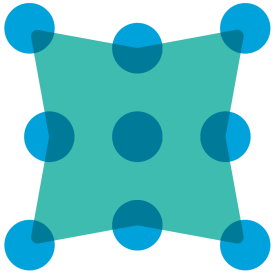
PACKETBEATS

PACKETBEAT

Analizador de paquetes que reenvía datos a Logstash o Elasticsearch.

Útil para saber qué está ocurriendo en las aplicaciones, aprovechando los datos intercambiados entre ellas.



1.

INTRODUCCIÓN

INTRODUCCIÓN

- **Monitoriza Servicios y Aplicaciones en tiempo real**
  Protocolos de red como HTTP aportan información sobre latencia, errores, tiempo de respuesta, SLAs, accesos de usuarios, tendencias… entre otros.

  Packetbeat permite acceder a esta información, formatearla en tiempo real y enviarla a ELK.
  Su despliegue no afecta a la infraestructura y *no genera latencia*.

INTRODUCCIÓN

- **Selecciona un protocolo o construye uno propio**

HTTP

Thrift-RPC

DNS

MySQL

PostgreSQL

Redis

Memcached

MongoDB

ICMP

AMQP

Cassandra

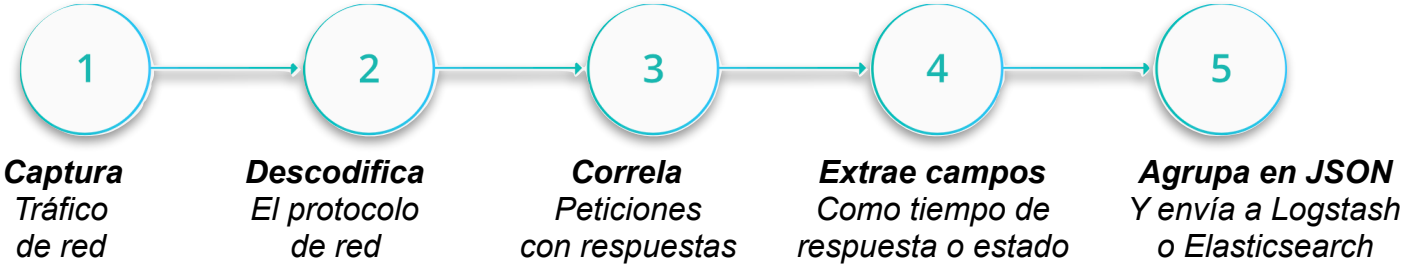
...

Añadir propio

INTRODUCCIÓN

- **Busca y analiza el tráfico de red**

  Subprocesos que recogen los datos en un formato apropiado para su búsqueda posterior y análisis.



2.

INSTALACIÓN

PACKETBEAT

- Descarga & instalación Ubuntu

  $ 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

- Ejecución en Ubuntu

  $ service packetbeat start/status/stop

- Ejecución en MAC

  $ ./packetbeat -e -c packetbeat.yml

- Ejecución en Windows

  (Powershell como administrador)

  $ PS C:\Program Files\Packetbeat> Start-Service packetbeat

3.

CONFIGURACIÓN Y MÓDULOS

PACKETBEAT 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.

PACKETBEAT OPCIONES DE CONFIGURACIÓN

- Network Device (Interfaces)

  Configura el dónde monitorizar (*sniffer*), se puede configurar distintos parámetros como:

  - Los dispositivos de donde se quiere obtener información
  - Máximo tamaño de paquetes (*snaplen*)
  - Tipos de sniffers (*pcap*, *pf_ring*)
  - Tamaño del buffer
  - *Ignore_outgoing* si no se desea que se registre el tráfico saliente.

PACKETBEAT OPCIONES DE CONFIGURACIÓN

- Flows

  Permite configurar los flujos en ambas direcciones que por defecto están deshabilitados. Se puede configurar:

  - *Enabled*: Indica si está habilitado o no.
  - *Timeout*: Tiempo de vida de un *flow* (def. 30s), si lo sobrepasa se mata al flow y se reporta.
  - *Period*: Intervalo de reporting.

4.

CASO DE USO

PACKETBEATS *DASHBOARDS*