Network Working Group — M. Wahl
Request for Comments: DRAFT — Innosoft International, Inc.
Expires in six months from — August 7, 1998
Intended Category: Standards Track

LDAPv3 Triggered Search Control

<draft-ietf-ldapext-trigger-01.txt>

1. Status of this Memo

This document is an Internet-Draft. 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.''

To learn the current status of any Internet-Draft, please check the ``1id-abstracts.txt'' listing contained in the Internet-Drafts Shadow Directories on ftp.is.co.za (Africa), nic.nordu.net (Europe), munnari.oz.au (Pacific Rim), ftp.ietf.org (US East Coast), or ftp.isi.edu (US West Coast).

Copyright Notice

2. Abstract

This document defines a LDAPv3 [2] control to be used on the Search Request to allow a client to retrieve information on changes which are made to the directory information tree held by that server.

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 RFC 2119 [1].

3. Definition of control sent by client

A client may provide a control of a particular type when invoking a search request.

The controlType is "1.3.6.1.4.1.1466.29539.10", the criticality field may be TRUE or FALSE, and the controlValue field is absent.

The search request size and time limits SHOULD both be 0.

The server will return SearchResultEntry responses for all entries which match the client's search filter. However, the server will not return a SearchResultDone as it would normally.

Instead, the server will preserve the client's message id, search filter and requested attribute list and associate it with the client's connection and this message id.

The server will only return the SearchResultDone if there is an error condition (e.g. unwillingToPerform), and will not return the SearchResultDone if the request was successful.

So long as the connection to the client is open and the client does not abandon the request or reuse the request message id, the server will return additional SearchResultEntry responses as entry addition, deletions and modifications occur resulting in entries which match the search. These responses have the same message id as the original request.

The client may terminate the return of responses by abandoning the request.

4. Using the control in a naming context other than the changelog

The client can use this control when performing a search of all or part of one or more naming contexts. When the naming context is not the change log [3], the server includes a control defined in section 4.1 with each SearchResultEntry returned by the server.

The entries in the naming contexts to which the client has access, are in the scope of the search and match the filter are termed the result set.

As entries enter the result set, leave the result set, or are modified in place, then an additional SearchResultEntry is returned to the client.

An entry can enter the result set for the following reasons:

- a new entry is added which matches the scope and filter,
- an entry which did not match the filter is modified to add attributes which cause it to now match the filter,
- an entry which matches the filter but was outside of the scope is renamed (or one of its superior entries is renamed) so that it is now in scope, or
- a change to access control or other administrative function cause an entry which matches the scope and filter to be visible to the client.

An entry can leave the result set for the following reasons:

- an entry which matched the scope and filter is deleted,
- an entry which matched the scope and filter is modified so that it no longer matches the filter,
- an entry which matched the scope and filter is renamed (or one of its superior entries is renamed) so that it is no longer in scope,

- a change to access control or other administrative function cause an entry which was visible to the client and matched the scope and filter to no longer be visible, and the resulting access control allows the client to be notified of this.

4.1. Definition of control returned by server

The controlType is 1.3.6.1.4.1.1466.29539.13, the criticality is TRUE, and the controlValue contains the bytes of the BER-encoding of the following ASN.1 type:

```
TriggerResultControl ::= SEQUENCE {
  resultType ENUMERATED {
    notChange     (0),
    enteredSet    (1),
    leftSet       (2),
    modified      (3) },
  [1] changeType LDAPString OPTIONAL,
  [2] previousDN LDAPDN OPTIONAL,
  [3] changeNumber LDAPString OPTIONAL }
```

The resultType is defined as follows:

- notChange: the entry existed in the directory and matched the search at the time the operation is being performed,
- enteredSet: the entry entered the result set for one of the reasons defined in section 4 above,
- leftSet: the entry left the result set for one of the reasons defined in section 4 above,
- modified: the entry was part of the result set, was modified or renamed, and still is in the result set.

The changeType field is as defined to have the same value as the changeType attribute in the change log, such as "add", "delete", "modify" or "modrdn".

If the changeType is "modrdn", then the previousDN field contains the name of the entry before the rename.

The changeNumber is defined to have the same value as the changeNumber attribute in the change log: the string representation of change number assigned by the server for the change. It SHOULD be present if the server supports the change log.

4.2. Example

To be provided in a later revision of this draft.

5. Using the triggered search control in the changelog

The client can also use this control when performing a search of the change log [3]. In this case, the search request MUST have the baseObject field set to the name of the base of the server's change log and the scope MUST be either singleLevel or wholeSubtree.

5.1. Example

To be provided in a later revision of this draft.

5.2. Matching Rule

A matching rule is defined to allow the client to request changes from only a particular portion of the tree when using the changelog.

A server will advertise support for this matching rule by having the following rule definition present in the subschema subentry governing the changelog. (A client can determine the subschema subentry for the changelog by retrieving the attribute subschemaSubentry from the base entry of the changelog.)

```
( 1.3.6.1.4.1.1466.29539.10.1 NAME 'dnSubordinateTo'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 )
```

An extensibleMatch filter will evaluate to TRUE for an entry to which the client has access if the matchingRule field is 1.3.6.1.4.1.1466.29539.10.1, the type field is any attribute with DN syntax (1.3.6.1.4.1.1466.115.121.1.12), and there is a value of that attribute present in an entry which is the same as or subordinate to the matchValue field.

For example, if a client presented the following filter:

```
(targetDN:1.3.6.1.4.1.1466.29539.10.1:=dc=acme,dc=com)
```

the filter would evaluate as follows for the following values, assuming the client had sufficient access rights to perform the filtering:

```
targetDn: dc=org                           FALSE
targetDn: dc=com                           FALSE
targetDn: dc=acme,dc=com                   TRUE
targetDn: dc=www,dc=acme,dc=com            TRUE
targetDn: dc=www,dc=acme,dc=com,dc=sg      FALSE
targetDn: cn=server,dc=www,dc=acme,dc=com   TRUE
```

6. Scaling Considerations

The use of this control may greatly increase the amount of server processing for modification operations, as well as the amount of network traffic as clients are notified of changes. Server implementations used on the Internet MUST have support administrative restrictions on the use of search triggers.

7. Security Considerations

The changes attribute of the change log entries should not be generally readable. The administrator will typically configure specific users who are authorized to retrieve this attribute.

8. Acknowledgements

This document is a product of the LDAPEXT working group. The ideas of Mark Smith, Gordon Good, Tim Howes and Rob Weltman in their persistent search draft are particularly acknowledged as contributing to this document.

9. Bibliography

[1] S. Bradner, "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119.

[2] "Lightweight Directory Access Protocol (v3)", RFC 2251.

[3] "Definition of An Object Class to Hold LDAP Change Records", INTERNET DRAFT <draft-good-ldap-changelog-00.txt>.

10. Authors Address

Mark Wahl

Innosoft International Inc.
8911 Capital of Texas Hwy Suite 4140
Austin, TX 78759 USA

Phone: +1 626 919 3600
EMail: M.Wahl@innosoft.com

Full Copyright Statement