                        The LDAP URL Format
                    <draft-ietf-ldapbis-url-01.txt>

1. **Status of this Memo**

   This document is an Internet-Draft and is in full conformance with
   all provisions of Section 10 of RFC2026. Internet-Drafts are working
   documents of the Internet Engineering Task Force (IETF), its areas,
   and its working groups. Note that other groups may also distribute
   working documents as Internet-Drafts.

   Internet-Drafts are draft documents valid for a maximum of six months
   and may be updated, replaced, or obsoleted by other documents at any
   time. It is inappropriate to use Internet- Drafts as reference
   material or to cite them other than as "work in progress."

   The list of current Internet-Drafts can be accessed at
   http://www.ietf.org/ietf/1id-abstracts.txt

   The list of Internet-Draft Shadow Directories can be accessed at
   http://www.ietf.org/shadow.html.

   Discussion of this document should take place on the LDAP (v3)
   Revison (ldapbis) Working Group mailing list <ietf-
   ldapbis@openldap.org>. After appropriate review and discussion, this
   document will be submitted as a Standards Track replacement for RFC
   2255.

Copyright Notice

2. **Abstract**

   LDAP is the Lightweight Directory Access Protocol, defined in
   [RFC2251bis], [RFC2252bis], and [RFC2253bis]. This document
   describes a format for an LDAP Uniform Resource Locator. The format
   describes an LDAP search operation used to retrieve information from

an LDAP directory, or, in the context of an LDAPv3 referral or
reference, the format describes a service where an LDAP operation may
be progressed. Note: not all of the parameters of the LDAP search
operation described in [RFC2251bis] can be expressed using the format
defined in this document.

This document specifies the LDAP URL format for version 3 of LDAP and
clarifies how LDAP URLs are resolved. This document also defines an
extension mechanism for LDAP URLs, so that future documents can
extend their functionality, for example, to provide access to new
LDAPv3 extensions as they are defined.

This document replaces RFC 2255. See Appendix A for a list of changes
relative to RFC 2255.

The key words "MUST", "MAY", and "SHOULD" used in this document are
to be interpreted as described in [RFC2119].

3. URL Definition

An LDAP URL begins with the protocol prefix "ldap" and is defined by
the following grammar, following the ABNF notation defined in
[RFC2234].

```
    ldapurl    = scheme "://" [hostport] ["/" dn
                  ["?" [attributes] ["?" [scope]
                  ["?" [filter] ["?" extensions]]]]]
    scheme     = "ldap"
    hostport   = <hostport from Section 3.2.2 of [RFC2396]>
    dn         = <distinguishedName from Section 3 of [RFC2253bis]>
    attributes = attrdesc *("," attrdesc)
    attrdesc   = <AttributeDescription from Section 4.1.5 of [RFC2251bis]> /
"*"
    scope      = "base" / "one" / "sub"
    filter     = <filter from Section 4 of [RFC2254bis]>
    extensions = extension *("," extension)
    extension  = ["!"] extype ["=" exvalue]
    extype     = oid / oiddescr
    exvalue    = <LDAPString from section 4.1.2 of [RFC2251bis]>
    oid        = <LDAPOID from section 4.1.2 of [RFC2251bis]>
    oiddescr   = <name from section 3.2 of [LDAP-IANA]>
```

The "ldap" prefix indicates an entry or entries residing in the LDAP
server running on the given hostname at the given portnumber.

The dn is an LDAP Distinguished Name using the string format
described in [RFC2253bis]. It identifies the base object of the LDAP
search or the target of a non-search operation.

The attributes construct is used to indicate which attributes should
be returned from the entry or entries. Individual attrdesc names are
as defined for AttributeDescription in [RFC2251bis].

The scope construct is used to specify the scope of the search to
perform in the given LDAP server. The allowable scopes are "base"
for a base object search, "one" for a one-level search, or "sub" for
a subtree search.

The filter is used to specify the search filter to apply to entries
within the specified scope during the search. It has the format
specified in [RFC2254bis].

The extensions construct provides the LDAP URL with an extensibility
mechanism, allowing the capabilities of the URL to be extended in the
future. Extensions are a simple comma-separated list of type=value
pairs, where the =value portion MAY be omitted for options not
requiring it. Each type=value pair is a separate extension. These
LDAP URL extensions are not necessarily related to any of the LDAPv3
extension mechanisms. Extensions may be supported or unsupported by
the client resolving the URL. An extension prefixed with a '!'
character (ASCII 33) is critical. An extension not prefixed with a
'!' character is non-critical.

