



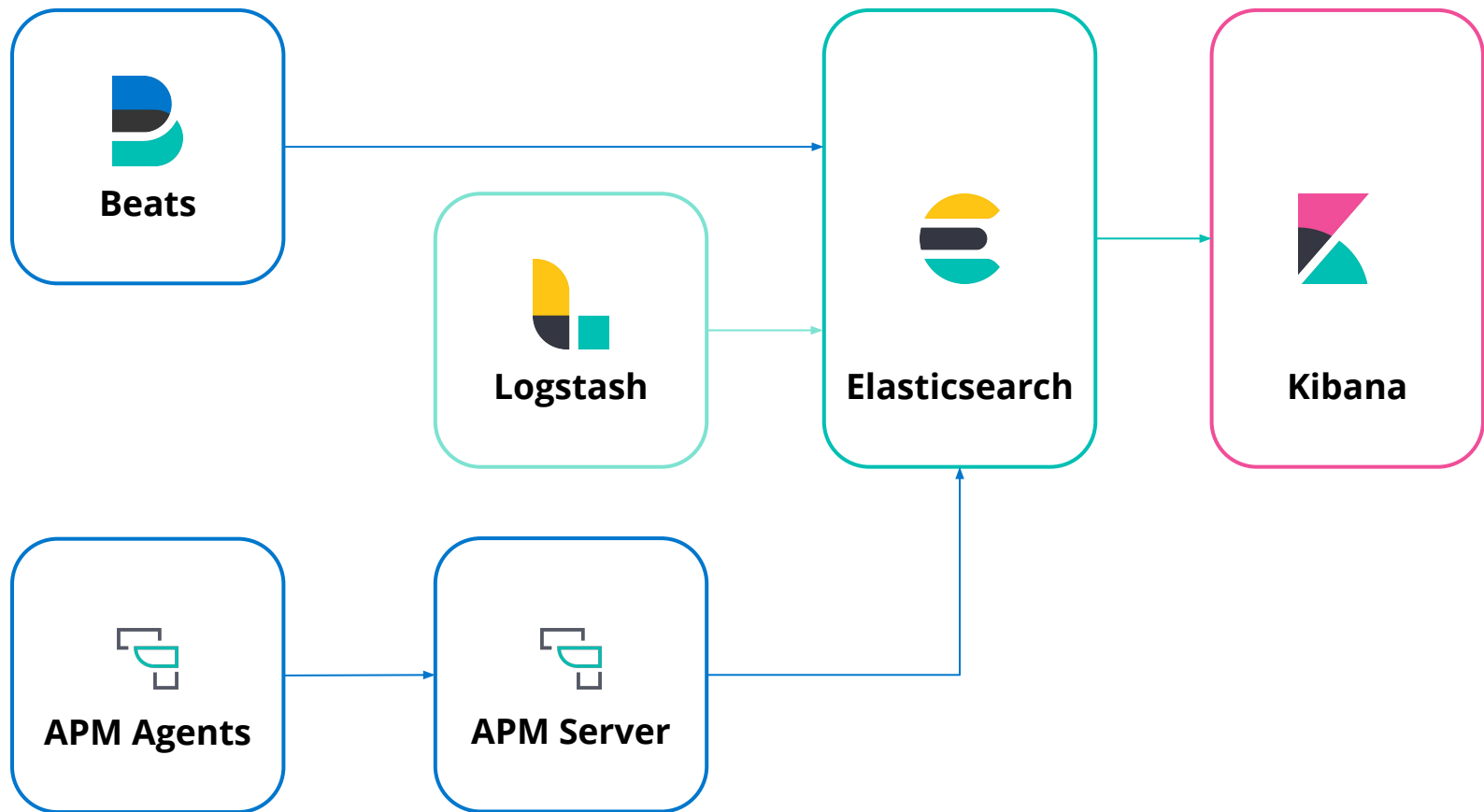
# Workshop de Introdução à Elastic Stack

