LogLens - Log Analysis and Monitoring Tool

Ibrahim Nanitalwala, Rahil Vaghasia, Ramisa Zaman, Vincenzo Langone

LogLens is a command-line tool designed to parse, analyze, and generate reports from log files. It supports various filtering options, generates statistical summaries, and provides error alerts based on specified thresholds.

Features

- Parse and filter log files by date range, severity level, or regex pattern.
- Generate reports in TXT or CSV format.
- Produce statistical summaries of log data.
- Generate alerts for error rates exceeding a specified threshold.

Installation

Clone the repository or download manually:

```
git clone https://github.com/nakk0/loglens
```

Usage

Enter the `dist/<your operating system>` folder and run LogLens using the following syntax in your preferred terminal:

Linux/Mac:

```
./loglens <log_file> [options]
```

Windows:

```
.\loglens.exe “<log_file>” [options]
```

Extra Info:

Paired with the program, each installation contains an `example-log.txt` to help the user test/get familiar with the commands and syntax

Expected Inputs/Outputs

The following are the arguments you can input in the above commands

- `-f [txt|csv]`, `--format`: Output format (`txt` or `csv`). Default is `txt`.
- `-o [file_path]`, `--output`: Path to the output file. If not specified, results are printed to `stdout`.
- `-d [start_date]:[end_date]`, `--date-range`: Filter logs by date range. Format: `YYYY-MM-DD:YYYY-MM-DD`.
- `-s [severity_level]`, `--severity`: Filter logs by severity (`INFO`, `WARNING`, `ERROR`, or `CRITICAL`).
- `-p [regex]`, `--pattern`: Filter logs using a regex pattern.
- `--stats`: Generate and display statistical summaries.
- `--alerts [threshold]`: Generate alerts if the error rate exceeds a specified threshold (provide a float value).

*note, arguments must still be provided when using the long form --[word] commands in place of the -[letter] ones

Examples

Analyze a log file and generate a report in CSV format:

Linux/Mac:
```
./loglens <log_file> -f csv -o report.csv
```
Windows:
```
.\loglens “<log_file>” -f csv -o report.csv
```

Filter logs by severity level and display statistics:

Linux/Mac:
```
./loglens <log_file> -s ERROR --stats
```
Windows:
```
.\loglens “<log_file>” -s ERROR --stats
```

Generate alerts for error rates exceeding 0.2 (20%):

Linux/Mac:
```
./loglens <log_file> --alerts 0.2
```
Windows:
```
.\loglens “<log_file>” --alerts 0.2
```

Troubleshooting

This program is designed to be a lightweight executable to be run from your console or terminal and to be provided a log file to analyze and instructions on what analysis to apply. Any attempt to run the program outside these circumstances (aka. double-clicking on the executable or executing commands without a log file or arguments) will fail and raise errors.

Possible syntax mistakes you may make:

- **Invalid Date Format Error:** Ensure dates are in the correct `YYYY-MM-DD` format.
- **Invalid Regex Pattern:** Check for syntax errors in the regex pattern used for filtering. Test the regex with a validator.
- **Unsupported Report Format:** Only `txt` and `csv` formats are supported.
- **Missing or Corrupted Log Data:** Ensure logs are properly formatted with `[timestamp] SEVERITY - Source: Message` fields.
- **File Not Found Error:** Ensure the correct log file path is provided and the file exists.