```
######################## 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
# exclude_lines. By default, no lines are dropped.
#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. The include_lines is called before
# exclude_lines. By default, all the lines are exported.
#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 fields can be freely picked
# to add additional information to the crawled log files for filtering
#fields:
#  level: debug
#  review: 1

# Set to true to store the additional fields as top level fields instead
# of under the "fields" sub-dictionary. In case of name conflicts with the
# fields added by Filebeat itself, the custom fields overwrite the default
# fields.
#fields_under_root: false
```

```
# Set to true to publish fields with null values in events.
#keep_null: false

# Ignore files which were modified more then the defined timespan in the past.
# ignore_older is disabled by default, so no files are ignored by setting it to 0.
# Time strings like 2h (2 hours), 5m (5 minutes) can be used.
#ignore_older: 0

# How often the input checks for new files in the paths that are specified
# for harvesting. Specify 1s to scan the directory as frequently as possible
# without causing Filebeat to scan too frequently. Default: 10s.
#scan_frequency: 10s

# Defines the buffer size every harvester uses when fetching the file
#harvester_buffer_size: 16384

# Maximum number of bytes a single log event can have
# All bytes after max_bytes are discarded and not sent. The default is 10MB.
# This is especially useful for multiline log messages which can get large.
#max_bytes: 10485760

# Characters which separate the lines. Valid values: auto, line_feed, vertical_tab, form_feed,
# carriage_return, carriage_return_line_feed, next_line, line_separator, paragraph_separator.
#line_terminator: auto

### Recursive glob configuration

# Expand "**" patterns into regular glob patterns.
#recursive_glob.enabled: true

### JSON configuration

# Decode JSON options. Enable this if your logs are structured in JSON.
# JSON key on which to apply the line filtering and multiline settings. This key
# must be top level and its value must be string, otherwise it is ignored. If
# no text key is defined, the line filtering and multiline features cannot be used.
#json.message_key:

# By default, the decoded JSON is placed under a "json" key in the output document.
# If you enable this setting, the keys are copied top level in the output document.
#json.keys_under_root: false

# If keys_under_root and this setting are enabled, then the values from the decoded
```

```
  # JSON object overwrite the fields that Filebeat normally adds (type, source, offset, etc.)
  # in case of conflicts.
  #json.overwrite_keys: false

  # If this setting is enabled, Filebeat adds a "error.message" and "error.key: json" key in case of
JSON
  # unmarshaling errors or when a text key is defined in the configuration but cannot
  # be used.
  #json.add_error_key: false

  ### Multiline options

  # Multiline 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

  # The maximum number of lines that are combined to one event.
  # In case there are more the max_lines the additional lines are discarded.
  # Default is 500
  #multiline.max_lines: 500

  # After the defined timeout, an multiline event is sent even if no new pattern was found to start
a new event
  # Default is 5s.
  #multiline.timeout: 5s

  # Setting tail_files to true means filebeat starts reading new files at the end
  # instead of the beginning. If this is used in combination with log rotation
  # this can mean that the first entries of a new file are skipped.
  #tail_files: false
  # The Ingest Node pipeline ID associated with this input. If this is set, it
  # overwrites the pipeline option from the Elasticsearch output.
  #pipeline:

  # If symlinks is enabled, symlinks are opened and harvested. The harvester is opening the
  # original for harvesting but will report the symlink name as source.
  #symlinks: false

  # Backoff values define how aggressively filebeat crawls new files for updates
  # The default values can be used in most cases. Backoff defines how long it is waited
  # to check a file again after EOF is reached. Default is 1s which means the file
  # is checked every second if new lines were added. This leads to a near real time crawling.
  # Every time a new line appears, backoff is reset to the initial value.
  #backoff: 1s

  # Max backoff defines what the maximum backoff time is. After having backed off multiple
times
  # from checking the files, the waiting time will never exceed max_backoff independent of the
  # backoff factor. Having it set to 10s means in the worst case a new line can be added to a log
  # file after having backed off multiple times, it takes a maximum of 10s to read the new line
  #max_backoff: 10s

  # The backoff factor defines how fast the algorithm backs off. The bigger the backoff factor,
  # the faster the max_backoff value is reached. If this value is set to 1, no backoff will happen.
  # The backoff value will be multiplied each time with the backoff_factor until max_backoff is
reached
  #backoff_factor: 2

  # Max number of harvesters that are started in parallel.
  # Default is 0 which means unlimited
  #harvester_limit: 0

  ### Harvester closing options

  # Close inactive closes the file handler after the predefined period.
  # The period starts when the last line of the file was, not the file ModTime.
  # Time strings like 2h (2 hours), 5m (5 minutes) can be used.
  #close_inactive: 5m

  # Close renamed closes a file handler when the file is renamed or rotated.
  # Note: Potential data loss. Make sure to read and understand the docs for this option.
  #close_renamed: false

  # When enabling this option, a file handler is closed immediately in case a file can't be found
  # any more. In case the file shows up again later, harvesting will continue at the last known
position
  # after scan_frequency.
  #close_removed: true

  # Closes the file handler as soon as the harvesters reaches the end of the file.
  # By default this option is disabled.
  # Note: Potential data loss. Make sure to read and understand the docs for this option.
  #close_eof: false

  ### State options

  # Files for the modification data is older then clean_inactive the state from the registry is
removed
  # By default this is disabled.
  #clean_inactive: 0

  # Removes the state for file which cannot be found on disk anymore immediately
  #clean_removed: true

  # Close timeout closes the harvester after the predefined time.
  # This is independent if the harvester did finish reading the file or not.
  # By default this option is disabled.
  # Note: Potential data loss. Make sure to read and understand the docs for this option.
  #close_timeout: 0

  # Defines if inputs is enabled
  #enabled: true

#---------------------------- Stdin input ------------------------------
# Configuration to use stdin input
#- type: stdin

#------------------------ Redis slowlog input --------------------------
# Experimental: Config options for the redis slow log input
#- type: redis
  #enabled: false

  # List of hosts to pool to retrieve the slow log information.
  #hosts: ["localhost:6379"]

  # How often the input checks for redis slow log.
  #scan_frequency: 10s
  # Timeout after which time the input should return an error
  #timeout: 1s

  # Network type to be used for redis connection. Default: tcp
  #network: tcp

  # Max number of concurrent connections. Default: 10
  #maxconn: 10

