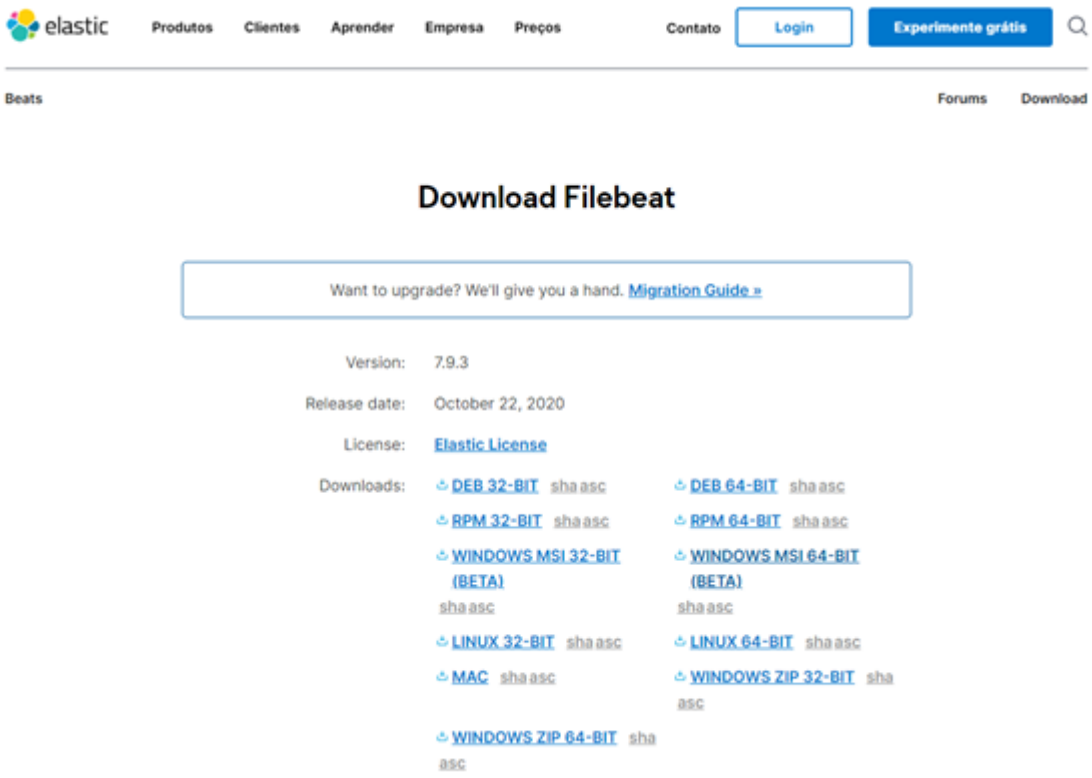
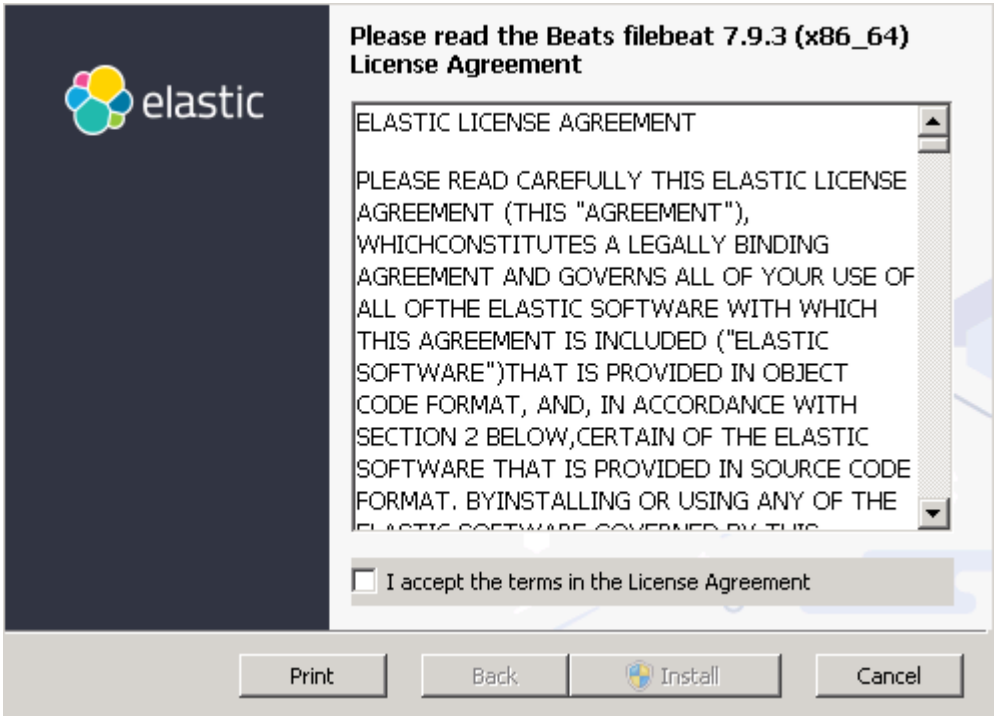
Olá meus caros hoje vou passar um overview de como instalar o novo Filebeat .msi no Windows de forma bem simples, let’s go.

