                         The LDAP No-Op Control
                    <draft-zeilenga-ldap-noop-05.txt>

Status of this Memo

  This document is intended to be, after appropriate review and
  revision, submitted to the IESG for consideration 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/ietf/1id-abstracts.txt>. The list of
  Internet-Draft Shadow Directories can be accessed at
  <http://www.ietf.org/shadow.html>.

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 a directory operation
   [Protocol] 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)
   [Roadmap] No-Op control extension. The presence of the No-Op control
   in an operation request message disables its normal effect upon the
   directory which operation would otherwise have. Instead of updating
   the directory and return the normal indication of success, the server
   does not update the directory and indicates so by returning the
   noOperation resultCode (introduced below).

   For example, when the No-Op control is present in a LDAP modify
   operation [Protocol], the server is do all processing necessary to
   perform the operation without actually updating the directory. If it
   detects an error during this processing, it returns a non-success
   (other than noOperation) resultCode as it normally would. Otherwise,
   it returns the noOperation. In either case, the directory is left
   unchanged.

   This No-Op control is not intended to be to an "effective access"
   mechanism [RFC2820, U12].

1.1. Terminology

   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].

   DN stands for Distinguished Name.
   DSA stands for Directory System Agent.
   DSE stands for DSA-specific entry.

2. No-Op Control

The No-Op control is an LDAP Control [Protocol] whose controlType is
IANA-ASSIGNED-OID and controlValue is absent. Clients MUST provide a
criticality value of TRUE to prevent unintended modification of the
directory.

The control is appropriate for request messages of LDAP Add, Delete,
Modify and ModifyDN operations [Protocol]. The control is also
appropriate for requests of extended operations which update the
directory (or other data stores), such as Password Modify Extended
Operation [RFC3062]. There is no corresponding response control.

When the control is attached to an LDAP request, the server does all
normal processing possible for the operation without modification of
the directory. That is, when the control is attached to an LDAP
request, the directory SHALL NOT be updated and the response SHALL NOT
have a resultCode of success (0).

A result code other than noOperation (IANA-ASSIGNED-CODE) means that
the server is unable or unwilling to complete the processing for the
reason indicated by the result code. A result code of noOperation
(IANA-ASSIGNED-CODE) indicates that the server discovered no reason
why the operation would fail if submitted without the No-Op control.

Servers SHOULD indicate their support for this control by providing
IANA-ASSIGNED-OID as a value of the 'supportedControl' attribute type
[Models] in their root DSE entry. 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 effective security auditing
tools.

Implementors of this LDAP extension should be familiar with security
considerations applicable to the LDAP operations [Protocol] extended
by this control, as well as general LDAP security considerations
[Roadmap].

4. IANA Considerations

4.1. Object Identifier

It is requested that IANA assign an LDAP Object Identifier [BCP64bis] to identify the LDAP No-Op Control 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 No-Op Control
```

4.2 LDAP Protocol Mechanism

Registration of this protocol mechanism is requested [RFC3383].

```
Subject: Request for LDAP Protocol Mechanism Registration
Object Identifier: IANA-ASSIGNED-OID
Description: No-Op 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
```

4.3 LDAP Result Code

Assignment of an LDAP Result Code called 'noOperation' is requested.

```
Subject: LDAP Result Code Registration
Person & email address to contact for further information:
    Kurt Zeilenga <kurt@OpenLDAP.org>
Result Code Name: noOperation
Specification: RFC XXXX
Author/Change Controller: IESG
Comments:  none
```

5. Author's Address

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

6. References

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

6.1. Normative References

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

[Protocol]   Sermersheim, J. (editor), "LDAP: The Protocol", draft-ietf-ldapbis-protocol-xx.txt, a work in progress.

[Roadmap]   Zeilenga, K. (editor), "LDAP: Technical Specification Road Map", draft-ietf-ldapbis-roadmap-xx.txt, a work in progress.

[Models]   Zeilenga, K. (editor), "LDAP: Directory Information Models", draft-ietf-ldapbis-models-xx.txt, a work in progress.

6.2. Informative References

[X.500]   International Telecommunication Union - Telecommunication Standardization Sector, "The Directory -- Overview of concepts, models and services," X.500(1993) (also ISO/IEC 9594-1:1994).

[RFC2820]   Stokes, E., et. al., "Access Control Requirements for LDAP", RFC 2820, May 2000.

[RFC3062]   Zeilenga, K., "LDAP Password Modify Extended Operation", RFC 3062, February 2000.

[BCP64bis]   Zeilenga, K., "IANA Considerations for LDAP", draft-ietf-ldapbis-bcp64-xx.txt, a work in progress.

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