---

Luiz Guilherme P. Santos  
27/04/2019, Support Engineer, Elastic

# Arquitetura de Elastic Stack

## Componentes



# Elasticsearch

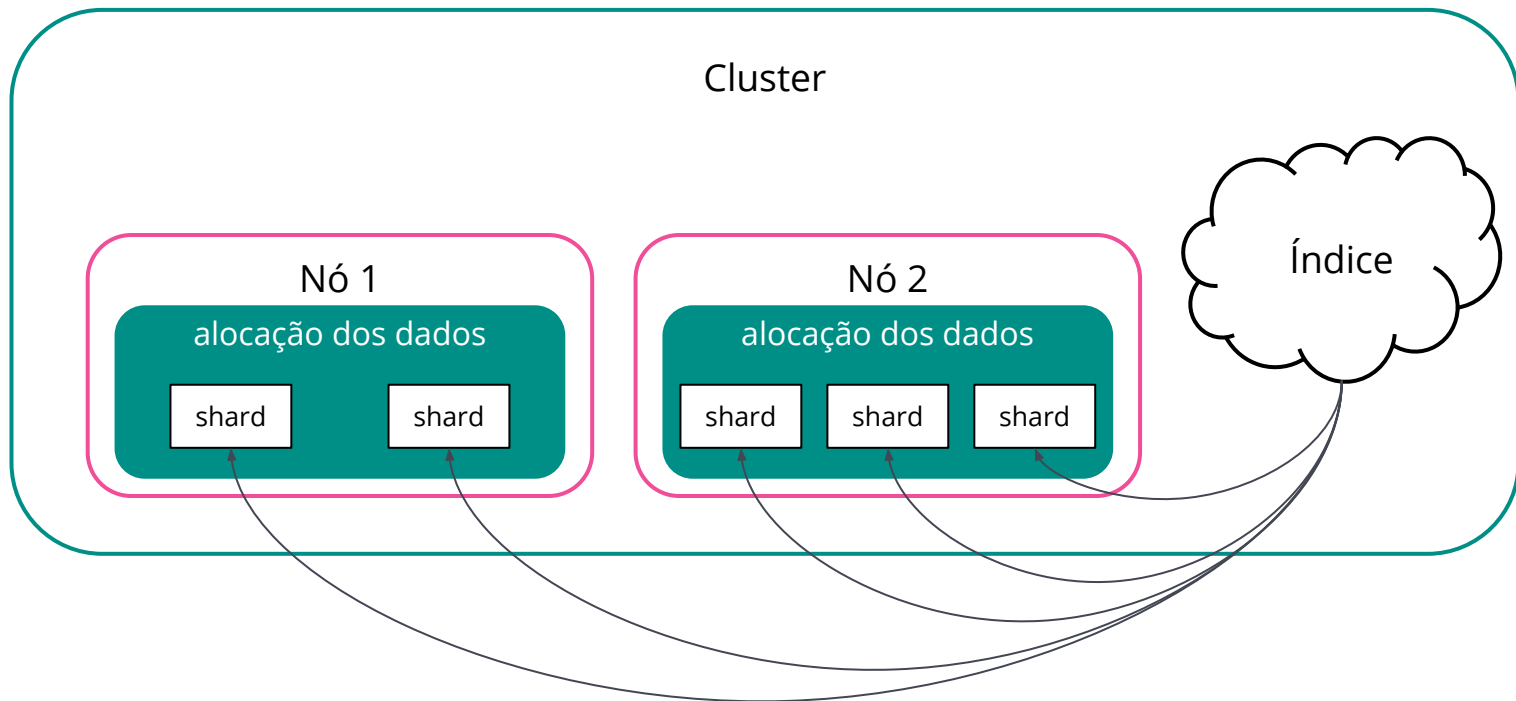
# Elasticsearch

## Principais características

- É um sistema distribuído
- Possui uma interface de busca e analytics RESTful performática
- Escalável, resiliente e alta disponibilidade
- Os tipos de nó são configuráveis
- Existem clientes disponíveis para diversas linguagens de programação como Java, Python, Ruby, .NET, PHP, etc

