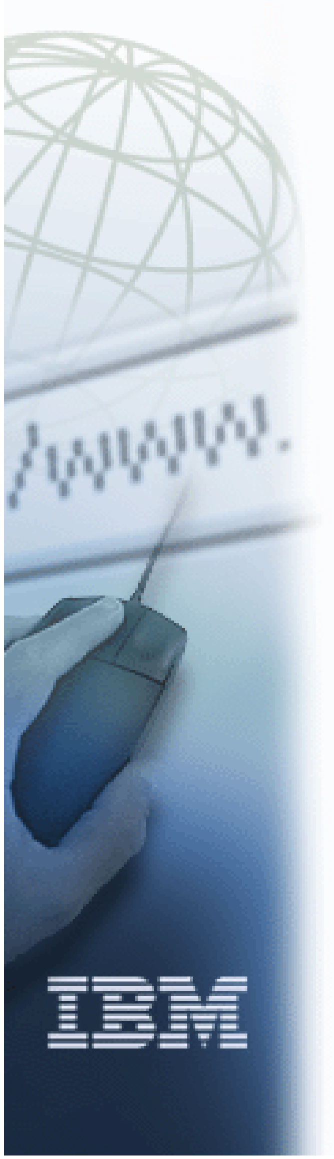
ibm.com

e-business



LDAP, Domino and iSeries
The Redbook

13MA

COMMON US, Spring 2002

John Taylor

Redbooks

International Technical Support Organization

Abstract

LDAP directories provide phone and e-mail addresses and help to manage server access, authorize B2B users, find experts via Knowledge Management and share a single signon. This presentation introduces directory concepts and shows how to implement Directory Services (LDAP) on the iSeries server. It also provides an overview of how to integrate and manage OS/400 with WebSphere, Domino Directory and other LDAP-enabled applications using OS/400 LDAP Directory Services.

Acknowledgments

Thanks to the following people who contributed to this presentation and the new IBM Redbook *Implementation and Practical Use of LDAP on the IBM eServer iSeries Server*, SG24-6193 during an ITSO residency at the Raleigh, North Carolina center:

• Wolfgang Eckert	- IBM Germany
• John Taylor	- Typex Group plc, United Kingdom
• Klaus Tebbe	- IBM Germany
• Wendy Thomson	- Contractor with IBM Australia
• Marc Willems	- IBM Belgium

The lead author of the presentation and redbook was Tom Barlen from the IBM ITSO Raleigh, North Carolina center.

Agenda

- Introduction to directories
- Directory & LDAP concepts
- Directory Support on iSeries
- Management of directories
- LDAP and Applications
- Redbooks & More Information
- Suggested Actions

Everything you learn during this presentation and much more is covered in the new IBM Redbook:
***Implementation and Practical Use of LDAP on the IBM eServer iSeries Server*, SG24-6193**

1. Introduction to directories

What is a Directory?

A list of information about people or objects, arranged in order and with associated attributes for each object, which can be searched on multiple criteria

Examples:

- telephone directory
  - name, address, phone number
- library card catalog
  - author, title, ISBN number
- Often used for e-mail

It is a specialized database

- optimized for read and search, not for update
- No SQL, ODBC or Referential Integrity

It is not the same as a file system directory (folder)

Notes What is a Directory?

A Directory need not be stored on a computer as some of the examples here show. However, many directories are now computerized. It functions as a specialized database and may indeed use a database as its underlying technology, but it does not usually support the standard database interfaces that we expect nowadays.

Be careful to distinguish between this form of directory and the former use of the term for the file system sub-tree that, for instance, is revealed by use of the DOS DIR (Directory) command. The latter refers to a container for discrete objects on disk. It is more commonly referred to nowadays, at least in Windows terminology, as a folder.

Directory Uses & Advantages

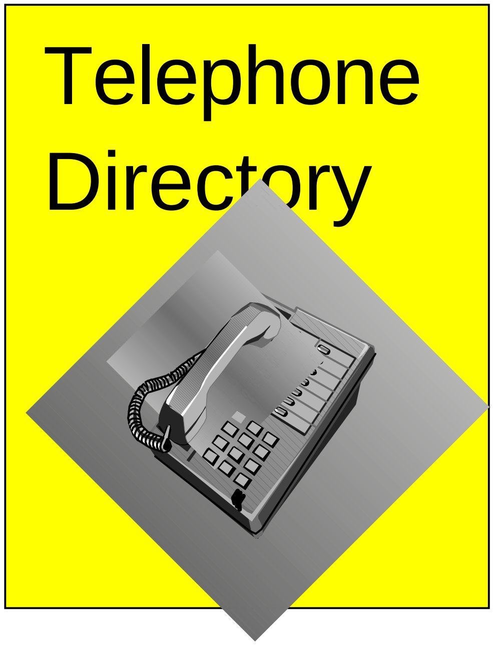
Uses

- E-mail
- People directories
- Authentication

...You use them every day

Advantages

- Find People
- Single Sign-On
- Faster Application Development
- Standards based



Telephone Directory

User registry

Notes Directory Uses & Advantages

The main use of computerized directories with which people will be familiar is for E-mail. Those of us who use e-mail use directories every day, perhaps without even thinking about it, for looking up addresses.

The advantages include

- Users can more quickly find people
- They can use Single Sign-On to multiple applications with a single UserID/Password combination
- Developers can achieve faster development of applications without having to design authentication into every application themselves. They can reuse authentication information and mechanisms provided with, for example, LDAP-based directories. Another advantage for developers, especially when developing Java applications, is that they can share elements, such as buttons or icons between different applications. The can publish these objects in serialized form to a directory. Using this approach, changes to, for example, a corporate design can be easily and quickly deployed.
- The standards based nature of directories which means that applications can be more portable

Existing People Data

Where is the existing data on people?

- Printed Telephone Lists
- Telephone PABX
- Organizational charts
- E-mail directories
- Human Resources applications
- Accounting systems
- Marketing and CRM databases
- Helpdesk applications
- Web enrollments

Where do you store your passwords?

- Passwords for office telephone system, house security alarm, office keypad/security alarm, credit cards, online banking, frequent flyer online, calling card, plus those you use on behalf of others.

You can consolidate all of these with a Directory

Notes Existing People Data

This chart tries to explore the wide variety of places and forms in which the information about a single person may be stored within an organization. In addition, we all keep an ever-growing volume of personal data which we need to maintain. A directory would help us to reduce the volume of this data, to store it more securely and to manage it more easily.

PABX = Public Access Branch eXchange

Directory Product Examples

Lotus Domino Directory

IBM SecureWay Directory

OS/400 System Distribution Directory

Novell NetWare eDirectory, Oracle, Netscape.....

Windows 2000 Active Directory

plus public LDAP

- Yahoo People Search
- Bigfoot
- InfoSpace
- Switchboard
- VeriSign
- WhoWhere

Notes Directory Product Example

This foil simply lists some of the main directory products by way of illustration that directories are in widespread use across many platforms.

Other directory services are available publicly without our needing to be aware of the underlying directory product.

2. Directory Concepts and Plans

Directory Standards: X.500 & LDAP

X.500

- Original OSI standard for directories

Lightweight Directory Access Protocol

- Was an IP-based way of accessing previous X.500
- Now an Internet-based standard of its own
  - X.500 structure is still largely the basis
  - Defined in IETF RFCs
- Well supported (IBM, Microsoft, Novell, Netscape, etc.)

What exactly is LDAP?

- LDAP is not a directory itself
- It is an access protocol. Directories that can be accessed via LDAP are often referred to as LDAP directories.

LDAP V3 is the latest release

- Now well established

Notes Standards: X.500 & LDAP

Open Systems Interconnection (OSI) X.500

X.500 was the original standard for directories agreed by the OSI standards body.

- International standard
- Well structured content
- Heavy communications overhead

Issues

- However, the communications overhead of X.500 was too high for many customers
- A TCP/IP-based access method was required

LDAP

The Lightweight Directory Access Protocol (LDAP) is an open industry standard that has evolved to meet the need for a variety of directory-based information to be maintained and accessed in a consistent and controlled manner.

LDAP defines a standard method for accessing and updating information in a directory. LDAP has gained wide acceptance as the directory access method of the Internet and is therefore also becoming strategic within corporate intranets. It is being supported by a growing number of software vendors and is being incorporated into a growing number of applications. For example, the two most popular Web browsers, Netscape Navigator/Communicator and Microsoft Internet Explorer as well as application middleware, such as WebSphere Application Server or the IBM HTTP Server support LDAP functionality as a base feature.

Note that LDAP is not a standard for directories themselves but for a method of accessing them.

LDAP V3 (and its sub-releases) is the latest standard with which virtually all directories now comply.

LDAP Structure

Largely based on X.500 content definitions

Directory stores and organizes *entries*

Entry

- Describes an object
  - e.g. person, printer..
- Has attributes, each with a type and value
  - for example, `type=telephoneNumber, value=191-256-4406`

Schema

- Defines
  - what object classes are allowed where
  - what attributes are required
  - what attributes are optional
  - syntax of attributes

Notes LDAP Structure

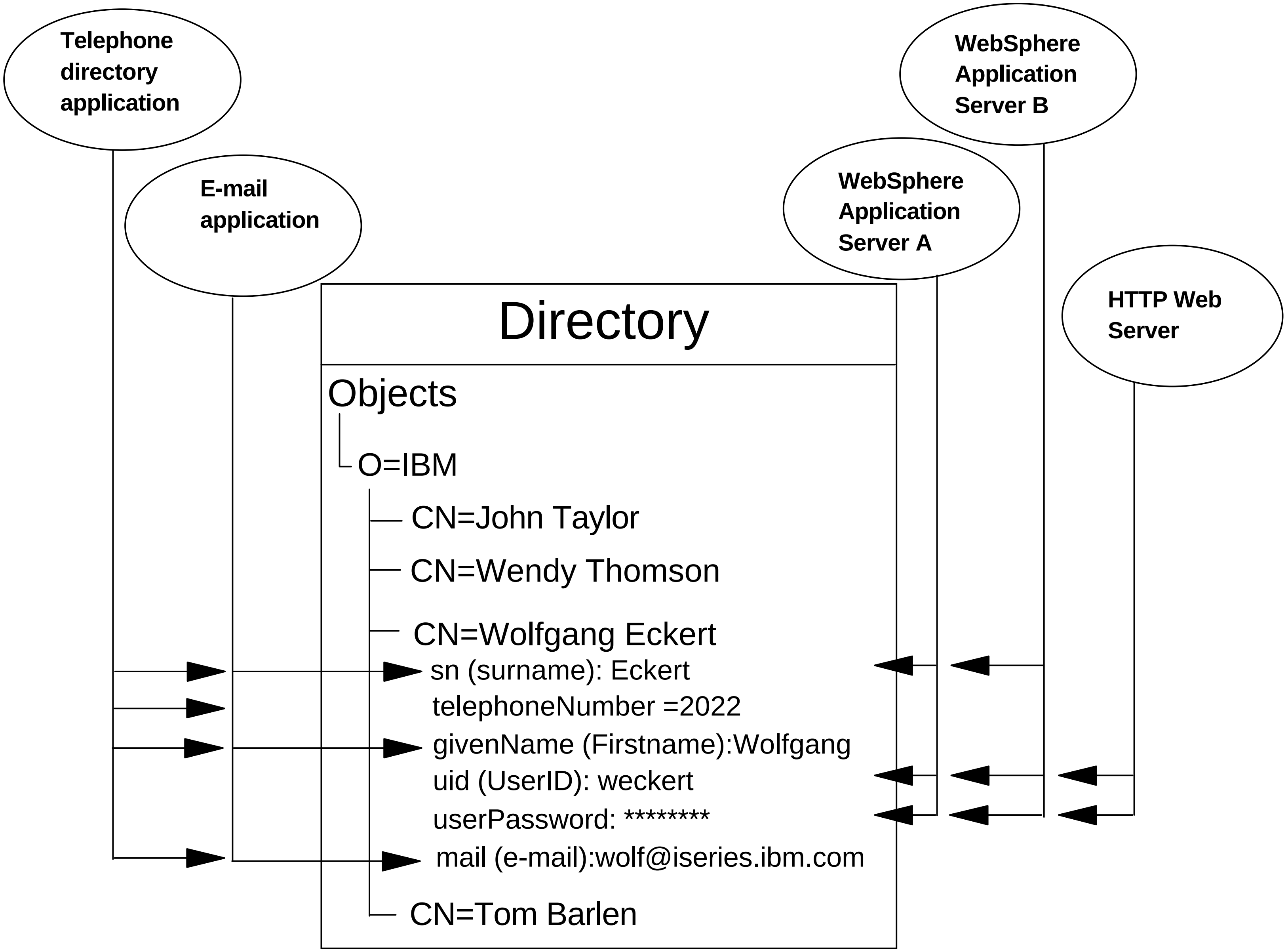
The structure of LDAP definitions is largely based on X.500 content definitions.

An LDAP-enabled directory stores and organizes 'entries'. An Entry

- describes an object, e.g. a person or printer..
- has attributes, each with a type and value, e.g. type=telephoneNumber, value=191-256-4406

All the objects and attributes with their characteristics are defined in Schemas. The schema specifies what can be stored in the directory. Schema-checking ensures that all required attributes for an entry are present before an entry is stored. Schema-checking also ensures that attributes not in the schema are not stored in the entry. Optional attributes can be filled in at any time. A schema also defines the inheritance and sub-classing of objects and where in the Directory Information Tree (DIT) structure (hierarchy) objects may appear.

Directory Entry



Telephone directory application

E-mail application

WebSphere Application Server B

WebSphere Application Server A

HTTP Web Server

Directory

Objects

O=IBM

CN=John Taylor

CN=Wendy Thomson

CN=Wolfgang Eckert

sn (surname): Eckert

telephoneNumber =2022

givenName (Firstname):Wolfgang

uid (UserID): weckert

userPassword: ********

mail (e-mail):wolf@iseries.ibm.com

CN=Tom Barlen

LDAP Structure, contd.

Object class

- A general description of an object, like a template
  - for example, Person, inetOrgPerson
- Described for each server by schema
- Listed in entry's *objectclass* attribute, one or more
  - for example, Person + residentialPerson + organizationalPerson

Directory Information Tree (DIT)

- Arranges entries hierarchically based on 'distinguished name'

Distinguished Name (DN)

- A unique ID, a *primary key*
- A sequence of *relative distinguished names* (RDNs)
  - like a path of directory names in a file name
    - for example, cn=John Smith, ou=ITSO, o=IBM, c=US

Notes LDAP Structure

Object class

Each entry in a directory belongs to one or more object classes. An object class describes the content and purpose of the object. It also contains a list of attributes, such as a telephone number or surname, that can be defined in an object of that class.

