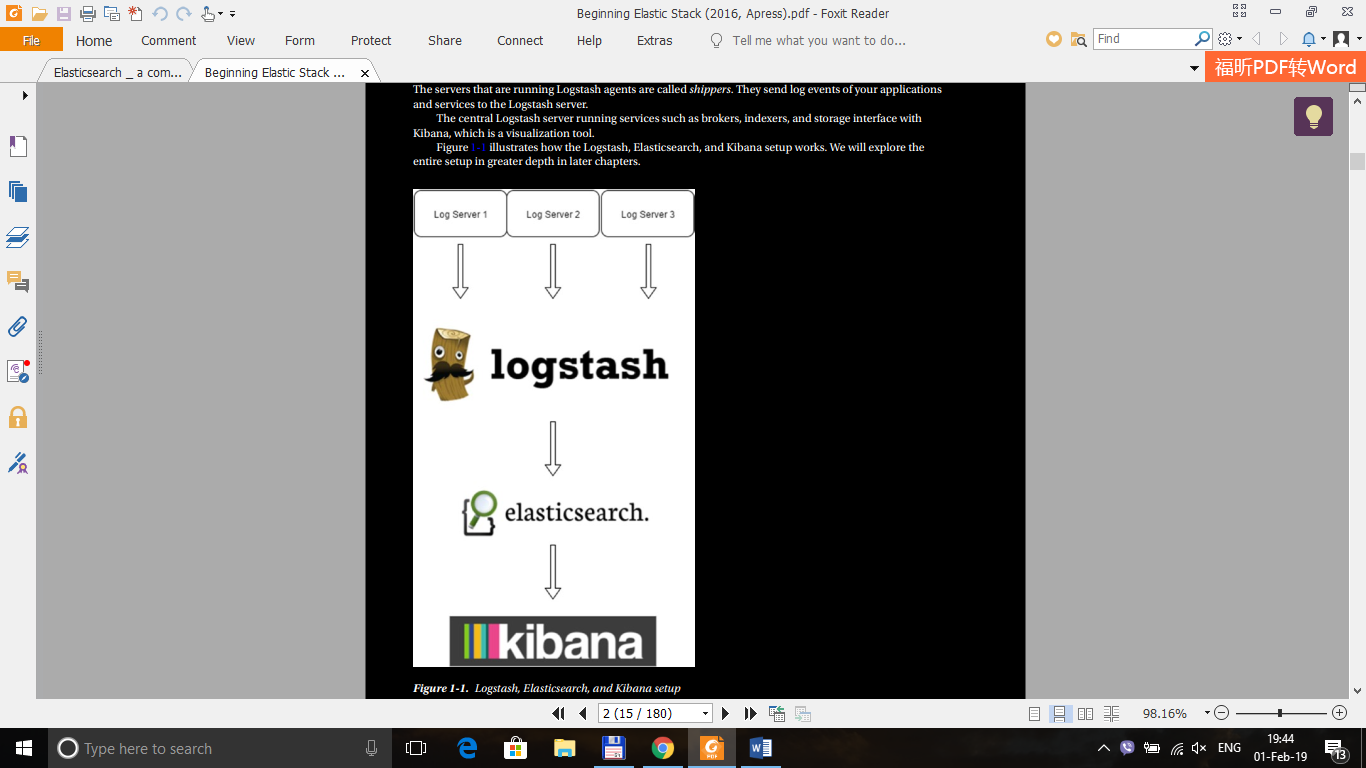
