Redis Enterprise Software Release Notes 5.2 (June 2018)

Redis Enterprise Software (RS) 5.2 is now available. Key features include new data types and Causal Consistency for active-active (also known as the Redis CRDT or CRDB Conflict-free Replicated Database), as well as enhanced security features.

Overview

If you are upgrading from a previous version, make sure to review the upgrade instructions before beginning the upgrade process. You can upgrade to RS 5.2 from RS 4.5 and above. If you have a version older than 4.5, you should first upgrade to version 5.0 (or at least 4.5).

New features

Active-Active Redis (CRDB) supports sorted sets and lists

RS 5.2 adds active-active Redis (CRDB) support for Sorted Sets and Lists. Now all major Redis data types are supported with CRDT, so you can use Redis Enterprise in an active-active manner for all your Redis use cases, with seamless conflict resolution. Click here for more information about how to develop applications with geo-replicated CRDBs.

Causal consistency in Active-Active Redis (CRDB)

Causal Consistency in active-active Redis (CRDB) guarantees that the order of operations on a specific key will be maintained across all CRDB instances. For instance, if operations A and B were applied on the same key, and B was performed after the effect of A was observed by the CRDB instance that initiated B, then all CRDB instances would observe the effect of A before observing the effect of B.

This way, any causal relationship between operations on the same key is also observed and maintained by every replica. Such capability is important for various applications, e.g. social network status updates or chat applications (assuring that the chronology of messages doesn’t get mixed up). For more information, click here.

Enhanced security features

- Admin action audit trail

Management actions performed with Redis Software are audited in order to fulfill two major objectives: (1) make sure that system management tasks are appropriately performed and/or monitored by the Administrator(s), and (2) facilitate compliance with regulatory standards such as HIPAA, SOC2, PCI, etc.

In order to fulfill both objectives, audit records contain the following information: (1) who performed the action, (2) what exactly was the performed action, (3) when the action was performed, and (4) whether the action succeeded.

To get the list of audit records/events, one can use the REST API or the Log page in the UI; the Log page displays the system and user events regarding alerts, notifications and configurations.

- Ability to disable TLS versions

Version 5.2 introduces the option to set the minimum TLS version that can be used for encrypting the various flows. You can do so using the REST API or the following radmin commands:

- For the management UI and the REST API:
For the data path encryption:

```
rladmin> cluster config min_data_TLS_version [version, e.g. 1.2]
```

Note that communications that use older TLS versions will not be allowed.

**HTTPS enforcement**

With this feature, you can restrict REST API access to only those using HTTPS. In order to do so, use the REST API or the following radmin command:

```
rladmin> cluster config http_support [disabled | enabled]
```

**Additional capabilities**

- Support for Redis version 4.0.9
- Fixes for Redis important security issues related to the Lua scripting engine

**Information**

- The end-of-service-life (EOSL) for Redis Enterprise Software 4.4.X is June 30th, 2018, in accordance with our published policy. We recommend that customers running version 4.4 or below upgrade to the latest version.

**Important fixes**

- RS19755 - Added the ability to enforce HTTPS communication when accessing REST API
- RS19571 - Fixed RHEL installation when FIPS mode is enabled
- RS19490 - Fixed a failure while upgrading from 4.5 to 5.0.2
- RS19475 - Added the ability to disable TLS versions for the control and data paths
- RS18712 - Fixed a failure in endpoint failover
- RS17208 - Added an option to disable Redis commands via Rest API
- RS14973 - Updated NGINX.conf template to turn off exposing the server version
- RS11181 - Set file permissions of log files, redis-conf files, rdb files and their rotations to “640”

**Known limitations**

- After creating Redis Enterprise CRDBs which “Require SSL for CRDB communication only,” one can set definitions via Rest API to activate “Require SSL for All Communication” without providing a certificate. In such case, connections to the cluster will be blocked.

**Updated:** July 12, 2021