

Elasticsearch, Logstash y Kibana. ELK

1. He desplegado la pila de ELK en docker con el siguiente docker-compose.yml
version: '3.7'

services:

elasticsearch:

```
image: elasticsearch:7.9.2
container_name: elasticsearch
ports:
  - '9200:9200'
environment:
  - discovery.type=single-node
ulimits:
  memlock:
    soft: -1
    hard: -1
```

kibana:

```
image: kibana:7.9.2
container_name: kibana
ports:
  - '5601:5601'
environment:
  - ELASTICSEARCH_HOSTS=http://elasticsearch:9200
depends_on:
  - elasticsearch
```

logstash:

```
image: logstash:7.9.2
ports:
  - '5000:5000'
volumes:
  - type: bind
    source: ./logstash_pipeline
    target: /usr/share/logstash/pipeline
  - type: bind
    source: ./data
    target: /usr/share/logs
```

```
root@iker-Classic:/home/iker/Documentos/Ciberseguridad/ELK# ls
03_Iker_Macaya_Faber.odt  data  docker-compose.yml  logstash_pipeline
root@iker-Classic:/home/iker/Documentos/Ciberseguridad/ELK# docker ps
CONTAINER ID   IMAGE                COMMAND                  CREATED
37cf3d5df2f4   kibana:7.9.2         "/usr/local/bin/dumb..." 20 minutes ago
97fb111a4e17   elasticsearch:7.9.2  "/tini -- /usr/local..." 20 minutes ago
abf48d89c100   logstash:7.9.2       "/usr/local/bin/dock..." 20 minutes ago
root@iker-Classic:/home/iker/Documentos/Ciberseguridad/ELK#
```

2. He usado el siguiente fichero de configuración en logstash:

```
input {
  file {
    path => ["/usr/share/logs/auth.log"]
    start_position => "beginning"
  }
}

filter {
  grok {
    match => { "message" => "%{DATE:timestamp}" }
  }
}

output {
  file {
    path => "./test-%{+YYYY-MM-dd}.txt"
  }
  elasticsearch { hosts => ["http://elasticsearch:9200"] }
  stdout {
  }
}
```

*** El filtro de Grok me ha funcionado en el debugger pero no desde el fichero de configuración ***

The screenshot shows the Logstash Grok Debugger interface. At the top, there are tabs for 'Console', 'Search Profiler', 'Grok Debugger' (which is active), and 'Painless Lab' with a 'BETA' badge. Below the tabs, the 'Sample Data' section displays a JSON object with fields: 'host' (abf48d89c100), '@timestamp' (2021-05-24T18:58:31.778Z), 'path' (/usr/share/logs/auth.log), 'message' (May 9 21:39:01 iker-Classic CRON[5445]: pam_unix(cron:session): session closed for user root), and '@version' (1). The 'Grok Pattern' section shows a single pattern: '%{DATE:timestamp}'. Below this is a section for 'Custom Patterns' with a 'Simulate' button. The 'Structured Data' section shows the result of the Grok filter: a JSON object with a 'timestamp' field set to '21-05-24'.

Sample Data
1 "host" => "abf48d89c100",
2 "@timestamp" => 2021-05-24T18:58:31.778Z,
3 "path" => "/usr/share/logs/auth.log",
4 "message" => "May 9 21:39:01 iker-Classic CRON[5445]: pam_unix(cron:session): session closed for user root",
5 "@version" => "1"