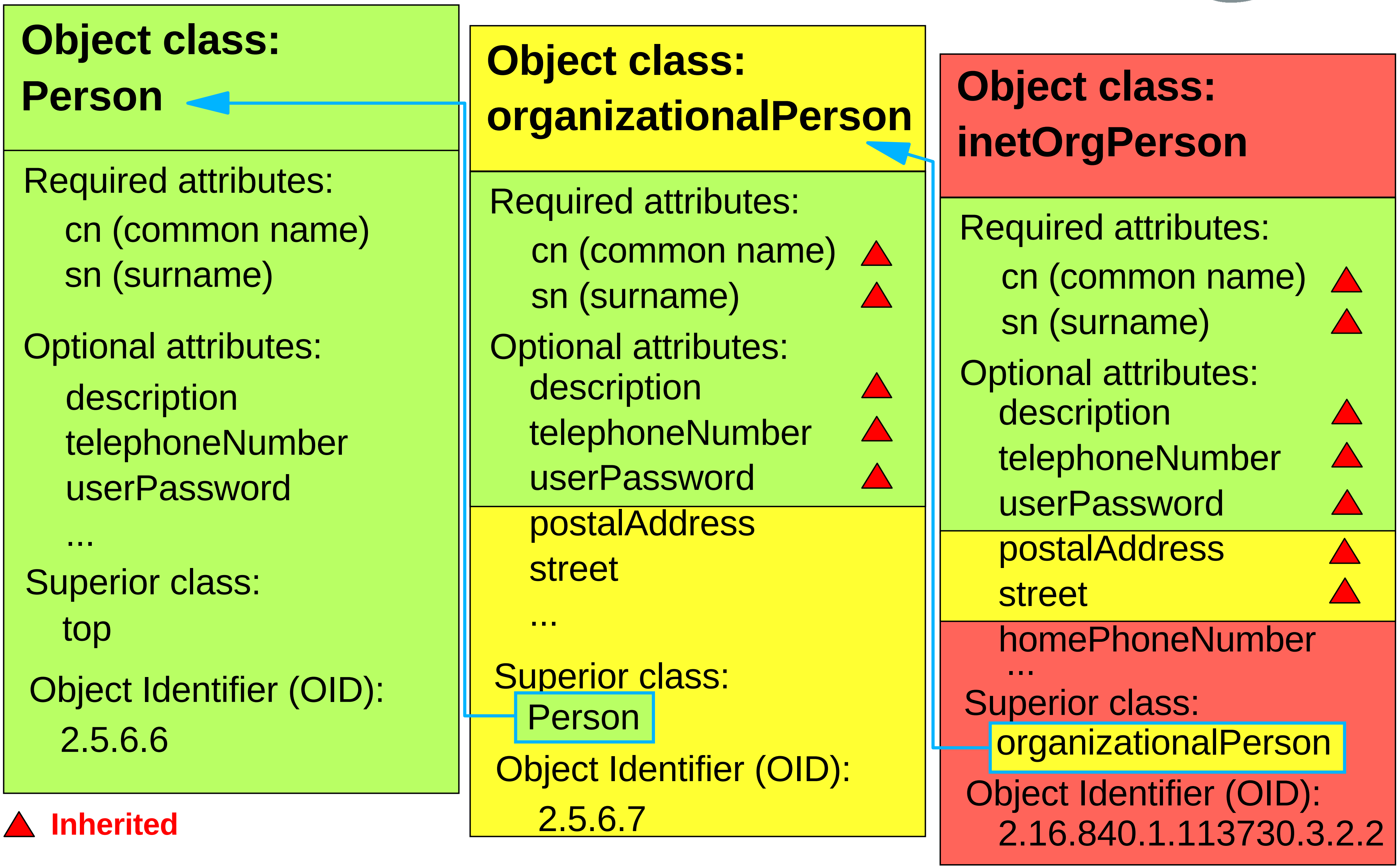
Directory Information Tree (DIT)

A directory contains a collection of objects organized in a tree structure. The LDAP naming model defines how entries are identified and organized. Entries are organized in a treelike structure called the Directory Information Tree (DIT). Entries are arranged within the DIT based on their distinguished name (DN).

Distinguished Name (DN)

A DN is a unique name that unambiguously identifies a single entry. It is like the primary key in a database file. DNs are made up of a sequence of relative distinguished names (RDNs). Each RDN in a DN corresponds to a branch in the DIT leading from the root of the DIT to the directory entry. A DN is composed of a sequence of RDNs separated by commas, such as cn=thomas,ou=itso,o=ibm.

Object classes - Inheritance



Object class: Person

Required attributes:
- cn (common name)
- sn (surname)

Optional attributes:
- description
- telephoneNumber
- userPassword
- ...

Superior class:
- top

Object Identifier (OID):
- 2.5.6.6

Object class: organizationalPerson

Required attributes:
- cn (common name) ▲
- sn (surname) ▲

Optional attributes:
- description ▲
- telephoneNumber ▲
- userPassword ▲
- postalAddress
- street
- ...

Superior class:
- Person

Object Identifier (OID):
- 2.5.6.7

Object class: inetOrgPerson

Required attributes:
- cn (common name) ▲
- sn (surname) ▲

Optional attributes:
- description ▲
- telephoneNumber ▲
- userPassword ▲
- postalAddress ▲
- street ▲
- homePhoneNumber
- ...

Superior class:
- organizationalPerson

Object Identifier (OID):
- 2.16.840.1.113730.3.2.2

▲ **Inherited**

Notes Object classes - Inheritance

Each object also referred to as entry in a directory belongs to one or more object classes. An object class describes the content and purpose of the object. It also contains a list of attributes, such as a telephone number or surname, that can be defined in an object of that class. You can publish entries of different object classes under another object.

The object class also defines which of the attributes must be defined (required) when creating an object of this class and which attributes are optional. As shown in the previous chart, the object class with the name Person has the required attributes sn and cn and several optional attributes that may or may not be filled in when creating a Person object. Object classes can also inherit characteristics, such as attributes from other object classes. In the example of the inetOrgPerson, the class inherits all the attributes that are defined in the classes organizationalPerson and Person. That means, when you create an inetOrgPerson object you have to define the sn and cn attribute and optionally you can specify all the optional attributes as defined in the Person, organizationalPerson, and inetOrgPerson class.

Also attributes themselves have certain characteristics. The surname (sn) attribute name, for example, is defined as sn and surName, and describes a person's family name. The attribute definition specifies also the syntax rules for the attribute value. A telephone number may only contain numbers and hyphens while the surname consists of alpha characters.Other specifications include whether this attribute can contain only one or many values, the matching rules, the Object Identifier (OID), and so forth. The IBM SecureWay Directory product as used on the iSeries server provides also some IBM proprietary extensions. Other manufactures, such as Microsoft have similar extensions. The IBM extensions on the iSeries server include also an access class, which is used in combination with Access Control Lists (ACLs) to control who can perform a certain action on the attribute value, such as read, write, search, or compare operations.

The object identifier (OID) is a unique identifier in ASN.1 notation for an object class or an attribute. The OIDs defined in commercially available directory solutions are registered with a public organization, such as the ANSI organization (//www.ansi.org) for the United States. The number notation refers to a hierarchy. A Web site that allows you to query OIDs to determine their meaning is:

`http://www.alvestrand.no/objectid/index.html`

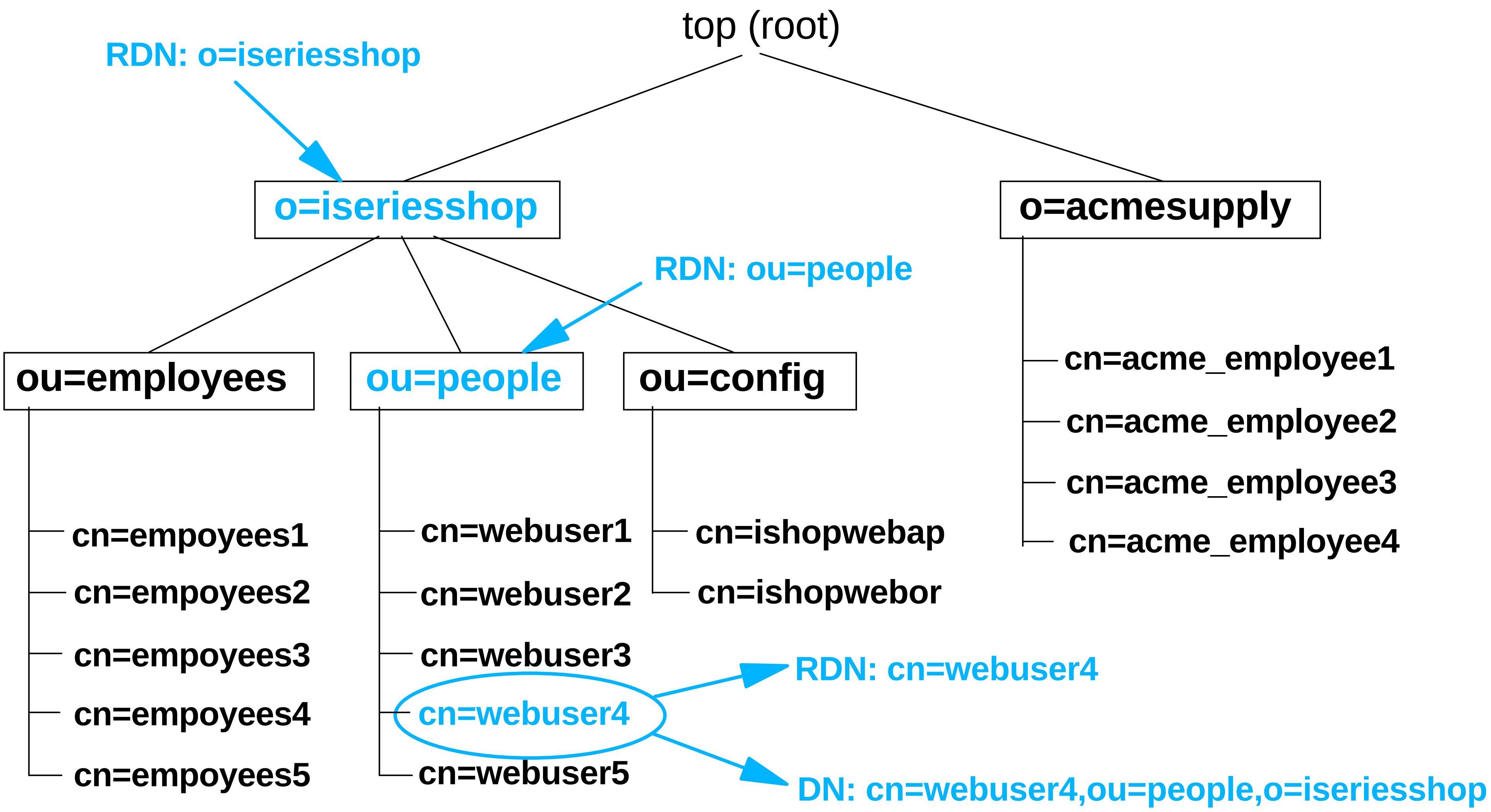
The OID for the Person class, for example, has the following meaning:

2.5.6.6

2 - ISO/ITU-T jointly assigned OIDs
  5 - X.500 Directory Services
    6 - X.500 standard object classes
      6 - id-oc-person

If you want to extend your directory schema with new object classes or attributes you should consider registering your OIDs to ensure compatibility.

Directory Information Tree (DIT)



top (root)

RDN: o=iseriesshop

o=iseriesshop

o=acmesupply

RDN: ou=people

ou=employees

cn=empoyees1

cn=empoyees2

cn=empoyees3

cn=empoyees4

cn=empoyees5

ou=people

cn=webuser1

cn=webuser2

cn=webuser3

cn=webuser4

cn=webuser5

ou=config

cn=ishopwebap

cn=ishopwebor

cn=acme_employee1

cn=acme_employee2

cn=acme_employee3

cn=acme_employee4

RDN: cn=webuser4

DN: cn=webuser4,ou=people,o=iseriesshop

Notes Directory Information Tree

A DN is a unique name that unambiguously identifies a single entry. DNs are made up of a sequence of relative distinguished names (RDNs). Each RDN in a DN corresponds to a branch in the DIT leading from the root of the DIT to the directory entry. A DN is composed of a sequence of RDNs separated by commas, such as cn=thomas,ou=itso,o=ibm.

You can organize entries, for example, after organizations and within a single organization you can further split the tree into organizational units, and so forth.

You can define your DIT based on your organizational needs as shown in a simple example on the previous chart. If you have, for example, one company with different divisions, you may want to start with your company name under the root as the organization (o) and then branch into organizational units (ou) for the individual divisions. In case you store data for multiple organizations within a country, you may want to start with a country (c) and then branch into organizations.

Requirements and Data Design

Requirements

- Applications
- Users
- Infrastructure

Data Design

- Sources for Data
- Characteristics of Data Elements
- Related Data
- There will probably be more data (and worse quality) than you expect

Notes Requirements and Data Design

Requirements

What type of application/applications will use the directory? What directory-enabled applications are to be deployed and what are their data needs? Determine the organization's other mission-critical applications. Find out if those applications can directly access and/or update the directory. What are the requirements for manageability and scalability? Will the LDAP service be participating with an X.500 directory service?

Who needs access to the data as a user. Can users directly access and/or update the directory. Determine the location of Clients (users or applications). What expectations are there for privacy concerns? How accurate and up-to-date must the directory content be?

What resources will be available for deployment? What people and skills are available? Can this be done as part of another project, e.g. messaging migration, or will it require dedicated resources?

What hardware configurations are already in use and which, if any, are available to the project? What operating systems, middleware and applications are in use? What directory applications are already available? Obtain a network diagram. Is the directory to be protected behind a firewall or exposed to the Internet?

Data Design

Planning the directory's data is the most important aspect of the directory planning activities, and it is probably the most time-consuming aspect as well. Planning the directory content includes deciding on what existing data to store in the directory. Survey the organization and identify where the data comes from (such as OS/400 User Profiles, SDD, Windows NT or Novel NetWare directories, Human Resources databases, e-mail systems, and so forth). Plans must be made to identify resources for keeping the data up to date and identifying resources with the authority to decide on access control policies regarding the data residing in the directory tree. If data is going to be imported from other sources, develop a strategy for both bulk imports and incremental updates. Try to limit the number of applications that can change the data. Doing this will help ensure the data integrity while reducing the organization's administration. Identify duplications and data that is not actually used or required.

Data is made up of data elements which possess several characteristics such as format, size, frequency, ownership, relationship with other data elements, etc. Examine each planned data element to determine its characteristics and which are shared with other elements. For each piece of data, determine the location where it will be mastered and who owns the data - that is, who is responsible for ensuring that the data is up-to-date.

Plan for related data sources which contain directory-related data but which may not, initially at least, use the directory itself. For example, the human resources database must bear a close relationship to entries in a directory containing staff data. Consider appropriate replication and synchronization techniques and procedures to maintain the relationships.

