Network Working Group
Request for Comments: 3771
Updates: 2251
Category: Standards Track

R. Harrison
Novell, Inc.
K. Zeilenga
OpenLDAP Foundation

April 2004

The Lightweight Directory Access Protocol (LDAP) Intermediate Response Message

Status of this Memo

Copyright Notice

Abstract

This document defines and describes the IntermediateResponse message, a general mechanism for defining single-request/multiple-response operations in Lightweight Directory Access Protocol (LDAP). The IntermediateResponse message is defined in such a way that the protocol behavior of existing LDAP operations is maintained. 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 for the addition of operations to LDAP, without requiring revisions 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 others.

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 perform 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 to perform the operation more efficiently.

Operations that are completed in stages or that progress through various states as they are completed 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 is completed 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 notifications ([RFC2251] 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 using the IntermediateResponse message will define the circumstances in which an IntermediateResponse message can be sent by a server and the associated meaning of the 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 [ZEILENGA] 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, IntermediateResponse messages usually 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 for 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 supportedExtension ([RFC2252] Section 5.2.3) and supportedControl ([RFC2252] Section 5.2.4) attributes of the root DSE), there is no need for a separate means of advertising support for intermediate response messages.

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 4.5.2). 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 has been completed [RFC3383].

7.1. LDAP Message Type

The IANA has registered an LDAP Message Type (25) 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: RFC3771
Author/Change Controller: IESG
Comments: Identifies the LDAP IntermediateResponse Message

8. 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 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.

9. References

9.1. 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.

[RFC2252] Wahl, M., Coulbeck, A., Howes, T. and S. Kille, "Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions", RFC 2252, 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)", BCP 64, RFC 3383, September 2002.

9.2. Informative References

[ZEILENGA] Zeilenga, K., "LDAP Content Synchronization Operation", Work in Progress, February 2004.

10. Authors' Addresses

Roger Harrison
Novell, Inc.
1800 S. Novell Place
Provo, UT 84606

Phone: +1 801 861 2642
EMail: roger_harrison@novell.com

Kurt D. Zeilenga
OpenLDAP Foundation

EMail: Kurt@OpenLDAP.org

11. Full Copyright Statement

Intellectual Property

Acknowledgement

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