servers (including IBM) also support access control based on specific attributes
  - Examples: anybody can read "normal" attributes, or the "mail" attribute, members of the administrators group can write to userPassword.

Directory Information Model

- Search criteria
  - Base DN - o=acme
  - Search Scope - object, one level or subtree
  - Filter - sn=McMeeking or more complex: objectclass=printer and location=...
- Supports two styles of queries
  - "whitepages" queries: retrieve a entries with known names
  - "yellowpages" queries: look for entries matching specific criteria
- Filters support
  - AND/ORing components
  - existance of values, =, >=, <=, approximate, wildcards

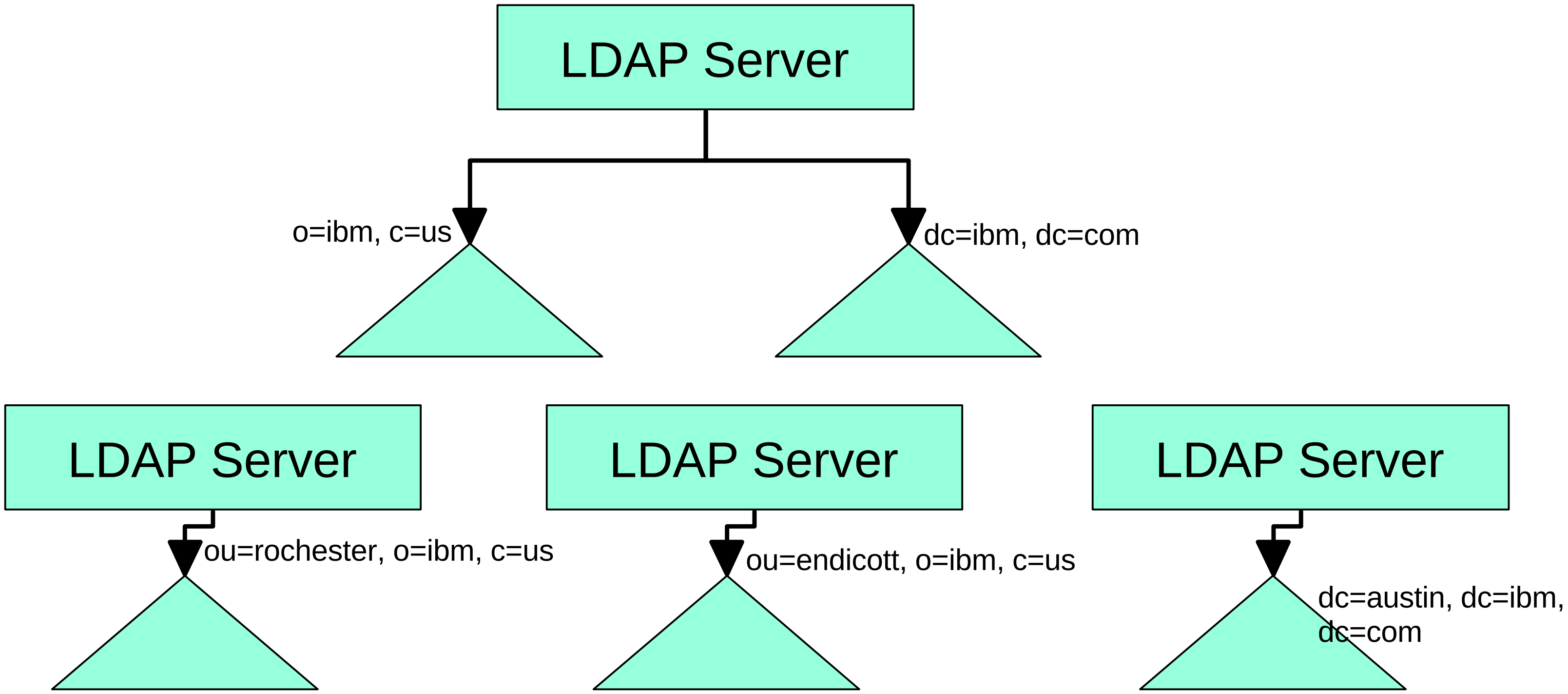
Directory Servers

- A Directory Server
  - Accepts and responds to directory requests
  - Manages a portion (set of "sub-trees") of a directory "namespace"
  - Can contain referrals or "search continuation references". These are "chased" by the client, not the server.



