Redis Enterprise Software Release Notes 6.2.10 (February 2022)

Redis Enterprise Software version 6.2.10 is now available!

The following table shows the MD5 checksums for the available packages.

<table>
<thead>
<tr>
<th>Package</th>
<th>MD5 Checksum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ubuntu 16</td>
<td>b8697811177f99c3e9e51e0d9d788634</td>
</tr>
<tr>
<td>Ubuntu 18</td>
<td>411e86daa5478b9a761ec68904bcbb</td>
</tr>
<tr>
<td>RedHat Enterprise Linux (RHEL) 7</td>
<td>84f35f3f3c9cf23c5bfb91da1048513</td>
</tr>
<tr>
<td>Oracle Enterprise Linux (OL) 7</td>
<td></td>
</tr>
<tr>
<td>RedHat Enterprise Linux (RHEL) 8</td>
<td>db0fdb208a1bc45dae783258c6d79152</td>
</tr>
<tr>
<td>Oracle Enterprise Linux (OL) 8</td>
<td></td>
</tr>
<tr>
<td>K8s Ubuntu</td>
<td>099192416a70a12790535bdcd78a6e87</td>
</tr>
<tr>
<td>K8s RHEL</td>
<td>f267abe81770ddf36f022232f4c2cb2e</td>
</tr>
</tbody>
</table>

Features and enhancements

- Upgrade the Redis Enterprise infrastructure to Python v3.9.
- Red Hat Enterprise Linux (RHEL) v8.5 is now a supported platform.
- Compatibility with open source Redis 6.2.5.
- Compatibility with the security fixes of the latest open source Redis 6.2.6.
- Enhancements and bug fixes.

Version changes

Prerequisites and notes

- You can upgrade to v6.2.10 from Redis Enterprise Software v6.0 and later.
- Refer to v6.2.4 release notes for important notes regarding changes made to the upgrade.
- Upgrades from versions earlier than v6.0 are not supported.
- If you are using Active-Active or Active-Passive (ReplicaOf) databases and experience synchronization issues as a result of the upgrade, see RS67434 details in Resolved issues for help resolving the problem.

Product lifecycle updates

Redis Enterprise Software v6.0.x will reach end of life (EOF) on May 31, 2022.

To learn more, see the Redis Enterprise Software product lifecycle, which details the release number and the end-of-life schedule for Redis Enterprise Software.
Redis modules

Redis Enterprise Software v6.2.10 includes the following Redis modules:

- RediSearch v2.2.6
- RedisJSON v2.0.6
- RedisBloom v2.2.9
- RedisGraph v2.4.12
- RedisTimeSeries v1.4.13

Starting with Redis Enterprise Software v6.2.10 build 121, the included modules versions are:

- RediSearch v2.4.6
- RedisJSON v2.0.8
- RedisBloom v2.2.14
- RedisGraph v2.8.12
- RedisTimeSeries v1.6.9

For help upgrading a module, see Add a module to a cluster.

Interface enhancements

- When choosing RedisJSON, the user interface (UI) now suggests RediSearch as well. To learn more, see the RedisJSON preview announcement, which details the benefits of combining RedisJSON and RediSearch.
- Adds the ability to sort the columns of the node list (RS48256).
- When creating a new geo-distributed (Active-Active) database, an endpoint port is no longer required. The system assigns one if none if provided (RS27632).

Additional enhancements

- Added an option to run a connectivity health check for the management layer of Active-Active databases. Run the following REST API command:

  GET https://[host][:port]/v1/crdbs/<crdb_guid>/health_report

- Added TLS handshake error messages to the DMC proxy log (RS59346).

Resolved issues

- RS58219 - Fixes a UI error message that showed a path instead of a relevant error message.
- RS44958 - Fixes incorrect description for the graph “incoming traffic” in Active-Active (geo-distributed) database UI Metrics.
- RS66280 - Fixes the lexicographic SORT command on Active-Active databases (e.g. SORT mylist ALPHA). The SORT
command should only run on keys mapped to the same slot.

- RS64575 - Fixes a bug in the replication between primary and replica shards of a destination Active-active database in the scenario of using Replica-Of from a single to an Active-Active database, where the syncer process went down during the full sync.

