Reliable Server Pooling (RSerPool) Bakeoff Scoring
draft-dreibholz-rserpool-score-04.txt

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), 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 July 11, 2009.

Copyright Notice

Copyright (c) 2009 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.

Abstract

This memo describes some of the scoring to be used in the testing of
Internet-Draft          RSerPool Bakeoff Scoring            January 2009

Reliable Server Pooling protocols ASAP and ENRP at upcoming bakeoffs.

Table of Contents

1. Introduction ............................................. 3
   2.1. Pool Element Communication .......................... 3
   2.2. Pool User Communication ............................. 4
   2.3. ENRP Server Communication ........................... 4
3. Endpoint Handlespace Redundancy Protocol .................. 5
   3.1. Peer Management .................................... 5
   3.2. Update ............................................. 6
   3.3. Synchronization ..................................... 6
   3.4. Takeover ........................................... 7
4. Bonus Points .............................................. 7
5. Reference Implementation ................................... 7
6. Security Considerations ................................... 8
7. IANA Considerations ....................................... 8
8. References ................................................ 8
   8.1. Normative References ................................. 8
   8.2. Informative References ............................... 9
Authors’ Addresses .......................................... 9
1. Introduction

This document will be used as a basis for point scoring at upcoming RSerPool bakeoffs. Its purpose is similar to that described in RFC1025. It is hoped that a clear definition of where and how to score points will further the development of RSerPool.

Note that while attending a bakeoff no one else will score your points for you. We trust that all implementations will faithfully record their points that are received honestly. Note also that these scores are NOT to be used for marketing purposes. They are for the use of the implementations to know how well they are doing. The only reporting that will be done is a basic summary to the Reliable Server Pooling Working Group but please note that NO company or implementation names will be attached.

2. Aggregate Server Access Protocol

The ASAP protocol is described in the following documents:

- [RFC5352]
- [RFC5354]
- [I-D.dreibholz-rserpool-asap-hropt]
- [I-D.dreibholz-rserpool-delay]

2.1. Pool Element Communication

These points will be scored for EACH peer implementation that you successfully communicate with.

- 2 Successful ASAP Registration Request of a PE in a pool using Round Robin policy and handling of ASAP Registration Response.
- 2 Failing ASAP Registration Request of a PE requesting Least Used policy in a pool using Round Robin policy and appropriate handling of ASAP Registration Response (e.g. printing error message, but not retrying registration).
- 2 Successful re-registration of a PE in a pool using Round Robin policy.
- 2 Successful ASAP Deregistration Request of the PE from its pool and handling of ASAP Deregistration Response.
2.2. Pool User Communication

These points will be scored for EACH peer implementation that you successfully communicate with.

- 5 Successful ASAP Handle Resolution in a pool using Round Robin policy, correct handling of ASAP Handle Resolution Response.
- 2 Successful failure reporting using ASAP Endpoint Unreachable.
- 5 Successful connection to and handle resolution at ENRP server announcing itself via multicast ASAP Announces.
- 1 Successful handle resolution in a pool using Least Used policy.
- 1 Successful handle resolution in a pool using Weighted Round Robin policy.
- 1 Successful handle resolution in a pool using Random policy.
- 1 Successful handle resolution in a pool using Weighted Random policy.

2.3. ENRP Server Communication

These points will be scored for EACH peer implementation that you successfully communicate with.
o 2 Successful handling of an ASAP Registration Request into a pool using Round Robin policy (ENRP server answers with successful ASAP Registration Response).

o 2 Rejecting registration of a PE requesting Round Robin policy into a pool using Least Used policy.

o 5 Rejecting registration of a PE with all addresses *not* being part of the ASAP association.

o 5 Successful registration of a PE with some addresses *not* being part of the ASAP association. The invalid addresses may *not* go into the handlespace.

o 5 Successful handling of ASAP Endpoint Unreachable messages. The ENRP server must remove the given PE after MAX-BAD-PE-REPORTS=3 unreachability reports.

o 2 Sending regular ASAP Endpoint Keep-Alive to its PEs.

o 2 Removing PE not answering to ASAP Endpoint Keep-Alive.