Directory Service

- A Directory Service
  - is a set of servers which, together, serve a directory "namespace"
  - is a value to the Enterprise, across the Enterprise



Directory Clients

- LDAP client programming APIs
  - C/C++
  - Java through JNDI or Java LDAP (JDAP)
  - Directory Services Markup Language (DSML) can make LDAP a web service
- Applications that use the APIs
  - mail clients, web servers, ...
- Command-line tools to access/update the directory
  - ldapsearch, ldapmodify, ldapdelete, ...
- General LDAP "browser" GUIs
  - Directory Management Tool
  - LDAP Browser/Editor

Why Use LDAP?

Why use a Directory?

- Provides a place to store information that is accessible from multiple locations
- Provides a place to look up where to find other information or servers
- Provides a place to make information accessible to multiple applications
- If you have information that needs to be managed centrally but used across your enterprise, a directory can help

Why not use something else?

- You could use a database, flat files, or... but:
  - Information (like identities) must be redefined each time
  - You have yet another database for your administrators to manage
  - Can you easily access it from multiple applications (written by multiple vendors and running on multiple platforms)?
  - How do you manage authentication and access control?
- LDAP accessible directory is something lots of folks can agree on, particularly for identity and authentication.

What can be stored in a Directory?

- Directories can store just about any type of information
- Basic data types are string, integer, boolean, and binary
- Binary data can range from a few bytes to megabytes in size
- Directories are usually tuned to favor high read rates at the expense of lower write (add/modify/delete) rates
- Store information in the directory that is relatively static but used across your application environment (enterprise, e-business applications, etc.)

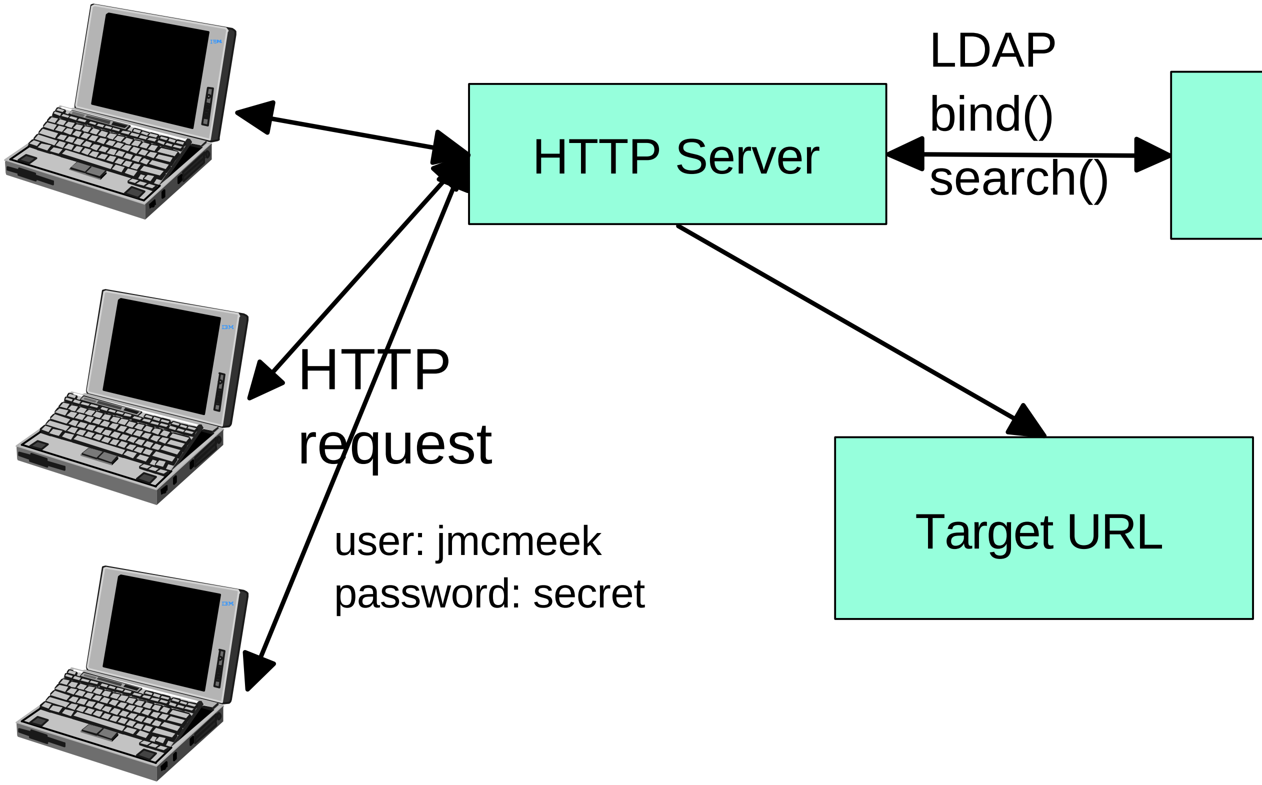
What types of applications use a directory?

