Session Initiation Protocol (SIP) Extension for logging and debugging.
draft-kaithal-dispatch-sip-log-information-00

Abstract

The current mechanisms to debug issues in SIP network are not very efficient. It requires to enable debugging logs across different devices, recreate the problem and then collect the logs. The idea is to provide a solution to automatically enable relevant logs (SIP messages and any other debugging logs meaningful to SIP devices), and also to indicate where the logs are to be collected or stored. The enabling of logs will happen at all the SIP devices (upstream or downstream). This will help to get the logs from all the SIP devices in a Common logging format (CLF). The solution extends SIP to provide the infrastructure to enable logging for upstream and downstream devices with each server deciding how much troubleshooting information it wants to log - with freedom to simply ignore requests if required. This document specifies a new header called "Log-Me" Header in all the SIP messages.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working 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 15, 2012.

Copyright Notice

Copyright (c) 2011 IETF Trust and the persons identified as the document authors. All rights reserved.
This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction .................................................. 3
2. Terminology .................................................... 3
3. Background ...................................................... 3
4. Applicability Statement .......................................... 4
5. Log-me Header Field Definition and Syntax ........................ 4
6. UAC Behaviour .................................................. 6
7. UAS Behaviour .................................................. 6
8. Proxy Behaviour ................................................ 7
9. Security Considerations .......................................... 7
10. IANA Considerations ............................................. 7
11. Normative References ........................................... 8
Authors’ Addresses ............................................... 8
1. Introduction

Session Initiation Protocol (SIP) is gaining popularity in the VoIP Network. Many deployments, currently, have deployed SIP for their VoIP network. Because of the huge deployments, isolating the problem in the network and troubleshooting it becomes very difficult. Also, if the problem happens in high traffic condition, or happens intermittently, collecting the right set of debugging logs is very difficult for further fault analysis.

There is need for an effective troubleshooting mechanisms embedded in the signalling so that logs from all the devices can be collected for that particular call and stored in a common location for troubleshooting.

2. 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 [RFC2119]. This document only uses these key words when referencing normative statements in existing RFCs.

3. Background

Troubleshooting in VOIP network is challenging as the signaling and media follow different path and Different equipment.

Scenario

UA1----B2BUA1-----P1-------P2-------B2BUA2------UA2

UA1 wishes to make a call to UA2, However, due to network Topology, UA1 has to go via B2BUA1 ,Proxy 1 (P1) , Proxy2 (P2) and B2BUA2 to reach UA2. Likewise, all requests between UA2 and UA1 must also traverse through the same path.

UA1 makes a SIP call to UA2. This call has some issue. In order to debug the issue, logs need to be enabled at all the SIP devices in the network. It involves a lot of time and effort collect the logs and troubleshoot it.

The "Log-Me" extension header field allows all the SIP devices (upstream and downstream) to start collecting desired logs, store it in to a common location and available for debugging. It may store the data in Common Logging Format so that It can be fed to a device
which make the troubleshooting faster moreover the logs are in a standard format and easier to troubleshoot. This header element’s function is to invoke tracing and troubleshooting functions at each "hop" in the signaling path for the call. Additionally, it includes a unique "tag" to allow the information to be associated with the particular call for proper correlation.

4. Applicability Statement

The Log-me mechanism is applicable to all the SIP entity in the network which includes UAS, UAC, Proxy, B2BUA etc.

1) Each entity is free to simply ignore request, if it is not interested in log collection, or busy with other activities.

2) Each entity can add its own "Log-Me" header and provide the path for the log collection.

3) Each entity is free to log any information which is useful for troubleshooting.

4) If an entity does not understand the header then it can simply ignore it. However, it should not remove the header, as removing stops the possibility for logging at the next hop.

5) If SIP signalling is secure then logging MUST be secure.

6) If B2BUA gets a "Log-Me" header then it MUST NOT remove it. It MAY modify or append "Log-Me" header.

