Searchguard version : 5.4.1-14

Kibana Version: 5.4.1

Elasticsearch: 5.4.1-1

Logstash: 5.4.1

Filebeat: 5.4.1

cd /usr/share/elasticsearch/bin

- > **Installing Searchguard plugin in elasticsearch**

1) ./elasticsearch-plugin install -b com.floragunn:search-guard-5:5.4.1-14

Output:

-> Downloading com.floragunn:search-guard-5:5.4.1-14 from maven central

[=================================================] 100%

@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@

@ WARNING: plugin requires additional permissions @

@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@

\* java.io.FilePermission /proc/sys/net/core/somaxconn read

\* java.lang.RuntimePermission accessClassInPackage.sun.misc

\* java.lang.RuntimePermission accessClassInPackage.sun.nio.ch

\* java.lang.RuntimePermission accessClassInPackage.sun.security.x509

\* java.lang.RuntimePermission accessDeclaredMembers

\* java.lang.RuntimePermission getClassLoader

\* java.lang.RuntimePermission loadLibrary.\*

\* java.lang.RuntimePermission setContextClassLoader

\* java.lang.RuntimePermission shutdownHooks

\* java.lang.reflect.ReflectPermission suppressAccessChecks

\* java.security.SecurityPermission getProperty.ssl.KeyManagerFactory.algorithm

\* java.security.SecurityPermission setProperty.ocsp.enable

\* java.util.PropertyPermission com.sun.security.enableCRLDP write

\* java.util.PropertyPermission es.set.netty.runtime.available.processors write

\* java.util.PropertyPermission java.security.debug write

\* java.util.PropertyPermission java.security.krb5.conf write

\* java.util.PropertyPermission javax.security.auth.useSubjectCredsOnly write

\* java.util.PropertyPermission sun.nio.ch.bugLevel write

\* java.util.PropertyPermission sun.security.krb5.debug write

\* java.util.PropertyPermission sun.security.spnego.debug write

\* javax.security.auth.AuthPermission doAs

\* javax.security.auth.AuthPermission modifyPrivateCredentials

\* javax.security.auth.kerberos.ServicePermission \* accept

See http://docs.oracle.com/javase/8/docs/technotes/guides/security/permissions.html

for descriptions of what these permissions allow and the associated risks.

–-------> search-guard-5 Installed ←--------------------

2) chmod u+x search-guard-5/tools/install\_demo\_configuration.sh && search-guard-5/tools/install\_demo\_configuration.sh

Output:

## Search Guard Demo Installer ##

Warning: Do not use on production or public reachable systems

Continue? [y/N] y

This script maybe require your root password for 'sudo' privileges

Elasticsearch install type: rpm/deb

Elasticsearch config dir: /etc/elasticsearch

Detected Elasticsearch Version: 5.4.1

Detected Search Guard Version: 5.4.1-14

### Success

### Execute this script now on all your nodes and then start all nodes

### After the whole cluster is up execute:

sudo /usr/share/elasticsearch/plugins/search-guard-5/tools/sgadmin.sh -cd /usr/share/elasticsearch/plugins/search-guard-5/sgconfig -cn searchguard\_demo -ks /etc/elasticsearch/kirk.jks -ts /etc/elasticsearch/truststore.jks -nhnv

### or run ./sgadmin\_demo.sh

### Then open https://localhost:9200 an login with admin/admin

### (Just ignore the ssl certificate warning because we installed a self signed demo certificate)

Note: Searchguard plugin will append its own configuration at the bottom of the /etc/elasticsearch/elasticsearch.yml. You may have to reconfigure certain parameters to avoid duplicity.

If you get sg\_admin.sh inside “/usr/share/elasticsearch/plugins”, please move it to “search-guard-5/tools/”.

3) ./sgadmin\_demo.sh

WARNING: JAVA\_HOME not set, will use /usr/bin/java

Search Guard Admin v5

Will connect to localhost:9300 ... done

### LICENSE NOTICE Search Guard ###

If you use one or more of the following features in production

make sure you have a valid Search Guard license

(See https://floragunn.com/searchguard-validate-license)

\* Kibana Multitenancy

\* LDAP authentication/authorization

\* Active Directory authentication/authorization

\* REST Management API

\* JSON Web Token (JWT) authentication/authorization

\* Kerberos authentication/authorization

\* Document- and Fieldlevel Security (DLS/FLS)

\* Auditlogging

In case of any doubt mail to <sales@floragunn.com>

###################################

Contacting elasticsearch cluster 'searchguard\_demo' and wait for YELLOW clusterstate ...