Grok Pattern
1 %{DATE:timestamp}

> Custom Patterns

Simulate

Structured Data
1 {
2 "timestamp": "21-05-24"
3 }

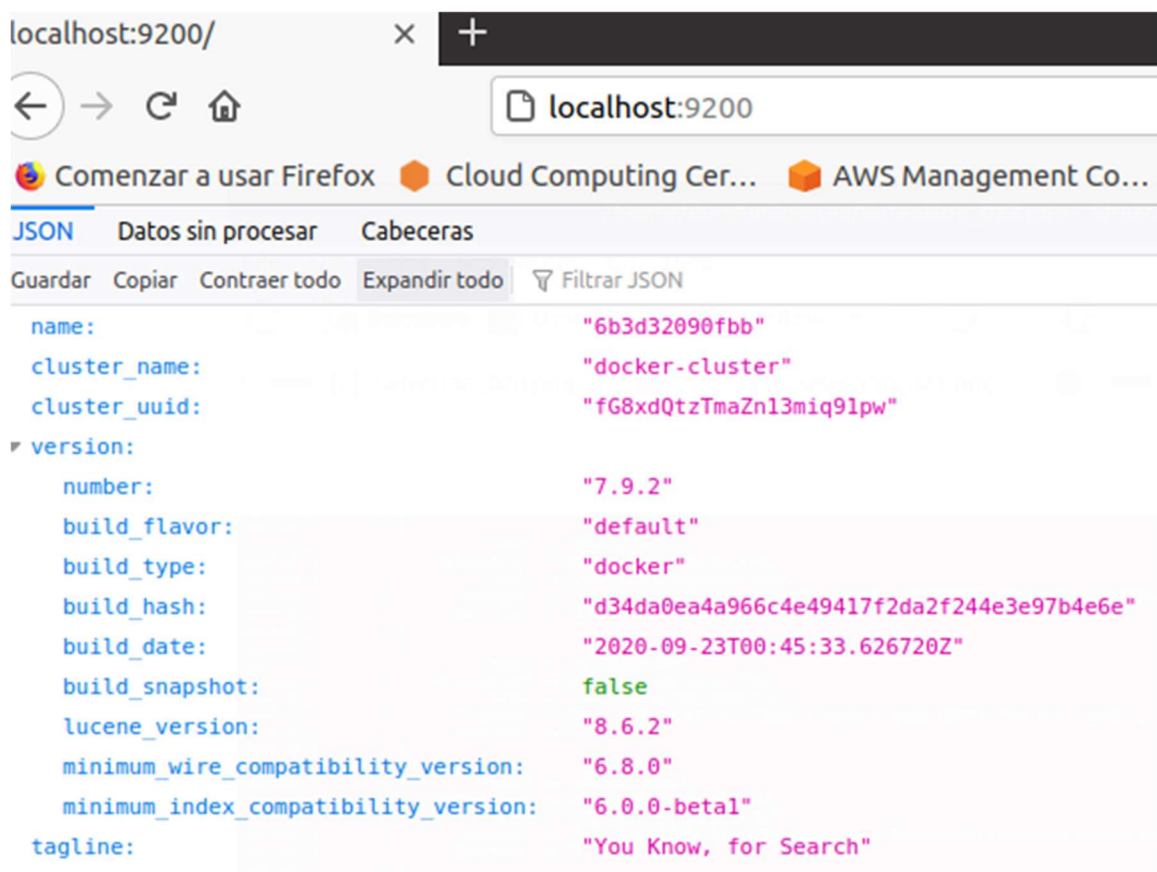
3. Pasando el siguiente fichero de logs: auth.log

```
2668 May 24 18:32:51 iker-Classic su: (to root) iker on pts/1
2669 May 24 18:32:51 iker-Classic su: pam_unix(su:session): session opened for user root by (uid=0)
2670 May 24 18:39:01 iker-Classic CRON[13253]: pam_unix(cron:session): session opened for user root by (uid=0)
2671 May 24 18:39:01 iker-Classic CRON[13253]: pam_unix(cron:session): session closed for user root
2672 May 24 18:45:37 iker-Classic systemd-logind[904]: Power key pressed.
```

Aquí se puede ver como logstash coge la información del fichero:

```
logstash_1 {
logstash_1   "host" => "abf48d89c100",
logstash_1   "@timestamp" => 2021-05-24T18:58:29.734Z,
logstash_1   "path" => "/usr/share/logs/auth.log",
logstash_1   "message" => "Apr 26 15:49:42 iker-Classic systemd-logind[890]: System is powering down.",
logstash_1   "@version" => "1"
logstash_1 }
logstash_1 {
logstash_1   "host" => "abf48d89c100",
logstash_1   "@timestamp" => 2021-05-24T18:58:29.734Z,
logstash_1   "path" => "/usr/share/logs/auth.log",
logstash_1   "message" => "May 5 08:22:52 iker-Classic systemd-logind[909]: New seat seat0.",
logstash_1   "@version" => "1"
logstash_1 }
logstash_1 {
logstash_1   "host" => "abf48d89c100",
logstash_1   "@timestamp" => 2021-05-24T18:58:29.735Z,
logstash_1   "path" => "/usr/share/logs/auth.log",
logstash_1   "message" => "May 5 08:22:52 iker-Classic systemd-logind[909]: Watching system buttons on /dev/input/event2 (Power Button)",
logstash_1   "@version" => "1"
logstash_1 }
```

4. Información sobre elasticsearch en el puerto 9200:



The screenshot shows a web browser window with the address bar set to `localhost:9200/`. The page content is a JSON response from the Elasticsearch API. The JSON is displayed in a light blue theme with syntax highlighting. The data includes cluster information and version details.

```
{
  "name": "6b3d32090fbb",
  "cluster_name": "docker-cluster",
  "cluster_uuid": "fG8xdQtzTmaZn13miq91pw",
  "version": {
    "number": "7.9.2",
    "build_flavor": "default",
    "build_type": "docker",
    "build_hash": "d34da0ea4a966c4e49417f2da2f244e3e97b4e6e",
    "build_date": "2020-09-23T00:45:33.626720Z",
    "build_snapshot": false,
    "lucene_version": "8.6.2",
    "minimum_wire_compatibility_version": "6.8.0",
    "minimum_index_compatibility_version": "6.0.0-beta1",
    "tagline": "You Know, for Search"
  }
}
```

5. Kibana y Dashboards:

Como se puede ver en el índice generado (y también mas arriba en la imagen del fichero auth.log) este dispone de 2672 entradas.

logstash-2021.05.24-000001

[Summary](#) [Settings](#) [Mappings](#) [Stats](#) [Edit settings](#)

General

Health	● yellow	Status	open
Primaries	1	Replicas	1
Docs Count	2672	Docs Deleted	
Storage Size	354kb	Primary Storage Size	
Aliases	logstash		

Index lifecycle management

Lifecycle policy	logstash-policy	Current phase	hot
Current action	unfollow	Current action time	2021-05-24 21:38:59
Failed step	-	Phase definition	Show definition

Que se pueden ver de la siguiente manera en el dashboard:

