Directory

LDAP Features for Certification, Version 2

The Open Group

Directory

LDAP Features for Certification, Version 2

Document Number: I041

Published in the U.K. by The Open Group, April 2004.

Any comments relating to the material contained in this document may be submitted to:

The Open Group
Apex Plaza
Forbury Road
Reading
Berkshire, RG1 1AX
United Kingdom

or by Electronic Mail to:

OGSpecs@opengroup.org

Contents

Chapter 1

Introduction

This document presents an analysis of the features of the Lightweight Directory Access Protocol, Version 3 (LDAP v3), as a basis for the LDAP Certified V2 Product Standard.[1]

LDAP v3 is specified by the Internet Engineering Task Force (IETF) in a number of their Requests For Comments (RFCs). These RFCs are identified by *IETF RFC 3377*.[2] They specify the protocol, but do not completely specify the requirements for LDAP clients or servers. For example, a server is not required by the RFCs to carry out all operations requested by clients through the protocol; it may return an ‘‘unwilling to perform’’ response to an operation.

This presents a problem for organizations that wish to use products that are LDAP clients or servers. Those organizations need to know whether servers will support the client applications that they want to use, and need to know whether client applications will interoperate with the servers that they have.

The *LDAP Certified* and *LDAP Ready* certification programs meet these needs for information. A server that is LDAP Certified is warranted by its vendor to support a particular set of clearly identified features of LDAP. Such a set of features is an *LDAP Profile*. An application that is LDAP Ready is warranted by its vendor to interoperate with any LDAP Certified server that supports the LDAP Profile that it requires.

This document contains:

- An Overview of Directory Solutions
- Descriptions of the LDAP Profiles that LDAP Certified servers can support
- A list of LDAP features that:
  - — Describes each feature
  - — Identifies the RFC sections and other places where each feature is specified
  - — States to which profile each feature belongs

The functional requirements that LDAP servers must meet in order to be LDAP Certified are stated in the LDAP Certified V2 Product Standard. The options within the LDAP Certified V2 Product Standard that products support are detailed in their *LDAP Certified Conformance Statements*. The features that LDAP Ready products require are detailed in their *LDAP Ready Conditions Statements*.

The LDAP Certified V2 Product Standard, LDAP Certified Conformance Statements, and LDAP Ready Conditions Statements make normative references to the descriptions of LDAP Profiles in Chapter 3 and the list of LDAP Features in Chapter 4.

1. Brand Program Documentation, April 2004, Directory: LDAP Certified V2 (X04DJ), published by The Open Group.
2. IETF RFC 3377, Lightweight Directory Access Protocol (v3): Technical Specification, September 2002.

The overview of Directory Solutions in Chapter 2 is presented for information purposes. It does not state any normative requirements on products for LDAP Certified or LDAP Ready certification.

Chapter 2

Directory Solutions

Many solutions to the problems of managing and operating enterprises rely on directory technology. The following is not an exhaustive list, and there is much overlap between its members, but it does give an indication of the prevalence and value of directory-based solutions.

2.1 Authentication and Discovery

These solutions use directory infrastructure to authenticate users' usage of the network, of system resources, or of applications.

A simple example that fits into this category is *auth_ldap* from the Apache.org module list. This is an LDAP authentication module that allows Apache to authenticate HTTP clients using user entries in an LDAP directory. This module performs:

- Either anonymous or authenticated binds with or without TLS
- Verification using DN comparison
- Verification using group membership
- Support for startTLS

Authentication and discovery solutions typically use features from all feature groups.

2.2 Data Storage

This is the use of a directory to store, manage, and retrieve data. Typically this data will encompass application configuration and application-specific data that pertains to the solution. Solutions in this category include basic data management functionality such as add, delete, rename, and modify.

2.3 Directory-Enabled Networking (DEN)

The Directory-Enabled Network (DEN) initiative is designed to provide the building blocks for more intelligent management by mapping concepts such as systems, services, and policies to a directory, and integrating this information with other elements in the management infrastructure. This utilizes existing user and enterprise-wide data already present in a company's directory, empowers end-to-end services, and supports distributed network-wide service creation, provisioning, and management.

The concepts that are mapped are derived from the Common Information Model (CIM) of the *Distributed Management Task Force*.

