

Инструкция к приложению ELKLogReader

Запуск

- 1) [скачайте доккер](#)
- 2) запустите его (возможно он попросит доустановить wsl2, в таком случае там будет ссылка на инструкцию)
- 3) если у вас настроен доккер под windows контейнеры, кликните правой кнопкой мыши по значку докера и нажмите “перейти на линукс контейнеры” (рисунок 1)

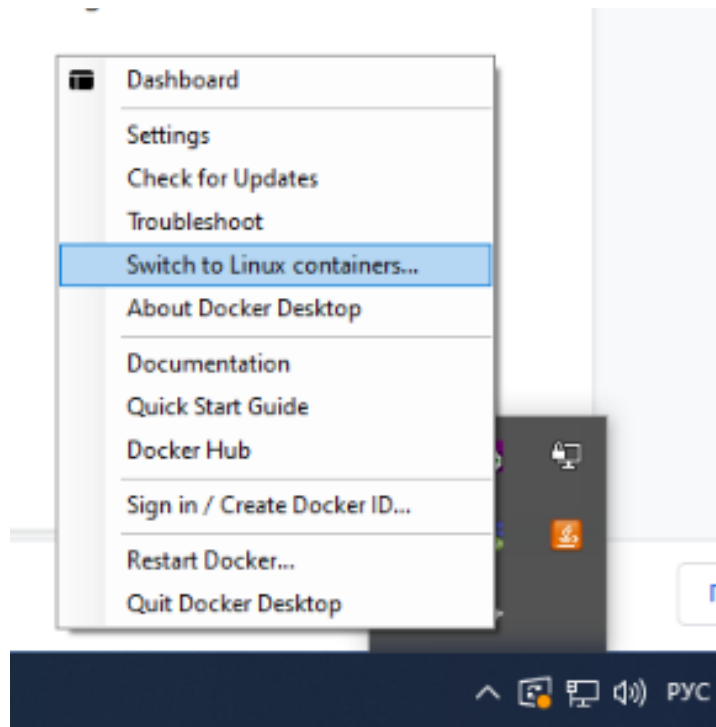


рисунок 1 - switch to linux containers

- 4) перейдите в папку где будет располагаться программа и выполните следующие команды в консоли
 - а) `git clone https://github.com/AVTarasov2000/ELKLogReader.git`
 - б) `cd ELKLogReader`
 - в) `docker build -t logreader:latest .`
 - г) `docker compose up`
- 5) если не запускается контейнер logreader, откройте boot.sh в notepad++ и поменяйте формат переноса строки на unix LF(рисунок 2)

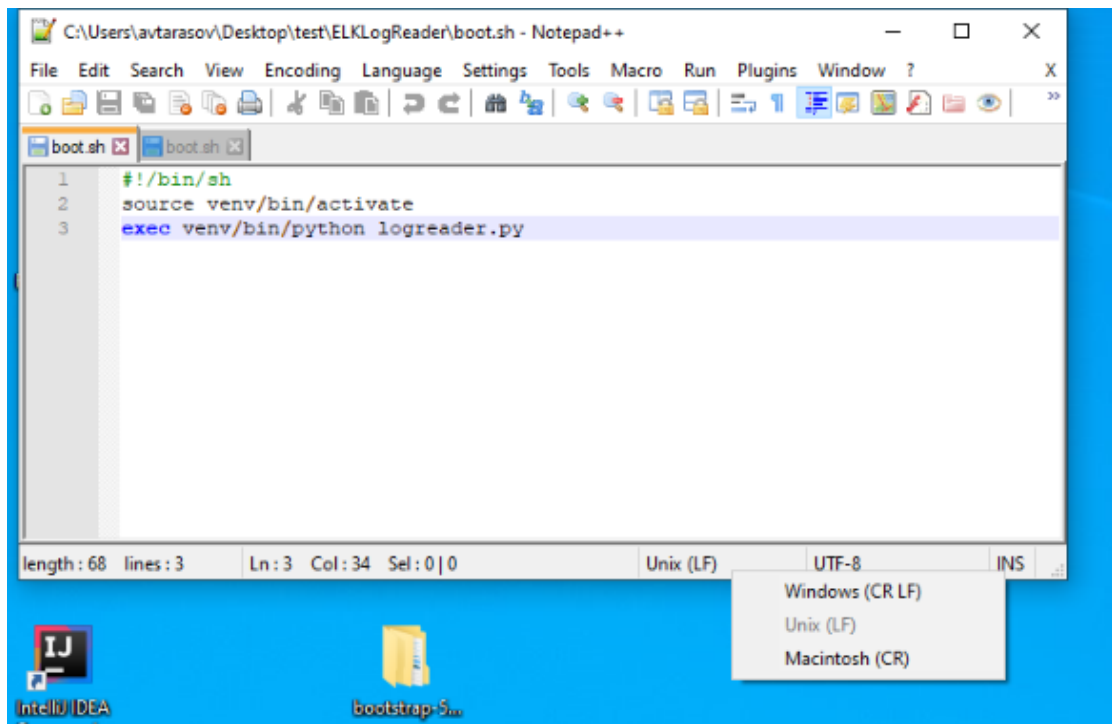


рисунок 2

6) логи добавлять в папку logs

Использование

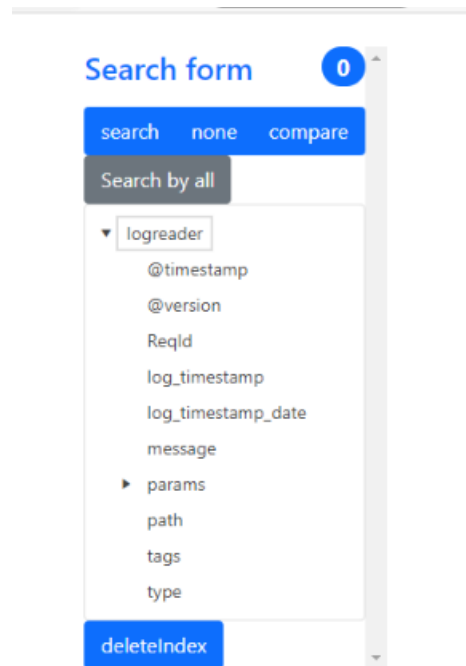


рисунок 3

В правом верхнем углу расположено меню управления.

