Internet-Draft   Ryan Moats
draft-ietf-lsd-server-finding-01.txt   AT&T
Expires in six months   January 1998

               LDAP Servers Finding Other LDAP Servers
             Filename: draft-ietf-lsd-server-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 ``1id-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 an LDAP server to
   discover other LDAP servers. It is based on previous 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 an LDAP server can discover the existence of other LDAP servers.
   This documents discusses the methods available based on current and
   previous IETF work.

2. Server Discovery of Other Servers

A LDAP server may always hae a list of other servers configured into
it by an administrator. Additionally, a LDAP server discovers other
LDAP servers by either using a proposed naming scheme and the DNS, by
using an additional server to server indexing protocol, or by using
the Service Location Protocol [2]. 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 [3] or, if
the server uses the "dc-naming" scheme ([4, 5]), 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 [6]. 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 [7].

As an example, consider a server with the RDN "dc=foo,dc=bar,dc=com"
(i.e. in domain foo.bar.com) and the following DNS RRs:

ldap.tcp.bar.com SRV 0 0 389 ldap1.bar.com

ldap1.bar.com A 100.100.100.100
ldap1.bar.com TXT "service:wp:ldap://ldap1.bar.com:389/o=foo,c=us"

To find its parent server, it would first look for a SRV record for
ldap.tcp.bar.com and then follow [6] by looking for ldap.bar.com. In
this case, the lookup for ldap.tcp.bar.com would provide a SRV record
pointing at ldap1.bar.com. Once an A record for the parent server
were found the server would then look for a TXT record for the same
FQDN (here ldap1.bar.com) to determine the root of its parent
server's sub-tree.

Because of limitations in the size of a DNS response, each TXT record
should only have one URL in it. If multiple URLs are to be
specified, multiple TXT records should be used and the client is
responsible for choosing between them (there is no way to specify
preference between TXT records in DNS)

2.2. Discovery via the Common Indexing Protocol [8, 9]

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.

2.3. Discovery via the Service Location Protocol

It is also possible for a LDAP server to discover other LDAP servers
via the Service Location Protocol (SRVLOC) through use of the
proposed "wp" and "yp" abstract service types [10]. To advertise a
LDAP server, the administator would register the LDAP server under
SRVLOC, including registering the server's DN as part of the
attributes of the service.

A LDAP server would then issue a request and recieve URL information
about advertised LDAP servers and what portions of the DIT they
serve.

3. 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.

4. 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.

5. References

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

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

[2]   J. Veizades, E. Guttman, C. Perkins, S. Kaplan, "Service
           Location Protocol," RFC 2165, June 1997.

[3]   A. Gulbrandsen, P. Vixie, "A DNS RR for specifying the loca-
           tion of services (DNS SRV)," RFC 2052, October 1996.

[4]   A. Grimstad et al., "Naming Plan for an Internet Directory
           Service," Internet Draft (work in progress), March 19, 1997.

[5]   S. Kille et al., "Using Domains in LDAP Distinguished
            Names," Internet Draft (work in progress), August 1997.

[6]   M. Hamilton, R. Wright, "Use of DNS Aliases for Network Ser-
            vices," RFC 2219 (Also BCP 17), October, 1997.

[7]   R. Moats, M. Hamilton, "Advertising Services," Internet
            Draft (work in progress), June 1997.

[8]   M. Mealling, J. Allen, "MIME Object Definitions for the Com-
            mon Indexing Protocol(CIP)," Internet Draft (work in
            progress), June 11, 1997.

[9]   M. Mealling, J. Allen, "The Architecture of the Common
            Indexing Protocol (CIP)," Internet Draft (work in progress),
            June 11, 1997.

[10]   R. Moats, "The 'wp' and 'yp' Abstract Service Types", Inter-
            net Draft (work in progress), January, 1998.

6. Author's address

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

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