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 доккера и нажмите “перейти на линукс контейнеры” (рисунок 1)

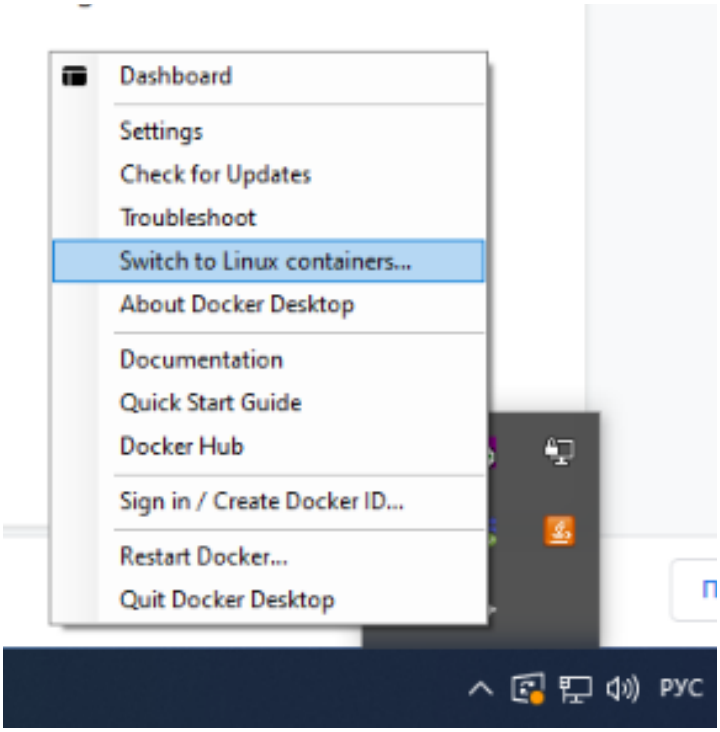

рисунок 1 - switch to linux containers

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)

