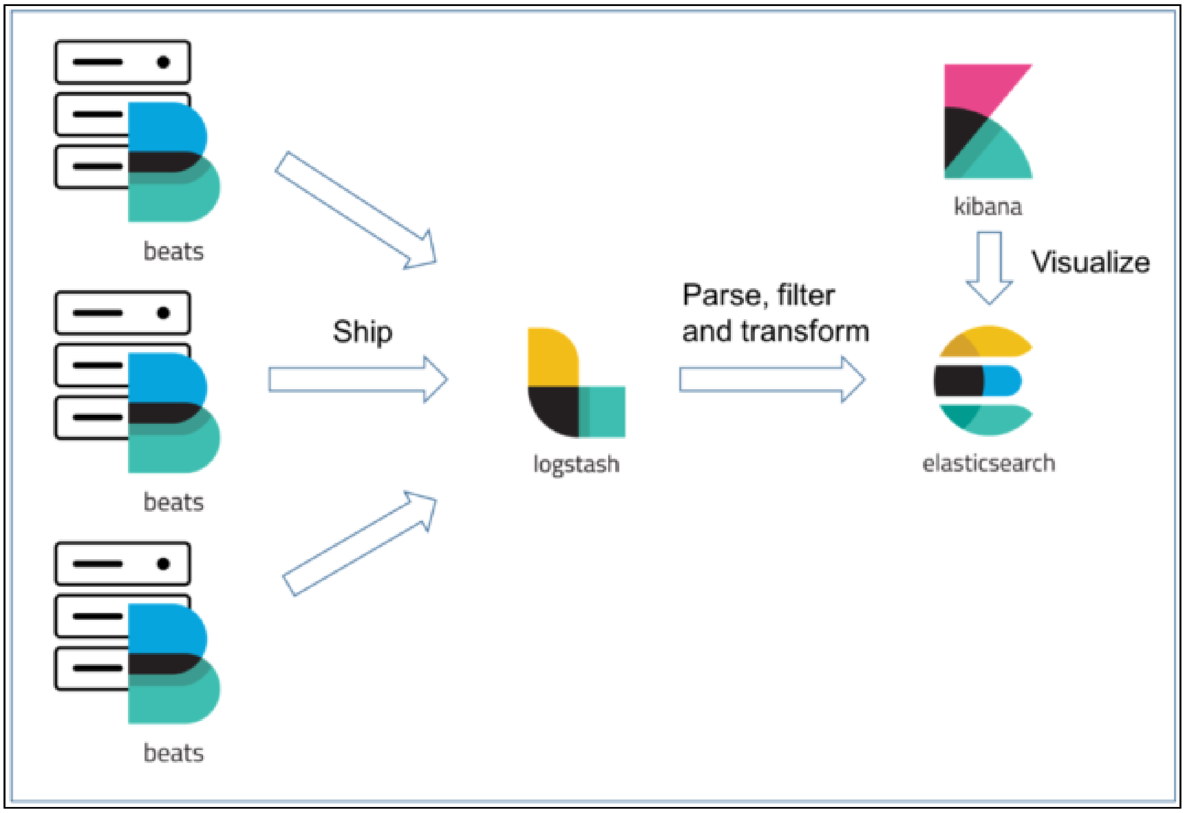
ELK Stack 7.5.2 Deployment



This document covers downloading and installing Elasticsearch, Logstash and Kibana (ELK) technology stack and running the stack as background services.

Backup Procedure

	Action	Team
1		

Prerequisites

	Action	Team
1	Install JAVA jre version 8 or above and set JAVA_HOME environment variable	
2	Make sure these ports are usable/open for external communication if needed [5601, 8888] Elastic Search Default Port 9200 Kinana used Port 5601 Logstach Default Port 5000 Filebeat user Port 8888	

Variables Reference

Variable name	Description
$ELASTICSEARCH_HOME	points to the main directory of Elasticsearch (bin directory of ElasticSearch installation)

$KIBANA_HOME	points to the main directory of Kibana (bin directory of Kibana installation)
$LOGSTASH_HOME	points to the main directory of Logstash (bin directory of LogStash installation)

Elasticsearch Installation Procedure

	Action	Team	Comment
1	**Download Elasticsearch version 7.5.2**		
2	Unzip downloaded file into **D:\ELK\Elasticsearch**		

3	Install and run Elasticsearch as a service:
	- Open CMD as Admin
	- Navigate to Elasticsearch folder:
	`cd D:\ELK\Elasticsearch\bin`
	- Run:
	`elasticsearch-service.bat install`
	- Run:
	`elasticsearch-service.bat start`
	- Make sure windows service named **[Elasticsearch]** has been *installed* and *started*.		