Вкладка search

Выберите из списка полей те, по значениям которых будете производить выборку. При выборке по дате вводится диапазон, при поиске по полю в текстовом формате - поиск по максимальному совпадению (значения id записаны в формате X'356662366638663633346662626634356565373663623339' но для поиска можно ввести только значение в кавычках)(рисунок 4).

По нажатию на кнопку search by all, происходит выборка. Если предварительно не выбрать поля для выборки, будут выведены все логи.

Search form 0

search none compare

log_timestamp_date From
ДД.ММ.ГГГГ

log_timestamp_date To
ДД.ММ.ГГГГ

delete

ReqId
ReqId

delete

Search by all

▼ logreader

- @timestamp
- @version
- ReqId
- log_timestamp
- log_timestamp_date
- message
- ▶ params
- path
- tags
- type

deleteIndex

рисунок 4

Вкладка compare

The screenshot shows a web interface titled "Search form" with a blue header bar containing the text "172". Below the header, there are three tabs: "search", "none", and "compare", with "compare" being the active tab. The main form area contains three input fields: "file1" with the value "/usr/share/logstash/input/Enter.l", "file2" with the value "/usr/share/logstash/input/Reque", and "field" with the value "ReqId". Below these fields is a button labeled "compare dates". At the bottom of the form is a button labeled "deleteIndex".

Below the form, there is a tree view of fields under the "logreader" category. The fields listed are: @timestamp, @version, ReqId (highlighted in red), log_timestamp, log_timestamp_date, message, params, path, tags, and type.

рисунок 5

Введите имена файлов, для сравнения. Третье поле, общий признак. Например сравнить логи с общим ReqId из файлов '/usr/share/logstash/input/Enter.log' и '/usr/share/logstash/input/Request.log'.

Указывать путь к файлу надо тот, который выделен синим в логах(рисунок 6). Как вариант, сделать выборку по какому-то id из всех логов, скопировать оттуда пути файлов и сделать сравнение.

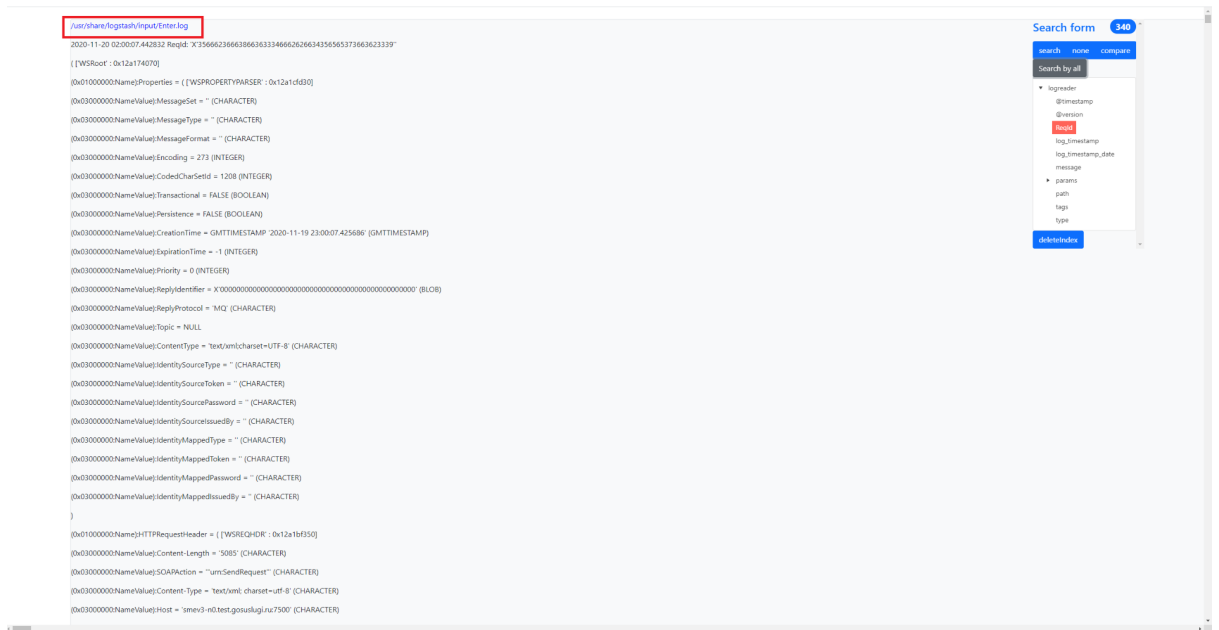


рисунок 6

Delete Index

Удалит все подгруженные данные. При повторной загрузке надо отчистить папку logs и заново скопировать в нее нужные вам логи.

None

Скрывает меню для более удобного чтения логов.

Примечания

- 1) при загрузке лога требуется время на его парсинг и загрузку в elasticsearch. моментально удалить его не получится, иначе удалится только загруженная часть, а оставшаяся часть лога дозагрузится.
- 2) при большом объеме данных сравнение дат логов происходить довольно медленно.