

ELK: Beats (Winlogbeats & Heartbeats)

4.4_winlogbeat_heartbeat.pdf

winlogbeats

- monitoriza cualquier evento de log de windows
- todos los eventos
- la información recogida se formatea antes de enviar a ELK

heartbeat

- monitorización de servicios y disponibilidad de forma activa
- lista de URLs, si está activo, tiempo de respuesta
- permite cambios en caliente (sin reiniciar servicio)
- ICMP, TCP, HTTP (TLS, proxies)

instalación

- ```
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
```

- ```
heartbeat.monitors:
```

 - type: http
 - urls: ["http://localhost:80"]
 - schedule: '@every 10s'
 - 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

```
output.elasticsearch:
```

 - hosts: ["172.16.2.21:9200"]

- ```
service heartbeat { start | status | stop }
```

From:

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

Permanent link:

<https://matebcn.eu/info:cursos:openwebinars:elk:beats:winlogbeat-heartbeat>

Last update: **05/12/2021 12:01**

