Workgroup: Syslog Working Group
Internet-Draft:
draft-chen-syslog-syscinfo-credibility-00
Updates: RFC5424 (if approved)
Published: 6 March 2022
Intended Status: Standards Track
Expires: 7 September 2022
Authors: F. Wang China Mobile
M. Chen China Mobile
L. Su China Mobile

Improve logging credibility by adding synchronization time information

Abstract

This document proposes a scheme to improve the credibility of log reporting time by adding time synchronization information.

This document updates the "timeQuality" structured Data in RFC 5424 [RFC5424], The Syslog Protocol. By appending "SYNCINFO" information after the "isSynced" parameter, the log collector can judge the credibility of logs when correlating logs of different devices.

Status of This Memo

This Internet-Draft is submitted 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 https://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 7 September 2022.

Copyright Notice

Copyright (c) 2022 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 (https://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 Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction

The following content is from RFC 5424[RFC5424]

In the protocol, the timestamp parameter of the reported log and the parameter of whether the time has been synchronized have been set to indicate whether the reported time has been synchronized with the external time source. Although the standard has considered the accuracy requirements of time recording and designed a time "isSynced" parameter, it is impossible to ensure the credibility of time recording only through the synchronization flag parameters.

If the external time source of the originator is attacked or a fake time source, the log reported by the originator only records whether the time is synchronized, but does not report the synchronization time source information.By constructing a higher-level fake source time synchronization server, the attacker can easily affect the credibility of the log reporting time.

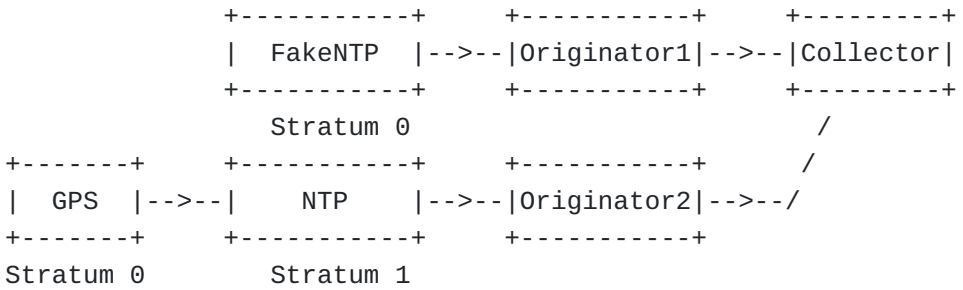

Figure 1: Attack Scenario

Take the above figure as an example. If Originator1 synchronizes to a fake NTP time source and Originator2 synchronizes to an NTP time source whose superior external time source is GPS, attacker can modify the system time of the fake NTP time source to affect the log reporting time of Originator1, which can further affect the time accuracy of Collector when correlating logs of different devices.

In order to solve the problem of the credibility of log reporting time, it is proposed to add synchronization time information after the synchronization flag parameter.

2. Terminology

The readers should be familiar with the terms defined in.

In addition, this document makes use of the following terms:

syncInfo: The syncInfo parameter is used to record current synchronization NTP source host IP or host name, remote refers to the NTP upper-level source host address, and stratum class;

3. Setting syncInfo

The parameters in RFC 5424 [RFC5424]does not have the function of Setting synchronization NTP information. This chapter proposes to add this new parameter after the "isSynced" parameter.

3.1. Setting new parameter

The following new parameter is defined.

SYNCINFO: The parameter indicates the synchronization time source information of the originator. The syncInfo parameter is included current synchronization NTP source host IP or host name, remote refers to the NTP upper-level source host address, and stratum class.

If the value "0" is used for "isSynced", this parameter MUST NOT be specified. If the value "1" is used for "isSynced" ,the originator's synchronization time source information needs to be added.

3.2. Examples

The following is an example of an originator that knows both its synchronization time source information and that it is externally synchronized:

[timeQuality isSynced="1" syncInfo="remote:time-d.nist.gov|
refid:NIST|st:1"]

The syncInfo parameter records that the current synchronization NTP source host name is time-d.nist.gov, the remote refers to the NTP upper-level source host address is NIST, and the stratum class is 1.

