How to find LDAP Servers
Filename: draft-moats-finding-01.txt

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 "id-abstracts.txt" listing contained in the Internet-Drafts Shadow Directories on ftp.is.co.za (Africa), nic.nordu.net (Europe), munnari.oz.au (Pacific Rim), ds.internic.net (US East Coast), or ftp.isi.edu (US West Coast).

Abstract

This document discusses methods available for LDAP server discovery and advertisement based on previous IETF and ongoing IETF work.

1. Introduction

The Lightweight Directory Access Protocol (LDAP) [1] can be used to build "islands" of servers that are not a priori tied into a single Directory Information Tree (DIT.) Here, it is necessary to determine how a client can discover LDAP servers and how LDAP servers can discover each other’s existence. This document discusses the methods available based on current and previous IETF work.

2. Server Discovery of Other Servers

An LDAP server discovers other LDAP servers by either using a proposed naming scheme and the DNS or by using an additional server
to server indexing protocol. Once a server discovers other servers it can collect information for returning LDAP v3 referrals (as LDAP URLs) to clients.

2.1. Discovery via DNS

An LDAP server may either be registered using SRV records \[2\] or, if the server uses the "dc-naming" scheme ([3, 4]), it can attempt to find the server managing its parent node by using DNS to look for the LDAP server for the parent domain. Additionally, an LDAP server may be named using a common alias as described in [5]. In either case, it is necessary to include information about the root of the LDAP server’s subtree by using DNS TXT records as discussed in [6].

As an example, consider a server with the RDN "dc=foo,dc=bar,dc=com" (i.e. in domain foo.bar.com). To find its parent server, it would first look for a SRV record for ldap.tcp.bar.com and then follow [5] by looking for ldap.bar.com. If any of these records were found, it would then look for a TXT record for the same domain to determine the root of its parent server’s sub-tree.

2.2. Discovery via the Common Indexing Protocol [7, 8]

Independent of what DIT is being managed, LDAP servers could export index information about their portion of the tree via the Common Indexing Protocol. This requires some a priori discovery and set up of the index mesh and the inclusion of the root DN of the server's portion of the tree in the exported index information.

3. Client Discovery of LDAP Servers

To discover LDAP servers, clients should follow the sequence of steps specified in [9] (which uses DNS and the service location protocol) with the target service being LDAP. If a DNS record is found for a name that begins with ldap (i.e. ldap.tcp.foo.com or ldap.foo.com) a further DNS lookup for a TXT record under that name would return the root of that server’s subtree. If a client supports DHCP, it may use the DHCP extension specified in [10] to locate LDAP servers.

Alternatively, LDAP clients may have a list of preconfigured LDAP servers included with them that a user can select from. Here, some of the servers in the preconfigured list might provide the functionality described in this document, to allow for simpler clients.
4. Security Considerations

Since this draft only summarizes available methods, it adds no additional security considerations to those inherent in the referenced documents. Implementors are strongly recommended to read and follow the security considerations provided in the referenced documents.

5. Acknowledgments

Many thanks to the members of the LSD working group, for their contributions to previous drafts. The work described in this document is partially supported by the National Science Foundation, Cooperative Agreement NCR-9218179.

6. References

Request For Comments (RFC) and Internet Drafts documents are available from <URL:ftp://ftp.internic.net> and numerous mirror sites.


7. Author’s address

Ryan Moats
AT&T
15621 Drexel Circle
Omaha, NE 68135-2358
USA

Phone:  +1 402 894-9456
EMail:  jayhawk@att.com