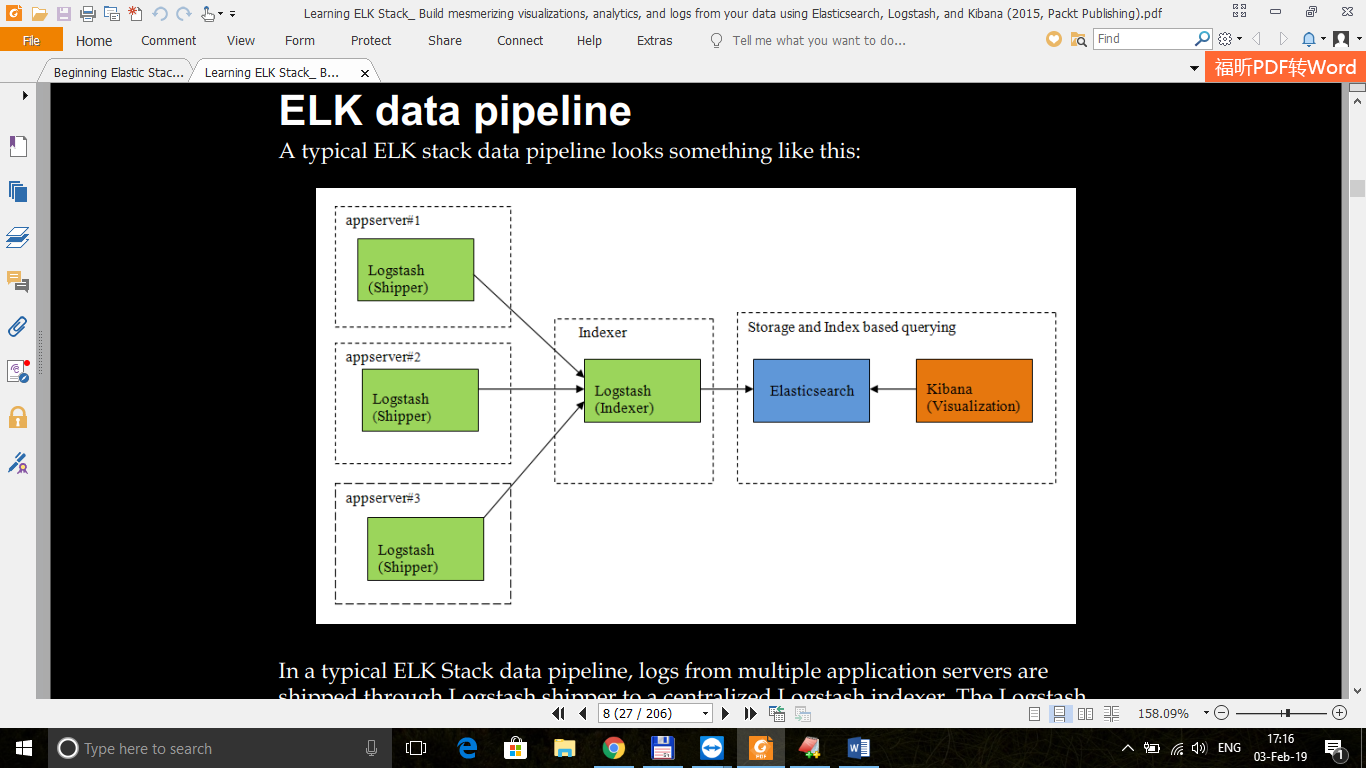
**LOGSTASH**