The goals of the DEN effort are to use a directory as follows: first to ‘‘direct’’ clients to relevant management services, and second to hold a subset of management data. Current efforts are focused on defining directory schema and usage for:

- Common identity and security administration
- Common understanding of managed systems and services
- Information related to locations, groupings, and policy

2.4 Identity Management

Identity Management is the process of identifying, storing, and managing individual, group, and network resource information. This is most often done using a directory as a repository for the managed information. Today, the information managed (identities) can be utilized in a myriad of applications from simple password verification to complex PKIs.

Facilities that utilize directory services include:

- Provisioning (to include add, change, and delete) for individuals and network resources
- Password management
- Application and network resource access privileges
- Group membership
- External (web-based) resource access (for customers, suppliers, partners, and so on)
- Policy provisioning (for example, for access and security)
- Quality of Service and Service Level Agreement (SLA) parameters

The ultimate (identity) information that is managed will have a plethora of uses including authentication, authorization, application access, role-based privilege determination, and information distribution.

For security purposes, the directory must also ensure that communication between the management applications and the directory can itself be secured using protocols such as TLS.

2.5 Public Directory

All companies and organizations manage information on their employees and customers, networks, devices and applications, products and services, and much more. These directories are used both for reference purposes and as the basis for a growing number of applications such as e-business, e-procurement, white/yellow pages, public key infrastructure services (PKI), single sign-on applications, messaging systems, or computer telephony integration, to name just a few. Directories are used as public directories in Internet, intranet, extranet, Web portal, or service provider environments. As a basis for identity management, they manage user and subscriber profiles, digital certificates for PKI services, authentication and authorization information, access permissions, and other relevant attributes for users and subscribers to provide secure access to information, network resources, or distributed services.

Directories are also incorporating solutions to allow their users to access directory information in a number of different ways. Besides web browser access and access via application programming interfaces, which today comes as standard with most directory products, the other trend is access via wireless devices, such as PDAs and cell phones. Since directories are designed to support multiple applications and platforms, it makes their adherence to standards a must to make sure that they are compatible with other directory solutions and applications on the market.

While data stored in a public directory is accessed in read-only mode by search and read operations, directory operations like add, modify, or delete operations are also required to manage directory contents. Many public directory solutions also require that users and applications authenticate when binding to a directory service. In the world of e-business, controlling access to security-critical information is of greater importance than ever before.

2.6 Reporting

Many directory applications read information from directories but do not add to or change the directory contents. They include ‘‘white pages’’, report creation, and auditing.

They typically use features from all the feature groups except Storage and Update.

2.7 Security

These solutions use directory resources and facilities, in conjunction with specific security functionality, to protect and safeguard all online resources. Common examples of directory-supported security applications include:

- Single or Simplified Sign-On (SSO)
- Secure Messaging (S/MIME)
- Public Key Infrastructure (PKI)
- Virtual Private Network (VPN)
- Access Control (AC) and Role-Based Access Control (RBAC)
- Firewall
- Demilitarized Zones (DMZ)
- Certificate-based ‘‘tunneled’’ encryption such as SSL and TLS

- Token-based authentication and authorization (such as smartcards or biometrics)

A common aspect of all these applications is authorization and, to a lesser degree, authentication.

For true security, the directory must also ensure that communication between the applications and the directory can itself be secured using protocols such as TLS.

Chapter 3

LDAP Profiles

This document defines two profiles for LDAP Certification: the BASE profile and the STANDARD profile. It also identifies features that will form part of an ADVANCED profile or of several distinct ADVANCED profiles. The definition of this profile (or of these profiles) is for further study.

3.1 BASE Profile

The BASE profile includes the most commonly used LDAP features. Applications that use only features from the BASE profile will be relatively simple to create, and can expect good interoperability with most LDAP servers.

A server supports the BASE profile if it implements all of the features marked as ‘‘BASE’’ in Chapter 4.

3.2 STANDARD Profile

The STANDARD profile includes the most commonly implemented LDAP features. Applications that use only features from the STANDARD profile may be relatively complex to create, but can still rely on interoperability with LDAP Certified servers that support the STANDARD profile.

A server supports the STANDARD profile if it implements all of the features marked as ‘‘BASE’’ or as ‘‘STANDARD’’ in Chapter 4.