Organizing your directory

Schema Design

- Attributes and Object Classes
- Predefined Schemas
- Schema extensions

Namespace Design

- Choosing a directory suffix
- Branching the directory tree
- Creating a naming style

Notes Organizing your directory

Schema Design

A schema is the collection of attribute type definitions and object class definitions. A server uses these to determine how to match a filter or attribute against the attributes of a specific entry and whether to permit given attribute(s) to be added. This is similar to the data definitions of a relational database system. The purpose of a schema is to control the nature and format of the data stored in the directory. This means that they can be used for data validation and to control redundant data. A schema is also used by users and applications as the basis for directory search criteria. LDAP directory Schemas consist of Attributes and Object Classes. Schema design involves several stages. Firstly, identify any Schemas provided by the applications you have in plan, plus any standard and vendor-supplied Schemas. Secondly, select any predefined Schemas that meet your needs. Thirdly, plan for any schema extensions.

Namespace Design

Namespace design is a very important task in planning the directory as it is the means by which directory data is uniquely named and referenced. It is the equivalent of the 'unique key field' for the entry. The namespace provides a way to organize the data. It can be used to partition (group) the data and to provide a basis for replication. It can affect your access control methods. Finally, it is the basic support for directory-enabled applications. Before designing your namespace you need to understand the requirements upon it.

The usual method of namespace design will set the root of the directory tree to a specific organization in a specific country or to a specific organization and organizational unit.

Choosing to branch a directory tree based on the organizational structure, such as departments, can lead to a large administrative overhead if the organization is very dynamic and changes often. On the other hand, branching the tree based on geography may restrict the ability to reflect information about the organizational structure. A branching methodology that is flexible, and which still reflects enough information about the organization, must be created. If your organization has separate units that are either physically separated or have their own management authorities, you might have a "natural" requirement to split and separate parts of the DIT.

The first goal of a naming style is to provide unique identifiers for entries. Once this is achieved, the next major goal should be to make querying of the directory tree intuitive. In general, the standard attribute types should be used as documented in the standards whenever possible. It is important to decide, within the organization, which attributes to use for what purpose and not to deviate from that structure.

Securing directory entries

Purpose

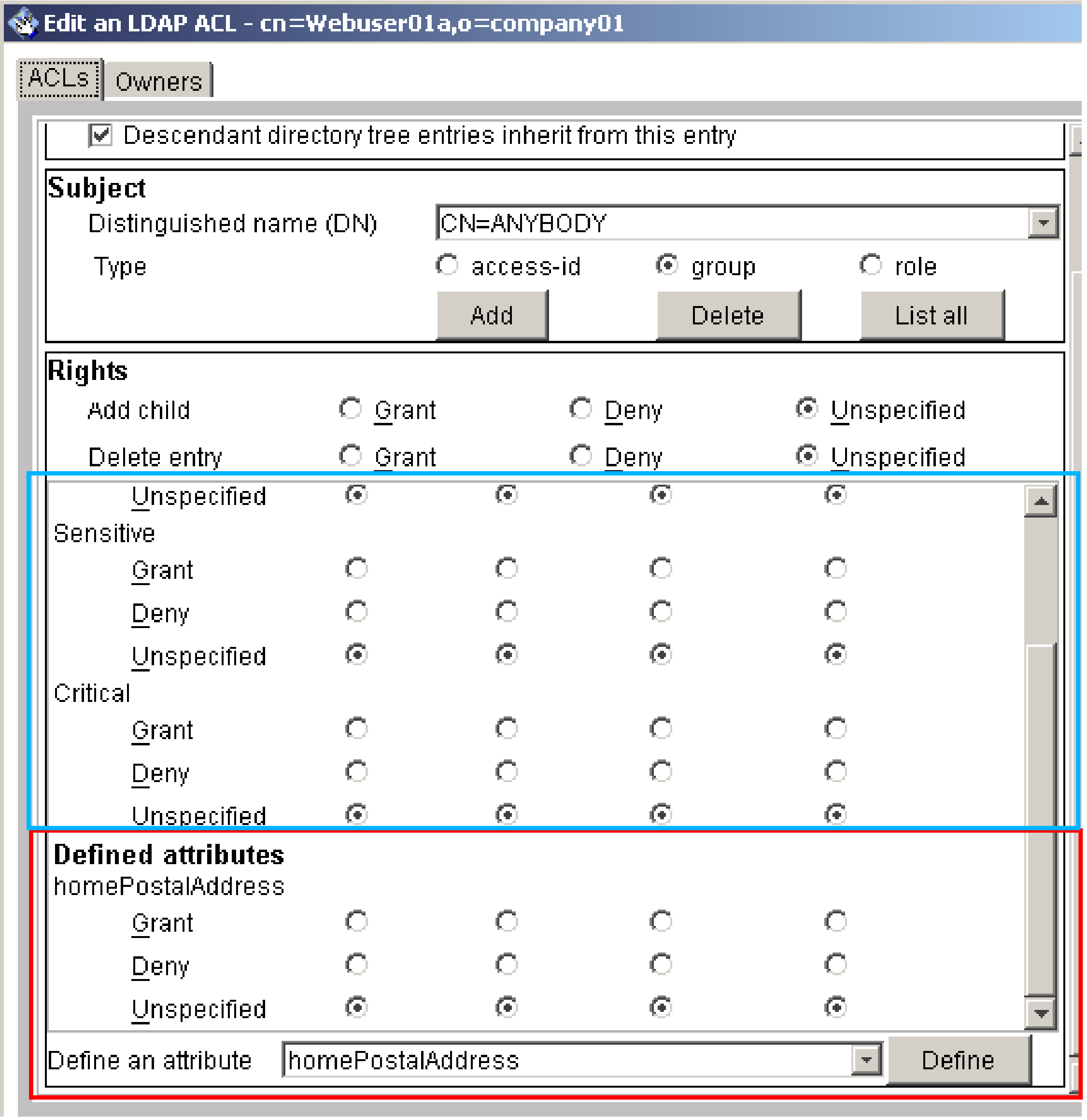
- Control who can view what information
- Control who can perform what changes

Analysis

- Who needs to access what information
- Evaluate organizational needs

Design

- Authentication
- Authorization
  - Access class permissions
  - Attribute-level permissions



Edit an LDAP ACL - cn=Webuser01a,o=company01

☑ Descendant directory tree entries inherit from this entry

Subject

Distinguished name (DN): CN=ANYBODY

Type: ○ access-id ● group ○ role

Rights

Add child: ○ Grant ○ Deny ● Unspecified

Delete entry: ○ Grant ○ Deny ● Unspecified

Unspecified	●	●	●	●
Sensitive				
Grant	○	○	○	○
Deny	○	○	○	○
Unspecified	●	●	●	●
Critical				
Grant	○	○	○	○
Deny	○	○	○	○
Unspecified	●	●	●	●
Defined attributes				
homePostalAddress				
Grant	○	○	○	○
Deny	○	○	○	○
Unspecified	●	●	●	●

Define an attribute: homePostalAddress

Notes Securing directory entries

The degree of security controls you require will depend on the nature of the information you are storing, the ways in which clients will be accessing the directory, the methods which will be used to update and manage the directory and an acceptable level of administration effort for security. A security policy should be strong enough to prevent sensitive information from being modified or retrieved by unauthorized users while simple enough that administration is kept simple so authorized parties can easily access it. Ease of administration is very important when it comes to designing a security policy. Too complex a security policy can lead to mistakes that either prevent people from accessing information that they should have access to, or allow people to modify or retrieve directory information that they should not have access to. The most basic purpose of security is to protect the data in your directory. It needs to be protected against unauthorized access, tampering with information and denial of service.

To plan for the required level of security, two basic areas must be considered to answer the following question: What level of security is needed when clients identify themselves to the directory server, and what methodology will be used when authorizing access to the different kinds of information in the directory? These areas are Authentication and Authorization.

Authentication Design

Conceptually, directory authentication can be thought of as logging in to the directory. LDAP terminology refers to this operation as binding to the directory. Generally, bind operations consist of providing the equivalent of a user ID and a password. However, in the case of an LDAP directory, the user ID is actually a distinguished name (or a distinguished name derived from a user ID). The distinguished name used to access the directory is referred to as the bind DN. So, what level of authentication should be considered? There are, generally speaking, three different approaches:

No Authentication: This is the simplest approach, which might be perfectly suitable for most directories when all users are equally granted read (or even write) access to all data. There is no need for user authentication when this is the case.

Basic (Simple) Authentication: This lets the client bind by entering a DN and a password. Using basic authentication will not ensure integrity and confidentiality of the login data since it is being sent over the network in a readable form.

Secure Authentication: SASL (Simple Authentication and Security Layer) is an extensible authentication framework. It was added to LDAP Version 3, and it supports Kerberos and other security methods, like S/Key.

Authorization Design

The data in the directory tree will have to be protected in different ways. Certain information must be searchable for everybody, some must be readable, and most of it will be write protected. In LDAP Version 3, there are no defined attributes to handle this. As a result, vendors support their own implementations of authorization. This is done by different implementations of access control lists (ACLs).

Starting with OS/400 V5R1, you can also enable attribute-level permissions.

Designing Infrastructure

Availability, scalability and manageability requirements

Topology Design

- Centralized or Distributed?
  - If Distributed then...
- ...Partitioned or Replicated?
  - If Replicated then...

...Replication Design

- Server to server
- Exchanges data

Referral Design

- Client to server search
- Server refers search to another server

Notes Designing Infrastructure

Physical design involves building a network and server infrastructures to support availability, scalability and manageability.

Availability, scalability and manageability requirements

Availability may not be an issue if the directory is not business-critical. However, if it is then there is a need to design a highly available system. This involves more than is supported in LDAP. The LDAP components that are needed are partitioning and replication. Since high availability involves eliminating single points of failure or reducing their impact, it is necessary to have redundant hardware, software and networks to spread the risk. Scaling up servers is done much the same way, either by increasing availability or by upgrading hardware performance. Manageability aspects involve almost all parts of a directory design. Tradeoffs may have to be made regarding scalability, availability, flexibility, and manageability and are related to cost in hardware, software and systems management.

Topology Design

Topology Design concerns the distribution of directory servers. The first choice is between a centralized or a distributed approach. A simple approach to create a highly available directory service is to create a master and a slave directory server, each one on its own physical machine. By replicating the data, we have eliminated the single point of failure for both hardware and software failures. There is also the issue of network bandwidth and its reliability to take into consideration.

Partitioned or Replicated?

The second choice for topology design is only applicable when a distributed approach has been selected for the first choice. The options are between a partitioned and a replicated approach. The decision criteria are usually based on performance and availability issues and will be influenced by the size of the directory.

Replication Design

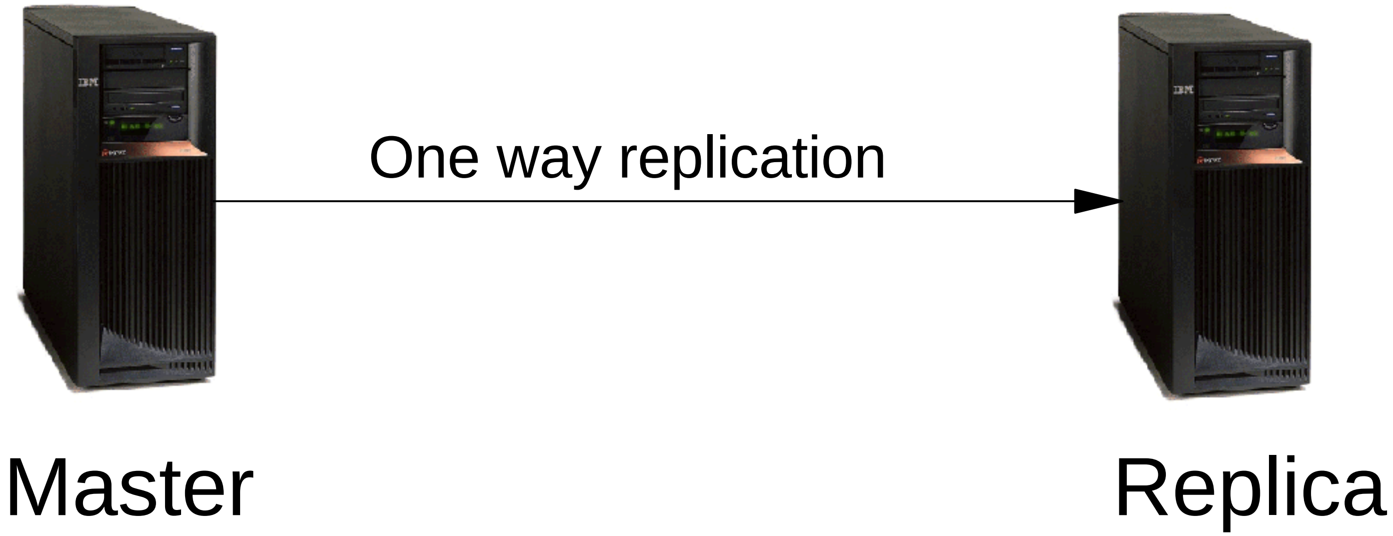
The Replication Design stage is only required when, firstly, a distributed approach is chosen to server deployment and, secondly, a replicated approach is chosen over a partitioned approach. Replication aims to improve the reliability and performance of your directory service. By making directory data available in more than one location you improve the reliability of the service in the event of server or network failure. You also improve the performance by distributing the load across multiple servers and reducing network traffic.

Referral Design

A referral is information returned by an LDAP server to a client making a search request and which indicates to the client that other servers need to be asked to fulfill the request. Support for referrals is standard in LDAP V3. The method of configuring referrals depends on the server software.

Replication

For backup and availability reasons



One way replication

Master

Replica

- Changes are performed on master
- Master replicates changes updates immediately or on a scheduled basis
- Update requests to replica will be rerouted to master
- Replicates the entire DIT; no subtree replication....yet

Notes Replication

You can set up replicas of the LDAP directory server to directory servers on other iSeries 400 systems. Directory Services uses the standard LDAP version 3 protocol to replicate.

The information stored on replica LDAP directory servers is identical to the information on your main, or "master", LDAP directory server.