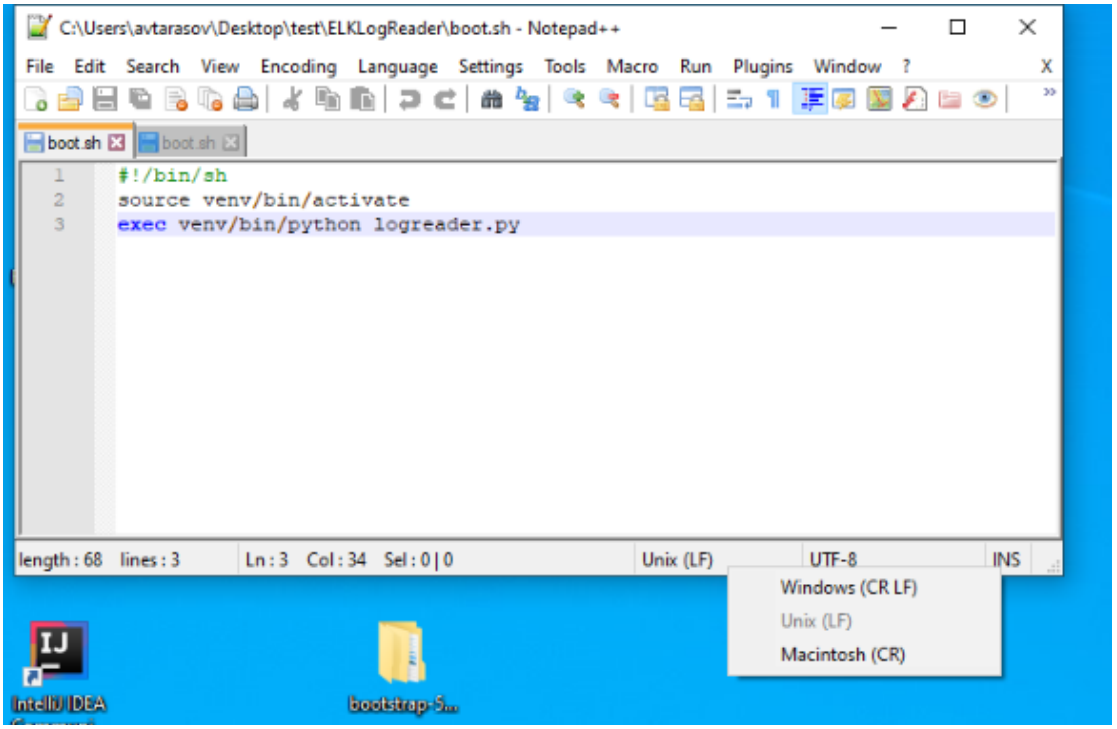

рисунок 2

6) логи добавлять в папку logs

Использование

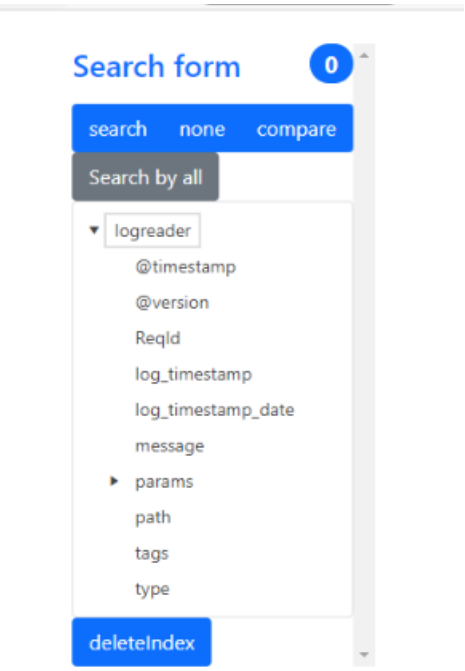

рисунок 3

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'35666236663866363334666262663435656537366362333 9' 