3.3 ADVANCED Features

Features that are not marked as ‘‘BASE’’ or as ‘‘STANDARD’’ in Chapter 4 are marked as ‘‘ADVANCED’’. These features are required by relatively few applications, generally of a specialized nature. Applications that do use these features are unlikely to interoperate with a wide range of LDAP servers.

The extension of profiling and certification to these features is for further study.

Chapter 4

LDAP Features

This section lists the features of LDAP v3 as defined in *IETF RFC 3377*.

For the purposes of this analysis, a *feature* is: ‘‘a capability provided by directories to clients though the LDAP protocol’’.

IETF RFC 3377 describes no LDAP features, but it references eight other RFCs which, together with IETF RFC 3377, make up the specification of the Lightweight Directory Access Protocol, Version 3 (LDAP v3). Those RFCs are:

- *IETF RFC 2251*: Lightweight Directory Access Protocol (v3), December 1997. (The specification of the LDAP on-the-wire protocol.)
- *IETF RFC 2252*: Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions, December 1997.
- *IETF RFC 2253*: Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names, December 1997.
- *IETF RFC 2254*: The String Representation of LDAP Search Filters, December 1997.
- *IETF RFC 2255*: The LDAP URL Format, December 1997.
- *IETF RFC 2256*: A Summary of the X.500(96) User Schema for use with LDAP v3, December 19997.
- *IETF RFC 2829*: Authentication Methods for LDAP, May 2000.
- *IETF RFC 2830*: Lightweight Directory Access Protocol (v3): Extension for Transport Layer Security, May 2000.

The features listed in this section are confined to those described in the above RFCs. There are other RFCs that describe extensions to LDAP v3. As of November 2002, these are:

- *IETF RFC 2589*: Lightweight Directory Access Protocol (v3): Extensions for Dynamic Directory Services, May 1999.
- *IETF RFC 2596*: Use of Language Codes in LDAP, May 1999.
- *IETF RFC 2696*: LDAP Control Extension for Simple Paged Results Manipulation, September 1999.
- *IETF RFC 2891*: LDAP Control Extension for Server Side Sorting of Search Results, August 2000.

The inclusion in profiles of features defined in RFCs that are not referenced by IETF RFC 3377 is for further study.

The features are listed below by feature group.

Certain aspects of some features are not completely described by the RFCs, and the feature descriptions include substantive additions to the RFC provisions. These cases are indicated by the word ‘‘Here’’ in the ‘‘Specified’’ column of the list.

4.1 Publication

Feature	Description	Specified	Profile
Core Operational Attributes	The server implements and maintains the values of the core operational attributes *createTimestamp*, *modifyTimestamp*, *creatorsName*, *modifiersName*, *subschemaSubentry*, *attributeTypes*, and *objectClasses*.	IETF RFC 2251 §3.2.1 IETF RFC 2252 §5 IETF RFC 2252 §5.1 IETF RFC 2252 §5.1.1 IETF RFC 2252 §5.1.2 IETF RFC 2252 §5.1.3 IETF RFC 2252 §5.1.4 IETF RFC 2252 §5.1.5 IETF RFC 2252 §5.1.6 IETF RFC 2252 §5.1.7	Standard
Matching Rules Attribute	The server implements and maintains the values of the *matchingRules* operational attribute.	IETF RFC 2251 §3.2.1 IETF RFC 2252 §5 IETF RFC 2252 §5.1 IETF RFC 2252 §5.1.8	Advanced
Matching Rule Use Attribute	The server implements and maintains the values of the *matchingRuleUse* operational attribute.	IETF RFC 2251 §3.2.1 IETF RFC 2252 §5 IETF RFC 2252 §5.1 IETF RFC 2252 §5.1.9	Advanced
LDAP Syntaxes Attribute	The server implements and maintains the values of the *ldapSyntaxes* operational attribute.	IETF RFC 2251 §3.2.1 IETF RFC 2252 §5 IETF RFC 2252 §5.3 IETF RFC 2252 §5.3.1	Standard
RootDSE - LDAP v3	The server maintains a *supportedLDAPVersion* attribute in the root DSE that identifies the LDAP versions that it implements. These include LDAP v3.	IETF RFC 2251 §3.2.1 IETF RFC 2251 §3.4 IETF RFC 2252 §5 IETF RFC 2252 §5.2 IETF RFC 2252 §5.2.6	Standard
RootDSE - Controls	The server maintains a *supportedControl* attribute in the root DSE that identifies its supported controls.	IETF RFC 2251 §3.2.1 IETF RFC 2251 §3.4 IETF RFC 2252 §5 IETF RFC 2252 §5.2 IETF RFC 2252 §5.2.4	Advanced
RootDSE - Extensions	The server maintains a *supportedExtension* attribute in the root DSE that identifies its supported extended operations.	IETF RFC 2251 §3.2.1 IETF RFC 2251 §3.4 IETF RFC 2252 §5 IETF RFC 2252 §5.2 IETF RFC 2252 §5.2.3	Standard

