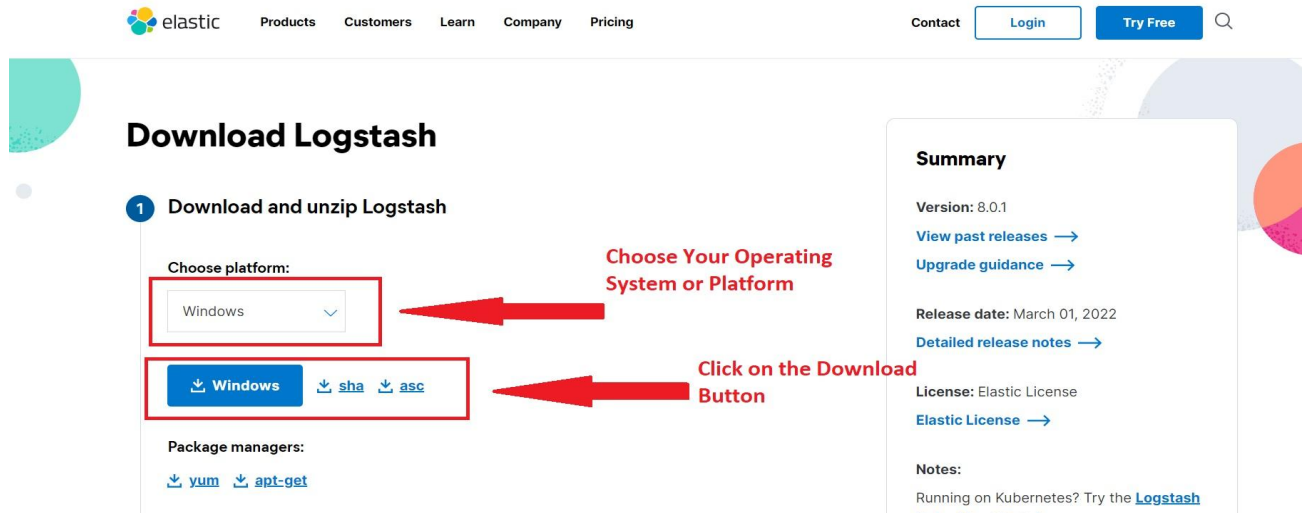
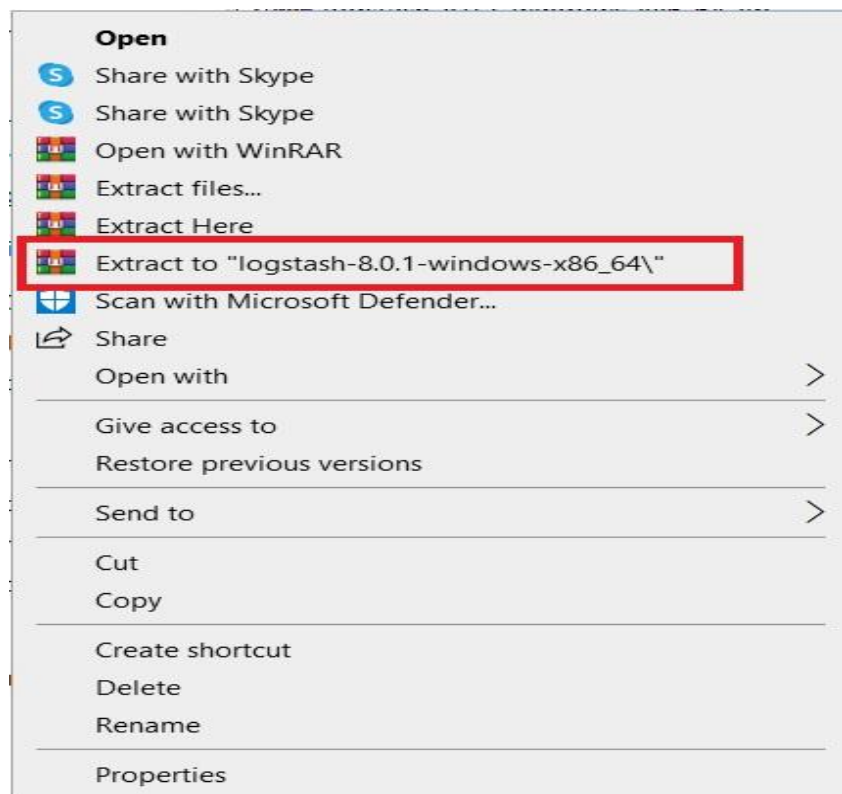


