FILEBEATS

FILEBEAT

Servicio ligero que ayuda a reenviar logs y archivos.

Muy útil para centralizar en un único punto los registros que van generando decenas, cientos o miles de servidores, máquinas virtuales o contenedores…

1.

INTRODUCCIÓN

INTRODUCCIÓN

- **Robusto pero sin perder nada**

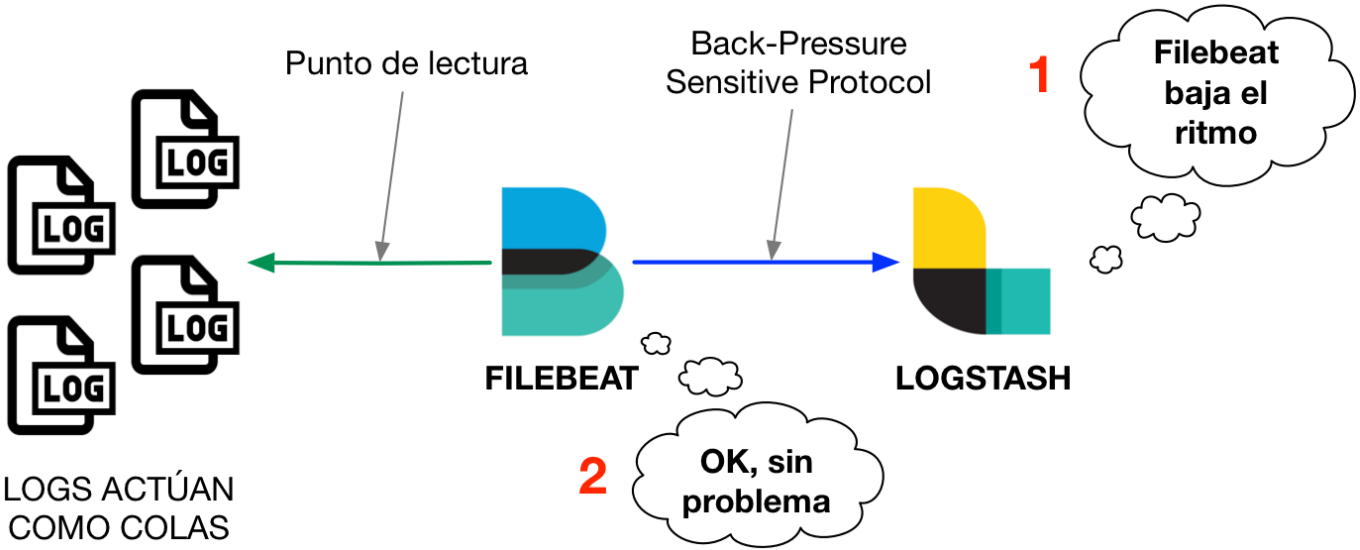
  ***Filebeat* lee y reenvía logs** (Elasticsearch / Logstash). Si se produce una interrupción recuerda por dónde se quedó para cuando vuelva a estar *online*.

- **Hace las cosas simples**

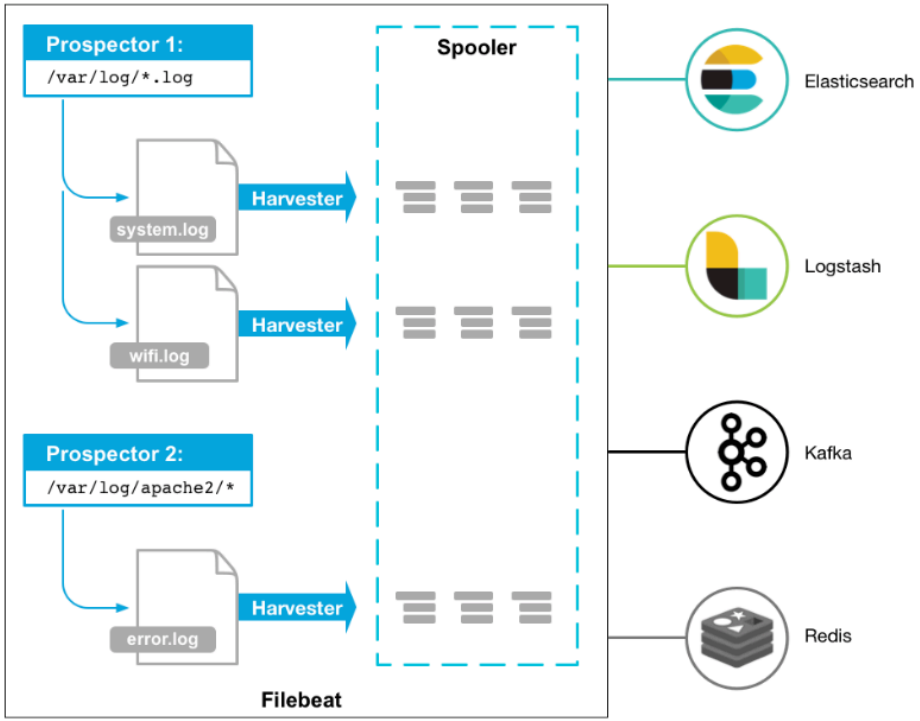
  Dispone de **módulos** (*auditd*, *Apache*, *Nginx*, *System* y *MySQL*) que simplifica la recolección de logs, tratamiento y visualización de los mismos.

INTRODUCCIÓN

- **No sobrecargará el sistema**



INTRODUCCIÓN



2.

INSTALACIÓN

FILEBEAT

- Descarga & instalación Ubuntu

  $ 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

- Descarga & instalación MAC

  $ curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-5.4.2-darwin-x86_64.tar.gz
  $ tar xzvf filebeat-5.4.2-darwin-x86_64.tar.gz

FILEBEAT

- Ejecución en Ubuntu

  $ service filebeat start/status/stop

- Ejecución en MAC

  $ ./filebeat -e -c filebeat.yml

- Ejecución en Windows

  (Powershell como administrador)

  $ PS C:\Program Files\Filebeat> Start-Service filebeat

3.

CONFIGURACIÓN Y MÓDULOS

FILEBEAT OUTPUT

- Salida directa a Elasticsearch:

```
$ output.elasticsearch:
  hosts: ["localhost:9200"]
```

- Salida para procesar a través de Logstash:

```
$ #output.logstash:
  hosts: [“localhost:5044"]
```

Parámetros de autenticación en Elasticsearch y certificados para Logstash.

FILEBEAT EJEMPLO DE EXPORTAR LOGS

Enviar los logs de Apache a Logstash.

```
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”]
```

4.

CASO DE USO

FILEBEATS APACHE2 LOGS