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.

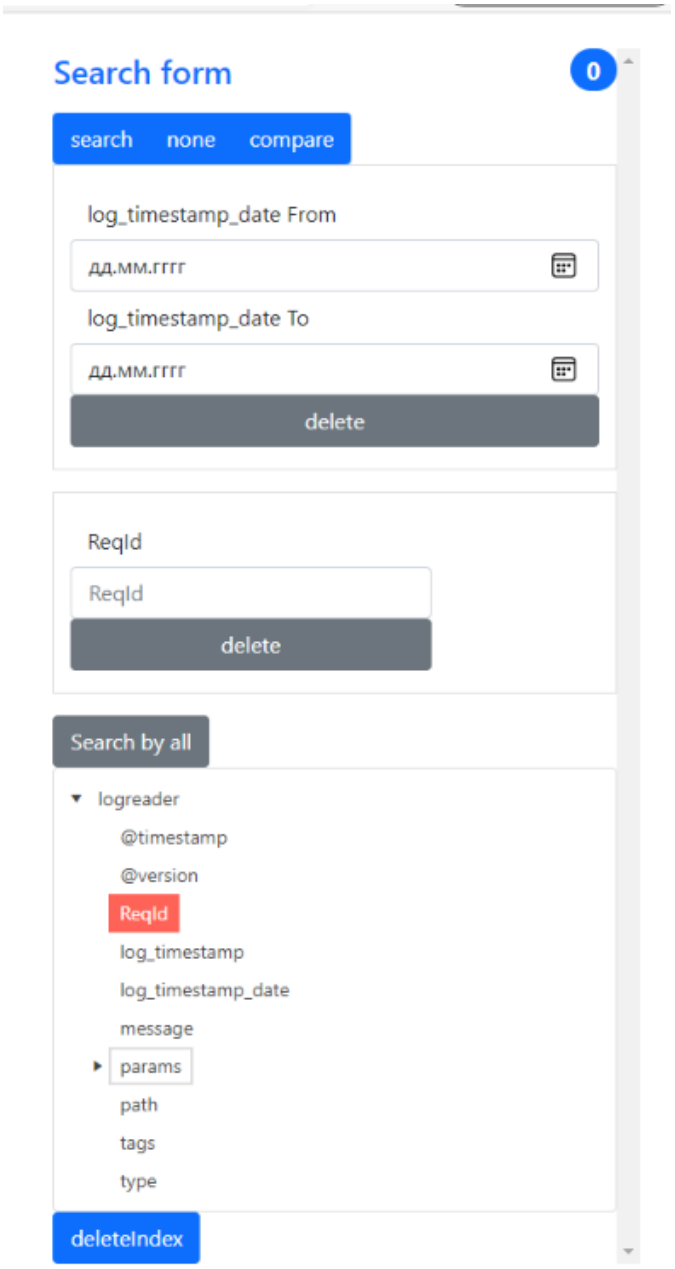

рисунок 4

Дата лога записана в формате даты и текстового поля(log_timestamp_date и log_timestamp). Поэтому поиск по дате можно производить как по текстовому полю. Т.е.

