Redis Enterprise Software Release Notes 6.0.20 (April 2021)

Redis Enterprise Software version 6.0.20 is now available! This version includes the following new features and improvements:

- A new integration for LDAP authentication and authorization into RS role-based access controls (RBAC). You can now use LDAP to authorize access to the admin console and to authorize database access.

- An enhanced clients mutual authentication mechanism, adding the ability to authenticate client connections using a Certificate Authority (CA).

- Support of Redis eviction policies on Active-Active Redis databases.

- A new migration process for Active-Active Redis database using the Active-Passive (Replica Of) mechanism.

- Support for the BITFIELD data type on Active-Active Redis databases.

And other functional and stability improvements.

Version information

Upgrade instructions

- Follow these instructions for upgrading to Redis Software 6.0.20 from Redis Software 5.6.0 and above.

- Note that upgrades from earlier Redis Software versions are not supported.

- For Active-Active deployments, this release requires that you upgrade the CRDB featureset version.

- Upgrades of Active-Active databases to Redis Software 6.0.20, will require all their instances to run with protocol version 1 and featureset version 1 or above. Active-Active databases running on protocol version 0 and/or featureset version 0 will block the upgrade.

Product lifecycle information

- End of Life (EOL) for Redis Enterprise Software 6.0 and earlier versions, can be found here.

- EOL for Redis modules can be found here.

Deprecation Notice

- Upgrades to the next Redis Software will be enabled from version 6.0 and above.

- Support for the SASL-based LDAP mechanism is considered deprecated, it will be removed in a future version.

- Starting with Redis Software version 6.0.12, Envoy replaces Nginx for internal cluster administration. Support for Nginx is considered deprecated, it will be removed in a future version.

New Features

New LDAP integration
Redis Enterprise Software integrates Lightweight Directory Access Protocol (LDAP) authentication and authorization into its [role-based access controls] (RBAC). You can now use LDAP to authorize access to the admin console and to authorize database access.

**Clients Mutual TLS authentication using a Certificate Authority (CA)**
Redis Enterprise Software adds the ability to use a Certificate Authority (CA) for client authentications, allowing clients to rotate their certificates without the need to load new certificates to your database.

**Redis eviction policies on Active-Active Redis databases**
All Redis eviction policies are now supported on Active-Active Redis databases. You can create new Active-Active databases or edit existing ones using the UI console to enable it.

- Note that eviction is not supported yet for Active-Active Redis databases running with Redis on Flash (Rof).

**Migration to an Active-Active Redis database**
Redis Enterprise Software adds the ability to easily migrate your Redis database to an Active-Active Redis database using the Active-Passive (Replica Of) mechanism.

**BITFIELD on Active-Active Redis databases**
Redis Enterprise Software adds the ability to use the BITFIELD data type on Active-Active Redis databases. Please read more about developing for Active-Active with BITFIELD to understand the conflict resolution and limitations.

**Redis modules**
The following GA releases of Redis modules are bundled with Redis Software 6.0.20: (Please read the below updates for 6.0.20-97)

- RedisSearch, version 2.0.6
- RedisJSON, version 1.0.7
- RedisGraph, version 2.2.14
- RedisTimeSeries, version 1.4.8
- RedisBloom, version 2.2.4

To use the updated modules with a database, you must upgrade the module on the database.

**Additional capabilities**

- Redis Software 6.0.20 includes open source Redis 6.0.9. For more information about Redis 6.0.9, check out the release notes.
- Redis Software 6.0.20 adds new rladmin commands for setting Ciphers suites and minimal TLS version for:
  - Control plane: setting Envoy
  - Data plane: setting the Proxy for clients connections
  - Sentinel discovery service
- Starting with Redis Software 6.0.20, new clusters will be set with minimal TLS version v1.2
All known bugs around setting ciphers were fixed. To learn more, see Updating certificates.

- Starting with Redis Software 6.0.20, the syncer process was improved to automatically recover and resume synchronisation after reaching out-of-memory.

- Envoy updated and verified with multiple security headers.

- Starting with Redis Software 6.0.20:
  - The replication backlog size of new databases is allocated dynamically according to shard size.
  - The Active-Active replication backlog size of new Active-Active databases is allocated dynamically according to shard size.