  # Redis AUTH password. Empty by default.
  #password: foobared

#------------------------------ Udp input --------------------------------
# Experimental: Config options for the udp input
#- type: udp
  #enabled: false

  # Maximum size of the message received over UDP
  #max_message_size: 10KiB

  # Size of the UDP read buffer in bytes
  #read_buffer: 0


#------------------------------ TCP input --------------------------------
# Experimental: Config options for the TCP input
#- type: tcp
  #enabled: false

  # The host and port to receive the new event
  #host: "localhost:9000"

  # Character used to split new message
  #line_delimiter: "\n"

  # Maximum size in bytes of the message received over TCP
  #max_message_size: 20MiB

  # Max number of concurrent connections, or 0 for no limit. Default: 0
  #max_connections: 0

  # The number of seconds of inactivity before a remote connection is closed.
  #timeout: 300s
  # Use SSL settings for TCP.
  #ssl.enabled: true

  # List of supported/valid TLS versions. By default all TLS versions 1.0 up to
  # 1.2 are enabled.
  #ssl.supported_protocols: [TLSv1.0, TLSv1.1, TLSv1.2]

  # SSL configuration. By default is off.
  # List of root certificates for client verifications
  #ssl.certificate_authorities: ["/etc/pki/root/ca.pem"]

  # Certificate for SSL server authentication.
  #ssl.certificate: "/etc/pki/client/cert.pem"

  # Server Certificate Key,
  #ssl.key: "/etc/pki/client/cert.key"

  # Optional passphrase for decrypting the Certificate Key.
  #ssl.key_passphrase: ''

  # Configure cipher suites to be used for SSL connections.
  #ssl.cipher_suites: []

  # Configure curve types for ECDHE based cipher suites.
  #ssl.curve_types: []

  # Configure what types of client authentication are supported. Valid options
  # are `none`, `optional`, and `required`. When `certificate_authorities` is set it will
  # default to `required` otherwise it will be set to `none`.
  #ssl.client_authentication: "required"

#------------------------------ Syslog input --------------------------------
# Experimental: Config options for the Syslog input
# Accept RFC3164 formatted syslog event via UDP.
#- type: syslog
  #enabled: false
  #protocol.udp:
    # The host and port to receive the new event
    #host: "localhost:9000"

    # Maximum size of the message received over UDP
    #max_message_size: 10KiB

# Accept RFC3164 formatted syslog event via TCP.
```

```
#- type: syslog
  #enabled: false

  #protocol.tcp:
    # The host and port to receive the new event
    #host: "localhost:9000"

    # Character used to split new message
    #line_delimiter: "\n"

    # Maximum size in bytes of the message received over TCP
    #max_message_size: 20MiB

    # The number of seconds of inactivity before a remote connection is closed.
    #timeout: 300s

    # Use SSL settings for TCP.
    #ssl.enabled: true

    # List of supported/valid TLS versions. By default all TLS versions 1.0 up to
    # 1.2 are enabled.
    #ssl.supported_protocols: [TLSv1.0, TLSv1.1, TLSv1.2]

    # SSL configuration. By default is off.
    # List of root certificates for client verifications
    #ssl.certificate_authorities: ["/etc/pki/root/ca.pem"]

    # Certificate for SSL server authentication.
    #ssl.certificate: "/etc/pki/client/cert.pem"

    # Server Certificate Key,
    #ssl.key: "/etc/pki/client/cert.key"

    # Optional passphrase for decrypting the Certificate Key.
    #ssl.key_passphrase: ''

    # Configure cipher suites to be used for SSL connections.
    #ssl.cipher_suites: []

    # Configure curve types for ECDHE based cipher suites.
    #ssl.curve_types: []

    # Configure what types of client authentication are supported. Valid options
    # are `none`, `optional`, and `required`. When `certificate_authorities` is set it will
    # default to `required` otherwise it will be set to `none`.
    #ssl.client_authentication: "required"

#------------------------------ Container input --------------------------------
#- type: container
  #enabled: false

  # Paths for container logs that should be crawled and fetched.
  #paths:
  #  -/var/lib/docker/containers/*/*.log

  # Configure stream to filter to a specific stream: stdout, stderr or all (default)
  #stream: all

#========================== Filebeat autodiscover
==============================

# Autodiscover allows you to detect changes in the system and spawn new modules
# or inputs as they happen.

#filebeat.autodiscover:
  # List of enabled autodiscover providers
#  providers:
#    - type: docker
#      templates:
#        - condition:
#            equals.docker.container.image: busybox
#          config:
#            - type: container
#              paths:
#                - /var/lib/docker/containers/${data.docker.container.id}/*.log

#========================= Filebeat global options ============================

# Registry data path. If a relative path is used, it is considered relative to the
# data path.
#filebeat.registry.path: ${path.data}/registry

# The permissions mask to apply on registry data, and meta files. The default
# value is 0600.  Must be a valid Unix-style file permissions mask expressed in
# octal notation.  This option is not supported on Windows.
#filebeat.registry.file_permissions: 0600

# The timeout value that controls when registry entries are written to disk
# (flushed). When an unwritten update exceeds this value, it triggers a write
# to disk. When flush is set to 0s, the registry is written to disk after each
# batch of events has been published successfully. The default value is 0s.
#filebeat.registry.flush: 0s


# Starting with Filebeat 7.0, the registry uses a new directory format to store
# Filebeat state. After you upgrade, Filebeat will automatically migrate a 6.x
# registry file to use the new directory format. If you changed
# filebeat.registry.path while upgrading, set filebeat.registry.migrate_file to
# point to the old registry file.
#filebeat.registry.migrate_file: ${path.data}/registry

# By default Ingest pipelines are not updated if a pipeline with the same ID
# already exists. If this option is enabled Filebeat overwrites pipelines
# everytime a new Elasticsearch connection is established.
#filebeat.overwrite_pipelines: false

# How long filebeat waits on shutdown for the publisher to finish.
# Default is 0, not waiting.
#filebeat.shutdown_timeout: 0

# Enable filebeat config reloading
#filebeat.config:
  #inputs:
    #enabled: false
    #path: inputs.d/*.yml
    #reload.enabled: true
    #reload.period: 10s
  #modules:
    #enabled: false
    #path: modules.d/*.yml
    #reload.enabled: true
    #reload.period: 10s

#================================ 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.