There are two principal benefits to having one or more replicas of your LDAP

directory:

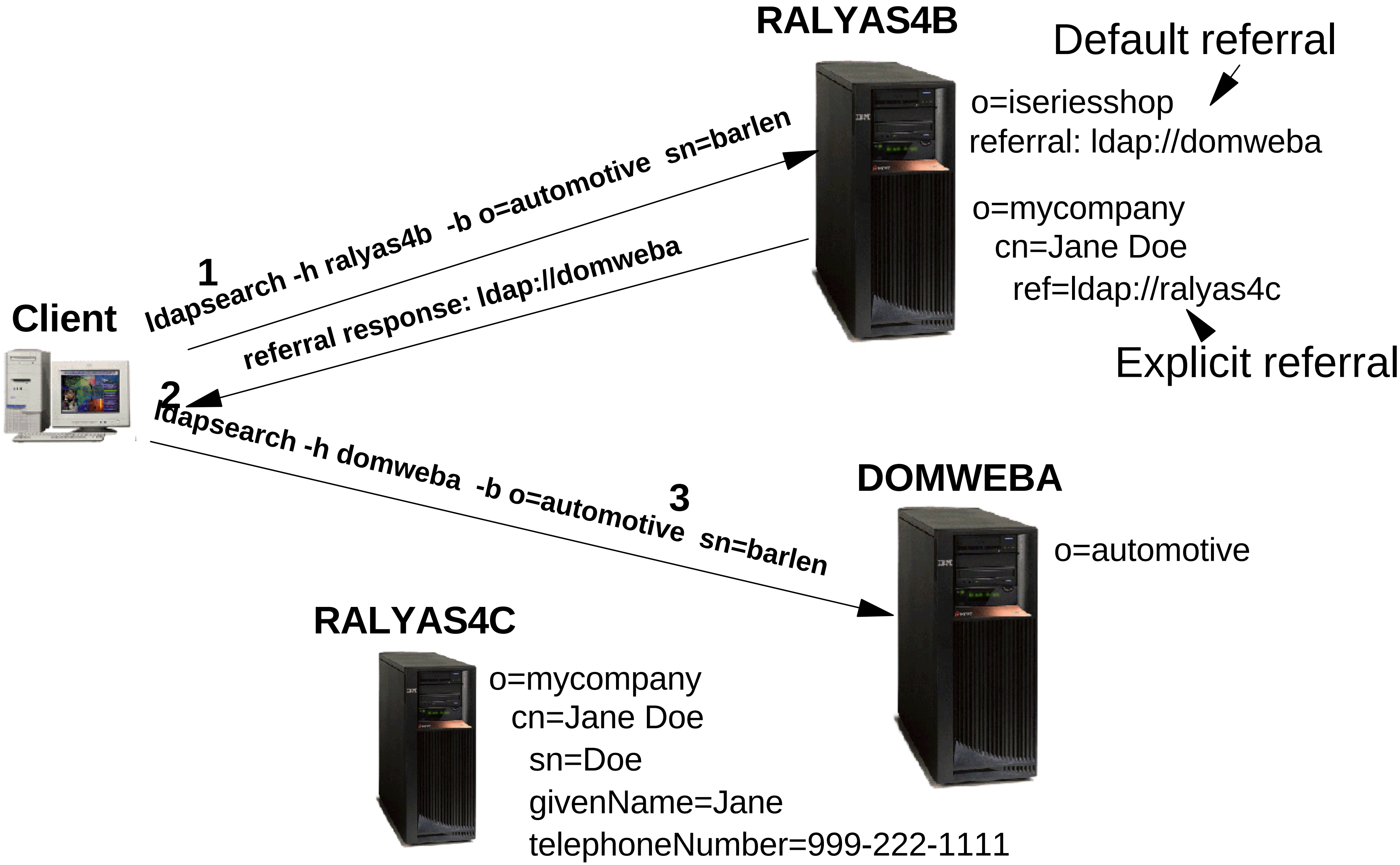
- Replicas make directory searches faster. Instead of having all clients direct search requests to a single master server, you can split requests between the master server and the replica servers.
- Replicas provide a backup to the master server. If the master server is unavailable, a replica can still fulfill search requests and provide access to directory data.

Replica servers are read-only. When an authorized user attempts to change an entry on a replica server, it refers the request to the master directory server.

Note: You cannot replicate between LDAP version 3 and LDAP version 2 servers. Therefore, the system that you replicate to must be using the same version of LDAP as the system from which you replicate. V4R3 and V4R4 of OS/400 support LDAP version 2. V4R5 and later releases support LDAP version 3 .

You can replicate the Directory Services directory to IBM SecureWay V3.2 servers on other platforms.

Referrals



RALYAS4B

Default referral

o=iseriesshop
referral: ldap://domweba

o=mycompany
cn=Jane Doe
ref=ldap://ralyas4c

Explicit referral

Client

1 ldapsearch -h ralyas4b -b o=automotive sn=barlen

referral response: ldap://domweba

2

ldapsearch -h domweba -b o=automotive sn=barlen 3

DOMWEBA

o=automotive

RALYAS4C

o=mycompany
cn=Jane Doe
sn=Doe
givenName=Jane
telephoneNumber=999-222-1111

Notes Referrals

Referrals allow LDAP directory servers to work in teams. If the DN that a client requests is not in one directory, the server can automatically send (refer) the request to any other LDAP server. Directory Services allows you to use two different types of referrals. You can specify default referral servers, where the LDAP server will refer clients whenever any DN is not in the directory. You can also use your LDAP client to add explicit entries to the directory server that have the objectClass "referral". This allows you to specify referrals that are based on what specific DN a client requests.

An important aspect that you need to understand when planning to implement referrals is that the LDAP server that receives a client request is actually not contacting the LDAP server listed as a referral server. It rather returns all configured referral server entries to the client which in turn retries the initial request on a server returned as a referral as shown in previous chart. In the example of a default referral, the client submits, for instance, a search request. When the server receives the search request and does not find the entry for `sn=barlen` and `o=automotive` , it returns the `ldap://domweba` reference to the client.

Important: Understanding that a client is actually contacting the individual LDAP servers that are returned in a referral response raises another question. What happens if firewalls restrict traffic in your network? You may want to limit clients to access only hosts in a certain subnet. One of these hosts might be an LDAP server that returnes referral responses. The client might not be able to contact the server listed in the response as this one is on another subnet. That means, you also need to consider network traffic constraints when implementing referrals.

3. Directory Support on iSeries

iSeries as a Directory Server

iSeries server support several types of directories

System Distribution Directory (SDD)

- Does not support access via LDAP

IBM SecureWay Directory

- OS/400 - Directory Services option
- LDAP-enabled directory

Premier platform for Domino Directory

- LDAP access can be activated

Standard OS/400 functions and other tools are available to synchronize directories

Notes iSeries as Directory Server

OS/400, the operating system for the iSeries and AS/400 platforms, is an excellent basis for a directory server but, as with any platform, there may be one or two challenges in building what is required on top of the existing data. This is not a directory in itself but performs some of the functions of a directory.

With OS/400 the enrollment & security are in the User Profile. Every user has one. Directories are not yet used for the majority of OS/400-based applications.

Every OS/400 server also possesses a System Distribution Directory.

From V4R3 each server has an optional LDAP-enabled directory in the form of IBM SecureWay Directory which is known as OS/400 Directory Services. From V5R1 this is integrated into the base of OS/400.

OS/400 is also the premier platform for Domino Directory which too is LDAP-enabled. It outsells all UNIX variants of Domino combined.

The challenge is to synchronize iSeries directories. Fortunately, there are some OS/400 functions as well as other products available that help you automating your synchronization.

OS/400 System Distribution Directory

Most users in OS/400 SDD

- Client Access, OV/400, Distribution, POP3, cc:Mail, Shared Folders

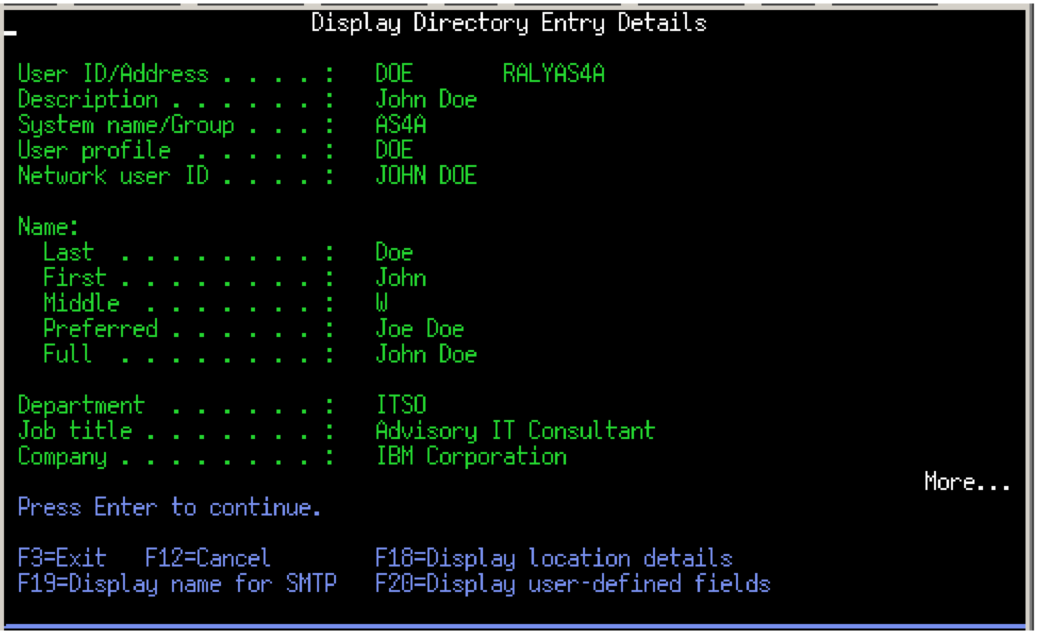
SDD is X.500 compatible

SMTP addressing

Hierarchical Departments

- Prompt for Department and Location
- Reports to

OS/400 APIs available (CL)



```
                            Display Directory Entry Details

 User ID/Address . . . . :   DOE       RALYAS4A
 Description . . . . . . :   John Doe
 System name/Group . . . :   AS4A
 User profile  . . . . . :   DOE
 Network user ID . . . . :   JOHN DOE

 Name:
   Last  . . . . . . . . :   Doe
   First . . . . . . . . :   John
   Middle  . . . . . . . :   W
   Preferred . . . . . . :   Joe Doe
   Full  . . . . . . . . :   John Doe

 Department  . . . . . . :   ITSO
 Job title . . . . . . . :   Advisory IT Consultant
 Company . . . . . . . . :   IBM Corporation
                                                                        More...
 Press Enter to continue.

 F3=Exit   F12=Cancel         F18=Display location details
 F19=Display name for SMTP    F20=Display user-defined fields
```

Notes System Distribution Directory

Most OS/400 users are already registered in OS/400's SDD. This applies if they have been users of any of the following

- Client Access, OV/400, Distribution, POP3, cc:Mail, Shared Folders

The SDD is X.500 compatible and hence its field structure is very similar to, and in some ways superior to, that of LDAP.

It allows for SMTP, X.400, Lotus Domino and cc:Mail addressing

It allows for a hierarchical department structure (company/department/sub-department):

- F4 Prompt for Department and Location, and
- a 'Reports' to field

OS/400 APIs are available (CL) to add, display, change, remove and rename entries and to perform similar operations with Distribution Lists and Nicknames.

Lotus Domino Directory

The cornerstone of Domino

Basis for security, for server and people registration

27% of Enterprise Directory Market

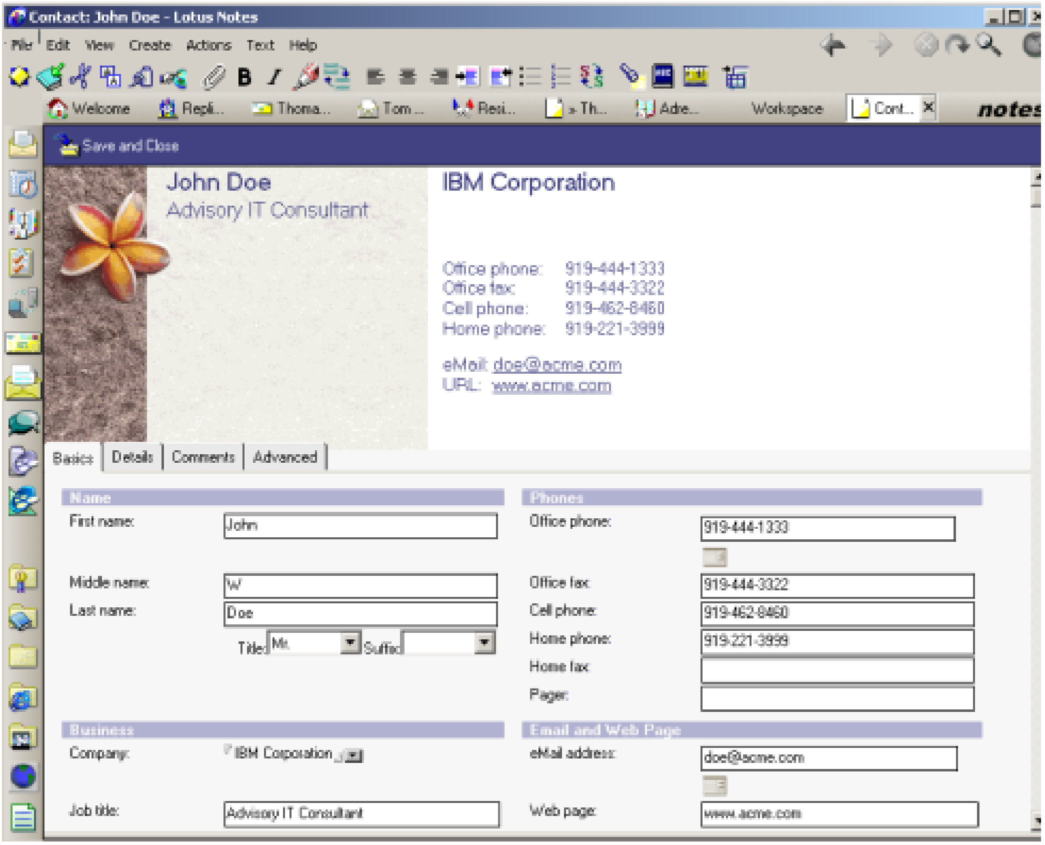
Directory Catalog

- index of directories

Directory Assistance

- lightweight, off-line-capable subset

LDAP V3 from Domino R5



John Doe
Advisory IT Consultant

IBM Corporation

Office phone: 919-444-1333
Office fax: 919-444-3322
Cell phone: 919-462-8460
Home phone: 919-221-3999

eMail: doe@acme.com
URL: www.acme.com

Name

First name: John
Middle name: W
Last name: Doe
Title: Mr. Suffix:

Phones

Office phone: 919-444-1333
Office fax: 919-444-3322
Cell phone: 919-462-8460
Home phone: 919-221-3999
Home fax:
Pager:

Business

Company: IBM Corporation
Job title: Advisory IT Consultant

Email and Web Page

eMail address: doe@acme.com
Web page: www.acme.com

Notes Lotus Domino Directory

The Domino Directory is the cornerstone of Domino. It is the basis for security, for server and people registration. To Domino users it is hard to conceive of Domino without it.

Domino is targeted at, and is widely used in, Directory Consolidation and Lotus estimates that it has 27% of the Enterprise Directory market.

It possesses several specific functions including:

Directory Catalog

  - A lightweight, quick access store of directory information primarily for use by mobile and disconnected users.

- Directory Assistance
  - A mechanism to federate one or more secondary directories, making them transparently accessible to directory users. These secondary directories can be either Domino, SecureWay Directory Services or third-party LDAP-compliant directories.