- Logstash is an open source tool designed to manage all of your server logs in a centralized location.

- The servers that are running Logstash agents are called shippers. They send log events of your applications and services to the Logstash server.  
- The central Logstash server running services such as brokers, indexers, and storage interface with Kibana, which is a visualization tool.





- **Logstash** collects data from the different sources defined by using the configuration file.

- **Elasticsearch** does real-time data analysis from different data sources.

- **Kibana** is a web application designed to visualize data in Elasticsearch.

**SETUP ENVIRONMENT**

1. Install Java

sudo yum install java-1.8.0-openjdk

2. Install LogStash

a. Download and install the public signing key

rpm --import <https://artifacts.elastic.co/GPG-KEY-elasticsearch>

b. Create a new file /etc/yum.repos.d/logstash.rep

[logstash-6.x]

name=Elastic repository for 6.x packages

baseurl=https://artifacts.elastic.co/packages/6.x/yum

gpgcheck=1

gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch

enabled=1

autorefresh=1

type=rpm-md

c. Run sudo yum install logstash

Note : logstash will be installed etc/share/logstash

Start and check statu service of logstash :

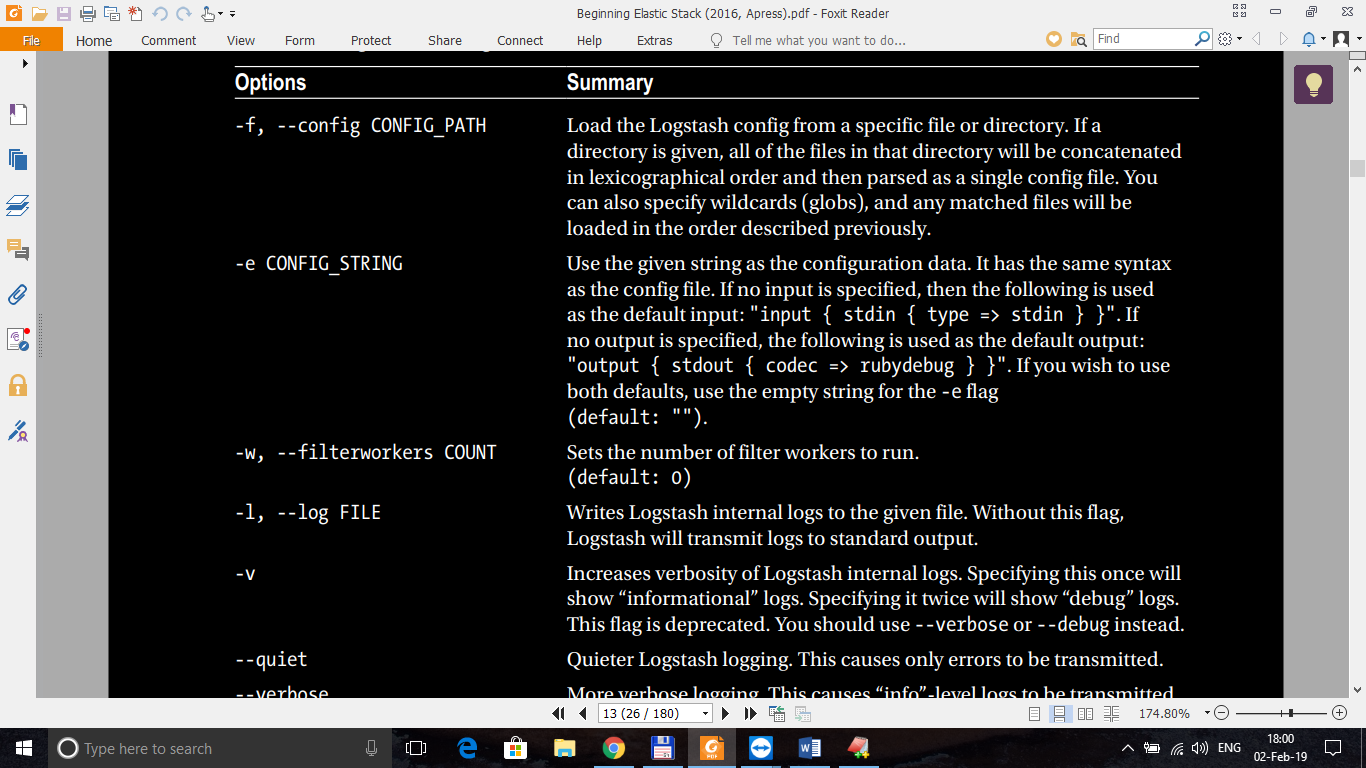
*systemctl enable logstash.service*

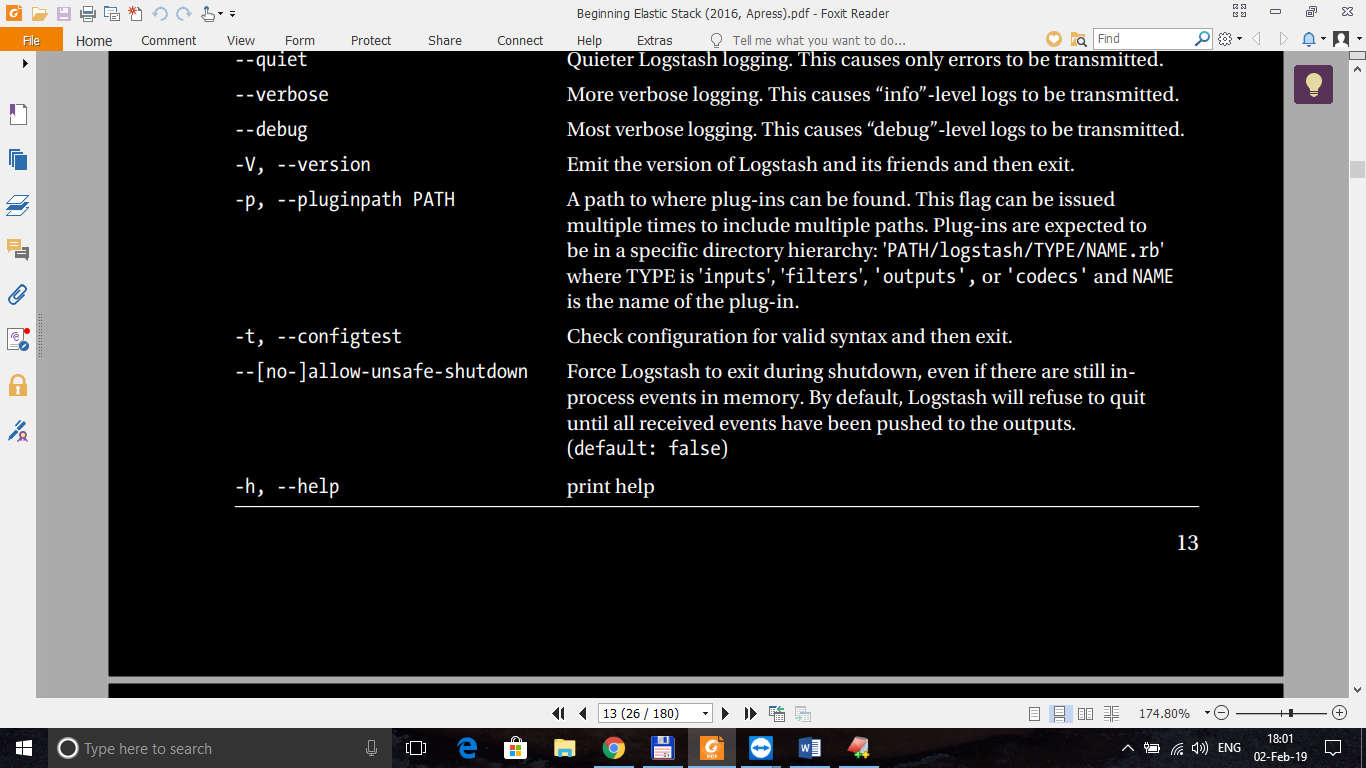
*systemctl start logstash.service*

*systemctl status logstash.service*

RUN CONFIGURE FILE :

./logstash -f /etc/logstash/conf.d/config.conf





**3. Install Elasticsearch**

a. Do as 2.a

b. Create a new file /etc/yum.repos.d/elasticsearch.rep

[elasticsearch-6.x]

name=Elasticsearch repository for 6.x packages

baseurl=https://artifacts.elastic.co/packages/6.x/yum

gpgcheck=1

gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch

enabled=1

autorefresh=1