# If this options is not defined, the hostname is used.
#name:

# The tags of the shipper are included in their own field with each
# transaction published. Tags make it easy to group servers by different
# logical properties.
#tags: ["service-X", "web-tier"]

# Optional fields that you can specify to add additional information to the
# output. Fields can be scalar values, arrays, dictionaries, or any nested
# combination of these.
#fields:
#  env: staging

# If this option is set to true, the custom fields are stored as top-level
# fields in the output document instead of being grouped under a fields
# sub-dictionary. Default is false.
#fields_under_root: false

# Internal queue configuration for buffering events to be published.
#queue:
  # Queue type by name (default 'mem')
  # The memory queue will present all available events (up to the outputs
  # bulk_max_size) to the output, the moment the output is ready to server
  # another batch of events.
  #mem:
    # Max number of events the queue can buffer.
    #events: 4096

    # Hints the minimum number of events stored in the queue,
    # before providing a batch of events to the outputs.
    # The default value is set to 2048.
    # A value of 0 ensures events are immediately available
    # to be sent to the outputs.
    #flush.min_events: 2048

    # Maximum duration after which events are available to the outputs,
    # if the number of events stored in the queue is < `flush.min_events`.
    #flush.timeout: 1s

  # The spool queue will store events in a local spool file, before
  # forwarding the events to the outputs.
  #
  # Beta: spooling to disk is currently a beta feature. Use with care.
  #
  # The spool file is a circular buffer, which blocks once the file/buffer is full.
  # Events are put into a write buffer and flushed once the write buffer
  # is full or the flush_timeout is triggered.
  # Once ACKed by the output, events are removed immediately from the queue,
  # making space for new events to be persisted.
  #spool:
    # The file namespace configures the file path and the file creation settings.
    # Once the file exists, the `size`, `page_size` and `prealloc` settings
    # will have no more effect.
    #file:
      # Location of spool file. The default value is ${path.data}/spool.dat.
      #path: "${path.data}/spool.dat"

      # Configure file permissions if file is created. The default value is 0600.
      #permissions: 0600

      # File size hint. The spool blocks, once this limit is reached. The default value is 100 MiB.
      #size: 100MiB

      # The files page size. A file is split into multiple pages of the same size. The default value is
4KiB.
      #page_size: 4KiB

      # If prealloc is set, the required space for the file is reserved using
      # truncate. The default value is true.
      #prealloc: true

    # Spool writer settings
    # Events are serialized into a write buffer. The write buffer is flushed if:
    # - The buffer limit has been reached.
    # - The configured limit of buffered events is reached.
    # - The flush timeout is triggered.
    #write:
      # Sets the write buffer size.
      #buffer_size: 1MiB

      # Maximum duration after which events are flushed if the write buffer
      # is not full yet. The default value is 1s.
      #flush.timeout: 1s

      # Number of maximum buffered events. The write buffer is flushed once the
      # limit is reached.
      #flush.events: 16384

      # Configure the on-disk event encoding. The encoding can be changed
      # between restarts.
      # Valid encodings are: json, ubjson, and cbor.
      #codec: cbor
    #read:
      # Reader flush timeout, waiting for more events to become available, so
      # to fill a complete batch as required by the outputs.
      # If flush_timeout is 0, all available events are forwarded to the
      # outputs immediately.
      # The default value is 0s.
      #flush.timeout: 0s

# Sets the maximum number of CPUs that can be executing simultaneously. The
# default is the number of logical CPUs available in the system.
#max_procs:

#================================ Processors
=====================================

# Processors are used to reduce the number of fields in the exported event or to
# enhance the event with external metadata. This section defines a list of
# processors that are applied one by one and the first one receives the initial
# event:
#
#   event -> filter1 -> event1 -> filter2 ->event2 ...
#
# The supported processors are drop_fields, drop_event, include_fields,
# decode_json_fields, and add_cloud_metadata.
#
# For example, you can use the following processors to keep the fields that
# contain CPU load percentages, but remove the fields that contain CPU ticks
# values:
#
#processors:
#- include_fields:
#    fields: ["cpu"]
#- drop_fields:
#    fields: ["cpu.user", "cpu.system"]
#
# The following example drops the events that have the HTTP response code 200:
#
#processors:
#- drop_event:
#    when:
#       equals:
#           http.code: 200
#
```

```
# The following example renames the field a to b:
#
#processors:
#- rename:
#    fields:
#       - from: "a"
#         to: "b"
#
# The following example tokenizes the string into fields:
#
#processors:
#- dissect:
#    tokenizer: "%{key1} - %{key2}"
#    field: "message"
#    target_prefix: "dissect"
#
# The following example enriches each event with metadata from the cloud
# provider about the host machine. It works on EC2, GCE, DigitalOcean,
# Tencent Cloud, and Alibaba Cloud.
#
#processors:
#- add_cloud_metadata: ~
#
# The following example enriches each event with the machine's local time zone
# offset from UTC.
#
#processors:
#- add_locale:
#    format: offset
#
# The following example enriches each event with docker metadata, it matches
# given fields to an existing container id and adds info from that container:
#
#processors:
#- add_docker_metadata:
#    host: "unix:///var/run/docker.sock"
#    match_fields: ["system.process.cgroup.id"]
#    match_pids: ["process.pid", "process.ppid"]
#    match_source: true
#    match_source_index: 4
#    match_short_id: false
#    cleanup_timeout: 60
#    labels.dedot: false
#    # To connect to Docker over TLS you must specify a client and CA certificate.
#    #ssl:
#    #  certificate_authority: "/etc/pki/root/ca.pem"
#    #  certificate:           "/etc/pki/client/cert.pem"
#    #  key:                   "/etc/pki/client/cert.key"
#
# The following example enriches each event with docker metadata, it matches
# container id from log path available in `source` field (by default it expects
# it to be /var/lib/docker/containers/*/*.log).
#
#processors:
#- add_docker_metadata: ~
#
# The following example enriches each event with host metadata.
#
#processors:
#- add_host_metadata:
#   netinfo.enabled: false
#
# The following example enriches each event with process metadata using
# process IDs included in the event.
#
#processors:
#- add_process_metadata:
#    match_pids: ["system.process.ppid"]
#    target: system.process.parent
#
# The following example decodes fields containing JSON strings
# and replaces the strings with valid JSON objects.
#
#processors:
#- decode_json_fields:
#    fields: ["field1", "field2", ...]
#    process_array: false
#    max_depth: 1
#    target: ""
#    overwrite_keys: false
#
#processors:
#- decompress_gzip_field:
#    from: "field1"
#    to: "field2"
#    ignore_missing: false
#    fail_on_error: true
#
```

```
# The following example copies the value of message to message_copied
#
#processors:
#- copy_fields:
#    fields:
#        - from: message
#          to: message_copied
#    fail_on_error: true
#    ignore_missing: false
#
# The following example truncates the value of message to 1024 bytes
#
#processors:
#- truncate_fields:
#    fields:
#      - message
#    max_bytes: 1024
#    fail_on_error: false
#    ignore_missing: true
#
# The following example preserves the raw message under event.original
#
#processors:
#- copy_fields:
#    fields:
#        - from: message
#          to: event.original
#    fail_on_error: false
#    ignore_missing: true
#- truncate_fields:
#    fields:
#      - event.original
#    max_bytes: 1024
#    fail_on_error: false
#    ignore_missing: true

#
==============================ElasticCloud====================================

# These settings simplify using Filebeat 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:
  # 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" # TODO: Change this to the password you set

  # Set gzip compression level.
  #compression_level: 0

  # Configure escaping HTML symbols in strings.
  #escape_html: false

  # Optional protocol and basic auth credentials.
  #protocol: "https"
  #username: "elastic"
  #password: "changeme"

  # Dictionary of HTTP parameters to pass within the URL with index operations.
  #parameters:
    #param1: value1
    #param2: value2

  # Number of workers per Elasticsearch host.
  #worker: 1

  # Optional index name. The default is "filebeat" plus date
  # and generates [filebeat-]YYYY.MM.DD keys.
  # In case you modify this pattern you must update setup.template.name and
setup.template.pattern accordingly.
  #index: "filebeat-%{[agent.version]}-%{+yyyy.MM.dd}"

  # Optional ingest node pipeline. By default no pipeline will be used.
  #pipeline: ""

  # Optional HTTP path
  #path: "/elasticsearch"

  # Custom HTTP headers to add to each request
  #headers:
  #  X-My-Header: Contents of the header

  # Proxy server URL
  #proxy_url: http://proxy:3128

  # Whether to disable proxy settings for outgoing connections. If true, this
  # takes precedence over both the proxy_url field and any environment settings
  # (HTTP_PROXY, HTTPS_PROXY). The default is false.
  #proxy_disable: false

  # The number of times a particular Elasticsearch index operation is attempted. If
  # the indexing operation doesn't succeed after this many retries, the events are
  # dropped. The default is 3.
  #max_retries: 3

  # The maximum number of events to bulk in a single Elasticsearch bulk API index request.
  # The default is 50.
  #bulk_max_size: 50

  # The number of seconds to wait before trying to reconnect to Elasticsearch
  # after a network error. After waiting backoff.init seconds, the Beat
  # tries to reconnect. If the attempt fails, the backoff timer is increased
  # exponentially up to backoff.max. After a successful connection, the backoff
  # timer is reset. The default is 1s.
  #backoff.init: 1s

  # The maximum number of seconds to wait before attempting to connect to
  # Elasticsearch after a network error. The default is 60s.
  #backoff.max: 60s

  # Configure HTTP request timeout before failing a request to Elasticsearch.
  #timeout: 90

  # Use SSL settings for HTTPS.
  #ssl.enabled: true

  # Configure SSL verification mode. If `none` is configured, all server hosts
  # and certificates will be accepted. In this mode, SSL-based connections are
  # susceptible to man-in-the-middle attacks. Use only for testing. Default is
  # `full`.
  #ssl.verification_mode: full

  # List of supported/valid TLS versions. By default all TLS versions from 1.0 up to
  # 1.2 are enabled.
  #ssl.supported_protocols: [TLSv1.0, TLSv1.1, TLSv1.2]

  # 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"

  # Optional passphrase for decrypting the certificate key.
  #ssl.key_passphrase: ''

  # Configure cipher suites to be used for SSL connections
  #ssl.cipher_suites: []

  # Configure curve types for ECDHE-based cipher suites
  #ssl.curve_types: []

  # Configure what types of renegotiation are supported. Valid options are
  # never, once, and freely. Default is never.
  #ssl.renegotiation: never

#---------------------------- Logstash output --------------------------------
#output.logstash:
  # Boolean flag to enable or disable the output module.
  #enabled: true

  # The Logstash hosts
  #hosts: ["localhost:5044"]
```

```
# Number of workers per Logstash host.
#worker: 1

# Set gzip compression level.
#compression_level: 3

# Configure escaping HTML symbols in strings.
#escape_html: false

# Optional maximum time to live for a connection to Logstash, after which the
# connection will be re-established.  A value of `0s` (the default) will
# disable this feature.
#
# Not yet supported for async connections (i.e. with the "pipelining" option set)
#ttl: 30s

# Optionally load-balance events between Logstash hosts. Default is false.
#loadbalance: false

# Number of batches to be sent asynchronously to Logstash while processing
# new batches.
#pipelining: 2

# If enabled only a subset of events in a batch of events is transferred per
# transaction.  The number of events to be sent increases up to `bulk_max_size`
# if no error is encountered.
#slow_start: false

# The number of seconds to wait before trying to reconnect to Logstash
# after a network error. After waiting backoff.init seconds, the Beat
# tries to reconnect. If the attempt fails, the backoff timer is increased
# exponentially up to backoff.max. After a successful connection, the backoff
# timer is reset. The default is 1s.
#backoff.init: 1s

# The maximum number of seconds to wait before attempting to connect to
# Logstash after a network error. The default is 60s.
#backoff.max: 60s

# Optional index name. The default index name is set to filebeat
# in all lowercase.
#index: 'filebeat'
```

```
# SOCKS5 proxy server URL
#proxy_url: socks5://user:password@socks5-server:2233

# Resolve names locally when using a proxy server. Defaults to false.
#proxy_use_local_resolver: false

