Authentication and authorization

You can configure users and roles for the admin console. This section details how you can set users and roles, configure external identity providers for authentication, and set up user account security within Redis Enterprise Software.

Role-based access control

Redis Enterprise Software includes five pre-built roles to help users who need limited access to the admin console.

1. **DB Viewer** - Read any settings for databases
2. **DB Member** - Administer databases
3. **Cluster Viewer** - Read any cluster settings
4. **Cluster Member** - Administrator the cluster
5. **Admin** - Full cluster access

The following table elaborates on the privileges for each of these roles:

<table>
<thead>
<tr>
<th>Database</th>
<th>Nodes</th>
<th>Cluster</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>View metrics</td>
<td>View config</td>
</tr>
<tr>
<td>DB Viewer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DB Member</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cluster Viewer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cluster Member</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Admin</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Configuring users with roles

To add a user to the cluster:

1. Go to the access control tab
2. Select +
3. Enter the name, email and password of the new user and select the role to assign to the user.
4. Select the internal user type
5. For email alerts, select “Edit” and then choose the alerts that the user should receive. You can select:
   - Receive alerts for databases - The alerts that are enabled for the selected databases will be sent to the user. You can either select “All databases”, or you can select “Customize” and select the individual databases to send alerts for.
   - Receive cluster alerts - The alerts that are enabled for the cluster in settings > alerts are sent to the user.
6. Select the save icon.
User Account Security

Redis Enterprise supports the following user account security settings:

1. Password complexity
2. Password expiration
3. User Lockouts
4. Account inactivity timeout

To enforce a more advanced password policy, we recommend using LDAP integration with an external identity provider, such as Active Directory.

Enabling the password complexity profile

Redis Enterprise Software provides an optional password complexity profile that meets most organizational needs. When enabled, this password profile requires the following:

- At least 8 characters
- At least one uppercase character
- At least one lowercase character
- At least one number (not first or last character)
- At least one special character (not first or last character)

In addition, the password:

- Cannot contain the user ID or reverse of the user ID
- Cannot have more than three repeating characters

Note: The password complexity profile applies when a new user is added or an existing user changes their password. This profile does not apply to users authenticated through an external identity provider.

To enable the password complexity profile, run the following curl command against the REST API:

```
```

To disable the password complexity requirement, run the same command, but set "password_complexity" to "false".

Enabling password expiration

To enforce an expiration of a user’s password after a specified number of days, run the following command:

```
```
To disable password expiration, set the number of days to 0.

**User Login Lockout**

The parameters for the user login lockout are:

- **Login Lockout Threshold** - The number of failed login attempts allowed before the user account is locked. (Default: 5)
- **Login Lockout Counter Reset** - The amount of time during which failed login attempts are counted. (Default: 15 minutes)
- **Login Lockout Duration** - The amount of time that the user account is locked after excessive failed login attempts. (Default: 30 minutes)

By default, after 5 failed login attempts within 15 minutes, the user account is locked for 30 minutes.

You can view the user login restrictions for your cluster with:

```
rladmin info cluster | grep login_lockout
```

**Change the login lockout threshold**

You can set the login lockout threshold with the command:

```
rladmin tune cluster login_lockout_threshold <login_lockout_threshold>
```

For example, to set the lockout threshold to 10 failed login attempts.

```
rladmin tune cluster login_lockout_threshold 10
```

Setting the lockout threshold to 0 disables account lockout. In this case, the cluster settings show: login_lockout_threshold: disabled

**Change the login lockout counter**

You can set the login lockout reset counter in seconds with the command:

```
rladmin tune cluster login_lockout_counter_reset_after <login_lockout_counter_reset_after>
```

To set the lockout reset to 1 hour, run:

```
rladmin tune cluster login_lockout_counter_reset_after 3600
```

**Change the login lockout duration**

You can set the login lockout duration in seconds with the command:

```
rladmin tune cluster login_lockout_duration <login_lockout_duration>
```

For example, to set the lockout duration to 1 hour use the command:

```
rladmin tune cluster login_lockout_duration 3600
```

If you set the lockout duration to 0, then the account can be unlocked only when an administrator changes the account’s password. In this case, the cluster settings show: login_lockout_duration: admin-release
Unlock locked user accounts

To unlock a user account or reset a user password from the CLI, run:

```
rladmin cluster reset_password <user email>
```

To unlock a user account or reset a user password from the REST API, run:

```
curl -k -X PUT -v -H "cache-control: no-cache"
-H "content-type: application/json"
-u "<administrator_user>:<password>"
-d '{"password": "<new_password>"}'
https://<RS_server_address>:9443/v1/users/<uid>
```

Session timeout

The Redis Enterprise admin console supports session timeouts. By default, users are automatically logged out after 15 minutes of inactivity.

To customize the session timeout you can run the following command:

```
rladmin cluster config cm_session_timeout_minutes <number_of_min>
```

Here, `number_of_min` is the number of minutes after which sessions will time out.

Update Active-Active cluster admin credentials

Active-Active databases use administrator credentials to manage operations for Active-Active database. To update the administrator user password on a cluster with Active-Active databases:

1. From the user management page, update the administrator user password on the clusters you wish to update.
2. For each participating cluster and each Active-Active database, update the admin user credentials to match the changes in Step 1.

Warning - Do not perform any management operation on the databases until these steps are complete.

LDAP integration

As of version 6.0.20, 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.

To learn more, including how to set up LDAP or to migrate an existing LDAP integration to the new mechanism, see LDAP authentication.

Updated: April 11, 2022