LDAP V3 was introduced from Domino R5 onwards.

IBM SecureWay Directory

IBM Tivoli brand

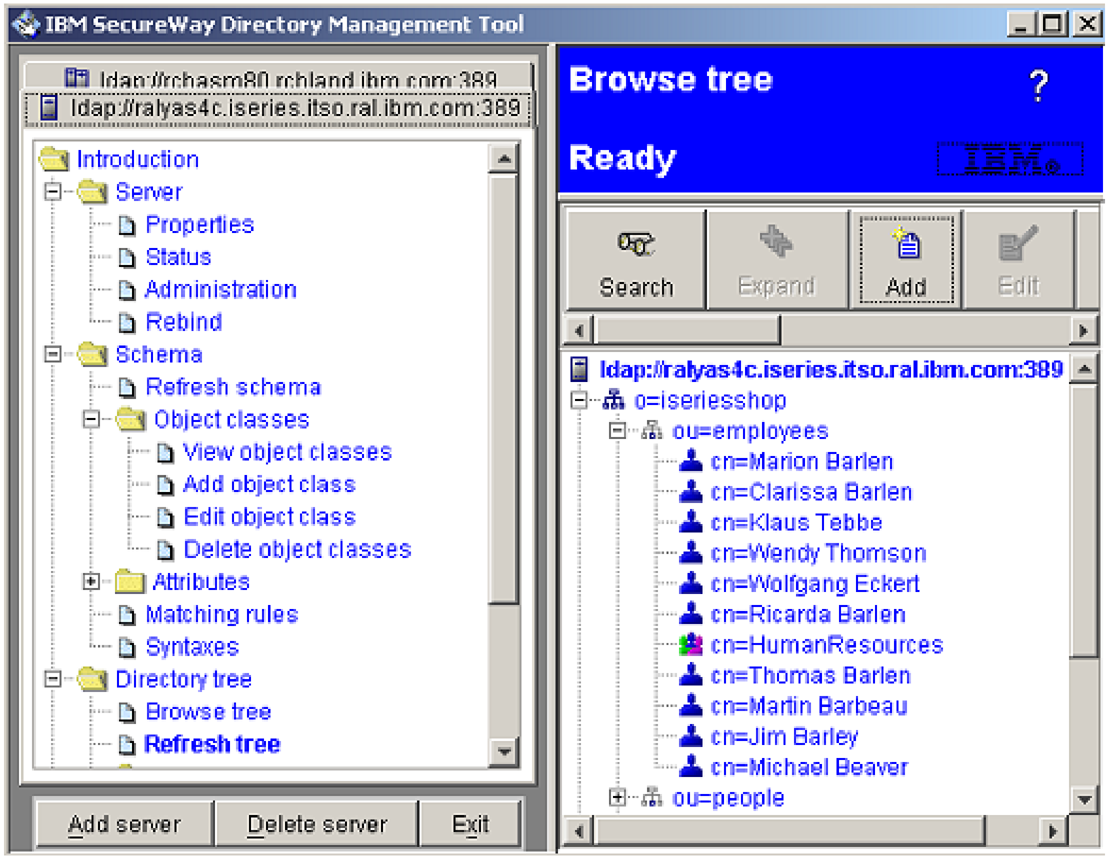
Cross-platform

- OS/400, AIX, OS/390, Win NT/2000

LDAP-enabled

Free with OS/400

- Known on iSeries as Directory Services
- Available from V4R3
- SecureWay Directory V3 at V4R5
- SecureWay Directory V3.2 at V5R1



Notes IBM SecureWay Directory

OS/400 Directory Services provides LDAP on OS/400 which includes both AS/400 and iSeries. Directory Services is part of the IBM Tivoli SecureWay® Directory family of products and services and is sometimes referred to as SecureWay Directory for OS/400.

SecureWay is a cross-platform product available on:

- OS/400, AIX, OS/390, NT& Windows 2000

OS/400 Directory Services includes an LDAP server and complete set of LDAP clients and utilities.

In releases V4R3 to V4R5, LDAP is included free in OS/400 as part of Directory Services for OS/400 (BOSS option 32). In V5R1, Directory Services was integrated as part of the base operating system.

LDAP V2 support was provided at OS/400 V4R3, LDAP V3 (SecureWay Directory V3) at V4R5 and SecureWay Directory V3.2 at V5R1.

OS/400 Directory Services

Based on IBM's SecureWay Directory product

Underlying directory repository is a DB/2 database

Configured via Operations Navigator (V5R1) or iSeries Navigator (V5R2)

A management tool, APIs, and utilities are included with OS/400 Directory Services

OS/400 provides support to publish system and user (SDD) to the LDAP directory

- User information from SDD is mapped to directory attributes

Print shares can be published to Microsoft Active Directory

Notes OS/400 Directory Services

An IBM SecureWay Directory implementation is supported on iSeries. LDAP clients and an LDAP server are provided free with Directory Services. Starting with OS/400 V5R1, Directory Services is included with the base operating system. LDAP clients for Windows and OS/400 provide APIs for use by both C and Java applications. The OS/400 client also provides APIs for use by all Integrated Language Environment (ILE) programming languages. LDAP utilities are provided for common administrative tasks such as searching or modifying the directory and can be run from the OS/400 QShell command environment or a Windows command prompt. To allow mail clients to search for e-mail addresses of OS/400 users, Directory Services enables System Distribution Directory (SDD) information to be published to an LDAP directory. All IBM SecureWay Directory LDAP server implementations use the IBM Universal Database (UDB). When implemented on iSeries, this results in an LDAP directory that is scalable, robust and easy to manage. Millions of entries can be added to the directory with little impact on performance. Backup and recovery of the LDAP directory is performed using standard OS/400 administrative procedures. Configuration of the LDAP server is made easy using a wizard within Operations Navigator in the TCP/IP Servers folder for your system.

Implementation

Starting with V5R1 there is an automatic configuration of directory services

- Once directory service is started, a default configuration is created
- By default, system information is published

Change configuration via Operations Navigator

- Reconfigure the directory server using a configuration wizard
- Server is listed as *Directory* under TCP/IP servers

Three OS/400 jobs in subsystem QSYSWRK for directory server and publishing

- QDIRSRV
- QGLDPUBA
- QGLDPUBE

Notes Implementation

Beginning with V5R1, Directory Services (LDAP) is automatically installed when you install OS/400. The directory server includes a default configuration that automatically start the directory server when TCP/IP is started. It also start publishing of computer (system) information from OS/400 to the directory server.

To customize the LDAP directory server's settings for your own use, run the Directory Services Configuration Wizard. You must have *ALLOBJ and *IOSYSCFG special authorities to use the wizard. If you want to configure OS/400 security auditing, you must also have *AUDIT special authority. Prior to V5R1, is was necessary to install the OS/400 Directory Services option of the OS/400 to install the directory server.

QDIRSRV

The Directory Services server job QDIRSRV is running in subsystem QSYSWRK. This is the only job running for the Directory server. This job will contain information about failing client requests and replication errors. Client errors include all requests that do not complete successfully and might include bind failures, attempts to delete objects that do not exist, schema errors if a client application is missing required attributes, and so on. We should point out that an error message here means only that the server did not return a successful return code to the client. It does not necessarily indicate a failure. For example, an application may assume an object exists and create it only in event of an error, rather than doing a search first. Look in this job log when you have reason to believe an error has occurred, rather than assuming that a message here indicates an error.

QGLDPUBA

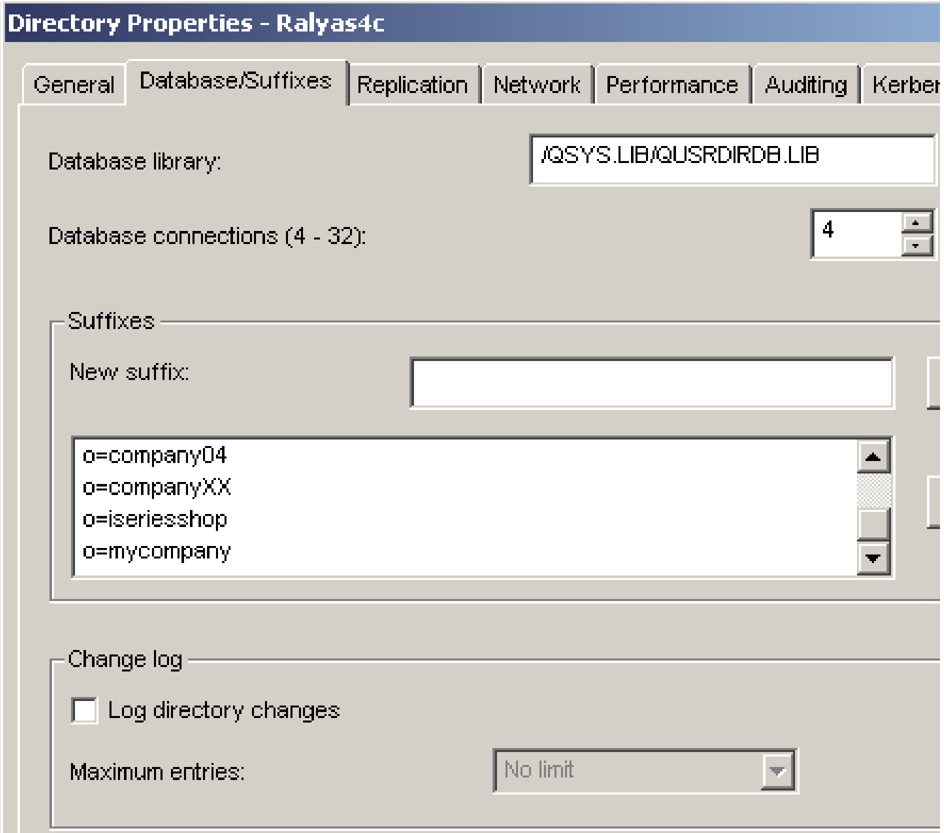
This job also runs under the subsystem QSYSWRK and takes care of the synchronization between the System Distribution Directory (SDD) and the LDAP Directory server. This job acts as the publishing agent for user (SDD) and system information, generating LDAP requests that are put into a publishing queue. However if changes are made in the LDAP directory, these changes are not synchronized back to the system distribution directory.

QGLDPUBE

This job acts as the publishing engine, taking changes from the queue (put there by QGLDPUBA and other publishing agents -- printers, user defined agents), and processes the requests using the server, authentication, and location information defined in the agent configuration. If the requests is successful, the change is removed from the queue. If it fails (for example, because the server was down), the requests is left in the queue to be retried.

Configuration steps

1. **Configure Directory Services manually or with wizard**
   - Specify administrator distinguished name and password
   - Add suffixes
2. **Add suffix names as entries to the directory**
   - Exception when publishing system information
   - Otherwise, each suffix, for example `o=iseriesshop` must be added to the directory
3. **Publish data into the directory**



Directory Properties - Ralyas4c

Database library: /QSYS.LIB/QUSRDIRDB.LIB

Database connections (4 - 32): 4

Suffixes

New suffix:

o=company04
o=companyXX
o=iseriesshop
o=mycompany

Change log

□ Log directory changes

Maximum entries: No limit

Notes Configuration steps

If your system has not been configured to publish information to another LDAP server and no LDAP servers are known to the TCP/IP DNS server, then Directory Services is automatically installed with a limited default configuration. Directory Services provides a wizard to assist you in configuring the LDAP directory server for your specific situation. You may run this wizard as part of EZ-Setup, or run it later from Operations Navigator. Use this wizard when you initially configure the directory server. During the wizard configuration and afterwards when changing the Directory server properties, you can specify the directory administrator's DN and password. This user DN will be the administrator for the Directory Server. This userid is only used inside the Directory Server and is not related to an OS/400 user profile. You also have to add at least one suffix to the server configuration. Typical suffixes are of object class organization (o), country (c), and organizational unit (ou). Without a suffix you will not be able to create any entry in the directory. In this example, we add a suffix o=iseriesshop . Adding the suffix does not automatically add the organization iseriesshop to the directory. It rather allows us to add the organization under the root of the directory. You still need to create the organization object in the directory. Beginning with V5R1, the system will add the organization to the directory in case you publish system information and the suffix does not exist.

After the basic configuration has been performed and the suffixes as defined in the Directory server properties are added to the directory, you can start publishing data. Data can be published by importing them, using the LDAP utilities, APIs, or by automatically publishing system or user (SDD) data.

4. Management of directories

Management Characteristics

We need directory management tools and utilities to:

- Define structure
- Import data
- Synchronize data
- Edit entries
- Manage security
- Manage schema
- Export data

Notes Management Characteristics

Management of a directory involves several tasks. You need tools that allow you to perform the following:

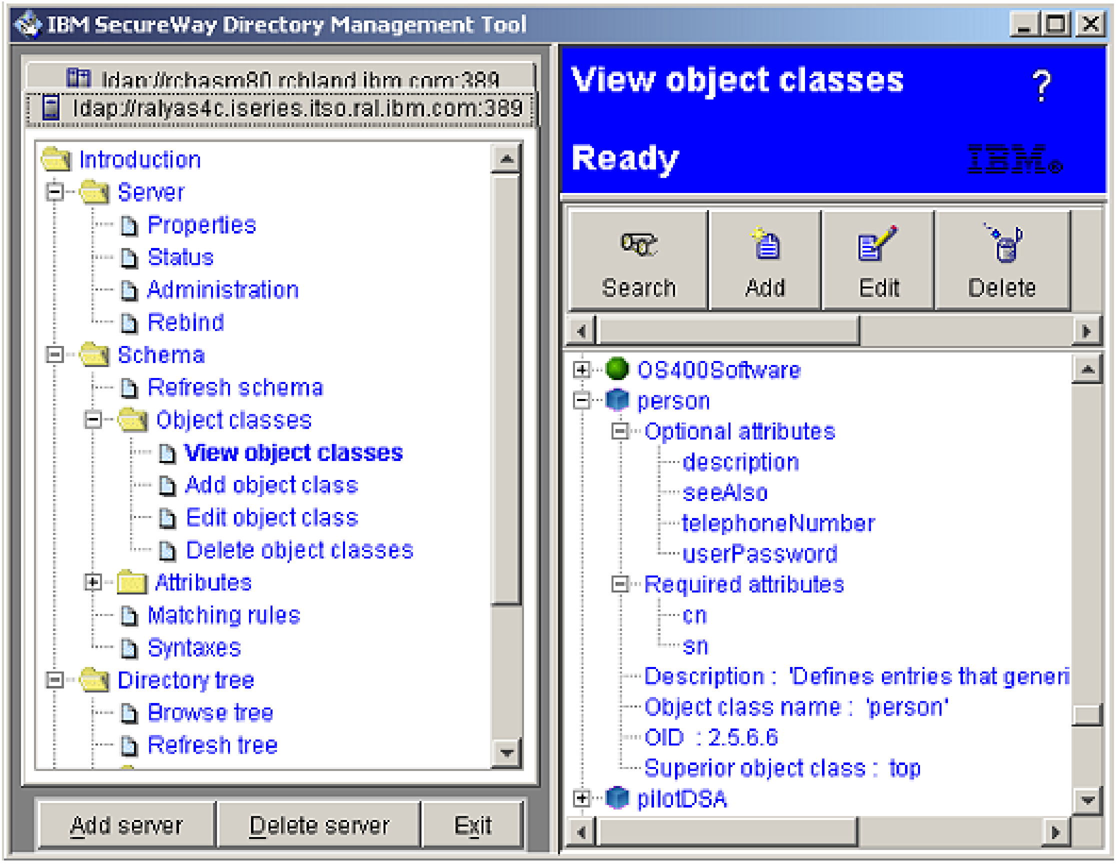
- Define the directory information tree structure
- Import data from various sources, such as other directories or existing data repositories
- Synchronize data
- Edit entries
- Manage security
- Managing the schema
- Export data for import into another directory or for backup purposes

Most of the management tasks can be performed by tools and utilities that are shipped with OS/400 Directory Services. A graphical management tool as well as application programming interfaces and LDAP utilities are part of the IBM SecureWay Directory product as packaged on the iSeries server as Directory Services. However, for certain synchronization tasks you may need additional tools, such as tools from the BlueNotes product suite.

SecureWay DMT

Directory Management Tool

- GUI to manage directory information
- Use the tool to:
  - Connect to directory servers via SSL or non-SSL connections
  - Display server properties and rebind
  - List, add, edit, and delete schema attributes and object classes
  - List, add, edit, and delete directory entries
  - Modify directory ACLs
  - Search the directory tree
- For additional information see Getting Started document



Notes SecureWay DMT

The IBM SecureWay Directory Management Tool (DMT) provides a graphical user interface for managing LDAP directory content. The DMT is part of the Windows LDAP client that is included with Directory Services. The client is shipped in an OS/400 Integrated File System (IFS) directory.

You can use the tool to:

- 1. Connect to directory servers via SSL or non-SSL connections
- 2. Display server properties and rebind
- 3. List, add, edit, and delete schema attributes and object classes
- 4. List, add, edit, and delete directory entries
- 5. Modify directory ACLs
- 6. Search the directory tree

The DMT includes also the PC LDAP utilities.

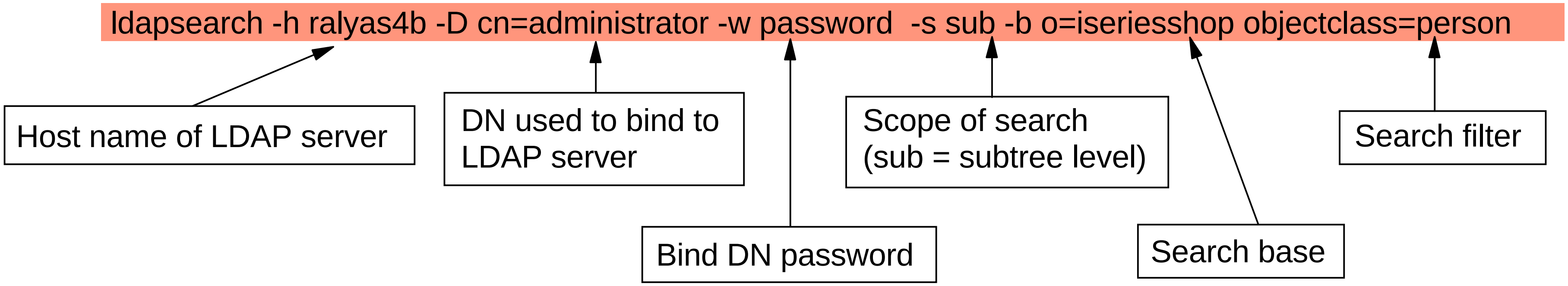
LDAP Management

LDAP utilities

- Included in OS/400 Directory Services
  - ldapadd and ldapmodify utilities, which add and modify LDAP directory entries.
  - ldapdelete utility, which removes entries from the LDAP directory.
  - ldapsearch utility, which searches the LDAP directory for entries
  - ldapmodrdn utility, which allows you to change the Relative Distinguished Name (RDN).

Example of a directory search:

```
ldapsearch -h ralyas4b -D cn=administrator -w password  -s sub -b o=iseriesshop objectclass=person
```



Host name of LDAP server

DN used to bind to LDAP server

Bind DN password

Scope of search (sub = subtree level)

Search base

Search filter

Notes LDAP Management

LDAP Utilities

OS/400 Directory Services includes five utilities that allow you to perform actions on the LDAP directory server from the Qshell command environment in OS/400. They use the LDAP APIs. You can use these utilities from the Qshell command line or call them from programs. You may also find them useful as programming examples. When you install the Windows LDAP client

that is included with Directory Services, you also install the LDAP utilities for the Windows platform. The utilities are:

- The ldapadd and ldapmodify utilities are used to add and modify LDAP directory entries.
- The ldapdelete utility removes entries from the LDAP directory.
- With ldapsearch utility you can search the LDAP directory for entries.
- The ldapmodrdn utility allows you to change the Relative Distinguished Name (RDN) of an entry.

The ldapsearch example binds with DN cn=administrator (D) and its password password (w) to the LDAP server ralyas4b (-h) and searches in all subtree levels (s sub) within the search base o=iseriesshop (b) for entries of an object class person .

Management (cont'd)

LDIF

- LDAP Data Interchange Format
- Used for data import to, and export from, LDAP directories
- File format
  - records and line separators
- Available from Operations Navigator and LDAP utilities

```
version:1
dn:cn=Jane Doe,ou=employees,o=iseriesshop
changetype:modify
add:title
title:Senior staff member
-
replace:employeetype
employeetype:Permanent
-
replace:employeenumber
employeenumber:55555553
-
delete:homepostaladdress
```

Example of a LDIF file that adds, changes, and deletes attributes for a DN

LDAP utility to perform the update

```
ldapmodify -h ralyas4b -D cn=administrator -w password -f /as2318/ldif/update.ldif
```

Notes LDAP Management

LDIF

When an LDAP directory is loaded for the first time or when many entries have to be changed at once, it is not very convenient to change every single entry on a one-by-one basis. For this purpose, LDAP supports the LDAP Data Interchange Format (LDIF) that can be seen as a convenient, yet necessary, data management mechanism. It enables easy manipulation of mass amounts of data. LDIF is typically used to import and export directory information between LDAP-based directory servers, for example when an LDAP server has to be moved to other hardware or to describe a set of changes that are to be applied to a directory. Additionally, by using a well-defined interchange format, development of data import tools from legacy systems is facilitated. Simple tools can be developed, for example using the UNIX shell script language, to convert a database of personnel information into an LDIF file, which can then in turn be imported into the LDAP directory, regardless of the internal database representation the target directory server uses.

The LDIF format is used to convey directory information or a description of a set of changes made to directory entries. An LDIF file consists of a series of records separated by line separators. A record consists of a sequence of lines describing a directory entry or a sequence of lines describing a set of changes to a single directory entry. An LDIF file specifies a set of directory entries or a set of changes to be applied to directory entries, but not both at the same time. In the example shown on the previous chart, the command string binds with DN cn=administrator (D) and its password password (w) to the LDAP server ralyas4b (h) and performs the modifcations provided in the LDIF input file (f) /as2318/ldif/update.ldif . The LDIF file performs an update for `dn:cn=Jane Doe,ou=employees,o=iseriesshop` .The change type is modify indicating that the modification actions can consist of adding, replacing, or deleting attributes values. In this example, the title attribute is added, the employeetype and employeenumber attributes updated, and the homepostaladdress attribute deleted.

Note the '-' character between the different modification entries. This character serves as a separation character and must be included.

For more information about the LDIF format refer to the LDIF RFC 2849 found at

http://www.rfc-editor.org/rfcsearch.html

Operations Navigator allows you to export the LDAP database to an LDIF file. You can export the entire directory with all entries or a specific subtree. However, whether you export the entire directory or a subtree, the export function always exports the entries with all attributes. You have no way of specifying that you only want to export a subset of attributes for the entries to be exported. You also cannot specify a search criteria to export only certain entries within the selected subtree. The Operations Navigator export function is rather designed to allow you export the directory for backup or replication purposes.

User-Written Applications

Used for

- directory management
  - complement the tools if required
- directory-enabling applications
  - for example, applications using LDAP for authentication
  - retrieving e-mail addresses to send electronic notifications
  - ...there are almost no limits in what you can use a directory for

ILE APIs

- Application Program Interfaces available for all ILE programming languages
- Binding to a directory, searching the directory, adding, deleting, modifying, and renaming entries

JNDI

- Java Naming and Directory Interface is a package that allows you to search a directory or adding, deleting, modifying, and renaming entries

Notes User-Written Applications

APIs

Whether you want to write new applications using one of the Integrated Language Environment (ILE) programming languages or modernize existing applications on your iSeries server, you certainly should consider directory-enabling them. OS/400 Directory Services provides a rich set of application programming interfaces (APIs) that allow you to search and update entries in your LDAP directory.

The set of LDAP APIs are designed to provide a suite of functions that can be used to develop directory enabled applications. Directory enabled applications will typically connect to one or more directories and perform various directory-related operations, such as:

- Adding entries
- Searching the directory and obtaining the resulting list of entries
- Deleting entries
- Modifying entries
- Renaming entries

JNDI

Any Java application, whether it is a servlet, a server application, or a client application can be directory enabled. You can exploit LDAP directory information, for example, for automatically addressing and sending e-mail notifications, retrieving employee's addresses to send the payment slip, for retrieving user information at a user help desk, and perform your own application authentication. You can even serialize Java objects, such as GUI elements, into an LDAP directory and dynamically load them by all Java applications. The advantage of this method is, for example, that corporate-wide GUI design requirements can be deployed and changed very easily without recompiling programs or even touching the Java programs. The Java package that allows you to directory-enable your applications is the Java Naming and Directory Interface (JNDI) developed by Sun Microssystems.

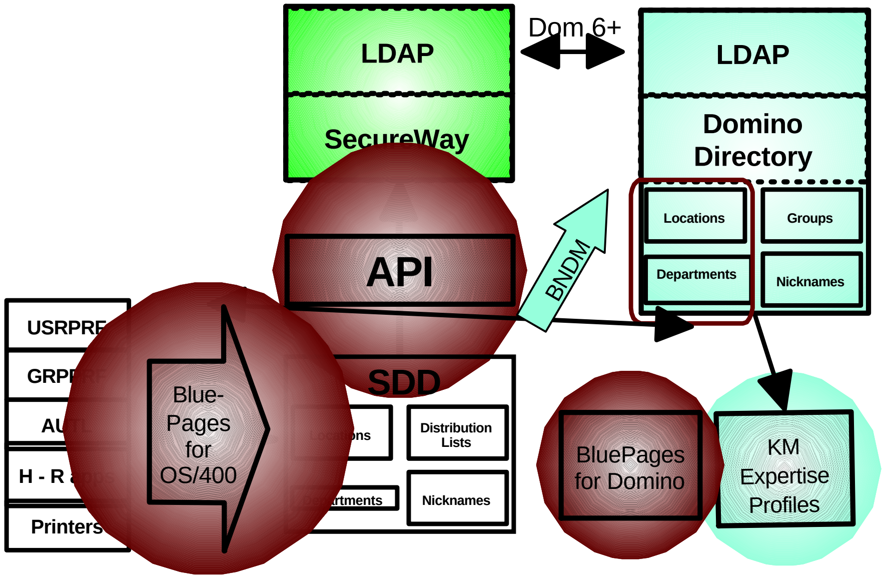
For example, JNDI could be used to retrieve files from a file system. In this case, a file system acting as a naming service could return the file that is bound to a particular file name. JNDI could also be used to access an LDAP directory, performing searches and retrieving attributes. This redbook *Implementation and Practical Use ofm LDAP on the IBM eServer iSeries Server,* SG24-6193 shows you, based on a sample application, how to use the JNDI interface.

BlueNotes Directory Synchronisation

Member of IBM BlueNotes family of OS/400-Domino integration products

OS/400 to LDAP Enablement

- Publishing of User Profiles to System Distribution Directory
- Publishing of SDD to SecureWay (via API)
- Hence OS/400 to Domino Directory Integration
  - Automated referrals and/or import of LDAP to Domino
  - Domino 6 dirsynch substitute



Directory Consolidation

- for iSeries and/or Domino

Notes BlueNotes Directory Synch

The BlueNotes suite of products provide complete office productivity. They provide integration between servers (including IBM eServer iSeries, xSeries (and other Intel platforms), pSeries (and other UNIX platforms)) and Lotus Domino and Notes. They improve efficiency and productivity in an office workplace environment. The BlueNotes Suite is developed by Typex and marketed by IBM and Typex. BlueNotes products can be used to enhance and automate directory management tasks as well as utilizing directory data for Knowledge Management, CRM, and other applications.

The BlueNotes Directory tool has two optional modules which provide directory integration and enhancement of the Domino Directory.

The BlueNotes Directory Synchronisation module adds selected OS/400 user profiles to the System Distribution Directory, exports them to the IBM SecureWay directory which is LDAP enabled and then makes them available to the Domino Directory, hence providing a replacement for the Domino DirSynch function withdrawn in Domino 6 for OS/400.

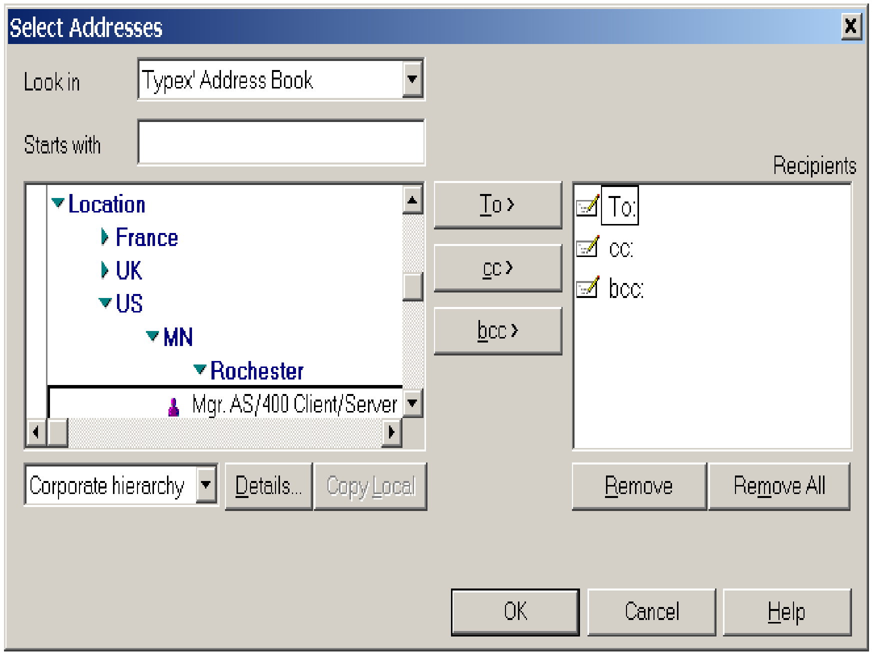
Clearly, this product in the suite is the one with the most impact in Directory projects. The close affinity with OS/400's SDD, SecureWay Directory and Domino means that it is used to obtain and maintain a common, cross-platform set of directory-related data and then to provide enhanced Domino user access to that data.

