USER MANUAL

Splunk Installation

1. Go to http://www.splunk.com/en_us/download/splunk-light.html. Download the .deb file for linux for splunk light
2. Run the .deb file. or .tar file
3. If it's the .tar file then untar it and do the below.
4. Run the following steps:
    a. sudo su
    b. cd /opt/splunk/bin
    c. ./splunk start --accept-licence
    d. Set the Path for $SPLUNK_HOME.
    e. Go to the the shown web address and login using
    username : admin
    password : changeme
    change the password

The subsequent usage:

1. ./splunk start
2. Go to the the shown web address and login using
3. login to the website
    username: admin
    password : *******
4. ./splunk stop

ELK Installation

1. sudo apt-get update
2. sudo apt-get upgrade

Install Java

3. sudo apt-get install openjdk-7-jre-headless

Install ElasticSearch

4. wget -qO - https://packages.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add –
5. echo "deb http://packages.elastic.co/elasticsearch/1.7/debian stable main" | sudo tee -a /etc/apt/sources.list.d/elasticsearch-1.7.list
6. sudo apt-get update
7. sudo apt-get install elasticsearch
8. sudo service elasticsearch restart

   check status using the following command
   curl localhost:9200
   the output should be :

```
{
    "status" : 200,
    "name" : "Jigsaw",
    "cluster_name" : "elasticsearch",
    "version" : {
            "number" : "1.7.1",
            "build_hash" : "b88f43fc40b0bcd7f173a1f9ee2e97816de80b19",
            "build_timestamp" : "2015-07-29T09:54:16Z",
            "build_snapshot" : false,
            "lucene_version" : "4.10.4"
    },
    "tagline" : "You Know, for Search"
}
```

9. sudo update-rc.d elasticsearch defaults 95 10

Install Logstash

10. echo "deb http://packages.elasticsearch.org/logstash/1.5/debian stable main" | sudo tee -a /etc/apt/sources.list
11. sudo apt-get update
12. sudo apt-get install logstash
13. sudo update-rc.d logstash defaults 97 8
14. sudo service logstash start

    check status using the following command

    sudo service logstash status
15. Create and configure the /etc/logstash/conf.d/logstash.conf file
16. sudo vim sudo service logstash restart
17. cd

Installing Kibana4

18. wget https://download.elastic.co/kibana/kibana/kibana-4.1.1-linux-x64.tar.gz
19. tar -xzf kibana-4.1.1-linux-x64.tar.gz
20. sudo mkdir -p /opt/kibana
21. sudo mv kibana-4.1.1-linux-x64/* /opt/kibana
22. cd /etc/init.d && sudo wget https://raw.githubusercontent.com/akabdog/scripts/master/kibana4_init -O kibana4
23. sudo chmod +x /etc/init.d/kibana4
24. sudo update-rc.d kibana4 defaults 96 9
25. sudo service kibana4 start
26. In your browser type the following URL to open the kibana dashboard

    http://localhost:5601

Making communication between the servers passwordless

1. Login to main server (for us 10.10.1.97)

i. ssh-keygen
ii. ssh-copy-id -i ~/.ssh/id_rsa.pub ubuntu@10.10.1.98
iii. ssh-copy-id -i ~/.ssh/id_rsa.pub ubuntu@10.10.1.99
iv. Now ssh to 10.10.1.98 and 10.10.1.99 should be passwordless

Login to 10.10.1.98

i. ssh-keygen
ii. ssh-copy-id -i ~/.ssh/id_rsa.pub ubuntu@10.10.1.97
iii. Now ssh to 10.10.1.97 should be passwordless

Login to 10.10.1.99

i. ssh-keygen
ii. ssh-copy-id -i ~/.ssh/id_rsa.pub ubuntu@10.10.1.97
iii. Now ssh to 10.10.1.97 should be passwordless

Making communication between the servers passwordless

sudo visudo

ALL ALL = (root) NOPASSWD: /home/ubuntu/Logs/Logs_script

Makes the above script run without asking for password

Using the webpage

Go to http://10.10.1.97/OLAV