Feature	Description	Specified	Profile
RootDSE - Naming Contexts	The server maintains in the root DSE a *namingContext* attribute that identifies the naming contexts held in the server.	IETF RFC 2251 §3.2.1 IETF RFC 2251 §3.4 IETF RFC 2252 §5 IETF RFC 2252 §5.2 IETF RFC 2252 §5.2.1	Standard
RootDSE - Alt Server	The server maintains an *altServer* attribute in the root DSE that identifies alternative servers that may be used when it is unavailable.	IETF RFC 2251 §3.2.1 IETF RFC 2251 §3.4 IETF RFC 2252 §5 IETF RFC 2252 §5.1 IETF RFC 2252 §5.2.2	Standard
RootDSE - Supported SASL Mechanisms	The server maintains a *supportedSASLMechanisms* attribute in the root DSE that identifies its supported SASL security features.	IETF RFC 2251 §3.2.1 IETF RFC 2251 §3.4 IETF RFC 2252 §5 IETF RFC 2252 §5.2 IETF RFC 2252 §5.2.2 IETF RFC 2252 §5.2.5	Advanced
DIT Structure Rules Attribute	The server implements and maintains the values of the *dITStructureRules* operational attribute.	IETF RFC 2251 §3.2.1 IETF RFC 2252 §5 IETF RFC 2252 §5.4 IETF RFC 2252 §5.4.1	Advanced
Name Forms Attribute	The server implements and maintains the values of the *nameForms* operational attribute.	IETF RFC 2251 §3.2.1 IETF RFC 2252 §5 IETF RFC 2252 §5.4 IETF RFC 2252 §5.4.2	Advanced
DIT Content Rules Attribute	The server implements and maintains the values of the *ditContentRules* operational attribute.	IETF RFC 2251 §3.2.1 IETF RFC 2252 §5 IETF RFC 2252 §5.4 IETF RFC 2252 §5.4.3	Advanced

4.2 Connection

Feature	Description	Specified	Profile
Client-Server Communication	When a client transmits a protocol request describing an operation to be performed to the server, the server performs the necessary operation(s) in the directory and, upon completion of the operation(s), the server returns a response containing any results or errors to the requesting client.	IETF RFC 2251 §3.1	Base
TCP as the transporting protocol	The server implements a mapping of LDAP over TCP in which the LDAP Message PDUs are mapped directly onto the TCP byte stream, and provides a protocol listener for this mode of operation on IP port 389 (it may also provide listeners on other ports).	Here IETF RFC 2251 §5.2.1	Base
SSL over TCP as the transporting protocol	The server implements a mapping of LDAP over SSL over TCP in which the LDAP Message PDUs are mapped directly onto the SSL byte stream, and provides a protocol listener for this mode of operation on IP port 636 (servers may also provide listeners on other ports).	Here	Base

Feature	Description	Specified	Profile
Transport Security - startTLS	The server allows a client to perform a Start TLS operation, and negotiates Transport Layer Security (TLS) as a result.	IETF RFC 2830 §2 IETF RFC 2830 §2.1 IETF RFC 2830 §2.2 IETF RFC 2830 §2.3 IETF RFC 2830 §3 IETF RFC 2830 §3.1 IETF RFC 2830 §3.2 IETF RFC 2830 §3.3 IETF RFC 2830 §3.4 IETF RFC 2830 §3.5 IETF RFC 2830 §4 IETF RFC 2830 §4.1 IETF RFC 2830 §4.2 IETF RFC 2830 §5 IETF RFC 2830 §5.1 IETF RFC 2830 §5.1.1 IETF RFC 2830 §5.2	Advanced
Notice of Disconnection	The server sends unsolicited notifications to signal extraordinary conditions in the server or in the connection between the client and the server. The server uses a Notice of Disconnection notification to advise a client that it is about to close the connection.	IETF RFC 2251 §4.4 IETF RFC 2251 §4.4.1	Standard

