Network Working Group
Request for Comments: DRAFT
Obsoletes: RFC 2255

Mark Smith, Editor
Netscape Communications Corp.
Tim Howes
Loudcloud, Inc.

21 February 2001

The LDAP URL Format
<draft-ietf-ldapbis-url-00.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.

2. Abstract

LDAP is the Lightweight Directory Access Protocol, defined in [RFC2251], [RFC2253], and [RFC2252]. 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 [RFC2251] 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 RFC 2396 [RFC2396]>
      dn         = <distinguishedName from Section 3 of [RFC2253]>
      attributes = attrdesc *("," attrdesc)
      attrdesc   = <AttributeDescription from Section 4.1.5 of [RFC2251]> /
"*"
      scope      = "base" / "one" / "sub"
      filter     = <filter from Section 4 of [RFC2254]>
      extensions = extension *("," extension)
      extension  = ["!"] extype ["=" exvalue]
      extype     = token / xtoken
      exvalue    = <LDAPString from section 4.1.2 of [RFC2251]>
      token      = <oid from section 4.1 of [RFC2252]>
      xtoken     = "x-" token
```

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 [RFC2253]. 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 [RFC2251].

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 [RFC2254].

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.

Extension types prefixed by "X-" or "x-" are reserved for use in bilateral agreements between communicating parties. Other extension types MUST be defined in this document, or in other standards-track documents.

One LDAP URL extension is defined in this document (see the section "The Bindname Extension" below). 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 RFC 2396 [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 RFC 2396 [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 [RFC 2251] 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. The Bindname Extension

This section defines an LDAP URL extension for representing the distinguished name for a client to use when authenticating to an LDAP directory during resolution of an LDAP URL. Clients MAY implement this extension.

The extension type is "bindname". The extension value is the distinguished name of the directory entry to authenticate as, in the same form as described for dn in the grammar above. The dn may be the NULL string to specify unauthenticated access. The extension may be either critical (prefixed with a '!' character) or non-critical (not prefixed with a '!' character).

If the bindname extension is critical, the client resolving the URL MUST authenticate to the directory using the given distinguished name and an appropriate authentication method. Note that for a NULL distinguished name, no bind MAY be required to obtain anonymous access to the directory. If the extension is non-critical, the client MAY bind to the directory using the given distinguished name.

6. URL Processing

This section describes how an LDAP URL SHOULD be resolved by a client.

First, the client obtains a connection to the LDAP server referenced in the URL, or an LDAP server of the client's choice if no LDAP server is explicitly referenced. This connection MAY be opened specifically for the purpose of resolving the URL or the client MAY reuse an already open connection if the open connection is compatible with the URL. The connection MAY provide confidentiality, integrity, or other services, e.g., using TLS. Use of security services is at the client's discretion if not specified in the URL but is encouraged if the request or any potential responses contains sensitive information. If the URL represents a referral for an update operation, security services SHOULD be used.

Next, the client authenticates itself to the LDAP server. This step is optional, unless the URL contains a critical bindname extension with a non-NULL value. If a bindname extension is given, the client proceeds according to the section above.

If a bindname extension is not specified, the client MAY bind to the directory using an appropriate authentication method of its own choosing (including NULL authentication). The client may interrogate the server to determine the most appropriate method.

Next, the client performs the LDAP search operation specified in the URL. Additional fields in the LDAP protocol search request, such as sizelimit, timelimit, deref, and anything else not specified or defaulted in the URL specification, MAY be set at the client's discretion.

Once the search has completed, the client MAY close the connection to the LDAP server, or the client MAY keep the connection open for future use.

7. 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 final example shows the use of the bindname extension to specify the dn a client should use for authentication when resolving the URL.

