Network Working Group
Request for Comments: 2247
Category: Standards Track

S. Kille
Isode Ltd.
M. Wahl
Critical Angle Inc.
A. Grimstad
AT&T
R. Huber
AT&T
S. Sataluri
AT&T

January 1998

Using Domains in LDAP/X.500 Distinguished Names

Status of this Memo

Copyright Notice

1. Abstract

The Lightweight Directory Access Protocol (LDAP) uses X.500-compatible distinguished names [3] for providing unique identification of entries.

This document defines an algorithm by which a name registered with the Internet Domain Name Service [2] can be represented as an LDAP distinguished name.

2. Background

The Domain (Nameserver) System (DNS) provides a hierarchical resource labeling system. A name is made up of an ordered set of components, each of which are short strings. An example domain name with two components would be "CRITICAL-ANGLE.COM".

LDAP-based directories provide a more general hierarchical naming framework. A primary difference in specification of distinguished names from domain names is that each component of an distinguished name has an explicit attribute type indication.

X.500 does not mandate any particular naming structure. It does contain suggested naming structures which are based on geographic and national regions, however there is not currently an established registration infrastructure in many regions which would be able to assign or ensure uniqueness of names.

The mechanism described in this document automatically provides an enterprise a distinguished name for each domain name it has obtained for use in the Internet. These distinguished names may be used to identify objects in an LDAP directory.

An example distinguished name represented in the LDAP string format [3] is "DC=CRITICAL-ANGLE,DC=COM". As with a domain name, the most significant component, closest to the root of the namespace, is written last.

This document does not define how to represent objects which do not have domain names. Nor does this document define the procedure to locate an enterprise’s LDAP directory server, given their domain name. Such procedures may be defined in future RFCs.

3. Mapping Domain Names into Distinguished Names

This section defines a subset of the possible distinguished name structures for use in representing names allocated in the Internet Domain Name System. It is possible to algorithmically transform any Internet domain name into a distinguished name, and to convert these distinguished names back into the original domain names.

The algorithm for transforming a domain name is to begin with an empty distinguished name (DN) and then attach Relative Distinguished Names (RDNs) for each component of the domain, most significant (e.g. rightmost) first. Each of these RDNs is a single AttributeTypeAndValue, where the type is the attribute "DC" and the value is an IA5 string containing the domain name component.

Thus the domain name "CS.UCL.AC.UK" can be transformed into

```
DC=CS,DC=UCL,DC=AC,DC=UK
```

Distinguished names in which there are one or more RDNs, all containing only the attribute type DC, can be mapped back into domain names. Note that this document does not define a domain name equivalence for any other distinguished names.

4. Attribute Type Definition

The DC (short for domainComponent) attribute type is defined as follows:

```
( 0.9.2342.19200300.100.1.25 NAME 'dc' EQUALITY caseIgnoreIA5Match
  SUBSTR caseIgnoreIA5SubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 SINGLE-VALUE )
```

The value of this attribute is a string holding one component of a domain name. The encoding of IA5String for use in LDAP is simply the characters of the string itself. The equality matching rule is case insensitive, as is today's DNS.

5. Object Class Definitions

An object with a name derived from its domain name using the algorithm of section 3 is represented as an entry in the directory. The "DC" attribute is present in the entry and used as the RDN.

An attribute can only be present in an entry held by an LDAP server when that attribute is permitted by the entry's object class.

This section defines two object classes. The first, dcObject, is intended to be used in entries for which there is an appropriate structural object class. For example, if the domain represents a particular organization, the entry would have as its structural object class 'organization', and the 'dcObject' class would be an auxiliary class. The second, domain, is a structural object class used for entries in which no other information is being stored. The domain object class is typically used for entries that are placeholders or whose domains do not correspond to real-world entities.

5.1. The dcObject object class

The dcObject object class permits the dc attribute to be present in an entry. This object class is defined as auxiliary, as it would typically be used in conjunction with an existing structural object class, such as organization, organizationalUnit or locality.

The following object class, along with the dc attribute, can be added to any entry.

```
( 1.3.6.1.4.1.1466.344 NAME 'dcObject' SUP top AUXILIARY MUST dc )
```

An example entry would be:

```
dn: dc=critical-angle,dc=com
objectClass: top
objectClass: organization
objectClass: dcObject
dc: critical-angle
o: Critical Angle Inc.
```

5.2. The domain object class

If the entry does not correspond to an organization, organizational unit or other type of object for which an object class has been defined, then the "domain" object class can be used. The "domain" object class requires that the "DC" attribute be present, and permits several other attributes to be present in the entry.

The entry will have as its structural object class the "domain" object class.

```
( 0.9.2342.19200300.100.4.13 NAME 'domain' SUP top STRUCTURAL
 MUST dc
 MAY ( userPassword $ searchGuide $ seeAlso $ businessCategory $
 x121Address $ registeredAddress $ destinationIndicator $
 preferredDeliveryMethod $ telexNumber $ teletexTerminalIdentifier $
 telephoneNumber $ internationaliSDNNumber $ facsimileTelephoneNumber $
 street $ postOfficeBox $ postalCode $ postalAddress $
 physicalDeliveryOfficeName $ st $ l $ description $ o $
 associatedName ) )
```

The optional attributes of the domain class are used for describing the object represented by this domain, and may also be useful when searching. These attributes are already defined for use with LDAP [4].

An example entry would be:

```
dn: dc=tcp,dc=critical-angle,dc=com
objectClass: top
objectClass: domain
dc: tcp
description: a placeholder entry used with SRV records
```

The DC attribute is used for naming entries of the domain class, and this can be represented in X.500 servers by the following name form rule.

(1.3.6.1.4.1.1466.345 NAME 'domainNameForm' OC domain MUST (dc))

6. References

[1] The Directory: Selected Attribute Types. ITU-T Recommendation X.520, 1993.

[2] Mockapetris, P., " Domain Names - Concepts and Facilities," STD 13, RFC 1034, November 1987.

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

[4] Wahl, M., "A Summary of the X.500(96) User Schema for use with LDAP", RFC 2256, December 1997.

7. Security Considerations

This memo describes how attributes of objects may be discovered and retrieved. Servers should ensure that an appropriate security policy is maintained.

An enterprise is not restricted in the information which it may store in DNS or LDAP servers. A client which contacts an untrusted server may have incorrect or misleading information returned (e.g. an organization's server may claim to hold naming contexts representing domain names which have not been delegated to that organization).

8. Authors' Addresses

Steve Kille
Isode Ltd.
The Dome
The Square
Richmond, Surrey
TW9 1DT
England

Phone: +44-181-332-9091
EMail: S.Kille@ISODE.COM

Mark Wahl
Critical Angle Inc.
4815 W. Braker Lane #502-385
Austin, TX 78759
USA

Phone: (1) 512 372 3160
EMail: M.Wahl@critical-angle.com

Al Grimstad
AT&T
Room 1C-429, 101 Crawfords Corner Road
Holmdel, NJ 07733-3030
USA

EMail: alg@att.com

Rick Huber
AT&T
Room 1B-433, 101 Crawfords Corner Road
Holmdel, NJ 07733-3030
USA

EMail: rvh@att.com

Sri Sataluri
AT&T
Room 4G-202, 101 Crawfords Corner Road
Holmdel, NJ 07733-3030
USA

EMail: sri@att.com

9. Full Copyright Statement