Filebeat-config.yml

######################## Filebeat Configuration ############################

# This file is a full configuration example documenting all non-deprecated

# options in comments. For a shorter configuration example, that contains only

# the most common options, please see filebeat.yml in the same directory.

#

# You can find the full configuration reference here:

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

filebeat.config.modules:

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

​

#========================== Modules configuration =============================

filebeat.modules:

​

#-------------------------------- System Module --------------------------------

#- module: system

# Syslog

#syslog:

#enabled: true

​

# Set custom paths for the log files. If left empty,

# Filebeat will choose the paths depending on your OS.

#var.paths:

​

# Input configuration (advanced). Any input configuration option

# can be added under this section.

#input:

​

# Authorization logs

#auth:

#enabled: true

​

# Set custom paths for the log files. If left empty,

# Filebeat will choose the paths depending on your OS.

#var.paths:

​

# Input configuration (advanced). Any input configuration option

# can be added under this section.

#input:

​

#-------------------------------- Apache Module --------------------------------

#- module: apache

# Access logs

#access:

#enabled: true

​

# Set custom paths for the log files. If left empty,

# Filebeat will choose the paths depending on your OS.

#var.paths:

​

# Input configuration (advanced). Any input configuration option

# can be added under this section.

#input:

​

# Error logs

#error:

#enabled: true

​

# Set custom paths for the log files. If left empty,

# Filebeat will choose the paths depending on your OS.

#var.paths:

​

# Input configuration (advanced). Any input configuration option

# can be added under this section.

#input:

#-------------------------------- Auditd Module --------------------------------

#- module: auditd

#log:

#enabled: true

​

# Set custom paths for the log files. If left empty,

# Filebeat will choose the paths depending on your OS.

#var.paths:

​

# Input configuration (advanced). Any input configuration option

# can be added under this section.

#input:

​

#---------------------------- Elasticsearch Module ----------------------------

- 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

# Set custom paths for the log files. If left empty,

# Filebeat will choose the paths depending on your OS.

#var.paths:

​

#------------------------------- Haproxy Module -------------------------------

- module: haproxy

# All logs

log:

enabled: true

​

# Set which input to use between syslog (default) or file.

#var.input:

​

# Set custom paths for the log files. If left empty,

# Filebeat will choose the paths depending on your OS.

#var.paths:

​

#-------------------------------- Icinga Module --------------------------------

#- module: icinga

# Main logs

#main:

#enabled: true

​

# Set custom paths for the log files. If left empty,

# Filebeat will choose the paths depending on your OS.

#var.paths:

​

# Input configuration (advanced). Any input configuration option

# can be added under this section.

#input:

​

# Debug logs

#debug:

#enabled: true

​

# Set custom paths for the log files. If left empty,

# Filebeat will choose the paths depending on your OS.

#var.paths:

​

# Input configuration (advanced). Any input configuration option

# can be added under this section.

#input:

​

# Startup logs

#startup:

#enabled: true

​

# Set custom paths for the log files. If left empty,

# Filebeat will choose the paths depending on your OS.

#var.paths:

​

# Input configuration (advanced). Any input configuration option

# can be added under this section.

#input:

​

#--------------------------------- IIS Module ---------------------------------

#- module: iis

# Access logs

#access:

#enabled: true

​

# Set custom paths for the log files. If left empty,

# Filebeat will choose the paths depending on your OS.

#var.paths:

​

# Input configuration (advanced). Any input configuration option

# can be added under this section.

#input:

​

# Error logs

#error:

#enabled: true

​

# Set custom paths for the log files. If left empty,

# Filebeat will choose the paths depending on your OS.

#var.paths:

​

# Input configuration (advanced). Any input configuration option

# can be added under this section.

#input:

​

#-------------------------------- Kafka Module --------------------------------

- module: kafka

# All logs

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

​

# Set custom paths for the log files. If left empty,

# Filebeat will choose the paths depending on your OS.

#var.paths:

​

#------------------------------- Logstash Module -------------------------------

#- module: logstash

# logs

#log:

#enabled: true

​

# Set custom paths for the log files. If left empty,

# Filebeat will choose the paths depending on your OS.

# var.paths:

​

# Slow logs

#slowlog:

