Converting LDAP/X.500 Distinguished Names to DNS Domain Names to Support Server Location

Status of this memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

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.

Distribution of this memo is unlimited. It is filed as <draft-slone-dn2fqdn-00.txt>, and expires on October 11, 2001. Please send comments to the author.

Copyright Notice

Copyright (C) The Internet Society (2001). All Rights Reserved.

Abstract

A Lightweight Directory Access Protocol (LDAP) request must be directed to an appropriate server for processing. This document specifies an extension to the Domain Name System (DNS) and specifies a method for discovering such servers using information in DNS. This document complements and enhances previously specified methods of locating an appropriate server in that it works for distinguished names constructed with or without the "dc" attribute type.

The DNS extension is specified as an AVA Resource Record. The method of discovering servers queries DNS for AVA records to resolve a DN to a fully qualified domain name, then queries DNS for SRV records to complete the location process.
Definitions

The key words "MUST", "MUST NOT", "SHOULD", "SHOULD NOT" and "MAY" used in this document are to be interpreted as specified in [RFC 2119].

1. Background and Intent

This specification assumes familiarity with X.500 [X.500] and the concept of Distinguished Name (DN), and it assumes familiarity with the basic aspects of the Domain Name System [RFC 1034], [RFC 1035], and [RFC 2181].

1.1 LDAP/X.500 Alignment

The Lightweight Directory Access Protocol (LDAP) was originally designed to be a lightweight access protocol for X.500 directory services. Beginning with version 3 [RFC 2251], LDAP was positioned as a lightweight access protocol for potentially standalone directory services supporting X.500 models. Experience with practical implementations has revealed some misalignment between LDAP and X.500, resulting in interoperability problems and inconsistent user views of system behavior. In response, the X.500 committee is working to maximize alignment between LDAP and X.500 by both updating X.500 and supporting updates to LDAP as appropriate. This memo specifies a mechanism to resolve one aspect of LDAP/X.500 misalignment.

1.2 Directory naming usage and conventions

Each entry in an LDAP or X.500 directory server is known and referenced by its Distinguished Name (DN). Although the set of attributes that can be used in the DN structure is completely arbitrary, practical implementations typically construct DNs according to one of two conventions. [X.521] defines a convention that corresponds to a geopolitical hierarchy of countries, states, organizations, and so on. [RFC 2247] defines a convention that corresponds to the structure of the Domain Name Service (DNS). Neither convention is mandated by its respective specification, and both conventions are commonly used in practice. Applications that use directory services typically specify conformance with both conventions. For example, [RFC 2459] mandates that conforming implementations accept DNs constructed according to either convention.

1.3 Distribution of directory information
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 both LDAP and X.500, nearly all operations specify the DN on which the operation is to be 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.

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, since LDAP servers typically do not maintain such server location information. Alternatively, [LOCATE] defines a method of managing server location information using DNS. In practice, however, the method specified in [LOCATE] only permits location of servers for the subset of DNs conforming to the [RFC 2247] convention; DNs conforming to the [X.521] convention cannot be located using that method.

This document defines an additional method of managing server location information using DNS. This method is compatible with the method defined in [LOCATE], but extends the capability to permit the location of servers holding DNs that conform to both commonly implemented conventions.

2. Requirements

This section outlines and articulates the basic requirements of a generally useful server location service capable of locating servers for DNs constructed using either of the common conventions.

2.1 Variation in naming

As discussed, there are two commonly deployed conventions for constructing DNs. The convention recommended by [RFC 2247] provides a convenient mechanism for mapping DNS names to DNs and vice versa. However, the convention recommended by [X.521] is widely deployed. Although the convenience and ease of directly mapping DNS names and DNs is quite compelling, practical experience has shown that a single naming convention fails to meet all business requirements. Moreover, many organizations have valid business requirements for continuing to use [X.521] names indefinitely. As such, the requirement exists to develop mechanisms that support both naming conventions, allowing implementers and users to choose the naming convention most suitable to their business needs.
2.2 Flexible delegation

Both LDAP/X.500 and DNS implement hierarchical naming constructs. This does not mean that the LDAP/X.500 delegation model for registration authorities is, or need be, identical to the DNS delegation model.

To be useful on a global scale, it is necessary for the server location mechanism to allow for variation in the supported delegation models. For example, in some countries, the lines of delegation for LDAP/X.500 names may mirror those currently in place to support DNS registration under that country’s ccTLD; in other cases, delegation may occur along completely separate lines. The server location mechanism must be sufficiently flexible to allow LDAP/X.500 delegation to occur independently of DNS delegation.

