Semantix

Elastic Essential I

Aula 1

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

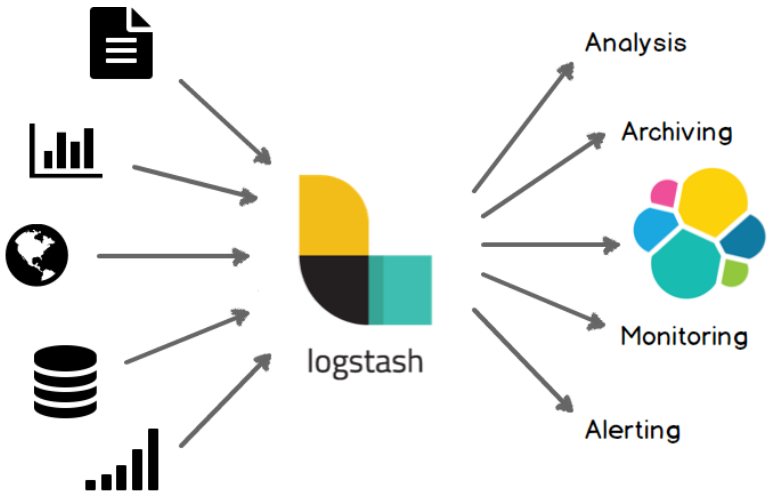
Logstash

Conceitos

Plugins

Semantix

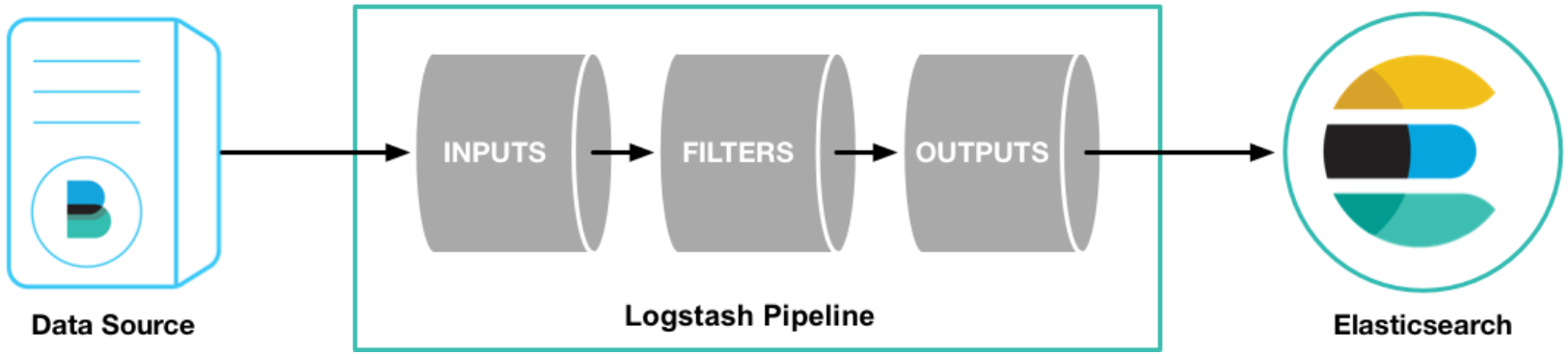
Logstash Conceitos



- Alterar o logstash.conf
- Plugin
  - Input
  - Filter
  - Output

- Estrutura do json

```
input{
}
filter{
}
output {
}
```



Semantix

Logstash Instalação e Configuração

- Version Elasticsearch 7.9.2
- Documentação da Elastic: https://www.elastic.co/guide/en/logstash/current/getting-started-with-logstash.html
- Estrutura pastas

  docker-compose.yml

  - pipeline/logstash.conf
  - settings
    - elasticsearch.yml
    - kibana.yml
    - logstash.yml

Logstash Instalação e Configuração

- Adicionar o serviço do logstash no docker-compose.yml

```
services:
    elasticsearch: …
    kibana: …
    logstash:
        image: docker.elastic.co/logstash/logstash:7.9.2
        volumes:
          - ./pipeline/logstash.conf:/usr/share/logstash/pipeline/logstash.conf:ro
          - ./settings/logstash.yml:/usr/share/logstash/config/logstash.yml:ro
        ports:
          - "9600:9600“
          - “5044:5044“
        networks:
          - elastic
```

