The Lightweight Directory Access Protocol (LDAP)
Intermediate Response Message

Status of this Memo

Copyright Notice

Abstract

   The Lightweight Directory Access Protocol (LDAP) version 3 is a
   client-request/server-response based protocol. With the exception
   of the search operation, the entire response to an operation request
   is returned in a single LDAP message. While this single-
   request/single-response paradigm is sufficient for many operations
   (including all but one of those currently defined by LDAP), both
   intuition and practical experience validate the notion that it is

insufficient for some operations. When multiple messages are sent

   in response to a single request, all but the last of these response
   messages are referred to as "intermediate responses".

   This document defines and describes the IntermediateResponse
   message, a general mechanism for defining single-request/multiple-
   response operations in LDAP. The IntermediateResponse message is
   defined in a way that maintains the protocol behavior of existing
   LDAP operations. This message is intended to be used in conjunction
   with the LDAP ExtendedRequest and ExtendedResponse to define new
   single-request/multiple-response operations or in conjunction with a
   control when extending existing LDAP operations in a way that
   requires them to return intermediate response information.

[1]. Introduction

   The Lightweight Directory Access Protocol (LDAP), version 3
   [RFC3377] is an extensible protocol. Extended operations ([RFC2251]
   Section 4.12) are defined to allow operations to be added to LDAP
   without requiring a new revision of the protocol. Similarly,
   controls ([RFC2251] section 4.1.12) are defined to extend or modify
   the behavior of existing LDAP operations.

   LDAP is a client-request/server-response based protocol. With the
   exception of the search operation, the entire response to an
   operation request is returned in a single protocol data unit (i.e.
   LDAP message). While this single-request/single-response paradigm
   is sufficient for many operations (including all but one of those
   currently defined by [RFC3377]), both intuition and practical
   experience validate the notion that it is insufficient for some
   operations.

   For example, the LDAP delete operation could be extended via a
   subtree control to mean that an entire subtree is to be deleted. A
   subtree delete operation needs to return continuation references
   based upon subordinate knowledge information contained in the server
   so that the client can complete the operation. Returning references
   as they are found instead of with the final result allows the client
   to progress the operation more efficiently because it does not have
   to wait for the final result to get this continuation reference
   information.

   Similarly, an engineer might choose to design the subtree delete
   operation as an extended operation of its own rather than using a
   subtree control in conjunction with the delete operation. Once
   again, the same continuation reference information is needed by the
   client to complete the operation, and sending the continuation
   references as they are found would allow the client progress the
   operation more efficiently.

Operations that complete in stages or that progress through various
states as they complete might want to send intermediate responses to
the client, thereby informing it of the status of the operation.
For example, an LDAP implementation might define an extended

operation to create a new replica of an administrative area on a
server, and the operation completes in three stages: (1) begin
creation of replica, (2) send replica data to server, (3) replica
creation complete. Intermediate messages might be sent from the
server to the client at the beginning of each stage with the final
response for the extended operation being sent after stage (3) is
complete.

As LDAP [RFC3377] is currently defined, there is no general LDAP
message type that can be used to return intermediate results. A
single, reusable LDAP message for carrying intermediate response
information is desired to avoid repeated modification of the
protocol. Although the ExtendedResponse message is defined in LDAP,
it is defined to be the one and only response message to an
ExtendedRequest message ([RFC2251] Section 4.12), for unsolicited
responses (LDAP Section 4.4), and to return intermediate responses
for the search operation ([RFC3377] Section 4.5.2, also see Section
5 below). The adaptation of ExtendedResponse as a general
intermediate response mechanism would be problematic. In
particular, existing APIs would likely have to be redesigned. It is
believed (based upon operational experience) that the addition of a
new message to carry intermediate result information is easier to
implement and is less likely to cause interoperability problems with
existing deployed implementations.

This document defines and describes the LDAP IntermediateResponse
message. This message is intended to be used in conjunction with
ExtendedRequest and ExtendedResponse to define new single-
request/multiple-response operations or in conjunction with a
control when extending existing LDAP operations in a way that
requires them to return intermediate response information.

