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

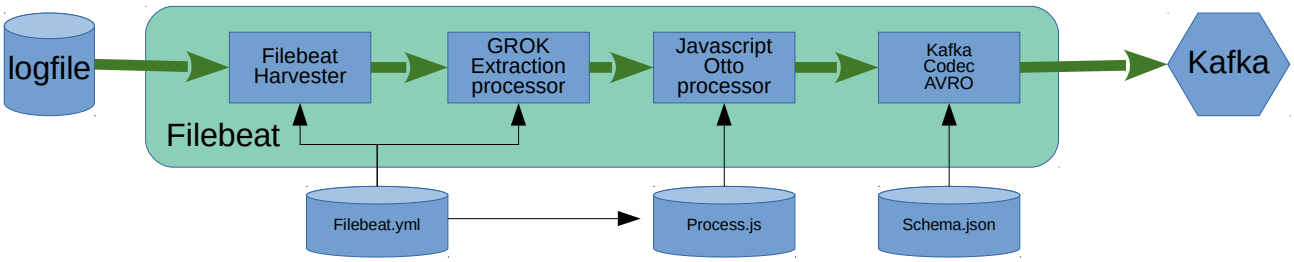

Table of Contents

Grok

Important :

Optimize 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

>Patterns

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
            }
```

Files changed in beats github from elastic

- Changed github.com/elastic/beats/libbeat/publisher/includes/includes.go
- Added github.com/elastic/beats/libbeat/outputs/codec/avro/avro.go
- Added github.com/elastic/beats/libbeat/processors/actions/grok.go
- Added github.com/elastic/beats/libbeat/processors/actions/javascript.go
- Apaprently all files are Apache license , so NOTICE.txt should be extended with changes

Example filebeat config

fb.yml

```
filebeat.inputs:
- type: log
  enabled: true
  paths:
    - /var/log/syslog


processors:
- grok:
    patterns: ["%{SYSLOGTIMESTAMP:timestamp} %{SYSLOGHOST:host} %{DATA:component}(?:\\[%
{POSINT:forget}\\])?: %{GREEDYDATA:syslog_message}"]
    timestamps: ["Jan _2 15:04:05"]
- javascript:
    file: "fb.js"


output.console:
  enabled: false
  codec.avro:
    file: "fb.json"
output.kafka:
  enabled: true
  # initial brokers for reading cluster metadata
  hosts: ["192.168.0.163:9092"]

  # message topic selection + partitioning
  topic: 'topic_avro_syslog'
  partition.round_robin:
    reachable_only: true
  compression_level: 0
  required_acks: 0
  codec.avro:
    file: "fb.json"
```

Javascript fb.js

```
console.log("Javascript engine loaded ");
process = function(fields){
       fields.message = fields.syslog_message
       console.log(JSON.stringify(fields))
       fields.attributes={}
       fields.attributes.text = "just some Javascript code"
       fields.metrics={}
       fields.metrics.temp=34.5
       fields.javascript="running in GO!"
//     var d = new Date(fields.timestamp)
//     console.log(" date " + d)
       return fields
       }
```

Test files can be found here : https://github.com/vortex314/beats/tree/master/filebeat

Logstash output after kafka

```
{
          "attributes" => {
         "text" => "just some Javascript code"
    },
              "spanId" => "",
        "parentSpanId" => "",
          "datacenter" => "",
         "userSession" => "",
        "errorMessage" => "",
         "environment" => "",
    "componentVersion" => "",
                "user" => "",
             "metrics" => {
        "temp" => 34.5
    },
       "confidential" => {},
     "executerSession" => "",
          "eventClass" => "TECH",
          "stacktrace" => "",
              "thread" => "",
          "@timestamp" => 2018-09-09T21:34:33.409Z,
               "level" => "INFO",
             "traceId" => "",
            "@version" => "1",
           "component" => "dbus-daemon",
          "initVector" => "",
           "requestor" => "",
       "schemaVersion" => 3,
                "host" => "pcpav2",
           "timestamp" => -62145361530,
             "cmdbId" => "",
             "hashKey" => "",
            "executer" => "",
    "requesterSession" => "",
          "errorTrail" => "",
           "errorCode" => "",
              "logger" => "",
       "transactionId" => "",
             "message" => "[system] Successfully activated service
'org.freedesktop.hostname1'",
           "operation" => "",
           "eventType" => "",
           "arguments" => [],
           "encrypted" => ""
}
{
          "attributes" => {
```

```
        "text" => "just some Javascript code"
    },
           "spanId" => "",
        "parentSpanId" => "",
          "datacenter" => "",
         "userSession" => "",
        "errorMessage" => "",
         "environment" => "",
    "componentVersion" => "",
              "user" => "",
           "metrics" => {
        "temp" => 34.5
    },
       "confidential" => {},
     "executerSession" => "",
          "eventClass" => "TECH",
          "stacktrace" => "",
             "thread" => "",
          "@timestamp" => 2018-09-09T21:34:33.409Z,
              "level" => "INFO",
            "traceId" => "",
           "@version" => "1",
          "component" => "systemd",
          "initVector" => "",
           "requestor" => "",
       "schemaVersion" => 3,
                "host" => "pcpav2",
           "timestamp" => -62145361530,
             "cmdbId" => "",
            "hashKey" => "",
           "executer" => "",
    "requesterSession" => "",
          "errorTrail" => "",
           "errorCode" => "",
             "logger" => "",
       "transactionId" => "",
             "message" => "Starting Hostname Service...",
           "operation" => "",
           "eventType" => "",
           "arguments" => [],
           "encrypted" => ""
}
```