See also open issues 1 and 2.

2.3 Registration mechanism

Once a registration authority (RA) has been delegated the authority to register names, the RA must have a mechanism for registering the names. This mechanism must support a sufficiently large character set to accommodate all reasonably constructed names conformant to both naming conventions. For the [X.521] convention, UTF-8 or something with equivalent expressiveness is deemed appropriate.

2.4 Automated location of LDAP/X.500 server

To be of practical use, given a reasonably constructed DN, the mechanism must permit a client, or server acting on behalf of the client, to automatically locate an LDAP/X.500 server capable of locating the entry associated with that DN. This process must be capable of being completed without user intervention.

3. Approach to implementation

The mechanism specified in this document includes three components: a new DNS Resource Record type, a delegation and registration model for these new DNS records, and an algorithm for resolving a DN to an LDAP/X.500 server or set of servers.

3.1 The AVA Resource Record Type

The new DNS Resource Record type resolves attribute value assertions to fully qualified domain names, hence it is named an AVA record. The format of the AVA record is as follows:
AttributeTypeAndValue TTL Class AVA Target

(An example is provided near the end of this section.)

AttributeTypeAndValue

The AttributeTypeAndValue is encoded as the string representation of the AttributeType, followed by an equals character (‘’ ASCII 61), followed by the string representation of the AttributeValue, according to the specification in [LDAPBIS-DN]. Characters that are not safe (e.g., spaces) (as defined in section 2.1 of RFC 2396 [RFC2396]) MUST be escaped using the % method described in section 2.4 of RFC 2396 [RFC2396].

TTL

Standard meaning [RFC 1035].

Class

Standard meaning [RFC 1035]. AVA records occur in the IN class.

Target

The domain name of the target RDN. There MUST be either one or more NS records or one or more address records for this name, the name MUST NOT be an alias (in the sense of RFC 1034 or RFC 2181). Implementers are urged, but not required, to return the address record(s) in the Additional Data section. Unless and until permitted by future standards action, name compression is not to be used for this field.

See also open issue 3.

Illustrative example

The following example describes how a DN assigned to the author could be registered using a combination of AVA and SRV records. Assume the DN is "cn=Joe User, o=The Corporation for Examples, c=US". Also assume, for the purposes of this illustration, that AVA records are rooted under ".", that ANSI is the appropriate Registration Authority for the US, that The Corporation for Examples has registered an AVA with ANSI, and that The Corporation for Examples has an LDAP server listening to port 389 on a machine called ldap.example.com. Given those assumptions, the following DNS records would exist.
The following records would appear in the "." zone file:

```
; skip the SOA, NS, and similar records...
c=US       AVA       ansi.org ; name server for ansi.org
```

The following records would appear in the ansi.org zone file:

```
; skip the SOA, NS, and similar records...
o=The%20Corporation%20for%20Examples       AVA  example.com
```

The following records would appear in the example.com zone file:

```
; skip the SOA, NS, and similar records...
ldap._tcp.example.com     SRV  0 0 389 ldap.example.com
ldap.example.com          A    192.168.0.1 ; obviously bogus
```

3.2 Registration of RDNs

RDNs are to be registered in DNS in a manner that facilitates the hierarchical delegation of registration authority and in a manner that provides an unambiguous correspondence between DNS names and registered RDNs. An RA MAY create multiple AVA records for a given RDN as long as the servers identified in Target are equally capable of resolving names for that RDN.

Registration begins with those RDNs immediately below the LDAP/X.500 root. For each RDN so registered, at least one AVA record is to be published in the DNS name servers corresponding to the AVA root (see open issues 1 and 2). Each of these AVA records will have a Target value corresponding to a DNS domain under the administrative control of the RA for that RDN. For example, to represent the RDN "c=US" an AVA record could specify a Target value of ansi.org, indicating that ANSI is the RA for c=US. (See open issue 4.)

Beneath the first level RDNs, RDN registration occurs recursively as appropriate until no further levels are needed. No further levels are needed when the value in Target is sufficient to locate the LDAP/X.500 server with no further AVA record lookups.