например, указать начало даты(‘2021-06-11’ или ‘2021-06-11 11:’)(рисунок 5) и все логи, даты которых совпадают началом с этим текстом попадут в выборку.

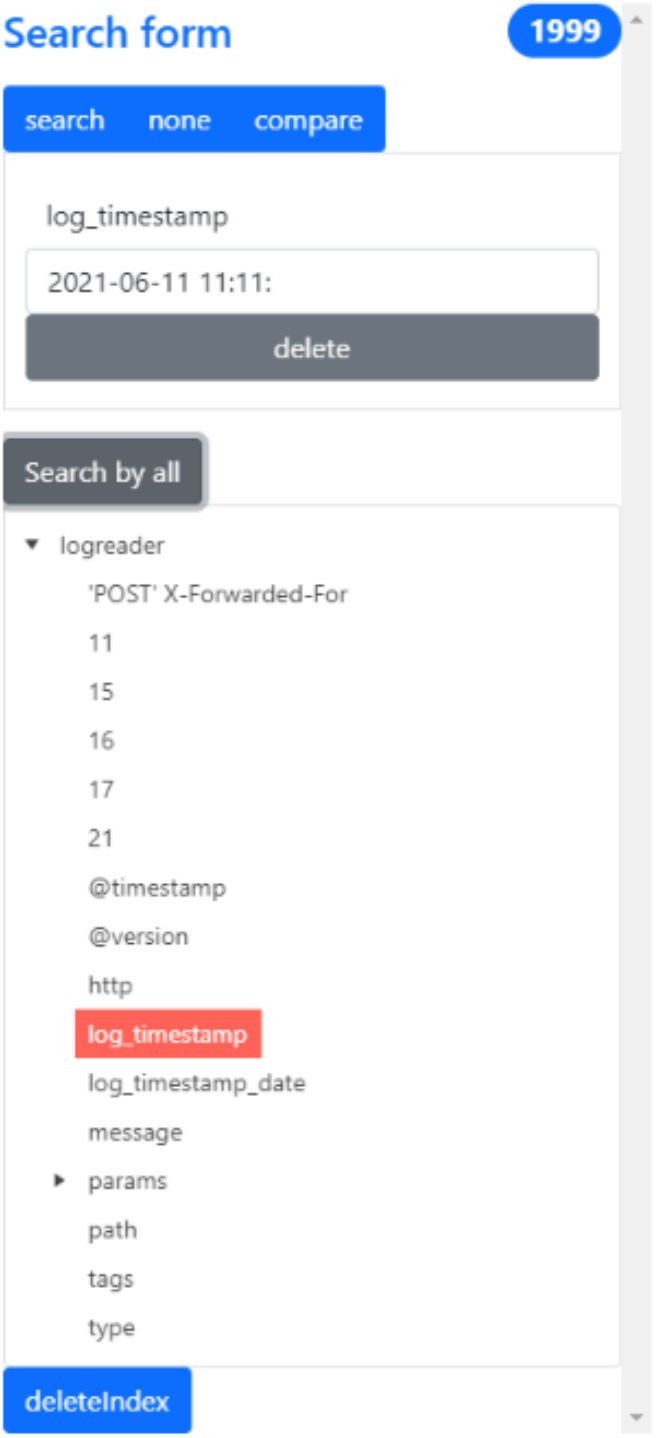

рисунок 5

Вкладка compare

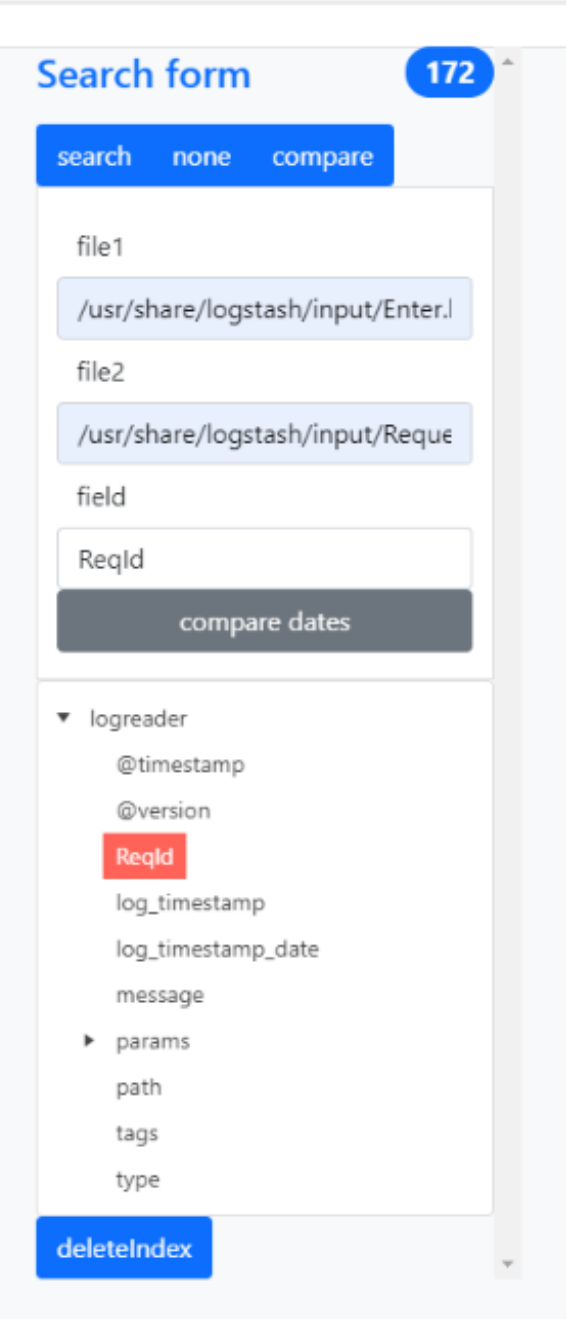

рисунок 6

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’.(рисунок 6)

Указывать путь к файлу надо тот, который выделен синим в логах(рисунок 7). Как вариант, сделать выборку по какому-то id из всех логов, скопировать оттуда пути файлов и сделать сравнение.