# Enable SSL support. SSL is automatically enabled if any SSL setting is set.
#ssl.enabled: true

# Configure SSL verification mode. If `none` is configured, all server hosts
# and certificates will be accepted. In this mode, SSL based connections are
# susceptible to man-in-the-middle attacks. Use only for testing. Default is
# `full`.
#ssl.verification_mode: full

# List of supported/valid TLS versions. By default all TLS versions from 1.0 up to
# 1.2 are enabled.
#ssl.supported_protocols: [TLSv1.0, TLSv1.1, TLSv1.2]

# Optional SSL configuration options. SSL is off by default.
# 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"

# Optional passphrase for decrypting the Certificate Key.
#ssl.key_passphrase: ''

# Configure cipher suites to be used for SSL connections
#ssl.cipher_suites: []

# Configure curve types for ECDHE-based cipher suites
#ssl.curve_types: []

# Configure what types of renegotiation are supported. Valid options are
# never, once, and freely. Default is never.
#ssl.renegotiation: never

# The number of times to retry publishing an event after a publishing failure.
# After the specified number of retries, the events are typically dropped.
```

```
  # Some Beats, such as Filebeat and Winlogbeat, ignore the max_retries setting
  # and retry until all events are published.  Set max_retries to a value less
  # than 0 to retry until all events are published. The default is 3.
  #max_retries: 3

  # The maximum number of events to bulk in a single Logstash request. The
  # default is 2048.
  #bulk_max_size: 2048

  # The number of seconds to wait for responses from the Logstash server before
  # timing out. The default is 30s.
  #timeout: 30s

#------------------------------- Kafka output ----------------------------------
#output.kafka:
  # Boolean flag to enable or disable the output module.
  #enabled: true

  # The list of Kafka broker addresses from which to fetch the cluster metadata.
  # The cluster metadata contain the actual Kafka brokers events are published
  # to.
  #hosts: ["localhost:9092"]

  # The Kafka topic used for produced events. The setting can be a format string
  # using any event field. To set the topic from document type use `%{[type]}`.
  #topic: beats

  # The Kafka event key setting. Use format string to create a unique event key.
  # By default no event key will be generated.
  #key: ''

  # The Kafka event partitioning strategy. Default hashing strategy is `hash`
  # using the `output.kafka.key` setting or randomly distributes events if
  # `output.kafka.key` is not configured.
  #partition.hash:
    # If enabled, events will only be published to partitions with reachable
    # leaders. Default is false.
    #reachable_only: false

    # Configure alternative event field names used to compute the hash value.
    # If empty `output.kafka.key` setting will be used.
    # Default value is empty list.
    #hash: []
```

```
# Authentication details. Password is required if username is set.
#username: ''
#password: ''

# Kafka version Filebeat is assumed to run against. Defaults to the "1.0.0".
#version: '1.0.0'

# Configure JSON encoding
#codec.json:
  # Pretty-print JSON event
  #pretty: false

  # Configure escaping HTML symbols in strings.
  #escape_html: false

# Metadata update configuration. Metadata contains leader information
# used to decide which broker to use when publishing.
#metadata:
  # Max metadata request retry attempts when cluster is in middle of leader
  # election. Defaults to 3 retries.
  #retry.max: 3

  # Wait time between retries during leader elections. Default is 250ms.
  #retry.backoff: 250ms

  # Refresh metadata interval. Defaults to every 10 minutes.
  #refresh_frequency: 10m

  # Strategy for fetching the topics metadata from the broker. Default is false.
  #full: false

# The number of concurrent load-balanced Kafka output workers.
#worker: 1

# The number of times to retry publishing an event after a publishing failure.
# After the specified number of retries, events are typically dropped.
# Some Beats, such as Filebeat, ignore the max_retries setting and retry until
# all events are published.  Set max_retries to a value less than 0 to retry
# until all events are published. The default is 3.
#max_retries: 3

# The maximum number of events to bulk in a single Kafka request. The default
# is 2048.
#bulk_max_size: 2048
```

```
# Duration to wait before sending bulk Kafka request. 0 is no delay. The default
# is 0.
#bulk_flush_frequency: 0s

# The number of seconds to wait for responses from the Kafka brokers before
# timing out. The default is 30s.
#timeout: 30s

# The maximum duration a broker will wait for number of required ACKs. The
# default is 10s.
#broker_timeout: 10s

# The number of messages buffered for each Kafka broker. The default is 256.
#channel_buffer_size: 256

# The keep-alive period for an active network connection. If 0s, keep-alives
# are disabled. The default is 0 seconds.
#keep_alive: 0

# Sets the output compression codec. Must be one of none, snappy and gzip. The
# default is gzip.
#compression: gzip

# Set the compression level. Currently only gzip provides a compression level
# between 0 and 9. The default value is chosen by the compression algorithm.
#compression_level: 4

# The maximum permitted size of JSON-encoded messages. Bigger messages will be
# dropped. The default value is 1000000 (bytes). This value should be equal to
# or less than the broker's message.max.bytes.
#max_message_bytes: 1000000

# The ACK reliability level required from broker. 0=no response, 1=wait for
# local commit, -1=wait for all replicas to commit. The default is 1.  Note:
# If set to 0, no ACKs are returned by Kafka. Messages might be lost silently
# on error.
#required_acks: 1

# The configurable ClientID used for logging, debugging, and auditing
# purposes.  The default is "beats".
#client_id: beats

# Enable SSL support. SSL is automatically enabled if any SSL setting is set.
```

```
  #ssl.enabled: true

  # Optional SSL configuration options. SSL is off by default.
  # List of root certificates for HTTPS server verifications
  #ssl.certificate_authorities: ["/etc/pki/root/ca.pem"]

  # Configure SSL verification mode. If `none` is configured, all server hosts
  # and certificates will be accepted. In this mode, SSL based connections are
  # susceptible to man-in-the-middle attacks. Use only for testing. Default is
  # `full`.
  #ssl.verification_mode: full

  # List of supported/valid TLS versions. By default all TLS versions from 1.0 up to
  # 1.2 are enabled.
  #ssl.supported_protocols: [TLSv1.0, TLSv1.1, TLSv1.2]

  # Certificate for SSL client authentication
  #ssl.certificate: "/etc/pki/client/cert.pem"

  # Client Certificate Key
  #ssl.key: "/etc/pki/client/cert.key"