Future enhancements will focus on extracting further data from OS/400 and LDAP to populate Domino.

BlueNotes Directory Taxonomy

Administrator

- Imports selected Domino Directory fields
  - e.g. Location, Department, etc.
- Defines Enterprise Taxonomy
- set of hierarchical definitions of the organization
  - e.g. Americas/US/MN/Rochester, or IBM/Products/eServer/iSeries...
- Exports to Directory's Corporate Hierarchy



Select Addresses

Look in: Typex' Address Book

Starts with:

Location
France
UK
US
MN
Rochester
Mgr. AS/400 Client/Server

Corporate hierarchy

End User

- Gains hierarchical view of Directory
  - Easier to find people

Taxonomy can populate other databases

Notes BlueNotes Directory Taxonomy

The BlueNotes Directory Taxonomy for Domino module provides users with hierarchical views of the Domino Directory when selecting addresses. A four-category, seven-level enterprise taxonomy can be defined for people-related information based on Directory fields such as Department, Location and Internet address. The taxonomy database then updates Corporate Hierarchy Information in the Directory's Person documents.

The same taxonomy is also available to categorize data in other Notes applications including BlueNotes Document Warehouse and MailStore for Domino.

5. LDAP and Applications

Introduction

Directory-enabled Applications

- Nowadays use LDAP mostly for:
  - storing and retrieving configuration information
  - user authentication

Advantages

- Consolidating configuration and user information
- Reduces administration and maintenance efforts
- Users need to remember only a single user/password for all applications

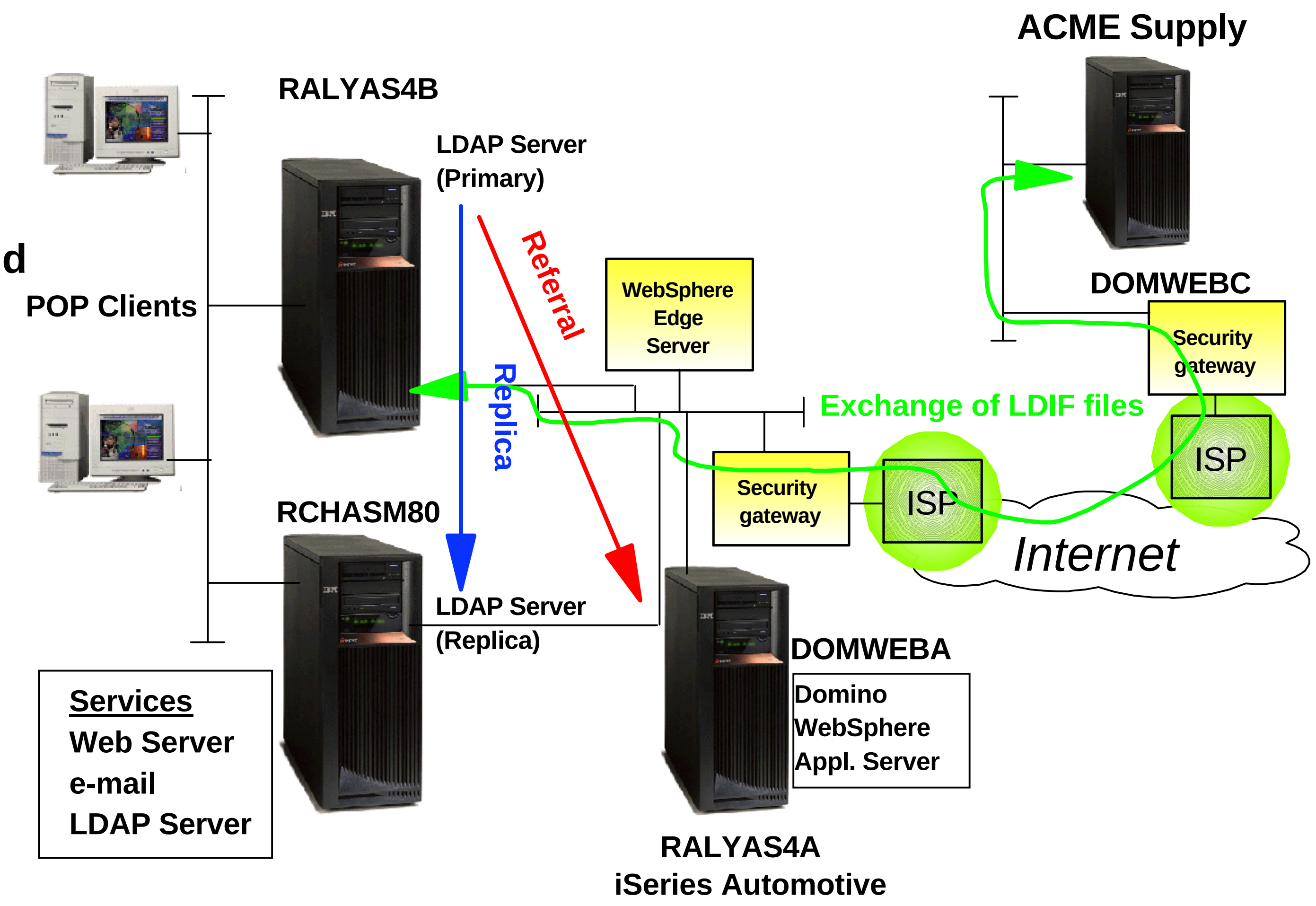
Key LDAP-enabled iSeries products

- WebSphere (Application Server, Host On-Demand, Commerce Suite)
- Domino
- HTTP Server (original) and (powered by Apache)
- e-mail clients

Introduction (cont'd)

New IBM Redbook *Implementation and Practical Use of LDAP on the IBM eServer iSeries Server,* SG24-6193

- Uses an example scenario to explain the implementation and practical use of LDAP for many applications
- Scenario starts with a company that uses only the SDD as a directory and evolves over several stages to activating and using an LDAP directory for configuration and authentication purposes



Notes Introduction

Directory-Enabled Applications

OS/400 and many other applications are already LDAP enabled. They utilize LDAP directories for various purposes, such as storing and retrieving configuration information, for user authentication, and so forth.

The key LDAP-enabled applications running on iSeries server include WebSphere, Domino, HTTP Server and a wide variety of e-mail clients.

The real advantage of implementing directory services is reusing directory data for various purposes in different applications. LDAP directory implementations also provide functions to improve scalability and availability. Bearing this in mind, the redbook explains LDAP directory planning, implementation, and management by using an example scenario throughout the book.

Scenario

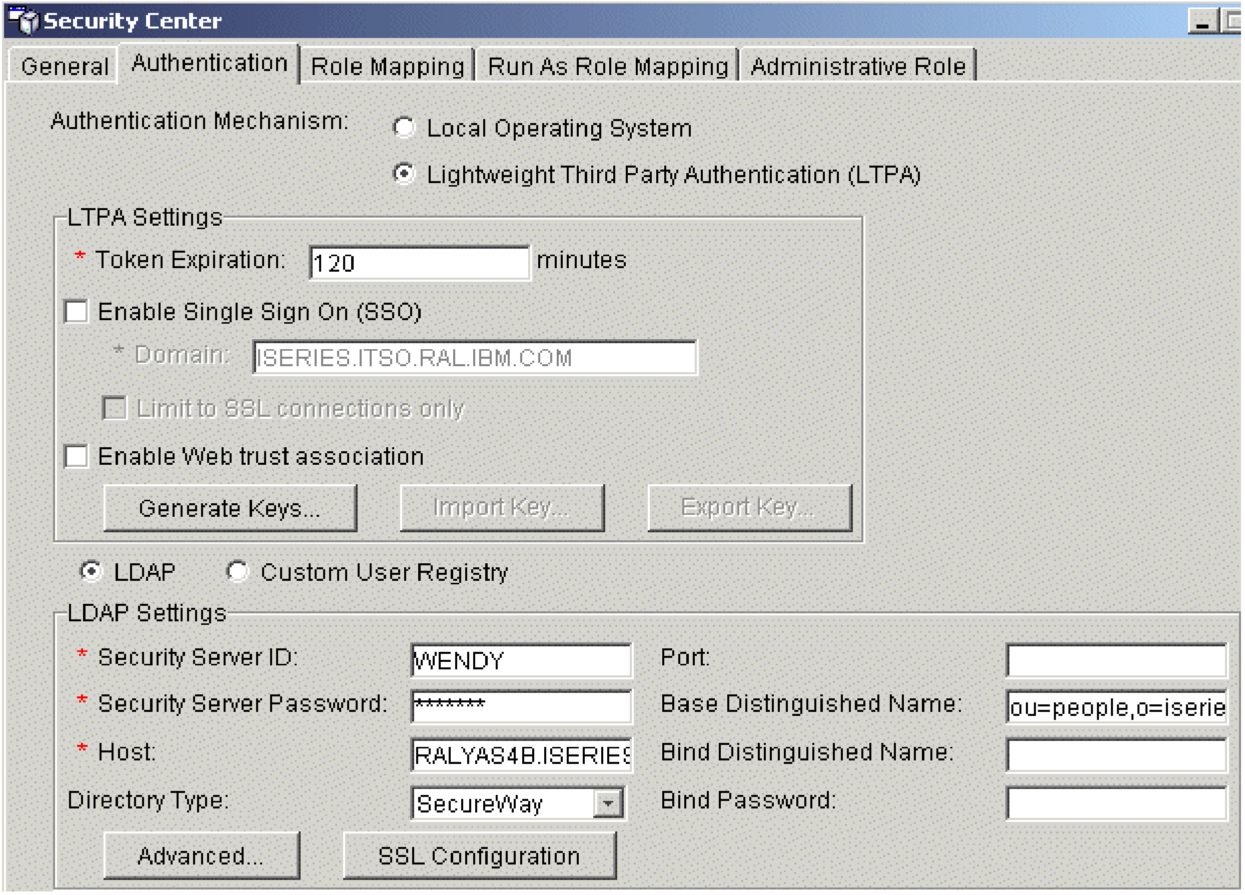
- 1. Customer uses SDD to maintain an OS/400 directory of users and partners.
- 2. On two iSeries servers the customer runs HTTP intranet servers (powered by Apache). One server is the primary and one the backup server. Users need to authenticate to access confidential information. Initially an administrator manually adds new users to a validation list (authentication). The user information entered is based on SDD information. Company deploys authentication using LDAP a directory. They also store the Web server configuration in the directory allowing them to extend their server cluster without maintaining multiple sets of configuration files.
- 3. Customer plans to deploy a Web application using Domino and WebSphere. Users need to authenticate to use these services. Application is used by business partners and employees. Single Sign-On (SSO) is the solution.
- 4. Company has acquired two other firms. In the enterprise they use now three different mail clients. We use an enterprise address book with LDAP to allow individual mail clients to find the recipients mail addresses and other information (phone number, location, etc.).
- 5. To keep directory information current, an user interface will be written to allow people to update their own information. However, they should only be able to update phone number, location, job responsibility, and their user password. This scenario introduces APIs and JNDI.

WebSphere Application Server

High-performance, scalable platform for dynamic e-business applications handling transactions and extending back-end business data and applications to the Web

LDAP-enabled for authentication

- allows Single Sign-On
- can use SecureWay, Domino or any other LDAP-enabled directory



Authentication Mechanism: ○ Local Operating System ● Lightweight Third Party Authentication (LTPA)

LTPA Settings

* Token Expiration: 120 minutes

□ Enable Single Sign On (SSO)

* Domain: ISERIES.ITSO.RAL.IBM.COM

□ Limit to SSL connections only

□ Enable Web trust association

● LDAP ○ Custom User Registry

LDAP Settings

* Security Server ID:	WENDY	Port:	
* Security Server Password:	*******	Base Distinguished Name:	ou=people,o=iserie
* Host:	RALYAS4B.ISERIES	Bind Distinguished Name:	
Directory Type:	SecureWay	Bind Password:	

WebSphere. software

Notes WebSphere Application Server

You can use Single Sign-On (SSO) to allow users to log on once per session rather than requiring them to log on to each resource or application separately. The applications could be on the same or different physical servers. SSO implies that a user will not be prompted for authentication credentials more than once during a session. WebSphere Application Server supports third-party authentication, a mechanism for achieving single sign-on across the Internet domain that contains your resources. You can use single sign-on to allow users to log on once per session rather than requiring them to log on to each resource or application separately. A mechanism called Lightweight Third Party Authentication (LTPA). LTPA can use a trusted third-party Lightweight Directory Access Protocol (LDAP) server, or a custom user registry to authenticate the user. LTPA supports the basic form and client certificate authentication methods. All server participating in the SSO realm need to belong to the same TCP/IP domain.

Note that WebSphere is acting as a LDAP client in that it passes authentication requests to an LDAP server.

Lotus Domino

The premier platform for collaborative Web applications

Domino Directory

- is basis for all application security
- is LDAP V3 enabled

Domino can authenticate users via information stored in a LDAP directory

Domino can participate in a SSO domain with WebSphere Application Server

Notes Lotus Domino

By way of contrast with WebSphere, Domino can act in a variety of roles in an LDAP context.

Domino as LDAP Server

Domino can be an LDAP server to respond to SSO-based authentication requests from other applications such as WebSphere. It can also handle LDAP queries.

Domino as LDAP Client

Domino can act as an LDAP client and passes authentication requests to an LDAP server such as WebSphere.

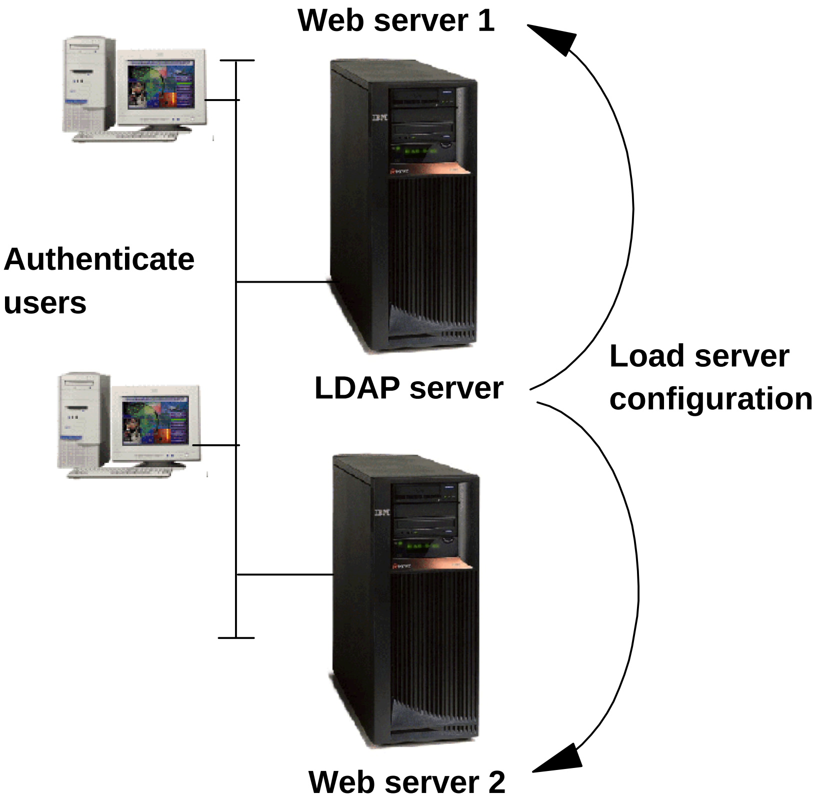
In addition, Lotus Notes, a client to Domino, can pass authentication requests to an LDAP server other than Domino.