# Elasticsearch

Conceitos Básicos: cluster, nós, índices, documentos, shards e réplicas



# CRUD

## Indexar um documento

```
PUT workshop/_doc/1
{
  "name" : "Introdução ao Elasticsearch",
  "date" : "2019-04-27T13:00:00"
}
```

```
PUT my_logs/_doc
{
  "timestamp" : "2019-04-27T13:00:00",
  "application" : "nginx"
}
```

# CRUD

## Criar um documento

```
PUT workshop/_doc/1/_create
{
  "name" : "Introdução ao Elasticsearch",
  "date" : "2019-04-27T13:00:00"
}
```

# CRUD

## GET de um documento

```
GET workshop/_doc/1
```



# CRUD

## Atualizar um documento

```
PUT workshop/_doc/1/_update
{
  "doc" : {
    "name" : "Introdução à Elastic Stack"
  }
}
```

# CRUD

Apagar um documento

```
DELETE workshop/_doc/1
```

# CRUD

Buscar documentos

```
GET workshop/_search
```

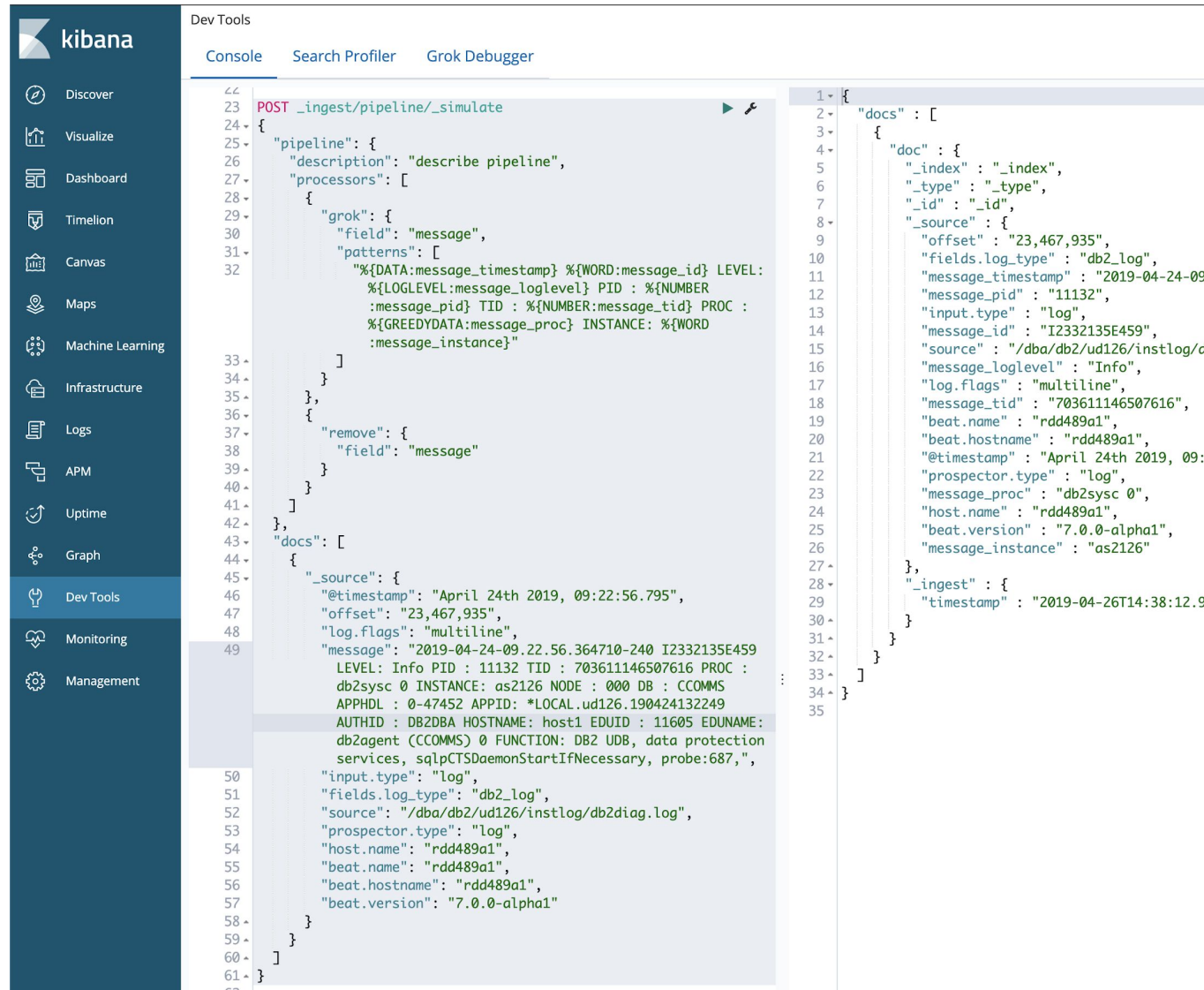
# Kibana

# Kibana

## Principais características

- Visualizar dados cadastrados no Elasticsearch
  - Criar dashboards
    - Third-line bullets are Open Sans 12pt
  - Jobs de machine learning
  - Watchers
  - etc
- Administrar o cluster de Elasticsearch
  - Alterar configurações de índices
  - Política de lifecycle dos índices
  - etc
- Monitorar o cluster de Elasticsearch

# Dev Tools Console



The screenshot shows the Kibana Dev Tools Console with the 'Console' tab selected. The left sidebar contains various navigation options, with 'Dev Tools' highlighted. The main area displays a POST request to the endpoint `POST _ingest/pipeline/_simulate`. The request body is a JSON object defining a pipeline with a 'describe pipeline' processor and a 'grok' processor. The 'grok' processor uses a pattern to parse log messages. The console shows the response, which is a JSON object containing a 'docs' array with one document. The document has fields like '\_index', '\_type', '\_id', '\_source', and '\_ingest'.

```
23 POST _ingest/pipeline/_simulate
24 {
25   "pipeline": {
26     "description": "describe pipeline",
27     "processors": [
28       {
29         "grok": {
30           "field": "message",
31           "patterns": [
32             "%{DATA:message_timestamp} %{WORD:message_id} LEVEL:
              %{LOGLEVEL:message_loglevel} PID : %{NUMBER
              :message_pid} TID : %{NUMBER:message_tid} PROC :
              %{GREEDYDATA:message_proc} INSTANCE: %{WORD
              :message_instance}"
33           ]
34         }
35       },
36       {
37         "remove": {
38           "field": "message"
39         }