  # Optional passphrase for decrypting the Certificate Key.
  #ssl.key_passphrase: ''

  # Configure cipher suites to be used for SSL connections
  #ssl.cipher_suites: []

  # Configure curve types for ECDHE-based cipher suites
  #ssl.curve_types: []

  # Configure what types of renegotiation are supported. Valid options are
  # never, once, and freely. Default is never.
  #ssl.renegotiation: never

#------------------------------- Redis output ----------------------------------
#output.redis:
  # Boolean flag to enable or disable the output module.
  #enabled: true

  # Configure JSON encoding
  #codec.json:
    # Pretty print json event
    #pretty: false
  # Configure escaping HTML symbols in strings.
  #escape_html: false

# The list of Redis servers to connect to. If load-balancing is enabled, the
# events are distributed to the servers in the list. If one server becomes
# unreachable, the events are distributed to the reachable servers only.
#hosts: ["localhost:6379"]

# The name of the Redis list or channel the events are published to. The
# default is filebeat.
#key: filebeat

# The password to authenticate to Redis with. The default is no authentication.
#password:

# The Redis database number where the events are published. The default is 0.
#db: 0

# The Redis data type to use for publishing events. If the data type is list,
# the Redis RPUSH command is used. If the data type is channel, the Redis
# PUBLISH command is used. The default value is list.
#datatype: list

# The number of workers to use for each host configured to publish events to
# Redis. Use this setting along with the loadbalance option. For example, if
# you have 2 hosts and 3 workers, in total 6 workers are started (3 for each
# host).
#worker: 1

# If set to true and multiple hosts or workers are configured, the output
# plugin load balances published events onto all Redis hosts. If set to false,
# the output plugin sends all events to only one host (determined at random)
# and will switch to another host if the currently selected one becomes
# unreachable. The default value is true.
#loadbalance: true

# The Redis connection timeout in seconds. The default is 5 seconds.
#timeout: 5s

# The number of times to retry publishing an event after a publishing failure.
# After the specified number of retries, the events are typically dropped.
# Some Beats, such as Filebeat, ignore the max_retries setting and retry until
# all events are published. Set max_retries to a value less than 0 to retry
# until all events are published. The default is 3.
#max_retries: 3

# The number of seconds to wait before trying to reconnect to Redis
# after a network error. After waiting backoff.init seconds, the Beat
# tries to reconnect. If the attempt fails, the backoff timer is increased
# exponentially up to backoff.max. After a successful connection, the backoff
# timer is reset. The default is 1s.
#backoff.init: 1s

# The maximum number of seconds to wait before attempting to connect to
# Redis after a network error. The default is 60s.
#backoff.max: 60s

# The maximum number of events to bulk in a single Redis request or pipeline.
# The default is 2048.
#bulk_max_size: 2048

# The URL of the SOCKS5 proxy to use when connecting to the Redis servers. The
# value must be a URL with a scheme of socks5://.
#proxy_url:

# This option determines whether Redis hostnames are resolved locally when
# using a proxy. The default value is false, which means that name resolution
# occurs on the proxy server.
#proxy_use_local_resolver: false

# Enable SSL support. SSL is automatically enabled, if any SSL setting is set.
#ssl.enabled: true

# Configure SSL verification mode. If `none` is configured, all server hosts
# and certificates will be accepted. In this mode, SSL based connections are
# susceptible to man-in-the-middle attacks. Use only for testing. Default is
# `full`.
#ssl.verification_mode: full

# List of supported/valid TLS versions. By default all TLS versions 1.0 up to
# 1.2 are enabled.
#ssl.supported_protocols: [TLSv1.0, TLSv1.1, TLSv1.2]

# Optional SSL configuration options. SSL is off by default.
# 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"

  # Optional passphrase for decrypting the Certificate Key.
  #ssl.key_passphrase: ''

  # Configure cipher suites to be used for SSL connections
  #ssl.cipher_suites: []

  # Configure curve types for ECDHE based cipher suites
  #ssl.curve_types: []

  # Configure what types of renegotiation are supported. Valid options are
  # never, once, and freely. Default is never.
  #ssl.renegotiation: never

#------------------------------- File output -----------------------------------
#output.file:
  # Boolean flag to enable or disable the output module.
  #enabled: true

  # Configure JSON encoding
  #codec.json:
    # Pretty-print JSON event
    #pretty: false

    # Configure escaping HTML symbols in strings.
    #escape_html: false

  # Path to the directory where to save the generated files. The option is
  # mandatory.
  #path: "/tmp/filebeat"

  # Name of the generated files. The default is `filebeat` and it generates
  # files: `filebeat`, `filebeat.1`, `filebeat.2`, etc.
  #filename: filebeat

  # Maximum size in kilobytes of each file. When this size is reached, and on
  # every Filebeat restart, the files are rotated. The default value is 10240
  # kB.
  #rotate_every_kb: 10000
  # Maximum number of files under path. When this number of files is reached,
  # the oldest file is deleted and the rest are shifted from last to first. The
  # default is 7 files.
  #number_of_files: 7

  # Permissions to use for file creation. The default is 0600.
  #permissions: 0600

#----------------------------- Console output ---------------------------------
#output.console:
  # Boolean flag to enable or disable the output module.
  #enabled: true

  # Configure JSON encoding
  #codec.json:
    # Pretty-print JSON event
    #pretty: false

    # Configure escaping HTML symbols in strings.
    #escape_html: false

#================================= Paths
======================================

# The home path for the Filebeat installation. This is the default base path
# for all other path settings and for miscellaneous files that come with the
# distribution (for example, the sample dashboards).
# If not set by a CLI flag or in the configuration file, the default for the
# home path is the location of the binary.
#path.home:

# The configuration path for the Filebeat installation. This is the default
# base path for configuration files, including the main YAML configuration file
# and the Elasticsearch template file. If not set by a CLI flag or in the
# configuration file, the default for the configuration path is the home path.
#path.config: ${path.home}

# The data path for the Filebeat installation. This is the default base path
# for all the files in which Filebeat needs to store its data. If not set by a
# CLI flag or in the configuration file, the default for the data path is a data
# subdirectory inside the home path.
#path.data: ${path.home}/data
```