Indexing Log Files to Solr

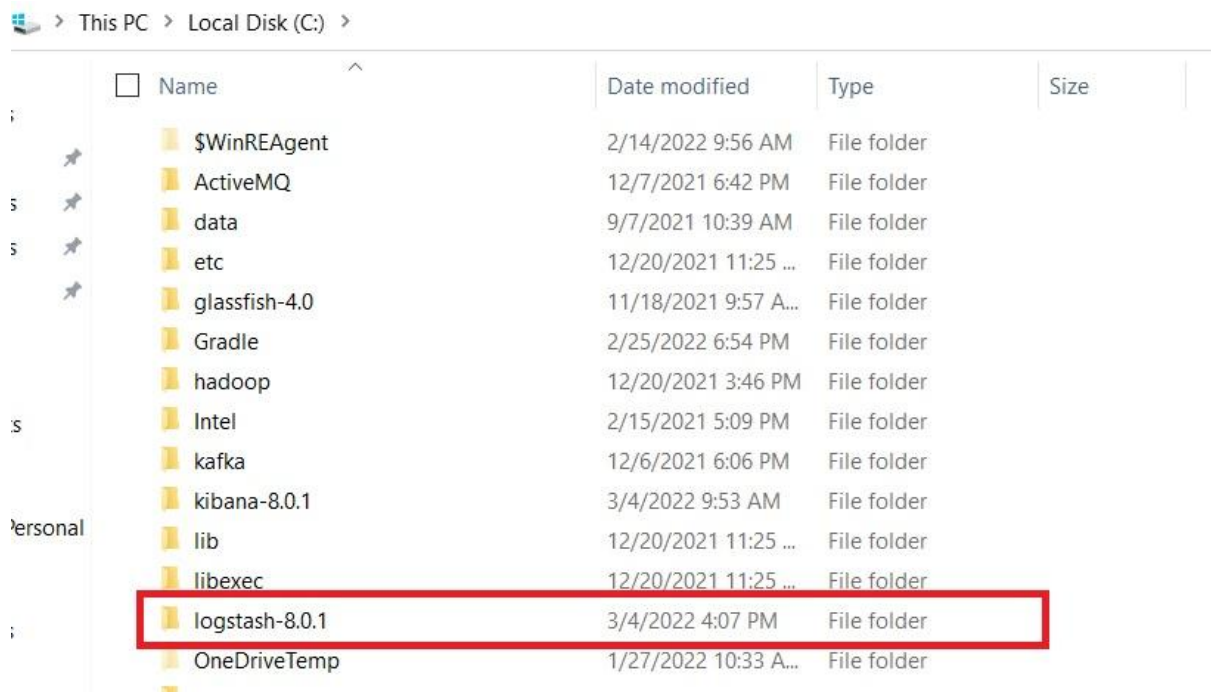
Step 1: Installing the latest Logstash , we need to download the latest logstash version from the following link , [Download Logstash](#) .



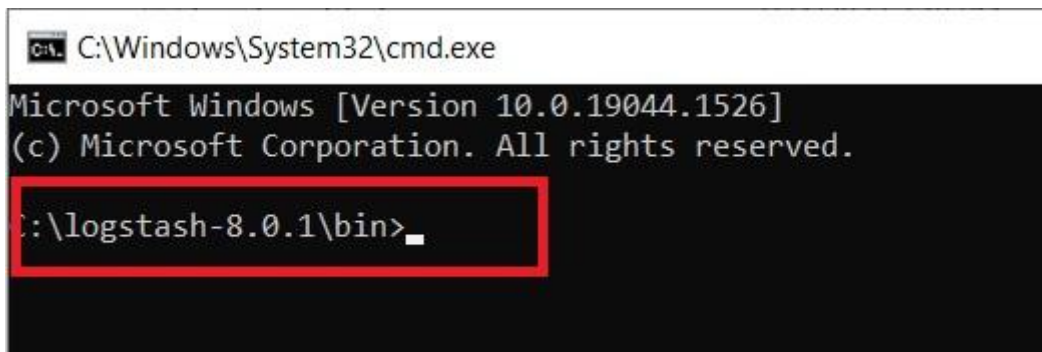
Step 2: After clicking on the download button an rar file will be downloaded , which we need to extract .



Step 3: We need to now move our extracted logstash folder to an appropriate location , in our case we have moved to C:/ .

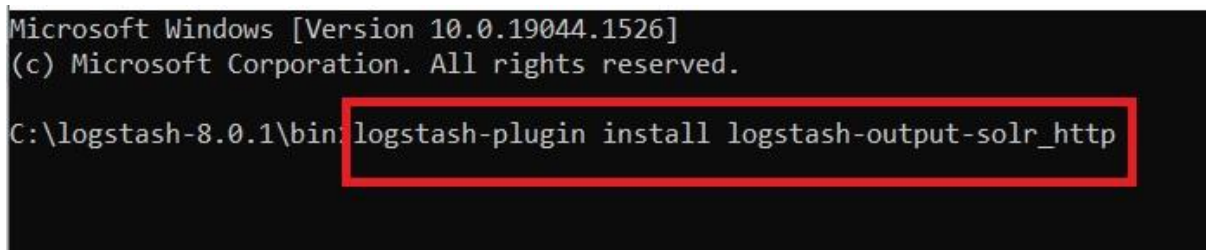


Step 4: The next step is to install the logstash solr plugin for connecting logstash to the solr server . For this first we will need to open cmd having path of logstash bin :



Then we need to run the following command :

logstash-plugin install logstash-output-solr_http



After clicking enter the plugin will be downloaded in to logstash

Step 5: The next step is to install ruby , Ruby latest version can be downloaded from the following link , [Download Ruby](#) .

RubyInstallers **Archives»**

Not sure what version to download? Please read the right-hand column for recommendations. **Click to Download**

WITH DEVKIT

- => Ruby+Devkit 3.1.1-1 (x64)**
- Ruby+Devkit 3.1.1-1 (x86)
- Ruby+Devkit 3.0.3-1 (x64)

WHICH VERSION TO DOWNLOAD?

If you don't know what version to install and you're getting started with Ruby, we recommend that you use the **Ruby+Devkit 3.1.X (x64)** it provides the biggest number of compatible gems and installs the Devkit alongside Ruby, so gems with C-extensions can be compiled immediately. The 32 bit (x86) version is recommended only if custom native DLLs or COM objects have to be used.

File Name	Date Modified	Type	Size
rubyinstaller-devkit-3.1.1-1-x64.exe	3/4/2022 2:56 PM	Application	140,339 KB

After that we need to open the installer and follow the steps , ruby will be installed .
For getting sure with the installation go to cmd and type command `ruby -v`

```
C:\Users\user>ruby -v
ruby 3.1.1p18 (2022-02-18 revision 53f5fc4236) [x64-mingw-ucrt]
C:\Users\user>
```

Step 6: The next step is to install Rsolr , here we have used version 1.1.2 , for that we need to open cmd and type the following command:

`gem install rsolr -v 1.1.2`

```
C:\Users\user>gem install rsolr -v 1.1.2
```

Step 7: Now we need to update the logstash solr http plugin , for which we need to first we need to follow the path:

`C:\logstash-8.0.1\vendor\bundle\jruby\2.5.0\gems\logstash-output-solr_http-3.0.5\lib\logstash\outputs`

PC > Local Disk (C:) > logstash-8.0.1 > vendor > bundle > jruby > 2.5.0 > gems > logstash-output-solr_http-3.0.5 > lib > logstash > outputs

Name	Date modified	Type	Size
solr_http.rb	3/4/2022 7:08 PM	Ruby File	3 KB

We need to open this file and make necessary changes :

1. In this file there will be a line as `require "rsolr"` , we need to replace this with `require "/C:/Ruby31-x64/lib/ruby/gems/3.1.0/gems/rsolr-1.1.2/lib/rsolr"` .