3. Endpoint Handlespace Redundancy Protocol

The ENRP protocol is described in the following documents:

o [RFC5353]

o [RFC5354]

o [I-D.dreibholz-rserpool-enrp-takeover]

3.1. Peer Management

These points will be scored for EACH peer implementation that you successfully communicate with.

o 2 Sending ENRP Presence to a new ENRP server.

o 2 Sending ENRP Presences in the interval given by PEER-HEARTBEAT-CYCLE.

o 5 Requesting peer list from new ENRP server using ENRP Peer List Request, handling ENRP Peer List Response and adding entries to its own peer list.
o 2 Handling ENRP Peer List Request and replying with own peer list in ENRP Peer List Response.

o 5 Requesting handlespace from new ENRP server using ENRP Handle Table Request, handling ENRP Handle Table Response (without M-bit set) and inserting entries into its own handlespace copy.

o 5 Requesting handlespace from new ENRP server using ENRP Handle Table Request, handling ENRP Handle Table Response with M-bit set, requesting more entries and inserting entries into its own handlespace copy.

o 2 Handling ENRP Handle Table Request and replying own handlespace in ENRP Handle Table Response (without M-bit).

o 10 Handling ENRP Handle Table Request and replying own handlespace in ENRP Handle Table Response with M-bit set, remembering point to continue from, responding next block of handlespace entries upon following ENRP Handle Table Request, etc. until transfer of handlespace data is complete.

o 5 Successful addition of new ENRP server announcing itself via multicast ENRP Presence (including association establishment as well as download of peer list and handlespace).

3.2. Update

These points will be scored for EACH peer implementation that you successfully communicate with.

o 2 Handling an ENRP Handle Update adding a PE.

o 2 Handling an ENRP Handle Update updating a PE. The changes must be entered into the local handlespace copy.

o 2 Handling an ENRP Handle Update removing a PE.

3.3. Synchronization

These points will be scored for EACH peer implementation that you successfully communicate with.

o 5 Successful detection of different handlespace checksums upon reception of ENRP Presence (due to additional PE), request of Handle Table with W-bit set, integration of missing PE into local handlespace copy and reporting the correct checksum in own ENRP Presence.
5. Successful detection of different handlespace checksums upon reception of ENRP Presence (due to out-of-date PE), request of Handle Table with W-bit set, removal of PE from local handlespace copy and reporting the correct checksum in own ENRP Presence.

10. Successful detection of different handlespace checksums upon reception of ENRP Presence (due to multiple new and out-of-date PE identities; size of PE identities is larger than maximum ENRP message size), request of Handle Table with W-bit set, handling of ENRP Handle Table Responses with M-bit set, removal of out-of-date PEs, integration of new PEs into the local handlespace copy and reporting correct checksum in own ENRP Presence.

3.4. Takeover

These points will be scored for EACH peer implementation that you successfully communicate with. The setup contains your ENRP server plus a set of peers running another implementation.

- 5 Successfully detecting the failure of a remote peer and initiating a takeover procedure.
- 5 Acknowledging another peer’s takeover and aborting own takeover procedure.
- 10 Correctly handling a remote peer’s Takeover Server message, including ownership change for the remote peer’s PEs.
- 10 Successfully taking over a dead peer, including ownership change and informing the PEs taken over.

4. Bonus Points

You can also earn Bonus Points:

- 20 points for the ENRP server handling the largest number of PEs.
- 20 points for the ENRP server achieving the highest handle resolution throughput for a pool containing 100 (should this be larger?) PEs.

Please note that the whole period of the bakeoff is relevant.

5. Reference Implementation

The RSerPool reference implementation RSPLIB can be found at
It supports the functionalities defined by [RFC5351], [RFC5352], [RFC5353], [RFC5354] and [RFC5356] as well as the options [I-D.dreibholz-rserpool-asap-hropt], [I-D.dreibholz-rserpool-enrp-takeover] and [I-D.dreibholz-rserpool-delay]. An introduction to this implementation is provided in [Dre2006].

6. Security Considerations

This document does only describe test scenarios and therefore does not introduce any new security issues.

For security considerations of the RSerPool protocols see [RFC3237], [RFC5351], [RFC5352], [RFC5353], [RFC5354]. [RFC5356] and in particular [RFC5355].

7. IANA Considerations

This document introduces no additional considerations for IANA.

8. References

8.1. Normative References


8.2. Informative References


Authors’ Addresses

Thomas Dreibholz
University of Duisburg-Essen, Institute for Experimental Mathematics
Ellernstrasse 29
45326 Essen, Nordrhein-Westfalen
Germany

Phone: +49-201-1837637
Fax: +49-201-1837673
Email: dreibh@iem.uni-due.de
URI: http://www.iem.uni-due.de/~dreibh/

Michael Tuexen
University of Applied Sciences Muenster
Stegerwaldstrasse 39
48565 Steinfurt, Nordrhein-Westfalen
Germany

Email: tuexen@fh-muenster.de