Sieve Notification Mechanism: xmpp
draft-ietf-sieve-notify-xmpp-04

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

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.

This Internet-Draft will expire on September 2, 2007.

Copyright Notice

Copyright (C) The IETF Trust (2007).

Abstract

This document describes a profile of the Sieve extension for notifications, to allow notifications to be sent over the Extensible Messaging and Presence Protocol (XMPP), also known as Jabber.
Table of Contents

1. Introduction ................................................. 3
   1.1. Overview ............................................... 3
   1.2. Terminology ............................................ 3
2. Definition .................................................. 3
   2.1. Notify parameter "method" .............................. 3
   2.2. Notify tag ":from" ................................... 4
   2.3. Notify tag ":options" .................................. 4
   2.4. Notify tag ":importance" ............................... 4
   2.5. Notify tag ":message" .................................. 4
3. Examples ..................................................... 4
4. Requirements Conformance ................................. 5
5. Internationalization Considerations .................. 6
6. Security Considerations .................................. 7
7. References .................................................. 7
   7.1. Normative References ................................. 7
   7.2. Informative References ............................... 8
Authors’ Addresses ............................................. 8
Intellectual Property and Copyright Statements .......... 9
1. Introduction

1.1. Overview

The [NOTIFY] extension to the [SIEVE] mail filtering language is a framework for providing notifications by employing URIs to specify the notification mechanism. This document defines how xmpp URIs (see [XMPP-URI]) are used to generate notifications via the Extensible Messaging and Presence Protocol (see [XMPP]), which is widely implemented in Jabber instant messaging technologies.

1.2. Terminology

This document inherits terminology from [NOTIFY], [SIEVE], and [XMPP]. The capitalized key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [TERMS].

2. Definition

The xmpp mechanism results in the sending of an XMPP message to notify a recipient about an email message. The general XMPP syntax is as follows:

- The notification MUST be an XMPP <message/> stanza.
- The value of the XMPP ‘type’ attribute MUST be ‘headline’ or ‘normal’.
- The value of the XMPP ‘from’ attribute MUST be the XMPP address of the notification service.
- The XMPP <message/> stanza MAY include a <subject/> child element whose value is some configurable text indicating that the message is a Sieve notification.
- The notification SHOULD include a URL for the recipient to use as a hint in locating the message, encapsulated as the XML character data of a <url/> child element of an <x/> element qualified by the 'jabber:x:oob' namespace as specified in [OOB].

The recommended mapping of the Sieve notify action into XMPP syntax is described in the following sections.

2.1. Notify parameter "method"

The "method" parameter MUST be a URI that conforms to the xmpp URI scheme (as specified in [XMPP-URI]) and that identifies an XMPP
account associated with the email inbox. The URI MAY include the resource identifier portion of an XMPP address but SHOULD NOT include an authority component, query component, or fragment identifier component. The processing application MUST extract an XMPP address from the URI in accordance with the processing rules specified in [XMPP-URI]. The resulting XMPP address MUST be encapsulated in XMPP syntax as the value of the XMPP 'to' attribute.

2.2. Notify tag ":from"

The ":from" tag has no special meaning for this notification mechanism, and this specification puts no restriction on its use. As noted, the value of the XMPP 'from' attribute specified in the XMPP notification message MUST be the XMPP address of the notification service itself. The value of the ":from" tag MAY be transformed into XMPP syntax; if so, it SHOULD be encapsulated as the value of an XMPP [SHIM] header named "Reply-To".

2.3. Notify tag ":options"

The ":options" tag has no special meaning for this notification mechanism. Any handling of this tag is the responsibility of an implementation.

2.4. Notify tag ":importance"

The ":importance" tag has no special meaning for this notification mechanism, and this specification puts no restriction on its use. The value of the ":importance" tag MAY be transformed into XMPP syntax (in addition to or instead of including in the default message); if so, it MUST be encapsulated as the value of an XMPP [SHIM] header named "Urgency", and the XML character of that header MUST be "high" if the value of the ":importance" tag is "1", "medium" if the value of the ":importance" tag is "2", or "low" if the value of the ":importance" tag is "3".

2.5. Notify tag ":message"

If included, the ":message" tag SHOULD be transformed into the XML character data of an XMPP <body/> element. If not included, the rule specified in [NOTIFY] SHOULD be followed, as shown in the examples below.

3. Examples

In the following examples, the sender of the email has an address of <mailto:juliet@example.org>, the entity to be notified has an XMPP
The address of <xmpp:romeo@example.com>, and the notification service has an XMPP address <xmpp:notify.example.com>.

