

Elastic Essential I

Aula 6



Eu sou Rodrigo Augusto Rebouças.

Engenheiro de dados da Semantix Instrutor do Semantix Academy

Você pode me encontrar em: rodrigo.augusto@semantix.com.br







Beats

Família de beats



Beats Família

- Enviam dados de centenas ou milhares de máquinas e sistemas
 - Logstash
 - Elasticsearch
- Download
 - https://www.elastic.co/pt/downloads/beats/



Filebeat

Arquivos de log



Logs de evento do Windows

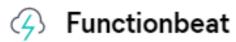


Metricbeat

Métricas

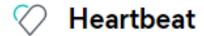


Dados de auditoria





Dados de rede



Monitoramento de disponibilidade







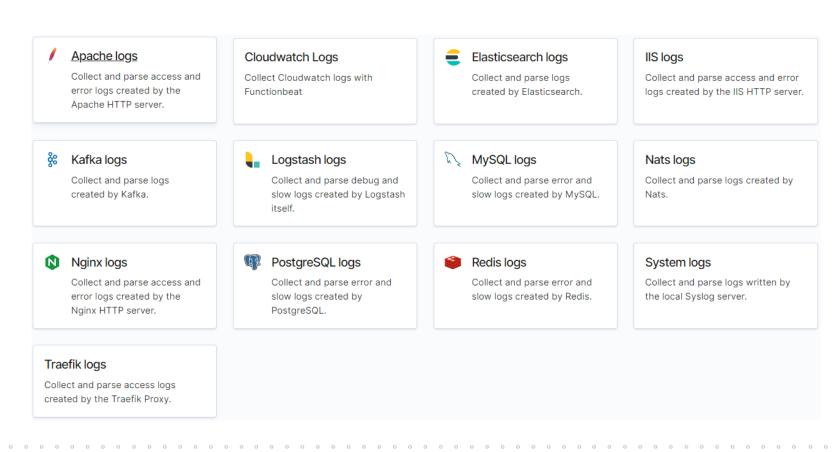
Filebeat

Conceitos Configuração Execução



Filebeat Conceitos

- Módulos de Filebeat
 - Leitura de logs
 - o 0, 1 ou vários arquivos de log





Filebeat Instalação e Configuração

- Version Elasticsearch 7.9.2
- Olhar na documentação da Elastic:

https://www.elastic.co/guide/en/beats/filebeat/master/filebeat-getting-started.html

Download

\$ curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat-7.9.2-linux-x86_64.tar.gz

Descompactar

\$ tar xzvf filebeat-7.9.2-linux-x86_64.tar.gz

- Usar módulo de comunicação
- \$./filebeat modules list
- \$./filebeat modules enable <módulo>
- Testar Beat
- \$./filebeat test config
- \$./filebeat test output



Filebeat Configuração

Configurar o arquivo: filebeat.yml

```
filebeat.prospectors:
```

- type: log

enabled: true

paths:

- /var/log/*.log

output.elasticsearch:

hosts: ["<es_url>"]

username: "<user>"

password: "<password>"

output.logstash:



Filebeat Inicialização

- Inicializar de modo simples
 - \$ sudo chown root filebeat.yml
 - \$ sudo chown root modules.d/system.yml
 - Apenas para os módulos habilitados
 - \$ sudo ./filebeat –e
 - Exibir a configuração e saída do beat
- Inicializar como serviço
 - \$ sudo service filebeat start
 - \$ sudo service filebeat status
 - \$ sudo service filebeat stop
 - \$ sudo service filebeat restart





