Sieve Working Group	A. Melnikov	
Internet-Draft	Isode Limited	
Intended status: Standards Track	B. Leiba	
Expires: April 25, 2011	Huawei Technologies	
	October 22, 2010	

Sieve Extension: Externally Stored Lists
draft-ietf-sieve-external-lists-03

Abstract

The Sieve scripting language can be used to implement whitelisting, blacklisting, personal distribution lists, and other sorts of list matching. Currently, this requires that all members of such lists be hardcoded in the script itself. Whenever a member of a list is added or deleted, the script needs to be updated and possibly uploaded to a mail server.
This document defines a Sieve extension for accessing externally stored lists -- lists whose members are stored externally to the script, such as using LDAP (RFC 4510), ACAP (RFC 2244), or relational databases.

ToDo

*Do we need support for URI schemes in ihave? From IETF 77 minutes: "Can use ihave to test if a URI is valid, both that the scheme is supported and that the URI can be retrieved/queried."

*Do we need to say anything about comparators? We can be silent (as now), we can say that comparators MAY be ignored as a list-specific thing, or we can say that comparators MUST NOT be used.

*Should we add a mandatory-to-implement tag? Ned suggests (and I agree) that it might be good to add a registry of well-defined strings that can be used instead of URIs, and define the initial string "pab" to represent the user's personal address book.

Status of this Memo

documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.
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."
This Internet-Draft will expire on April 25, 2011.

Copyright Notice

Table of Contents

1. Introduction

This document specifies an extension to the Sieve language [RFC5228] (Guenther, P. and T. Showalter, "Sieve: An Email Filtering Language," January 2008.) for checking membership in an external list or for redirecting messages to an external list of recipients. An "external list" is a list whose members are stored externally to the Sieve script, such as using LDAP [RFC4510] (Zeilenga, K., "Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map," June 2006.), ACAP [RFC2244] (Newman, C. and J. Myers, "ACAP -- Application Configuration Access Protocol," November 1997.), or relational databases.
This extension adds a new match type to apply to supported tests, and a new tagged argument to the "redirect" action.

1.1. Conventions used in this document

Conventions for notations are as in [RFC5228] (Guenther, P. and T. Showalter, "Sieve: An Email Filtering Language," January 2008.) section 1.1, including the use of [RFC5234] (Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF," January 2008.).
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] (Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," March 1997.).

2. Extlists extension

2.1. Capability Identifier

The capability string associated with the extension defined in this document is "extlists".

2.2. :list match type for supported tests

ABNF:

   MATCH-TYPE =/ ":list" ; only valid for supported tests

The new ":list" match type changes the interpretation of the "key-list"
parameter (the second parameter) to supported tests. When the match
type is ":list", the key-list becomes a list of names of externally
stored lists. The external lists are queried, perhaps through a list-
specific mechanism, and the test evaluates to "true" if any of the
specified values matches any member of one or more of the lists.
Implementations MUST support "address", "envelope" and "header" tests.
Implementations that include the Variables extension [RFC5229] (Homme,
K., "Sieve Email Filtering: Variables Extension," January 2008.) MUST
also support "string" tests.
Implementations MAY support other tests but MUST raise an error (which
SHOULD be a compile-time error, but MAY be a runtime error) when a
script uses :list with a test for which it is not supported. To
maintain interoperability, other tests that can be used with :list
SHOULD be documented in a specification that defines a capability
string that can be tested (in a "require" statement, or using ihave
[RFC5463] (Freed, N., "Sieve Email Filtering: Ihave Extension,"
March 2009.)).
For example, testing ':header ["to", "cc"]' against a list would cause
each "to" and "cc" value, ignoring leading and trailing whitespace, to
be queried. If any value is found to belong to the list, the test
returns "true". If no value belongs to the list, the test returns
"false". Once a value is found in the list, there is no need for the
query mechanism to look further.
For some lists, the Sieve engine might directly retrieve the list and
make its own comparison. Other lists might not work that way -- they
might provide a way to ask if a value is in the list, but not permit
retrieval of the list itself. It is up to the Sieve implementation to
understand how to interact with any supported list. If the Sieve engine
is permanently unable to query the list (perhaps because the list
doesn't support the required operation), the test MUST result in a
runtime error in the Sieve script.
See Section 2.5 (Syntax of an externally stored list name) for the
detailed description of syntax used for naming externally stored lists.