4	Validate Installation by running one of the following: - Run cmd: curl http://localhost:9200/ - PowerShell: Invoke-RestMethod http://localhost:9200 - Browser go to: http://localhost:9200/		
5	Haitham Mohamed Gamal Ahmed Mohamed Elazouny Add step to change default location of Elasticsearch database location.		

Kibana Installation Procedure

	Action	Team	Comment
1	**Download Kibana version 7.5.2**		
2	unzip Kibana downloaded file into: **D:\ELK\Kibana**		
3	By default Kibana connects to Elasticsearch on [localhost:9200] if Elasticsearch default port changed, do the following: - Open **D:\ELK\Kibana\config\kibana.yml** in an editor - Set **elasticsearch.hosts** to point at your Elasticsearch instance - If your Elasticsearch is protected with basic authentication, set these settings Haitham Mohamed Gamal Ahmed Mohamed Elazouny From where did we set the user name /pass of elasticsearch? you need to add it as step while installing Elasticsearch. - **elasticsearch.username: "kibana"** - **elasticsearch.password: "pass"** - Set **server.host: "MACHINE_IP_ADDRESS"** to IP address of the machine to be able to visit Kibana app from outside the machine Haitham Mohamed Gamal Ahmed Mohamed Elazouny Can we set the IP address to 127.0.0.1? **For more customization refer to the documentation**		

4	Install and run Kibana as a service:
	• Download NSSM
	• Unzip nssm inside **D:\ELK\Kibana\service**
	• Open cmd as Admin and navigate to: **D:\ELK\Kibana\service**
	• Run CMD as admin and run the following commands:
	`cd D:\ELK\Kibana\service\win64`
	`nssm.exe install`
	`Path: D:\ELK\Kibana\bin\kibana.bat`
	Startup Directory: D:\ELK\Kibana\bin
	Service name: Kibana Service
	Click **Install service**
	nssm.exe start Kibana Service"
	• Make sure "**Kibana service**" is in "**started**" mode.		

5	Validate Installation • Browser go to: http://localhost:5601/		

Logstash Installation Procedure

	Action	Team	Comment
1	**Download Logstash version 7.5.2**		
2	unzip Logstash to: D:\ELK\Logstash		

3 Configure Logstash

- Create new file named "**logstash.conf**" in "**D:\ELK\Logstash\config"** directory
- Open **D:\ELK\Logstash\config\logstash.conf** in an editor
- Replace its content with the following

```
####################################################################
#################################################
#  The configuration of a plugin consists of the plugin name
followed by a block of settings for that plugin.       #
####################################################################
#################################################
input {
####################################################################
#########
# https://www.elastic.co/guide/en/logstash/current/plugins-inputs-
beats.html#
####################################################################
#########
        beats {
                # host => "0.0.0.0"
                port => 8888
        }
}

####################################################################
#################################################
#  If you specify multiple filters, they are applied in the order
of their appearance in the configuration file.    #
####################################################################
#################################################
filter {
        fingerprint {
                source => "message"
                target => "[@metadata][fingerprint]"
                method => "MD5"
                key => "duplicate_key_check"
        }

        if([applicationType] == "tomcat"){
                dissect {
                        mapping => {
                                "message" => "%{ts} %{+ts} %
{logLevel} [%{thread}] %{msg}"
                        }
                }
        }

        if([applicationType] == "inspectionLog") {
                dissect {
                        mapping => {
                                "message" => "%{ts} %{+ts} %{+ts} [%
{logLevel}] [%{msg}] [%{properties}]%{exception}"
                                "[insp][FullappService]" => "%
{appService}-%{appEnv}-logs-%{}.txt"
                        }
                }
        }
}

output {
        elasticsearch {
                hosts => ["localhost:9200"]
                index => "%{[@metadata][beat]}-%{[@metadata]
[version]}-%{+YYYY.MM.dd}"
                document_id => "%{[@metadata][tsprefix]}%
{[@metadata][fingerprint]}"
        }
        stdout {
                codec => rubydebug
        }
}
```

