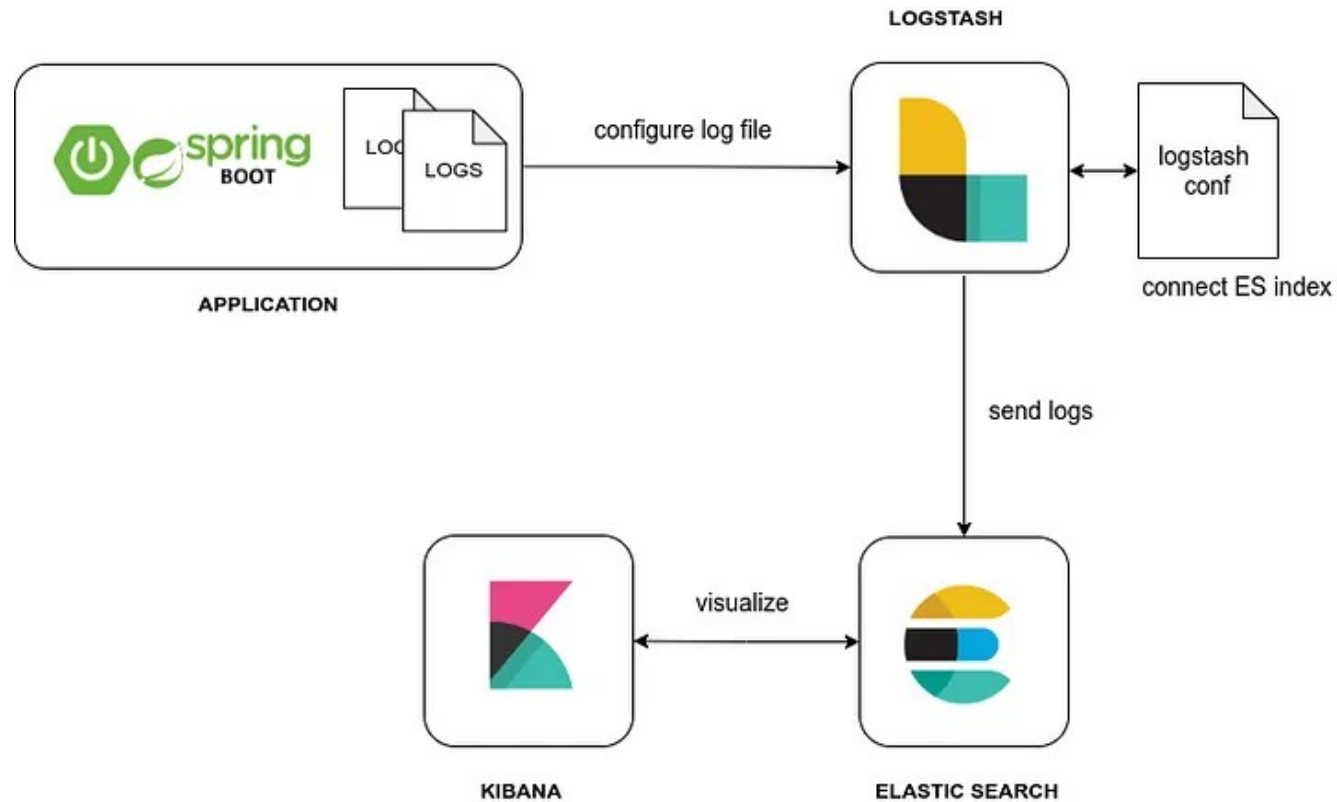


Observabilidade com ELK Stack (ElasticSearch, Logstash e Kibana)

O que é cada um

- ElasticSearch: Um bando de dados nosql para armazenar os logs;
- Logstash: É o alimentador de logs para o ElasticSearch;
- Kibana: UI que exhibe os logs e permite fazer querys e filtros.

Visão Geral

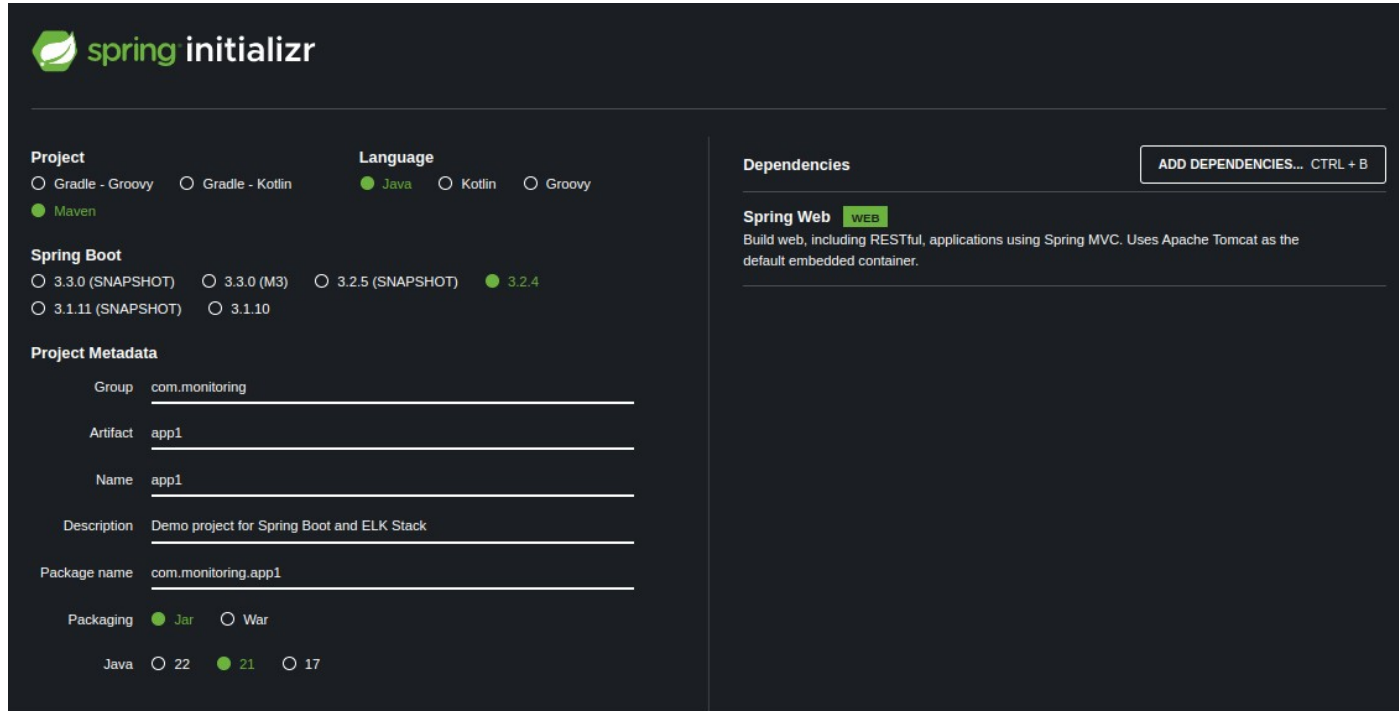


Logs em Aplicação SpringBoot

- Criaremos uma aplicação Java com Springboot que gerará os logs em arquivo texto para ser importado pela ELK stack.

