Network Working Group
Request for Comments: 4527
Category: Standards Track

K. Zeilenga
OpenLDAP Foundation

June 2006

Lightweight Directory Access Protocol (LDAP) Read Entry Controls

Status of This Memo

Copyright Notice

Abstract

This document specifies an extension to the Lightweight Directory Access Protocol (LDAP) to allow the client to read the target entry of an update operation. The client may request to read the entry before and/or after the modifications are applied. These reads are done as an atomic part of the update operation.

Table of Contents

1. Background and Intent of Use 2
2. Terminology 2
3. Read Entry Controls 3
   3.1. The Pre-Read Controls 3
   3.2. The Post-Read Controls 3
4. Interaction with Other Controls 4
5. Security Considerations 4
6. IANA Considerations 5
   6.1. Object Identifier 5
   6.2. LDAP Protocol Mechanisms 5
7. Acknowledgement 5
8. References 6
   8.1. Normative References 6
   8.2. Informative References 7

1. Background and Intent of Use

This document specifies an extension to the Lightweight Directory Access Protocol (LDAP) [RFC4510] to allow the client to read the target entry of an update operation (e.g., Add, Delete, Modify, ModifyDN). The extension utilizes controls [RFC4511] attached to update requests to request and return copies of the target entry. One request control, called the Pre-Read request control, indicates that a copy of the entry before application of update is to be returned. Another control, called the Post-Read request control, indicates that a copy of the entry after application of the update is to be returned. Each request control has a corresponding response control used to return the entry.

To ensure proper isolation, the controls are processed as an atomic part of the update operation.

The functionality offered by these controls is based upon similar functionality in the X.500 Directory Access Protocol (DAP) [X.511].

The Pre-Read controls may be used to obtain replaced or deleted values of modified attributes or a copy of the entry being deleted.

The Post-Read controls may be used to obtain values of operational attributes, such as the 'entryUUID' [RFC4530] and 'modifyTimestamp' [RFC4512] attributes, updated by the server as part of the update operation.

2. Terminology

Protocol elements are described using ASN.1 [X.680] with implicit tags. The term "BER-encoded" means the element is to be encoded using the Basic Encoding Rules [X.690] under the restrictions detailed in Section 5.1 of [RFC4511].

DN stands for Distinguished Name.
DSA stands for Directory System Agent (i.e., a directory server).
DSE stands for DSA-specific Entry.

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].

3. Read Entry Controls

3.1. The Pre-Read Controls

The Pre-Read request and response controls are identified by the 1.3.6.1.1.13.1 object identifier. Servers implementing these controls SHOULD publish 1.3.6.1.1.13.1 as a value of the 'supportedControl' [RFC4512] in their root DSE.

The Pre-Read request control is a LDAP Control [RFC4511] whose controlType is 1.3.6.1.1.13.1 and whose controlValue is a BER-encoded AttributeSelection [RFC4511], as extended by [RFC3673]. The criticality may be TRUE or FALSE. This control is appropriate for the modifyRequest, delRequest, and modDNRequest LDAP messages.

The corresponding response control is a LDAP Control whose controlType is 1.3.6.1.1.13.1 and whose the controlValue, an OCTET STRING, contains a BER-encoded SearchResultEntry. The criticality may be TRUE or FALSE. This control is appropriate for the modifyResponse, delResponse, and modDNResponse LDAP messages with a resultCode of success (0).

When the request control is attached to an appropriate update LDAP request, the control requests the return of a copy of the target entry prior to the application of the update. The AttributeSelection indicates, as discussed in [RFC4511][RFC3673], which attributes are requested to appear in the copy. The server is to return a SearchResultEntry containing, subject to access controls and other constraints, values of the requested attributes.

The normal processing of the update operation and the processing of this control MUST be performed as one atomic action isolated from other update operations.

If the update operation fails (in either normal or control processing), no Pre-Read response control is provided.

3.2. The Post-Read Controls

The Post-Read request and response controls are identified by the 1.3.6.1.1.13.2 object identifier. Servers implementing these controls SHOULD publish 1.3.6.1.1.13.2 as a value of the 'supportedControl' [RFC4512] in their root DSE.

The Post-Read request control is a LDAP Control [RFC4511] whose controlType is 1.3.6.1.1.13.2 and whose controlValue, an OCTET STRING, contains a BER-encoded AttributeSelection [RFC4511], as extended by [RFC3673]. The criticality may be TRUE or FALSE. This

control is appropriate for the addRequest, modifyRequest, and modDNRequest LDAP messages.