**Important fixes**

- RS50905, RS54809, 54940 - Fix in Redis preventing missing process PID
- RS53639 - Fix to avoid stuck state machine when assigning incorrect Redis ACL with the allkeys alias or -* and also with ~<somekey>
- RS47983 - Fixed dependencies with installation using custom directories
- RS54382 - Fixed missing API documentation
- RS52433, RS53417, RS42195, RS42194, RS30526, RS46821, RS48928 - Fixed security headers for Envoy

**Starting 6.0.20-69**

- RS55504 - Fixed issue that caused RediSearch cursor to break.

**Starting 6.0.20-97**

- RS57659 - Fixed force removing an Active-Active instance which is hosted on an inaccessible cluster
- RS57315 - Fixed creation and editing of an Active-Active database with LDAP users of the new RBAC LDAP integration. This applies to UI access and REST API and does not apply to LDAP users for database access via Redis Clients
- RS57073 - Fixed a bug caused in the shard migration process which could leave unattended shards on the node
- RS56508 - Fixed backwards compatibility of client certificate when upgrading from earlier versions and using a certificate chain with Extended Key Usage extension being set to "TLS Web Server Authentication" instead of "TLS Web Client Authentication"
- RS49289 - Fixed updating the log rotation config file according to the custom config path that was set during the installation
- The bundled RedisGraph module was upgraded to v2.4.6
- The bundled RedisTimeSeries module was upgraded to v1.4.9
- The bundled RediSearch module was upgraded to v2.0.8

**Known limitations**

- RS59983 - Clients may get disconnected by the proxy when one client sends an UNSUBSCRIBE command without being subscribed to any channel and disconnect before the response returns back from the server (from the proxy).
• RS60068 - The pdns might not resolve the master node after master node change. Restarting the pdns service is required in this case.

• RS61114 - Active-Active synchronization will fail in the following scenario: a new syncer connection is established AND a partial sync (psync) was initiated AND a cron job runs before the first ACK of the psync was received.

• RS55504 - Bug RS6.0.20-66 (Build #66) causes RediSearch cursor to break. Please upgrade to a higher build when running with RediSearch.

Upgrade

• Redis Software 5.4.2 introduced new Active-Active Redis Database capabilities that improve its compatibility with open source Redis. Now the string data-type in Active-Active Redis Database is implicitly and dynamically typed, just like open source Redis. To use the new capabilities on nodes that are upgraded from version RS 5.4.2 or lower, you must upgrade the Active-Active Redis Database protocol.

• When you upgrade an Active-Active Redis with active AOF from Redis Software 5.4.2 or earlier to version Redis Software 5.4.4 or later:
  • If replication is enabled, you must run the BGREWRITEAOF command on all replica shards after the upgrade.
  • If replication is not enabled, you must run the BGREWRITEAOF command on all shards after the upgrade.
  • Node upgrade fails if the SSL certificates were configured in version 5.0.2 or above by manually updating the certificates on the disk instead of updating them through the API. For help with this issue, contact Support.
  • Starting from Redis Software 5.4.2, to preserve the current Redis major.minor version during database upgrade you must use the keep_redis_version option instead of keep_current_version.

Redis commands

• The capability of disabling specific Redis commands does not work on commands specific to Redis modules.

• CLIENT UNBLOCK command is not supported in RS 5.4 and above

• Starting from RS 5.4.2 and after upgrading the CRDB, TYPE commands for string data-type in CRDBs return "string" (OSS Redis standard).

Security

• As part of Redis commitment to security, the following Open Source Redis CVE's have been addressed in Redis Enterprise 6.0.20:
  • CVE-2021-32626 - Lua scripts can overflow the heap-based Lua stack. This has been addressed in Redis Enterprise 6.0.20-62
  • CVE-2021-32627 - Integer overflow issue with Streams. This has been addressed in Redis Enterprise 6.0.20-1
  • CVE-2021-32628 - Vulnerability in handling large ziplists. This has been addressed in Redis Enterprise 6.0.20-1
  • CVE-2021-32687 - Integer overflow issue with intsets. This has been addressed in Redis Enterprise 6.0.20-89

• 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)

Updated: March 11, 2022