Criar Aplicação Java SpringBoot

- <https://start.spring.io/>



The screenshot shows the Spring Initializr web application interface. The header features the Spring logo and the text "spring initializr". The main content area is divided into several sections:

- Project:** Includes radio buttons for "Gradle - Groovy", "Gradle - Kotlin", "Maven" (selected), and "Language" with options for "Java" (selected), "Kotlin", and "Groovy".
- Spring Boot:** Includes radio buttons for "3.3.0 (SNAPSHOT)", "3.3.0 (M3)", "3.2.5 (SNAPSHOT)", "3.2.4" (selected), "3.1.11 (SNAPSHOT)", and "3.1.10".
- Project Metadata:** Includes input fields for "Group" (com.monitoring), "Artifact" (app1), "Name" (app1), "Description" (Demo project for Spring Boot and ELK Stack), and "Package name" (com.monitoring.app1).
- Packaging:** Includes radio buttons for "Jar" (selected) and "War".
- Java:** Includes radio buttons for "22", "21" (selected), and "17".
- Dependencies:** Includes a button "ADD DEPENDENCIES... CTRL + B" and a section for "Spring Web" with a "WEB" tag and a description: "Build web, including RESTful, applications using Spring MVC. Uses Apache Tomcat as the default embedded container."

Configurar Dependências

- Excluir dependência de logs padrão do springboot-starter-web e adicionar dependência do log4j2

```
<dependency>
  <groupId>org.springframework.boot</groupId>
  <artifactId>spring-boot-starter-web</artifactId>
  <exclusions>
    <exclusion>
      <groupId>org.springframework.boot</groupId>
      <artifactId>spring-boot-starter-logging</artifactId>
    </exclusion>
  </exclusions>
</dependency>
<dependency>
  <groupId>org.springframework.boot</groupId>
  <artifactId>spring-boot-starter-log4j2</artifactId>
</dependency>
```

Código para teste de log

- Criando um controller que gerará logs para nossos testes:

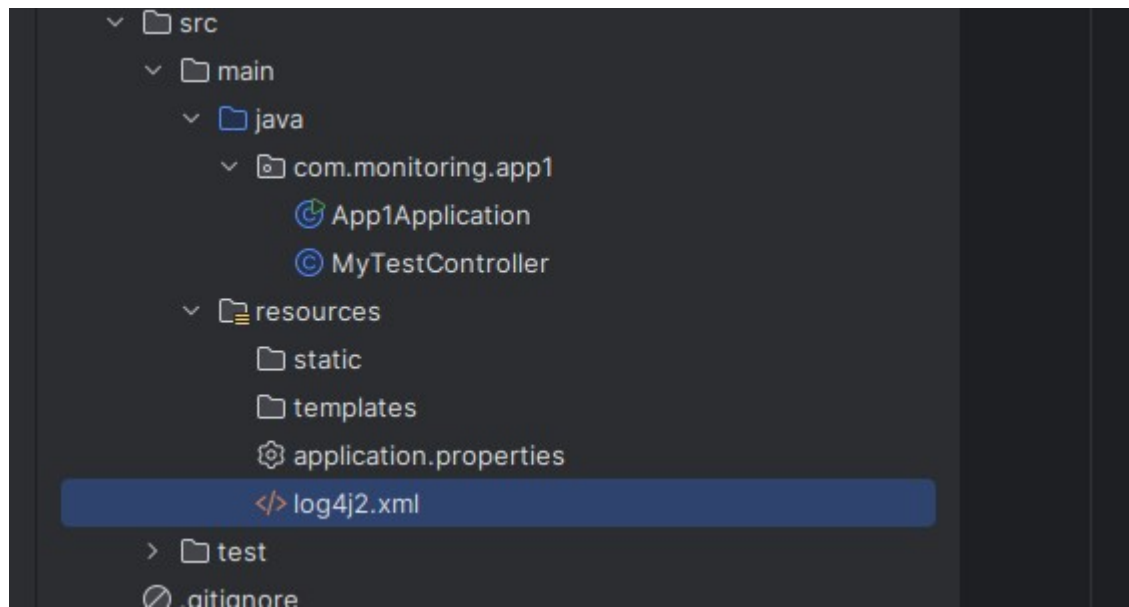
```
@RestController
public class MyTestController {

    private static final Logger logger = LogManager.getLogger(MyTestController.class);

    @GetMapping(path = "/users/{name}")
    public ResponseEntity<String> getUserByName(@PathVariable String name) {
        if (name.equalsIgnoreCase("admin")) {
            logger.info("Access by ADMIN triggered");
            return ResponseEntity.ok("Access Granted to " + name);
        } else {
            logger.error("Access denied for: {}", name);
            return new ResponseEntity<>("Access Denied for " + name), HttpStatus.BAD_REQUEST);
        }
    }
}
```

Configurando a Geração de Logs Pela Aplicação


- Crie um arquivo chamado “log4j2.xml” na pasta resources do projeto:



Configure o arquivo log4j2.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<Configuration status="INFO">
  <Properties>
    <Property name="LOG_PATTERN">
      [%${spring:application.name}] [%-5level] %d{dd-MM-yyyy HH:mm:ss.SSS} [%t] %c{1} - %msg%n
    </Property>
    <Property name="BASE_PATH">/home/renan/estudo/javaELK/log_files</Property>
  </Properties>
  <Appenders>
    <Console name="ConsoleAppender" target="SYSTEM_OUT" follow="true">
      <PatternLayout pattern="%${LOG_PATTERN}"/>
    </Console>
    <RollingFile name="FileAppender" fileName="%${BASE_PATH}/elk_log_app1.log"
      filePattern="%${BASE_PATH}/elk_log_app1-%d{yyyy-MM-dd}.log">
      <PatternLayout>
        <Pattern>%${LOG_PATTERN}</Pattern>
      </PatternLayout>
      <Policies>
        <SizeBasedTriggeringPolicy size="10MB" />
      </Policies>
      <DefaultRolloverStrategy max="10"/>
    </RollingFile>
  </Appenders>
  <Loggers>
    <Logger name="com.monitoring.app1" level="INFO" additivity="false">
      <AppenderRef ref="FileAppender"/>
      <AppenderRef ref="ConsoleAppender"/>
    </Logger>
    <Root level="INFO">
      <AppenderRef ref="FileAppender"/>
    </Root>
  </Loggers>
</Configuration>
```

Execute a aplicação e confira os logs

```
. _ _ _ _ _  
/\ / ___' _ _ _ _ _(\) _ _ _ _ \ \ \ \ \  
( ( )\___ | ' _ | ' _ | ' _ \/_ _ | \ \ \ \ \  
\_ / ___)| |_) | | | | | | |_(| | ) ) ) )  
 ' |____| .__|_| |_|_|_|_\___| | / / / /  
=====|_|=====|___/_/_/_/_/  
:: Spring Boot ::                (v3.2.4)  
  
