############################

# GRAYLOG CONFIGURATION FILE

############################

#

# This is the Graylog configuration file. The file has to use ISO 8859-1/Latin-1 character encoding.

# Characters that cannot be directly represented in this encoding can be written using Unicode escapes

# as defined in https://docs.oracle.com/javase/specs/jls/se8/html/jls-3.html#jls-3.3, using the \u prefix.

# For example, \u002c.

#

# \* Entries are generally expected to be a single line of the form, one of the following:

#

# propertyName=propertyValue

# propertyName:propertyValue

#

# \* White space that appears between the property name and property value is ignored,

# so the following are equivalent:

#

# name=Stephen

# name = Stephen

#

# \* White space at the beginning of the line is also ignored.

#

# \* Lines that start with the comment characters ! or # are ignored. Blank lines are also ignored.

#

# \* The property value is generally terminated by the end of the line. White space following the

# property value is not ignored, and is treated as part of the property value.

#

# \* A property value can span several lines if each line is terminated by a backslash (‘\’) character.

# For example:

#

# targetCities=\

# Detroit,\

# Chicago,\

# Los Angeles

#

# This is equivalent to targetCities=Detroit,Chicago,Los Angeles (white space at the beginning of lines is ignored).

#

# \* The characters newline, carriage return, and tab can be inserted with characters \n, \r, and \t, respectively.

#

# \* The backslash character must be escaped as a double backslash. For example:

#

# path=c:\\docs\\doc1

#

# If you are running more than one instances of Graylog server you have to select one of these

# instances as master. The master will perform some periodical tasks that non-masters won't perform.

is\_master = true

# The auto-generated node ID will be stored in this file and read after restarts. It is a good idea

# to use an absolute file path here if you are starting Graylog server from init scripts or similar.

node\_id\_file = /usr/share/graylog/data/config/node-id

# You MUST set a secret to secure/pepper the stored user passwords here. Use at least 64 characters.

# Generate one by using for example: pwgen -N 1 -s 96

password\_secret = replacethiswithyourownsecret!

# The default root user is named 'admin'

#root\_username = admin

# You MUST specify a hash password for the root user (which you only need to initially set up the

# system and in case you lose connectivity to your authentication backend)

# This password cannot be changed using the API or via the web interface. If you need to change it,

# modify it in this file.

# Create one by using for example: echo -n yourpassword | shasum -a 256

# and put the resulting hash value into the following line

# Default password: admin

# CHANGE THIS!

root\_password\_sha2 = 8c6976e5b5410415bde908bd4dee15dfb167a9c873fc4bb8a81f6f2ab448a918

# The email address of the root user.

# Default is empty

#root\_email = ""

# The time zone setting of the root user. See http://www.joda.org/joda-time/timezones.html for a list of valid time zones.

# Default is UTC

#root\_timezone = UTC

# Set plugin directory here (relative or absolute)

plugin\_dir = /usr/share/graylog/plugin

###############

# HTTP settings

###############

#### HTTP bind address

#

# The network interface used by the Graylog HTTP interface.

#

# This network interface must be accessible by all Graylog nodes in the cluster and by all clients

# using the Graylog web interface.

#

# If the port is omitted, Graylog will use port 9000 by default.

#

# Default: 127.0.0.1:9000

#http\_bind\_address = 127.0.0.1:9000

#http\_bind\_address = [2001:db8::1]:9000

http\_bind\_address = 0.0.0.0:9000

#### HTTP publish URI

#

# The HTTP URI of this Graylog node which is used to communicate with the other Graylog nodes in the cluster and by all

# clients using the Graylog web interface.

#

# The URI will be published in the cluster discovery APIs, so that other Graylog nodes will be able to find and connect to this Graylog node.

#

# This configuration setting has to be used if this Graylog node is available on another network interface than $http\_bind\_address,

# for example if the machine has multiple network interfaces or is behind a NAT gateway.

#

# If $http\_bind\_address contains a wildcard IPv4 address (0.0.0.0), the first non-loopback IPv4 address of this machine will be used.