- Single sign-on frameworks
- Enterprise phone books
- Distributed access control checkers
- Centralized configuration database
- Distributed object look-ups
- Web application personalization
- Directory for PKI environments (certificates and CRLs)

LDAP usage in the enterprise

- HTTP server Authentication and Access Control
- Websphere EJB Naming
- Tivoli SecureWay Policy Director User Registry
- IBM "Bluepages" internal phone book

HTTP Authentication and Access Control



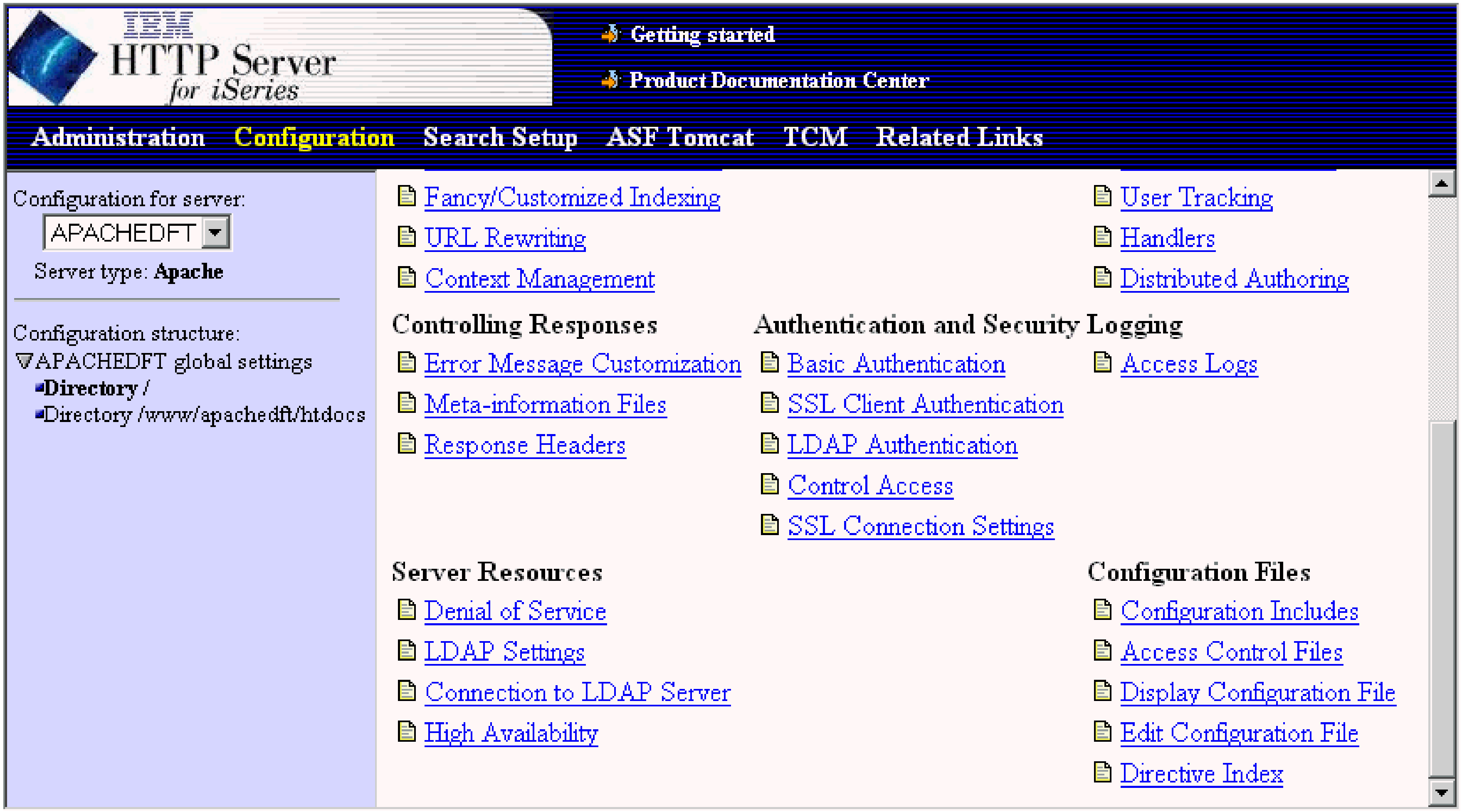
When users attempt to access a URL, the web server will:

- ➤ use LDAP directory for authentication
- ➤ determine group membership based on LDAP directory
- ➤ determine access to URL

dn: cn=john mcmeeking,cn=users,o=acme
objectclass: inetOrgPerson
uid: jmcmeek
userPassword: secret

dn: cn=developers, cn=users,o=acme
objectclass: groupOfNames
member: cn=John McMeeking,cn=users,...
member: cn=Marla Berg,cn=users,...

IBM HTTP Server for iSeries (powered by Apache)



Configuration for server: APACHEDFT

Server type: **Apache**

Configuration structure:

▽APACHEDFT global settings
- **Directory /**
- Directory /www/apachedft/htdocs

Fancy/Customized Indexing
URL Rewriting
Context Management

User Tracking
Handlers
Distributed Authoring

Controlling Responses
- Error Message Customization
- Meta-information Files
- Response Headers

Authentication and Security
- Basic Authentication
- SSL Client Authentication
- LDAP Authentication
- Control Access
- SSL Connection Settings

Logging
- Access Logs

Server Resources
- Denial of Service
- LDAP Settings
- Connection to LDAP Server
- High Availability

Configuration Files
- Configuration Includes
- Access Control Files
- Display Configuration File
- Edit Configuration File
- Directive Index

- Detail information in Redbook: LDAP Implementation and Practical Use SG24-6193.

Domino Server and LDAP

- Domino for iSeries provides services to simplify user and system mangement and provides a flexible directory infrastructure.

- Domino Directory Services includes:
  - Directory Catalog - An aggregation of directories located on either the server or client.
  - Directory Assistance - Provides access to federated directories that can include secondary Domino directories or third-party LDAP directories (ie iSeries Directory Services (LDAP) server).
  - Domino LDAP server task - This is the Domino LDAP server that runs on the Domino server and provides LDAP v3 access to Domino and third-party directories for both clients and applications.

- Lotus Domino Release 5 consists of a primary Domino Directory and can combine secondary Domino directories, Directory Catalogs, Directory Assistance database and LDAP service.