[app1] [INFO ] 07-04-2024 17:31:40.049 [main] App1Application - Starting App1Application using Java 21.0.2 with PID 14932 (/home/renan/estudo/app1/target/app1.jar)  
[app1] [INFO ] 07-04-2024 17:31:40.053 [main] App1Application - No active profile set, falling back to 1 default profile: "default"  
[app1] [INFO ] 07-04-2024 17:31:40.929 [main] App1Application - Started App1Application in 1.157 seconds (process running for 1.937)  
  
src > main > java > com > monitoring > app1 >  App1Application
```

Confira o arquivo de log

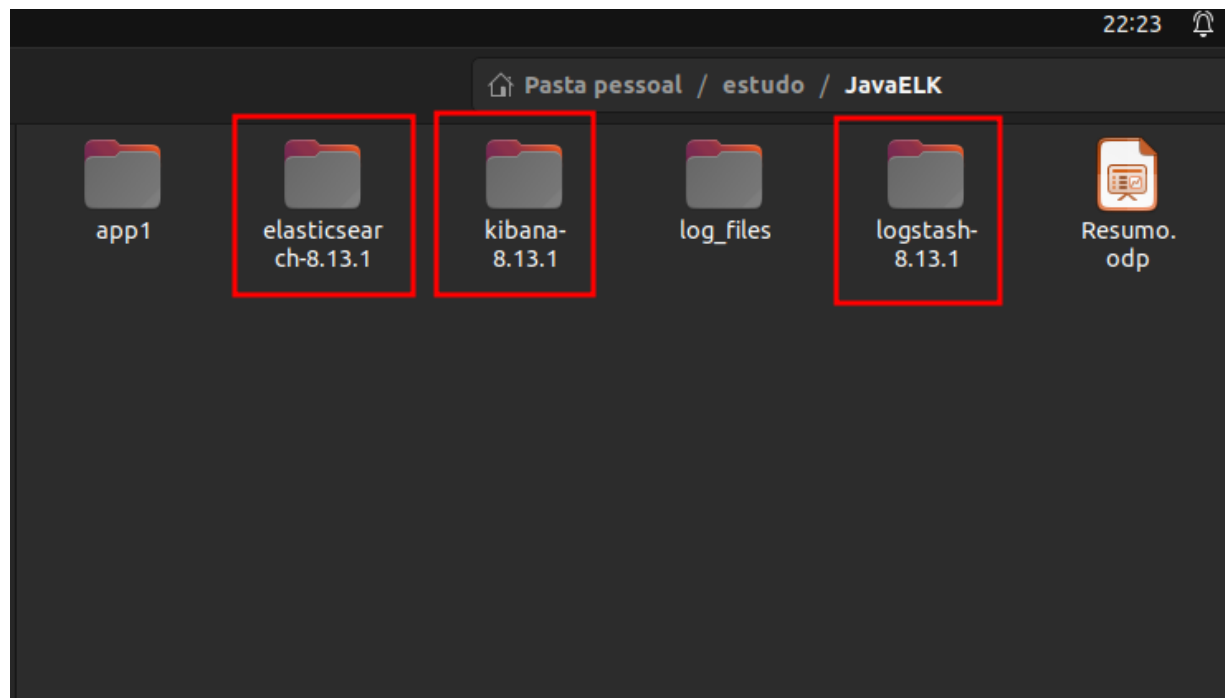
```
renan@renan-Inspiron-3501: ~/estudo/JavaELK/log_files
renan@renan-Inspiron-3501:~$ cd estudo/JavaELK/log_files/
renan@renan-Inspiron-3501:~/estudo/JavaELK/log_files$ cat elk_log_app1.log
[app1] [INFO ] 07-04-2024 17:31:40.049 [main] App1Application - Starting App1Application using Java 21.0.2 with PID 14932 (/home/renan/estudo/JavaELK/JavaELK/app1)
[app1] [INFO ] 07-04-2024 17:31:40.053 [main] App1Application - No active profile set, falling back to 1 default profile: "default"
[app1] [INFO ] 07-04-2024 17:31:40.652 [main] TomcatWebServer - Tomcat initialized with port 8080 (http)
[app1] [INFO ] 07-04-2024 17:31:40.660 [main] Http11NioProtocol - Initializing ProtocolHandler ["http-nio-8080"]
[app1] [INFO ] 07-04-2024 17:31:40.662 [main] StandardService - Starting service [Tomcat]
[app1] [INFO ] 07-04-2024 17:31:40.663 [main] StandardEngine - Starting Servlet engine: [Apache Tomcat/10.1.19]
[app1] [INFO ] 07-04-2024 17:31:40.688 [main] [/] - Initializing Spring embedded WebApplicationContext
[app1] [INFO ] 07-04-2024 17:31:40.689 [main] ServletWebServerApplicationContext - Root WebApplicationContext: initialization completed in 605 ms
[app1] [INFO ] 07-04-2024 17:31:40.915 [main] Http11NioProtocol - Starting ProtocolHandler ["http-nio-8080"]
[app1] [INFO ] 07-04-2024 17:31:40.923 [main] TomcatWebServer - Tomcat started on port 8080 (http) with context path ''
[app1] [INFO ] 07-04-2024 17:31:40.929 [main] App1Application - Started App1Application in 1.157 seconds (process running for 1.937)
renan@renan-Inspiron-3501:~/estudo/JavaELK/log_files$
```

- Pronto, sua aplicação já está funcionando e gerando logs no arquivo.
- Agora vamos para a configuração do ELK Stack.

Obtendo o ELK Stack

- Nesse caso estou utilizando sistema operacional Ubuntu Linux 22.04 e baixar a versão 8.13.1 do ELK.
- Download:
<https://www.elastic.co/downloads/elasticsearch>
<https://www.elastic.co/downloads/logstash>
<https://www.elastic.co/downloads/kibana>
- Extraia o conteúdo compactado para alguma pasta de seu computador.

- No meu caso ficou assim:



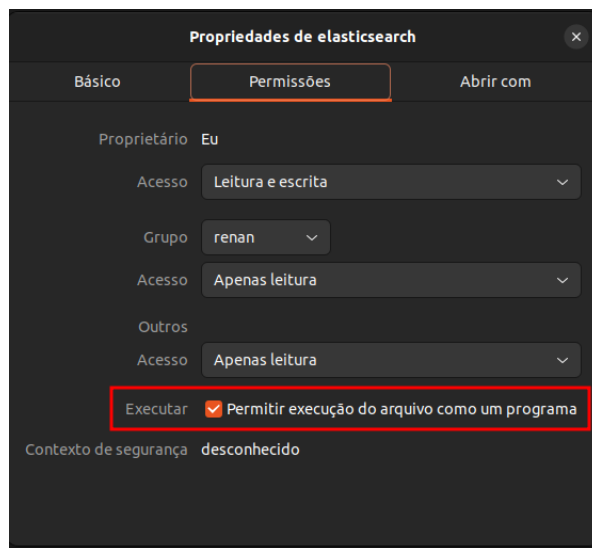
Configurando Elasticsearch para execução local

- Agora vamos configurar para rodar o elasticsearch localmente.
- A versão 8.x vem com definições de segurança default que devemos desabilitar para intuito de estudo, mas que em produção deve-se levar em conta.
- O arquivo de configurações que devemos editar é:
`elasticsearch-8.13.1/config/elasticsearch.yml`

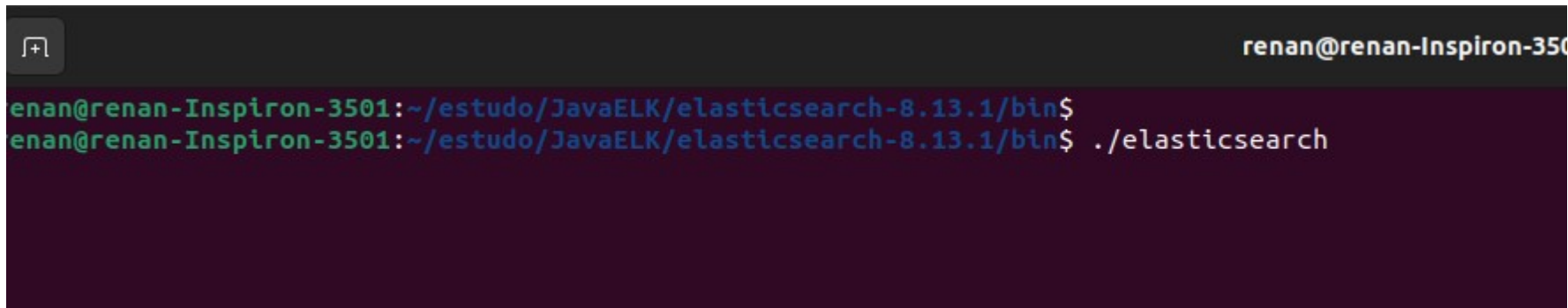
- Descomentar e setar o node.name: node-1
- Descomentar e definir network.host: 0.0.0.0
- Adicione ao final do arquivo as seguintes linhas de configuração:

```
xpack.security.enabled: false  
cluster.initial_master_nodes: ["node-1"]  
http.host: 0.0.0.0
```


- Feito isso, salve o arquivo
- Vá na pasta elasticsearch-8.13.1/bin e veja se o arquivo elasticsearch tem permissão de execução, se não tiver, habilite:



- Ainda na pasta bin, execute: `./elasticsearch`

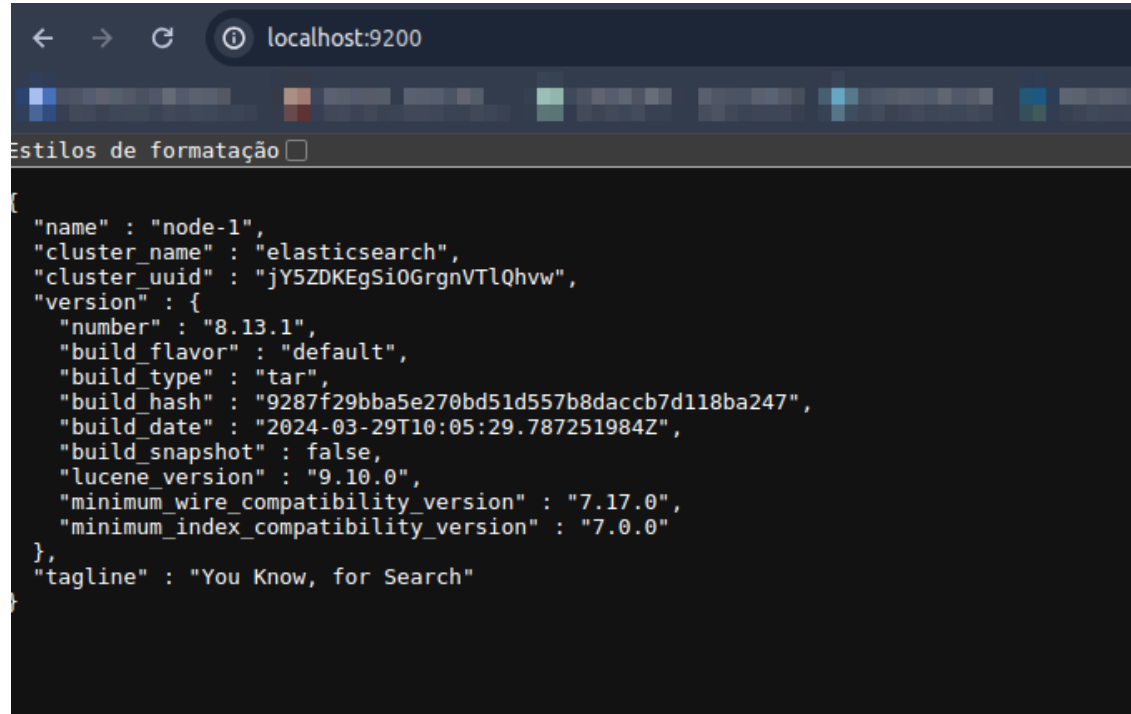
A terminal window with a dark background. The title bar shows a window icon and the text "renan@renan-Inspiron-3501". The terminal content shows the user "enan" at host "renan-Inspiron-3501" in the directory "~/estudo/JavaELK/elasticsearch-8.13.1/bin". The prompt is a green "\$". The command `./elasticsearch` has been entered and is shown on the line following the prompt.

```
renan@renan-Inspiron-3501
enan@renan-Inspiron-3501:~/estudo/JavaELK/elasticsearch-8.13.1/bin$
enan@renan-Inspiron-3501:~/estudo/JavaELK/elasticsearch-8.13.1/bin$ ./elasticsearch
```

- Se tudo deu certo, irá ficar assim ao final, sem nenhuma mensagem de exit com erro

