**Filebeat Configuration on Servers**

1. Install filebeat on server as:

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

This will install filebeat 5.4.1 . In case there felt need to change version, we also need to change elasticsearch, kibana and logstash version.

2. Copy logstash-forwarder.crt to /etc/pki/tls/certs and logstash-forwarder.key in /etc/pki/tls/private . You need to take these files from server in which logstash is running from same location.

3. Edit /etc/filebeat/filebeat.yml as

Provide Logs path according to server. Like for ubuntu path to system messages log file is /var/log/syslog while for Centos it is /var/log/messages. Also You can add as no of log files as you want to passed to logstash, evaluated by it, saved in elasticsearch and visualized on kibana.

**###################### Filebeat Configuration Example #########################**

**# This file is an example configuration file highlighting only the most common**

**# options. The filebeat.full.yml file from the same directory contains all the**

**# supported options with more comments. You can use it as a reference.**

**#**

**# You can find the full configuration reference here:**

**# https://www.elastic.co/guide/en/beats/filebeat/index.html**

**#=========================== Filebeat prospectors =============================**

**filebeat.prospectors:**

**# Each - is a prospector. Most options can be set at the prospector level, so**

**# you can use different prospectors for various configurations.**

**# Below are the prospector specific configurations.**

**#- input\_type: log**

**# Paths that should be crawled and fetched. Glob based paths.**

**# paths:**

**# - /var/log/\*.log**

**# - /var/log/httpd/accesslog**

**# - /var/log/httpd/errorlog**

**# - /var/log/messages**

**# - /var/log/secure**

**-**

**paths:**

**- /var/log/syslog**

**input\_type: log**

**document\_type: messages**

**fields\_under\_root: true**

**-**

**paths:**

**- /var/log/apache2/access.log**

**- /var/log/apache2/ssl\_access.log**

**input\_type: log**

**ignore\_older: 10s**

**document\_type: apache\_access**

**fields\_under\_root: true**

**-**

**paths:**

**- /var/log/apache2/error.log**

**input\_type: log**

**document\_type: apache\_error**

**fields\_under\_root: true**

**-**

**paths:**

**- /var/log/audit/audit.log**

**input\_type: log**

**document\_type: audit**

**fields\_under\_root: true**

**-**

**paths:**

**- /var/log/auth.log**

**input\_type: log**

**document\_type: secure**

**fields\_under\_root: true**

**#Custom Static fields**

**fields:**

**server\_name: Bluebook**

**env: Production**

**#- c:\programdata\elasticsearch\logs\\***

**# Exclude lines. A list of regular expressions to match. It drops the lines that are**

**# matching any regular expression from the list.**

**#exclude\_lines: ["^DBG"]**

**# Include lines. A list of regular expressions to match. It exports the lines that are**

**# matching any regular expression from the list.**

**#include\_lines: ["^ERR", "^WARN"]**

**# Exclude files. A list of regular expressions to match. Filebeat drops the files that**

**# are matching any regular expression from the list. By default, no files are dropped.**

**#exclude\_files: [".gz$"]**

**# Optional additional fields. These field can be freely picked**

**# to add additional information to the crawled log files for filtering**

**#fields:**

**# level: debug**

**# review: 1**

**### Multiline options**

**# Mutiline can be used for log messages spanning multiple lines. This is common**

**# for Java Stack Traces or C-Line Continuation**

**# The regexp Pattern that has to be matched. The example pattern matches all lines starting with [**

**#multiline.pattern: ^\[**

**# Defines if the pattern set under pattern should be negated or not. Default is false.**

**#multiline.negate: false**

**# Match can be set to "after" or "before". It is used to define if lines should be append to a pattern**

**# that was (not) matched before or after or as long as a pattern is not matched based on negate.**

**# Note: After is the equivalent to previous and before is the equivalent to to next in Logstash**

**#multiline.match: after**

**#================================ General =====================================**

**# The name of the shipper that publishes the network data. It can be used to group**

**# all the transactions sent by a single shipper in the web interface.**

**#name:**

**# The tags of the shipper are included in their own field with each**

**# transaction published.**

**#tags: ["service-X", "web-tier"]**

**# Optional fields that you can specify to add additional information to the**

**# output.**

**#fields:**

**# env: staging**

**#================================ Outputs =====================================**

**# Configure what outputs to use when sending the data collected by the beat.**

**# Multiple outputs may be used.**

**#-------------------------- Elasticsearch output ------------------------------**

**#output.elasticsearch:**

**# Array of hosts to connect to.**

**# hosts: ["localhost:9200"]**

**# Optional protocol and basic auth credentials.**

**#protocol: "https"**

**#username: "elastic"**

**#password: "changeme"**

**#----------------------------- Logstash output --------------------------------**

**output.logstash:**

**# The Logstash hosts**

**hosts: ["34.205.106.254:5044"]**

**# Optional SSL. By default is off.**

**# List of root certificates for HTTPS server verifications**

**ssl.certificate\_authorities: ["/etc/pki/tls/certs/logstash-forwarder.crt"]**

**# Certificate for SSL client authentication**

**ssl.certificate: "/etc/pki/tls/certs/logstash-forwarder.crt"**

**# Client Certificate Key**

**ssl.key: "/etc/pki/tls/private/logstash-forwarder.key"**

**#================================ Logging =====================================**

**# Sets log level. The default log level is info.**

**# Available log levels are: critical, error, warning, info, debug**

**logging.level: debug**

**# At debug level, you can selectively enable logging only for some components.**

**# To enable all selectors use ["\*"]. Examples of other selectors are "beat",**

**# "publish", "service".**

**#logging.selectors: ["\*"]**

Now save and exit from filebeat.yml and restart filebeat.

4. Now open 5044 port on server on which logstash is running for IP of server on which you are installing filebeat.

5. Now check by tail /var/log/filebeat/filebeat.log, if logs starts comming and no error is comming that means everything is working fine.

6. Now configure logstash by writng suitable grok that can deal with log format you are providing in log files configured in filebeat.yml and extract useful information from it. To configure it you need to edit files in /etc/logstash/conf.d

7. Now restart logstash.

8. Now create profile in searchguard for that particular server and provide username and password to user who will monitor server on kibana.