2.3. :list tagged argument to the "redirect" action

   Usage: redirect :list <ext-list-name: string>

The "redirect" action with the ":list" argument is used to send the message to one or more email addresses stored in the externally stored list 'ext-list-name'. This variant of the redirect command can be used to implement a personal distribution list.
For this feature to work, one of the following conditions has to be true:

1. The list resolves to a list of email addresses, and the Sieve engine is able to enumerate those addresses.

2. The list handler is able to take care of the redirection on behalf of the Sieve engine.

In cases where, for example, a list contains hashed email address values or an email address pattern ("sz*@example.com", "*+ietf@example.net"), the Sieve engine will not be able to redirect to that list, and responsibility must pass to the list handler.
If neither the Sieve engine nor the list handler can enumerate (or iterate) the list, or the list does not resolve to email addresses, the situation MUST result in a runtime error in the Sieve script.
See Section 2.5 (Syntax of an externally stored list name) for the detailed description of syntax used for naming externally stored lists.

2.4. Other uses for external lists   TOC

The uses for external lists specified here represent the useful cases and situations at the time of this writing. Other uses for external lists, using other Sieve features, might be devised in the future, and such uses can be described in extensions to this document.

2.5. Syntax of an externally stored list name   TOC

A name of an externally stored list is always an absolute URI [RFC3986] (Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax," January 2005.). Implementations might find URIs such as [RFC4510] (Zeilenga, K., "Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map," June 2006.), [I-D.ietf-vcarddav-carddav] (Daboo, C., "vCard Extensions to WebDAV (CardDAV)," November 2009.), or [RFC4151] (Kindberg, T. and S. Hawke, "The 'tag' URI Scheme," October 2005.) to be useful for naming external lists.
The "tag" URI scheme [RFC4151] (Kindberg, T. and S. Hawke, "The 'tag' URI Scheme," October 2005.) MUST be supported, and can be used to represent opaque, but user friendlier identifiers. Resolution of such

identifiers is going to be implementation specific and it can help in
hiding the complexity of an implementation from end users. For example,
an implementation can provide a web interface for managing lists of
users stored in LDAP. Requiring users to know generic LDAP URI syntax
might not be very practical, due to its complexity. An implementation
can instead use a fixed tag URI prefix such as
"tag:example.com,<date>:" (where <date> can be, for example, a date
generated once on installation of the web interface and left untouched
upon upgrades) and the prefix doesn't even need to be shown to end
users.

2.6. Interaction with ManageSieve

This extension defines the following new capability for ManageSieve
(see [RFC5804] (Melnikov, A. and T. Martin, "A Protocol for Remotely
Managing Sieve Scripts," July 2010.) section 1.7):
EXTLISTS - A space-separated list of URI schema parts [RFC3986]
(Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource
Identifier (URI): Generic Syntax," January 2005.) for supported
externally stored list types. This capability MUST be returned if the
Sieve implementation supports the "extlists" extension defined in this
document.
This also extends the ManageSieve ABNF as follows:

```
single-capability  =/ DQUOTE "EXTLISTS" DQUOTE SP ext-list-types
   CRLF ; single-capability is defined in [RFC5804] (Melnikov, A.
   and T. Martin, "A Protocol for Remotely Managing Sieve Scripts,"
   July 2010.)

ext-list-types  = string ; space separated list of URI schema parts
   ; for supported externally stored list types.
   ; MUST NOT be empty.
```

2.7. Examples

This example uses the "envelope" option [RFC5228] (Guenther, P. and T.
Showalter, "Sieve: An Email Filtering Language," January 2008.) and the
"subaddress" extension [RFC5233] (Murchison, K., "Sieve Email
Filtering: Subaddress Extension," January 2008.):

```
        require ["extlists", "envelope", "subaddress"];

        # Submission from list members is sent to all members
        if allof (envelope :detail :list "to"
                           "tag:example.com,2009-05-28:mylist",
                 header :list "from"
                           "tag:example.com,2009-05-28:mylist") {
           redirect :list "tag:example.com,2009-05-28:mylist";
        }
```