Clustername: searchguard\_demo

Clusterstate: YELLOW

Number of nodes: 1

Number of data nodes: 1

searchguard index already exists, so we do not need to create one.

Populate config from /usr/share/elasticsearch/plugins/search-guard-5/sgconfig/

Will update 'config' with /usr/share/elasticsearch/plugins/search-guard-5/sgconfig/sg\_config.yml

SUCC: Configuration for 'config' created or updated

Will update 'roles' with /usr/share/elasticsearch/plugins/search-guard-5/sgconfig/sg\_roles.yml

SUCC: Configuration for 'roles' created or updated

Will update 'rolesmapping' with /usr/share/elasticsearch/plugins/search-guard-5/sgconfig/sg\_roles\_mapping.yml

SUCC: Configuration for 'rolesmapping' created or updated

Will update 'internalusers' with /usr/share/elasticsearch/plugins/search-guard-5/sgconfig/sg\_internal\_users.yml

SUCC: Configuration for 'internalusers' created or updated

Will update 'actiongroups' with /usr/share/elasticsearch/plugins/search-guard-5/sgconfig/sg\_action\_groups.yml

SUCC: Configuration for 'actiongroups' created or updated

Done with success

4) Now edit /etc/elasticsearch/elasticsearch.yml and make this parameter from true to false as

searchguard.ssl.http.enabled: false

and add following lines to avoid shards failure in large log query result,

thread\_pool.search.queue\_size: 10000 (there is underscore between thread and pool from elasticsearch 5 but not before)

5) Now restart elasticsearch

6) check by

curl -XGET –-user admin:admin [http://localhost:9200](http://localhost:9200/)

Output:

{

"name" : "ELK1",

"cluster\_name" : "searchguard\_demo",

"cluster\_uuid" : "NhkUm3j7RLuKrYf1P1etuA",

"version" : {

"number" : "5.4.1",

"build\_hash" : "2cfe0df",

"build\_date" : "2017-05-29T16:05:51.443Z",

"build\_snapshot" : false,

"lucene\_version" : "6.5.1"

},

"tagline" : "You Know, for Search"

}

Note: Don't copy command from word as it will format it and thus wrong command can be copied

–--> Searchguard configured in elasticsearch ←----------

**Applying Searchguard in Kibana**

7) mkdir -p /opt/package

8) cd /opt/package

9) wget https://github.com/floragunncom/search-guard-kibana-plugin/releases/download/v5.4.1-3/searchguard-kibana-5.4.1-3.zip

10) bin/kibana-plugin install <file:///opt/package/searchguard-kibana-5.4.1-3.zip>

11) Edit kibana.yml as

server.host: "local-ip-address"

elasticsearch.url: [https://127.0.0.1:9200](https://127.0.0.1:9200/)

elasticsearch.username: "kibanaserver"

elasticsearch.password: "kibanaserver"

elasticsearch.ssl.verificationMode: none

server.ssl.enabled: false

also uncomment elasticsearch.requestTimeout and set it to 50000 in place of 30000 , as in case of fetching large result, this timout can prove to be smaller

12. Edit /usr/share/elasticsearch/plugins/search-guard-5/sgconfig/sg\_config.yml

Under authz add

type: noop

**Curator Installation**

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

14. yum install elasticsearch-curator -y

15. cd /opt/

16. mkdir curator\_config

17. cd curator\_config/

**Installation of s3-repository plugin**

18. cd /usr/share/elasticsearch

19. bin/elasticsearch-plugin install repository-s3

20. service elasticsearch restart

Command to register s3-repository

21. curl --insecure -XPUT --user admin:admin 'https://localhost:9200/\_snapshot/s3\_repository?verify=false' -H 'Content-Type: application/json' -d '

{

"type": "s3",

"settings": {

"bucket": "elkstackbucket",

"region": "us-east-1"

}

}'

**Make Curator Removal Script**

#!/bin/bash

22. curator\_cli --ssl-no-validate --use\_ssl --http\_auth admin:admin show\_indices

23. curator\_cli --ssl-no-validate --use\_ssl --http\_auth admin:admin snapshot --repository s3\_repository --ignore\_unavailable --partial --filter\_list '[{"filtertype":"age","source":"creation\_date","direction":"older","unit":"days","unit\_count":45},{"filtertype":"pattern","kind":"prefix","value":"filebeat"}]'