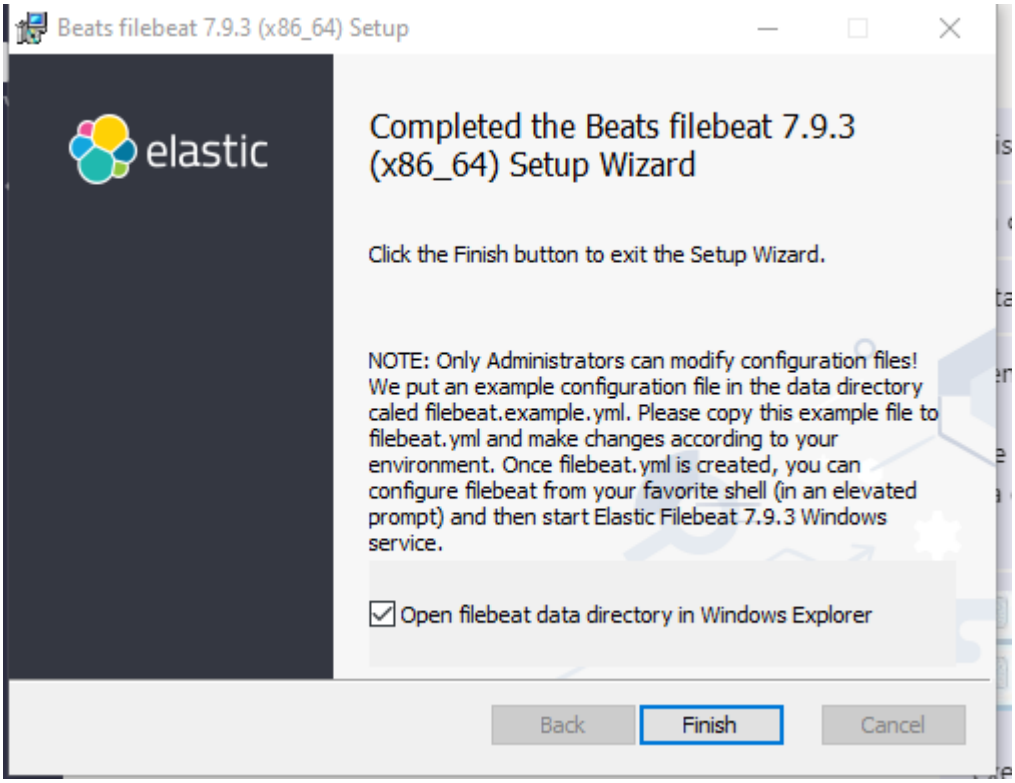
Primeiro passo acessar o site da Elastic e ir até a pagina de download do filebeat (não vou passar um link para não ficar restrito a uma opção ok)



Primeiramente realizar o Download do instalador do Filebeat, pode utilizar a versão MSI (ela apenas reduz os passos de ter que criar o serviço na mão posteriormente)