```
renan@renan-Inspiron-3501: ~/estudo/javaELK/elasticsearch-8.13.1/bin
[2024-04-07T23:02:05,631][INFO ][o.e.p.PluginsService ][node-1] loaded module [x-pack-write-load-forecaster]
[2024-04-07T23:02:05,631][INFO ][o.e.p.PluginsService ][node-1] loaded module [search-business-rules]
[2024-04-07T23:02:05,631][INFO ][o.e.p.PluginsService ][node-1] loaded module [elasticsearch]
[2024-04-07T23:02:05,631][INFO ][o.e.p.PluginsService ][node-1] loaded module [ingest-attachment]
[2024-04-07T23:02:05,631][INFO ][o.e.p.PluginsService ][node-1] loaded module [x-pack-apm-data]
[2024-04-07T23:02:05,631][INFO ][o.e.p.PluginsService ][node-1] loaded module [untyped-long]
[2024-04-07T23:02:05,631][INFO ][o.e.p.PluginsService ][node-1] loaded module [x-pack-sql]
[2024-04-07T23:02:05,631][INFO ][o.e.p.PluginsService ][node-1] loaded module [x-pack-async]
[2024-04-07T23:02:05,631][INFO ][o.e.p.PluginsService ][node-1] loaded module [runtime-fields-common]
[2024-04-07T23:02:05,631][INFO ][o.e.p.PluginsService ][node-1] loaded module [vector-tile]
[2024-04-07T23:02:05,631][INFO ][o.e.p.PluginsService ][node-1] loaded module [lang-expression]
[2024-04-07T23:02:05,632][INFO ][o.e.p.PluginsService ][node-1] loaded module [x-pack-eql]
[2024-04-07T23:02:06,112][INFO ][o.e.e.NodeEnvironment ][node-1] using [1] data paths, mounts ["/dev/nvme0n1p2"], net usable_space [179.9gb], net total_space [219.4gb], types [ext4]
[2024-04-07T23:02:06,113][INFO ][o.e.e.NodeEnvironment ][node-1] heap size [5.7gb], compressed ordinary object pointers [true]
[2024-04-07T23:02:06,150][INFO ][o.e.n.Node ][node-1] node name [node-1], node ID [knesDBKuRT-PhrcBCwSUQ], cluster name [elasticsearch], roles [transform, data_hot, ml, data_frozen, ingest, data_cold, data_remote_cluster_client, master, data_warm, data_content]
[2024-04-07T23:02:08,489][INFO ][o.e.f.FeatureService ][node-1] Registered local node features [data_stream.rollover.lazy, desired_node.version.deprecated, features_supported, health.dsl.info, health.extend.ed_repository.indicator, usage_data_tiers.precalculate_stats]
[2024-04-07T23:02:09,055][INFO ][o.e.x.m.p.l.CpplogMessageHandler ][node-1] [controller/24707] Main.cc[123] controller (64 bit): Version 8.13.1 (Build cb13a96dfe8883) Copyright (c) 2024 Elasticsearch BV
[2024-04-07T23:02:09,247][INFO ][o.e.t.a.APM ][node-1] Sending apm metrics is disabled
[2024-04-07T23:02:09,247][INFO ][o.e.t.a.APM ][node-1] Sending apm tracing is disabled
[2024-04-07T23:02:09,266][INFO ][o.e.x.s.Security ][node-1] Security is disabled
[2024-04-07T23:02:09,420][INFO ][o.e.x.w.Watcher ][node-1] Watcher initialized components at 2024-04-08T02:02:09.420Z
[2024-04-07T23:02:09,461][INFO ][o.e.x.p.ProfilingPlugin ][node-1] Profiling is enabled
[2024-04-07T23:02:09,473][INFO ][o.e.x.p.ProfilingPlugin ][node-1] profiling index templates will not be installed or reinstalled
[2024-04-07T23:02:09,478][INFO ][o.e.x.a.APMPlugin ][node-1] APM ingest plugin is disabled
[2024-04-07T23:02:09,703][INFO ][o.e.t.n.NettyAllocator ][node-1] creating NettyAllocator with the following configs: [name=elasticsearch_configured, chunk_size=1mb, suggested_max_allocation_size=1mb, factors={es.unsafe.use.netty.default.chunk.and.page.size=false, glibc.enabled=true, glibc.region.size=4mb}]
[2024-04-07T23:02:09,781][INFO ][o.e.t.r.RecoverySettings ][node-1] using rate limit [40mb] with [default=40mb, read=0b, write=0b, max=0b]
[2024-04-07T23:02:09,815][INFO ][o.e.d.DiscoveryModule ][node-1] using discovery type [multi-node] and head-boss providers [settings]
[2024-04-07T23:02:10,804][INFO ][o.e.n.Node ][node-1] initialized
[2024-04-07T23:02:10,805][INFO ][o.e.n.Node ][node-1] starting ...
[2024-04-07T23:02:10,824][INFO ][o.e.x.s.c.f.PersistentCache ][node-1] persistent cache index loaded
[2024-04-07T23:02:10,824][INFO ][o.e.x.d.i.DeprecationIndexingComponent ][node-1] deprecation component started
[2024-04-07T23:02:10,907][INFO ][o.e.t.TransportService ][node-1] publish_address [192.168.0.167:9300], bound_addresses [:::9300]
[2024-04-07T23:02:11,064][INFO ][o.e.b.BootstrapChecks ][node-1] bound or publishing to a non-loopback address, enforcing bootstrap checks
[2024-04-07T23:02:11,066][WARN ][o.e.c.c.ClusterBootstrapService ][node-1] this node is locked into cluster UUID [j5SZDKEg5UGrGNvLQhw] but [cluster.initial_master_nodes] is set to [node-1]; remove this settin g to avoid possible data loss caused by subsequent cluster bootstrap attempts; for further information see https://www.elastic.co/guide/en/elasticsearch/reference/8.13/important-settings.html#initial_master_node
[2024-04-07T23:02:11,153][INFO ][o.e.c.s.MasterService ][node-1] elected-as-master ([1] nodes joined in term 3)[_FINISH_ELECTION_, {node-1}[knesDBKuRT-PhrcBCwSUQ](2_czAX0RRjSGCnEF6vc1A)(node-1)[192.168.0.167][192.168.0.167:9300][cdfhlmrstw][8.13.1]{7000099-8503000} completing election], term: 3, version: 43, delta: master node changed [previous [], current [node-1][knesDBKuRT-PhrcBCwSUQ](2_czAX0RRjSGCnEF6vc1A)(node-1)[192.168.0.167:9300][cdfhlmrstw][8.13.1]{7000099-8503000}]]
[2024-04-07T23:02:11,190][INFO ][o.e.c.s.ClusterApplierService ][node-1] master node changed [previous [], current [node-1][knesDBKuRT-PhrcBCwSUQ](2_czAX0RRjSGCnEF6vc1A)(node-1)[192.168.0.167:9300][cdfhlmrstw][8.13.1]{7000099-8503000}]], term: 3, version: 43, reason: Publication[term=3, version=43]
[2024-04-07T23:02:11,213][INFO ][o.e.c.f.AbstractFileWatchingService ][node-1] starting file watcher ...
[2024-04-07T23:02:11,215][INFO ][o.e.c.f.AbstractFileWatchingService ][node-1] file settings service up and running [tid=73]
[2024-04-07T23:02:11,223][INFO ][o.e.c.c.NodeJoinExecutor ][node-1] node-join: [node-1][knesDBKuRT-PhrcBCwSUQ](2_czAX0RRjSGCnEF6vc1A)(node-1)[192.168.0.167][192.168.0.167:9300][cdfhlmrstw][8.13.1]{7000099-8503000}] with reason [completing election]
[2024-04-07T23:02:11,224][INFO ][o.e.h.AbstractHttpServerTransport ][node-1] publish_address [192.168.0.167:9200], bound_addresses [:::9200]
[2024-04-07T23:02:11,235][INFO ][o.e.n.Node ][node-1] started [node-1][knesDBKuRT-PhrcBCwSUQ](2_czAX0RRjSGCnEF6vc1A)(node-1)[192.168.0.167][192.168.0.167:9300][cdfhlmrstw][8.13.1]{7000099-8503000}[ml.config_version=12.0.0, ml.max_jvm_size=4018143232, ml.allocated_processors_double=0.0, ml.allocated_processors=8, ml.machine_memory=8032481280, transform.config_version=10.0.0, xpack.installed=true]
[2024-04-07T23:02:11,588][INFO ][o.e.l.ClusterStateLicenseService ][node-1] license [c0f893f-3fcc-4261-87d5-5d7a92c134d9] node [basic] - valid
[2024-04-07T23:02:11,591][INFO ][o.e.g.GatewayService ][node-1] recovered [0] indices into cluster state
[2024-04-07T23:02:11,630][INFO ][o.e.h.n.s.HealthNodeTaskExecutor ][node-1] Node [node-1][knesDBKuRT-PhrcBCwSUQ] is selected as the current health node.
```

- Teste o healthcheck do elasticsearch acessando pelo browser:



A screenshot of a web browser window with the address bar showing 'localhost:9200'. The browser's developer tools are open, displaying a JSON response from the Elasticsearch healthcheck endpoint. The response is a JSON object containing node information, cluster details, and version data.

