

LDAP Read Entry Controls
<[draft-zeilenga-ldap-readentry-04.txt](#)>

1. Status of this Memo

This document is intended to be, after appropriate review and revision, submitted to the RFC Editor as a Standard Track document. Distribution of this memo is unlimited. Technical discussion of this document will take place on the IETF LDAP Extensions mailing list <ldapext@ietf.org>. Please send editorial comments directly to the author <Kurt@OpenLDAP.org>.

By submitting this Internet-Draft, I accept the provisions of [Section 4 of RFC 3667](#). By submitting this Internet-Draft, I certify that any applicable patent or other IPR claims of which I am aware have been disclosed, or will be disclosed, and any of which I become aware will be disclosed, in accordance with [RFC 3668](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/1id-abstracts.html>

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>

Copyright (C) The Internet Society (2005). All Rights Reserved.

Please see the Full Copyright section near the end of this document for more information.

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.

1. Background and Intent of Use

This document specifies an extension to the Lightweight Directory Access Protocol (LDAP) [[Roadmap](#)] to allow the client to read the target entry of an update operation (e.g., Add, Delete, Modify, ModifyDN). The extension utilizes controls [[Protocol](#)] 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' [[EntryUUID](#)] and 'modifyTimestamp' [[Models](#)] 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 5.2 of [[Protocol](#)].

DN stands for Distinguished Name.

DSA stands for Directory System Agent (i.e., a directory server).

DSE stands for DSA-specific Entry.

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 [BCP 14](#) [[RFC2119](#)].

3. Read Entry Controls

3.1. The Pre-Read Controls

The Pre-Read request and response controls are identified by the IANA-ASSIGNED-OID.1 object identifier. Servers implementing these controls SHOULD publish IANA-ASSIGNED-OID.1 as a value of the 'supportedControl' [[Models](#)] in their root DSE.

The Pre-Read request control is an LDAP Control [[Protocol](#)] whose controlType is IANA-ASSIGNED-OID.1 and whose controlValue is a BER-encoded AttributeSelection [[Protocol](#)], 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 IANA-ASSIGNED-OID.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 target entry prior to the application of the update. The AttributeSelection indicates, as discussed in [[Protocol](#)][[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 response control is provided.

3.2. The Post-Read Controls

The Post-Read request and response controls are identified by the IANA-ASSIGNED-OID.2 object identifier. Servers implementing these controls SHOULD publish IANA-ASSIGNED-OID.2 as a value of the

'supportedControl' [[Models](#)] in their root DSE.

The Post-Read request control is an LDAP Control [[Protocol](#)] whose controlType is IANA-ASSIGNED-OID.2 and whose controlValue, an OCTET STRING, contains a BER-encoded AttributeSelection [[Protocol](#)], 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 IANA-ASSIGNED-OID.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 target entry after the application of the update. The AttributeSelection indicates, as discussed in [[Protocol](#)][[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 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 [[Assertion](#)] and/or the manageDsaIT control [[RFC3296](#)], the semantics of each control included in the combination apply. 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 both for reading of the information provided in this control in addition to ensuring the client is authorized to perform the requested directory update.

Security considerations for the update operations [[Protocol](#)] extended by this control, as well as general LDAP security considerations [[Roadmap](#)], generally apply to implementation and use of this extension

6. IANA Considerations

Registration of the following protocol values [[BCP64bis](#)] is requested.

6.1. Object Identifier

It is requested that IANA register 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 XXXX
Author/Change Controller: IESG
Comments:
Identifies the LDAP Read Entry Controls

6.2. LDAP Protocol Mechanisms

It is requested that IANA register the LDAP Protocol Mechanism described in this document.

Subject: Request for LDAP Protocol Mechanism Registration
Object Identifier: IANA-ASSIGNED-OID.1
Description: LDAP Pre-read Control
Person & email address to contact for further information:
Kurt Zeilenga <kurt@openldap.org>
Usage: Control
Specification: RFC XXXX
Author/Change Controller: IESG
Comments: none
in 2

Subject: Request for LDAP Protocol Mechanism Registration
Object Identifier: IANA-ASSIGNED-OID.2
Description: LDAP Post-read Control
Person & email address to contact for further information:
Kurt Zeilenga <kurt@openldap.org>
Usage: Control
Specification: RFC XXXX
Author/Change Controller: IESG

Comments: none

[7. Acknowledgment](#)

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

[8. References](#)

[[Note to the RFC Editor: please replace the citation tags used in referencing Internet-Drafts with tags of the form RFCnnnn where possible.]]

[8.1. Normative References](#)

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#) (also [RFC 2119](#)), March 1997.
- [Roadmap] Zeilenga, K. (editor), "LDAP: Technical Specification Road Map", [draft-ietf-ldapbis-roadmap-xx.txt](#), a work in progress.
- [Protocol] Sermersheim, J. (editor), "LDAP: The Protocol", [draft-ietf-ldapbis-protocol-xx.txt](#), a work in progress.
- [Models] Zeilenga, K. (editor), "LDAP: Directory Information Models", [draft-ietf-ldapbis-models-xx.txt](#), a work in progress.
- [RFC3296] Zeilenga, K., "Named Subordinate References in Lightweight Directory Access Protocol (LDAP) Directories", [RFC 3296](#), July 2002.
- [RFC3673] Zeilenga, K., "LDAPv3: All Operational Attributes", [RFC 3673](#), December 2003.
- [Assertion] Zeilenga, K., "LDAP Assertion Control", [draft-zeilenga-ldap-assert-xx.txt](#), a work in progress.
- [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

- [BCP64bis] Zeilenga, K., "IANA Considerations for LDAP", [draft-ietf-ldapbis-bcp64-xx.txt](#), a work in progress.
- [EntryUUID] Zeilenga, K., "The LDAP EntryUUID Operational Attribute", [draft-zeilenga-ldap-uuid-xx.txt](#), a work in progress.
- [X.511] International Telecommunication Union - Telecommunication Standardization Sector, "The Directory: Abstract Service Definition", X.511(1993) (also ISO/IEC 9594-3:1993).

10. Author's Address

Kurt D. Zeilenga
OpenLDAP Foundation

Email: Kurt@OpenLDAP.org

Intellectual Property Rights

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in [BCP 78](#) and [BCP 79](#).

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Full Copyright

Copyright (C) The Internet Society (2005). This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