This example uses the "currentdate" test [RFC5260] (Freed, N., "Sieve Email Filtering: Date and Index Extensions," July 2008.) and a list containing the dates of local holidays. If today is a holiday, the script will notify [RFC5435] (Melnikov, A., Leiba, B., Segmuller, W., and T. Martin, "Sieve Email Filtering: Extension for Notifications," January 2009.) the user via XMPP [RFC5437] (Saint-Andre, P. and A. Melnikov, "Sieve Notification Mechanism: Extensible Messaging and Presence Protocol (XMPP)," January 2009.) about the message.

```
        require ["extlists", "date", "enotify"];
        if currentdate :list "date"
            "tag:example.com,2010-01-01:localHolidays" {
            notify "xmpp:romeo@im.example.com";
        }
```

This example uses a personal address book, along with spamtest [RFC5235] (Daboo, C., "Sieve Email Filtering: Spamtest and Virustest Extensions," January 2008.) and the relational extension [RFC5231] (Segmuller, W. and B. Leiba, "Sieve Email Filtering: Relational Extension," January 2008.) to give a different level of spam tolerance to known senders.

```
        require ["envelope", "extlists", "fileinto", "spamtest",
                 "relational", "comparator-i;ascii-numeric"];
        if allof (
             envelope :list "from" "tag:example.com,2010-04-10:pab",
             spamtest :value "ge" :comparator "i;ascii-numeric" "8"
                  )
          { /* Known: allow high spam score */
            fileinto "spam";
          }
        elsif spamtest :value "ge" :comparator "i;ascii-numeric" "3"
          { /* Unknown: less tolerance in spam score */
            fileinto "spam";
          }
```

3. Security Considerations

Security considerations related to the "address"/"envelope"/"header" tests and "redirect" action discussed in [RFC5228] (Guenther, P. and T. Showalter, "Sieve: An Email Filtering Language," January 2008.) also apply to this document.
External list memberships ought to be treated as if they are an integral part of the script, so a temporary failure to access an external list SHOULD be handled in the same way as a temporary failure to retrieve the Sieve script itself.
For example, if the Sieve script is stored in the Lightweight Directory Access Protocol [RFC4510] (Zeilenga, K., "Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map," June 2006.) and the script can't be retrieved when a message is processed (perhaps the LDAP server is unavailable), then the Sieve engine might delay message delivery until the script can be retrieved successfully. Similarly, if an external list is stored in LDAP and that LDAP server is unavailable, the Sieve engine would take the same action -- delay message delivery and try again later.
Protocols/APIs used to retrieve/verify external list membership MUST provide an appropriate level of confidentiality and authentication. Usually, that will be at least the same level of confidentiality as protocols/APIs used to retrieve Sieve scripts, but only the implementation (or deployment) will know what is appropriate. There's a difference, for example, between making an LDAP request on a closed LAN that's only used for trusted servers (it may be that neither encryption nor authentication is needed), on a firewalled LAN internal to a company (it might be OK to skip encryption, depending upon policy), and on the open Internet (encryption and authentication are probably both required). It also matters whether the list being accessed is private or public (no encryption or authentication may be needed for public data, even on the Internet).
Implementations of this extension should keep in mind that matching values against an externally stored list can be IO and/or CPU intensive. This can be used to deny service to the mailserver and/or to servers providing access to externally stored mailing lists. A naïve implementation, such as the one that tries to retrieve content of the whole list to perform matching can make this worse.
But note that many protocols that can be used for accessing externally stored lists support flexible searching features that can be used to minimize network traffic and load on the directory service. For example, LDAP allows for search filters. Implementations SHOULD use such features whenever they can.
Many organizations support external lists with thousands of recipients. In order to avoid mailbombs when redirecting a message to an externally stored list, implementations SHOULD enforce limits on the number of recipients and/or on domains to which such recipients belong.

4. IANA Considerations

4.1. Registration of Sieve extension

The following template specifies the IANA registration of the Sieve
extension specified in this document:
To: iana@iana.org
Subject: Registration of new Sieve extension
Capability name: extlists
Description: adds the ':list' match type to certain Sieve tests, and
the ':list' argument to the 'redirect' action. The ':list' match type
changes tests to match values against values stored in one or more
externally stored lists. The ':list' argument to the redirect action
changes the redirect action to forward the message to email addresses
stored in the externally stored list.
RFC number: this RFC
Contact address:
    The Sieve discussion list <sieve@ietf.org>
This information should be added to the list of sieve extensions given
on http://www.iana.org/assignments/sieve-extensions.

