

ELK: Beats (Packetbeats)

4.3_packetbeats.pdf

- analizador de paquetes que reenvía datos a logstash o elasticsearch
- monitorización servicios y aplicaciones en tiempo real.
- no genera latencia
- uso protocolos estandard o a medida
- busca y analiza el tráfico de red:



instalación y configuración

- `sudo apt-get install libpcap0.8`
`curl -L -O`
`https://artifacts.elastic.co/downloads/beats/packetbeat/packetbeat-5.4.2-amd64.deb`
`sudo dpkg -i packetbeat-5.4.2-amd64.deb`

- `packetbeat.interfaces.device: any`
`packetbeat.flows:`
 `timeout: 30s`
 `period: 10s`

`packetbeat.protocols.icmp:`
 `enabled: true`
`packetbeat.protocols.amqp:`
 `ports: [5672]`
`packetbeat.protocols.cassandra:`
 `ports: [9042]`
`packetbeat.protocols.dns:`
 `ports: [53]`
 `include_authorities: true`
 `include_additional: true`
`packetbeat.protocols.http:`
 `ports: [80, 8080, 8000, 5000, 8002]`
`packetbeat.protocols.memcache:`
 `ports: [11211]`
`packetbeat.protocols.mysql:`
 `ports: [3306]`
`packetbeat.protocols.pgsql:`
 `ports: [5432]`
`packetbeat.protocols.redis:`

```
ports: [6379]
packetbeat.protocols.thrift:
  ports: [9090]
packetbeat.protocols.mongodb:
  ports: [27017]
packetbeat.protocols.nfs:
  ports: [2049]

output.elasticsearch:
  hosts: ["172.16.2.21:9200"]
```

- Network device (interfaces)
 - donde colocar el sniffer
 - máximo tamaño de paquetes
 - tipos de sniffer
 - tamaño del buffer
 - *ignore_outgoing* si no se desea que registre el tráfico saliente
- flows
 - permite configurar flujos en ambas direcciones
- dashboards ejemplo: `/usr/share/packetbeat/scripts/import_dashboards`
 - `/usr/share/packetbeat/scripts/import_dashboards -es`
`http://192.168.1.10:9200 [-user <USERNAME> -password <PASSWORD>]`

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

Permanent link:
<https://matebcn.eu/info:cursos:openwebinars:elk:beats:packetbeats>

Last update: **05/12/2021 11:40**