Domino Server and LDAP *(continued)*

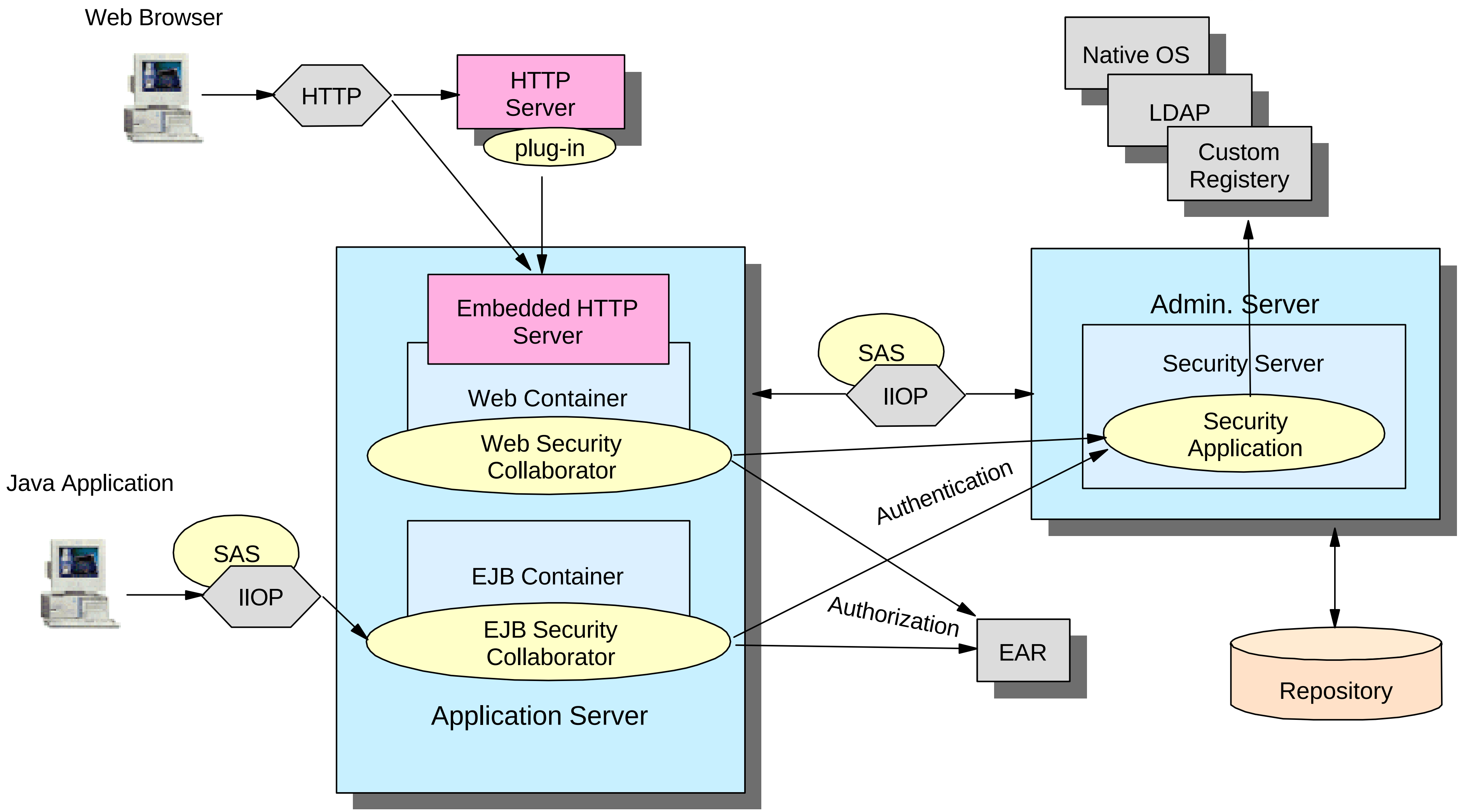
- You can use Directory Assistance to refer LDAP Lotus Notes clients that connect to the Domino LDAP service to another LDAP directory.
- Mail address lookup and resolution service can include LDAP directories. LDAP service can use the Directory Catalog and Directory Assistance together to process LDAP searches, providing the functionality of both.
- Detail information on Setting up and using LDAP on Domino Server for iSeries can be found in Redbook: LDAP Implementation and Practical Use SG24-6193.

WebSphere and LDAP

- WebSphere Application Server security supports either local OS authentication or Lightweight Third Party Authentication (LTPA). For LTPA, users are defined in an LDAP directory (Domino, IBM Directory, iPlanet)

- IBM WebSphere Application Server provides a number of features that can be used to secure applications:
  - Authentication policies and services that verifies the identity of a user.
  - Authorization policies and services that determines if a user has rights to use a secured resource in some way.
  - Single sign-on support - Websphere supports third-party authentication across the Internet domain that controls your resources and allows users to log on once per session vs logging on to each application separately.
  - LDAP over Secure Sockets Layer (SSL) is supported between the WebSphere security server and the LDAP server.

WebSphere Advanced Edition security architecture



- Detail information on using LDAP with WebSphere can be found in Redbook: LDAP Implementation and Practical Use SG24-6193.

IBM and iSeries Directory Offerings

IBM Directory Server

- IBM Directory Server (formerly IBM SecureWay Directory and IBM eNetwork Directory) -- current release is 3.2.2 (Sept 2001)
  - Server
    - DB2 backend
    - Web administration GUI
    - AIX 4.3.3 or later, Windows NT 4.0 and 2000, Linux (SuSe, Turbo Linux, Red Hat, and Linux 390), Solaris
    - GSKit SSL support
  - Directory Client SDK
    - Command line utilities
    - C APIs
    - Directory Management Tool (Java directory content management GUI)
    - Also available for Windows 9x and HP-UX
- z/OS LDAP server is closely related

iSeries Directory Services

- Introduced in V4R3
  - Option 32 through V4R5
  - Included in base OS with V5R1
- Based on the IBM Directory
  - V5R1 is equivalent to IBM SecureWay 3.2
- Includes:
  - LDAP V3 server (V2 prior to V4R5)
  - ILE C APIs (callable from other ILE languages)
  - QSHELL utilities
  - Operations Navigator configuration/administration GUI
  - Publishing services
  - Directory Client SDK for Windows (includes DMT)