```
ldap:///??sub??bindname=cn=Manager%2co=Foo
ldap:///??sub??!bindname=cn=Manager%2co=Foo
```

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

8. Security Considerations

General URL security considerations discussed in RFC 2396 [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 [RFC2829] 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.

9. 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.

10. References

[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.

[RFC2251] Wahl, M., Howes, T., and S. Kille, "Lightweight Directory Access Protocol (v3)", RFC 2251, December 1997.

[RFC2252] Wahl, M., Coulbeck, A., Howes, T. and S. Kille, "Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions", RFC 2252, December 1997.

[RFC2253] Wahl, M., Kille, S., and T. Howes, "Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names", RFC 2253, December 1997.

[RFC2254] Howes, T., "A String Representation of LDAP Search Filters", RFC 2254, December 1997.

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

[RFC2829] Wahl, M., Alvestrand, H., Hodges, J. and R. Morgan, "Authentication Methods for LDAP", RFC 2829, May 2000.

11. 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

12. Full Copyright Statement

13. Appendix A: Changes Since RFC 2255

13.1. 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", "exvalue", and "token" rules. Simplified the "xtoken" rule by removing the "X-" option (case insensitivity is taken care of by the ABNF). Reordered rules to more closely follow the order the elements appear in the URL.

13.2. 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 [RFC2251] 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.

"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 [RFC2251] style throughout the document. Added references to RFCs 2234 and 2829. Updated RFC 1738 references to the appropriate sections within RFC 2396.

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

Copyright: updated the year.

"Appendix C: Loose Ends" section: added.

"Table of Contents" section: added.

14. Appendix B: Changes Since Previous Document Revision

This appendix lists all changes relative to the last published revision, draft-smith-ldapv3-url-update-01.txt. Note that these changes are also included in Appendix A, but are included here for those who have already reviewed draft-smith-ldapv3-url-update-01.txt.

14.1. Technical Changes

"URL Definition" section: added angle brackets around free-form prose in the "dn", "hostport", "attrdesc", "filter", "exvalue", and "token" rules. Simplified the "xtoken" rule by removing the "X-" option (case insensitivity is taken care of by the ABNF). Reordered rules to more closely follow the order the elements appear in the URL.

14.2. Editorial Changes

Header: changed document from an individual submission to an ldapbis working group submission. Discussion referred to the ietf-ldapbis@openldap.org mailing list.

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

"Abstract" section: 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 [RFC2251] can be expressed using this format.

"URL Definition" section: added text that refers to the ABNF from RFC 2234.

"Defaults for Fields of the LDAP URL" section: added a note to clarify that other specifications MAY specify different defaulting rules.

Copyright: changed the year to 2001.

References: changed from [1] style to [RFC2251] style throughout the document. Added a reference to RFC 2234. Updated RFC 1738 references to the appropriate sections within RFC 2396.

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

"Loose Ends" section: removed item about referencing RFC 2396 instead

of 1738 (done). Removed "Search URLs vs. Referral URLs" item (the editor believe this has been resolved)." Added item about potentially supporting userinfo in LDAP URLs. Added item about not supporting all parameters of the LDAPv3 search operation.

15. Appendix C: Loose Ends

Other Extensions: Suggestions for TLS and SASL URL extensions have been made, but more discussion is needed about whether they are needed, how they will be specified, and whether they should be added to this document.

We need to consider whether it makes sense to support constructs like <userinfo>@<host>:<port> within the hostport field. We do not want to preclude this in the future, but we may keep the details out of this document. Note this specification uses the "hostport" construct from RFC 2396, but not the "server" construct (which is the one that contains "userinfo"):

```
server      = [ [ userinfo "@" ] hostport ]
hostport    = host [ ":" port ]
```

Therefore, it may be necessary to replace "hostport" with "server" in this specification.

Some parameters of the LDAPv3 search operation defined in section 4.5.1 of RFC 2251 are not supported by the LDAP URL format, e.g., derefAliases, sizeLimit, timeLimit, typesOnly, controls. Some ldapbis working group participants would like to see them supported, while others see this as "out of scope" for ldapbis. Support for these options could be added using the extension mechanism.

This Internet Draft expires on 21 August 2001.