INTERNET-DRAFT
<draft-ietf-ldapext-locate-08.txt>
June 5, 2002
Expires: December 5, 2002

Michael P. Armijo
Levon Esibov
Paul Leach
Microsoft Corporation
R.L. Morgan
University of Washington

Discovering LDAP Services with DNS

Status of this Memo

Abstract

A Lightweight Directory Access Protocol (LDAP) request must be directed to an appropriate server for processing. This document specifies a method for discovering such servers using information in the Domain Name System.

1. Introduction

The LDAPv3 protocol [1] is designed to be a lightweight access protocol for directory services supporting X.500 models. As a distributed directory service, the complete set of directory information (known as the Directory Information Base) is spread across many different servers. Hence there is the need to determine, when initiating or processing a request, which servers hold the relevant information. In LDAP, the Search, Modify, Add, Delete, ModifyDN, and Compare operations all specify a Distinguished Name (DN) [2] on which the operation is performed. A client, or a server acting on behalf of a client, must be able to determine the server(s) that hold the naming context containing that DN, since that server (or one of that set of servers) must receive and process the request. This determination process is called "server location". To support dynamic distributed operation, the information needed to support server location must be available via lookups done at request processing time, rather than, for example, as static data configured into each client or server.

It is possible to maintain the information needed to support server location in the directory itself, and X.500 directory deployments typically do so. In practice, however, this only permits location of servers within a limited X.500-connected set. LDAP-specific methods of maintaining server location information in the directory have not yet been standardized. This document defines an alternative method of managing server location information using the Domain Name System. This method takes advantage of the global deployment of the DNS, by allowing LDAP server location information for any existing DNS domain to be published by creating the records described below. A full discussion of the benefits and drawbacks of the various directory location and naming methods is beyond the scope of this document.

RFC 2247[3] defines an algorithm for mapping DNS domain names into DNs. This document defines the inverse mapping, from DNs to DNS domain names, based on the conventions in [3], for use in this server location method. The server location method described in this document is only defined for DNs that can be so mapped, i.e., those DNs that are based on domain names. In practice this is reasonable because many objects of interest are named with domain names, and use of domain-name-based DNs is becoming common.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [9].

2. Mapping Distinguished Names into Domain Names

This section defines a method of converting a DN into a DNS domain name for use in the server location method described below. Some DNs cannot be converted into a domain name. Converted DNs result in a fully qualified domain name.

The output domain name is initially empty. The DN is processed in right-to-left order (i.e., beginning with the first RDN in the sequence of RDNs). An RDN is able to be converted if it (1) consists of a single AttributeTypeAndValue; (2) the attribute type is "DC"; and (3) the attribute value is non-null. If it can be converted, the attribute value is used as a domain name component (label). The first such value becomes the rightmost (i.e., most significant) domain name component, and successive converted RDN values extend to the left. If an RDN cannot be converted, processing stops. If the output domain name is empty when processing stops, the DN cannot be converted into a domain name.

For DN:

cn=John Doe,ou=accounting,dc=example,dc=net

The client would convert the DC components as defined above into DNS name:

example.net

The determined DNS name will be submitted as a DNS query using the algorithm defined in section 3.

3. Locating LDAPv3 servers through DNS

LDAPv3 server location information is to be stored using DNS Service Location Record (SRV)[5]. The data in a SRV record contains the DNS name of the server that provides the LDAP service, corresponding Port number, and parameters that enable the client to choose an appropriate server from multiple servers according to the algorithm described in [5]. The name of this record has the following format:

   <Service>.<Proto>.<Domain>.

where <Service> is "ldap", and <Proto> is "tcp". <Domain> is the domain name formed by converting the DN of a naming context mastered by the LDAP Server into a domain name using the algorithm in Section 2. Note that "ldap" is the symbolic name for the LDAP service in Assigned Numbers[6], as required by [5].

Presence of such records enables clients to find the LDAP servers using standard DNS query [4]. A client (or server) seeking an LDAP server for a particular DN converts that DN to a domain name using the algorithm of Section 2, does a SRV record query using the DNS name formed as described in the preceding paragraph, and interprets the response as described in [5] to determine a host (or hosts) to contact. As an example, a client that searches for an LDAP server for the DN "ou=foo,dc=example,dc=net" that supports the TCP protocol will submit a DNS query for a set of SRV records with owner name:

```
_ldap._tcp.example.net.
```

The client will receive the list of SRV records published in DNS that satisfy the requested criteria. The following is an example of such a record:

```
_ldap._tcp.example.net.   IN   SRV  0 0 389 phoenix.example.net.
```

The set of returned records may contain multiple records in the case where multiple LDAP servers serve the same domain. If there are no matching SRV records available for the converted DN the client SHOULD NOT attempt to 'walk the tree' by removing the least significant portion of the constructed fully qualified domain name.

4. IANA Considerations

This document does not require any IANA actions.

5. Security Considerations

DNS responses can typically be easily spoofed. Clients using this location method SHOULD ensure, via use of strong security mechanisms, that the LDAP server they contact is the one they intended to contact. See [7] for more information on security threats and security mechanisms.

When using LDAP with TLS the client MUST check the server's name, as described in section 3.6 of [RFC 2830]. As specified there, the name the client checks for is the server's name before any potentially insecure transformations, including the SRV record lookup specified in this memo. Thus the name the client MUST check for is the name obtained by doing the mapping step defined in section 2 above. For example, if the DN "cn=John Doe,ou=accounting,dc=example,dc=net" is converted to the DNS name "example.net", the server's name MUST match "example.net".

This document describes a method that uses DNS SRV records to discover LDAP servers. All security considerations related to DNS SRV records are inherited by this document. See the security considerations section in [5] for more details.

6. References

[1] Wahl, M., Howes, T. and S. Kille, "Lightweight Directory Access Protocol(v3)", RFC 2251, December 1997.

[2] Wahl, M., Kille, S. and T. Howes, "Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names", RFC 2253, December 1997.

[3] Kille, S. and M. Wahl, "Using Domains in LDAP/X.500 Distinguished Names", RFC 2247, January 1998.

[4] Mockapetris, P., "DOMAIN NAMES - CONCEPTS AND FACILITIES", RFC 1034, STD 13, November 1987.

[5] Gulbrandsen, A., Vixie, P. and L. Esibov, "A DNS RR for specifying the location of services (DNS SRV)", RFC 2782, February 2000.

[6] Reynolds, J. and J. Postel, "Assigned Numbers", STD 2, RFC 1700, October 1994.

[7] Wahl, M., Alvestrand, H., Hodges, J. and Morgan, R., "Authentication Methods for LDAP", RFC 2829, May 2000.

[8] Hodges, J., Morgan, R., Wahl, M., "Lightweight Directory Access Protocol (v3): Extension for Transport Layer Security", RFC 2830, May 2000.

[9] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

7. Authors' Addresses

Michael P. Armijo
One Microsoft Way
Redmond, WA 98052
micharm@microsoft.com

Paul Leach
One Microsoft Way
Redmond, WA 98052
paulle@microsoft.com

Levon Esibov
One Microsoft Way
Redmond, WA 98052
levone@microsoft.com

RL "Bob" Morgan
University of Washington
4545 15th Ave NE
Seattle, WA 98105
US

Phone: +1 206 221 3307
EMail: rlmorgan@washington.edu
URI: http://staff.washington.edu/rlmorgan/

8. Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in BCP-11. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

9. Full Copyright Statement

10. Expiration Date

This document is filed as <draft-ietf-ldapext-locate-08.txt>, and expires December 5, 2002.