Server features

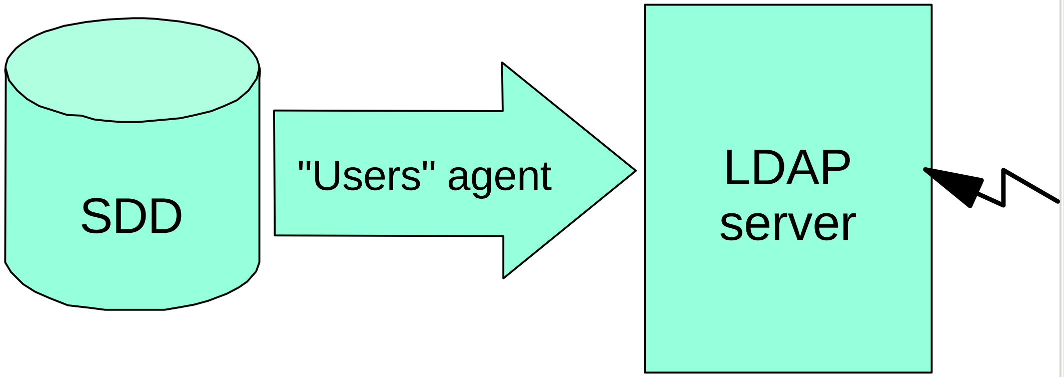
- LDAP V3 RFC support (RFCs 2251-2256, others)
  - Does not support modify DN with new superior (i.e. move)
- NLS Data support using UTF-8
- Large, extensible schema
  - Base schema includes about 250 object classes and 1050 attribute types
  - Add new schema via standard APIs, LDIF files, DMT, etc.
- Security Features:
  - Various authentication methods (DN/password, Kerberos, digital certificate)
  - Access control model
  - Secure connections using SSL and TLS
  - Encrypted or hashed passwords stored in validation lists
  - Server auditing integrated with operating sytem audit journal support
- Limited transaction and event notification support (not standards based)

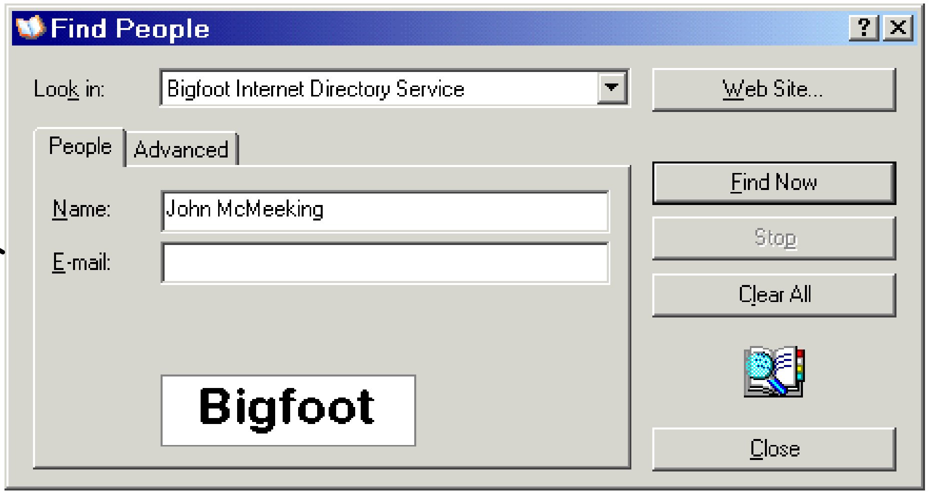
Client Features

- Based on Internet draft for LDAP C API
- Standard LDAP APIs:
  - ldap_init, ldap_bind, ldap_modify, ...
- Server Configuration APIs
- QSHELL utilities:
  - ldapsearch, ldapadd, ldapmodify, ldapdelete, ldapmodrdn
- Java Naming and Directory Interfaces (JNDI)
  - Use Sun LDAP provider (J2EE 1.3) or IBMJNDI provider (1.2.2 and earlier)
    - Sun provider is part of J2EE 1.3, can also be downloaded to use with J2EE 1.2

Publishing Services

- Framework for "publishing" information to LDAP
  - "agent" allows application to be isolated from knowledge of the destination server
  - "engine" provides reliable connection to server.
    - Establishes authenticated connection to appropriate server
    - Determines proper location in directory to create entries
    - Retries operations in event of failure
- System defined publishing agents for SDD, system configuration, printers
- User defined publishing "agents"