24. curator\_cli --ssl-no-validate --use\_ssl --http\_auth admin:admin delete\_indices --ignore\_empty\_list --filter\_list '[{"filtertype":"age","source":"creation\_date","direction":"older","unit":"days","unit\_count":45},{"filtertype":"pattern","kind":"prefix","value":"filebeat"}]'

→ → At this point searchguard is applied in elasticsearch and kibana on master node ← ←

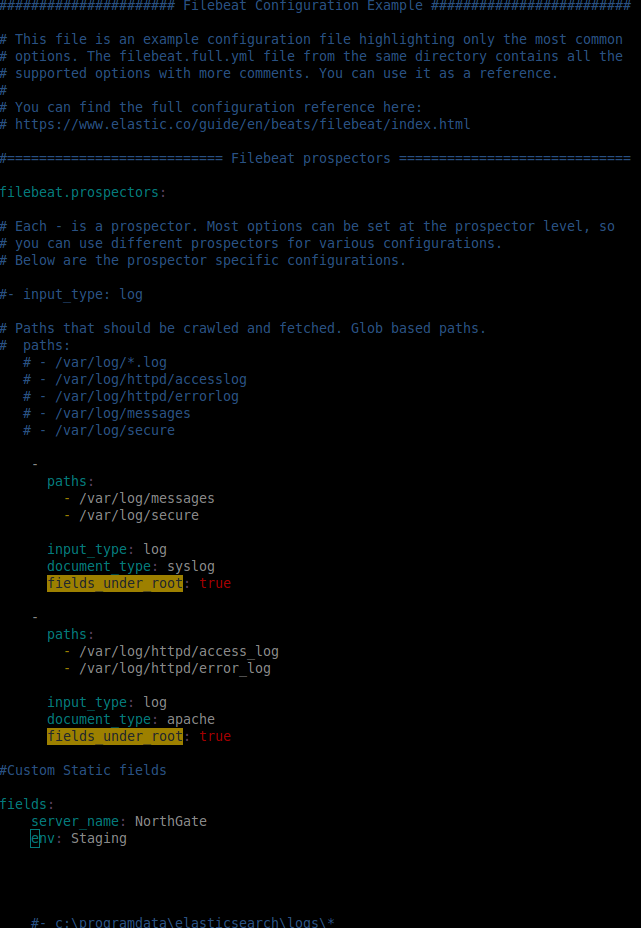
**Configuring Data Node**

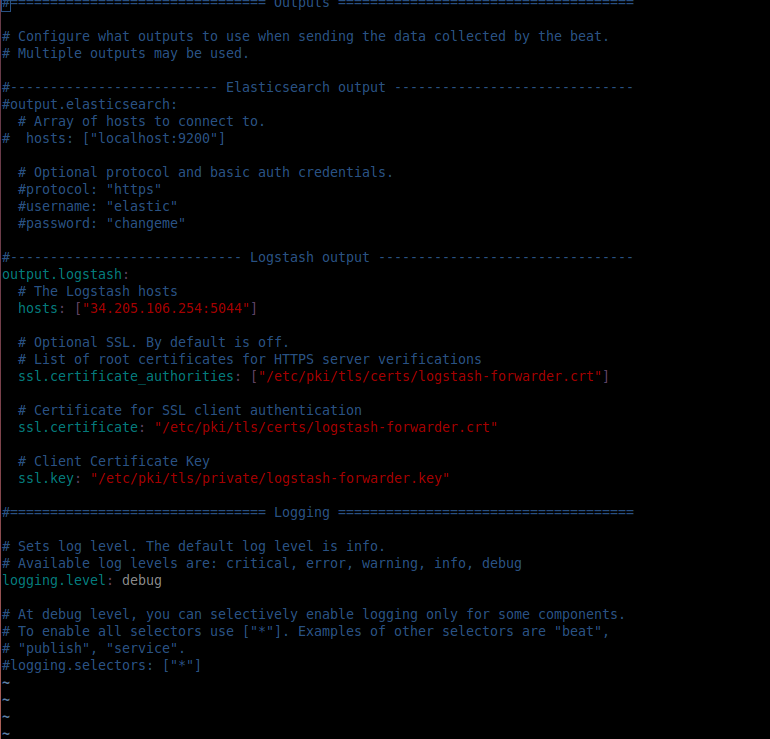
**Installing Filebeat on Data Node**

1) curl -L -O <https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-5.4.1-x86_64.rpm>

2) sudo rpm -vi filebeat-5.4.1-x86\_64.rpm

3) configure /etc/filebeat/filebeat.yml as



Expand images to see configuration.

