

Workgroup: Network Working Group
Internet-Draft:
draft-coene-rserpool-applic-ipfix-20
Published: 26 March 2023

Intended Status: Informational

Expires: 27 September 2023

Authors: T. Dreibholz L. Coene
 SimulaMet Nokia Siemens Networks
 P. Conrad
 University of Delaware

Reliable Server Pooling Applicability for IP Flow Information Exchange

Abstract

This document describes the applicability of the Reliable Server Pooling architecture to the IP Flow Information Exchange using the Aggregate Server Access Protocol (ASAP) functionality of RSerPool only. Data exchange in IPFIX between the router and the data collector can be provided by a limited retransmission protocol.

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 27 September 2023.

Copyright Notice

Copyright (c) 2023 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](#)
 - [1.1. Scope](#)
 - [1.2. Terminology](#)
- [2. IPFIX using RSerPool](#)
 - [2.1. Architecture](#)
- [3. Transport protocols suitable for IPFIX](#)
- [4. Security considerations](#)
- [5. Reference Implementation](#)
- [6. Testbed Platform](#)
- [7. Security Considerations](#)
- [8. IANA Considerations](#)
- [9. Acknowledgments](#)
- [10. References](#)
 - [10.1. Normative References](#)
 - [10.2. Informative References](#)
- [Authors' Addresses](#)

1. Introduction

Reliable Server Pooling provides protocols for providing highly available services. The services are located in a pool of redundant servers and if a server fails, another server will take over. The only requirement put on these servers belonging to the pool is that if state is maintained by the server, this state must be transferred to the other server taking over.

The goal is to provide server-based redundancy. Transport and network level redundancy are handled by the transport and network layer protocols.

The application may choose to distribute its traffic over the servers of the pool conforming to a certain policy.

The application wishing to make use of RSerPool protocols may use different transport layers (such as UDP, TCP and SCTP). However, some transport layers may have restrictions built in the way they might be operating in the RSerPool architecture and its protocols.

1.1. Scope

The scope of this document is to explain the way that a minimal version of Reliable Server Pooling protocols have to be used in order to provide a highly available service towards IP Flow Information Exchange (IPFIX) protocols.

1.2. Terminology

The terms are commonly identified in related work and can be found in the Aggregate Server Access Protocol and Endpoint Handlespace Redundancy Protocol Common Parameters document [7]

2. IPFIX using RSerPool

2.1. Architecture

IP flow information is exchanged between observation points and collector points. The observation points may try to find out via the Aggregate Server Access Protocol (ASAP, see [5]) which collector point(s) are active. Both the observation and the collector point may have limitations for exchanging the information (observation point may have limited buffer space and collectors points may be overburdened with receiving lots of flow information from different observation points).

The observation point will query the ENRP server for resolution of a particular collector pool name and the ENRP server will return a list of one or more collector points to the observation point.

The observation point will use its own transport protocols (TCP, UDP, SCTP, SCTP with PR-SCTP extension) for exchanging the IPFIX data between the observation point and the collector point. If a collector point would fail, then the observation point will send its data towards a different collector point, belonging to the same collector pool.

Collector points will announce themselves to the ENRP server and will be monitored for their availability. The observation point will only query the ENRP server for server pool name resolution.

3. Transport protocols suitable for IPFIX

The exchange of IP flow information data between an observation point and a collection point consists of massive amounts of data.

One collection point can service many observation points, therefore transport protocols must do congestion control (example: modifying the receive buffer space, thus reducing the incoming flow of data), so that the collection point is not overburdened by its observation points. Some data must arrive at the collector while other data might arrive (if it gets lost: no problem). The choice of reliable or partial reliable delivery has to be made by the observation point. These requirements demand a protocol which provides variable transport reliability of its data: it should be able to choose the reliability by the IPFIX protocols on a per-message base.

SCTP [3] with PR-SCTP extension [2] is the only known protocol which allows the choice of full, partial or unreliable delivery of the message to its peer node. TCP will only allow fully reliable delivery, while UDP only provides unreliable delivery and NO congestion control.

4. Security considerations

The protocols used in the Reliable Server Pooling architecture only try to increase the availability of the servers in the network. RSerPool protocols do not contain any protocol mechanisms which are directly related to user message authentication, integrity and confidentiality functions. For such features, it depends on the IPSEC protocols or on Transport Layer Security (TLS) protocols for its own security and on the architecture and/or security features of its user protocols.

The RSerPool architecture allows the use of different transport protocols for its application and control data exchange. These transport protocols may have mechanisms for reducing the risk of blind denial-of-service attacks and/or masquerade attacks. If such measures are required by the applications, then it is advised to check the SCTP applicability statement [RFC2057](#) [1] for guidance on this issue.

5. Reference Implementation

The RSerPool reference implementation RSPLIB can be found at [15]. It supports the functionalities defined by [4], [5], [6], [7] and [9] as well as the options [10], [12] and [11]. An introduction to this implementation is provided in [13].

6. Testbed Platform

A large-scale and realistic Internet testbed platform with support for the multi-homing feature of the underlying SCTP protocol is NorNet. A description of NorNet is provided in [14], some further information can be found on the project website [16].

7. Security Considerations

Security considerations for RSerPool systems are described by [8].

8. IANA Considerations

This document introduces no additional considerations for IANA.

9. Acknowledgments

The authors wish to thank Maureen Stillman and many others for their invaluable comments.