4.3 Authentication

Feature	Description	Specified	Profile
Anonymous Simple Bind	The server accepts a simple bind request where the password is of zero length, and treats the client as being anonymously authenticated. It also treats a client that has not bound successfully as anonymously authenticated.	IETF RFC 2251 §4.2 IETF RFC 2251 §4.2.2 IETF RFC 2251 §4.2.3 IETF RFC 2251 §4.3 IETF RFC 2829 §4 IETF RFC 2829 §5 IETF RFC 2829 §5.1	Base
Anonymous Bind over SSL	The server accepts a simple bind request over an SSL connection where the password is of zero length, and treats the client as being anonymously authenticated. It also treats a client connected by SSL that has not bound successfully as anonymously authenticated.	Here IETF RFC 2251 §4 IETF RFC 2251 §4.2 IETF RFC 2251 §4.2.2 IETF RFC 2251 §4.2.3 IETF RFC 2251 §4.3	Base
Anonymous Bind after START TLS	The server treats a client that has invoked TLS via START TLS but has not bound as anonymously authenticated, until the client uses the EXTERNAL SASL mechanism to negotiate the recognition of the client's certificate.	IETF RFC 2829 §4 IETF RFC 2829 §5 IETF RFC 2829 §5.2 IETF RFC 2829 §10	Advanced
Authenticated Simple Bind	The server accepts a simple bind request with the contents of the authentication field consisting of a password, and authenticates the client by that password.	IETF RFC 2251 §4.2 IETF RFC 2251 §4.2.2 IETF RFC 2251 §4.2.3 IETF RFC 2251 §4.3	Base
Simple Bind with Password exchange over SSL	The server accepts a simple bind request over an SSL connection with the contents of the authentication field consisting of a password, and authenticates the client by that password.	Here IETF RFC 2251 §4.2 IETF RFC 2251 §4.2.2 IETF RFC 2251 §4.2.3 IETF RFC 2251 §4.3	Base

Feature	Description	Specified	Profile
Simple Bind with Password exchange after START TLS	The server negotiates TLS following a START TLS request, and then accepts a simple bind request with the contents of the authentication field consisting of a password, and authenticates the client by that password.	IETF RFC 2829 §4 IETF RFC 2829 §6 IETF RFC 2829 §6.2 IETF RFC 2829 §10	Advanced
SASL Bind	The server accepts a SASL bind request and authenticates the client by the SASL credentials.	IETF RFC 2251 §4.2 IETF RFC 2251 §4.2.1 IETF RFC 2251 §4.2.2 IETF RFC 2251 §4.2.3 IETF RFC 2251 §4.3 IETF RFC 2829 §4 IETF RFC 2829 §9 IETF RFC 2829 §11	Advanced
Certificate-based authentication with TLS	The server negotiates TLS following a START TLS request, and authenticates the client by the user's TLS certificate.	IETF RFC 2829 §4 IETF RFC 2829 §7 IETF RFC 2829 §7.1 IETF RFC 2829 §10 IETF RFC 2830 §5.1.2 IETF RFC 2830 §5.1.2.1 IETF RFC 2830 §5.1.2.2 IETF RFC 2830 §5.1.2.3	Advanced
External SASL mechanism	The server accepts a SASL bind request specifying the SASL EXTERNAL mechanism and authenticates the client by information from a lower-layer protocol by using the SASL EXTERNAL mechanism.	IETF RFC 2251 §4.2.2 IETF RFC 2829 §4 IETF RFC 2829 §8	Advanced
SASL Bind - Digest-MD5	The server accepts a SASL bind request specifying the DIGEST-MD5 mechanism and authenticates the client by the DIGEST-MD5 mechanism.	IETF RFC 2829 §4 IETF RFC 2829 §6 IETF RFC 2829 §6.1	Advanced

