Audit using Service Log

Service logs collect and report actions performed on various entities in your Redis Enterprise Cloud subscription. These entities include the account itself, users, API Keys, subscriptions, databases, accounts, payment methods, and more. For each entity, various lifecycle events are logged in the system log.

You can view the system service log in the Redis Enterprise Cloud admin console by selecting Service log from the console menu. This displays recent service log entries for the current account.

### Service Log

<table>
<thead>
<tr>
<th>Time</th>
<th>Originator</th>
<th>Resource</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/21/2020 14:25:12</td>
<td>System</td>
<td>Subscription</td>
<td>Subscription #1318651 created - Essentials/AWS/us-east-1b/Standard/Pay-As-You-Go...</td>
<td></td>
</tr>
<tr>
<td>12/21/2020 14:25:09</td>
<td>Noah Lessie (noah.l...</td>
<td>Subscription</td>
<td>Subscription #1318651 created - Essentials/AWS/us-east-1b/Standard/Pay-As-You-Go...</td>
<td></td>
</tr>
<tr>
<td>12/21/2020 12:56:51</td>
<td>Noah Lessie (noah.l...</td>
<td>Account</td>
<td>MFA enforcement has been disabled</td>
<td></td>
</tr>
<tr>
<td>12/21/2020 12:54:13</td>
<td>Noah Lessie (noah.l...</td>
<td>Account</td>
<td>MFA enforcement has been enabled</td>
<td></td>
</tr>
<tr>
<td>12/20/2020 11:42:35</td>
<td>Noah Lessie (noah.l...</td>
<td>Configuration</td>
<td>Zone Mapping completed</td>
<td></td>
</tr>
<tr>
<td>12/17/2020 18:08:22</td>
<td>Noah Lessie (noah.l...</td>
<td>Account</td>
<td>Password reset</td>
<td></td>
</tr>
<tr>
<td>12/16/2020 23:06:25</td>
<td>Noah Lessie (noah.l... noah</td>
<td>Configuration</td>
<td>Backup disabled</td>
<td></td>
</tr>
</tbody>
</table>

### System service log API

The API operation for querying the system service log is GET /logs.

For example, the following request returns the latest 100 system log entries, in descending order:

```
curl -X GET "https://$HOST/logs?limit=100&offset=0" \
-H "accept: application/json" \
-H "x-api-key: $ACCOUNT_KEY" \
-H "x-api-secret-key: $SECRET_KEY"
```

The /logs API operation accepts the following parameters:

- **offset** - The starting point for the results. The default value of 0 starts with the latest log entry. A value of 11 skips the first 10 entries and retrieves entries starting with the 11 and older.

- **limit** - The maximum number of entries to return per request. The default value is 100.

The system log reports activity for the entire account. It reports log entries for all types of entities, including subscriptions, databases, and so on.

### Request results

An API system log request results in data that includes an entries array. The entries are sorted by system log entry ID in
descending order and include the following properties:

- **id** - A unique identifier for each system log entry.

- **time** - The system log entry timestamp, defined in ISO-8601 date format and in the UTC timezone (for example: `2019-03-15T14:26:02Z`).

- **originator** - The name of the user who performed the action described by the system log entry.

- **apiKeyName** - The name of the API key used to perform the action described by the system log entry. This field only appears if the action was performed through the API. If the operation was performed through the Redis Enterprise Cloud admin console, this property is omitted.

- **resource** - The name of the entity associated with the logged action (for example, database name). This property is omitted if it is not applicable to the specific log entry.

- **type** - The category associated with the action log entry.

- **description** - The detailed description of the action in the log entry.

*Updated: August 10, 2021*