Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: May 23, 2009

P. Masarati
Politecnico di Milano
H. Chu
Symas Corp.

November 19, 2008

LDAP Dereference Control
draft-masarati-ldap-deref-00.txt

Status of this Memo

Abstract

This document describes the Dereference Control for LDAP. This control is intended to provide a concise means to collect extra information related to cross-links present in entries returned as part of search responses.

Table of Contents

1. Background and Intended Use

Cross-links between entries are often used to describe relationships between entries. To exploit the uniqueness of entries naming, these links are usually represented by the distinguished name (DN) of the linked entries.

In many cases, DUAs need to collect information about linked entries. This requires to explicitly dereference each linked entry in order to collect the desired attributes, resulting in the need to perform a specific sequence of search operations, using the links as search base, with a SearchRequest.scope of baseObject [RFC4511].

This document describes a LDAP Control [RFC4511] that allows a DUA to request the DSA to return specific attributes of linked entries along with the link, under the assumption that this operation can be performed by the DSA in a more efficient manner than the DUA would itself by performing the complete sequence of required search operations.

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 [RFC2119].

2. The LDAP Dereference Control

2.1. Control Semantics

This control allows specifying a dereference attribute and a set of attributes to be dereferenced, as illustrated in Section 2.2. The dereference attribute's syntax MUST be 1.3.6.1.4.1.1466.115.121.1.12 (DN) [RFC4517]. Each value of the dereference attribute in a SearchResultEntry SHOULD result in dereferencing the corresponding entry, collecting the values of the attributes to be dereferenced, and returning them as part of the control value in the SearchResultEntry response, in the format detailed in Section 2.3.

The control value may contain dereference attribute values without any dereferenced attribute values, as detailed in Section 2.3. The control semantics does not specify whether this is a consequence of a dangling link or of the application of access restrictions on the values of the attributes to be dereferenced.

Attribute description hierarchy [RFC4512] SHALL NOT be exploited when collecting the values of the attributes to be dereferenced. On the contrary, all of the attribute descriptions in an attribute hierarchy SHOULD be treated as distinct and unrelated descriptions.

This control is only appropriate for the search operation [RFC4511].

The semantics of the criticality field are specified in [RFC4511]. In detail, the criticality of the control determines whether the control will or will not be used, and if it will not be used, whether the operation will continue without returning the control in the response, or fail, returning unavailableCriticalExtension. If the control is appropriate for an operation and, for any reason, it cannot be applied in its entirety to a single SearchResultEntry response, it MUST NOT be applied to that specific SearchResultEntry response, without affecting its application to any subsequent SearchResultEntry response.

Servers implementing this technical specification SHOULD publish the object identifier deref-oid (IANA assigned; see Section 6) as a value of the 'supportedControl' attribute [RFC4512] in their root DSE.

This control is totally unrelated to alias dereferencing [RFC4511].

2.2. Control Request

The control type is deref-oid (IANA assigned; see Section 6). The specification of the Dereference Control request is:

```
controlValue ::= SEQUENCE OF derefSpec DerefSpec

DerefSpec ::= SEQUENCE {
    derefAttr       attributeDescription,    ; with DN syntax
    attributes      AttributeList }

AttributeList ::= SEQUENCE OF attr AttributeDescription
```

Each derefSpec.derefAttr MUST be unique within controlValue.

2.3. Control Response

The control type is deref-oid (IANA assigned; see Section 6). The specification of the Dereference Control response is:

```
controlValue ::= SEQUENCE OF derefRes DerefRes

DerefRes ::= SEQUENCE {
    derefAttr       AttributeDescription,
    derefVal        LDAPDN,
    attrVals        [0] PartialAttributeList OPTIONAL }

PartialAttributeList ::= SEQUENCE OF
                partialAttribute PartialAttribute
```

PartialAttribute is defined in [RFC4511]; the definition is reported here for clarity:

```
PartialAttribute ::= SEQUENCE {
    type       AttributeDescription,
    vals       SET OF value AttributeValue }
```

If partialAttribute.vals is empty, the corresponding partialAttribute is omitted. If all partialAttribute.vals in attrVals are empty, that derefRes.attrVals is omitted.

3. Examples

Given these entries:

```
dn: cn=Howard Chu,ou=people,dc=example,dc=org
objectClass: inetOrgPerson
cn: Howard Chu
sn: Chu
uid: hyc

dn: cn=Pierangelo Masarati,ou=people,dc=example,dc=org
objectClass: inetOrgPerson
cn: Pierangelo Masarati
sn: Masarati
uid: ando

dn: cn=Test Group,ou=groups,dc=example,dc=org
objectClass: groupOfNames
cn: Test Group
member: cn=Howard Chu,ou=people,dc=example,dc=org
member: cn=Pierangelo Masarati,ou=people,dc=example,dc=org
```

A search could be performed with a Dereference request control value specified as

```
{ member, uid }
```

and the "cn=Test Group" entry would be returned with the response control value

```
{ { member, cn=Howard Chu,ou=people,dc=example,dc=org,
    { { uid, [hyc] } } },
  { member, cn=Pierangelo Masarati,ou=people,dc=example,dc=org,
    { { uid, [ando] } } } }
```

4. Implementation Notes

This LDAP extension is currently implemented in OpenLDAP software using the temporary OID 1.3.6.1.4.1.4203.666.5.16 under OpenLDAP's experimental OID arc.

5. Security Considerations

The control result MUST NOT disclose information the client's identity could not have accessed by performing the related search operations. The presence of a derefRes.derefVal in the response control, with no derefRes.attrVals, does not imply neither the existence of nor any access privilege to the corresponding entry. It is merely a consequence of the read access the client's identity has on the corresponding value of the derefRes.derefAttr that would be returned as part of the attributes of a SearchResultEntry response [RFC4511].

Security considerations described in documents listed in [RFC4510] apply.

6. IANA Considerations

6.1. Object Identifier Registration

It is requested that IANA register upon Standards Action an LDAP Object Identifier for use in this technical specification.

Subject: Request for LDAP OID Registration
Person & email address to contact for further information:
    Pierangelo Masarati <ando@OpenLDAP.org>
Specification: (I-D)
Author/Change Controller: IESG
Comments:
    Identifies the LDAP Dereference Control request
    and response

7. Acknowledgments

TBD

8. Normative References

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

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

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

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

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

Authors' Addresses

Pierangelo Masarati
Politecnico di Milano
Dipartimento di Ingegneria Aerospaziale
via La Masa 34
Milano 20156
IT

Phone: +39 02 2399 8309
Fax: +39 02 2399 8334
Email: ando@OpenLDAP.org
URI: http://www.aero.polimi.it/masarati/

Howard Y. Chu
Symas Corporation
18740 Oxnard St., Suite 313A
Tarzana, California 91356
USA

Phone: +1 818 757-7087
Email: hyc@symas.com
URI: http://www.symas.com/

Full Copyright Statement

Intellectual Property