In ssl.certificate\_authorities same .crt goes that lies in ELK Server or Master Node.

During Installation we keep it in /etc/pki/tls, in folder certs logstash\_forwarder.crt and in folder private as logstash\_forwarder.key

IP in hosts is of ELK Server or Master node or node in which logstash is running.

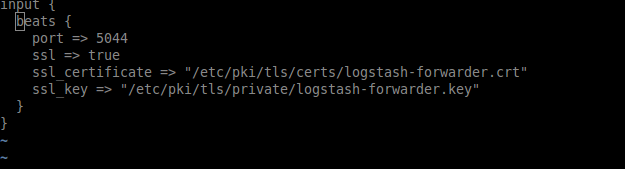
4) Start Filebeat by /etc/init.d/filebeat restart

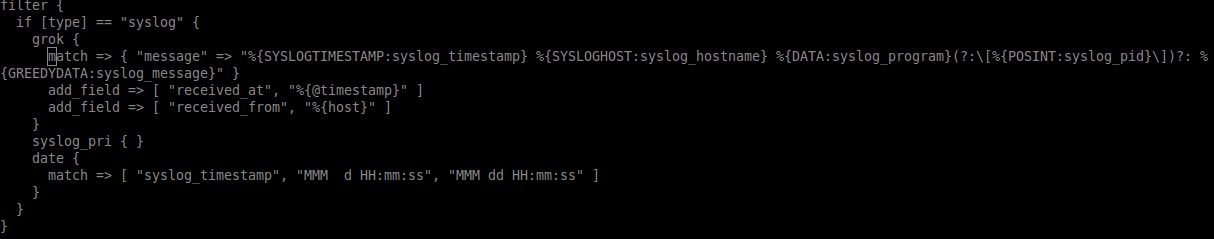
**Switch to ELK Server**

1) Now we need to add configuration files that hear filebeat, collect logs, apply filters and push to elasticsearch.

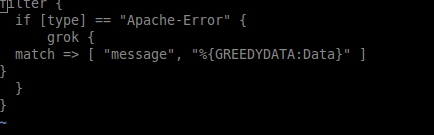
2) We add these configuration files in /etc/logstash/conf.d as

02-beats-input.conf(to hear beats)

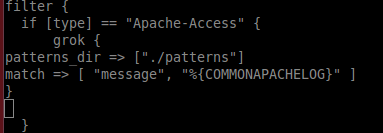
10-syslog-filter.conf(to filter syslogs)



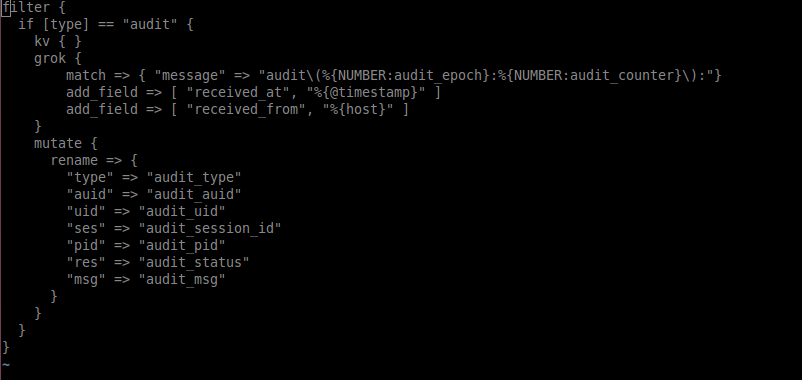
15-apache-error.conf(to filter apache error logs)

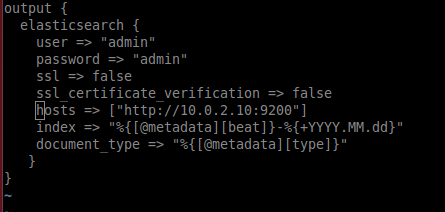


20-apache-access.conf(to filter apache access logs)



25-audit.conf(to filter audit logs)

30-elasticsearch-output.conf (to push to elasticsearch)



3) Now to run this configurations go to /usr/share/logstash/bin and type

./logstash -f /etc/logstash/conf.d (If logstash not previously running)

(else first stop logstash and then run this command)

4) Hit kibana, enter admin:admin password in secureguard and go to Discover, Hit on Data node server, you must be able to see logs coming in access log of Data node server on Kibana in last 15 minutes check.