User password rotation

Redis Enterprise Software lets you implement password rotation policies using its API.

You can add a new password for a database user without immediately invalidating the old one (which might cause authentication errors in production).

Note: Password rotation does not work for the default user. Add additional users to enable password rotation.

For user access to the Redis Enterprise Software admin console, you can set a password expiration policy to prompt the user to change their password. However, for database connections that rely on password authentication, you need to allow for authentication with the existing password while you roll out the new password to your systems.

With the Redis Enterprise Software REST API, you can add additional passwords to a user account for authentication to the database or the admin console and API. After the old password is replaced in the database connections, just delete the old password to finish the password rotation process.

Warning: Multiple passwords are only supported using the REST API. If you reset the password for a user in the admin console, the new password replaces all other passwords for that user.

The new password cannot already exist as a password for the user and must meet the password complexity requirements, if enabled.

Rotating the password of a user account

To rotate the password of a user account:

1. Add an additional password to a user account with this POST command:

   
   ```bash
   curl -k -v -X POST -H "content-type: application/json" -u "<administrator_user>:<password>" -d '{"username":"<username>", "old_password":"<an_existing_password>", "new_password":"<a_new_password>"}' https://<RS_server_address>:9443/v1/users/password
   
   After you run this command, you can authenticate with both the old and the new password.
   ```

2. Update the password in all database connections that connect with the user account.

3. Delete the original password with this DELETE command:

   ```bash
   curl -k -v -X DELETE -H "content-type: application/json" -u "<administrator_user>:<password>" -d '{"username":"<username>", "old_password":"<an_existing_password>"}' https://<RS_server_address>:9443/v1/users/password
   
   If there is only one valid password for a user account, you cannot delete that password.
   ```

Replacing all existing passwords with a single password

You can also replace all existing passwords for a user account with a single password that is not an existing password. This can be helpful if you suspect that your passwords are compromised and you want to quickly resecure the account.

To replace all existing passwords for a user account with a single new password, use this PUT command:
curl -k -v -X PUT -H "content-type: application/json" -u "<administrator_user>:<password>" -d '{"username":"<username>", "old_password":"<an_existing_password>", "new_password":"<a_new_password>"}' https://<RS_server_address>:9443/v1/users/password

All of the existing passwords are deleted and only the new password is valid.

Note: If you run the above command without -X PUT, the new password is added to the list of existing passwords.

Updated: May 12, 2021