4·Linux Open Software Specialists™

# CERTIFICADO

*Certificate*

## Kauê Renan De Moraes Bortolotti

Concluiu seus estudos no curso **815 - Especialista Elastic Stack - Elasticsearch, Logstash, Beats e Kibana - AC** ministrado pela empresa 4Linux e cumprindo a carga horária de 40 horas.

3 de julho de 2023



**RODOLFO** GOBBI

DIRETOR GERAL

Para validar a autenticidade deste certificado acesse aia.4linux.com.br/admin/tool/certificate/ e digite o código: 5068651826KR

# Ementa de Curso

Kauê Renan De Moraes Bortolotti
Concluiu seus estudos no curso **815 - Especialista Elastic Stack - Elasticsearch, Logstash, Beats e Kibana - AC** ministrado pela empresa 4Linux e cumprindo a carga horária de 40 horas.
3 de julho de 2023

A autenticidade deste documento pode ser verificado em aia.4linux.com.br/admin/tool/certificate/ digitando o código 5068651826KR

---

**Conteúdo Programático**

**Parte 1 - Introdução ao Elastic Stack**

**Introdução a Stack Elatic**

- História, evolução e futuro
- Produtos da Stack Elastic: Elasticsearch, Logstash, Beats e Kibana
- Comparação entre versões OSS, Basic e Enterprise
- Escalabilidade and resiliencia
- Conceito de documentos, indices, busca e agregações

**Iniciando seu primeiro Cluster Elasticsearch Enterprise**

**Instalação e Configuração do Elasticsearch**

- Configuração de Sistema Operacional
- Entendendo os aquivos de configuração elasticsearch.yml, jvm.options e logs
- Ferramentas de linha comando do Elasticsearch
- Iniciando o cluster Elasticsearch
- API de operações básicas
- Operações de inserção, alteração, busca, deleção e processamento de batch
- Explorando os Dados: Query Language, Searches, Filters e Aggregations
- API de monitoramento _CAT
- Adicionado novos nós no cluster
- Tipos de nós de Elasticsearch e sua aplicabilidade

**Indices, Shards e Réplicas**

**Conceito Indice Invertido e Apache Lucene**

- Entendendo a estrutura e configuração do Índice
- Analogia entre um banco de dados tradicional e o indice Elasticsearch
- Settings
- Estrutura no filesystem do índice Elasticsearch
- Aliases de Indice
- Entendendo o Mapping e a sua importância
- Meta Fields
- Fields datatypes
- Parâmetros de mapeamento
- Mapeamento dinâmico

**Entendendo os Analisadores e sua importância**

- O que é um analisador e seu funcionamento
- Testando um analisador
- Analizers, Tokenizers, Token Filters e Character Filters

**Shard, réplicas e sua estrutura**

- O que é um Shard e porque fragmentar
- Shard primário e réplicas
- Distribuição de documentos nos Shards
- Size, Quantidade e limitações do Shard

**Alocação e roteamento de Shards**

- Em nível de cluster

**Baseado em Disco**

- Baseado em posição de Rack
- Baseado em Filtros

**Uma palavra sobre escalabilidade e Capacity Planning**

- Horizontal X Vertical
- Réplicas X Shards X Tamanho da Shards
- CPU X Memória X Disco X Tamanho do Cluster

**Como estimar a minha capacidade?**

- Volumetria X tamanho médio/dia X tempo de retenção
- Perfil do cliente: Ingestão, Consulta ou Ambos?

**Parte 2 - Ingestão de Dados**

**Ingestão de dados no Elasticsearch**

- Diferenças entre o Ingest Node X Beats X Logstash

**Ingest Node**

- Pipelines
- API do Ingest
- Condicionais em pipelines
- Processors

**Beats**

- O que é o Beats
- Tipos de Beats

**Instalando e Configurando um Beat(Metricbeat e Filebeat)**

**Entendendo os arquivos de configuração do Beat**

- Habilitando e configurando Módulos do Beat
- Ingestão de logs com Filebeat
- Throubleshoting e Debug do Beat

**Logstash**

- O que é o Logstash e como ele funciona

**Instalando e configurando o Logstash**

- Entendendo os arquivos de configuração do Logstash

**Pipelines e Multiple Pipelines**

- Plugins do Logstash
- Inputs - Plugins mais usuais
- Beats, file, http, jdbc, stdin, tcp, udp e twitter
- Filters - Plugins mais usuais
- date, dissect, grok, geoip, mutate, extractnumber, translate, codec multiline e kv
- Outputs - Plugins mais usuais
- elasticsearch, file, stdout
- Logstash em linha de comando
- Debug e Throubleshoting do Logstash

**Parte 3 - Visualização e Análise de Dados**

**Kibana para visualização de dados**

- O que é o Kibana
- Instalando e configurando o Kibana
- Entendendo o arquivo kibana.yml

**Kibana e suas aplicações**

- Discover, visualize, Dashboard, Maps, Infraestructure, Logs, Uptime, DevTools, Monitoring e Management
- Configurando um Indice no Kibana
- Buscando e Analisando dados com Discover
- Criando gráficos e métricas com Visualize
- Criando Dashboards
- Analisando logs com Logs
- UpTime
- Dev Tools
- Monitoramento da Stack
- Gerenciamento da Stack
- Kibana Spaces

**Parte 4 - Administrando e Monitorando o Elastic Stack**

**Segurança**

- Modulo Security
- Ativando e Configurando a Segurança no Cluster Elasticsearch
- Criando Usuários e Perfis no Elasticsearch
- Encriptando a comunicação entre os nós do Cluster

**Monitoramento e Alertas**

- Monitoramento
- Ativando e configurando o monitoramento do Cluster Elasticsearch
- Coletando dados do Elasticsearch
- Coletando dados do Logstash
- Coletando dados do Beats
- Coletando dados do Kibana

**Backup/Restore**

- Shapshot e Restore
- Criando repositórios
- Executando Snapshot e Restore
- Monitorando o progresso do Snapshots e Restore

**Lifecycle Management**

- Gerenciando o Ciclo de vida com ILM
- Policies e Actions do ILM

**Parte 5 - Cenários com Elastic Stack**

**Ingestão de logs com Elatic Stack**

- Coletando logs de serviços e aplicações web

**Indexando e enriquecendo banco de dados com Elastic Stack**

- Coletando dados de banco de dados
- Criando visões analíticas dos dados

**Indexando e analisando de sentimento do Twiter com Elastic Stack**

- Coletando Tweets e indexando no Elasticsearch