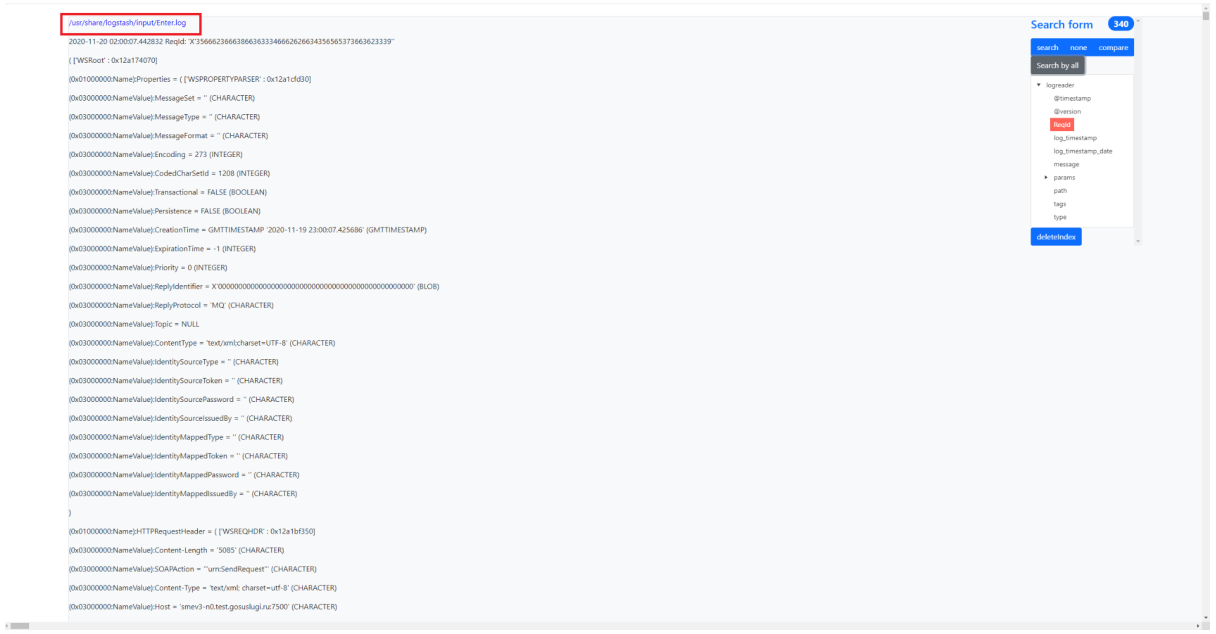
/usr/share/logstash/input/Enter.log
2020-11-20 02:00:07.442832 ReqId: X'3566623666386633346662626634356565373663623339'
{ ['WSRoot' : 0x12a174070]
(0x01000000:Name):Properties = { ['WSPROPERTYPARSER' : 0x12a1cfd30]
(0x03000000:NameValue):MessageSet = '' (CHARACTER)
(0x03000000:NameValue):MessageType = '' (CHARACTER)
(0x03000000:NameValue):MessageFormat = '' (CHARACTER)
(0x03000000:NameValue):Encoding = 273 (INTEGER)
(0x03000000:NameValue):CodedCharSetId = 1208 (INTEGER)
(0x03000000:NameValue):Transactional = FALSE (BOOLEAN)
(0x03000000:NameValue):Persistence = FALSE (BOOLEAN)
(0x03000000:NameValue):CreationTime = GMTTIMESTAMP '2020-11-19 23:00:07.425686' (GMTTIMESTAMP)
(0x03000000:NameValue):ExpirationTime = -1 (INTEGER)
(0x03000000:NameValue):Priority = 0 (INTEGER)
(0x03000000:NameValue):ReplyIdentifier = X'00000000000000000000000000000000000000000000000000000000' (BLOB)
(0x03000000:NameValue):ReplyProtocol = 'MQ' (CHARACTER)
(0x03000000:NameValue):Topic = NULL
(0x03000000:NameValue):ContentType = 'text/xml;charset=UTF-8' (CHARACTER)
(0x03000000:NameValue):IdentitySourceType = '' (CHARACTER)
(0x03000000:NameValue):IdentitySourceToken = '' (CHARACTER)
(0x03000000:NameValue):IdentitySourcePassword = '' (CHARACTER)
(0x03000000:NameValue):IdentitySourceIssuedBy = '' (CHARACTER)
(0x03000000:NameValue):IdentityMappedType = '' (CHARACTER)
(0x03000000:NameValue):IdentityMappedToken = '' (CHARACTER)
(0x03000000:NameValue):IdentityMappedPassword = '' (CHARACTER)
(0x03000000:NameValue):IdentityMappedIssuedBy = '' (CHARACTER)
}
(0x01000000:Name):HTTPRequestHeader = { ['WSREQHDR' : 0x12a1bf350]
(0x03000000:NameValue):Content-Length = '5085' (CHARACTER)
(0x03000000:NameValue):SOAPAction = '"urn:SendRequest"' (CHARACTER)
(0x03000000:NameValue):Content-Type = 'text/xml; charset=utf-8' (CHARACTER)
(0x03000000:NameValue):Host = 'smev3-n0.test.gosuslugi.ru:7500' (CHARACTER)
Search form
340
search
none
compare
Search by all
logreader
@timestamp
@version
fileqId
log_timestamp
log_timestamp_date
message
params
path
tags
type
deleteIndex

рисунок 7

Delete Index

Удалит все загруженные данные. Перед удалением, отчистите папку logs. После удаления обновите страницу в браузере.

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 еполучится, иначе удалится только загруженная часть, а оставшаяся часть лога дозагрузится.
2) при большом объеме данных сравнение дат логов происходить довольно медленно.