5. Log-me Header Field Definition and Syntax
Log-Me = "Log-Me" HCOLON log-value *(COMMA log-value)
log-value = log-type 1*(SEMI log-params)
log-type =  "mailto" / "http"/ "syslog" / "tftp" / "ftp" /"sftp" / "local" / other-type
log-params = log-maddr /log-uri/
    log-username/log-password/log-tag
log-maddr= "maddr" EQUALS host
log-uri = "uri" EQUALS userinfo
userinfo = user "@" host
log-username = "username" EQUALS user
user = 1*( unreserved / escaped / user-unreserved )
log-password= "password" EQUALS*( unreserved /
    escaped / "=" / "+" / "$" / "," )
log-tag = tag EQUALS token
other-type = token

Example :
Log-Me:mailto;uri=akaithal@cisco.com;tag=sdfrfgf43
Log-Me:syslog;maddr=9.45.45.34;username=akaithal;
password=addfere2;tag=sdfdsfe
Log-Me:local;tag=sdfdsfe

local means it should store the data locally.

Support for the Log-me header field MAY be indicated by a UA by including the option-tag "log" in a Supported header field.

Log-me header field value MUST consist of exactly one log-type. If the log-type is mailto then it should have a log-uri (i.e. an email address). For any other log-type log-username.log-password and log-maddr is MUST. One entity can put more than one Log-me header in multiple line or separated by comma. In case there are more than one Log-me header then it is the intermediate end point’s decision to put the log in all places mentioned, or choose any one of them. If log-uri and log-username are present then user portion of log-uri and log-username MUST be same.

This is an optional header and can be built only in a SIP request and response. The header can also be inserted by any intermediate entity in the network.
If a SIP REFER message is sent to an endpoint and contains the "Log-Me" header, not only is the REFER method itself traced, but any call initiated via the REFER mechanism is also traced. If "Log-Me" header is present in the request then entity should at least log SIP messages and any other relevant information which is required for debugging.

6. UAC Behaviour

If UAC supports this extension the it should add "log" tag in the supported header in the request or response. In case UAC wants the call to be logged then it MUST add a Log-me header with the details to enable logging.

UAC receives response with the "Log-Me" header then it starts collecting the data from that response on words till the end of the call. It logs messages which is mandatory along with other logging information which is essential for troubleshooting from that device point of view.

7. UAS Behaviour

UAS receives request with the "Log-Me" header then it starts
collecting the data from that request on words till the end of the
call. It logs messages which is mandatory along with other logging
information which is essential for troubleshooting from that device
point of view.

If UAS supports this extension the it should add debug tag in the
supported header in the request or response. In case UAS wants the
call to be logged then it MUST add a "Log-Me" header with the details
in any of the responses to enable logging.

8. Proxy Behaviour

1) If proxy supports "log" extension and it gets "Log-Me" header in
any of the request or response then it SHOULD process it and collect
relevant logs. Additionally it can do one of the following

a) Forward the received "Log-Me" header as is.

b) Add additional "Log-Me" header with details.

c) Add its own "Log-Me" header and removing the received "Log-Me"
header.

The above action are applicable for the forked requests as well.

2) If proxy does not support "log" extension and it receives "Log-Me"
header then it MUST NOT remove it from the requests or responses.

9. Security Considerations

There are security consideration with this header as password is
exposed.

1) It is RECOMMENDED to have calls over TLS to send "Log-Me" header.

2) It is RECOMMENDED for Intermediate devices to remove "Log-Me"
header if the next hop is not TLS. Alternatively it MAY modify
"Log-Me" header local log type.

10. IANA Considerations

There is no IANA consideration for this draft.
11. Normative References


Authors’ Addresses

Adarsh Kaithal
Cisco Systems, Inc.
Cessna Business Park,
Kadabeesanahalli Village, Varthur Hobli,
Sarjapur-Marathahalli Outer Ring Road
Bangalore, Karnataka 560103
India

Email: akaithal@cisco.com

Sandeep K S
Cisco Systems, Inc.
Cessna Business Park,
Kadabeesanahalli Village, Varthur Hobli,
Sarjapur-Marathahalli Outer Ring Road
Bangalore, Karnataka 560103
India

Email: sandks@cisco.com