

Sysmon installatie



context

dit document beschrijft de installatie van Sysmon op Windows

installatie

- Kibana: Observability > Overview: Add integrations
- filter op **Beats only**, zoek: Windows
- kies: **Windows Event Logs**
- volg de installatie instructies
 - [download](#) Zip file
 - pak uit onder **C:\Program Files** en hernoem naar **winlogbeat**
 - start powershell-as-admin en voer uit:

```
powershell.exe -ExecutionPolicy UnRestricted -File "C:\Program Files\winlogbeat\install-service-winlogbeat.ps1"
```

configuratie

bestand

1. open winlogbeat.yml
 1. output.elasticsearch:
 1. zet in commentaar (#)
 2. #output.logstash:
 1. #hosts: ["localhost:5044"]
 1. zet beide uit commentaar en vul de logstash server in
2. bewaar je wijzigingen
3. start Winlogbeat: Start-Service winlogbeat

In geval van een **eerste** installatie van Winlogbeat, dien je nog onderstaande stappen **eenmalig** uit te voeren:

indexing

1. laad de indexing template:
 1. start powershell-as-admin en voer uit:

```
.\winlogbeat.exe setup --index-management -E  
output.logstash.enabled=false -E  
'output.elasticsearch.hosts=["elk:9200"] '
```

kibana dashboards

1. start powershell-as-admin en voer uit:

```
.\winlogbeat.exe setup -e -E output.logstash.enabled=false -E  
output.elasticsearch.hosts=["elk:9200"] -E  
setup.kibana.host=kibana:5601
```

2. start Winlogbeat: Start-Service winlogbeat

meer info

1. [installatie](#)
2. [logstash_configuratie](#)

[elk stack](#), [filebeat](#)

From:

<https://louslab.be/> - **Lou's lab**

Permanent link:

https://louslab.be/doku.php?id=elk_stack:syslog_installatie

Last update: **2024/11/16 18:14**