Lotus Domino can also participate in an LTPA-based Single Sign-On (SSO) domain. The L2PA-based SSO concept can currently be used with WebSphere Application Server, Lotus Domino, Tivoli Policy Director, and new also with WebSphere Commerce Suite.

HTTP Server

A complete Web server product which offers:

- Two types of Web servers (original and powered by Apache)
- Java Servlet and JavaServer Pages
- Webserver Search Engine and Web Crawler
- Highly Available HTTP Server
- Triggered Cache Manager
- Advanced security and application development features



Can use LDAP for:

- authentication
- loading server configuration

IBM HTTP Server for iSeries

Notes HTTP Server

Authentication

The HTTP Server for iSeries allows you to minimize user and configuration administration and management by leveraging LDAP directory services. You can use the LDAP server for authenticating Web users that want to access protected

resources on your HTTP Web server. The advantage of using a centralized storage for user information is that many different applications, such as WebSphere Application Server, Lotus Domino, and HTTP Server, can use authentication information that is kept in a single directory. For example, a user needs to change his password only once and all applications that use LDAP for

authenticating users will perform authentication with the changed user password. Authentication verifies that users are who they say they are. A user name and password is a basic authentication. Once users are authenticated, it must be determined if they have the authorization or permission to perform the requested operation on the specific object.

Load Configuration

Another feature of the HTTP Server for iSeries allows you to store server configuration directives in an LDAP directory. This is especially useful when operating a cluster of servers that are used for load sharing or backup purposes.

In this case, the webmaster has to maintain only one set of configuration directives that are shared by all servers.

Note: The IBM HTTP Server for iSeries does not support Single Sign-On. Therefore, a customer would have to authenticate once to the Web server and another time for the Web applications running on the server. The Tivoli Policy Director is a product that also supports Single Sign-On. By combining the SSO capabilities of Tivoli’s Policy Director, WebSphere Application Server, and Lotus Domino a user would have to authenticate only once. For more information about Tivoli products, refer to: http://www.tivoli.com

e-mail clients

Most of the popular e-mail client applications in the market are LDAP-enabled

- Lotus Notes
- Netscape Messenger
- Microsoft Outlook

e-mail clients use LDAP directory for address lookup

- multiple LDAP directory configuration supported
- depending on e-mail client, search can be initiated using various search criteria
- watch out for different search behavior

Notes e-mail clients

Everybody knows the hassle of keeping individual address books for different mail clients or other applications. For example, some users might use Outlook as their mail client while others might use Netscape Messenger or Lotus Notes.

Maintaining address books for each software product requires some effort and many companies cannot afford this luxury. One solution would be to maintain a single company-wide or cross-company directory that contains information about all employees, contractors, customers, and so forth. Then, whatever mail client is used to send an e-mail to one of these recipients, the recipient’s e-mail address can be easily retrieved from the central directory. An LDAP directory is the right choice, since most of the currently available mail clients support LDAP search capabilities.

Searches can be performed by specifying different search criteria. Most e-mail clients provide a GUI that allows you to compose a search filter. However, the way how searches are performed and when clients automatically extend searches to other configured directories varies for each client.

Additional Information

Appendix: Directory Futures & Trends

Dominance of LDAP

DSML

Directory-Enabled Applications

Directory-Enabled Networks

Metadirectories

Directories and databases

Database Tools

OS Integration

More Content Types

Remote Printing

Knowledge Management

Taxonomies

Pervasive Access

Applications & Infrastructure

Extranet/Internet Directories

Organizational Sharing

Reuniting Friends

Genealogy

One World?

Notes Directory Futures & Trends

Appendix D speculates on trends and possible future directions in the world of directories. The views expressed here for information and guidance are not necessarily those of IBM Corporation.

Dominance of LDAP

LDAP directories continue to dominate the directory services arena. Few people would plan to implement a new non-LDAP directory today. Directory products continue to enhance their LDAP capabilities. The support of the major application and operating system vendors for LDAP means that it is a de facto standard. There is no sign of an end to this trend and nor do we expect to see one.

DSML

Directories are increasingly storing metadata about available Web services, what they do, what they require for input, how to execute them, what the results will be, who wrote them and how to pay for them. The definition of the XML schema for describing directory structure and data is Directory Services Markup Language (DSML). Lotus has committed to DSML V2 for the Domino Directory.

Directory-Enabled Applications

A directory-enabled application is an application that uses a directory service to improve its functionality, ease of use, and administration. Several leading ERP companies have directory-enabled their applications. This is a trend that should, in the short term, spread to other vendors' as well as customers' applications.

Directory-Enabled Networks (DEN)

The DEN specification is designed to provide the building blocks for more intelligent networks by mapping users to services, and mapping business criteria to the delivery or network services. This will enable applications and services to leverage network infrastructure, empower end-to-end services, and support distributed network-wide service creation, provisioning and management.

Metadirectories

The term Metadirectory is used to describe a variety of ways of maintaining directory coexistence. It is an alternative to a single, shared directory solution. A metadirectory contains information about all other relevant directories and maintains synchronicity with them. As the number of servers grows users will have many combinations of user IDs and passwords. LDAP directories and Metadirectories are one of the most effective solutions to this problem. You can encrypt user IDs and passwords stored in the LDAP directory. This trend will eventually lead to the complete elimination of user IDs and passwords. By using certificates instead of ID/password pairs, companies can better secure their networks. Several companies implement these solutions today, at least for network signon. Coupled with the growth of directory-enabled applications, we expect ever-increasing support for these solutions.

Notes Directory Futures & Trends

Directories and databases

A directory is more than a limited-function database but some products, such as SecureWay, use a relational database under the covers. Proposals are being discussed to add database functions such as for transactional update to future versions of LDAP.

Database Tools

We expect to see those tools that provide access to databases to extend their range to cover LDAP. One such example BlueNotes Direct Messaging, which performs the 'letter-merge' function of a word processing tool but can also do so based on Domino Directory and can use the directory to route the output to e-mail, fax, print or Web posting according to customer preferences.

OS Integration

Directory vendors are increasingly tying their directory service into the operating systems upon which they run. In the case of the iSeries the SecureWay directory was always a free, optional part of OS/400. At V5R1 it became fully integrated with the operating system. Some may argue that this diminishes the importance of the server operating system. Application developers no longer need to tie themselves to specific operating systems. To an extent this is true, but then of course for highly manageable, scalable and reliable operating systems like OS/400 this may be an opportunity. The majority of new applications will be able to run on the customer's choice of the best platform without this being dictated by the application, and the large installed base of existing native applications can readily be network-enabled without a migration.

More Content Types

To date we have seen directories largely used as repositories of information about people. Increasingly we are seeing the addition of printers, servers, and even File System links, to the directory. We expect this trend to accelerate.

Remote Printing

A remote user can access an LDAP directory to locate a suitable printer and to prints directly to it across the Internet. IBM's latest InfoPrinters even have an inbuilt Web server that enables him to respond to printer messages when addressed in this way. We expect these remote printing scenarios to grow strongly in the near future both for traveling staff and public print shops.

Notes Directory Futures & Trends

Knowledge Management

KM is all about finding the right expert with the right knowledge in the right place at the right time. The three cornerstones of KM are known as 'People, Places and Things'. Clearly, a clean, up-to-date, secure and accessible list of people, both inside and outside of the organization, must be at the heart of KM. The Directory is the ideal place for this. One of the key steps in preparing for KM is clearly to clean up your directory. As KM grows in importance as an application so, we believe, will directories and the role they play in KM.

Taxonomies

One of the core components of Knowledge Management is a taxonomy - a set of hierarchical definitions of an organization and its attributes. Lotus Domino Corporate Hierarchy Information fields in the Person document provide for four six-level hierarchical structures and allow users to 'drill down' through the directory and find users by department or job title without necessarily even knowing their names. The BlueNotes Directory Taxonomy for Domino product provides a way for the administrator to build the taxonomy and automatically apply it to these fields. We can expect to see this trend of requiring more intelligent views of the data to spread.

Pervasive Access

Now think of directory users with a smaller device 'footprint' - that of a mobile cell phone or palmtop device. These users are on the ideal platform to require the fast lookup of a telephone number. We expect this form of access to grow and we think that the taxonomy-based view of the directory will enable better navigation than scrolling through thousands of surnames.

Applications & Infrastructure

Lotus has announced an intention both for Domino Directory to be used by non-Lotus applications as at present and also for Lotus applications, potentially such as Notes, to be used with non-Domino LDAP-enabled directories. This means that the applications become separated even further from the infrastructure. We expect other vendors to follow this lead.

Extranet/Internet Directories

Most directories today are wholly or largely contained within the organization. As you have seen from the Scenario in this Redbook, it is now both feasible and in many cases desirable to extend this to a broader group of enterprises. Firms like IBM already make available their entire worldwide e-mail directory in the Web via LDAP and many more do so every day. This we expect to be the major trend in the near future. It will become commonplace for people to use the Web and LDAP, rather than a call center or switchboard, to find an appropriate member of staff in your organization.

Notes Directory Futures & Trends

Organizational Sharing

Rather than just publish directories as above, the Scenario in this Redbook has also shown how the directories from one organization can be replicated to another. Taking this trend a stage further we might expect whole communities, for instance IBM and its 95,000 Business partners, to share directory information securely in this way. One advantage of this is that the BP could add further information to the IBMer's entries about their relationship with them, for instance, who is the contact for a particular product or marketing program. They could also work with an off-line copy of the directory for mobile workers. Other sectors where shared semi-private databases of people-based information would be useful include government (particularly the security services), missing persons bureaus, medical records and credit control.

Reuniting Friends

The recent success of the Friends Reunited Web site (www.friendsreunited.co.uk) that allows you to find out what your old school or workplace friends are now doing illustrates the popularity of public sites to look for people. This trend could reach the stage where you can identify the majority of Web users in the world, albeit through separate sites at this stage.

Genealogy

Some of the largest non-governmental people-based databases in the world include those providing genealogical information. These are of two main kinds. The first consists of simple listings such as church burials or immigration records where the people entries are otherwise unrelated. The second is more structured sets of family trees where the genealogy (ancestors, siblings, descendants) is part of the database structure. In the brief time available to the researchers of this Redbook we found only limited use of LDAP in such databases but it would make the searching for relatives, ancestors and descendants much easier. Conversely, the current LDAP standards do not appear to support genealogy-based Schemas. Both developments would seem to be predictable.

One World?

Taking these three last items to their logical conclusion, we may well reach the point where a single worldwide directory image emerges, at least for people-based entries. Such an image need not and would not contain all the data from all the constituent directories because most of the searches would be handled by referrals, but we could reasonably expect to see at least the ability to perform one worldwide search to find a person's e-mail address.

Related Publications

- ***The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this workshop.***

International Technical Support Organization Publications

- For information on ordering ITSO publications, visit us at **http://www.redbooks.ibm.com** (Internet Web site) or
- **http://w3.itso.ibm.com** (intranet Web site)

For Technical Support see http://www.ibm.com/support and **http://w3.ibm.com/support**

Redbooks on CD-ROMs

- Redbooks are available on CD-ROMs.

CD-ROM Title	**Collection Kit Number**
System/390 Redbooks Collection	SK2T-2177
Networking and Systems Management Redbooks Collection	SK2T-6022
Transaction Processing and Data Management Redbook	SK2T-8038
AS/400 Redbooks Collection	SK2T-2849
RS/6000 Redbooks Collection (HTML, BkMgr)	SK2T-8040
RS/6000 Redbooks Collection (PostScript)	SK2T-8041
Application Development Redbooks Collection	SK2T-8037
Personal Systems Redbooks Collection	SK2T-8042

Related Publications - Continued

Other Publications

- ***These publications are also relevant as further information sources:***

Title	Publication Number
Implementation and Practical Use of LDAP on the IBM eServer iSeries Server	SG24-6193
Understanding LDAP	SG24-4986
LDAP Implementation Cookbook	SG24-5110
Using LDAP for Directory Integration: A Look at IBM SecureWay Directory, Active Directory, and Domino	SG24-6163
IBM eServer iSeries Wired Network Security	SG24-6168
Getting the Most from Your Domino Directory	SG24-5986

Related Publications - Continued

Other Publications

- ***These publications are also relevant as further information sources:***

Title	Publication Number
Domino and WebSphere Integration on iSeries	SG24-6223
Lotus Domino for AS/400 R5: Implementation	SG24-5592-01
e-Directories - Enterprise Software, Solutions, and Services, Addison Wesley	ISBN 0-201-70039-5

More Information

Web Sites

- IBM ITSO Redbooks
  - http://www.ibm.redbooks.com
- Technical documentation
  - http://www.ibm.com/support/techdocs
- iSeries LDAP
  - http://www-1.ibm.com/servers/eserver/iseries/ldap/
- Lotus Domino
  - http://www.lotus.com/home.nsf/welcome/domino
- IBM SecureWay Directory
  - http://www.ibm.com/software/network/directory/
- IBM WebSphere
  - http://www.ibm.com/software/info1/websphere/index.jsp
- IBM public LDAP Directory
  - http://whois.ibm.com
- BlueNotes Product Suite
  - http://www.bluenotes.com

More Information - Conference

Related Conference Sessions

- 13MA LDAP, Domino & iSeries - The Redbook
- 16MF File Server Consolidation with Domino & iSeries
- 36MB Domino and iSeries Integration with BlueNotes
- 37PD Get Ready for Knowledge Management

Summary

What Have We Learned?

- Importance of directories
- Significance of LDAP
- Strength of iSeries
- LDAP role on iSeries and in Domino, WebSphere, and HTTP Server

Suggested Actions

Order the Redbook

Review your directories

Develop your strategy

- Adopt LDAP as standard

Review your applications

Clean up and consolidate

Questions?

Contact me

- John Taylor, Typex
- +44 191 256 4406
- john_taylor@typex.com

...and while you are thinking of questions....

- your evaluation forms please