INTERNET-DRAFT
Intended Category: Standard Track
Expires in six months

Kurt D. Zeilenga
OpenLDAP Foundation

3 May 2003

The LDAP No-Op Control
<draft-zeilenga-ldap-noop-01.txt>

Status of this Memo

Abstract

This document defines the Lightweight Directory Access Protocol (LDAP) No-Op control which can be used to disable the normal effect of an operation. The control can be used to discover how a server might react to a particular update request without updating the directory.

1. Overview

It is often desirable to be able to determine if an operation would successful complete or not without having the normal effect of the operation take place. For example, an administrative client might want to verify that new user could update their entry (and not other entries) without the directory actually being updated. The mechanism could be used to build more sophisticated security auditing tools.

This document defines the Lightweight Directory Access Protocol (LDAP) [RFC3377] No-Op control. The presence of the No-Op control in an operation request message disables the normal effect of the operation.

For example, when present in a LDAP modify operation [RFC2251], the modify operation will do all processing necessary to perform the operation but not actually modify the directory.

The No-Op control is not intended to be used by user clients to determine "effective rights".

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].

2. No-Op Control

The No-Op control is an LDAP Control [RFC2251] whose controlType is 1.3.6.1.4.1.4203.1.10.2, criticality is TRUE, and controlValue is absent. Criticality of TRUE is REQUIRED to prevent unintended modification of the directory. There is no corresponding response control.

The control is appropriate for LDAP Add, Delete, Modify and Modify DN operations [RFC2251].

When the control is attached to an LDAP request, the server SHALL do all normal processing possible for the operation without modification of the directory. A result code other than success (0) means that the server is not able or willing to complete the processing for the reasons indicated by the result code. A result code of success (0) indicates that the server found no reason why the operation would fail if submitted without the No-Op control.

Servers SHOULD indicate their support for this control by providing 1.3.6.1.4.1.4203.1.10.2 as a value of the supportedControl attribute type in their root DSE. A server MAY choose to advertise this extension only when the client is authorized to use this operation.

3. Security Considerations

The No-Op control mechanism allows directory administrators (and users) to verify that access control and other administrative policy controls are properly configured. The mechanism may also lead to the development (and deployment) of more sophisticated security auditing tools.

The No-Op control mechanism is believed not to introduce any security risks beyond those of the base operation it is attached to. Security considerations for the base operations, as well as general LDAP security considerations, are discussed discussed in RFCs comprising the LDAP Technical Specification [RFC3377].

4. IANA Considerations

This OID 1.3.6.1.4.1.4203.1.10.2 to identify the LDAP No-Op control. This OID was assigned [ASSIGN] by OpenLDAP Foundation, under its IANA-assigned private enterprise allocation [PRIVATE], for use in this specification.

Registration of this protocol mechanism is requested [RFC3383].

```
Subject: Request for LDAP Protocol Mechanism Registration
Object Identifier: 1.3.6.1.4.1.4203.1.10.2
Description: No-Op Control
Person & email address to contact for further information:
    Kurt Zeilenga <kurt@openldap.org>
Usage: Control
Specification: RFCxxxx
Author/Change Controller: IESG
Comments: none
```

5. Author's Address

Kurt D. Zeilenga
OpenLDAP Foundation
<Kurt@OpenLDAP.org>

6. Normative References

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

[RFC2251] M. Wahl, T. Howes, S. Kille, "Lightweight Directory Access

Protocol (v3)", RFC 2251, December 1997.

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

7. Informative References

[RFC3383] K. Zeilenga, "IANA Considerations for LDAP", BCP 64 (also RFC 3383), September 2002.

[ASSIGN] OpenLDAP Foundation, "OpenLDAP OID Delegations", http://www.openldap.org/foundation/oid-delegate.txt.

[PRIVATE] IANA, "Private Enterprise Numbers", http://www.iana.org/assignments/enterprise-numbers.