- RS65370 - Adds logic to remove old syncer entries in the cluster configuration during upgrades.

- RS67434 - Version 6.2.10 fixes the mTLS handshake between the syncer process and the proxy (DMC), where the proxy presented a leaf certificate without its full chain to the syncer. After upgrading to 6.2.10, syncer connections using invalid certificates will break the synchronization between Active-Active instances or deployments using Replica Of when TLS is enabled. To ensure certificates are valid before upgrading do the following:

  - For Active-Active databases, run the following command from one of the clusters:
    
    ```bash
    crdb-cli crdb update --crdb-guid <CRDB-GUID> --force
    ```

  - For Active-Passive (Replica Of) databases: use the admin console to verify that the destination syncer has the correct certificate for the source proxy (DMC). For details, see Configure TLS for Replica Of.

Issues resolved in build 96

- RS67133 - An issue in Redis Enterprise Software affected replication in replica databases using RedisGraph, RediSearch, and RedisGears in specific scenarios. The problem appeared when importing an RDB file or while synchronizing target Active-Passive (ReplicaOf) databases.

  This issue is fixed in Redis Enterprise Software v6.2.10-96 and RedisGraph v2.8.11. We recommend upgrading to these versions at your earliest opportunity. (Failure to upgrade can lead to data loss.)

  Once the upgrades are complete, secondary shards might need to be restarted. You can use `rlutil` to restart secondary shards:

  ```bash
  rlutil redis_restart redis=<shard-id1>,<shard-id2>,...
  ```

Issues resolved in build 100

- RS74171 - A new command was added as part of Redis 6.2: XAUTOCLAIM. When used in an Active-Active configuration, this command may cause Redis shards to crash, potentially resulting in data loss. The issue is fixed in Redis Enterprise Software version 6.2.12. Additionally, we recommend enabling AOF persistence for all Active-Active configurations.

Issues resolved in build 121

- RS68668, RS72082 - Improvements for internode encryption certification rotation

- RS72304 - Avoid starting a master shard when both master and replica shards crash and the replica did not finish recovery

- RS74469 - Fix for some Redis Active-Active + Redis Streams scenarios that could lead to shard crash during backup; failure to backup```

Security

Open Source Redis Security fixes compatibility

As part of Redis commitment to security, Redis Enterprise Software implements the latest security fixes available with open source Redis. The following Open Source Redis CVE’s do not affect Redis Enterprise:
- **CVE-2021-32625** - Redis Enterprise is not impacted by the CVE that was found and fixed in open source Redis since Redis Enterprise does not implement LCS. Additional information about the open source Redis fix is on the Redis GitHub page (Redis 6.2.4, Redis 6.0.14)

- **CVE-2021-32672** - Redis Enterprise is not impacted by the CVE that was found and fixed in open source Redis because the LUA debugger is unsupported in Redis Enterprise. Additional information about the open source Redis fix is on the Redis GitHub page (Redis 6.2.6, Redis 6.0.16)

- **CVE-2021-32675** - Redis Enterprise is not impacted by the CVE that was found and fixed in open source Redis because the proxy in Redis Enterprise does not forward unauthenticated requests. Additional information about the open source Redis fix is on the Redis GitHub page (Redis 6.2.6, Redis 6.0.16)

- **CVE-2021-32762** - Redis Enterprise is not impacted by the CVE that was found and fixed in open source Redis because the memory allocator used in Redis Enterprise is not vulnerable. Additional information about the open source Redis fix is on the Redis GitHub page (Redis 6.2.6, Redis 6.0.16)

- **CVE-2021-41099** - Redis Enterprise is not impacted by the CVE that was found and fixed in open source Redis because the proto-max-bulk-len CONFIG is blocked in Redis Enterprise. Additional information about the open source Redis fix is on the Redis GitHub page (Redis 6.2.6, Redis 6.0.16)security fixes for recent CVE’s. Redis Enterprise has already included the fixes for the relevant CVE’s. Some CVE’s announced for Open Source Redis do not affect Redis Enterprise due to different and additional functionality available in Redis Enterprise that is not available in Open Source Redis.

**Updated:** May 24, 2022