type=rpm-md

[sudo systemctl enable elasticsearch.service], [sudo chkconfig --add elasticsearch],

[sudo /bin/systemctl daemon-reload

sudo /bin/systemctl enable elasticsearch.service]

* : will add Elasticsearch to init scripts, so  
  that it will start while CentOS is booting

Elasticsearch can be started and stopped using the service command:

* sudo -i service elasticsearch start
* sudo -i service elasticsearch stop

c. Test Server

- Uncomment *network.host* and *http.port* in file **/etc/elasticsearch/ elasticsearch.yml**

**-** Restart server : sudo service elasticsearch restart

**-** To test our installation to see if it is running on port 9200

C1. Run : curl -X GET http://huydu02-e20652:9200/

C2. Go <http://huydu02-e20652:9200/> to test server

**4. Install Kabian**

a. Do 2.a or 3.a

b. Create a new file /etc/yum.repos.d/kibana.rep

[kibana-6.x]

name=Kibana repository for 6.x packages

baseurl=https://artifacts.elastic.co/packages/6.x/yum

gpgcheck=1

gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch

enabled=1

autorefresh=1

type=rpm-md

Run : sudo yum install kibana

Use the chkconfig command to configure Kibana to start automatically when the system boots up:

sudo chkconfig --add kibana

You can start and stop Kibana using the service command:

sudo -i service kibana start

sudo -i service kibana stop

The output that you see is the most common output that we generally see  
from Logstash:  
• "message" includes the complete input message or the event line  
• "@timestamp" will include the timestamp of the time when the event was  
indexed; or if date filter is used, this value can also use one of the fields in the  
message to get a timestamp specific to the event  
• "host" will generally represent the machine where this event was generated

Check config before run : bin/logstash –configtest ../conf/logstash.conf

