Network Working Group
Request for Comments: 1959
Category: Standards Track

T. Howes
M. Smith
University of Michigan
June 1996

An LDAP URL Format

Status of this Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

1. Abstract

LDAP is the Lightweight Directory Access Protocol, defined in [1] and [2]. This document describes a format for an LDAP Uniform Resource Locator which will allow Internet clients to have direct access to the LDAP protocol. While LDAP currently is used only as a front end to the X.500 directory, the URL format described here is general enough to handle the case of stand-alone LDAP servers (i.e., LDAP servers not back-ended by X.500).

2. URL Definition

An LDAP URL begins with the protocol prefix "ldap" and is defined by the following grammar.

```
<ldapurl> ::= "ldap://" [ <hostport> ] "/" <dn> [ "?" <attributes>
                    [ "?" <scope> "?" <filter> ] ]

<hostport> ::= <hostname> [ ":" <portnumber> ]

<dn> ::= a string as defined in RFC 1485

<attributes> ::= NULL | <attributelist>

<attributelist> ::= <attributetype>
                    | <attributetype> [ "," <attributelist> ]

<attributetype> ::= a string as defined in RFC 1777

<scope> ::= "base" | "one" | "sub"

<filter> ::= a string as defined in RFC 1558
```

The ldap prefix indicates an entry or entries residing in the LDAP server running on the given <hostname> at the given <portnumber>. The default port is TCP port 389. The <dn> is an LDAP Distinguished Name using the string format described in [1], with any URL-illegal characters (e.g., spaces) escaped using the % method described in RFC 1738.

The <attributes> construct is used to indicate which attributes should be returned from the entry or entries. Individual <attributetype> names are as defined for AttributeType in RFC 1777. If the <attributes> part is omitted, all attributes of the entry or entries should be returned.

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], with any URL-illegal characters escaped using the % method described in RFC 1738. If <filter> is omitted, a filter of "(objectClass=*)" is assumed.

Note that if the entry resides in the X.500 namespace, it 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.

3. Examples

The following are some example LDAP URLs using the format defined above. 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
```

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
```

This URL corresponds to a base object search of the "o=University of Michigan, c=US" entry using a filter of (objectclass=*), requesting all attributes.

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.

An LDAP URL referring to the set of entries found by querying any X.500-capable LDAP server and doing a subtree search of the University of Michigan for any entry with a common name of "Babs Jensen", retrieving all attributes:

ldap:///o=University%20of%20Michigan,c=US??sub?(cn=Babs%20Jensen)

An LDAP URL referring to all children of the c=GB entry:

ldap://ldap.itd.umich.edu/c=GB?objectClass?one

The objectClass attribute is requested to be returned along with the entries.

4. 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. The security implications of resolving an LDAP URL are the same as those of resolving any LDAP query. See the RFC 1777 for more details.

5. Prototype Implementation Availability

There is a prototype implementation of the specification defined in this document available. It is an extension to the libwww client library, provided in both source and binary forms. Also included are binary versions of the Mosaic WWW client for various platforms. See the following URL for more details:

ftp://terminator.rs.itd.umich.edu/ldap/url/

6. Bibliography

[1] Kille, S., "A String Representation of Distinguished Names", RFC 1779, March 1995.

[2] Yeong, W., Howes, T., and S. Kille, "Lightweight Directory Access Protocol", RFC 1777, March 1995.

[3] Howes, R., Kille, S., Yeong, W., and C. Robbins, "The String Representation of Standard Attribute Syntaxes", RFC 1778, March 1995.

[4] Howes, T., "A String Representation of LDAP Search Filters", RFC 1558, December 1993.

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

7. Acknowledgements

This material is based upon work supported by the National Science Foundation under Grant No. NCR-9416667.

8. Authors' Addresses

Tim Howes
University of Michigan
ITD Research Systems
535 W William St.
Ann Arbor, MI 48103-4943
USA

Phone: +1 313 747-4454
EMail: tim@umich.edu

Mark Smith
University of Michigan
ITD Research Systems
535 W William St.
Ann Arbor, MI 48103-4943
USA

Phone: +1 313 764-2277
EMail: mcs@umich.edu