                 Lightweight Directory Access Protocol (LDAP)
                        entryUUID Operational Attribute

Status of This Memo

   This document specifies an Internet standards track protocol for the
   Internet community, and requests discussion and suggestions for
   improvements. Please refer to the current edition of the "Internet
   Official Protocol Standards" (STD 1) for the standardization state
   and status of this protocol. Distribution of this memo is unlimited.

Copyright Notice

Abstract

   This document describes the LDAP/X.500 'entryUUID' operational
   attribute and associated matching rules and syntax. The attribute
   holds a server-assigned Universally Unique Identifier (UUID) for the
   object. Directory clients may use this attribute to distinguish
   objects identified by a distinguished name or to locate an object
   after renaming.

Table of Contents

1. Background and Intended Use

   In X.500 Directory Services [X.501], such as those accessible using
   the Lightweight Directory Access Protocol (LDAP) [RFC4510], an object
   is identified by its distinguished name (DN). However, DNs are not
   stable identifiers. That is, a new object may be identified by a DN
   that previously identified another (now renamed or deleted) object.

   A Universally Unique Identifier (UUID) is "an identifier unique
   across both space and time, with respect to the space of all UUIDs"
   [RFC4122]. UUIDs are used in a wide range of systems.

   This document describes the 'entryUUID' operational attribute, which
   holds the UUID assigned to the object by the server. Clients may use
   this attribute to distinguish objects identified by a particular
   distinguished name or to locate a particular object after renaming.

   This document defines the UUID syntax, the 'uuidMatch' and
   'uuidOrderingMatch' matching rules, and the 'entryUUID' attribute
   type.

   Schema definitions are provided using LDAP description formats
   [RFC4512]. Definitions provided here are formatted (line wrapped)
   for readability.

Zeilenga   Standards Track   [Page 2]

In this document, the key words "MUST", "MUST NOT", "REQUIRED",
"SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY",
and "OPTIONAL" are to be interpreted as described in BCP 14
[RFC2119].

2. UUID Schema Elements

2.1. UUID Syntax

A Universally Unique Identifier (UUID) [RFC4122] is a 16-octet (128-
bit) value that identifies an object. The ASN.1 [X.680] type UUID is
defined to represent UUIDs as follows:

        UUID ::= OCTET STRING (SIZE(16))
             -- constrained to an UUID [RFC4122]

In LDAP, UUID values are encoded using the [ASCII] character string
representation described in [RFC4122]. For example,
"597ae2f6-16a6-1027-98f4-d28b5365dc14".

The following is an LDAP syntax description suitable for publication
in subschema subentries.

        (1.3.6.1.1.16.1 DESC 'UUID')

2.2. 'uuidMatch' Matching Rule

The 'uuidMatch' matching rule compares an asserted UUID with a stored
UUID for equality. Its semantics are the same as the
'octetStringMatch' [X.520][RFC4517] matching rule. The rule differs
from 'octetStringMatch' in that the assertion value is encoded using
the UUID string representation instead of the normal OCTET STRING
string representation.

The following is an LDAP matching rule description suitable for
publication in subschema subentries.

        (1.3.6.1.1.16.2 NAME 'uuidMatch'
           SYNTAX 1.3.6.1.1.16.1)

2.3. 'uuidOrderingMatch' Matching Rule

The 'uuidOrderingMatch' matching rule compares an asserted UUID with
a stored UUID for ordering. Its semantics are the same as the
'octetStringOrderingMatch' [X.520][RFC4517] matching rule. The rule
differs from 'octetStringOrderingMatch' in that the assertion value
is encoded using the UUID string representation instead of the normal
OCTET STRING string representation.

The following is an LDAP matching rule description suitable for
publication in subschema subentries.

```
( 1.3.6.1.1.16.3 NAME 'uuidOrderingMatch'
    SYNTAX 1.3.6.1.1.16.1 )
```

Note that not all UUID variants have a defined ordering; and even
where it does, servers are not obligated to assign UUIDs in any
particular order. This matching rule is provided for completeness.

2.4. 'entryUUID' Attribute

The 'entryUUID' operational attribute provides the Universally Unique
Identifier (UUID) assigned to the entry.

The following is an LDAP attribute type description suitable for
publication in subschema subentries.

```
( 1.3.6.1.1.16.4 NAME 'entryUUID'
    DESC 'UUID of the entry'
    EQUALITY uuidMatch
    ORDERING uuidOrderingMatch
    SYNTAX 1.3.6.1.1.16.1
    SINGLE-VALUE
    NO-USER-MODIFICATION
    USAGE directoryOperation )
```

Servers SHALL generate and assign a new UUID to each entry upon its
addition to the directory and provide that UUID as the value of the
'entryUUID' operational attribute. An entry's UUID is immutable.

UUID are to be generated in accordance with Section 4 of [RFC4122].
In particular, servers MUST ensure that each generated UUID is unique
in space and time.