#enabled: true

# Set custom paths for the log files. If left empty,

# Filebeat will choose the paths depending on your OS.

#var.paths:

​

#------------------------------- Mongodb Module -------------------------------

#- module: mongodb

# Logs

#log:

#enabled: true

​

# Set custom paths for the log files. If left empty,

# Filebeat will choose the paths depending on your OS.

#var.paths:

​

# Input configuration (advanced). Any input configuration option

# can be added under this section.

#input:

​

#-------------------------------- MySQL Module --------------------------------

#- module: mysql

# Error logs

#error:

#enabled: true

​

# Set custom paths for the log files. If left empty,

# Filebeat will choose the paths depending on your OS.

#var.paths:

​

# Input configuration (advanced). Any input configuration option

# can be added under this section.

#input:

​

# Slow logs

#slowlog:

#enabled: true

​

# Set custom paths for the log files. If left empty,

# Filebeat will choose the paths depending on your OS.

#var.paths:

​

# Input configuration (advanced). Any input configuration option

# can be added under this section.

#input:

​

#--------------------------------- Nats Module ---------------------------------

- module: nats

# All logs

log:

enabled: true

​

# Set custom paths for the log files. If left empty,

# Filebeat will choose the paths depending on your OS.

#var.paths:

​

#-------------------------------- Nginx Module --------------------------------

#- module: nginx

# Access logs

#access:

#enabled: true

​

# Set custom paths for the log files. If left empty,

# Filebeat will choose the paths depending on your OS.

#var.paths:

​

# Input configuration (advanced). Any input configuration option

# can be added under this section.

#input:

​

# Error logs

#error:

#enabled: true

​

# Set custom paths for the log files. If left empty,

# Filebeat will choose the paths depending on your OS.

#var.paths:

​

# Input configuration (advanced). Any input configuration option

# can be added under this section.

#input:

​

#------------------------------- Osquery Module -------------------------------

- module: osquery

result:

enabled: true

​

# Set custom paths for the log files. If left empty,

# Filebeat will choose the paths depending on your OS.

#var.paths:

​

# If true, all fields created by this module are prefixed with

# `osquery.result`. Set to false to copy the fields in the root

# of the document. The default is true.

#var.use\_namespace: true

​

#------------------------------ PostgreSQL Module ------------------------------

#- module: postgresql

# Logs

#log:

#enabled: true

​

# Set custom paths for the log files. If left empty,

# Filebeat will choose the paths depending on your OS.

#var.paths:

​

# Input configuration (advanced). Any input configuration option

# can be added under this section.

#input:

​

#-------------------------------- Redis Module --------------------------------

#- module: redis

# Main logs

#log:

#enabled: true

​

# Set custom paths for the log files. If left empty,

# Filebeat will choose the paths depending on your OS.

#var.paths: ["/var/log/redis/redis-server.log\*"]

​

# Slow logs, retrieved via the Redis API (SLOWLOG)

#slowlog:

#enabled: true

​

# The Redis hosts to connect to.

#var.hosts: ["localhost:6379"]

​

# Optional, the password to use when connecting to Redis.

#var.password:

​

#----------------------------- Google Santa Module -----------------------------

- module: santa

log:

enabled: true

# Set custom paths for the log files. If left empty,

# Filebeat will choose the the default path.

#var.paths:

​

#------------------------------- Traefik Module -------------------------------

#- module: traefik

# Access logs

#access:

#enabled: true

​

# Set custom paths for the log files. If left empty,

# Filebeat will choose the paths depending on your OS.

#var.paths:

​

# Input configuration (advanced). Any input configuration option

# can be added under this section.

#input:

​

​

#=========================== Filebeat inputs =============================

​

# List of inputs to fetch data.

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 for reading files with international characters

# following the W3C recommendation for HTML5 (http://www.w3.org/TR/encoding).

# Some sample encodings:

# plain, utf-8, utf-16be-bom, utf-16be, utf-16le, big5, gb18030, gbk,

# hz-gb-2312, euc-kr, euc-jp, iso-2022-jp, shift-jis, ...

#encoding: plain

​

​

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

# matching any regular expression from the list. The include\_lines is called before

...