40       }
41     ]
42   },
43   "docs": [
44     {
45       "_source": {
46         "@timestamp": "April 24th 2019, 09:22:56.795",
47         "offset": "23,467,935",
48         "log.flags": "multiline",
49         "message": "2019-04-24-09.22.56.364710-240 I2332135E459
              LEVEL: Info PID : 11132 TID : 703611146507616 PROC :
              db2sysc 0 INSTANCE: as2126 NODE : 000 DB : CCOMMS
              APPHDL : 0-47452 APPID: *LOCAL.ud126.190424132249
              AUTHID : DB2DBA HOSTNAME: host1 EDUID : 11605 EDUNAME:
              db2agent (CCOMMS) 0 FUNCTION: DB2 UDB, data protection
              services, sqlpCTS DaemonStartIfNecessary, probe:687,",
              "input.type": "log",
              "fields.log_type": "db2_log",
              "source": "/dba/db2/ud126/instlog/db2diag.log",
              "prospector.type": "log",
              "host.name": "rdd489a1",
              "beat.name": "rdd489a1",
              "beat.hostname": "rdd489a1",
              "beat.version": "7.0.0-alpha1"
50             }
51           ],
52           "fields.log_type": "db2_log",
53           "source": "/dba/db2/ud126/instlog/db2diag.log",
54           "prospector.type": "log",
55           "host.name": "rdd489a1",
56           "beat.name": "rdd489a1",
57           "beat.hostname": "rdd489a1",
58           "beat.version": "7.0.0-alpha1"
59         }
60       }
61     ]
62   }
63 }
```

```
1 {
2   "docs": [
3     {
4       "doc": {
5         "_index": "_index",
6         "_type": "_type",
7         "_id": "_id",
8         "_source": {
9           "offset": "23,467,935",
10          "fields.log_type": "db2_log",
11          "message_timestamp": "2019-04-24-09.22.56.364710-240",
12          "message_pid": "11132",
13          "input.type": "log",
14          "message_id": "I2332135E459",
15          "source": "/dba/db2/ud126/instlog/db2diag.log",
16          "message_loglevel": "Info",
17          "log.flags": "multiline",
18          "message_tid": "703611146507616",
19          "beat.name": "rdd489a1",
20          "beat.hostname": "rdd489a1",
21          "@timestamp": "April 24th 2019, 09:22:56.795",
22          "prospector.type": "log",
23          "message_proc": "db2sysc 0",
24          "host.name": "rdd489a1",
25          "beat.version": "7.0.0-alpha1",
26          "message_instance": "as2126"
27        },
28        "_ingest": {
29          "timestamp": "2019-04-26T14:38:12.9"
30        }
31      }
32    ]
33  }
```

