Network Working Group
INTERNET DRAFT
OBSOLETES: RFC 1959

Tim Howes
Mark Smith
Netscape Communications Corp.
May 1997

The LDAP URL Format
<draft-ietf-asid-ldapv3-url-02.txt>

1. Status of this Memo

This document is an Internet-Draft. 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.''

To learn the current status of any Internet-Draft, please check the ``1id-abstracts.txt'' listing contained in the Internet- Drafts Shadow Directories on ds.internic.net (US East Coast), nic.nordu.net (Europe), ftp.isi.edu (US West Coast), or munnari.oz.au (Pacific Rim).

2. Abstract

LDAP is the Lightweight Directory Access Protocol, defined in [1], [2] and [3]. This document describes a format for an LDAP Uniform Resource Locator. The format describes an LDAP search operation to perform to retrieve information from an LDAP directory. This document replaces RFC **1959. It updates the LDAP URL format for version 3 of LDAP.** This document also defines a second URL scheme prefix for LDAP running over the TLS protocol defined in [6].

3. URL Definition

An LDAP URL begins with the protocol prefix "ldap" (or the prefix "ldaps" for LDAP over TLS) and is defined by the following grammar.

```
    ldapurl    = scheme "://" [hostport] "/"
                 [dn ["?" [attributes] ["?" [scope]
                 ["?" [filter]]]]]
    scheme     = "ldap" / "ldaps"
    attributes = attrdesc *("," attrdesc)
    scope      = "base" / "one" / "sub"
    dn         = distinguishedName from Section 3 of [1]
    hostport   = hostport from Section 5 of RFC 1738 [5]
    attrdesc   = AttributeDescription from Section 4.1.5 of [2]
    filter     = filter from Section 4 of [4]
```

The "ldap" and "ldaps" prefixes indicate an entry or entries residing in the LDAP server running on the given hostname at the given portnumber. For regular LDAP servers, the default port is TCP port 389. For LDAP servers running over the TLS protocol [6], the default port is 636.

The dn is an LDAP Distinguished Name using the string format described in [1]. It identifies the base object of the LDAP search.

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 [2]. If the attributes part is omitted, all attributes of the entry or entries should be requested.

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

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

If the entry or entries reside in the X.500 namespace, they should be reachable from any LDAP server that is providing front-end access to the **X.500 directory. If the hostport part of the URL is missing, the URL can** be resolved by contacting any X.500-back-ended LDAP server.

Note that any URL-illegal characters (e.g., spaces) and the reserved character '?' occurring inside a dn, filter, or other element of an LDAP URL must be escaped using the % method described in RFC 1738 [5].

4. 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 any X.500-capable LDAP server:

```
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://ldap.itd.umich.edu/o=University%20of%20Michigan,c=US
```

The URL corresponds 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://ldap.itd.umich.edu/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://host.com:6666/o=University%20of%20Michigan,c=US??sub?
(cn=Babs%20Jensen)
```

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

```
ldaps://ldap.itd.umich.edu/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://ldap.question.com/o=Question%3f,c=US?mail
```

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

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

The filter used 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.

5. Security Considerations

The LDAP URL format does not provide a way to specify credentials to use when resolving the URL. Therefore, it is expected that such requests will be unauthenticated, unless some out-of-band mechanism is used.

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.

6. References

[1] Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names. M. Wahl, S. Kille, draft-ietf-asid-ldapv3-dn-02.txt, March 1997.

[2] Lightweight Directory Access Protocol (v3). M. Wahl, T. Howes, S. Kille, draft-ietf-asid-ldapv3-protocol-04.txt, March 1997.

[3] Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions. M. Wahl, A. Coulbeck, T. Howes, S. Kille, draft-ietf-asid-ldapv3-attributes-04.txt, March 1997.

[4] A String Representation of LDAP Search Filters. T. Howes, draft-ietf-asid-ldapv3-filter.01.txt, March 1997.

[5] Uniform Resource Locators (URL). T. Berners-Lee, L. Masinter, M. McCahill, Request for Comment (RFC) 1738, December 1994.

[6] The TLS Protocol Version 1.0., T. Dierks, C. Allen, draft-ietf-tls-protocol-02.txt, March 1997.

7. Author's Address

Tim Howes
Netscape Communications Corp.
501 E. Middlefield Rd.
Mountain View, CA 94043

USA
+1 415 937-3419
howes@netscape.com

Mark Smith
Netscape Communications Corp.
501 E. Middlefield Rd.
Mountain View, CA 94043
USA
+1 415 937-3477
mcs@netscape.com