Note : Here the location is according to my installation of Ruby , it can vary based on your installation path.

Installation path can be obtained by typing the following command:

gem environment

```
C:\Users\user>gem environment
RubyGems Environment:
- RUBYGEMS VERSION: 3.3.7
- RUBY VERSION: 3.1.1 (2022-02-18 patchlevel 18) [x64-mingw-ucrt]
- INSTALLATION DIRECTORY: C:/Ruby31-x64/lib/ruby/gems/3.1.0
- USER INSTALLATION DIRECTORY: C:/Users/user/.gem/ruby/3.1.0
- RUBY EXECUTABLE: C:/Ruby31-x64/bin/ruby.exe
- GIT EXECUTABLE: C:\Program Files\Git\cmd/git.EXE
- EXECUTABLE DIRECTORY: C:/Ruby31-x64/bin
- SPEC CACHE DIRECTORY: C:/Users/user/.gem/specs
- SYSTEM CONFIGURATION DIRECTORY: C:/ProgramData
- RUBYGEMS PLATFORMS:
  - ruby
  - x64-mingw-ucrt
- GEM PATHS:
  - C:/Ruby31-x64/lib/ruby/gems/3.1.0
  - C:/Users/user/.gem/ruby/3.1.0
- GEM CONFIGURATION:
  - :update_sources => true
  - :verbose => true
  - :backtrace => false
  - :bulk_threshold => 1000
- REMOTE SOURCES:
  - https://rubygems.org/
```

```
public
def register
  require "/C:/Ruby31-x64/lib/ruby/gems/3.1.0/gems/rsolr-1.1.2/lib/rsolr"
  @solr = RSolr.connect :uri => @solr_uri
  buffer_initialize(
    :max_items => @flush_size,
    :max_interval => @idle_flush_time,
    :logger => @logger
  )
end #def register
```

2. The next part is to replace to comment the line .iso8601 on line number 67 by just adding an # .

```
events.each do |event|
  document = event.to_hash()
  document["@timestamp"] = document["@timestamp"] #.iso8601 #make the timestamp ISO
  if @document_id.nil?
```

3. The next step is to replace line `@solr.add(documents)` with `@solr.add(documents, :add_attributes => {:commitWithin=>1000})`

```
#@solr.add(documents)
@solr.add(documents, :add_attributes => {:commitWithin=>1000})
rescue Exception => e
```


Step 8: Testing by Creating an sample application and adding log file properties :

```
logging.file.path=logs
#You can specify the own log file name using the property shown below
logging.file.name=logs/Test_Logs.log
```

```
@RequestMapping("/hello")
public String helloMessage() {
    logger.info("helloMessage() method called {} and status {}",new Date(),200);
    return "HELLO WORLD";
}
```

Step 9: The next step is to create an configuration file with name as *logstash_solr.conf* inside the logstash bin folder and add the following properties :

```
input {
    file {
        path =>
"C:/Users/user/eclipse-workspace/spring-boot-logstash/logs/Test_Logs.log"
        start_position => "beginning"
    }
}

output {
    solr_http {
        solr_url => "http://localhost:8983/solr/logTest"
    }
}
```

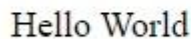
Step 9: The next step is to start the solr server and create an empty collection :