```
# The logs path for a Filebeat installation. This is the default location for
# the Beat's log files. If not set by a CLI flag or in the configuration file,
# the default for the logs path is a logs subdirectory inside the home path.
#path.logs: ${path.home}/logs

#================================= Keystore
===========================================
# Location of the Keystore containing the keys and their sensitive values.
#keystore.path: "${path.config}/beats.keystore"

#=============================== Dashboards
======================================
# These settings control loading the sample dashboards to the Kibana index. Loading
# the dashboards are disabled by default and can be enabled either by setting the
# options here, or by using the `-setup` CLI flag or the `setup` command.
#setup.dashboards.enabled: false

# The directory from where to read the dashboards. The default is the `kibana`
# folder in the home path.
#setup.dashboards.directory: ${path.home}/kibana

# The URL from where to download the dashboards archive. It is used instead of
# the directory if it has a value.
#setup.dashboards.url:

# The file archive (zip file) from where to read the dashboards. It is used instead
# of the directory when it has a value.
#setup.dashboards.file:

# In case the archive contains the dashboards from multiple Beats, this lets you
# select which one to load. You can load all the dashboards in the archive by
# setting this to the empty string.
#setup.dashboards.beat: filebeat

# The name of the Kibana index to use for setting the configuration. Default is ".kibana"
#setup.dashboards.kibana_index: .kibana

# The Elasticsearch index name. This overwrites the index name defined in the
# dashboards and index pattern. Example: testbeat-*
#setup.dashboards.index:

# Always use the Kibana API for loading the dashboards instead of autodetecting
# how to install the dashboards by first querying Elasticsearch.
#setup.dashboards.always_kibana: false
```

```
# If true and Kibana is not reachable at the time when dashboards are loaded,
# it will retry to reconnect to Kibana instead of exiting with an error.
#setup.dashboards.retry.enabled: false

# Duration interval between Kibana connection retries.
#setup.dashboards.retry.interval: 1s

# Maximum number of retries before exiting with an error, 0 for unlimited retrying.
#setup.dashboards.retry.maximum: 0


#============================== Template
=====================================

# A template is used to set the mapping in Elasticsearch
# By default template loading is enabled and the template is loaded.
# These settings can be adjusted to load your own template or overwrite existing ones.

# Set to false to disable template loading.
#setup.template.enabled: true

# Template name. By default the template name is "filebeat-%{[agent.version]}"
# The template name and pattern has to be set in case the Elasticsearch index pattern is
modified.
#setup.template.name: "filebeat-%{[agent.version]}"

# Template pattern. By default the template pattern is "-%{[agent.version]}-*" to apply to the
default index settings.
# The first part is the version of the beat and then -* is used to match all daily indices.
# The template name and pattern has to be set in case the Elasticsearch index pattern is
modified.
#setup.template.pattern: "filebeat-%{[agent.version]}-*"

# Path to fields.yml file to generate the template
#setup.template.fields: "${path.config}/fields.yml"

# A list of fields to be added to the template and Kibana index pattern. Also
# specify setup.template.overwrite: true to overwrite the existing template.
# This setting is experimental.
#setup.template.append_fields:
#- name: field_name
#  type: field_type
# Enable JSON template loading. If this is enabled, the fields.yml is ignored.
#setup.template.json.enabled: false

# Path to the JSON template file
#setup.template.json.path: "${path.config}/template.json"

# Name under which the template is stored in Elasticsearch
#setup.template.json.name: ""

# Overwrite existing template
#setup.template.overwrite: false

# Elasticsearch template settings
setup.template.settings:

  # A dictionary of settings to place into the settings.index dictionary
  # of the Elasticsearch template. For more details, please check
  # https://www.elastic.co/guide/en/elasticsearch/reference/current/mapping.html
  #index:
    #number_of_shards: 1
    #codec: best_compression
    #number_of_routing_shards: 30

  # A dictionary of settings for the _source field. For more details, please check
  # https://www.elastic.co/guide/en/elasticsearch/reference/current/mapping-source-field.html
  #_source:
    #enabled: false

#============================== Setup ILM
=====================================

# Configure index lifecycle management (ILM). These settings create a write
# alias and add additional settings to the index template. When ILM is enabled,
# output.elasticsearch.index is ignored, and the write alias is used to set the
# index name.

# Enable ILM support. Valid values are true, false, and auto. When set to auto
# (the default), the Beat uses index lifecycle management when it connects to a
# cluster that supports ILM; otherwise, it creates daily indices.
#setup.ilm.enabled: auto

# Set the prefix used in the index lifecycle write alias name. The default alias
# name is 'filebeat-%{[agent.version]}'.
#setup.ilm.rollover_alias: "filebeat"
```

```
# Set the rollover index pattern. The default is "%{now/d}-000001".
#setup.ilm.pattern: "{now/d}-000001"

# Set the lifecycle policy name. The default policy name is
# 'filebeat-%{[agent.version]}'.
#setup.ilm.policy_name: "mypolicy"

# The path to a JSON file that contains a lifecycle policy configuration. Used
# to load your own lifecycle policy.
#setup.ilm.policy_file:

# Disable the check for an existing lifecycle policy. The default is false. If
# you disable this check, set setup.ilm.overwrite: true so the lifecycle policy
# can be installed.
#setup.ilm.check_exists: false

# Overwrite the lifecycle policy at startup. The default is false.
#setup.ilm.overwrite: false

#============================== 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" # TODO: Change this to the IP address of your ELK server
  # 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"

  # Optional protocol and basic auth credentials.
  #protocol: "https"
  #username: "elastic"
  #password: "changeme"

  # Optional HTTP path
  #path: ""

  # Use SSL settings for HTTPS. Default is true.
  #ssl.enabled: true
  # Configure SSL verification mode. If `none` is configured, all server hosts
  # and certificates will be accepted. In this mode, SSL based connections are
  # susceptible to man-in-the-middle attacks. Use only for testing. Default is
  # `full`.
  #ssl.verification_mode: full

  # List of supported/valid TLS versions. By default all TLS versions from 1.0 up to
  # 1.2 are enabled.
  #ssl.supported_protocols: [TLSv1.0, TLSv1.1, TLSv1.2]

  # SSL configuration. The 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"

  # Optional passphrase for decrypting the certificate key.
  #ssl.key_passphrase: ''

  # Configure cipher suites to be used for SSL connections
  #ssl.cipher_suites: []

  # Configure curve types for ECDHE-based cipher suites
  #ssl.curve_types: []

