Add a Redis database

Before using any of the tools to work with your database, you must first add the database so RedisInsight can connect to it.

Each of these database configurations requires specific steps to add them to RedisInsight:

- Standalone Redis
- Redis cluster
- Redis Sentinel
- Redis with TLS authentication
- Elasticache

Note: Currently, RedisInsight supports Redis versions 4 and newer.

Add a standalone Redis database

This is the simplest setup of a Redis database with just a single Redis server.

To add a standalone Redis database to RedisInsight:

1. When you open RedisInsight, click Add Redis Database.

2. Select Add Database.

3. Enter the details for your database:
- **Host**: The hostname of your Redis database, for example `redis.acme.com`. If your Redis server is running on your local machine, you can enter either `127.0.0.1` or `localhost`. You can also paste a Connection URL. When pasted, the database details are automatically filled.

  The following Connection URLs are supported:
  - `redis://[[user]:[pass]]@host:port`
  - `rediss://[[user]:[pass]]@host:port`
  - `host:port`

- **Port**: The port your Redis database is available on. The default port for Redis is 6379.

- **Name**: A name for your Redis database. It does not have to match the name of the database in the Redis cluster.

- **Username**: The username, if your database is ACL enabled, otherwise leave this field empty. (If you plan to share RedisInsight across multiple users within the same project, you can enforce reentry of database usernames and passwords. For more information, see [Authenticate database users](#)).

- **Password**: The password, if any, for your Redis database. If your database doesn't require a password, leave this field empty.

- **Use TLS**: If your Redis database uses TLS to connect with clients, select this option.

After you enter the details for your database, click **Add Redis Database** to add the database to RedisInsight.

Your newly added database is shown in the home screen.
Add a Redis cluster database

To add a Redis Cluster database:

1. Follow steps 1 - 2 in the Add a Standalone Redis Database section above.
2. Enter the host, port and other details of your Redis Cluster database and click Add Redis Database.
3. Select the “seed nodes” of the cluster and click Add Redis Database.

For Redis cluster databases, a set of “seed nodes” or “startup nodes” are provided to clients. To make sure that RedisInsight has the same view of the cluster as your application, select the same seed nodes that your application or any other client uses to connect to this Redis database. If you don’t know which node to select or if there are no other clients for the database yet, select all of the nodes.

Add a Redis Sentinel database

Redis Sentinel is often used for High Availability deployments of Redis. It provides automatic master-to-replica failover. When you use Sentinel, clients connect to the Sentinel instance to get the current topology of the databases. The client then connects to the current master. If the connection fails, the client queries the Sentinel instance again to find the current master.

In this configuration, RedisInsight can connect to your database through the Sentinel instance. Then if a failover happens, RedisInsight changes the database connection just like any other client.

To add a Redis database with a Redis Sentinel configuration:

1. When you open RedisInsight, click Add Redis Database.
2. Select **Add Database**.

3. Enter the host, port and other details of your Redis Sentinel instance and click **Add Redis Database**.

4. Select the database to add.

A single set of Sentinel instances can monitor and manage the failover of multiple databases. If your database requires a password, enter the password and click **Add Selected Database**.

**Add a Redis database that uses TLS**

Some configurations of Redis use SSL/TLS for network communication.

To add a TLS-enabled Redis database:

1. When you open RedisInsight, click **Add Redis Database**.
2. Select **Add Database**.

3. Enter the host, port and username (if your database is ACL enabled), password (if any) of your database.

4. Select **Use TLS**.

5. If the server needs to be authenticated, pass a **CA Certificate**.

   1. If the certificate returned by the server needs to be verified, select **Verify TLS Certificate**.
If your database requires TLS client authentication to do mutual authentication:

1. **Select Requires TLS Client Authentication.**

Some implementations of Redis, such as Redis Enterprise, support **TLS Mutual Authentication** so that the Redis server also verifies the identity of the client.

1. **Provide the client certificate and private key to RedisInsight.**

- If you already have a certificate-key pair in RedisInsight, select it from the **Client Certificate** list.
- If you do not, create a certificate-key pair:
1. Select **Add New Certificate**.
2. Enter a name for your client certificate.
3. Enter the text of the TLS certificate and private key in the next two fields.

7. Click **Add Redis Database** to add your database.

**Connecting to ElastiCache**

ElastiCache Redis caches cannot be accessed from outside the VPC, as they don't have public IP addresses assigned to them.

If you want to work with ElastiCache Redis caches with RedisInsight, you can:

- If you are not using Redis Cluster, **set up an SSH Tunnel** between RedisInsight and your ElastiCache instance.

  1. To create an SSH tunnel, run:

     ```bash
     ssh -f -N -L <local_port>:<elasticache_endpoint> -i <path_to_pem_file> <ec2_endpoint>
     ```

  2. Go to **Add Instance** in RedisInsight and add an instance with:

     - host - `<localhost>`
     - port - `<local_port>`
     - name - `<your_instance_name>`

     **Install RedisInsight on an EC2 instance** that is in the same VPC and has access to the ElastiCache Redis cache.

     This option gives the best performance and works with Redis Cluster.

     **Set up a VPN to your AWS VPC using AWS VPN.**

     You can then access the ElastiCache Redis cache using the private endpoint.

---

**Updated:** May 24, 2022