Logstash Configuração

- pipeline/logstash.conf

```
input {
        beats {
        port => 5044
        }
}
output {
        stdout {
        codec => "json"
        }
        elasticsearch {
                hosts => ["elasticsearch:9200"]
        }
}
```

- settings/logstash.yml

```
http.host: "0.0.0.0"
xpack.monitoring.elasticsearch.hosts: [
"http://elasticsearch:9200" ]
```

Plugins de Entrada

Conceitos

Exemplo

Semantix

Plugins Entrada

- Permite que uma fonte específica de eventos seja lida pelo Logstash
  - https://www.elastic.co/guide/en/logstash/7.9/input-plugins.html

- Plugins de entrada
  - Azure_event_hubs, **beats**, cloudwatch, couchdb_changes, dead_letter_queue, **elasticsearch**, exec, **file**, ganglia, gelf, generator, github, google_cloud_storage, google_pubsub, graphite, **heartbeat**, **http**, http_poller, imap, irc, **jdbc**, jms, jmx, **kafka**, kinesis, log4j, lumberjack, meetup, pipe, puppet_facter, rabbitmq, **redis**, relp, rss, s3, salesforce, snmp, snmptrap, sqlite, sqs, stdin, stomp, **syslog**, **tcp**, twitter, udp, unix, varnishlog, websocket, wmi e xmpp

Plugin Entrada - Exemplo

- pipeline/logstash.conf

```
input {
  file {
    id => "test_log_sem_gz"
    path => "/var/log/*.log"
    exclude => "*.gz"
  }
}
```

Plugins de Saída

Conceitos

Exemplo

Semantix

Plugins Saída

- Permite o envio de dados de evento para um destino específico
  - https://www.elastic.co/guide/en/logstash/7.9/output-plugins.html

- Plugins de saída
  - Boundary, circonus, cloudwatch, **csv**, datadog, datadog_metrics, elastic_app_search, **elasticsearch**, email, exec, **file**, ganglia, gelf, google_bigquery, google_pubsub, graphite, graphtastic, **http**, influxdb, irc, juggernaut, kafka, librato, loggly, lumberjack, metriccatcher, mongodb, nagios, nagios_nsca, opentsdb, pagerduty, pipe, rabbitmq, redis, redmine, riak, riemann, s3, sns, solr_http, sqs, statsd, **stdout**, stomp, syslog, **tcp**, timber, udp, webhdfs, websocket, xmpp e zabbix

Plugin Saída - Exemplo

- pipeline/logstash.conf

```
output {
  stdout {
    codec => json
  }
  elasticsearch {
    hosts => [ "localhost:9200" ]
    index => "testes-%{+YYYY.MM.dd}"
  }
}
```

Plugins de Filtro

Conceitos

Exemplo

Semantix

Plugins Filtro

- Permite o processamento intermediário em um evento
  - https://www.elastic.co/guide/en/logstash/7.9/filter-plugins.html

- Plugins de Filtro
  - **Aggregate**, alter, bytes, cidr, cipher, clone, **csv**, date, de_dot, dissect, dns, drop, elapsed, **elasticsearch**, environment, extractnumbers, fingerprint, geoip, **grok**, http, i18n, jdbc_static, jdbc_streaming, json, json_encode, kv, memcached, metricize, metrics, **mutate**, prune, range, ruby, sleep, **split**, syslog_pri, throttle, tld, translate, truncate, urldecode, useragent, uuid e xml

Plugin Filtro - Exemplo

- pipeline/logstash.conf

```
filter {
  mutate { "convert" => [ "bytes " , "integer" ] }
  mutate { "convert" => [ "duration" , “float" ] }
}
```

Exercícios Logstash

1. Enviar o arquivo <local>/paris-925.logs para o logstash com uso do Filebeat
2. Configurar e executar o logstash com as seguintes configurações
   - Entrada:

```
beats {
    port => 5044
}
```

   - Saída:

```
elasticsearch {
    hosts => [ “elasticsearch:9200" ]
    index => “seu_nome-%{+YYYY.MM.dd}"
 }
```

3. Verificar a quantidade de documentos do índice criado pelo Logstash e visualizar seus 10 primeiros documentos

Semantix

Obrigado!

Alguma pergunta?

Você pode me encontrar em:

rodrigo.augusto@semantix.com.br

GET SMARTER