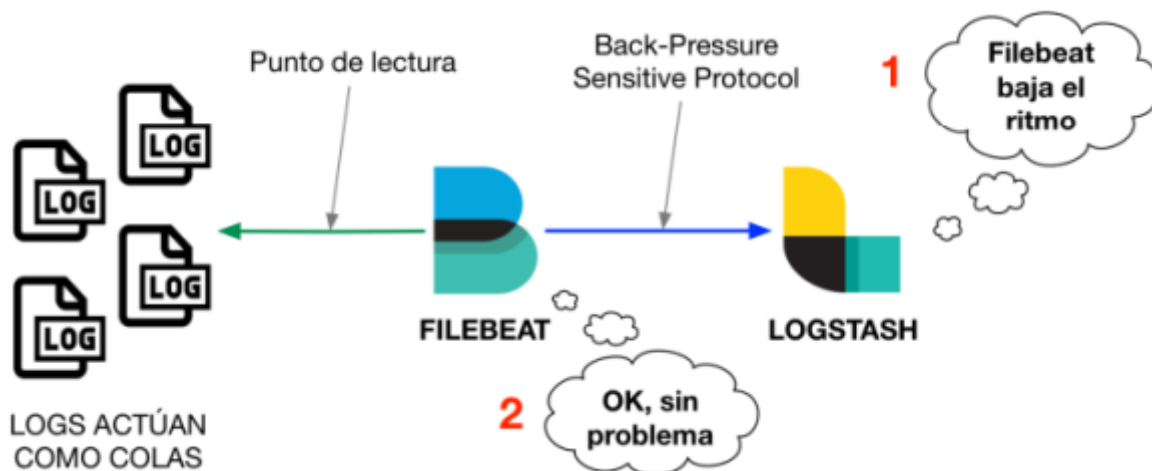


ELK: Beats (filebeats)

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 elasticsearh 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 {...}
  mutate {...}
  date {...}
  useragent {...}
  geopip {...}
}

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

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

From: <https://miguelangel.torresegea.es/wiki/> - miguel angel torres egea

Permanent link: <https://miguelangel.torresegea.es/wiki/info:cursos:openwebinars:elk:beats:filebeats?rev=1638699617>

Last update: 05/12/2021 02:20