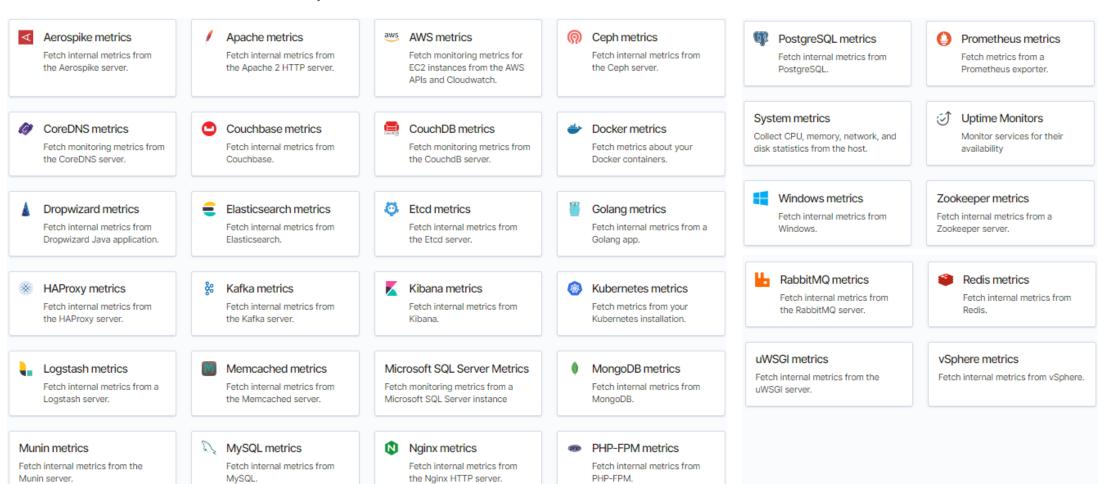
Metricbeat

Conceitos Configuração Execução



Metricbeat Conceitos

- Módulos de Metricbeat
 - Leitura de medidas quantitativas





Metricbeat Instalação e Configuração

- Version Elasticsearch 7.9.2
- Olhar na documentação da Elastic:

https://www.elastic.co/guide/en/beats/metricbeat/master/metricbeat-getting-started.html

Download

```
$ curl -L -O
https://artifacts.elastic.co/downloads/beats/metricbeat/metricbeat -
7.9.2-linux-x86_64.tar.gz
```

- Descompactar
- \$ tar xzvf metricbeat-7.9.2-linux-x86_64.tar.gz
- Usar módulo de comunicação
- \$./metricbeat modules list
- \$./metricbeat modules enable <módulo>
- Testar Beat
- \$./metricbeat test config
- \$./metricbeat test output



Metricbeat Configuração

Configurar o arquivo: metricbeat.yml - module: system

metricsets: ["cpu"]

enabled: true

period: 1s

output.elasticsearch:

hosts: ["<es_url>"]

username: "<user>"

password: "<password>"

output.logstash:



Metricbeat Inicialização

- Inicializar de modo simples
 - \$ sudo chown root metricbeat.yml
 - \$ sudo chown root modules.d/system.yml
 - Apenas para os módulos habilitados
 - \$ sudo ./metricbeat –e
 - Exibir a configuração e saída do beat
- Inicializar como serviço
 - \$ sudo service metricbeat start
 - \$ sudo service metricbeat status
 - \$ sudo service metricbeat stop
 - \$ sudo service metricbeat restart





Heartbeat

Conceitos Configuração Execução



Heartbeat Conceitos

- Monitoramento e disponibilidade
- Pings via
 - ICMP
 - TCP
 - HTTP,
- Configuração
 - TLS
 - Autenticação
 - Proxies



Heartbeat Instalação e Configuração

- Version Elasticsearch 7.9.2
- Olhar na documentação da Flastic:

https://www.elastic.co/guide/en/
beats/heartbeat/master/heartbe
at-installation-configuration.html

Download

\$ curl -L -O https://artifacts.elastic.co/downloads/beats/heartbeat/heartbeat-7.9.2-linux-x86_64.tar.gz

Descompactar

\$ tar xzvf heartbeat-7.9.2-linux-x86_64.tar.gz

- Testar Beat
- \$./heartbeat test config
- \$./heartbeat test output



Heartbeat Configuração

Configurar o arquivo: heartbeat.yml

```
heartbeat.monitors:
```

```
- type: http
```

```
urls: ["http://www.semantix.com.br"]
```

```
schedule: '@every 10s'
```

output.elasticsearch:

```
hosts: ["<es_url>"]
```

username: "<user>"

password: "<password>"

output.logstash:



Heartbeat Inicialização

- Inicializar de modo simples
 - \$ sudo chown root heartbeat.yml
 - \$ sudo ./heartbeat -e
 - Exibir a configuração e saída do beat
- Inicializar como serviço
 - \$ sudo service heartbeat start
 - \$ sudo service heartbeat status
 - \$ sudo service heartbeat stop
 - \$ sudo service heartbeat restart



Exercícios Beats

- 1. Enviar o arquivo <local>/paris-925.logs com uso do Filebeat
- 2. Verificar a quantidade de documentos do índice criado pelo Filebeat e visualizar seus 10 primeiros documentos
- 3. Monitorar as métricas do docker
 - Referência:

https://www.elastic.co/guide/en/beats/metricbeat/current/metricbeat-module-docker.html

Encontrar o socket do Docker

\$ sudo find / -name docker.sock

- 4. Verificar a quantidade de documentos do índice criado pelo Metricbeat e visualizar seus 10 primeiros documentos
- 5. Monitorar o site https://www.elastic.co/pt/ com uso do Heartbeat
- 6. Verificar a quantidade de documentos do índice criado pelo Heartbeat e visualizar seus 10 primeiros documentos



Heartbeat

Conceitos Configuração Execução





Obrigado!

Alguma pergunta?



Você pode me encontrar em: rodrigo.augusto@semantix.com.br

GET SMARTER