#
=================================Logging===================================
====
# There are four options for the log output: file, stderr, syslog, eventlog
# The file output is the default.

# Sets log level. The default log level is info.
# Available log levels are: error, warning, info, debug
#logging.level: info

# Enable debug output for selected components. To enable all selectors use ["*"]
# Other available selectors are "beat", "publish", "service"
# Multiple selectors can be chained.
#logging.selectors: [ ]
```

```
# Send all logging output to stderr. The default is false.
#logging.to_stderr: false

# Send all logging output to syslog. The default is false.
#logging.to_syslog: false

# Send all logging output to Windows Event Logs. The default is false.
#logging.to_eventlog: false

# If enabled, Filebeat periodically logs its internal metrics that have changed
# in the last period. For each metric that changed, the delta from the value at
# the beginning of the period is logged. Also, the total values for
# all non-zero internal metrics are logged on shutdown. The default is true.
#logging.metrics.enabled: true

# The period after which to log the internal metrics. The default is 30s.
#logging.metrics.period: 30s

# Logging to rotating files. Set logging.to_files to false to disable logging to
# files.
logging.to_files: true
logging.files:
  # Configure the path where the logs are written. The default is the logs directory
  # under the home path (the binary location).
  #path: /var/log/filebeat

  # The name of the files where the logs are written to.
  #name: filebeat

  # Configure log file size limit. If limit is reached, log file will be
  # automatically rotated
  #rotateeverybytes: 10485760 # = 10MB

  # Number of rotated log files to keep. Oldest files will be deleted first.
  #keepfiles: 7

  # The permissions mask to apply when rotating log files. The default value is 0600.
  # Must be a valid Unix-style file permissions mask expressed in octal notation.
  #permissions: 0600

  # Enable log file rotation on time intervals in addition to size-based rotation.
  # Intervals must be at least 1s. Values of 1m, 1h, 24h, 7*24h, 30*24h, and 365*24h
  # are boundary-aligned with minutes, hours, days, weeks, months, and years as
  # reported by the local system clock. All other intervals are calculated from the
  # Unix epoch. Defaults to disabled.
  #interval: 0

  # Rotate existing logs on startup rather than appending to the existing
  # file. Defaults to true.
  # rotateonstartup: true

# Set to true to log messages in JSON format.
#logging.json: false


#============================== X-Pack Monitoring
===============================
# Filebeat 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
# Filebeat instance will appear in the Stack Monitoring UI. If output.elasticsearch
# is enabled, the UUID is derived from the Elasticsearch cluster referenced by
output.elasticsearch.
#monitoring.cluster_uuid:

# Uncomment to send the metrics to Elasticsearch. Most settings from the
# Elasticsearch output are accepted here as well.
# Note that the settings should point to your Elasticsearch *monitoring* cluster.
# Any setting that is not set is automatically inherited from the Elasticsearch
# output configuration, so if you have the Elasticsearch output configured such
# that it is pointing to your Elasticsearch monitoring cluster, you can simply
# uncomment the following line.
#monitoring.elasticsearch:

  # 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: [":9200"]

  # Set gzip compression level.
  #compression_level: 0
```

```
# Optional protocol and basic auth credentials.
#protocol: "https"
#username: "beats_system"
#password: "changeme"

# Dictionary of HTTP parameters to pass within the URL with index operations.
#parameters:
  #param1: value1
  #param2: value2

# Custom HTTP headers to add to each request
#headers:
#  X-My-Header: Contents of the header

# Proxy server url
#proxy_url: http://proxy:3128

# The number of times a particular Elasticsearch index operation is attempted. If
# the indexing operation doesn't succeed after this many retries, the events are
# dropped. The default is 3.
#max_retries: 3

# The maximum number of events to bulk in a single Elasticsearch bulk API index request.
# The default is 50.
#bulk_max_size: 50

# The number of seconds to wait before trying to reconnect to Elasticsearch
# after a network error. After waiting backoff.init seconds, the Beat
# tries to reconnect. If the attempt fails, the backoff timer is increased
# exponentially up to backoff.max. After a successful connection, the backoff
# timer is reset. The default is 1s.
#backoff.init: 1s

# The maximum number of seconds to wait before attempting to connect to
# Elasticsearch after a network error. The default is 60s.
#backoff.max: 60s

# Configure HTTP request timeout before failing an request to Elasticsearch.
#timeout: 90

# Use SSL settings for HTTPS.
#ssl.enabled: true

# Configure SSL verification mode. If `none` is configured, all server hosts
```

```
  # and certificates will be accepted. In this mode, SSL based connections are
  # susceptible to man-in-the-middle attacks. Use only for testing. Default is
  # `full`.
  #ssl.verification_mode: full

  # List of supported/valid TLS versions. By default all TLS versions from 1.0 up to
  # 1.2 are enabled.
  #ssl.supported_protocols: [TLSv1.0, TLSv1.1, TLSv1.2]

  # SSL configuration. The 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"

  # Optional passphrase for decrypting the certificate key.
  #ssl.key_passphrase: ''

  # Configure cipher suites to be used for SSL connections
  #ssl.cipher_suites: []

  # Configure curve types for ECDHE-based cipher suites
  #ssl.curve_types: []

  # Configure what types of renegotiation are supported. Valid options are
  # never, once, and freely. Default is never.
  #ssl.renegotiation: never

  #metrics.period: 10s
  #state.period: 1m

#================================ HTTP Endpoint
======================================
# 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: false
```

```
# The HTTP endpoint will bind to this hostname, IP address, unix socket or named pipe.
# When using IP addresses, it is recommended to only use localhost.
#http.host: localhost

# Port on which the HTTP endpoint will bind. Default is 5066.
#http.port: 5066

# Define which user should be owning the named pipe.
#http.named_pipe.user:

# Define which the permissions that should be applied to the named pipe, use the Security
# Descriptor Definition Language (SDDL) to define the permission. This option cannot be used
with
# `http.user`.
#http.named_pipe.security_descriptor:

#============================== Process Security
=================================

# Enable or disable seccomp system call filtering on Linux. Default is enabled.
#seccomp.enabled: true

#================================== Migration
===================================

# This allows to enable 6.7 migration aliases
#migration.6_to_7.enabled: false
```