Filebeat++

Author : Lieven Merckx

Date : 09/09/18

Synopsis : The last filebeat you will ever need.

https://www.youtube.com/watch?v=Wmrwj6DDt-4

Features :

The filebeat version that does everything to enable local processing before pushing events, contrary to the Elastic company strategy.
It contains :

1. grok filter to extract fields from text
2. timestamp parser to extract time , date in native format
3. Javascript engine to do everything you cannot do with grok
4. AVRO codec to send this in a regular schema to kafka

The grok/Javascript are implemented as processors

Github : https://github.com/vortex314/beats

Table of Contents

Grok

Example :

```
- grok:
    patterns: ["%{SYSLOGTIMESTAMP:timestamp} %{SYSLOGHOST:syslog_host} %
{DATA:component}(?:\\[%{POSINT:forget}\\])?: %{GREEDYDATA:syslog_message}"]
    timestamps: ["Jan 2 15:04:05", "MMM dd HH:mm:ss"]
```

Patterns

>Example :

Timestamps

The timestamp format is is specified according to the GO language date formats, this means that the magical date : **Mon Jan 2 15:04:05 -0700 MST 2006**

Examples :

ANSIC = "Mon Jan _2 15:04:05 2006"
UnixDate = "Mon Jan _2 15:04:05 MST 2006"
RubyDate = "Mon Jan 02 15:04:05 -0700 2006"
RFC822 = "02 Jan 06 15:04 MST"
RFC822Z = "02 Jan 06 15:04 -0700" // RFC822 with numeric zone
RFC850 = "Monday, 02-Jan-06 15:04:05 MST"
RFC1123 = "Mon, 02 Jan 2006 15:04:05 MST"
RFC1123Z = "Mon, 02 Jan 2006 15:04:05 -0700" // RFC1123 with numeric zone
RFC3339 = "2006-01-02T15:04:05Z07:00"
RFC3339Nano = "2006-01-02T15:04:05.999999999Z07:00"
Kitchen = "3:04PM"
// Handy time stamps.
Stamp = "Jan _2 15:04:05"
StampMilli = "Jan _2 15:04:05.000"
StampMicro = "Jan _2 15:04:05.000000"
StampNano = "Jan _2 15:04:05.000000000"

Javascript processor
Example

```
- javascript:
    file: "fb.js"

fb.js
            console.log("Javascript engine loaded ");
            process = function(fields){
                  console.log(JSON.stringify(fields))
                  fields.javascript="running in GO!"
                  var d = new Date(fields.timestamp)
                  console.log(" date " + d)
                  return fields
            }
```