10. References

10.1. Normative References

- [1] Coene, L., "Stream Control Transmission Protocol Applicability Statement", RFC 3257, DOI 10.17487/RFC3257, April 2002, <<https://www.rfc-editor.org/info/rfc3257>>.
- [2] Stewart, R., Ramalho, M., Xie, Q., Tuexen, M., and P. Conrad, "Stream Control Transmission Protocol (SCTP) Partial Reliability Extension", RFC 3758, DOI 10.17487/RFC3758, May 2004, <<https://www.rfc-editor.org/info/rfc3758>>.
- [3] Stewart, R., Ed., "Stream Control Transmission Protocol", RFC 4960, DOI 10.17487/RFC4960, September 2007, <<https://www.rfc-editor.org/info/rfc4960>>.
- [4] Lei, P., Ong, L., Tuexen, M., and T. Dreibholz, "An Overview of Reliable Server Pooling Protocols", RFC 5351, DOI 10.17487/RFC5351, September 2008, <<https://www.rfc-editor.org/info/rfc5351>>.
- [5] Stewart, R., Xie, Q., Stillman, M., and M. Tuexen, "Aggregate Server Access Protocol (ASAP)", RFC 5352, DOI 10.17487/RFC5352, September 2008, <<https://www.rfc-editor.org/info/rfc5352>>.
- [6] Xie, Q., Stewart, R., Stillman, M., Tuexen, M., and A. Silverton, "Endpoint Handlespace Redundancy Protocol (ENRP)", RFC 5353, DOI 10.17487/RFC5353, September 2008, <<https://www.rfc-editor.org/info/rfc5353>>.
- [7] Stewart, R., Xie, Q., Stillman, M., and M. Tuexen, "Aggregate Server Access Protocol (ASAP) and Endpoint Handlespace Redundancy Protocol (ENRP) Parameters", RFC 5354, DOI 10.17487/RFC5354, September 2008, <<https://www.rfc-editor.org/info/rfc5354>>.
- [8] Stillman, M., Ed., Gopal, R., Guttman, E., Sengodan, S., and M. Holdrege, "Threats Introduced by Reliable Server Pooling (RSerPool) and Requirements for Security in Response to Threats", RFC 5355, DOI 10.17487/RFC5355, September 2008, <<https://www.rfc-editor.org/info/rfc5355>>.

- [9] Dreibholz, T. and M. Tuexen, "Reliable Server Pooling Policies", RFC 5356, DOI 10.17487/RFC5356, September 2008, <<https://www.rfc-editor.org/info/rfc5356>>.
- [10] Dreibholz, T., "Handle Resolution Option for ASAP", Work in Progress, Internet-Draft, draft-dreibholz-rserpool-asap-hropt-31, 17 September 2022, <<https://datatracker.ietf.org/doc/html/draft-dreibholz-rserpool-asap-hropt-31>>.
- [11] Dreibholz, T. and X. Zhou, "Definition of a Delay Measurement Infrastructure and Delay-Sensitive Least-Used Policy for Reliable Server Pooling", Work in Progress, Internet-Draft, draft-dreibholz-rserpool-delay-30, 17 September 2022, <<https://datatracker.ietf.org/doc/html/draft-dreibholz-rserpool-delay-30>>.
- [12] Dreibholz, T. and X. Zhou, "Takeover Suggestion Flag for the ENRP Handle Update Message", Work in Progress, Internet-Draft, draft-dreibholz-rserpool-enrp-takeover-28, 17 September 2022, <<https://datatracker.ietf.org/doc/html/draft-dreibholz-rserpool-enrp-takeover-28>>.

10.2. Informative References

- [13] Dreibholz, T., "Reliable Server Pooling - Evaluation, Optimization and Extension of a Novel IETF Architecture", 7 March 2007, <https://duepublico.uni-duisburg-essen.de/servlets/DerivateServlet/Derivate-16326/Dre2006_final.pdf>.
- [14] Dreibholz, T. and E. G. Gran, "Design and Implementation of the NorNet Core Research Testbed for Multi-Homed Systems", Proceedings of the 3rd International Workshop on Protocols and Applications with Multi-Homing Support (PAMS) Pages 1094-1100, ISBN 978-0-7695-4952-1, DOI 10.1109/WAINA.2013.71, 27 March 2013, <<https://www.simula.no/file/threfereedinproceedingsreference2012-12-207643198512pdf/download>>.
- [15] Dreibholz, T., "Thomas Dreibholz's RSerPool Page", 2022, <<https://www.nntb.no/~dreibh/rserpool/>>.
- [16] Dreibholz, T., "NorNet - A Real-World, Large-Scale Multi-Homing Testbed", 2022, <<https://www.nntb.no/>>.

Authors' Addresses

Thomas Dreibholz
Simula Metropolitan Centre for Digital Engineering
Pilestredet 52
0167 Oslo
Norway

Email: dreibh@simula.no
URI: <https://www.simula.no/people/dreibh>

Lode Coene
Nokia Siemens Networks
Atealaan 32
2200 Herentals
Belgium

Phone: [+32-14-252081](tel:+32-14-252081)
Email: lode.coene@nsn.com

Phillip Conrad
University of Delaware
103 Smith Hall
Newark, DE 19716
United States of America

Phone: [+1-302-831-8622](tel:+1-302-831-8622)
Email: conrad@acm.org