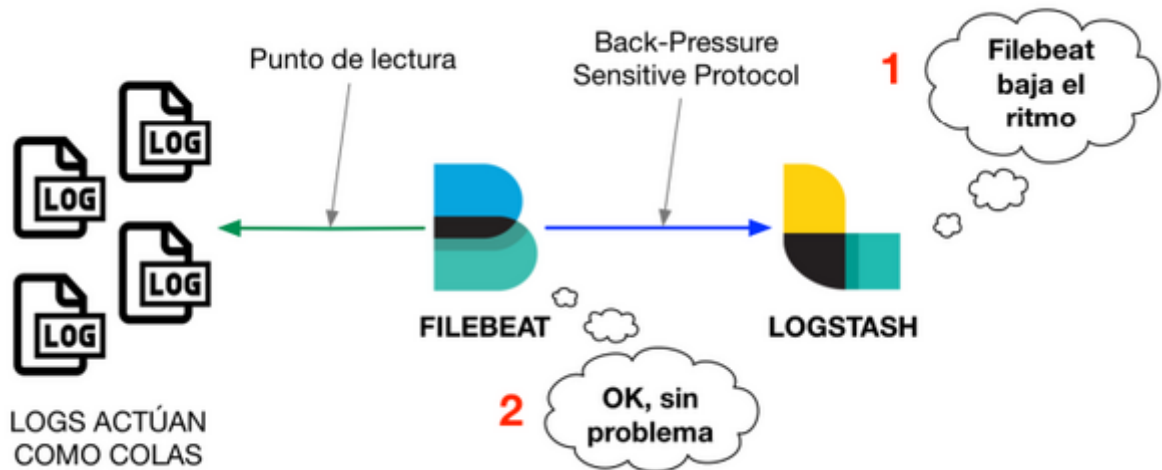


ELK: Beats (filebeats)

4.2_filebeats.pdf

- archivos en formato log
- servicio ligero
- robusto: filebeat lee y reenvía logs. Recuerda una interrupción y por donde se quedó.
- módulos: (apache, system, mysql, ...) para facilitar la captura
- no sobrecarga el sistema (back-pressure sensitive protocol):



- prospector: monitoriza ficheros, uno por cada uno, enviado a un spooler

instalación y configuración

- ```
curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-5.4.2-amd64.deb
sudo dpkg -i filebeat-5.4.2-amd64.deb
service filebeat { start | status | stop }
```

- como metricbeats, puede enviar a logstash o elasticsearch directamente
- **/etc/filebeat/filebeat.yml:**

```
filebeat.prospectors:
- input_type: log
 paths:
 - /var/log/apache2/access.log*
 - /var/log/apache2/other_vhosts_access.log*
 exclude_files: [".gz$"]
output.logstash:
 hosts: ["172.16.2.21:61000"]
```

- parámetros de autenticación para Elasticsearch
- certificados para Logstash

- **/etc/filebeat/filebeat.conf**

```
input {
 beats {
```

```

 port=>"61000"
 tags => ["apache2"]
 }
}

filter {
 grok {
 match => { "message" => ["%{IPORHOST:[apache2][access][remote_ip]}
- %{DATA:[apache2][access][user_name]}
\\[%{HTTPDATE:[apache2][access][time]}\\}
\\\"%{WORD:[apache2][access][method]} %{DATA:[apache2][access][url]}
HTTP/%{NUMBER:[apache2][access][http_version]}\\\"
%{NUMBER:[apache2][access][response_code]}
%{NUMBER:[apache2][access][body_sent][bytes]}(
\\\"%{DATA:[apache2][access][referrer]}\\\")?(
\\\"%{DATA:[apache2][access][agent]}\\\")?",
 "%{IPORHOST:[apache2][access][remote_ip]} -
%{DATA:[apache2][access][user_name]}
\\[%{HTTPDATE:[apache2][access][time]}\\} \\\"-\\\"
%{NUMBER:[apache2][access][response_code]} -"] }
 remove_field => "message"
 }
 mutate {
 add_field => { "read_timestamp" => "%{@timestamp}" }
 }
 date {
 match => ["[apache2][access][time]", "dd/MMM/YYYY:H:m:s Z"]
 remove_field => "[apache2][access][time]"
 }
 useragent {
 source => "[apache2][access][agent]"
 target => "[apache2][access][user_agent]"
 remove_field => "[apache2][access][agent]"
 }
 geoip {
 source => "[apache2][access][remote_ip]"
 target => "[apache2][access][geoip]"
 }
}

output {
 elasticsearch {
 host => ...
 manage_template => false
 index=>"%{[@metadata][beat]}-%{YYYY.MM.dd}"
 document_type => "%{[@metadata][type]}"
 }
}

```

- crear indice en kibana **filebeats-\***

From:

<https://matebcn.eu/> - miguel angel torres egea

Permanent link:

<https://matebcn.eu/info:cursos:openwebinars:elk:beats:filebeats>

Last update: **05/12/2021 11:30**