The corresponding response control is a LDAP Control whose controlType is 1.3.6.1.1.13.2 and whose controlValue is a BER-encoded SearchResultEntry. The criticality may be TRUE or FALSE. This control is appropriate for the addResponse, modifyResponse, and modDNResponse LDAP messages with a resultCode of success (0).

When the request control is attached to an appropriate update LDAP request, the control requests the return of a copy of the target entry after the application of the update. The AttributeSelection indicates, as discussed in [RFC4511][RFC3673], which attributes are requested to appear in the copy. The server is to return a SearchResultEntry containing, subject to access controls and other constraints, values of the requested attributes.

The normal processing of the update operation and the processing of this control MUST be performed as one atomic action isolated from other update operations.

If the update operation fails (in either normal or control processing), no Post-Read response control is provided.

4. Interaction with Other Controls

The Pre-Read and Post-Read controls may be combined with each other and/or with a variety of other controls. When combined with the assertion control [RFC4528] and/or the manageDsaIT control [RFC3296], the semantics of each control included in the combination applies. The Pre-Read and Post-Read controls may be combined with other controls as detailed in other technical specifications.

5. Security Considerations

The controls defined in this document extend update operations to support read capabilities. Servers MUST ensure that the client is authorized for reading of the information provided in this control and that the client is authorized to perform the requested directory update.

Security considerations for the update operations [RFC4511] extended by this control, as well as general LDAP security considerations [RFC4510], generally apply to implementation and use of this extension

6. IANA Considerations

Registration of the following protocol values [RFC4520] have been completed by the IANA.

6.1. Object Identifier

The IANA has registered an LDAP Object Identifier to identify LDAP protocol elements defined in this document.

```
Subject: Request for LDAP Object Identifier Registration
Person & email address to contact for further information:
     Kurt Zeilenga <kurt@OpenLDAP.org>
Specification: RFC 4527
Author/Change Controller: IESG
Comments: Identifies the LDAP Read Entry Controls
```

6.2. LDAP Protocol Mechanisms

The IANA has registered the LDAP Protocol Mechanism described in this document.

```
Subject: Request for LDAP Protocol Mechanism Registration
Object Identifier: 1.3.6.1.1.13.1
Description: LDAP Pre-read Control
Person & email address to contact for further information:
     Kurt Zeilenga <kurt@openldap.org>
Usage: Control
Specification: RFC 4527
Author/Change Controller: IESG
Comments: none
```

```
Subject: Request for LDAP Protocol Mechanism Registration
Object Identifier: 1.3.6.1.1.13.2
Description: LDAP Post-read Control
Person & email address to contact for further information:
     Kurt Zeilenga <kurt@openldap.org>
Usage: Control
Specification: RFC 4527
Author/Change Controller: IESG
Comments: none
```

7. Acknowledgement

The LDAP Pre-Read and Post-Read controls are modeled after similar capabilities offered in the DAP [X.511].

8. References

8.1. Normative References

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

[RFC3296] Zeilenga, K., "Named Subordinate References in Lightweight Directory Access Protocol (LDAP) Directories", RFC 3296, July 2002.

[RFC3673] Zeilenga, K., "Lightweight Directory Access Protocol version 3 (LDAPv3): All Operational Attributes", RFC 3673, December 2003.

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

[RFC4511] Sermersheim, J., Ed., "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.

[RFC4528] Zeilenga, K., "Lightweight Directory Access Protocol (LDAP) Assertion Control", RFC 4528, June 2006.

[X.680] International Telecommunication Union - Telecommunication Standardization Sector, "Abstract Syntax Notation One (ASN.1) - Specification of Basic Notation", X.680(1997) (also ISO/IEC 8824-1:1998).

[X.690] International Telecommunication Union - Telecommunication Standardization Sector, "Specification of ASN.1 encoding rules: Basic Encoding Rules (BER), Canonical Encoding Rules (CER), and Distinguished Encoding Rules (DER)", X.690(1997) (also ISO/IEC 8825-1:1998).

8.2. Informative References

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

[RFC4530] Zeilenga, K., "Lightweight Directory Access Protocol (LDAP) EntryUUID Operational Attribute", RFC 4530, June 2006.

[X.511] International Telecommunication Union - Telecommunication Standardization Sector, "The Directory: Abstract Service Definition", X.511(1993) (also ISO/IEC 9594-3:1993).

Author's Address

Kurt D. Zeilenga
OpenLDAP Foundation

EMail: Kurt@OpenLDAP.org

Full Copyright Statement

Intellectual Property

Acknowledgement

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).