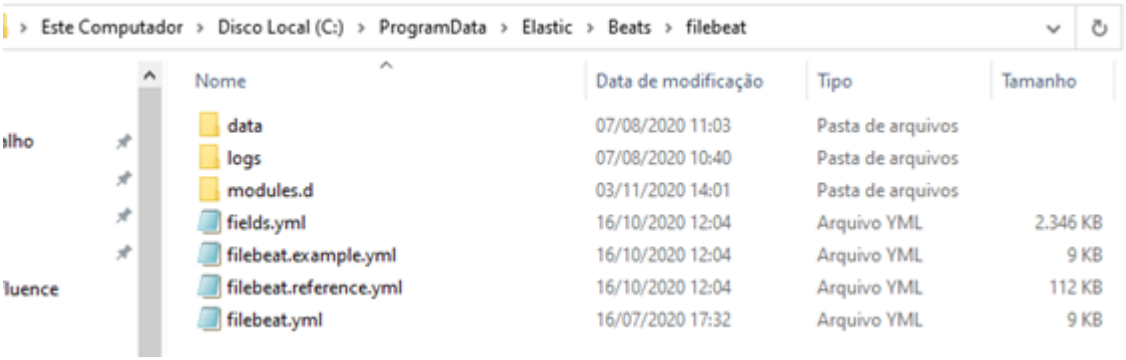
Siga o processo de instalação normalmente



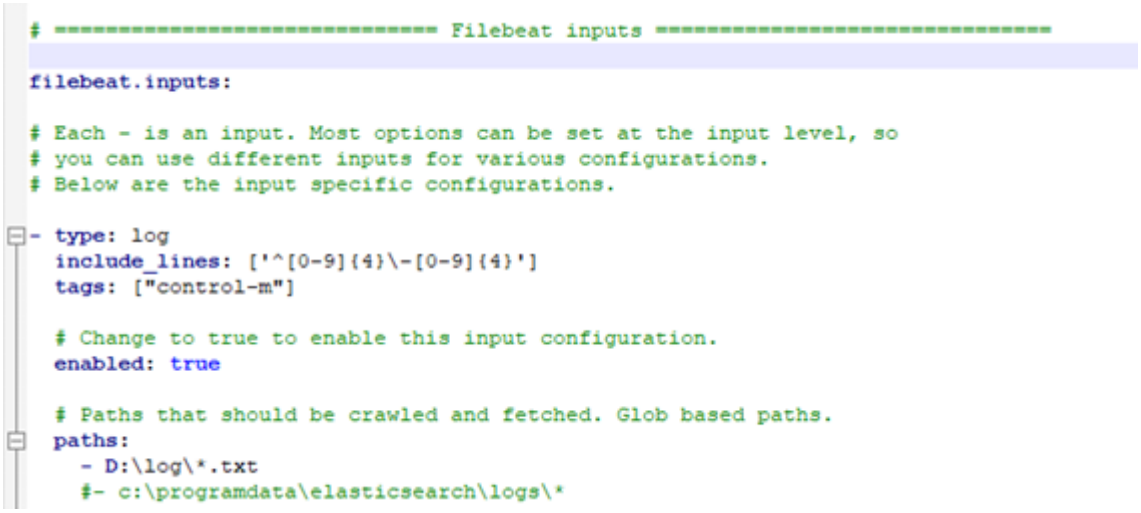


Quando finalizar deixe marcada a opção para abrir o diretório com as configurações.

Faça uma cópia do filebeat.example.yml renomeando para filebeat.yml



Configurando o Filebeats:



```
# ============================== Filebeat inputs ===============================

filebeat.inputs:

# Each - is an input. Most options can be set at the input level, so
# you can use different inputs for various configurations.
# Below are the input specific configurations.

- type: log
  include_lines: ['^[0-9]{4}\-[0-9]{4}']
  tags: ["control-m"]

  # Change to true to enable this input configuration.
  enabled: true

  # Paths that should be crawled and fetched. Glob based paths.
  paths:
    - D:\log\*.txt
    #- c:\programdata\elasticsearch\logs\*
```

Dentro deste arquivo na sessão Filebeat inputs:

Inclua o type (em sua maioria log)

include_lines: (um padrão de REGEX para capturar a linha, no exemplo temos o formato 0000-0000)

tags: (inclua uma que faça sentido com a sua aplicação)

enable: (altere para true)

paths: (local onde estão os seus logs, observe que usando um asterisco *.txt, ele vai ler de qualquer arquivo nesse diretório com essa extensão, claro atendendo o

critério de include_lines)

DICA COM REGEX:

Aqui temos um exemplo mais robusto para incluir as linhas.