If an extension is supported by the client, the client MUST obey the
extension if the extension is critical. The client SHOULD obey
supported extensions that are non-critical.

If an extension is unsupported by the client, the client MUST NOT
process the URL if the extension is critical. If an unsupported
extension is non-critical, the client MUST ignore the extension.

If a critical extension cannot be processed successfully by the
client, the client MUST NOT process the URL. If a non-critical
extension cannot be processed successfully by the client, the client
SHOULD ignore the extension.

The extension type (extype) MAY be specified using the oid form
(e.g., 1.2.3.4) or the oiddesc form (e.g., myLDAPURLExtension). Use
of the oiddesc form SHOULD be restricted to registered object
identifier descriptive names. See [LDAP-IANA] for registration
details and usage guidelines for descriptive names.

No LDAP URL extensions are defined in this document. Other documents
or a future version of this document MAY define other extensions.

Note that characters that are not safe (e.g., spaces) (as defined in
section 2.1 of [RFC2396]), and the single Reserved character '?'

occurring inside a dn, filter, or other element of an LDAP URL MUST
be escaped using the % method described in section 2.4 of [RFC2396].
If a comma character ',' occurs inside an extension value, the
character MUST also be escaped using the % method.

4. **Defaults for Fields of the LDAP URL**

Some fields of the LDAP URL are optional, as described above. In the
absence of any other specification, the following general defaults
SHOULD be used when a field is absent. Note: other documents MAY
specify different defaulting rules; for example, section 4.1.11 of
[RFC2251bis] specifies a different rule for determining the correct
DN to use when it is absent in an LDAP URL that is returned as a
referral.

hostport
   The default LDAP port is TCP port 389. If no hostport is given,
   the client must have some apriori knowledge of an appropriate LDAP
   server to contact.

dn
   If no dn is given, the default is the zero-length DN, "".

attributes
   If the attributes part is omitted, all user attributes of the
   entry or entries should be requested (e.g., by setting the
   attributes field AttributeDescriptionList in the LDAP search
   request to a NULL list, or (in LDAPv3) by requesting the special
   attribute name "*").

scope
   If scope is omitted, a scope of "base" is assumed.

filter
   If filter is omitted, a filter of "(objectClass=*)" is assumed.

extensions
   If extensions is omitted, no extensions are assumed.

5. **Examples**

The following are some example LDAP URLs using the format defined
above. The first example is an LDAP URL referring to the University
of Michigan entry, available from an LDAP server of the client's
choosing:

```
ldap:///o=University%20of%20Michigan,c=US
```

The next example is an LDAP URL referring to the University of
Michigan entry in a particular ldap server:

```
ldap://ldap1.example.net/o=University%20of%20Michigan,c=US
```

Both of these URLs correspond to a base object search of the
"o=University of Michigan,c=US" entry using a filter of
"(objectclass=*)", requesting all attributes.

The next example is an LDAP URL referring to only the postalAddress
attribute of the University of Michigan entry:

```
ldap://ldap1.example.net/o=University%20of%20Michigan,
        c=US?postalAddress
```

The corresponding LDAP search operation is the same as in the
previous example, except that only the postalAddress attribute is
requested.

The next example is an LDAP URL referring to the set of entries found
by querying the given LDAP server on port 6666 and doing a subtree
search of the University of Michigan for any entry with a common name
of "Babs Jensen", retrieving all attributes:

```
ldap://ldap1.example.net:6666/o=University%20of%20Michigan,
        c=US??sub?(cn=Babs%20Jensen)
```

The next example is an LDAP URL referring to all children of the c=GB
entry:

```
ldap://ldap1.example.com/c=GB?objectClass?one
```

The objectClass attribute is requested to be returned along with the
entries, and the default filter of "(objectclass=*)" is used.

The next example is an LDAP URL to retrieve the mail attribute for
the LDAP entry named "o=Question?,c=US" is given below, illustrating
the use of the escaping mechanism on the reserved character '?'.

```
ldap://ldap2.example.com/o=Question%3f,c=US?mail
```

The next example illustrates the interaction between LDAP and URL
quoting mechanisms.

```
ldap://ldap3.example.com/o=Babsco,c=US???(int=%5c00%5c00%5c00%5c04)
```

The filter in this example uses the LDAP escaping mechanism of \ to
encode three zero or null bytes in the value. In LDAP, the filter
would be written as (int=\00\00\00\04). Because the \ character must
be escaped in a URL, the \'s are escaped as %5c in the URL encoding.