4.2. Registration of ManageSieve capability

The following requests IANA to register a new ManageSieve Capability
according to the IANA registration template specified in [RFC5804]
(Melnikov, A. and T. Martin, "A Protocol for Remotely Managing Sieve
Scripts," July 2010.):
To: iana@iana.org
Subject: ManageSieve Capability Registration
Capability name: extlists
Description: This capability is returned if the server supports the
"extlists" [RFCXXXX] Sieve extension.
Relevant publications: this RFC, Section 2.6 (Interaction with
ManageSieve)
Person & email address to contact for further information: Alexey
Melnikov <alexey.melnikov@isode.com>
Author/Change controller: IESG

5. Acknowledgements

Thanks to Alexandros Vellis, Nigel Swinson, Ned Freed, Kjetil Torgrim Homme, Dave Cridland, Cyrus Daboo, Pete Resnick, and Robert Burrell Donkin for ideas, comments and suggestions. Kristin Hubner also helped greatly with the examples.

---

6. References   [TOC]

6.1. Normative References   [TOC]

[RFC2119]	Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," BCP 14, RFC 2119, March 1997 (TXT, HTML, XML).
[RFC3986]	Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax," STD 66, RFC 3986, January 2005 (TXT, HTML, XML).
[RFC4151]	Kindberg, T. and S. Hawke, "The 'tag' URI Scheme," RFC 4151, October 2005 (TXT).
[RFC5228]	Guenther, P. and T. Showalter, "Sieve: An Email Filtering Language," RFC 5228, January 2008 (TXT).
[RFC5234]	Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF," STD 68, RFC 5234, January 2008 (TXT).
[RFC5804]	Melnikov, A. and T. Martin, "A Protocol for Remotely Managing Sieve Scripts," RFC 5804, July 2010 (TXT).

6.2. Informative References   [TOC]

[I-D.ietf-vcarddav-carddav]	Daboo, C., "vCard Extensions to WebDAV (CardDAV)," draft-ietf-vcarddav-carddav-10 (work in progress), November 2009 (TXT).
[RFC2244]	Newman, C. and J. Myers, "ACAP -- Application Configuration Access Protocol," RFC 2244, November 1997 (TXT).
[RFC4510]	Zeilenga, K., "Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map," RFC 4510, June 2006 (TXT).
[RFC5229]	Homme, K., "Sieve Email Filtering: Variables Extension," RFC 5229, January 2008 (TXT).
[RFC5231]	

	Segmuller, W. and B. Leiba, "Sieve Email Filtering: Relational Extension," RFC 5231, January 2008 (TXT).
[RFC5233]	Murchison, K., "Sieve Email Filtering: Subaddress Extension," RFC 5233, January 2008 (TXT).
[RFC5235]	Daboo, C., "Sieve Email Filtering: Spamtest and Virustest Extensions," RFC 5235, January 2008 (TXT).
[RFC5260]	Freed, N., "Sieve Email Filtering: Date and Index Extensions," RFC 5260, July 2008 (TXT).
[RFC5435]	Melnikov, A., Leiba, B., Segmuller, W., and T. Martin, "Sieve Email Filtering: Extension for Notifications," RFC 5435, January 2009 (TXT).
[RFC5437]	Saint-Andre, P. and A. Melnikov, "Sieve Notification Mechanism: Extensible Messaging and Presence Protocol (XMPP)," RFC 5437, January 2009 (TXT).
[RFC5463]	Freed, N., "Sieve Email Filtering: Ihave Extension," RFC 5463, March 2009 (TXT).

Authors' Addresses

	Alexey Melnikov
	Isode Limited
	5 Castle Business Village
	36 Station Road
	Hampton, Middlesex TW12 2BX
	UK
Email:	Alexey.Melnikov@isode.com
	Barry Leiba
	Huawei Technologies
Phone:	+1 646 827 0648
Email:	barryleiba@computer.org
URI:	http://internetmessagingtechnology.org/