No caso só nos interessa mensagens do tipo WARN e ERROR logo nosso REGEX só precisa considerar estes.

Uma boa dica é usar o site do regex101.com assim é possível testar antes de colocar para rodar.

Para chegar no resultado o REGEX usado foi o seguinte:

^[0-9]{2}:[0-9]{2}:[0-9]{2},[0-9]{3}.*ERROR|[0-9]{2}:[0-9]{2}:[0-9]{2},[0-9]{3}.*WARN

OBS.: o “|” tem a função de OU

Agora basta adicionar esse REGEX no arquivo de configuração do filebeat (no meu caso)!

Segue o bloco com o log em usado para quem tiver interesse em testar e aprimorar.

```
04:41:27,113 |-INFO in ch.qos.logback.classic.LoggerContext[default] - Could NOT
find resource [logback.groovy]
04:41:27,113 |-INFO in ch.qos.logback.classic.LoggerContext[default] - Could NOT
find resource [logback-test.xml]
04:41:27,113 |-INFO in ch.qos.logback.classic.LoggerContext[default] - Found
resource [logback.xml] at [jar:file:/C:/Jobs/Anuidade/fin-anuidade-
batch.jar!/logback.xml]
04:41:27,128 |-INFO in
ch.qos.logback.core.joran.spi.ConfigurationWatchList@1c6b6478 - URL
[jar:file:/C:/Jobs/Anuidade/fin-anuidade-batch.jar!/logback.xml] is not of type
file
04:41:27,269 |-WARN in ch.qos.logback.core.joran.action.IncludeAction - Could
not find resource corresponding to
[org/springframework/boot/logging/logback/base.xml]
04:41:27,269 |-INFO in ch.qos.logback.core.joran.action.AppenderAction - About
to instantiate appender of type
[ch.qos.logback.core.rolling.RollingFileAppender]
04:41:27,269 |-INFO in ch.qos.logback.core.joran.action.AppenderAction - Naming
appender as [FILE]
04:41:27,300 |-INFO in
ch.qos.logback.core.rolling.FixedWindowRollingPolicy@2ac1fdc4 - Will use zip
compression
04:41:27,300 |-INFO in ch.qos.logback.core.joran.action.NestedComplexPropertyIA
- Assuming default type [ch.qos.logback.classic.encoder.PatternLayoutEncoder]
for [encoder] property
04:41:27,315 |-INFO in ch.qos.logback.core.rolling.RollingFileAppender[FILE] -
Active log file name: app.logging_IS_UNDEFINED/fin-anuidade-ear/fin-anuidade.log
04:41:27,315 |-INFO in ch.qos.logback.core.rolling.RollingFileAppender[FILE] -
File property is set to [app.logging_IS_UNDEFINED/fin-anuidade-ear/fin-
anuidade.log]
04:41:27,315 |-INFO in ch.qos.logback.core.joran.action.AppenderAction - About
to instantiate appender of type
[net.logstash.logback.appender.LogstashTcpSocketAppender]
04:41:27,331 |-INFO in ch.qos.logback.core.joran.action.AppenderAction - Naming
appender as [LOGSTASH]
```

```
04:41:27,331 |-ERROR in ch.qos.logback.core.joran.action.NestedBasicPropertyIA -
Unexpected aggregationType AS_BASIC_PROPERTY_COLLECTION
04:41:27,456 |-INFO in ch.qos.logback.core.joran.action.NestedComplexPropertyIA
- Assuming default type
[net.logstash.logback.composite.loggingevent.LoggingEventJsonProviders] for
[providers] property
04:41:27,471 |-INFO in ch.qos.logback.core.joran.action.NestedComplexPropertyIA
- Assuming default type
[net.logstash.logback.composite.loggingevent.MdcJsonProvider] for [mdc] property
Warning: Class 'net.logstash.logback.composite.loggingevent.MdcJsonProvider'
contains multiple setters for the same property 'fieldNames'.
04:41:27,471 |-INFO in ch.qos.logback.core.joran.action.NestedComplexPropertyIA
- Assuming default type [net.logstash.logback.composite.ContextJsonProvider] for
[context] property
04:41:27,471 |-INFO in ch.qos.logback.core.joran.action.NestedComplexPropertyIA
- Assuming default type
[net.logstash.logback.composite.LogstashVersionJsonProvider] for [version]
property
04:41:27,471 |-INFO in ch.qos.logback.core.joran.action.NestedComplexPropertyIA
- Assuming default type
[net.logstash.logback.composite.loggingevent.LogLevelJsonProvider] for
[logLevel] property
Warning: Class
