Contents

Tooling to fetch Audit Log Entries via API

About

This article shall describe my personal best-practice to fetch audit data via API and a CLI tool 'go-c8y-cli': https://goc8ycli.netlify.app/

The tool

Go-c8y-cli is a CLI tool built to efficiently work with the Cumulocity API. It is available for windows- and unix-based Operating systems. Additionally it is availabe in a docker image: ghcr.io/reubenmiller/c8y-shell.

Please find a nice introduction: https://goc8ycli.netlify.app/docs/introduction/

Run container and connect to your tenant

1) Create a session.env file with the following contents:

```
C8Y_HOST=https://example.cumulocity.com
C8Y_TENANT=t12345
C8Y_USER=my@user.com
C8Y_PASSWORD=secretpass
```

2) Run the docker container using the session file: `docker run --rm -it --env-file=session.env ghcr.io/reubenmiller/c8y-shell`

3) Sample request to test your connection: `c8y inventory list`. A list of (five) Inventory objects should be shown in a table view.

Audit Log Parametrization

The call to fetch auditlog entries is `c8y auditrecords list`, it can be parametrized with multiple parameters, e.g.:

- `--application "xyz"`: Show only auditrecords for a certain applicaton
- `--dateFrom "2022-02-15"`: Show only auditrecords from a certain date ongoing. Note that it supports relative times, e.g. "-3h" are the auditrecords of past 3 hours
- `--dateTo "2022-02-16"`: The equivalent of dateFrom but for the upper border of the date. Also supports relative times.
- `--type "User"`: Show only audit records of a certain type
- `--user "kb@sag.com"`: Show only audit records triggered by a certain user

Additionally, the output format can be specified via the `--output` parameter. The following output is supported: * `--output csv`: CSV Output without header fields * `--output csvHeader`: CSV Output including header fields * `--output json`: JSON output * `--outpuut table`: Ascii table output

Please find all parameters described in the tools API description here:

https://goc8ycli.netlify.app/docs/cli/c8y/auditrecords/c8y_auditrecords_list/

Audit Log Examples

Please find some samples that might be use cases.

Show all audit log entries of the past three hours

Show them in json

```
1 $ c8y auditrecords list --dateFrom "-3h" --includeAll | jq
```

Show them in CSV

```
1 $ c8y auditrecords list --dateFrom "-3h" --includeAll --output csv
```

Show them in CSV and output to a file

```
1 $ c8y auditrecords list --dateFrom "-3h" --includeAll --output csv >
    output.csv
```

Show all auditrecords with a certain keyword

show all Entries with 'Engine Percent load' of past 3 hours as json

```
$ c8y auditrecords list --dateFrom "-3h" --includeAll | jq -c | grep "
    Engine Percent Load" | jq
```

show all Entries with 'Engine Percent load' of past 3 hours as csv and output to file

```
$ c8y auditrecords list --dateFrom "-3h" --includeAll --output
    csvHeader > output.csv
```

Others

Show all audit records from a User related to Alarms

```
$ c8y auditrecords list --user Korbinian.Butz@softwareag.com --type
    Alarm --includeAll | jq
```

Show all audit records from a User done in cockpit done in the past 1.5 years and dump to file

```
$c8y auditrecords list --user Korbinian.Butz@softwareag.com --
    application cockpit --dateFrom "-1y6m" --includeAll | jq > output.
    csv
```