# Beats

# Beats

## Principais características

- Especializados em obter dados
  - Arquivos de logs
  - Métricas de servidores
  - Logs de auditoria (linux e windows)
  - Dados das interfaces de rede
- Otimizados para serem instalados nos servidores
  - Escritos na linguagem GO
  - Executado com binários
- Fáceis de fazer o deploy em diversas arquiteturas
- Vêm com diversos módulos prontos (nginx, apache, etc)



# Metricbeat

# Metricbeat

## Principais características

- Coleta dados do sistema operacional
  - CPU
  - Memória
  - I/O
- Coleta dados de serviços em execução no servidor
  - MySQL
  - MongoDB
  - NGINX
  - Redis

# Filebeat

# Filebeat

## Principais características

- Instalado em todos os servidores que você precisa coletar logs
- Monitora diretórios ou arquivos específicos
- Faz o tail dos arquivos
- Envia os logs extraídos para diversos outputs:
  - Elasticsearch
  - Logstash
  - Kafka
  - Redis

# APM

# APM

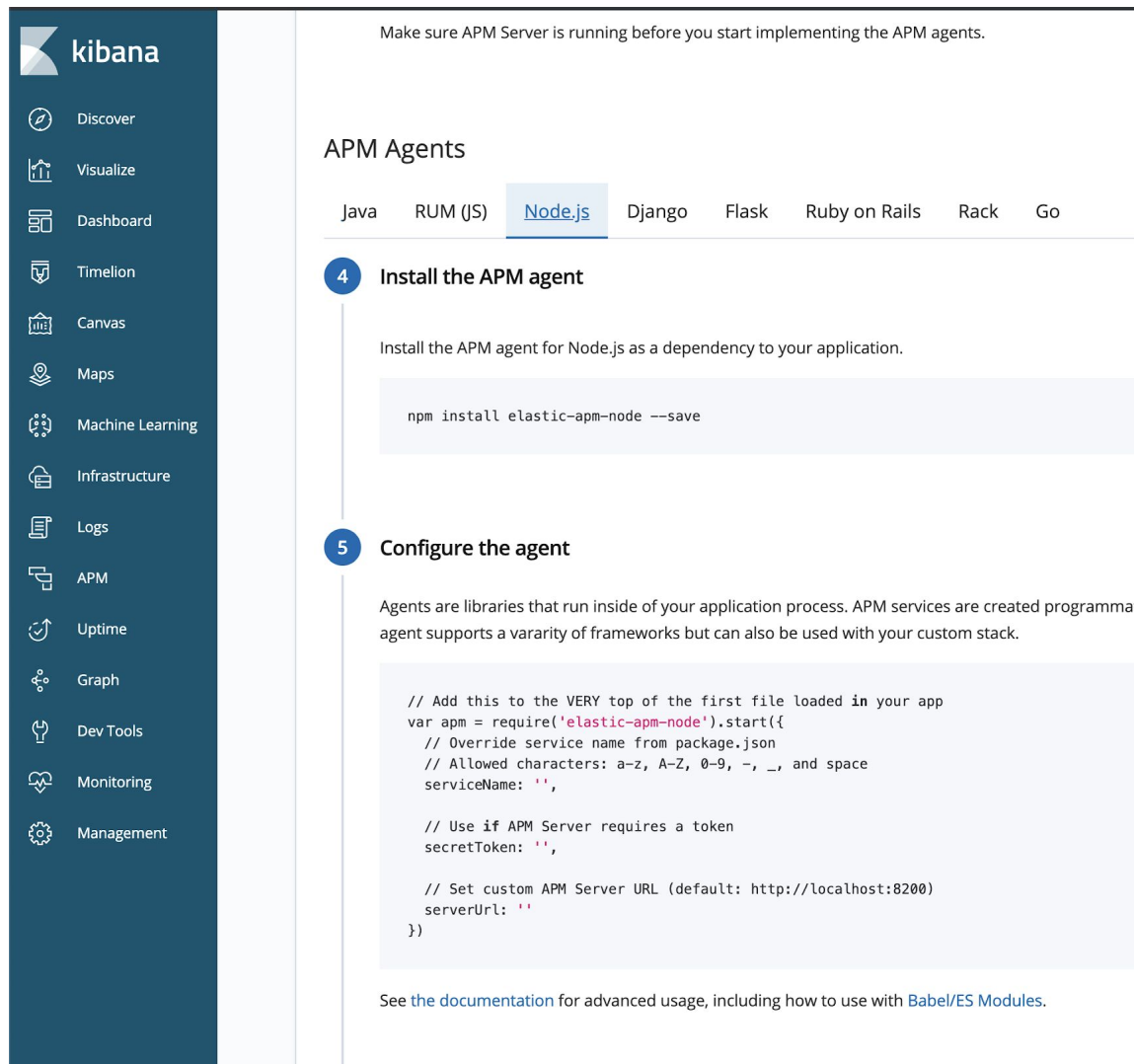
## Principais características

- Faz o track do usuário final interagindo com sua aplicação
- Deixa evidente como cada componente da aplicação interage e evidencia gargalos
- Torna mais simples entender o tempo que cada microserviço gasta
- Possibilita corrigir error da aplicação proativamente
- Aumenta a produtividade das equipes de desenvolvimento

# APM

## Comece a usar em minutos

- Aponte o APM server para ser Elasticsearch