4.4 Conversion

Feature	Description	Specified	Profile
Distinguished Name	The server correctly encodes and decodes protocol representations of distinguished names.	IETF RFC 2251 §4.1.3 IETF RFC 2253 §2 IETF RFC 2253 §2.1 IETF RFC 2253 §5	Base
Relative Distinguished Name	The server correctly encodes and decodes protocol representations of relative distinguished names.	IETF RFC 2253 §2.2 IETF RFC 2253 §2.3 IETF RFC 2253 §2.4 IETF RFC 2253 §5	Base
Parsing	The server correctly parses string representations of distinguished names.	IETF RFC 2253 §3 IETF RFC 2253 §5	Base
Relationship with LDAP v2	The server accepts but does not generate certain protocol constructs that are legal in LDAP v2 but not in LDAP v3.	IETF RFC 2253 §4 IETF RFC 2253 §5	Base

4.5 Retrieval

Feature	Description	Specified	Profile
Search	The server accepts search requests and performs the requested search operations.	IETF RFC 2251 §4.5 IETF RFC 2251 §4.5.1 IETF RFC 2251 §4.5.2	Base
Ability to dereference alias	The server supports alias objects and correctly handles references to them in search requests.	IETF RFC 2251 §4.5.1	Standard
Operational Attributes Retrieval	The server returns operational attributes in response to appropriate search requests.	IETF RFC 2251 §3.4	Standard
Compare	The server accepts compare requests and performs the requested compare operations.	IETF RFC 2251 §4.10	Base

4.6 Storage and Update

Feature	Description	Specified	Profile
Add	The server accepts add requests and performs the requested add operations.	IETF RFC 2251 §4.7	Base
Delete	The server accepts delete requests and performs the requested delete operations.	IETF RFC 2251 §4.8	Base
Modify (Add, Delete, Replace)	The server accepts modify requests and performs the requested modify operations, including additions, deletions, and replacements.	IETF RFC 2251 §4.6	Base
ModifyDN - Rename a Leaf Entry	The server accepts modify DN requests to rename leaf entries and performs the requested leaf rename operations.	IETF RFC 2251 §4.9	Base
ModifyDN - Move a Leaf Entry to a New Parent	The server accepts modify DN requests to move leaf entries to new parents and performs the requested leaf move operations.	IETF RFC 2251 §4.9	Base
ModifyDN - Move a Renamed Leaf Entry to a New Parent	The server accepts modify DN requests to rename leaf entries and move them to new parents and performs the requested leaf rename and move operations.	IETF RFC 2251 §4.9	Base
ModifyDN - Move Subtree of Entries	The server accepts modify DN requests to move subtrees of entries to new parents and performs the requested move subtree operations.	IETF RFC 2251 §4.9	Advanced
ModifyDN - Move a Renamed Subtree of Entries to a New Parent	The server accepts modify DN requests to rename subtrees of entries and move them to new parents and performs the requested rename and move subtree operations.	IETF RFC 2251 §4.9	Advanced

4.7 Protocol

Feature	Description	Specified	Profile
BER	The server correctly encodes and decodes protocol elements using ASN.1 BER as required by LDAP.	IETF RFC 2251 §5.1	Base
Simple Common Elements	The server correctly encodes, decodes, and processes the simple common elements of LDAPMessage envelope PDUs.	IETF RFC 2251 §4 IETF RFC 2251 §4.1 IETF RFC 2251 §4.1.1 IETF RFC 2251 §4.1.1.1 IETF RFC 2251 §4.1.10 IETF RFC 2251 §4.1.2 IETF RFC 2251 §4.1.4 IETF RFC 2251 §4.1.5 IETF RFC 2251 §4.1.5.1 IETF RFC 2251 §4.1.6 IETF RFC 2251 §4.1.7 IETF RFC 2251 §4.1.8 IETF RFC 2251 §5	Base
Controls	The server correctly encodes, decodes, and processes Controls elements of LDAPMessage envelope PDUs.	IETF RFC 2251 §4.1.12	Advanced
Extended Operations	The server accepts Extended Operations requests and performs any extended operations that it recognizes.	IETF RFC 2251 §4.12	Standard
Abandon	The server accepts abandon requests and performs the requested abandon operations.	IETF RFC 2251 §4.11	Base
Referral	The server can return referrals to enable requested operations to be performed by other servers.	IETF RFC 2251 §4.1.11 IETF RFC 2254 §3 IETF RFC 2254 §4 IETF RFC 2254 §5 IETF RFC 2255 §3 IETF RFC 2255 §4 IETF RFC 2255 §6	Standard
Continuation References	The server can return continuation references to enable requested operations to be continued by other servers.	IETF RFC 2251 §4.5.3 IETF RFC 2251 §4.5.3.1	Standard