# This configuration setting \*must not\* contain a wildcard address!

#

# Default: http://$http\_bind\_address/

#http\_publish\_uri = http://192.168.1.1:9000/

#### External Graylog URI

#

# The public URI of Graylog which will be used by the Graylog web interface to communicate with the Graylog REST API.

#

# The external Graylog URI usually has to be specified, if Graylog is running behind a reverse proxy or load-balancer

# and it will be used to generate URLs addressing entities in the Graylog REST API (see $http\_bind\_address).

#

# When using Graylog Collector, this URI will be used to receive heartbeat messages and must be accessible for all collectors.

#

# This setting can be overriden on a per-request basis with the "X-Graylog-Server-URL" HTTP request header.

#

# Default: $http\_publish\_uri

#http\_external\_uri =

#### Enable CORS headers for HTTP interface

#

# This is necessary for JS-clients accessing the server directly.

# If these are disabled, modern browsers will not be able to retrieve resources from the server.

# This is enabled by default. Uncomment the next line to disable it.

#http\_enable\_cors = false

#### Enable GZIP support for HTTP interface

#

# This compresses API responses and therefore helps to reduce

# overall round trip times. This is enabled by default. Uncomment the next line to disable it.

#http\_enable\_gzip = false

# The maximum size of the HTTP request headers in bytes.

#http\_max\_header\_size = 8192

# The size of the thread pool used exclusively for serving the HTTP interface.

#http\_thread\_pool\_size = 16

################

# HTTPS settings

################

#### Enable HTTPS support for the HTTP interface

#

# This secures the communication with the HTTP interface with TLS to prevent request forgery and eavesdropping.

#

# Default: false

#http\_enable\_tls = true

# The X.509 certificate chain file in PEM format to use for securing the HTTP interface.

#http\_tls\_cert\_file = /path/to/graylog.crt

# The PKCS#8 private key file in PEM format to use for securing the HTTP interface.

#http\_tls\_key\_file = /path/to/graylog.key

# The password to unlock the private key used for securing the HTTP interface.

#http\_tls\_key\_password = secret

# Comma separated list of trusted proxies that are allowed to set the client address with X-Forwarded-For

# header. May be subnets, or hosts.

#trusted\_proxies = 127.0.0.1/32, 0:0:0:0:0:0:0:1/128

# List of Elasticsearch hosts Graylog should connect to.

# Need to be specified as a comma-separated list of valid URIs for the http ports of your elasticsearch nodes.

# If one or more of your elasticsearch hosts require authentication, include the credentials in each node URI that

# requires authentication.

#

# Default: http://127.0.0.1:9200

elasticsearch\_hosts = http://elasticsearch:9200

# Maximum amount of time to wait for successfull connection to Elasticsearch HTTP port.

#

# Default: 10 Seconds

#elasticsearch\_connect\_timeout = 10s

# Maximum amount of time to wait for reading back a response from an Elasticsearch server.

#

# Default: 60 seconds

#elasticsearch\_socket\_timeout = 60s

# Maximum idle time for an Elasticsearch connection. If this is exceeded, this connection will

# be tore down.

#

# Default: inf

#elasticsearch\_idle\_timeout = -1s

# Maximum number of total connections to Elasticsearch.

#

# Default: 20

#elasticsearch\_max\_total\_connections = 20

# Maximum number of total connections per Elasticsearch route (normally this means per

# elasticsearch server).

#

# Default: 2

#elasticsearch\_max\_total\_connections\_per\_route = 2

# Maximum number of times Graylog will retry failed requests to Elasticsearch.

#

# Default: 2

#elasticsearch\_max\_retries = 2

# Enable automatic Elasticsearch node discovery through Nodes Info,

# see https://www.elastic.co/guide/en/elasticsearch/reference/5.4/cluster-nodes-info.html

#

# WARNING: Automatic node discovery does not work if Elasticsearch requires authentication, e. g. with Shield.

#

# Default: false

#elasticsearch\_discovery\_enabled = true

# Filter for including/excluding Elasticsearch nodes in discovery according to their custom attributes,

# see https://www.elastic.co/guide/en/elasticsearch/reference/5.4/cluster.html#cluster-nodes

#

# Default: empty

#elasticsearch\_discovery\_filter = rack:42

# Frequency of the Elasticsearch node discovery.

#

# Default: 30s

# elasticsearch\_discovery\_frequency = 30s

# Enable payload compression for Elasticsearch requests.

#

# Default: false

#elasticsearch\_compression\_enabled = true