It is intended that the definitions and descriptions of extended
operations and controls that make use of the IntermediateResponse
message will define the circumstances when an IntermediateResponse
message can be sent by a server and the associated meaning of an
IntermediateResponse message sent in a particular circumstance.
Similarly, it is intended that clients will explicitly solicit
IntermediateResponse messages by issuing operations that
specifically call for their return.

The LDAP Content Sync Operation [draft-zeilenga-ldup-sync] (a work
in progress) demonstrates one use of LDAP Intermediate Response
messages.

2. Conventions used in this document

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].

   The term "request control" is used to describe a control that is
   included in an LDAP request message sent from an LDAP client to an
   LDAP server.

3. **The IntermediateResponse Message**

   This document extends the protocolOp CHOICE of LDAPMessage
   ([RFC2251] Section 4.1.1) to include the field:

           intermediateResponse   IntermediateResponse

   where IntermediateResponse is defined as:

           IntermediateResponse ::= [APPLICATION 25] SEQUENCE {
                   responseName   [0] LDAPOID OPTIONAL,
                   responseValue   [1] OCTET STRING OPTIONAL }

   IntermediateResponse messages SHALL NOT be returned to the client
   unless the client issues a request that specifically solicits their
   return. This document defines two forms of solicitation: extended
   operation and request control.

   Although the responseName and responseValue are optional in some
   circumstances, generally speaking IntermediateResponse messages have
   a predefined responseName and a responseValue. The value of the
   responseName (if present), the syntax of the responseValue (if
   present) and the semantics associated with a particular
   IntermediateResponse message MUST be specified in documents
   describing the extended operation or request control that uses them.
   Sections 3.1 and 3.2 describe additional requirements on the
   inclusion of responseName and responseValue in IntermediateResponse
   messages.

3.1. **Usage with LDAP ExtendedRequest and ExtendedResponse**

   A single-request/multiple-response operation may be defined using a
   single ExtendedRequest message to solicit zero or more
   IntermediateResponse messages of one or more kinds followed by an
   ExtendedResponse message.

   An extended operation that defines the return of multiple kinds of
   IntermediateResponse messages MUST provide and document a mechanism
   for the client to distinguish the kind of IntermediateResponse
   message being sent. This SHALL be accomplished by using different
   responseName values for each type of IntermediateResponse message
   associated with the extended operation or by including identifying
   information in the responseValue of each type of
   IntermediateResponse message associated with the extended operation.

3.2. Usage with LDAP Request Controls

   Any LDAP operation may be extended by the addition of one or more
   controls ([RFC2251] Section 4.1.12). A control's semantics may

include the return of zero or more IntermediateResponse messages
prior to returning the final result code for the operation. One or
more kinds of IntermediateResponse messages may be sent in response
to a request control.

All IntermediateResponse messages associated with request controls
SHALL include a responseName. This requirement ensures that the
client can correctly identify the source of IntermediateResponse
messages when

> (a) two or more controls using IntermediateResponse messages
>   are included in a request for any LDAP operation or
>
> (b) one or more controls using IntermediateResponse messages
>   are included in a request with an LDAP extended
>   operation that uses IntermediateResponse messages.

A request control that defines the return of multiple kinds of
IntermediateResponse messages MUST provide and document a mechanism
for the client to distinguish the kind of IntermediateResponse
message being sent. This SHALL be accomplished by using different
responseName values for each type of IntermediateResponse message
associated with the request control or by including identifying
information in the responseValue of each type of
IntermediateResponse message associated with the request control.

4. Advertising Support for IntermediateResponse Messages

Because IntermediateResponse messages are associated with extended
operations or controls and LDAP provides a means for advertising the
extended operations and controls supported by a server (using the
supportedExtensions and supportedControls attributes of the root DSE
attributes), no separate means for advertising support for
IntermediateResponse messages is needed (or provided).