1. solr start -c
2. solr create -c collectionName

Step 10: Start the application and send some request for dummy logs :

```
spring-boot-logstash - SpringBootLogstashApplication [Spring Boot App] C:\Program Files\Java\jdk1.8.0_281\bin\javaw.exe (Mar 7, 2022, 11:48:49 AM)
=====
:: Spring Boot :: (v2.6.4)

2022-03-07 11:49:25.079 INFO 3920 --- [main] c.s.l.SpringBootLogstashApplication : Starting SpringBootLogstashApplicat
2022-03-07 11:49:25.107 INFO 3920 --- [main] c.s.l.SpringBootLogstashApplication : No active profile set, falling back
2022-03-07 11:49:29.673 INFO 3920 --- [main] o.s.b.w.embedded.tomcat.TomcatWebServer : Tomcat initialized with port(s): 8080
2022-03-07 11:49:29.705 INFO 3920 --- [main] o.apache.catalina.core.StandardService : Starting service [Tomcat]
2022-03-07 11:49:29.705 INFO 3920 --- [main] org.apache.catalina.core.StandardEngine : Starting Servlet engine: [Apache Tomcat/9.0.56]
2022-03-07 11:49:29.924 INFO 3920 --- [main] o.a.c.c.C.[Tomcat].[localhost].[/] : Initializing Spring embedded WebApplication
2022-03-07 11:49:29.925 INFO 3920 --- [main] w.s.c.ServletWebServerApplicationContext : Root WebApplicationContext: initialization completed
2022-03-07 11:49:30.984 INFO 3920 --- [main] o.s.b.w.embedded.tomcat.TomcatWebServer : Tomcat started on port(s): 8080 (http)
2022-03-07 11:49:31.007 INFO 3920 --- [main] c.s.l.SpringBootLogstashApplication : Started SpringBootLogstashApplication
```



```
C:\logstash-8.0.1\bin>logstash -f logstash_solr.conf
```

```
0.13+8 windy +jit [mswin32-x86_64]
2022-03-07T11:57:21,227][INFO][logstash.runner] JVM bootstrap flags: -Xmsg, -Xmxg, -XX:+UseConcMarkSweepGC, -XX:CHSInitiatingOccupancyFraction=75, -XX:+UseCHSInitiatingOccupancyOnly, -Djava.class.true, -Dfile.encoding=UTF-8, -Djruby.compile.invokedynamic=true, -Djruby.jit.threshold=0, -Djruby.rexexp.interruptible=true, -XX:-HeapDumpOnOutOfMemoryError, -Djava.security.epd.file:/dev/urandom, -DthreadContextClassLoader=, --add-opens=java.base/java.security=ALL-UNNAMED, --add-opens=java.base/java.io=ALL-UNNAMED, --add-opens=java.base/java.nio.channels=ALL-UNNAMED, --add-opens=java.base/java.management/sun.management=ALL-UNNAMED
2022-03-07T11:57:22,060][WARN][logstash.config.source.multilocal] Ignoring the 'pipelines.yml' file because modules or command line options are specified
2022-03-07T11:57:25,602][INFO][logstash.agent] Successfully started Logstash API endpoint {:port=>9600, :ssl.enabled=>false}
2022-03-07T11:58:00,074][INFO][org.reflections.Reflections] Reflections took 1168 ms to scan 1 urls, producing 120 keys and 417 values
2022-03-07T11:58:18,132][INFO][logstash.javapipeline] Pipeline 'main' is configured with 'pipeline.ecs_compatibility': v8' setting. All plugins in this pipeline will default to 'ecs_compatibility' => v8 unless explicitly configured otherwise.
2022-03-07T11:58:29,077][INFO][logstash.javapipeline] [main] Starting pipeline : {pipeline_id=>'main', 'pipeline.workers'=>4, 'pipeline.batch.size'=>125, 'pipeline.batch.delay'=>50, 'pipeline.max_inflight'=>100, 'pipeline.sources'=>["C:/logstash-8.0.1/bin/logstash.solver.conf"], :thread=>#Thread:0x40f51de9 >main"}, {thread=>#Thread:0x40f51de9 >main"}, {thread=>#Thread:0x40f51de9 >main"}, {thread=>#Thread:0x40f51de9 >main"}
2022-03-07T11:58:38,307][INFO][logstash.javapipeline] [main] Pipeline java execution initialization time ("seconds")=>0.82
2022-03-07T11:59:43,263][INFO][logstash.inputs.file] [main] No sincedb path set. Generating one based on the "path" setting : {sincedb_path=>"C:/logstash-8.0.1/data/plugins/inputs/file/.sincedb_a2f742f34382bbd2eadbf", :path=>"C:/Users/user/eclipse-workspace/spring-boot-logstash/logs/Test_Logs.log"}
2022-03-07T11:58:38,318][INFO][logstash.javapipeline] [main] Pipeline started ("pipeline_id"=>"main")
2022-03-07T11:58:39,047][INFO][filewatch.observertail] [main][92ab5193cbcdcad7352c14f9e35de9338ef20412568b1d6469cb33add61a6] START, creating Discoverer, Watch with the file based collectors
2022-03-07T11:58:39,700][INFO][logstash.agent] [Pipelines running : {count=>1, :running_pipelines=>{:main}, :non_running_pipelines=>{}}
```