3. Security Considerations

An entry's relative distinguish name (RDN) is composed from attribute
values of the entry, which are commonly descriptive of the object the
entry represents. Although deployers are encouraged to use naming
attributes whose values are widely disclosable [RFC4514], entries are
often named using information that cannot be disclosed to all
parties. As UUIDs do not contain any descriptive information of the
object they identify, UUIDs may be used to identify a particular
entry without disclosure of its contents.

General UUID security considerations [RFC4122] apply.

General LDAP security considerations [RFC4510] apply.

4. IANA Considerations

    The IANA has registered the LDAP values [RFC4520] specified in this
    document.

4.1. Object Identifier Registration

        Subject: Request for LDAP OID Registration
        Person & email address to contact for further information:
            Kurt Zeilenga <kurt@OpenLDAP.org>
        Specification: RFC 4530
        Author/Change Controller: IESG
        Comments:
            Identifies the UUID schema elements

4.2. UUID Syntax Registration

        Subject: Request for LDAP Syntax Registration
        Object Identifier: 1.3.6.1.1.16.1
        Description: UUID
        Person & email address to contact for further information:
            Kurt Zeilenga <kurt@OpenLDAP.org>
        Specification: RFC 4530
        Author/Change Controller: IESG
        Comments:
             Identifies the UUID syntax

4.3. 'uuidMatch' Descriptor Registration

        Subject: Request for LDAP Descriptor Registration
        Descriptor (short name): uuidMatch
        Object Identifier: 1.3.6.1.1.16.2
        Person & email address to contact for further information:
            Kurt Zeilenga <kurt@OpenLDAP.org>
        Usage: Matching Rule
        Specification: RFC 4530
        Author/Change Controller: IESG

4.4. 'uuidOrderingMatch' Descriptor Registration

        Subject: Request for LDAP Descriptor Registration
        Descriptor (short name): uuidOrderingMatch
        Object Identifier: 1.3.6.1.1.16.3
        Person & email address to contact for further information:
            Kurt Zeilenga <kurt@OpenLDAP.org>
        Usage: Matching Rule

          Specification: RFC 4530
          Author/Change Controller: IESG

4.5. 'entryUUID' Descriptor Registration

   The IANA has registered the LDAP 'entryUUID' descriptor.

          Subject: Request for LDAP Descriptor Registration
          Descriptor (short name): entryUUID
          Object Identifier: 1.3.6.1.1.16.4
          Person & email address to contact for further information:
              Kurt Zeilenga <kurt@OpenLDAP.org>
          Usage: Attribute Type
          Specification: RFC 4530
          Author/Change Controller: IESG

5. Acknowledgements

   This document is based upon discussions in the LDAP Update and
   Duplication Protocols (LDUP) WG. Members of the LDAP Directorate
   provided review.

6. References

6.1. Normative References

   [RFC2119]   Bradner, S., "Key words for use in RFCs to Indicate
                  Requirement Levels", BCP 14, RFC 2119, March 1997.

   [RFC4122]   Leach, P., Mealling, M., and R. Salz, "A Universally
                  Unique IDentifier (UUID) URN Namespace", RFC 4122, July
                  2005.

   [RFC4510]   Zeilenga, K., Ed., "Lightweight Directory Access
                  Protocol (LDAP): Technical Specification Road Map", RFC
                  4510, June 2006.

   [RFC4512]   Zeilenga, K., "Lightweight Directory Access Protocol
                  (LDAP): Directory Information Models", RFC 4512, June
                  2006.

   [RFC4517]   Legg, S., Ed., "Lightweight Directory Access Protocol
                  (LDAP): Syntaxes and Matching Rules", RFC 4517, June
                  2006.

   [ASCII]   Coded Character Set--7-bit American Standard Code for
                  Information Interchange, ANSI X3.4-1986.

    [X.501]   International Telecommunication Union -
                 Telecommunication Standardization Sector, "The
                 Directory -- Models," X.501(1993) (also ISO/IEC 9594-
                 2:1994).

    [X.520]   International Telecommunication Union -
                 Telecommunication Standardization Sector, "The
                 Directory: Selected Attribute Types", X.520(1993) (also
                 ISO/IEC 9594-6:1994).

    [X.680]   International Telecommunication Union -
                 Telecommunication Standardization Sector, "Abstract
                 Syntax Notation One (ASN.1) - Specification of Basic
                 Notation", X.680(2002) (also ISO/IEC 8824-1:2002).

6.2. Informative References

    [RFC4514]   Zeilenga, K., Ed., "Lightweight Directory Access
                 Protocol (LDAP): String Representation of Distinguished
                 Names", RFC 4514, June 2006.

    [RFC4520]   Zeilenga, K., "Internet Assigned Numbers Authority
                 (IANA) Considerations for the Lightweight Directory
                 Access Protocol (LDAP)", BCP 64, RFC 4520, June 2006.

Author's Address

    Kurt D. Zeilenga
    OpenLDAP Foundation

    EMail: Kurt@OpenLDAP.org