The following three URLs that are equivalent, assuming that the
defaulting rules specified in section 4 of this document are used:

      ldap://ldap.example.net
      ldap://ldap.example.net/
      ldap://ldap.example.net/?

These three URLs all point to the root DSE on the ldap.example.net
server.

The final two examples show use of a hypothetical, experimental bind
name extension (the value associated with the extension is an LDAP DN).

      ldap:///??sub??e-bindname=cn=Manager%2cdc=example%2cdc=com
      ldap:///??sub??!e-bindname=cn=Manager%2cdc=example%2cdc=com

The two URLs are the same, except that the second one marks the e-
bindname extension as critical. Notice the use of the % encoding
method to encode the commas within the distinguished name value in
the e-bindname extension.

6.   Security Considerations

General URL security considerations discussed in [RFC2396] are
relevant for LDAP URLs.

The use of security mechanisms when processing LDAP URLs requires
particular care, since clients may encounter many different servers
via URLs, and since URLs are likely to be processed automatically,
without user intervention. A client SHOULD have a user-configurable
policy about which servers to connect to using which security
mechanisms, and SHOULD NOT make connections that are inconsistent
with this policy. If a client chooses to reuse an existing
connection when resolving one or more LDAP URL, it MUST ensure that
the connection is compatible with the URL and that no security
policies are violated.

Sending authentication information, no matter the mechanism, may
violate a user's privacy requirements. In the absence of specific
policy permitting authentication information to be sent to a server,
a client should use an anonymous connection. (Note that clients
conforming to previous LDAP URL specifications, where all connections

are anonymous and unprotected, are consistent with this
specification; they simply have the default security policy.) Simply
opening a connection to another server may violate some users'
privacy requirements, so clients should provide the user with a way
to control URL processing.

Some authentication methods, in particular reusable passwords sent to
the server, may reveal easily-abused information to the remote server
or to eavesdroppers in transit, and should not be used in URL
processing unless explicitly permitted by policy. Confirmation by
the human user of the use of authentication information is
appropriate in many circumstances. Use of strong authentication
methods that do not reveal sensitive information is much preferred.
If the URL represents a referral for an update operation, strong
authentication methods SHOULD be used. Please refer to the Security
Considerations section of [RFC2829bis] for more information.

The LDAP URL format allows the specification of an arbitrary LDAP
search operation to be performed when evaluating the LDAP URL.
Following an LDAP URL may cause unexpected results, for example, the
retrieval of large amounts of data, the initiation of a long-lived
search, etc. The security implications of resolving an LDAP URL are
the same as those of resolving an LDAP search query.

7. Acknowledgements

The LDAP URL format was originally defined at the University of
Michigan. This material is based upon work supported by the National
Science Foundation under Grant No. NCR-9416667. The support of both
the University of Michigan and the National Science Foundation is
gratefully acknowledged.

This document is an update to RFC 2255 by Tim Howes and Mark Smith.
Changes included in this revised specification are based upon
discussions among the authors, discussions within the LDAP (v3)
Revision Working Group (ldapbis), and discussions within other IETF
Working Groups. The contributions of individuals in these working
groups is gratefully acknowledged. Several people in particular have
made valuable comments on this document; RL "Bob" Morgan, Mark Wahl,
Kurt Zeilenga, and Jim Sermersheim deserve special thanks for their
contributions.

8. References

[LDAP-IANA] IETF LDAPBis WG, "IANA Considerations for LDAP", a work
in progress.

[RFC2119] Bradner, S., "Key Words for use in RFCs to Indicate

Requirement Levels," RFC 2119, March 1997.

[RFC2234] Crocker, D., Overell, P., "Augmented BNF for Syntax
Specifications: ABNF", RFC 2234, November 1997.

[RFC2251bis] IETF LDAPBis WG, "Lightweight Directory Access Protocol
(v3)", a work in progress.

[RFC2252bis] IETF LDAPBis WG, "Lightweight Directory Access Protocol
(v3): Attribute Syntax Definitions", a work in progress.

[RFC2253bis] IETF LDAPBis WG, "Lightweight Directory Access Protocol
(v3): UTF-8 String Representation of Distinguished Names", a work in
progress.

[RFC2254bis] IETF LDAPBis WG, "A String Representation of LDAP Search
Filters", a work in progress.

[RFC2279] Yergeau, F., "UTF-8, a transformation format of ISO 10646",
RFC 2279, January 1998.

[RFC2396] Berners-Lee, T., Fielding, R., and Masinter, L., "Uniform
Resource Identifiers (URI): Generic Syntax", RFC 2396, August 1998.