'net.logstash.logback.composite.loggingevent.LogLevelJsonProvider' contains
multiple setters for the same property 'fieldNames'.
04:41:27,471 |-INFO in ch.qos.logback.core.joran.action.NestedComplexPropertyIA
- Assuming default type
[net.logstash.logback.composite.loggingevent.LoggerNameJsonProvider] for
[loggerName] property
Warning: Class
'net.logstash.logback.composite.loggingevent.LoggerNameJsonProvider' contains
multiple setters for the same property 'fieldNames'.
04:41:27,471 |-INFO in ch.qos.logback.core.joran.action.NestedComplexPropertyIA
- Assuming default type
[net.logstash.logback.composite.loggingevent.LoggingEventPatternJsonProvider]
for [pattern] property
04:41:27,471 |-INFO in ch.qos.logback.core.joran.action.NestedComplexPropertyIA
- Assuming default type
[net.logstash.logback.composite.loggingevent.ThreadNameJsonProvider] for
[threadName] property
Warning: Class
'net.logstash.logback.composite.loggingevent.ThreadNameJsonProvider' contains
multiple setters for the same property 'fieldNames'.
04:41:27,471 |-INFO in ch.qos.logback.core.joran.action.NestedComplexPropertyIA
```

```
- Assuming default type
[net.logstash.logback.composite.loggingevent.MessageJsonProvider] for [message]
property
Warning: Class 'net.logstash.logback.composite.loggingevent.MessageJsonProvider'
contains multiple setters for the same property 'fieldNames'.
04:41:27,471 |-INFO in ch.qos.logback.core.joran.action.NestedComplexPropertyIA
- Assuming default type
[net.logstash.logback.composite.loggingevent.LogstashMarkersJsonProvider] for
[logstashMarkers] property
04:41:27,471 |-INFO in ch.qos.logback.core.joran.action.NestedComplexPropertyIA
- Assuming default type
[net.logstash.logback.composite.loggingevent.ArgumentsJsonProvider] for
[arguments] property
04:41:27,471 |-INFO in ch.qos.logback.core.joran.action.NestedComplexPropertyIA
- Assuming default type
[net.logstash.logback.composite.loggingevent.StackTraceJsonProvider] for
[stackTrace] property
Warning: Class
'net.logstash.logback.composite.loggingevent.StackTraceJsonProvider' contains
multiple setters for the same property 'fieldNames'.
04:41:27,518 |-INFO in ch.qos.logback.core.joran.action.AppenderAction - About
to instantiate appender of type [ch.qos.logback.classic.AsyncAppender]
04:41:27,518 |-INFO in ch.qos.logback.core.joran.action.AppenderAction - Naming
appender as [ASYNC]
04:41:27,518 |-INFO in ch.qos.logback.core.joran.action.AppenderRefAction -
Attaching appender named [FILE] to ch.qos.logback.classic.AsyncAppender[ASYNC]
04:41:27,518 |-INFO in ch.qos.logback.classic.AsyncAppender[ASYNC] - Attaching
appender named [FILE] to AsyncAppender.
04:41:27,534 |-INFO in ch.qos.logback.classic.AsyncAppender[ASYNC] - Setting
discardingThreshold to 51
04:41:27,534 |-INFO in ch.qos.logback.classic.joran.action.RootLoggerAction -
Setting level of ROOT logger to DEBUG
04:41:27,534 |-INFO in ch.qos.logback.core.joran.action.AppenderRefAction -
Attaching appender named [ASYNC] to Logger[ROOT]
04:41:27,534 |-INFO in ch.qos.logback.core.joran.action.AppenderRefAction -
Attaching appender named [LOGSTASH] to Logger[ROOT]
04:41:27,534 |-INFO in ch.qos.logback.classic.joran.action.ConfigurationAction -
End of configuration.
04:41:27,534 |-INFO in ch.qos.logback.classic.joran.JoranConfigurator@1c72da34 -
Registering current configuration as safe fallback point
.04:41:28,561 |-WARN in
net.logstash.logback.appender.LogstashTcpSocketAppender[LOGSTASH] - Log
destination 10.1.10.169:5044: connection failed. Waiting 28957ms before
attempting reconnection. java.net.ConnectException: Connection refused: connect
```

```
at java.net.ConnectException: Connection refused: connect
```