# Disable checking the version of Elasticsearch for being compatible with this Graylog release.

# WARNING: Using Graylog with unsupported and untested versions of Elasticsearch may lead to data loss!

#elasticsearch\_disable\_version\_check = true

# Disable message retention on this node, i. e. disable Elasticsearch index rotation.

#no\_retention = false

# Do you want to allow searches with leading wildcards? This can be extremely resource hungry and should only

# be enabled with care. See also: http://docs.graylog.org/en/2.1/pages/queries.html

allow\_leading\_wildcard\_searches = false

# Do you want to allow searches to be highlighted? Depending on the size of your messages this can be memory hungry and

# should only be enabled after making sure your Elasticsearch cluster has enough memory.

allow\_highlighting = false

# Global request timeout for Elasticsearch requests (e. g. during search, index creation, or index time-range

# calculations) based on a best-effort to restrict the runtime of Elasticsearch operations.

# Default: 1m

#elasticsearch\_request\_timeout = 1m

# Global timeout for index optimization (force merge) requests.

# Default: 1h

#elasticsearch\_index\_optimization\_timeout = 1h

# Maximum number of concurrently running index optimization (force merge) jobs.

# If you are using lots of different index sets, you might want to increase that number.

# Default: 20

#elasticsearch\_index\_optimization\_jobs = 20

# Time interval for index range information cleanups. This setting defines how often stale index range information

# is being purged from the database.

# Default: 1h

#index\_ranges\_cleanup\_interval = 1h

# Batch size for the Elasticsearch output. This is the maximum (!) number of messages the Elasticsearch output

# module will get at once and write to Elasticsearch in a batch call. If the configured batch size has not been

# reached within output\_flush\_interval seconds, everything that is available will be flushed at once. Remember

# that every outputbuffer processor manages its own batch and performs its own batch write calls.

# ("outputbuffer\_processors" variable)

output\_batch\_size = 500

# Flush interval (in seconds) for the Elasticsearch output. This is the maximum amount of time between two

# batches of messages written to Elasticsearch. It is only effective at all if your minimum number of messages

# for this time period is less than output\_batch\_size \* outputbuffer\_processors.

output\_flush\_interval = 1

# As stream outputs are loaded only on demand, an output which is failing to initialize will be tried over and

# over again. To prevent this, the following configuration options define after how many faults an output will

# not be tried again for an also configurable amount of seconds.

output\_fault\_count\_threshold = 5

output\_fault\_penalty\_seconds = 30

# The number of parallel running processors.

# Raise this number if your buffers are filling up.

processbuffer\_processors = 5

outputbuffer\_processors = 3

# The following settings (outputbuffer\_processor\_\*) configure the thread pools backing each output buffer processor.

# See https://docs.oracle.com/javase/8/docs/api/java/util/concurrent/ThreadPoolExecutor.html for technical details

# When the number of threads is greater than the core (see outputbuffer\_processor\_threads\_core\_pool\_size),

# this is the maximum time in milliseconds that excess idle threads will wait for new tasks before terminating.

# Default: 5000

#outputbuffer\_processor\_keep\_alive\_time = 5000

# The number of threads to keep in the pool, even if they are idle, unless allowCoreThreadTimeOut is set

# Default: 3

#outputbuffer\_processor\_threads\_core\_pool\_size = 3

# The maximum number of threads to allow in the pool

# Default: 30

#outputbuffer\_processor\_threads\_max\_pool\_size = 30

# UDP receive buffer size for all message inputs (e. g. SyslogUDPInput).

#udp\_recvbuffer\_sizes = 1048576

# Wait strategy describing how buffer processors wait on a cursor sequence. (default: sleeping)

# Possible types:

# - yielding

# Compromise between performance and CPU usage.

# - sleeping

# Compromise between performance and CPU usage. Latency spikes can occur after quiet periods.

# - blocking

# High throughput, low latency, higher CPU usage.

# - busy\_spinning

# Avoids syscalls which could introduce latency jitter. Best when threads can be bound to specific CPU cores.

processor\_wait\_strategy = blocking

# Size of internal ring buffers. Raise this if raising outputbuffer\_processors does not help anymore.

# For optimum performance your LogMessage objects in the ring buffer should fit in your CPU L3 cache.

# Must be a power of 2. (512, 1024, 2048, ...)

ring\_size = 65536

inputbuffer\_ring\_size = 65536