[RFC2829bis] IETF LDAPBis WG, "Authentication Methods for LDAP", a
work in progress.

9. Authors' Address

Mark Smith, Editor
Netscape Communications Corp.
Mailstop USCA17-201
4170 Network Circle
Santa Clara, CA 95054
USA
+1 650 937-3477
mcs@netscape.com

Tim Howes
Loudcloud, Inc.
599 N. Mathilda Ave.
Sunnyvale, CA 94086
USA
+1 408 744-7509
howes@loudcloud.com

10. Full Copyright Statement

11. Appendix A: Changes Since RFC 2255

11.1. Technical Changes

"URL Definition" section: added missing "*" as an alternative for the
attrdesc part of the URL. It is believed that existing
implementations of RFC 2255 already support this. Added angle
brackets around free-form prose in the "dn", "hostport", "attrdesc",
"filter", and "exvalue" rules. Changed the ABNF for ldapurl to group
the dn component with the preceding slash. Changed the extype rule
to be an LDAPOID from RFC2251bis or an OID description from LDAP-
IANA. Changed the text about extension types so it references LDAP-
IANA. Reordered rules to more closely follow the order the elements
appear in the URL.

"Bindname Extension": removed due to lack of known implementations.

11.2. Editorial Changes

"Abstract" section: changed the text indicate that RFC 2255 is
replaced by this document (instead of RFC 1959). Added text to
indicate that LDAP URLs are used for references and referrals. Fixed
typo (replaced the nonsense phrase "to perform to retrieve" with
"used to retrieve"). Added a note to let the reader know that not
all of the parameters of the LDAP search operation described in
[RFC2251bis] can be expressed using this format.

IESG Note: removed note about lack of satisfactory mandatory
authentication mechanisms.

"URL Definition" section: removed second copy of ldapurl grammar and
following two paragraphs (editorial error in RFC 2255). Fixed line
break within '!' sequence. Reworded last paragraph to clarify which
characters must be URL escaped.   Added text to indicate that LDAP
URLs are used for references and referrals. Added text that refers
to the ABNF from RFC 2234.

"Defaults for Fields of the LDAP URL" section: added; formed by
moving text about defaults out of the "URL Definition" section.

"URL Processing" section: clarified that connections MAY be reused
only if the open connection is compatible with the URL. Added text
to indicate that use of security services is encouraged and that they
SHOULD be used when updates are involved. Removed "dn" from
discussion of authentication methods. Added note that the client MAY
interrogate the server to determine the most appropriate method.

"Examples" section: Modified examples to use example.com and
example.net hostnames. Added missing '?' to the LDAP URL example
whose filter contains three null bytes. Removed space after one
comma within a DN. Revised the bindname example to use e-bindname.
Added some examples to show URL equivalence with respect to the dn
portion of the URL.

"Security Considerations" section: Added a note about connection
reuse. Added a note about using strong authentication methods for
updates. Added a reference to RFC 2829. Added note that simply
opening a connection may violate some users' privacy requirements.

"Acknowledgements" section: added statement about this being an
update to RFC 2255. Added added Kurt Zeilenga and Jim Sermersheim.

"References" section: changed from [1] style to [RFC2251bis] style
throughout the document. Added references to RFCs 2234 and 2829.
Updated RFC 1738 references to the appropriate sections within RFC

2396. Updated the references to refer to LDAPBis WG documents.
Added a reference to the LDAP IANA document.

Header and "Authors' Addresses" sections: added "editor" next to Mark
Smith's name. Updated affiliation and contact information.

Copyright: updated the year.

"Table of Contents" section: added.

12. [Appendix B](): Changes Since Previous Document Revision

This appendix lists all changes relative to the last published
revision, [draft-ietf-ldapbis-url-00.txt](). Note that these changes are
also included in [Appendix A](), but are included here for those who have
already reviewed [draft-ietf-ldapbis-url-00.txt]().

12.1. Technical Changes

"URL Definition" section: changed the ABNF for ldapurl to group the
dn component with the preceding slash. Changed the extype rule to be
is an LDAPOID from RFC2251bis or an OID description from LDAP-IANA.
Changed the text about extension types so it references LDAP-IANA.

"Bindname Extension": removed due to lack of known implementations.

12.2. Editorial Changes

"Examples" section: revised the bindname example to use e-bindname
and added some examples to show URL equivalence with respect to the
dn portion of the URL.

"Appendix C: Loose Ends": removed this section entirely.

References: updated references to refer to LDAPBis WG documents.
Added a reference to the LDAP IANA document.

This Internet Draft expires on 10 November 2001.