Logging and Audit Events

Management actions performed with Redis Enterprise are audited in order to fulfill two major objectives:

1. To make sure that system management tasks are appropriately performed and/or monitored by the Administrators
2. To facilitate compliance with regulatory standards

In order to fulfill both objectives, the audit records contain the following information:

1. Who performed the action?
2. What exactly was the performed action?
3. When was the action performed?
4. Did the action succeed or not?

To get the list of audit records/events, you can use the REST API or the Log page in the UI. The Log page displays the system and user events regarding alerts, notifications and configurations.

If you need to look at the audit log of what a user on the cluster has done, e.g. edited a DB configuration, this is where you could look.

- Redis slow log
- rsyslog logging

Viewing logs in the admin console

Redis Enterprise provides log files for auditing and troubleshooting. You can see these logs in the admin console and on the host operating system.
To view the audit logs:

1. Log in to the Redis Enterprise Software admin console.
2. Go to the Log tab.
3. Review logs directly in the UI, or export them to CSV using the export button.

Viewing logs on the server

Server logs can be found by default in the directory `/var/opt/redislabs/log/`.

These log files are used by the Redis support team to troubleshoot issues. The logs you will most frequently interact with is `event_log.log`. This log file is where logs of configuration actions within Redis are stored and is useful to determine events that occur within Redis Enterprise.

Setting log timestamps

Redis Enterprise allows you to configure log timestamps. To configure log timestamps:

1. In Settings > General navigate to the timezone section.
2. Select the timezone for the logs based on your location.

Updated: March 11, 2022