                  Lightweight Directory Access Protocol (LDAP)
                              Cancel Operation

Status of this Memo

Copyright Notice

Abstract

   This specification describes a Lightweight Directory Access Protocol
   (LDAP) extended operation to cancel (or abandon) an outstanding
   operation. Unlike the LDAP Abandon operation, but like the X.511
   Directory Access Protocol (DAP) Abandon operation, this operation has
   a response which provides an indication of its outcome.

1. Background and Intent of Use

   The Lightweight Directory Access Protocol (LDAP) [RFC3377] provides
   an Abandon operation [RFC2251] which clients may use to cancel other
   operations. The Abandon operation does not have a response and
   requires no response from the abandoned operation. These semantics
   provide the client with no clear indication of the outcome of the
   Abandon operation.

   The X.511 Directory Access Protocol (DAP) [X.511] provides an Abandon
   operation which has a response and also requires the abandoned
   operation to return a response indicating it was canceled. The LDAP
   Cancel operation is modeled after the DAP Abandon operation.

   The LDAP Cancel operation SHOULD be used instead of the LDAP Abandon
   operation when the client needs an indication of the outcome. This
   operation may be used to cancel both interrogation and update
   operations.

   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 5.1 of [RFC2251].

   DSA stands for Directory System Agent (or 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].

2. Cancel Operation

   The Cancel operation is defined as an LDAP Extended Operation
   [RFC2251, Section 4.12] identified by the object identifier
   1.3.6.1.1.8. This section details the syntax of the Cancel request
   and response messages and defines additional LDAP resultCodes.

2.1. Cancel Request

   The Cancel request is an ExtendedRequest with the requestName field
   containing 1.3.6.1.1.8 and a requestValue field which contains a
   BER-encoded cancelRequestValue value.

       cancelRequestValue ::= SEQUENCE {
           cancelID   MessageID
                           -- MessageID is as defined in [RFC2251]
       }

   The cancelID field contains the message ID associated with the
   operation to be canceled.

2.2. Cancel Response

   A Cancel response is an ExtendedResponse where the responseName and
   response fields are absent.

2.3. Additional Result Codes

   Implementations of this specification SHALL recognize the following
   additional resultCode values:

       canceled   (118)
       noSuchOperation (119)
       tooLate   (120)
       cannotCancel   (121)

3. Operational Semantics

   The function of the Cancel Operation is to request that the server
   cancel an outstanding operation issued within the same session.

   The client requests the cancelation of an outstanding operation by
   issuing a Cancel Response with a cancelID set to the message ID of
   the outstanding operation. The Cancel Request itself has a distinct
   message ID. Clients SHOULD NOT request the cancelation of an
   operation multiple times.

   If the server is willing and able to cancel the outstanding operation
   identified by the cancelId, the server SHALL return a Cancel Response
   with a success resultCode, and the canceled operation SHALL fail with
   canceled resultCode. Otherwise the Cancel Response SHALL have a
   non-success resultCode and SHALL NOT have an impact upon the
   outstanding operation (if it exists).

   The protocolError resultCode is returned if the server is unable to
   parse the requestValue or the requestValue is absent,

   The noSuchOperation resultCode is returned if the server has no
   knowledge of the operation requested for cancelation.

   The cannotCancel resultCode is returned if the identified operation
   does not support cancelation or the cancel operation could not be
   performed. The following classes of operations are not cancelable:

   - operations which have no response,

   - operations which create, alter, or destroy authentication and/or
      authorization associations,

   - operations which establish, alter, or tear-down security services,
      and

   - operations which abandon or cancel other operations.

   Specifically, the Abandon, Bind, Start TLS [RFC2830], Unbind, and
   Cancel operations are not cancelable.

   The Cancel operation cannot be abandoned.

   The tooLate resultCode is returned to indicate that it is too late to
   cancel the outstanding operation. For example, the server may return
   tooLate for a request to cancel an outstanding modify operation which
   has already committed updates to the underlying data store.

Servers SHOULD indicate their support for this extended operation by
providing 1.3.6.1.1.8 as a value of the 'supportedExtension'
attribute type in their root DSE. A server MAY choose to advertise
this extension only when the client is authorized to use it.

4. Security Considerations

This operation is intended to allow a user to cancel operations they
previously issued during the current LDAP association. In certain
cases, such as when the Proxy Authorization Control is in use,
different outstanding operations may be processed under different
LDAP associations. Servers MUST NOT allow a user to cancel an
operation belonging to another user.

Some operations should not be cancelable for security reasons. This
specification disallows the cancelation of the Bind operation and
Start TLS extended operation so as to avoid adding complexity to
authentication, authorization, and security layer semantics.
Designers of future extended operations and/or controls should
disallow abandonment and cancelation when appropriate.

5. IANA Considerations

The following values [RFC3383] have been registered by the IANA.

5.1. Object Identifier

The IANA has registered upon Standards Action the LDAP Object
Identifier 1.3.6.1.1.8 to identify the LDAP Cancel Operation as
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 3909
    Author/Change Controller: IESG
    Comments:
        Identifies the LDAP Cancel Operation

5.2. LDAP Protocol Mechanism

   The IANA has registered upon Standards Action the LDAP Protocol
   Mechanism described in this document.

      Subject: LDAP Protocol Mechanism Registration
      Object Identifier: 1.3.6.1.1.8
      Description: LDAP Cancel Operation
      Person & email address to contact for further information:
           Kurt Zeilenga <kurt@openldap.org>
      Usage: Extended Operation
      Specification: RFC 3909
      Author/Change Controller: IESG
      Comments: none

5.3. LDAP Result Codes

   The IANA has registered upon Standards Action the LDAP Result Codes
   described in this document.

      Subject: LDAP Result Code Registration
      Person & email address to contact for further information:
           Kurt Zeilenga <kurt@OpenLDAP.org>
      Result Code Name: canceled (118)
      Result Code Name: noSuchOperation (119)
      Result Code Name: tooLate (120)
      Result Code Name: cannotCancel (121)
      Specification: RFC 3909
      Author/Change Controller: IESG

6. Acknowledgment

   The LDAP Cancel operation is modeled after the X.511 DAP Abandon
   operation.

7. References

7.1. 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.

   [RFC2830]   Hodges, J., Morgan, R., and M. Wahl, "Lightweight
               Directory Access Protocol (v3): Extension for Transport
               Layer Security", RFC 2830, May 2000.

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

   [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).

7.2. Informative References

   [RFC3383]   Zeilenga, K., "Internet Assigned Numbers Authority (IANA)
               Considerations for the Lightweight Directory Access
               Protocol (LDAP)", BCP 64, RFC 3383, September 2002.

   [X.511]   International Telecommunication Union - Telecommunication
               Standardization Sector, "The Directory: Abstract Service
               Definition", X.511(1993).

8. Author's Address

   Kurt D. Zeilenga
   OpenLDAP Foundation

   EMail: Kurt@OpenLDAP.org

9. Full Copyright Statement

Intellectual Property

Acknowledgement