

sample dashboards activeren



context

dit document beschrijft hoe je sample dashboards activeert in Kibana.

beats utility

Voor metricbeat, filebeat, heartbeat, ... worden dashboards meegeleverd bij installatie via yum/apt.

1. open `/etc/<file|metric|heart>beat/<file|metric|heart>beat.yml`
2. activeer de waarde:

```
setup.dashboards.enabled: true
```

3. herstart de beat service:

```
sudo systemctl restart <file|metric|heart>beat
```

Kibana

- dashboards worden geïmporteerd vanuit `/usr/share/<file|metric|heart>beat/kibana/7/dashboard`
- deze directory bevat JSON-bestanden:

CoreDNS-Overview-Dashboard.json	Filebeat-icinga-main-log.json	filebeat-netflow-conversation-partners.json
Filebeat-apache.json	Filebeat-icinga-startup-errors.json	filebeat-netflow-flow-exporters.json
Filebeat-auditd.json	Filebeat-iis.json	filebeat-netflow-flow-records.json
Filebeat-auth-sudo-commands.json	Filebeat-Iptables-Overview.json	filebeat-netflow-geo-location.json
Filebeat-aws-s3access-overview.json	Filebeat-Iptables-Ubiquiti-Firewall-Overview.json	filebeat-netflow-overview.json
Filebeat-azure-alerts-overview.json	Filebeat-Kafka-overview.json	filebeat-netflow-top-n.json
Filebeat-azure-overview.json	Filebeat-logstash-log.json	filebeat-netflow-traffic-analysis.json
Filebeat-azure-user-activity.json	Filebeat-logstash-slowlog.json	filebeat-network-flows-top-n.json
Filebeat-Cisco-ASA.json	Filebeat-MISP-Overview.json	Filebeat-new-users-and-groups.json
Filebeat-Envoyproxy-Overview.json	Filebeat-Mongodb-overview.json	Filebeat-nginx-logs.json
Filebeat-haproxy-overview.json	Filebeat-mysql.json	Filebeat-nginx-overview.json
Filebeat-IBMMQ-Overview.json	Filebeat-nats-overview.json	Filebeat-panw-network-overview.json
Filebeat-icinga-debug-log.json	filebeat-netflow-autonomous-systems.json	Filebeat-panw-threat-overview.json

- resultaat van de import kan je volgen in `/var/log/messages`
- als je 1 JSON-bestand wilt importeren, ga dan als volgt tewerk:
 - **Management > Kibana: Saved objects**
 - klik op de knop **import**
 - **blader** naar het bestand
 - vink uit: **Automatically overwrite all saved objects**
 - klik op **Import**

meer info

voeg hier linken toe naar verdere uitleg

[elk stack](#)

From:

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

Permanent link:

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

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

