Redis Enterprise Software Release Notes 6.2.4 (August 2021)

Redis Enterprise Software version 6.2.4 is now available!

This version offers:

- Encryption of all communications within cluster nodes
- Security enhancements
- Bug fixes
- Compatibility with the latest version of open source Redis 6.2.3

Version changes

Prerequisites and notes

You can upgrade to v6.2.4 from Redis Enterprise Software v6.0 and later.

Keep the following in mind:

- Upgrades from versions earlier than v6.0 are not supported
- The new internode encryption feature requires port 3342 to be open on all machines in the cluster.
- In v6.0.20, Redis Enterprise Software replaced Nginx with envoy to improve internal security and communication. As of v6.2.4, Nginx is no longer provided with Redis Enterprise Software.

Database upgrade default changes

The default behavior of the upgrade db command has changed. It is now controlled by a new cluster policy (redis_upgrade_policy), which defines the policy for creating new databases and upgrading existing databases. The policy supports the following values:

- When set to major, the policy allows databases to be created or updated to versions of Redis compatible with open source Redis major releases. This allows for longer upgrade cycles by supporting Redis versions across multiple Redis Enterprise Software releases.
  
  This is the default value for Redis Enterprise Software.

- When set to latest, the policy creates new databases and upgrades existing ones to be compatible with the latest (most recent) version of open source Redis, which was the default behavior of earlier versions of Redis Enterprise Software. This is no longer the default behavior.

  Setting the upgrade policy to latest ensures that the most recent Redis features are available to new databases and ones that are upgraded. It also requires more frequent upgrades, as open source Redis is updated more frequently than Redis Enterprise Software.

The Redis Enterprise Software 6.2.4 package includes compatibility with the most recent major Redis release (v6.0) and the latest (most recent) update to Redis (v6.2.3).

By default, compatibility with v6.0 will be installed. To change this, use rladmin to set the upgrade policy and the default Redis
version:

```
tune cluster redis_upgrade_policy latest
tune cluster default_redis_version 6.2
```

To learn more, see the upgrade instructions.

**Product lifecycle updates**

Redis Enterprise Software v5.6.0 will reach end of life (EOF) on October 31, 2021.

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 Enterprise modules have individual release numbers and lifecycles.

**Deprecation notices**

- In v6.0.20, the SASL-based LDAP mechanism was deprecated in favor of a new RBAC-based approach. As of v.6.2.4, support for the older mechanism has been removed.
  
  For help migrating to the LDAP-based mechanism, see Migrate to role-based LDAP.

- OpenStack Object Storage (“Swift”) has reached end-of-life. Consequently, you can no longer use ObjectStack Swift as a target for database backup or export operations.

**Features and enhancements**

**Internode encryption**

Internode encryption (INE) encrypts all communication between nodes in a cluster; it is available for the control plane and the data plane.

**Control plane internode encryption**

Control plane internode encryption encrypts all management communication within a cluster. It is enabled by default for all new clusters and upgraded clusters.

**Data plane internode encryption**

Data plane internode encryption encrypts communication between nodes within a cluster, such as database replication between nodes.

Data plane internode encryption is available for new or fully upgraded clusters. It is not enabled by default.

You can enable data plane internode encryption by:

- Setting the cluster policy to enable data plane internode encryption by default for new databases
  
  `rladmin tune cluster data_internode_encryption enabled`

- Enabling it for individual existing databases
  
  `rladmin tune db <db:id | name> data_internode_encryption enabled`
Internal certificate management

Internode encryption relies on internal certificates signed by a unique, private CA certificate created for your deployment. The private CA generates and signs leaf certificates for internode encryption only. It’s generated when you install or upgrade to Redis Enterprise 6.2.4. It’s used only within the cluster and is not exposed outside of the cluster.

The leaf certificates expire regularly; they’re automatically rotated before expiration and alerts are issued as needed.

Open source Redis compatibility

Redis 6.2 introduced new commands, feature improvements, and security fixes; it addresses many customer requests.

Redis Enterprise Software supports all new commands, except RESET and FAILOVER. (Redis Enterprise takes a different approach to connectivity; it also separates control plane operations from data plane operations.)

To learn more, see Redis Enterprise Software compatibility with open source.

Redis modules

Redis Enterprise Software v6.2.4 includes the following Redis modules:

- RediSearch v2.0.11
- RedisJSON v1.0.8
- RedisBloom v2.2.6
- RedisGraph v2.4.7
- RedisTimeSeries v1.4.10

Internode encryption for modules

To utilize data plane encryption for existing databases with modules, update the module to the latest version prior to enabling data plane encryption.

For help, see Upgrade the module for a database.

Module-related enhancements

Added the capability to update current module arguments for an existing database. In earlier versions, you could do this only when upgrading a module. To learn more, see radmin upgrade.

Resolved issues

- RS39954 - Changed the UI status indication for the default user from Active/Inactive to Enabled/Disabled
- RS42626 - Increased the max length for modules commands from 23 characters to 64 characters
- RS54732 - Fixed incorrect reporting of number database connections, which caused the number of connections to be reported as a 20 digit number
- RS52265 - Fixed excessive log lines reporting when an Active-Active database is on featureset 0. We recommend upgrading the featureset version to the latest
- RS56122 - Fixed a bug that was causing AOF files to grow when the replicas of two Active-Active databases became disconnected during full synchronization
- RS58184 - Fixed a bug when trying to create an Active-Active database with expired syncer certificates; participating clusters were creating replicas even though the create operation failed.
RS48988 - Add the username description in the log upon an unauthorized REST API request

Known issues

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.

Security

- 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-2021-32765 - 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-2021-41099 - 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: April 7, 2022