3.3. Handling of the collectors

When the log collector merges logs reported by different originators, it compares the synchronization time source information and the stratum class information in the logs:

If the different are synchronized with same time sources, the log time reported by different originators is credible;

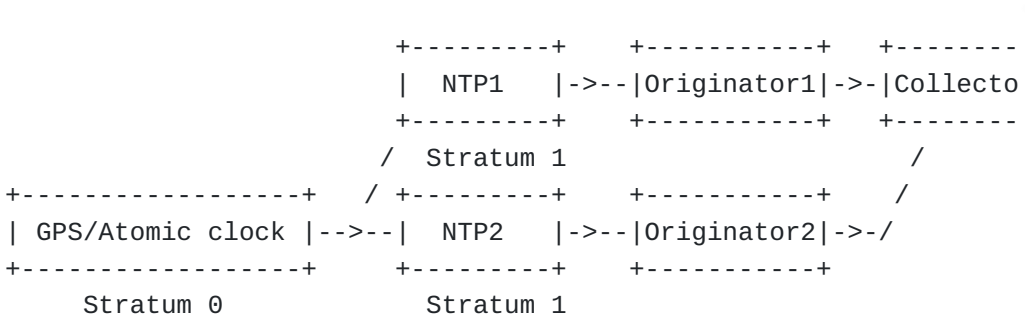

Figure 2: Trusted Scenario 1 for Log Reporting Time

If the different originators are synchronized with different time sources, it is necessary to determine whether the time source refers to a higher-quality external time source. If a higher-quality external time source is cited, the log time is credible. This log time cannot be trusted if a higher quality external time source is not referenced or the time is not synchronized.

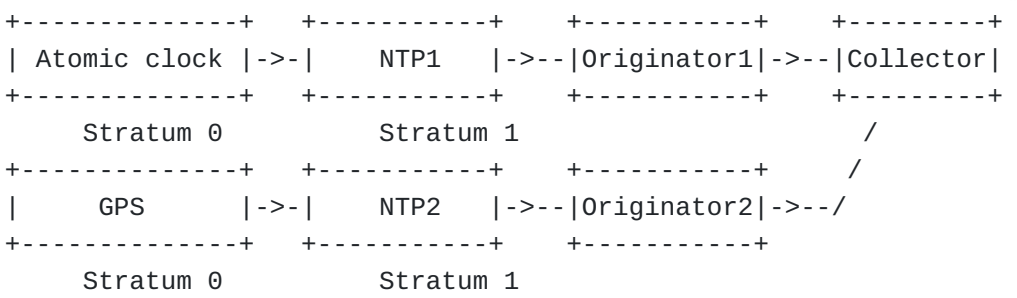

Figure 3: Trusted Scenario 2 for Log Reporting Time

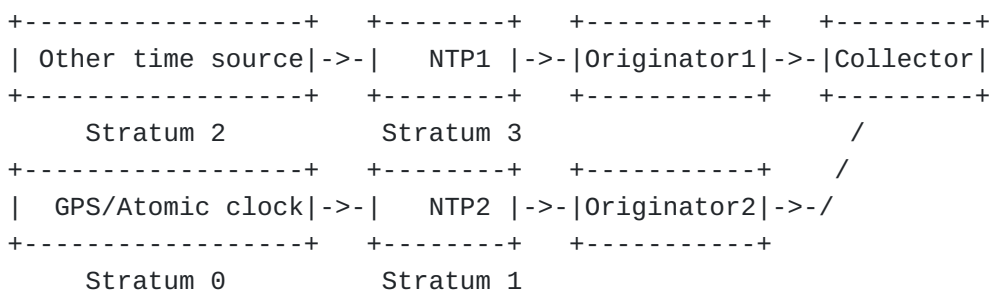

Figure 4: Untrusted Scenarios for Log Reporting Time

4. IANA Considerations

This requires registering a new parameter with IANA. This parameter is the same as the "isSynced" parameter and should be an optional parameter.

5. Contributors

TBD

6. Acknowledgements

TBD

7. Normative References

[RFC5424] Gerhards, R., "The Syslog Protocol", RFC 5424, DOI 10.17487/RFC5424, March 2009, <https://www.rfc-editor.org/info/rfc5424>.

Authors' Addresses

Fengsheng Wang
China Mobile
32, Xuanwumen West
BeiJing 100053
China

Email: wangfengsheng@chinamobile.com

Meiling Chen
China Mobile
32, Xuanwumen West
BeiJing 100053
China

Email: chenmeiling@chinamobile.com

Li Su
China Mobile
32, Xuanwumen West
BeiJing 100053
China

Email: suli@chinamobile.com