The following is a basic Sieve notify action with only a method:

```
notify "xmpp:romeo@example.com"
```

The resulting XMPP <message/> stanza might be as follows:

```
<message from='notify.example.com'
  to='romeo@example.com'
  xml:lang='en'>
  <subject>A Sieve instant notification!</subject>
  <body>&lt;juliet@example.org&gt; Wherefore art thou?</body>
</message>
```

The following is a more advanced Sieve notify action with a method, importance, subject, and message, as well as a URL pointing to the message:

```
notify :importance "1"
  :message "Contact Juliet immediately!"
  "xmpp:romeo@example.com?message;subject=SIEVE"
```

The resulting XMPP <message/> stanza might be as follows:

```
<message from='notify.example.com'
  to='romeo@example.com'
  xml:lang='en'>
  <subject>SIEVE</subject>
  <body>Contact Juliet immediately!</body>
  <headers xmlns='http://jabber.org/protocol/shim'>
    <header name='Urgency'>high</header>
  </headers>
  <x xmlns='jabber:x:oob'>
    <url>
      imap://romeo@example.com/INBOX;UIDVALIDITY=385759045;/UID=20
    </url>
  </x>
</message>
```

4. Requirements Conformance

Section 3.8 of [NOTIFY] specifies a set of requirements for Sieve notification methods. The conformance of the xmpp notification mechanism is provided here.
1. An implementation of the xmpp notification method MAY modify the final notification text (e.g., limit the length to a configurable number of characters, such as 200). Modification of characters themselves should not be necessary, since XMPP character data is encoded in [UTF-8].

2. An implementation MAY ignore parameters specified in the ":from", ":options", ":importance", and ":message" tags.

3. The xmpp notification method does not recommend the default message to be used if the ":message" argument is not specified.

4. A notification sent via the xmpp notification method MAY include a timestamp in the textual message.

5. The value of the XMPP 'from' attribute MUST be the XMPP address of the xmpp notification service. The value of the Sieve ":from" tag MAY be transformed into the value of an XMPP [SHIM] header named "Reply-To".

6. An implementation MUST NOT include any other extraneous information not specified in parameters to the notify action.

7. In accordance with [XMPP-URI], an implementation MUST ignore any URI action or parameter it does not understand (i.e., the URI MUST be processed as if the action or parameter were not present). It is RECOMMENDED to support the "message" action and the associated "body" and "subject" parameters, which parameters SHOULD be mapped to the XMPP <body/> and <subject/> child elements of the XMPP <message/> stanza type, respectively.

8. In response to a notify_method_capability test for the "online" notification-capability, an implementation SHOULD return a value of "yes" if it has knowledge of an active presence session for the specified notification-uri and a value of "no" if it does not have such knowledge.

9. An implementation SHOULD NOT attempt to retry delivery of a notification if it receives an XMPP error of type "auth" or "cancel", MAY attempt to retry delivery if it receives an XMPP error of type "wait", and MAY attempt to retry delivery if it receives an XMPP error of "modify" but only if it makes appropriate modifications to the notification (see [XMPP]); in any case the number of retries SHOULD be limited to a configurable number no less than 3 and no more than 10. An implementation MAY throttle notifications if the number of notifications within a given time period becomes excessive according to local service policy. Duplicate suppression (if any) is a matter of implementation and is not specified herein.

5. Internationalization Considerations

Although an XMPP address may contain nearly any [UNICODE] character, the value of the "method" parameter MUST be a Uniform Resource Identifier (see [URI]) rather than an Internationalized Resource
Identifier (see [IRI]). The rules specified in [XMPP-URI] MUST be
followed when generating XMPP URIs.

In accordance with Section 13 of RFC 3920, all data sent over XMPP
MUST be encoded in [UTF-8].

6. Security Considerations

Depending on the information included, sending a notification can be
comparable to forwarding mail to the notification recipient. Care
must be taken when forwarding mail automatically, to ensure that
confidential information is not sent into an insecure environment.
In particular, implementations MUST conform to the security
considerations given in [NOTIFY], [SIEVE], and [XMPP].

7. References

7.1. Normative References

[OOB]    Saint-Andre, P., "Out of Band Data", XSF XEP 0066,
          January 2006.

[NOTIFY] Melnikov, A., Leiba, B., Segmuller, W., and T. Martin,
          "Sieve Extension: Notifications",
          draft-ietf-sieve-notify-07 (work in progress),
          February 2007.

[SHIM]    Saint-Andre, P. and J. Hildebrand, "Stanza Headers and
          Internet Metadata", XSF XEP 0131, August 2005.

[SIEVE]   Showalter, T. and P. Guenther, "Sieve: An Email Filtering
          Language", draft-ietf-sieve-3028bis-12 (work in progress),
          February 2007.

[TERMS]   Bradner, S., "Key words for use in RFCs to Indicate

[XMPP-URI]
          Saint-Andre, P., "Internationalized Resource Identifiers
          (IRIs) and Uniform Resource Identifiers (URIs) for the
          Extensible Messaging and Presence Protocol (XMPP)",
          RFC 4622, August 2006.
7.2. Informative References


Authors’ Addresses

Peter Saint-Andre  
XMPP Standards Foundation  
Email: stpeter@jabber.org  

Alexey Melnikov  
Isode Limited  
Email: Alexey.Melnikov@isode.com