```
{
  "name" : "node-1",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "jY5ZDKEgSi0GrgrnVTlQhvw",
  "version" : {
    "number" : "8.13.1",
    "build_flavor" : "default",
    "build_type" : "tar",
    "build_hash" : "9287f29bba5e270bd51d557b8daccb7d118ba247",
    "build_date" : "2024-03-29T10:05:29.787251984Z",
    "build_snapshot" : false,
    "lucene_version" : "9.10.0",
    "minimum_wire_compatibility_version" : "7.17.0",
    "minimum_index_compatibility_version" : "7.0.0"
  },
  "tagline" : "You Know, for Search"
}
```

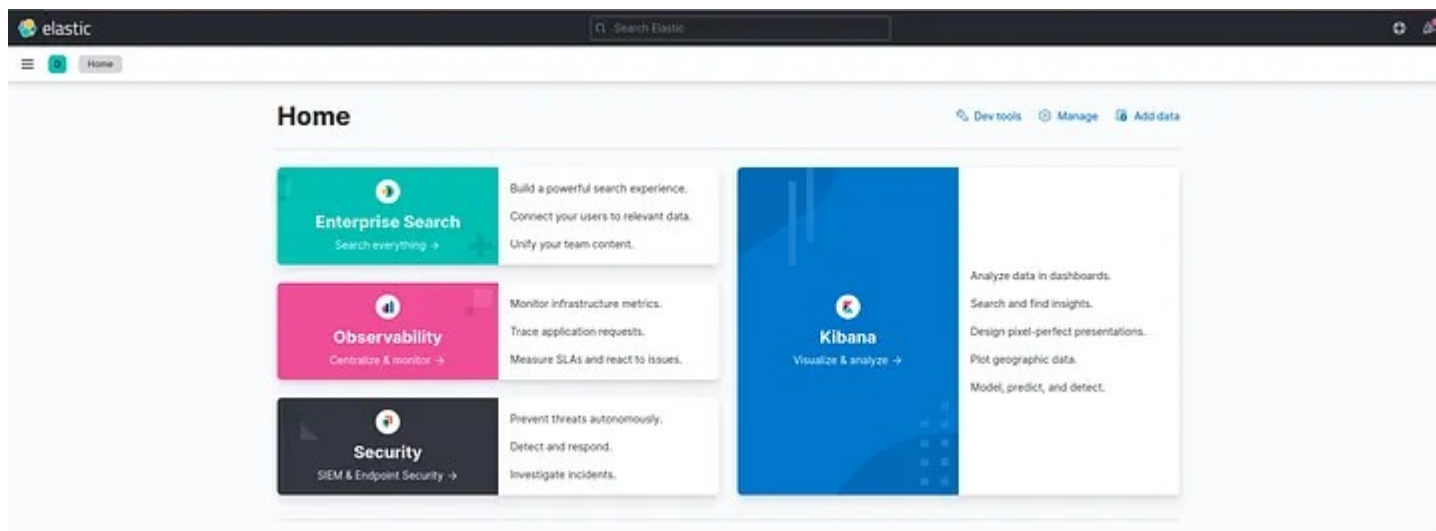
Iniciando o Kibana

- Vamos iniciar agora o Kibana, que é a interface onde vamos fazer as consultas aos logs coletados.
- Em kibana-8.13.1/bin, verifique se o arquivo kibana tem permissão de execução igual fizemos no arquivo elasticsearch e execute como ./kibana

- Se tudo correu bem, ao final verá uma mensagem assim:

```
[2024-04-07T23:09:24.567-03:00][INFO ][plugins.ecsDataQualityDashboard] Installing index template .kibana-data-quality-dashboard-resul
[2024-04-07T23:09:24.579-03:00][INFO ][plugins.observability] SLO index template found with version [3]
[2024-04-07T23:09:24.591-03:00][INFO ][plugins.observability] SLO index template found with version [3]
[2024-04-07T23:09:24.635-03:00][INFO ][plugins.fleet] Agent policies updated by license change: []
[2024-04-07T23:09:24.686-03:00][INFO ][plugins.ecsDataQualityDashboard] Updating data streams - .kibana-data-quality-dashboard-results
[2024-04-07T23:09:25.047-03:00][INFO ][plugins.observability] SLO ingest pipeline found with version [3]
[2024-04-07T23:09:25.199-03:00][INFO ][plugins.screenshotting.chromium] Browser executable: /home/renan/estudo/JavaELK/kibana-8.13.1/n
less_shell
[2024-04-07T23:09:25.357-03:00][INFO ][plugins.observabilityAIAssistant.service] Successfully set up index assets
[2024-04-07T23:09:28.864-03:00][INFO ][status.plugins.alerting] alerting plugin is now available: Alerting is (probably) ready
[2024-04-07T23:09:28.864-03:00][INFO ][status.plugins.fleet] fleet plugin is now available: Fleet is setting up
[2024-04-07T23:09:28.864-03:00][INFO ][status.plugins.licensing] licensing plugin is now available: License fetched
[2024-04-07T23:09:28.864-03:00][INFO ][status.plugins.taskManager] taskManager plugin is now available: Task Manager is healthy
[2024-04-07T23:09:28.945-03:00][INFO ][status] Kibana is now available
```

- Para testar, vá no browser e entre em “<http://localhost:5601/>”
Deverá ver a tela inicial assim:



Logstash

- Temos então o elasticsearch para armazenar os logs e o kibana para exibi-los, falta agora alimentar o elasticsearch com os logs que queremos da aplicação!

Configurando o Logstash

- Vá em `logstash-8.13.1/config/` crie um arquivo chamado `logstash.conf` e coloque o seguinte conteúdo:

```
input {  
  file {  
    path => "/home/renan/estudo/JavaELK/log_files/elk_log_app1.log"  
    start_position => "beginning"  
  }  
}  
output {  
  stdout {  
    codec => rubydebug  
  }  
  elasticsearch {  
    hosts => ["localhost:9200"]  
    index => "app1log"  
  }  
}
```

Executando o Logstash

- Vá para logstash-8.13.1/bin e execute o arquivo ./logstash da seguinte forma:
./logstash -f /home/renan/estudo/JavaELK/logstash-8.13.1/config/logstash.conf
* Substitua o caminho “/home/renan/estudo/JavaELK” pelo caminho em sua máquina

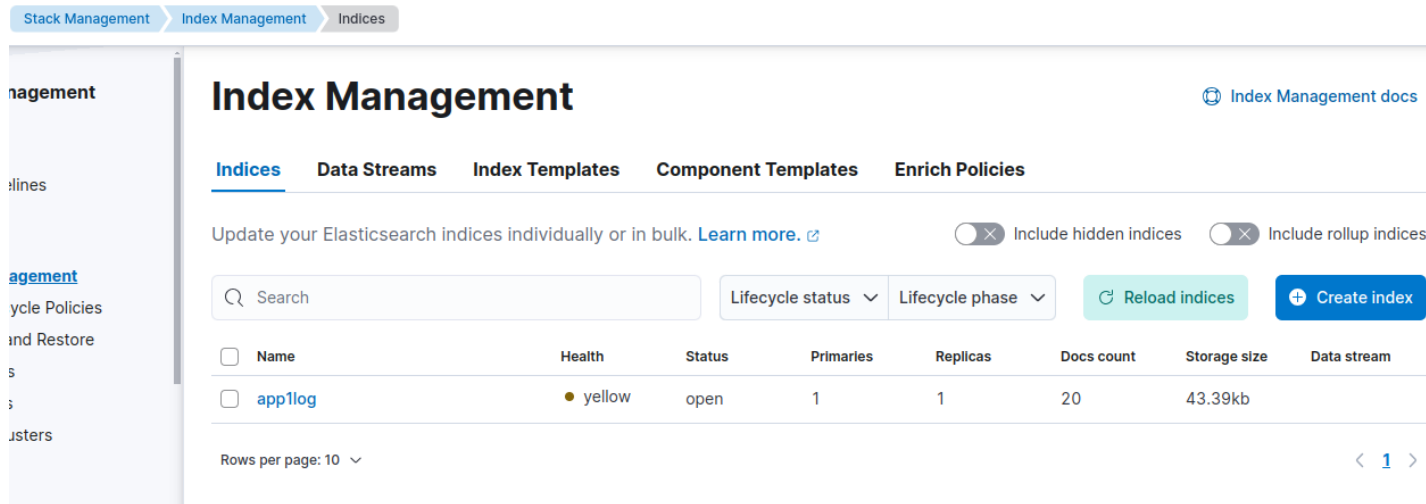
Conferindo a execução do Logstash

Se tudo deu certo, seu terminal ficará assim, aparecendo alguns log que já foram gerados pela inicialização da aplicação:

```
{
  "@timestamp" => 2024-04-08T03:21:40.709033533Z,
  "@version" => "1",
  "event" => {
    "original" => "[app1] [INFO ] 07-04-2024 23:49:31.340 [main] StandardService - Starting service [Tomcat]"
  },
  "log" => {
    "file" => {
      "path" => "/home/renan/estudo/JavaELK/log_files/elk_log_appl.log"
    }
  },
  "message" => "[app1] [INFO ] 07-04-2024 23:49:31.340 [main] StandardService - Starting service [Tomcat]",
  "host" => {
    "name" => "renan-Inspiron-3501"
  }
}
{
  "@timestamp" => 2024-04-08T03:21:40.710427563Z,
  "@version" => "1",
  "event" => {
    "original" => "[app1] [INFO ] 07-04-2024 23:53:13.929 [http-nio-8080-exec-2] DispatcherServlet - Initializing Servlet 'dispatcherServlet'"
  },
  "log" => {
    "file" => {
      "path" => "/home/renan/estudo/JavaELK/log_files/elk_log_appl.log"
    }
  },
  "message" => "[app1] [INFO ] 07-04-2024 23:53:13.929 [http-nio-8080-exec-2] DispatcherServlet - Initializing Servlet 'dispatcherServlet'",
  "host" => {
    "name" => "renan-Inspiron-3501"
  }
}
{
  "@timestamp" => 2024-04-08T03:21:40.709573127Z,
  "@version" => "1",
  "event" => {
    "original" => "[app1] [INFO ] 07-04-2024 23:49:31.369 [main] ServletWebServerApplicationContext - Root WebApplicationContext: initialization completed in 669 ms"
  },
  "log" => {
    "file" => {
      "path" => "/home/renan/estudo/JavaELK/log_files/elk_log_appl.log"
    }
  },
  "message" => "[app1] [INFO ] 07-04-2024 23:49:31.369 [main] ServletWebServerApplicationContext - Root WebApplicationContext: initialization completed in 669 ms",
  "host" => {
    "name" => "renan-Inspiron-3501"
  }
}
```

Configurando a UI do Kibana

- No Kibana, se formos no menu lateral, em Management, Stack Management e Index Management(Submenu Data) vamos ver que já detectou o índice de logs alimentado pelo logstash:

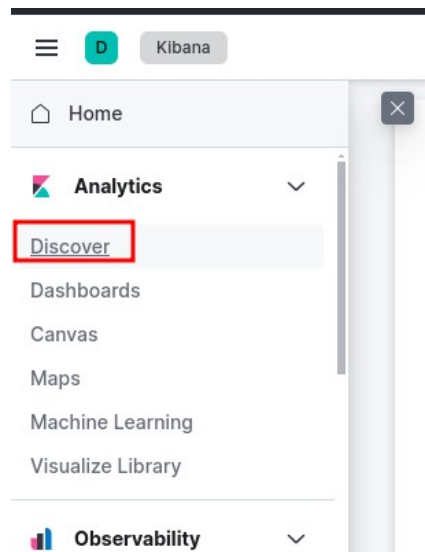


The screenshot shows the Kibana Index Management interface. The breadcrumb navigation at the top indicates the path: Stack Management > Index Management > Indices. The left sidebar shows the 'Management' section expanded, with 'Index Management' selected. The main content area is titled 'Index Management' and includes a link to 'Index Management docs'. Below the title are tabs for 'Indices', 'Data Streams', 'Index Templates', 'Component Templates', and 'Enrich Policies'. A message states: 'Update your Elasticsearch indices individually or in bulk. [Learn more.](#)' followed by toggle switches for 'Include hidden indices' and 'Include rollup indices'. There is a search bar, dropdowns for 'Lifecycle status' and 'Lifecycle phase', and buttons for 'Reload indices' and 'Create index'. A table lists the indices:

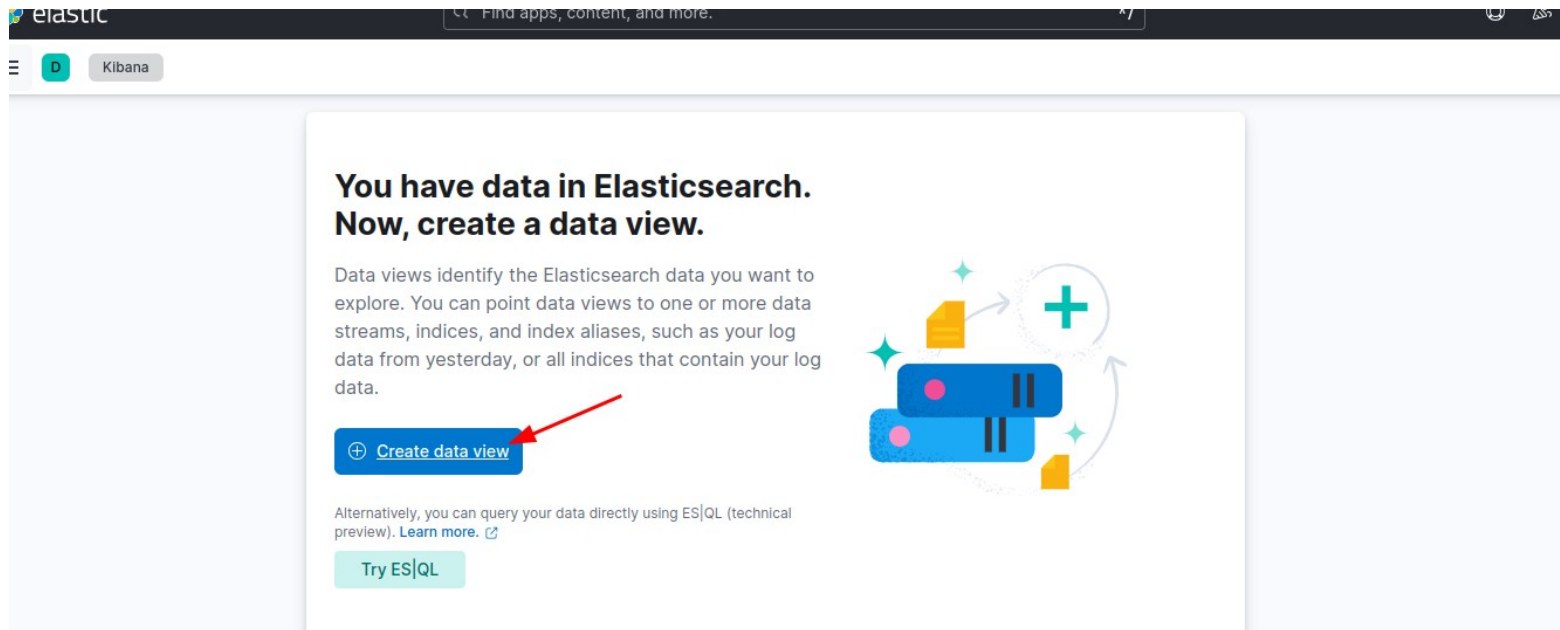
<input type="checkbox"/>	Name	Health	Status	Primaries	Replicas	Docs count	Storage size	Data stream
<input type="checkbox"/>	app1log	● yellow	open	1	1	20	43.39kb	

At the bottom, it shows 'Rows per page: 10' and a pagination control for page 1.

- No menu lateral, vá em Analytics e Discover



- Clique em Create Data View



- Preencha o nome do data view e o índice que deve buscar e depois clique em salvar mais abaixo na tela:

Create data view

Name
app1log

Index pattern
app1log*

Timestamp field
@timestamp

Select a timestamp field for use with the global time filter.

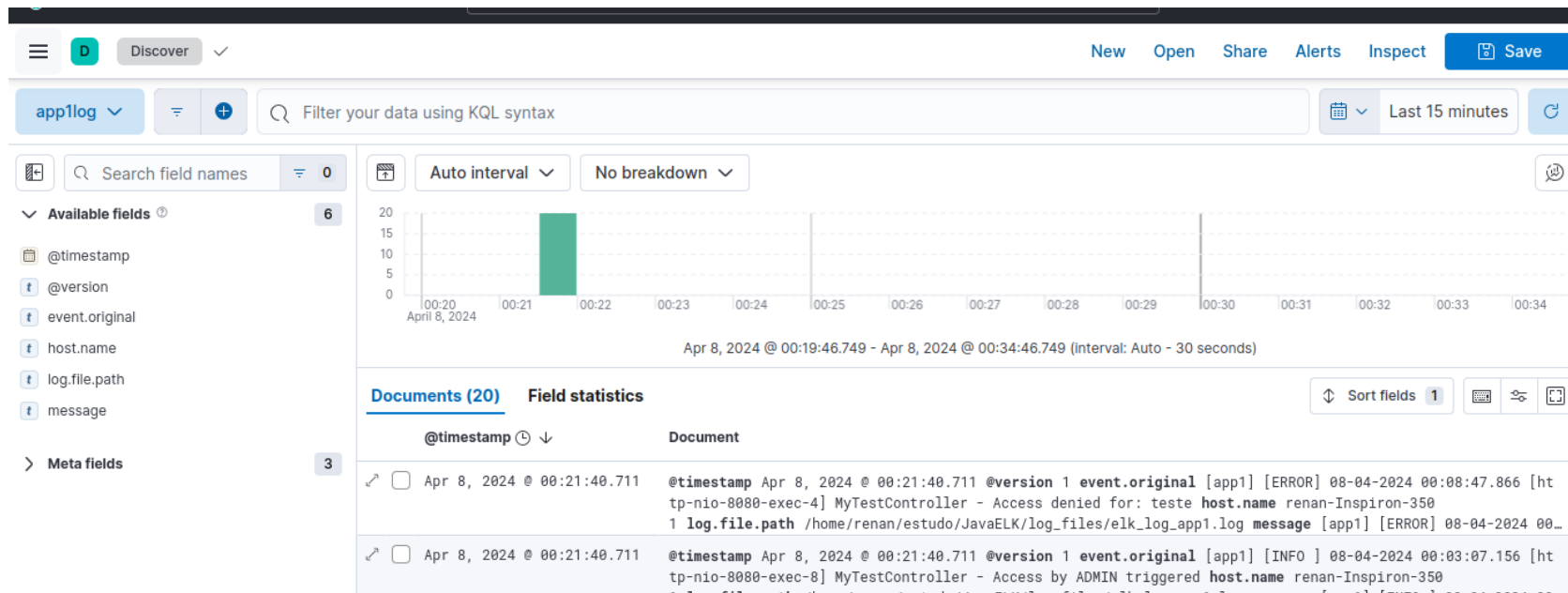
[Show advanced settings](#)

✓ Your index pattern matches 1 source.

All sources	Matching sources
app1log	Index

Rows per page: 10

- Agora, indo no menu lateral em Analytics, Discover já temos a exibição dos logs para este índice criado:



Filtrando logs

- Requisição para testar o filtro de logs:

The screenshot shows a web browser's developer tools interface. At the top, a GET request to `localhost:8080/users/jose` is displayed. Below the request bar, the 'Params' tab is selected, showing a table with two columns: 'Key' and 'Value'. The table is currently empty. Below the 'Params' tab, the 'Body' tab is selected, showing a status of '400 Bad Request' with a time of '19 ms' and a size of '166 B'. The 'Body' tab also shows a 'Text' dropdown menu and a 'Pretty' button. The response body is displayed as 'Access Denied for jose'.

Key	Value	Description
Key	Value	Description

Status: 400 Bad Request Time: 19 ms Size: 166 B

1 Access Denied for jose

- Para filtrar, use a barra acima para o texto que deseja e o tempo de log

