#================================== Description ========================================

# Filebeat Config to send Elasticsearch/Logstash/Kibana in a docker host to Elasticsea-

# sh cluster.

name: filebeat-elk-monitoring

filebeat.config:

modules:

path: ${path.config}/modules.d/\*.yml

reload.enabled: false

#================================ Autodiscover =======================================

# Autodiscover all containers with elasticsearch images, and add an separate input for

# each container and log type.

filebeat.autodiscover:

providers:

- type: docker

templates:

- condition:

contains:

docker.container.image: elasticsearch

config:

- module: elasticsearch

server:

input:

type: container

paths: '/var/lib/docker/containers/${data.docker.container.id}/\*.log'

gc:

input:

type: container

paths: '/var/lib/docker/containers/${data.docker.container.id}/\*.log'

audit:

input:

type: container

paths: '/var/lib/docker/containers/${data.docker.container.id}/\*.log'

slowlog:

input:

type: container

paths: '/var/lib/docker/containers/${data.docker.container.id}/\*.log'

deprecation:

input:

type: container

paths: '/var/lib/docker/containers/${data.docker.container.id}/\*.log'

- type: docker

templates:

- condition:

contains:

docker.container.image: kibana

config:

- module: kibana

log:

input:

type: container

paths: '/var/lib/docker/containers/${data.docker.container.id}/\*.log'

- type: docker

templates:

- condition:

contains:

docker.container.image: logstash

config:

- module: logstash

log:

input:

type: container

paths: '/var/lib/docker/containers/${data.docker.container.id}/\*.log'

slowlog:

input:

type: container

paths: '/var/lib/docker/containers/${data.docker.container.id}/\*.log'

processors:

- add\_cloud\_metadata: ~

# Output to ES directly.

output.elasticsearch:

hosts: '${ELASTICSEARCH\_HOST\_PORT}'

username: '${ELASTIC\_USERNAME}'

password: '${ELASTIC\_PASSWORD}'

ssl:

verification\_mode: "none"

#=================================== Kibana ==========================================

# Enable setting up 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: '${KIBANA\_HOST\_PORT}'

username: '${ELASTIC\_USERNAME}'

password: '${ELASTIC\_PASSWORD}'

#==================================== Monitoring =====================================

# Enable Monitoring Beats

# Filebeat can export internal metrics to a central Elasticsearch monitoring

# cluster. This requires xpack monitoring to be enabled in Elasticsearch

# Use deprecated option to avoid current UX bug in 7.3.0 where filebeat creates a

# standalone monitoring cluster in the monitoring UI.

# see: https://github.com/elastic/beats/pull/13182

xpack.monitoring:

enabled: true

# elasticsearch:

# hosts: '${ELASTICSEARCH\_HOST\_PORT}'

# username: '${ELASTIC\_USERNAME}'

# password: '${ELASTIC\_PASSWORD}'

#monitoring:

# enabled: true

# elasticsearch:

# hosts: '${ELASTICSEARCH\_HOST\_PORT}'

# username: '${ELASTIC\_USERNAME}'

# password: '${ELASTIC\_PASSWORD}'

# ssl.enabled: true

# ssl.verification\_mode: none

#================================ HTTP Endpoint ======================================

# Enabled so we can monitor filebeat using filebeat exporter if needed.

# Each beat can expose internal metrics through a HTTP endpoint. For security

# reasons the endpoint is disabled by default. This feature is currently experimental.

# Stats can be access through http://localhost:5066/stats . For pretty JSON output

# append ?pretty to the URL.

# Defines if the HTTP endpoint is enabled.

http.enabled: true

http.host: 0.0.0.0

http.port: 5066