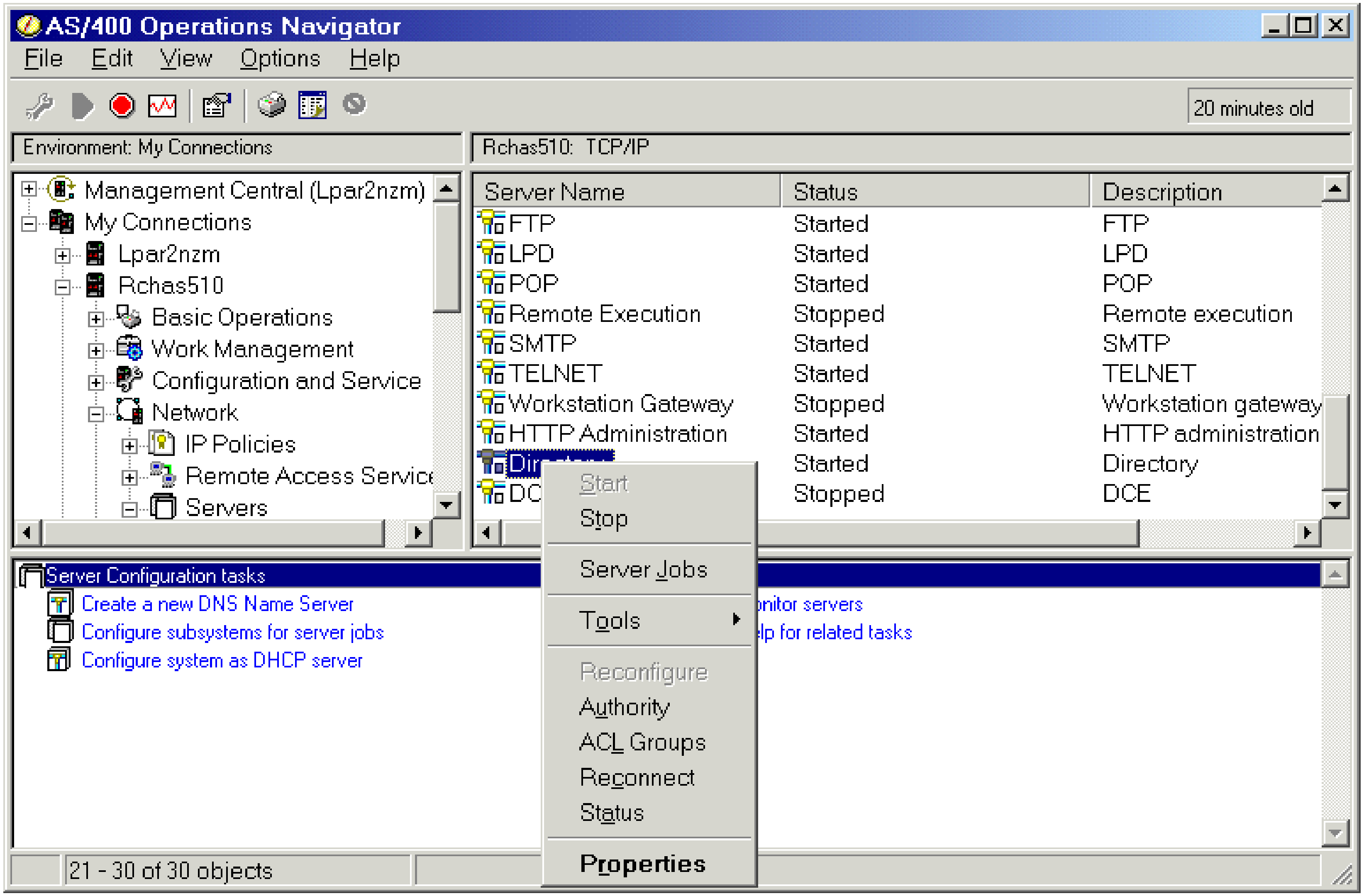


Look in: Bigfoot Internet Directory Service

Name: John McMeeking

E-mail:

Operations Navigator



Server Name	Status	Description
FTP	Started	FTP
LPD	Started	LPD
POP	Started	POP
Remote Execution	Stopped	Remote execution
SMTP	Started	SMTP
TELNET	Started	TELNET
Workstation Gateway	Stopped	Workstation gateway
HTTP Administration	Started	HTTP administration
Dir	Started	Directory
DC	Stopped	DCE

