SETUPS ON THE VIRTUAL MACHINE SIDE:

Install Elasticsearch w/ Docker:

**Pull the image from DockerHub:**

$ sudo docker pull docker.elastic.co/elasticsearch/elasticsearch-oss:7.9.3

**Starting a single node cluster container w/ Docker:**

$ docker run –-name Elasticsearch -p 9200:9200 -p 9300:9300 -e "discovery.type=single-node" docker.elastic.co/elasticsearch/elasticsearch-oss:7.9.3

Install Kibana w/ Docker:

**Pull the image from DockerHub:**

$ docker pull docker.elastic.co/kibana/kibana-oss:7.9.3

**Starting a Kibana container w/ Docker:**

$ docker run --link **YOUR\_ELASTICSEARCH\_CONTAINER\_NAME\_OR\_ID**:elasticsearch -p 5601:5601 docker.elastic.co/kibana/kibana-oss:7.9.3

SETUPS ON THE WINDOWS HOST SIDE:

Install Filebeat binary:

<https://www.elastic.co/downloads/past-releases/filebeat-oss-7-9-3>

**Run Powershell as Admin(A):**

$ .\install-service-filebeat.ps1

Configure Filebeat:

**Connect w/ Elasticsearch:**

In the *filebeat.yml*:

output.elasticsearch:

hosts: ["myEShost:9200"]

username: "filebeat\_internal"

password:

**Connect w/ Kibana:**

In the *filebeat.yml*:

setup.kibana:

host: "mykibanahost:5601"

username:

password:

**Enable IIS Module:**

Run Powershell (A):

$ .\filebeat.exe modules enable IIS

**Specify log files’ location:**

Edit file …\filebeat-oss-7.9.3-windows-x86\_64\filebeat-7.9.3-windows-x86\_64\modules.d\iis.yml

Apply the following changes:

- module: nginx

access:

var.paths: ["ABSOLUTE PATH TO THE LOG FILES\*"]

**Set up assets:**

Run Powershell(A):

.\filebeat.exe setup -e

Launch Filebeat:

Run Powershell(A):

C:\Program Files\filebeat> Start-Service filebeat -c .\filebeat.tml

Visit Kibana from Browser:

In you browser:

[Kibana Host]

e.g. 192.168.56.1:5601

Ta-da!!!