Now if we check our solr server , we can see the log records have been added .

Java Properties

Thread Dump

Suggestions

logTest

Overview

Analysis

Dataimport

Documents

Files

Query

Stream

Schema

Core Selector

q.op
OR

fq

sort

start_rows
0 10

fl

df

wt

☒ indent on

☐ debugQuery

defType
lucene

☐ hl

☐ facet

☐ spatial

```

"status":0,
"qtime":9,
"params":{
  "q":"*",
  "indent":"true",
  "q.op":"OR",
  "t":["1608383551648"]},
"response":{"numFound":129,"start":0,"numFoundExact":true,"docs":[
  {
    "log":["[\"file\", {\"path\"->\"C:/Users/user/eclipse-workspace/spring-boot-logstash/logs/Test_Logs.log\"}],",
    "message":["2022-03-04 19:20:07.296 INFO 10352 --- [main] c.s.l.SpringBootlogstashApplication   : Starting SpringBootlogstashApplication using Java 1.8.0_28",
    "event":["[\"@original\", \"2022-03-04 19:20:07.296 INFO 10352 --- [main] c.s.l.SpringBootlogstashApplication   : Starting SpringBootlogstashApplication using Java 1.8.0_28\",",
    "host":["[\"name\", \"DESKTOP-SQ99E4A\"],",
    "id":["dcad619b-0159-4f84-b56d-724821e422bc",
    "version":["],",
    "timestamp":["2022-03-04T13:53:05.820Z"],",
    "version":["1726377613802340352],",
    {
      "log":["[\"file\", {\"path\"->\"C:/Users/user/eclipse-workspace/spring-boot-logstash/logs/Test_Logs.log\"}],",
      "message":["2022-03-04 19:20:07.307 INFO 10352 --- [main] c.s.l.SpringBootlogstashApplication   : No active profile set, falling back to 1 default profile:",
      "event":["[\"@original\", \"2022-03-04 19:20:07.307 INFO 10352 --- [main] c.s.l.SpringBootlogstashApplication   : No active profile set, falling back to 1 default profile:",
      "host":["[\"name\", \"DESKTOP-SQ99E4A\"],",
      "id":["f9e4dc-3980-416b-8658-29fee2589598",
      "version":["],",
      "timestamp":["2022-03-04T13:53:05.903Z"],",
      "version":["1726377613750594560],",
      {
        "log":["[\"file\", {\"path\"->\"C:/Users/user/eclipse-workspace/spring-boot-logstash/logs/Test_Logs.log\"}],",
        "message":["2022-03-04 19:20:09.055 INFO 10352 --- [main] o.a.c.c.c.[Tomcat].[localhost].[/]   : Initializing Spring embedded WebApplicationContext"],",
        "event":["[\"@original\", \"2022-03-04 19:20:09.055 INFO 10352 --- [main] o.a.c.c.c.[Tomcat].[localhost].[/]   : Initializing Spring embedded WebApplicationContext"],",
        "host":["[\"name\", \"DESKTOP-SQ99E4A\"],",
        "id":["a1e995a6-1d4d-4270-b8da-cd37c7bdc81e"]}]
      }
    ]}
  ]}

```