Elk-playbook.yml

```
- name: Config ELK with Docker
 hosts: elk
 become: true
 tasks:
- name: Install docker.io
 apt:
 update_cache: yes
 name: docker.io
 state: present

 - name: Install pip3
 apt:
 force_apt_get: yes
 name: python3-pip
 state: present

 - name: Install Docker Python Module
 pip:
 name: docker
 state: present

- name: Download and launch a Docker web container
 docker_container:
 name: elk
 image: sebp/elk:761
 state: started
 restart_policy: always
 published_ports:
 - 5601:5601
 - 9200:9200
 - 5044:5044

- name: Configure elk VM to use more memory
 sysctl:
 name: vm.max_map_count
 value: "262144"
 state: present
 reload: yes

- name: Enable Docker service
 systemd:
 name: docker
```

Ansible Hosts

```
[webservers]
10.0.0.6 ansible_python_interpreter=/usr/bin/python3
10.0.0.7 ansible_python_interpreter=/usr/bin/python3
[elk]
10.1.0.4 ansible_python_interpreter=/usr/bin/python3
```

Filebeat-Configuration

```
# https://www.elastic.co/guide/en/beats/filebeat/index.html
filebeat.config.modules:
 path: ${path.config}/modules.d/*.yml
#========================= Modules configuration
============================
filebeat.modules:
- module: elasticsearch
 # Server log
 server:
 enabled: true

 # Set custom paths for the log files. If left empty,
 # Filebeat will choose the paths depending on your OS.
 #var.paths:

 gc:
 enabled: true
 # Set custom paths for the log files. If left empty,
 # Filebeat will choose the paths depending on your OS.
 #var.paths:

audit:
 enabled: true
 # Set custom paths for the log files. If left empty,
 # Filebeat will choose the paths depending on your OS.
 #var.paths:

slowlog:
 enabled: true
 # Set custom paths for the log files. If left empty,
 # Filebeat will choose the paths depending on your OS.
 #var.paths:

deprecation:
 enabled: true
```

```
- module: haproxy
 # All logs
 log:
 enabled: true
           # Set which input to use between syslog (default) or file.
           #var.input:
#------------------------------- Kafka Module
-------------------------------
- module: kafka
 log:
 enabled: true

 # Set custom paths for Kafka. If left empty,
 # Filebeat will look under /opt.
 #var.kafka_home:

 # Set custom paths for the log files. If left empty,
 # Filebeat will choose the paths depending on your OS.
 #var.paths:
#------------------------------- Kibana Module
-------------------------------
- module: kibana
 # All logs
 log:
 enabled: true

- module: nats
 # All logs
 log:
 enabled: true
#--------------------------- Google Santa Module
---------------------------
- module: santa
 log:
 enabled: true
filebeat.inputs:
# Each - is an input. Most options can be set at the input level, so
# you can use different inputs for various configurations.
# Below are the input specific configurations.

# Type of the files. Based on this the way the file is read is decided.
# The different types cannot be mixed in one input
#
# Possible options are:
```

```
# * log: Reads every line of the log file (default)
# * stdin: Reads the standard in
#------------------------------ Log input ----------------------------------
- type: log

 # Change to true to enable this input configuration.
 enabled: false

# Paths that should be crawled and fetched. Glob based paths.
 # To fetch all ".log" files from a specific level of subdirectories
 # /var/log/*/*.log can be used.
 # For each file found under this path, a harvester is started.
 # Make sure not file is defined twice as this can lead to unexpected
behaviour.
 paths:
 - /var/log/*.log
 #- c:\programdata\elasticsearch\logs\*
 # Configure the file encoding
#------------------------- Elasticsearch output
-------------------------------
output.elasticsearch:
 # Boolean flag to enable or disable the output module.
 #enabled: true
 # Array of hosts to connect to.
 # Scheme and port can be left out and will be set to the default (http
and 9200)
 # In case you specify and additional path, the scheme is required:
http://localhost:9200/path
 # IPv6 addresses should always be defined as: https://[2001:db8::1]:9200
 hosts: ["10.1.0.4:9200"]
 username: "elastic"
 password: "changeme"
 setup.template.settings:
 setup.kibana:
 host: "10.1.0.4:5601"
# files.
logging.to_files: true
logging.files:
```

Ansible-playbook.yml

```
 - name: Config Web VM with Docker
 hosts: webservers
 become: true
 tasks:
 - name: docker.io
 apt:
 update_cache: yes
 name: docker.io
 state: present
 - name: Install pip3
 apt:
 name: python3-pip
 state: present
 - name: Install Python Docker Module
 pip:
 name: docker
 state: present
 - name: Download and launch a docker web container
 docker_container:
 name: dvwa
 image: cyberxsecurity/dvwa
 state: started
 restart_policy: always
 published_ports: 80:80
```

Filebeat-playbook.yml

```
 - name: Installing and Launching Filebeat
 hosts: webservers
 become: yes
 tasks:

- name: Download filebeat .deb file
 command: curl -L -O
https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.4.0-
amd64.deb

 - name: Install filebeat.deb
 command: sudo dpkg -i filebeat-7.4.0-amd64.deb

 - name: Drop in filebeat.yml
 copy:
 src: /etc/ansible/files/filebeat-config.yml
 dest: /etc/filebeat/filebeat.yml

 - name: Enable and configure system module
 command: filebeat modules enable system

 - name: Setup filebeat
 command: filebeat setup
 - name: Start filebeat service
 command: service filebeat start

- name: Enable service filebeat on boot
 systemd:
 name: filebeat
 enabled: yes
```

