Network Working Group
Request for Comments: 5020
Category: Standards Track

K. Zeilenga
Isode Limited

August 2007

The Lightweight Directory Access Protocol (LDAP) entryDN Operational Attribute

Status of This Memo

Copyright Notice

Abstract

This document describes the Lightweight Directory Access Protocol (LDAP) / X.500 'entryDN' operational attribute. The attribute provides a copy of the entry's distinguished name for use in attribute value assertions.

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 entry is identified by its distinguished name (DN) [RFC4512]. However, as an entry's DN is not an attribute of the entry, it is not possible to perform attribute value assertions [RFC4511] against it.

This document describes the 'entryDN' operational attribute which holds a copy of the entry's distinguished name. This attribute may be used in search filters. For instance, searching the subtree <dc=example,dc=com> with the filter:

```
(entryDN:componentFilterMatch:=or:{
    item:{ component "3", rule rdnMatch, value "ou=A" },
    item:{ component "3", rule rdnMatch, value "ou=B" } })
```

would return entries in the subtree <ou=A,dc=example,dc=com> and entries in subtree <ou=B,dc=example,dc=com>, but would not return any other entries in the subtree <dc=example,dc=com>.

In the above paragraph, DNs are presented using the string representation defined in [RFC4514], and the example search filter is presented using the string representation defined in [RFC4515] with whitespace (line breaks and indentation) added to improve readability. The 'componentFilterMatch' and 'rdnMatch' rules are specified in [RFC3687].

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

2. 'entryDN' Operational Attribute

The 'entryDN' operational attribute provides a copy of the entry's current DN.

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

```
( 1.3.6.1.1.20 NAME 'entryDN'
    DESC 'DN of the entry'
    EQUALITY distinguishedNameMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
    SINGLE-VALUE
    NO-USER-MODIFICATION
    USAGE directoryOperation )
```

Note that the DN of the entry cannot be modified through this attribute.

3. Security Considerations

As this attribute only provides an additional mechanism to access an entry's DN, the introduction of this attribute is not believed to introduce new security considerations.

4. IANA Considerations

4.1. Object Identifier Registration

IANA has registered (upon Standards Action) an LDAP Object Identifier [RFC4520] for use in this document.

```
Subject: Request for LDAP OID Registration
Person & email address to contact for further information:
    Kurt Zeilenga <Kurt.Zeilenga@Isode.COM>
Specification: RFC 5020
Author/Change Controller: IESG
Comments:
    Identifies the 'entryDN' attribute type
```

4.2. 'entryDN' Descriptor Registration

IANA has registered (upon Standards Action) the LDAP 'entryDN' descriptor [RFC4520].

```
Subject: Request for LDAP Descriptor Registration
Descriptor (short name): entryDN
Object Identifier: 1.3.6.1.1.20
Person & email address to contact for further information:
    Kurt Zeilenga <Kurt.Zeilenga@Isode.COM>
Usage: Attribute Type
Specification: RFC 5020
Author/Change Controller: IESG
```

5. References

5.1. Normative References

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

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

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

5.2. Informative References

[RFC3687] Legg, S., "Lightweight Directory Access Protocol (LDAP) and X.500 Component Matching Rules", RFC 3687, February 2004.

[RFC4511] Sermersheim, J., Ed., "Lightweight Directory Access Protocol (LDAP): The Protocol", RFC 4511, June 2006.

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

[RFC4515] Smith, M., Ed., and T. Howes, "Lightweight Directory Access Protocol (LDAP): String Representation of Search Filters", RFC 4515, 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
Isode Limited

EMail: Kurt.Zeilenga@Isode.COM

Full Copyright Statement

Intellectual Property

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.