WINLOGBEATS & HEARTBEATS

1.

WINLOGBEATS

WINLOGBEAT

Monitoriza y envía aquello que está ocurriendo en un sistema operativo Windows.

WINLOGBEATS

- **Monitoriza cualquier evento de log de Windows**

  Existen muchos tipos de logs en Windows:

  - Eventos de seguridad como *login* (4624) y fallos de autenticación (4625).
  - Cuando un usb se conecta (4663).
  - Nuevo software instalado (11707).
  - …

Puede configurarse para leer cualquier canal.

Formatea la información recogida antes de enviarla a ELK.

2.

HEARTBEAT

HEARTBEAT

Monitoriza servicios y su disponibilidad de forma activa. Lista de URLs, recoge si está activo y el tiempo de respuesta y lo envía a ELK.

¿Estás vivo? ¿Estás vivo? …

HEARTBEATS

- **Fácil de usar, fácil de configurar**
  Lista de URLs y monitorizará uptime y tiempo de respuesta. Se pueden realizar cambios en caliente (sin reinicio).

- **Pings para todo**
  Heartbeat realiza *pings* a través de ICMP, TCP y HTTP (soporta también TLS, autenticación y proxies), por lo que se pueden monitorizar tras un proxy.

HEARTBEATS

- Descarga & instalación Ubuntu

  $ curl -L -O https://artifacts.elastic.co/downloads/beats/heartbeat/heartbeat-5.4.2-amd64.deb

  $ sudo dpkg -i heartbeat-5.4.2-amd64.deb

- Descarga & instalación MAC

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

  $ tar xzvf heartbeat-5.4.2-darwin-x86_64.tar.gz

HEARTBEATS

- Ejecución en Ubuntu
  $ service heartbeat start/status/stop

- Ejecución en MAC
  $ ./heartbeat -e -c heartbeat.yml

- Ejecución en Windows
  (Powershell como administrador)
  $ PS C:\Program Files\Heartbeat> Start-Service heartbeat

3.

CONFIGURACIÓN Y MÓDULOS

HEARTBEATS 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.

HEARTBEATS MONITORS

```
heartbeat.monitors:
- type: icmp
  schedule: '*/5 * * * * * *'
  hosts: ["myhost"]
- type: tcp
  schedule: '@every 5s'
  hosts: ["myhost:7"]  # default TCP Echo Protocol
  check.send: "Check"
  check.receive: "Check"
- type: http
  schedule: '@every 5s'
  urls: ["http://localhost:80/service/status"]
  check.response.status: 200
```

4.

CASO DE USO

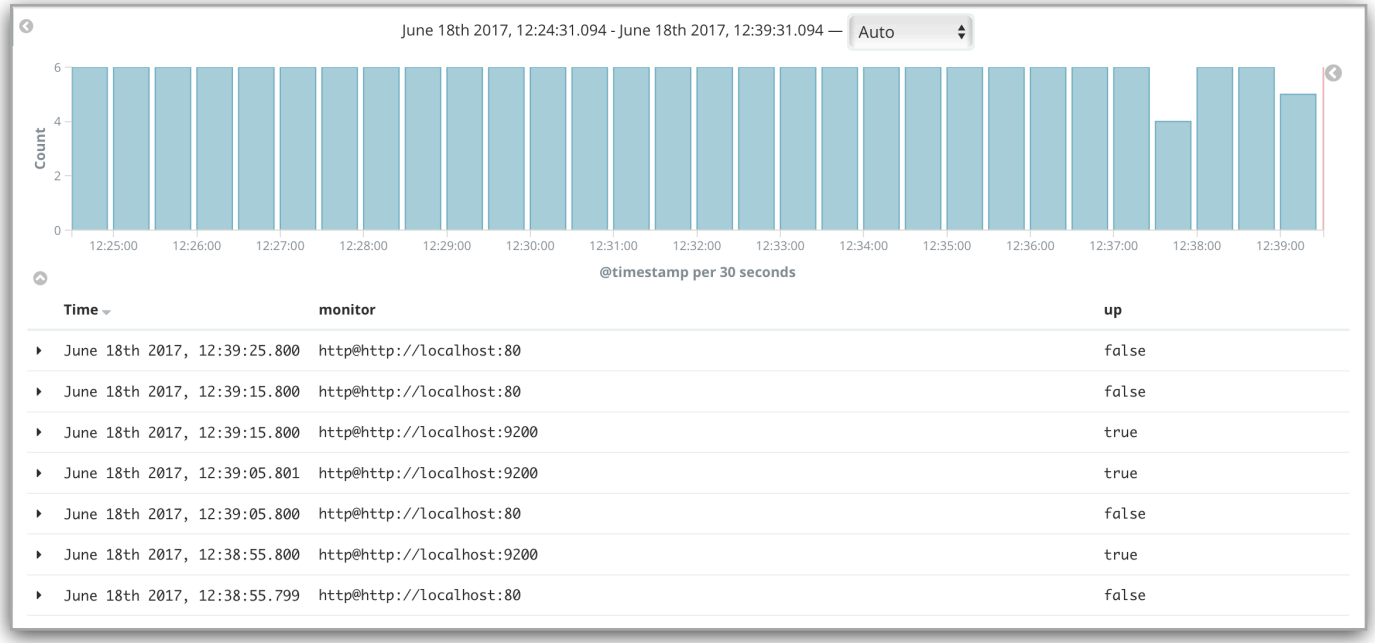
MONITORIZACIÓN HTTP

```
# Configure monitors
heartbeat.monitors:
- type: http

  # List or urls to query
  urls: ["http://localhost:9200","http://localhost:80"]

  # Configure task schedule
  schedule: '@every 10s'
```

MONITORIZACIÓN HTTP



Time	monitor	up
June 18th 2017, 12:39:25.800	http@http://localhost:80	false
June 18th 2017, 12:39:15.800	http@http://localhost:80	false
June 18th 2017, 12:39:15.800	http@http://localhost:9200	true
June 18th 2017, 12:39:05.801	http@http://localhost:9200	true
June 18th 2017, 12:39:05.800	http@http://localhost:80	false
June 18th 2017, 12:38:55.800	http@http://localhost:9200	true
June 18th 2017, 12:38:55.799	http@http://localhost:80	false