Metricbeat-configuration

```
# You can find the full configuration reference here:
# https://www.elastic.co/guide/en/beats/metricbeat/index.html
#========================== Modules configuration
============================
metricbeat.config.modules:
 # Glob pattern for configuration loading
 path: ${path.config}/modules.d/*.yml
 # Set to true to enable config reloading
 reload.enabled: false
 # Period on which files under path should be checked for changes
 #reload.period: 10s
#==================== Elasticsearch template setting
==========================
setup.template.settings:
 index.number_of_shards: 1
 index.codec: best_compression
 #_source.enabled: false
#================================ 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
#============================== Dashboards
=====================================
# These settings control loading the sample dashboards to the Kibana
index. Loading
```

```
# the dashboards is disabled by default and can be enabled either by
setting the
# options here or by using the `setup` command.
#setup.dashboards.enabled: false
# The URL from where to download the dashboards archive. By default this
URL
# has a value which is computed based on the Beat name and version. For
released
# versions, this URL points to the dashboard archive on the
artifacts.elastic.co
# website.
#setup.dashboards.url:
#============================== Kibana
=====================================
# Starting with Beats version 6.0.0, the dashboards are loaded via the
Kibana API.
# This requires a Kibana endpoint configuration.
setup.kibana:
 host: "10.1.0.4:5601"
 # Kibana Host
 # Scheme and port can be left out and will be set to the default (http
and 5601)
 # In case you specify and additional path, the scheme is required:
http://localhost:5601/path
 # IPv6 addresses should always be defined as: https://[2001:db8::1]:5601
 #host: "localhost:5601"
 # Kibana Space ID
 # ID of the Kibana Space into which the dashboards should be loaded. By
default,
 # the Default Space will be used.
 #space.id:
#============================= Elastic Cloud
==================================
# These settings simplify using Metricbeat with the Elastic Cloud
(https://cloud.elastic.co/).
# The cloud.id setting overwrites the `output.elasticsearch.hosts` and
# `setup.kibana.host` options.
# You can find the `cloud.id` in the Elastic Cloud web UI.
#cloud.id:
# The cloud.auth setting overwrites the `output.elasticsearch.username`
and
# `output.elasticsearch.password` settings. The format is `<user>:<pass>`.
#cloud.auth:
#================================ Outputs
```

```
=====================================
# Configure what output to use when sending the data collected by the
beat.
#-------------------------- Elasticsearch output
------------------------------
output.elasticsearch:
 # Array of hosts to connect to.
 hosts: ["10.1.0.4:9200"]
 username: "elastic"
 password: "changeme"
 # Optional protocol and basic auth credentials.
 #protocol: "https"
 #username: "elastic"
 #password: "changeme"
#----------------------------- Logstash output
--------------------------------
#output.logstash:
 # The Logstash hosts
 #hosts: ["localhost:5044"]
 # Optional SSL. By default is off.
 # List of root certificates for HTTPS server verifications
 #ssl.certificate_authorities: ["/etc/pki/root/ca.pem"]
 # Certificate for SSL client authentication
 #ssl.certificate: "/etc/pki/client/cert.pem"
 # Client Certificate Key
 #ssl.key: "/etc/pki/client/cert.key"
#================================ Processors
=====================================
# Configure processors to enhance or manipulate events generated by the
beat.
processors:
 - add_host_metadata: ~
 - add_cloud_metadata: ~
#================================ Logging
=====================================
# Sets log level. The default log level is info.
# Available log levels are: 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: ["*"]
```

```
#============================== X-Pack Monitoring
===============================
# metricbeat can export internal metrics to a central Elasticsearch
monitoring
# cluster. This requires xpack monitoring to be enabled in Elasticsearch.
The
# reporting is disabled by default.
# Set to true to enable the monitoring reporter.
#monitoring.enabled: false
# Sets the UUID of the Elasticsearch cluster under which monitoring data
for this
# Metricbeat instances will appear in the Stack Monitoring UI. If
output.elasticsearch
# is enabled, the UUID is derived from the Elasticsearch cluster
referenced by output.elasticsearch.
```

Metricbeat-playbook.yml

```
 - name: Installing and Launching metricbeat
 hosts: webservers
 become: yes
 tasks:
 - name: Download metricbeat .deb file
 command: curl -L -O
https://artifacts.elastic.co/downloads/beats/metricbeat/metricbeat-7.4>

 - name: Install metricbeat .deb
 command: dpkg -i metricbeat-7.4.0-amd64.deb

 - name: Drop in metricbeat.yml
 copy:
 src: /etc/ansible/files/metricbeat-config.yml
 dest: /etc/metricbeat/metricbeat.yml

 - name: Enable and configure system module
 command: metricbeat modules enable docker

 - name: Metricbeat setup
 command: metricbeat setup

 - name: Start metricbeat service
 command: service metricbeat start

 - name: Enable service metricbeat on boot
 systemd:
```

```
name: metricbeat
enabled: yes
```