

INTERNET-DRAFT
Intended Category: Experimental
Expires: 20 May 2002

Kurt D. Zeilenga
OpenLDAP Foundation
20 November 2001

Use of DNS SRV in LDAP Named Subordinate References
<[draft-zeilenga-ldap-dnsref-02.txt](#)>

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC2026](#).

This document is intended to be, after appropriate review and revision, submitted to the RFC Editor as an Experimental document. Distribution of this memo is unlimited. Technical discussion of this document will take place on the IETF LDAP Extension Working Group mailing list <ietf-ldapext@netscape.com>. Please send editorial comments directly to the author <Kurt@OpenLDAP.org>.

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>>.

Copyright 2001, The Internet Society. All Rights Reserved.

Please see the Copyright section near the end of this document for more information.

Abstract

This document describes how LDAP service location information stored on DNS SRV resource records may be used to in conjunction with named subordinate referral objects. This document defines the `dnsReferral` object class.

Conventions

Schema definitions are provided using LDAPv3 description formats [[RFC2252](#)]. Definitions provided here are formatted (line wrapped) for readability.

The key words ``MUST'', ``MUST NOT'', ``REQUIRED'', ``SHALL'', ``SHALL NOT'', ``SHOULD'', ``SHOULD NOT'', ``RECOMMENDED'', and ``MAY'' in this document are to be interpreted as described in [BCP 14](#) [[RFC2119](#)].

1. Background and Intended Use

Named subordinate referral [[NAMEDREF](#)] defines a specific method for representing subordinate references in LDAP [[RFC2251](#)] directories. This document describes a mechanism for using LDAP service location information [[LOCATE](#)] available in DNS SRV resource records [[RFC2782](#)] to rewrite select LDAP URLs [[RFC2255](#)] returned to clients as referrals and search continuations.

2. Schema

A `dnsReferral` object is a directory entry whose structural object class is the `dnsReferral` object class.

```
( 1.3.6.1.4.1.4203.1.4.8 NAME 'dnsReferral'
  DESC 'DNS SRV aware named subordinate referral object'
  SUP referral STRUCTURAL )
```

`dnsReferral` objects SHOULD have distinguished names comprising of RDNs consisting of only `dc` (domainComponent) attributes (e.g., `dc=example,dc=net`) as detailed in [[RFC2247](#)].

`dnsReferral` objects SHALL behave like referral objects [[NAMEDREF](#)] except as detailed in the following section.

3. Construction of Referrals and Search References

In the referral processing described by [[NAMEDREF](#)], if a LDAP URL with no hostpart is to be returned to the client as part of a referral or search continuation, it is replaced with one or more LDAP URLs based upon service location information.

The server SHOULD obtain service location information [[LOCATE](#)] for the DN [[RFC2253](#)] present in (or implied by) the LDAP URL [[RFC2255](#)]. If no service location information is available, the server MUST return the

LDAP URL as described in [[NAMEDREF](#)].

Otherwise, the server SHALL replace the LDAP URL with a set of constructed LDAP URLs. For each service host port pair provided, the server constructs an LDAP URL by replacing the empty hostport with concatenation of the service host, ":", and the port.

4. Example

Suppose a directory server contains:

```
dn: dc=sub,dc=example,dc=net
dc: sub
objectClass: dNSReferral
objectClass: extensibleObject
ref: ldap:///dc=sub,dc=example,dc=net
```

and DNS holds the following SRV records:

```
_ldap._tcp.sub.example.net. IN SRV 0 0 389 l1.sub.example.net.
_ldap._tcp.sub.example.net. IN SRV 0 0 389 l2.sub.example.net.
```

and a client requests a compareRequest with a target DN of "dc=sub,dc=example,dc=net". In response to this request, the server would return:

```
compareResponse "referral" {
    ldap://l1.sub.example.net:389/dc=sub,dc=example,dc=net
    ldap://l2.sub.example.net:389/dc=sub,dc=example,dc=net
}
```

5. Security Considerations

This mechanism extends [[NAMEDREF](#)] based upon [[LOCATE](#)]. The security considerations discussed in these documents generally apply to the specification described in this document.

In addition, this mechanism requires the server to make DNS queries. DNS responses are subject to spoofing. Use of DNSSEC is RECOMMENDED where appropriate. Also, DNS queries may require significant time and resources.

6. Acknowledgments

This document is borrows heavily from previous work by IETF LDAPext

Working Group including [[NAMEDREF](#)] and [[LOCATE](#)].

7. Author's Address

Kurt D. Zeilenga
OpenLDAP Foundation
<Kurt@OpenLDAP.org>

8. Normative References

- [RFC2119] S. Bradner, "Key Words for use in RFCs to Indicate Requirement Levels", [BCP 14](#) (Also [RFC 2119](#)), March 1997.
- [RFC2247] S. Kille, M. Wahl, A. Grimstad, R. Huber, S. Sataluri, "Using Domains in LDAP/X.500 Distinguished Names", [RFC 2247](#), January 1998.
- [RFC2251] M. Wahl, T. Howes, S. Kille, "Lightweight Directory Access Protocol (v3)", [RFC 2251](#), December 1997.
- [RFC2253] M. Wahl, S. Kille, T. Howes, "Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names", [RFC 2253](#), December 1997.
- [RFC2255] T. Howes, M. Smith, "The LDAP URL Format", [RFC 2255](#), December, 1997.
- [RFC2782] A. Gulbrandsen, P. Vixie, L. Esibov, "A DNS RR for specifying the location of services (DNS SRV)", [RFC 2782](#), February 2000.
- [LOCATE] M. Armijo, P. Leach, L Esibov, RL Morgan. "Discovering LDAP Services with DNS", [draft-ietf-ldapext-locate-xx.txt](#) (work in progress).
- [NAMEDREF] K. Zeilenga (editor), "Named Subordinate References in LDAP Directories" [draft-zeilenga-ldap-namedref-xx.txt](#) (work in progress)

Full Copyright Statement

Copyright 2001, The Internet Society. All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it

or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE AUTHORS, THE INTERNET SOCIETY, AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

