Security

Security is an important part of any production system. This section describes the security features and settings available in Redis Enterprise.

Architecture security

When deploying Redis Enterprise Software to production, we recommend the following practices:

- **Deploy Redis Enterprise inside a trusted network**: Redis Enterprise is database software and should be deployed on a trusted network not accessible to the public internet. Deploying Redis Enterprise in a trusted network reduces the likelihood that someone can obtain unauthorized access to your data or the ability to manage your database configuration.

- **Implement anti-virus exclusions**: To ensure that anti-virus solutions that scan files or intercept processes to protect memory do not interfere with Redis Enterprise software, customers should ensure that anti-virus exclusions are implemented across all nodes in their Redis Enterprise cluster in a consistent policy. This helps ensure that anti-virus software does not impact the availability of your Redis Enterprise cluster.

If you are replacing your existing antivirus solution or installing/supporting Redis Enterprise, make sure that the below paths are excluded:

<table>
<thead>
<tr>
<th>Path</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/opt/redislabs</td>
<td>Main installation directory for all Redis Enterprise Software binaries</td>
</tr>
<tr>
<td>/opt/redislabs/bin</td>
<td>Binaries for all the utilities for command line access and</td>
</tr>
<tr>
<td></td>
<td>management such as “rladmin” or “redis-cli”</td>
</tr>
<tr>
<td>/opt/redislabs/config</td>
<td>System configuration files</td>
</tr>
<tr>
<td>/opt/redislabs/lib</td>
<td>System library files</td>
</tr>
<tr>
<td>/opt/redislabs/sbin</td>
<td>System binaries for tweaking provisioning</td>
</tr>
</tbody>
</table>

- **Send logs to a remote logging server**: Redis Enterprise is configured to send logs by default to syslog. To send these logs to a remote logging server you must configure syslog based on the requirements of the remote logging server vendor. Remote logging helps ensure that the logs are not deleted so that you can rotate the logs so that your server disk does not fill up.

- **Deploy clusters with an odd number of 3 or more nodes** - Redis is an available and partition tolerant database. We recommend that Redis Enterprise be deployed in a cluster of an odd number of 3 or more nodes so that you are able to successfully failover in the event of a failure.

- **Reboot nodes in a sequence rather that all at once**: Customers will frequently maintain reboot schedules. There are cases, however, where our customers have rebooted too many servers at once, causing a quorum failure and resulting in loss of availability of the database. We recommend that rebooting be done in a phased manner so that quorum is not lost. For example, to maintain quorum in a 3 node cluster, at least 2 nodes must be up at all times. Only one server should be rebooted at any given time to maintain quorum.

- **Implement client-side encryption**: Client-side encryption, or the practice of encrypting data within an application before storing it in a database, such as Redis, is the most widely adopted method to achieve encryption in memory. Redis is an in-memory database and stores data in-memory. If you require encryption in memory, better known as encryption in use,
then client side encryption may be the right solution for you. Please be aware that when implementing solutions using client-side encryption database functions that need to operate on data — such as simple searching functions, comparisons, and incremental operations — don’t work with client-side encryption.

**Database Security**

Redis Enterprise offers several database security controls to help protect your data against unauthorized access and to improve the operational security of your database. The following section details configurable security controls available for implementation.

- **Implement role-based access for users**: With role-based access control (RBAC), you can manage ACLs for the entire cluster. You can reuse ACL templates across users, accounts, and multiple databases to precisely scale complex security configurations with a few simple clicks. RBAC lets you set permissions for your databases and for the Redis Enterprise management console itself, providing a complete security-management solution for your cluster.

- **Prevent database users from logging into the admin console**: Redis Enterprise allows users to be provisioned with both control plane access and access to the database. In some scenarios this may be helpful for administrative users, but for applications we recommend that you disable their access to the control plane.

- **Use strong Redis passwords**: A frequent recommendation in the security industry is to use strong passwords to authenticate users. This helps to prevent brute force password guessing attacks against your database. It’s important to check that your password aligns with your organization’s security policy.

- **Disable the default user**: Redis Enterprise comes with a “default” user for backwards compatibility with applications designed with versions of Redis prior to Redis Enterprise 6. The default user is turned on by default. This allows you to access the database without specifying a username and only using a shared secret. For applications designed to use access control lists, we recommend that you disable the default user.

- **Enable client certificate authentication**: To prevent unauthorized access to your data, Redis Enterprise databases support the TLS protocol, which includes authentication and encryption. Client certificate authentication can be used to ensure only authorized hosts can access the database.

- **Install trusted certificates**: Redis implements self-signed certificates for the database proxy and replication service, but many organizations prefer to use their own certificates.

- **Configure Transport Layer Security (TLS)**: Similar to the control plane, you can also configure TLS protocols to help support your security and compliance needs.

- **Configure and verify database backups**: Implementing a disaster recovery strategy is an important part of data security. Redis Enterprise supports database backups to many destinations.

**LDAP authentication**

If your organization uses the Lightweight Directory Access Protocol (LDAP), we recommend enabling Redis Software support for role-based LDAP authentication.

**Updated**: April 15, 2022