



Semantix

Elastic Essential I

Aula 6

Quem sou eu?

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



Metricbeat

Métricas



Packetbeat

Dados de rede



Winlogbeat

Logs de evento do Windows



Auditbeat

Dados de auditoria



Heartbeat

Monitoramento de disponibilidade



Functionbeat

Agente de envio sem servidor











Filebeat

Conceitos
Configuração
Execução

Filebeat Conceitos

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

 Apache logs Collect and parse access and error logs created by the Apache HTTP server.	Cloudwatch Logs Collect Cloudwatch logs with Functionbeat	 Elasticsearch logs Collect and parse logs created by Elasticsearch.	IIS logs Collect and parse access and error logs created by the IIS HTTP server.
 Kafka logs Collect and parse logs created by Kafka.	 Logstash logs Collect and parse debug and slow logs created by Logstash itself.	 MySQL logs Collect and parse error and slow logs created by MySQL.	Nats logs Collect and parse logs created by Nats.
 Nginx logs Collect and parse access and error logs created by the Nginx HTTP server.	 PostgreSQL logs Collect and parse error and slow logs created by PostgreSQL.	 Redis logs Collect and parse error and slow logs created by Redis.	System logs Collect and parse logs written by the local Syslog server.
Traefik logs Collect and parse access logs created by the Traefik Proxy.			

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/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

 Aerospike metrics Fetch internal metrics from the Aerospike server.	 Apache metrics Fetch internal metrics from the Apache 2 HTTP server.	 AWS metrics Fetch monitoring metrics for EC2 instances from the AWS APIs and Cloudwatch.	 Ceph metrics Fetch internal metrics from the Ceph server.	 PostgreSQL metrics Fetch internal metrics from PostgreSQL.	 Prometheus metrics Fetch metrics from a Prometheus exporter.
 CoreDNS metrics Fetch monitoring metrics from the CoreDNS server.	 Couchbase metrics Fetch internal metrics from Couchbase.	 CouchDB metrics Fetch monitoring metrics from the CouchDB server.	 Docker metrics Fetch metrics about your Docker containers.	System metrics Collect CPU, memory, network, and disk statistics from the host.	 Uptime Monitors Monitor services for their availability
 Dropwizard metrics Fetch internal metrics from Dropwizard Java application.	 Elasticsearch metrics Fetch internal metrics from Elasticsearch.	 Etcd metrics Fetch internal metrics from the Etcd server.	 Golang metrics Fetch internal metrics from a Golang app.	 Windows metrics Fetch internal metrics from Windows.	Zookeeper metrics Fetch internal metrics from a Zookeeper server.
 HAProxy metrics Fetch internal metrics from the HAProxy server.	 Kafka metrics Fetch internal metrics from the Kafka server.	 Kibana metrics Fetch internal metrics from Kibana.	 Kubernetes metrics Fetch metrics from your Kubernetes installation.	 RabbitMQ metrics Fetch internal metrics from the RabbitMQ server.	 Redis metrics Fetch internal metrics from Redis.
 Logstash metrics Fetch internal metrics from a Logstash server.	 Memcached metrics Fetch internal metrics from the Memcached server.	Microsoft SQL Server Metrics Fetch monitoring metrics from a Microsoft SQL Server instance	 MongoDB metrics Fetch internal metrics from MongoDB.	uWSGI metrics Fetch internal metrics from the uWSGI server.	vSphere metrics Fetch internal metrics from vSphere.
Munin metrics Fetch internal metrics from the Munin server.	 MySQL metrics Fetch internal metrics from MySQL.	 Nginx metrics Fetch internal metrics from the Nginx HTTP server.	 PHP-FPM metrics Fetch internal metrics from PHP-FPM.		

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 Elastic:

<https://www.elastic.co/guide/en/beats/heartbeat/master/heartbeat-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





Semantix

Obrigado!

Alguma pergunta?



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

GET SMARTER