3.3 Procedure for Locating LDAP/X.500 Server

This section specifies a pseudo-code method of converting a DN into a DNS domain name for use in the server location method described in [LOCATE] section 3. Some DNs cannot be converted into a domain name. Converted DNs result in a fully qualified domain name.

initialize:
set output_domain = null
set type = null

DN_loop (processed one RDN at a time, right-to-left) {
    if (RDN consists of a single AttributeTypeAndValue) AND (AttributeValue != null) {
        if (AttributeType == "DC") {
            set type = DC
            exit DN_loop
        }
        else {
            issue AVA DNS query for AttributeTypeAndValue
            if (DNS response type is AVA) {
                set output_domain = Target
            }
            else exit DN_loop
        }
    }
    else exit DN_loop
} // end DN_loop

after_exiting_loop:
  if (type == "DC") use process in [LOCATE] to set output_domain
  if (output_domain != null)
    issue SRV DNS query for _ldap._tcp.<output_domain>
  else stop // RDN cannot be converted

4. Open Issues

This section is intended to capture open issues requiring further discussion. It is not intended for inclusion in the final document(s).

Issue 1.

There is an issue regarding where to place the AVA root in DNS. One suggestion is that it should be rooted at the DNS root ("."). Dot-level AVA registrations would be relatively few -- on the order of one per ccTLD to provide mappings such as c=US to .us, c=GB to .uk, and so on. Other suggestions have included itu.int, for consistency with established registration procedures for X.500. Another suggestion is to create a new domain such as x521.net. Discussion on this issue is encouraged.

Issue 2.

Within the X.500 committee, there is an open issue regarding how to handle the concept of multiple, disjoint views of the DIT.
Specifically, the X.500 committee is considering the development of a new attribute type specifically for use in the construction of RDNs to provide explicit qualification of distinguished names that either exist in other (disjoint) views of the DIT or that would be duplicates if not for this special RDN. Combining this concept with the AVA record introduces the notion of having multiple AVA roots, with any given root being specified by the use of this new attribute type. This combined approach could obviate the need to resolve issue 1 by explicitly permitting a choice. For backward compatibility, it would still be necessary to specify a default AVA root (or at a minimum, to specify default behavior), but the existence of multiple roots could significantly reduce the difficulty of reaching consensus on "the" root. Discussion on this issue is encouraged.

Issue 3.

An issue to consider with respect to requirements is whether to support single-AVA RDNs only or to support multiple AVA RDNs. From the perspective of registrations and algorithm, there is very little change. The structure of the new DNS record type (would we still call it an AVA record?) would have to change, and the issue of maximum string length becomes more of an issue. Discussion on this issue is encouraged.

Issue 4.

Closely related to issue 1, do AVA records need to follow the already-established Registration Authority top-level delegations specified by ITU-T and ISO? If so, the suggested country-to-ccTLD mapping will need some modification. For example, in the US, the ITU-T/ISO delegated Registration Authority is ANSI, so the c=US mapping would be to ansi.org (or some other domain name specified by ANSI). Note: if issue 2 is resolved in favor of supporting multiple roots, this becomes a moot point, since the resulting ITU-T/ISO could co-exist with others. Discussion on this issue is encouraged.

Issue 5.

The organization of this draft will require consideration before it progresses through too many iterations. Specifically, it will most likely need to be split into multiple documents to allow separate progression of the DNS-related elements and the LDAP-related components. Also worth considering is whether this document should be treated as an update to [LOCATE] once that document is published. Comments are welcome.
5. IANA Considerations

There are two IANA considerations with respect to this document. First, IANA will need to assign a type value to the AVA Resource Record. Second, depending on the resolution of open issues 1, 2, and 4, IANA may need to establish registration procedures for the top level of DNS and to register the appropriate root-level AVA records.

6. 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 [RFC 2829] for more information on security threats and security mechanisms.

This document describes a method that uses DNS AVA records to lead to the discovery of LDAP servers using SRV records. All security considerations related to DNS SRV records are inherited by this document. See the security considerations section in [RFC 2782] for more details.

In addition, this document describes a method of handling DNs. All security considerations related to DNs are inherited by this document. See the security considerations section in [LDAPBIS-DN] for more details.

7. References


8. Author's Address

Skip Slone
Lockheed Martin Corporation
12506 Lake Underhill Road, MP 166
Orlando, FL 32825
Email: skip.slone@lmco.com

9. 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.

10. Full Copyright Statement

Copyright (C) The Internet Society (2001). 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 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.

11. Expiration Date

This document is filed as <draft-slone-dn2fqdn-00.txt>, and expires