5. Use of IntermediateResponse and ExtendedResponse with Search

It is noted that ExtendedResponse messages may be sent in response
to LDAP search operations with controls ([RFC2251] Section 4.5.1).
This use of ExtendedResponse messages SHOULD be viewed as deprecated
in favor of use of the IntermediateResponse messages.

6. Security Considerations

This document describes an enhancement to LDAP. All security
considerations of [RFC3377] apply to this document, however it does
not introduce any new security considerations to LDAP.

Security considerations specific to each extension using this

protocol mechanism shall be discussed in the technical specification
detailing the extension.

7. IANA Considerations

Registration of the following value is requested [RFC3383].

7.1. LDAP Message Type

It is requested that IANA register upon Standards Action an LDAP
Message Type to identify the LDAP IntermediateResponse message as
defined in section 3 of this document.

The following registration template is suggested:

Subject: Request for LDAP Message Type Registration
Person & email address to contact for further information:
    Roger Harrison <roger_harrison@novell.com>
    Specification: RFCXXXX
    Author/Change Controller: IESG
    Comments: Identifies the LDAP IntermediateResponse Message

Acknowledgments

The authors would like to acknowledge the members of the IETF LDAP
Extensions (ldapext) working group mail list who responded to the
suggestion that a multiple-response paradigm might be useful for
LDAP extended requests. Special thanks go to two individuals: David
Wilbur who first introduced the idea on the working group list, and
Thomas Salter, who succinctly summarized the group's discussion.

Normative References

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

  [RFC2251]
      Wahl, M., Howes, T., and S. Kille, "Lightweight Directory
      Access Protocol (v3)", RFC 2251, December 1997.

  [RFC3377]
      Hodges, J. and R. Morgan, "Lightweight Directory Access
      Protocol (v3): Technical Specification", RFC 3377, September
      2002.

  [RFC3383]
      Zeilenga, K., "Internet Assigned Numbers Authority (IANA)
      Considerations for the Lightweight Directory Access Protocol
      (LDAP)", RFC 3383, September 2002.

Informative References

[draft-zeilenga-ldup-sync]

Zeilenga, K., "LDAP Content Synchronization Operation", Work in Progress.

Authors' Addresses

Roger Harrison
Novell, Inc.
1800 S. Novell Place
Provo, UT 84606
+1 801 861 2642
roger_harrison@novell.com

Kurt D. Zeilenga
OpenLDAP Foundation
Kurt@OpenLDAP.org

Appendix A - Document Revision History
    Editors' Note: this appendix should be removed prior to publication
    as an RFC. It is provided as an aid to reviewers of this "work in
    progress."

A.1. draft-rharrison-ldap-extPartResp-00.txt

   Initial revision of draft.

A.2. draft-rharrison-ldap-extPartResp-01.txt

Changed responseName to be optional to align with [RFC3377] definition of ExtendedResponse.

A.3. draft-rharrison-ldap-extPartResp-02.txt

Minor terminology corrections. Clarified use of ExtendedPartialResponse with LDAP extended operations and other LDAP operations with controls.

A.4. draft-rharrison-ldap-intermediateResp-00.txt

- Changed name of ExtendedPartialResponse to IntermediateResponse.

- Retitled "Motivation" section to "Background and Intended Usage" and expanded its contents.

- Added detail surrounding the use of the IntermediateResponse with extended operations and request controls.

- Generalized the way that Intermediate response fits into the ASN.1 definition of LDAP.

- Added information on advertising IntermediateResponse.

- Added information on the use of IntermediateResponse with the search operation.

A.5. draft-rharrison-ldap-intermediateResp-01.txt

This draft was oriented primarily to preparing the draft for publication in accordance with established RFC formatting guidelines. No substantial change in overall content was made. Changes included the following:

- Retitled document

- Rewrote abstract

- Retitled "Background and Intended Usage" section to "Introduction" and expanded its contents.

- Retitled Section 3 from "The Intermediate Response PDU" to "The Intermediate Response Message".

- Renamed references to [RFCnnnn] format

- Added IANA Considerations section

- Retitled "References" section to "Normative References"

- Other small edits to bring draft in line with RFC formatting

guidelines.