Haitham Mohamed Gamal Ahmed Mohamed Elazouny
You need to tell in the beginning of the MRF what are the ports that you are going to use, and the communication matrix of the ports

Port	Source	Destination
8888	<component_name>	<component_name>
9200		
xxx		

For more customization refer to the documentation and the documentation

<table>
<tr>
<td>4</td>
<td>

Install and run Logstash as a service:

- Download NSSM
- Unzip nssm inside **D:\ELK\Logstash\service**
- Run CMD as admin and run the following commands:

```
cd D:\ELK\Logstash\service\win64
nssm.exe install
Path: D:\ELK\Logstash\bin\logstash.bat
Startup Directory: D:\ELK\Logstash\bin\
Arguments: -f D:\ELK\Logstash\config\logstash.conf
Service name: Logstash Service
Click Install service
nssm.exe start "Logstash Service"
```

</td>
<td></td>
<td></td>
</tr>
</table>

Elasticsearch-Curator

<table>
<tr>
<th>#</th>
<th>Action</th>
<th>Source code file</th>
<th>Team</th>
</tr>
<tr>
<td>1</td>
<td>Download Curator from Download (Windows)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Install the .msi file</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>

Create new folder: **D:\ELK\Curator**

Create new folder: **D:\ELK\Curator\Logs**

Create file named **curator-config.yml** in "**D:\ELK\Curator**" directory

add those properties on it

```
client:
  hosts:
    - localhost
  port: 9200
  use_ssl: False
  ssl_no_validate: False
  timeout: 30
  master_only: False

logging:
  loglevel: DEBUG
  logfile: C:\Users\mbali\Documents\curator\log
  logformat: default
  blacklist: ['elasticsearch', 'urllib3']
```

</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>

Create a file named **delete-old-indices.yml** in "**D:\ELK\Curator**" directory

Replace file "**delete-old-indices.yml**" content with the following:

```
actions:
  1:
    action: delete_indices
    description: >-
      Delete indices older than 3 days (based on index name), for filebeat-
      prefixed indices. Ignore the error if the filter does not result in an
      actionable list of indices (ignore_empty_list) and exit cleanly.
    options:
      ignore_empty_list: False
      timeout_override:
      continue_if_exception: True
      disable_action: False
      allow_ilm_indices: True
    filters:
    - filtertype: pattern
      kind: prefix
      value: filebeat-*
    - filtertype: age
      source: creation_date
      direction: older
      timestring: '%Y.%m.%d'
      unit: days
      unit_count: 30
```

</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Navigate to the installation folder - the default is (<b>C:\Program Files\elasticsearch-curator</b>)</td>
<td></td>
<td></td>
</tr>
</table>

6	run the command : `curator --config "D:\ELK\Curator\curator-config.yml" "D:\ELK\Curator\delete-old-indices.yml"`		
7	Haitham Mohamed Gamal Ahmed Mohamed Elazouny Add step to run Curator as windows service using NSSM tool		

Filebeat Installation

#	Action	Source code file	Team
1	Install and configure FileBeat as per below MRF Filebeat MRF		APP

ELK Initialization

#	Action	Source code file	Team
1	open **Kibana** throw the link http://localhost:5601/		
2	In "Welcome to Kibana" screen, Click **"Explore on my own"** option button.		
2	the site will ask you to select a space : go select "**default**"		
3	the site will ask you to add an index pattern : just type "filebeat-*" then press ext		
4	choose "@timestamp" as date filter : then press next		
5	set the created index-pattern as default by press star buttom		
6	press on **Index Management** link then **Index template** tab then click on filebeat row and press edit on actions		

7	press next till you reach aliases tab then type
	{
	"filebeat-7.5.2": {}
	}		

Rollback Procedure

	Action	Source code file	Team
1	Stop windows service Elasticsearch		
2	Delete Elasticsearch service		
3	Delete ELASTICSEARCH_HOME folder		
4	Stop windows service Kibana		
5	Delete Kibanaservice		
6	Delete KIBANA_HOME folder		
7	Stop windows service Logstash		
8	Delete Logstash service		
9	Delete LOGSTASH_HOME folder		

Release

	Release Number	URL	Team
1			

Known Bugs