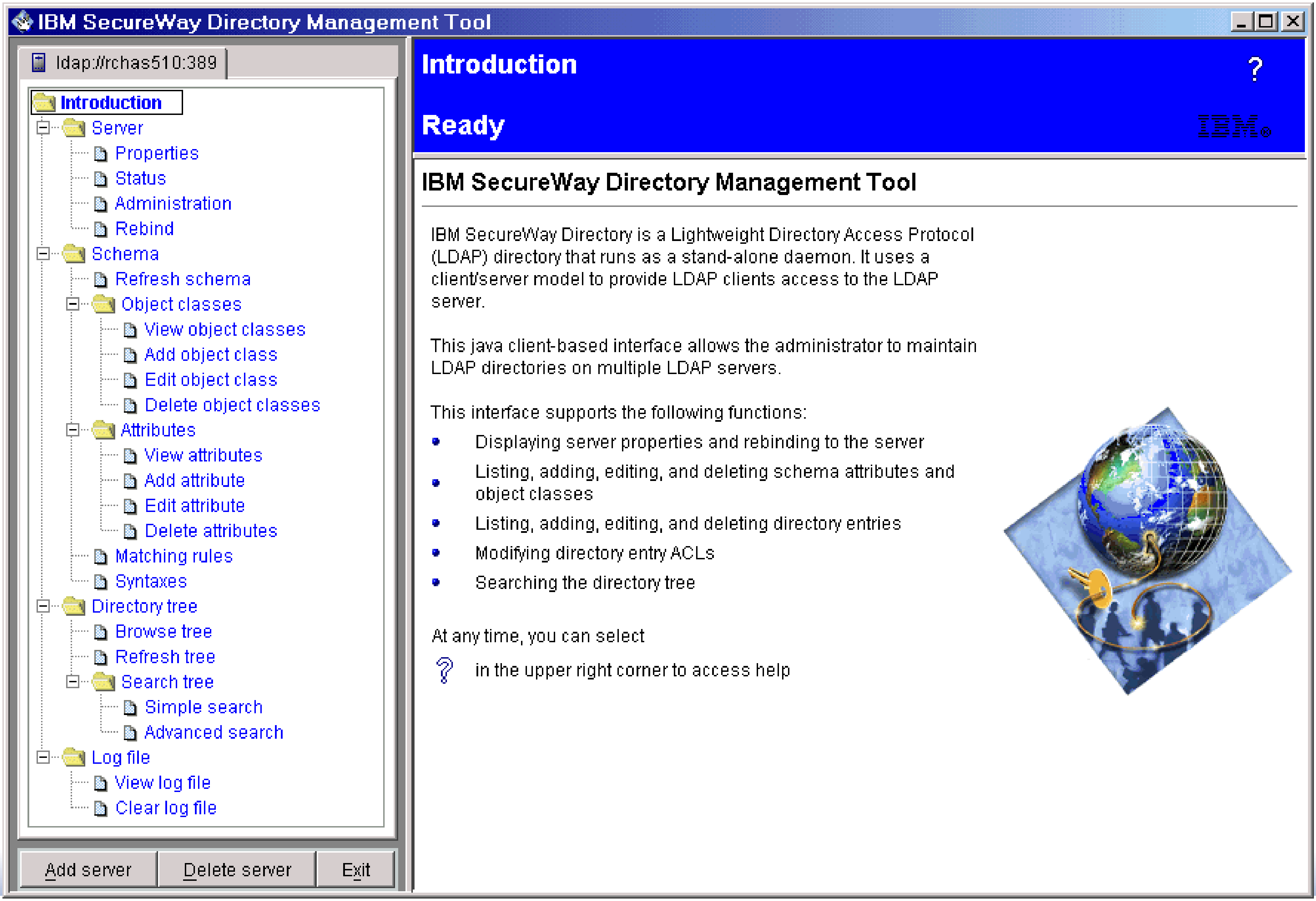
Server Configuration tasks

- Create a new DNS Name Server
- Configure subsystems for server jobs
- Configure system as DHCP server
- nitor servers
- lp for related tasks

21 - 30 of 30 objects

Directory Management Tool

IBM eserver iSeries



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

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.

Trademarks and Disclaimers

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
AS/400e
e (logo) business
IBM
IBM(logo)
iSeries
OS/400
DB2
WebSphere
AIX
z/OS
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.