- Adicione o agente ao seu código fonte
- Siga as instruções no Kibana



The screenshot shows the Kibana interface with a sidebar on the left containing various tool icons and labels: Discover, Visualize, Dashboard, Timelion, Canvas, Maps, Machine Learning, Infrastructure, Logs, APM, Uptime, Graph, Dev Tools, Monitoring, and Management. The main content area is titled 'APM Agents' and includes a warning: 'Make sure APM Server is running before you start implementing the APM agents.' Below this, there are tabs for different frameworks: Java, RUM (JS), Node.js (selected), Django, Flask, Ruby on Rails, Rack, and Go. Step 4, 'Install the APM agent', instructs to install the agent for Node.js as a dependency and provides the command: `npm install elastic-apm-node --save`. Step 5, 'Configure the agent', explains that agents are libraries that run inside the application process and provides a code snippet for configuration: 

```
// Add this to the VERY top of the first file loaded in your app
var apm = require('elastic-apm-node').start({
  // Override service name from package.json
  // Allowed characters: a-z, A-Z, 0-9, -, _, and space
  serviceName: '',

  // Use if APM Server requires a token
  secretToken: '',

  // Set custom APM Server URL (default: http://localhost:8200)
  serverUrl: ''
})
```

 At the bottom, it links to the documentation for advanced usage.