4.8 Organization

Feature	Description	Specified	Profile
Data Model	The LDAP protocol assumes there are one or more servers which jointly provide access to a Directory Information Tree (DIT). The tree is structured in accordance with the X.500 data model. It is made up of entries. Entries have names: one or more attribute values from the entry form its relative distinguished name (RDN), which *must* be unique among all its siblings. The concatenation of the relative distinguished names of the sequence of entries from a particular entry to an immediate subordinate of the root of the tree forms that entry's Distinguished Name (DN), which is unique in the tree.	IETF RFC 2251 §3.2 IETF RFC 2251 §3.2.1 IETF RFC 2251 §3.2.2	Base
Definition of Object Classes	The server associates entries with object classes in accordance with the X.500 model.	IETF RFC 2251 §3.2.1 IETF RFC 2252 §4.4	Base
Definition of Attributes	The server's entries have attributes in accordance with the X.500 model. The server supports entries, each of which consists of a set of attributes. An attribute is a type with one or more associated values.	IETF RFC 2251 §3.2.1 IETF RFC 2251 §6.1 IETF RFC 2252 §4.2 IETF RFC 2252 §4.3 IETF RFC 2252 §4.3.1 IETF RFC 2252 §4.3.2	Base
Definition of Matching Rules	The server supports matching rules in accordance with the X.500 model.	IETF RFC 2252 §4.5	Base

Feature	Description	Specified	Profile
Core Object Classes	The server recognizes the following object classes listed in IETF RFC 2256, Section 7 as values of the *objectClass* attribute: *subschema*, *top*, *alias*, *country*, *locality*, *organization*, *organizationalUnit*, *person*, *organizationalPerson*, *organizationalRole*, *groupOfNames*, *residentialPerson*, *device*, and *groupOfUniqueNames*.	Here IETF RFC 2252 §7 IETF RFC 2256 §7 IETF RFC 2256 §7.1 IETF RFC 2256 §7.2 IETF RFC 2256 §7.3 IETF RFC 2256 §7.4 IETF RFC 2256 §7.5 IETF RFC 2256 §7.6 IETF RFC 2256 §7.7 IETF RFC 2256 §7.8 IETF RFC 2256 §7.9 IETF RFC 2256 §7.10 IETF RFC 2256 §7.11 IETF RFC 2256 §7.15 IETF RFC 2256 §7.18	Standard
Extensible Object Object Class	The server recognizes the *extensibleObject* object class described in IETF RFC 2252, Section 7 as a value of the *objectClass* attribute.	Here IETF RFC 2252 §7 IETF RFC 2252 §7.1 IETF RFC 2252 §7.2	Advanced