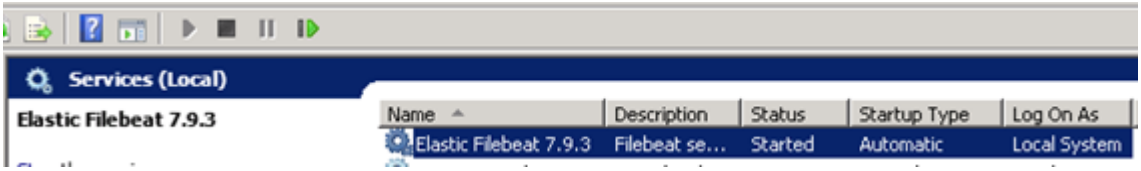
Entrando na última parte:

```
# ---------------------------- Elasticsearch Output ----------------------------
#output.elasticsearch:
  # Array of hosts to connect to.
  # hosts: ["localhost:9200"]

  # Protocol - either `http` (default) or `https`.
  #protocol: "https"

  # Authentication credentials - either API key or username/password.
  #api_key: "id:api_key"
  #username: "elastic"
  #password: "changeme"

# ------------------------------ Logstash Output -------------------------------
output.logstash:
  # The Logstash hosts
  hosts: ["localhost:5043"]

  # Optional SSL. By default is off. rchlo-logstash-dev.riachuelo.net:5045
  # List of root certificates for HTTPS server verifications
  #ssl.certificate_authorities: ["/etc/pki/root/ca.pem"]

  # Certificate for SSL client authentication
  #ssl.certificate: "/etc/pki/client/cert.pem"

  # Client Certificate Key
  #ssl.key: "/etc/pki/client/cert.key"

# ================================= Processors =================================
```

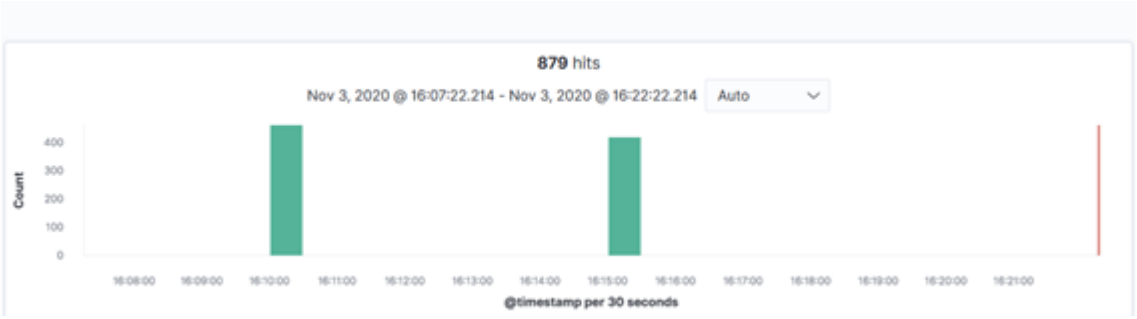
Aqui não tem segredos caso esteja enviando diretamente para o Elasticsearch basta inserir as credenciais.

Caso seja o Logstash apenas insira as credenciais da mesma forma.

IMPORTANTE! Deixe comentado o que não for usado, conforme exemplo foi utilizado o logstash para receber o log, logo o elasticsearch foi comentado.



Por fim vá nos serviços do Windows e inicie o filebeat.



Aguarde uns 2min e se tudo correu bem já pode configurar e ver seus logs no Kibana.

Bem colegas é isso, foi um artigo simples mas que ajuda bastante, acreditem já vi muitos colegas com dificuldades com esse carinha.

Espero que tenham gostado, dúvidas sugestões fico a disposição.