Feature	Description	Specified	Profile
Attribute Types	The server recognizes the following attribute types listed in IETF RFC 2256, Section 5: *objectClass*, *aliasedObjectName*, *cn*, *sn*, *serialNumber*, *c*, *l*, *st*, *street*, *o*, *ou*, *title*, *description*, *searchGuide*, *businessCategory*, *postalAddress*, *postalCode*, *postOfficeBox*, *physicalDeliveryOfficeName*, *telephoneNumber*, *telexNumber*, *teletexTerminalIdentifier*, *facsimileTelephoneNumber*, *x121Address*, *internationaliSDNNumber*, *registeredAddress*, *destinationIndicator*, *preferredDeliveryMethod*, *supportedApplicationContext*, *member*, *owner*, *roleOccupant*, *seeAlso*, *userPassword*, *name*, *givenName*, *initials*, *generationQualifier*, *x500UniqueIdentifier*, *dnQualifier*, *enhancedSearchGuide*, *distinguishedName*, *uniqueMember*, and *houseIdentifier.*	Here IETF RFC 2252 §5 IETF RFC 2256 §5 IETF RFC 2256 §5.1 IETF RFC 2256 §5.2 IETF RFC 2256 §5.4 IETF RFC 2256 §5.6 IETF RFC 2256 §5.7 IETF RFC 2256 §5.8 IETF RFC 2256 §5.9 IETF RFC 2256 §5.10 IETF RFC 2256 §5.11 IETF RFC 2256 §5.12 IETF RFC 2256 §5.13 IETF RFC 2256 §5.14 IETF RFC 2256 §5.15 IETF RFC 2256 §5.16 IETF RFC 2256 §5.17 IETF RFC 2256 §5.18 IETF RFC 2256 §5.19 IETF RFC 2256 §5.20 IETF RFC 2256 §5.21 IETF RFC 2256 §5.22 IETF RFC 2256 §5.23 IETF RFC 2256 §5.24 IETF RFC 2256 §5.25 IETF RFC 2256 §5.26 IETF RFC 2256 §5.27 IETF RFC 2256 §5.28 IETF RFC 2256 §5.29 IETF RFC 2256 §5.31 IETF RFC 2256 §5.32 IETF RFC 2256 §5.33 IETF RFC 2256 §5.34 IETF RFC 2256 §5.35 IETF RFC 2256 §5.36 IETF RFC 2256 §5.42 IETF RFC 2256 §5.43 IETF RFC 2256 §5.44 IETF RFC 2256 §5.45 IETF RFC 2256 §5.46 IETF RFC 2256 §5.47 IETF RFC 2256 §5.48 IETF RFC 2256 §5.5 IETF RFC 2256 §5.50 IETF RFC 2256 §5.51 IETF RFC 2256 §5.52	Standard

Feature	Description	Specified	Profile
Syntaxes	The server recognizes the following syntaxes listed in IETF RFC 2252, Section 6 and IETF RFC 2256, Section 6: Attribute Type Description, Bit String, Boolean, Country String, DN, Directory String, DIT Content Rule Description, Facsimile Telephone Number, Fax, Generalized Time, IA5 String, INTEGER, JPEG, Matching Rule Description, Matching Rule Use Description, Name And Optional UID, Name Form Description, Numeric String, Object Class Description, OID, Other Mailbox, Postal Address, Printable String, Telephone Number, UTC Time, LDAP Syntax Description, DIT Structure Rule Description, Delivery Method, Enhanced Guide, Guide, Octet String, Teletex Terminal Identifier, and Telex Number.	IETF RFC 2252 §6 IETF RFC 2252 §6.1 IETF RFC 2252 §6.3 IETF RFC 2252 §6.4 IETF RFC 2252 §6.8 IETF RFC 2252 §6.9 IETF RFC 2252 §6.10 IETF RFC 2252 §6.11 IETF RFC 2252 §6.12 IETF RFC 2252 §6.13 IETF RFC 2252 §6.14 IETF RFC 2252 §6.15 IETF RFC 2252 §6.16 IETF RFC 2252 §6.17 IETF RFC 2252 §6.18 IETF RFC 2252 §6.19 IETF RFC 2252 §6.21 IETF RFC 2252 §6.22 IETF RFC 2252 §6.23 IETF RFC 2252 §6.24 IETF RFC 2252 §6.25 IETF RFC 2252 §6.26 IETF RFC 2252 §6.27 IETF RFC 2252 §6.29 IETF RFC 2252 §6.30 IETF RFC 2252 §6.31 IETF RFC 2252 §6.32 IETF RFC 2252 §6.33 IETF RFC 2256 §6 IETF RFC 2256 §6.1 IETF RFC 2256 §6.2 IETF RFC 2256 §6.3 IETF RFC 2256 §6.4 IETF RFC 2256 §6.5 IETF RFC 2256 §6.6	Standard
Matching Rules (Extensible Match)	The server supports the *extensibleMatch* search filter and the *extensibleMatch* matching rules that are defined in IETF RFC 2256, Section 8.	IETF RFC 2251 §4.1.9 IETF RFC 2252 §8 IETF RFC 2252 §8.2 IETF RFC 2252 §8.3 IETF RFC 2252 §8.4 IETF RFC 2256 §8 IETF RFC 2256 §8.1	Advanced
Subschema Entries and Subentries	The server implements subschema entries and subentries.	IETF RFC 2251 §3.2.2	Standard