inputbuffer\_processors = 2

inputbuffer\_wait\_strategy = blocking

# Enable the disk based message journal.

message\_journal\_enabled = true

# The directory which will be used to store the message journal. The directory must me exclusively used by Graylog and

# must not contain any other files than the ones created by Graylog itself.

#

# ATTENTION:

# If you create a seperate partition for the journal files and use a file system creating directories like 'lost+found'

# in the root directory, you need to create a sub directory for your journal.

# Otherwise Graylog will log an error message that the journal is corrupt and Graylog will not start.

message\_journal\_dir = /usr/share/graylog/data/journal

# Journal hold messages before they could be written to Elasticsearch.

# For a maximum of 12 hours or 5 GB whichever happens first.

# During normal operation the journal will be smaller.

#message\_journal\_max\_age = 12h

#message\_journal\_max\_size = 5gb

#message\_journal\_flush\_age = 1m

#message\_journal\_flush\_interval = 1000000

#message\_journal\_segment\_age = 1h

#message\_journal\_segment\_size = 100mb

# Number of threads used exclusively for dispatching internal events. Default is 2.

#async\_eventbus\_processors = 2

# How many seconds to wait between marking node as DEAD for possible load balancers and starting the actual

# shutdown process. Set to 0 if you have no status checking load balancers in front.

lb\_recognition\_period\_seconds = 3

# Journal usage percentage that triggers requesting throttling for this server node from load balancers. The feature is

# disabled if not set.

#lb\_throttle\_threshold\_percentage = 95

# Every message is matched against the configured streams and it can happen that a stream contains rules which

# take an unusual amount of time to run, for example if its using regular expressions that perform excessive backtracking.

# This will impact the processing of the entire server. To keep such misbehaving stream rules from impacting other

# streams, Graylog limits the execution time for each stream.

# The default values are noted below, the timeout is in milliseconds.

# If the stream matching for one stream took longer than the timeout value, and this happened more than "max\_faults" times

# that stream is disabled and a notification is shown in the web interface.

#stream\_processing\_timeout = 2000

#stream\_processing\_max\_faults = 3

# Length of the interval in seconds in which the alert conditions for all streams should be checked

# and alarms are being sent.

#alert\_check\_interval = 60

# Since 0.21 the Graylog server supports pluggable output modules. This means a single message can be written to multiple

# outputs. The next setting defines the timeout for a single output module, including the default output module where all

# messages end up.

#

# Time in milliseconds to wait for all message outputs to finish writing a single message.

#output\_module\_timeout = 10000

# Time in milliseconds after which a detected stale master node is being rechecked on startup.

#stale\_master\_timeout = 2000

# Time in milliseconds which Graylog is waiting for all threads to stop on shutdown.

#shutdown\_timeout = 30000

# MongoDB connection string

# See https://docs.mongodb.com/manual/reference/connection-string/ for details

mongodb\_uri = mongodb://mongo/graylog

# Authenticate against the MongoDB server

#mongodb\_uri = mongodb://grayloguser:secret@mongo:27017/graylog

# Use a replica set instead of a single host

#mongodb\_uri = mongodb://grayloguser:secret@mongo:27017,mongo:27018,mongo:27019/graylog

# Increase this value according to the maximum connections your MongoDB server can handle from a single client

# if you encounter MongoDB connection problems.

mongodb\_max\_connections = 100

# Number of threads allowed to be blocked by MongoDB connections multiplier. Default: 5

# If mongodb\_max\_connections is 100, and mongodb\_threads\_allowed\_to\_block\_multiplier is 5,

# then 500 threads can block. More than that and an exception will be thrown.

# http://api.mongodb.com/java/current/com/mongodb/MongoOptions.html#threadsAllowedToBlockForConnectionMultiplier

mongodb\_threads\_allowed\_to\_block\_multiplier = 5

# Drools Rule File (Use to rewrite incoming log messages)

# See: http://docs.graylog.org/en/2.1/pages/drools.html

#rules\_file = /etc/graylog/server/rules.drl

# Email transport

#transport\_email\_enabled = false

#transport\_email\_hostname = mail.example.com

#transport\_email\_port = 587

#transport\_email\_use\_auth = true

#transport\_email\_use\_tls = true

#transport\_email\_use\_ssl = true

#transport\_email\_auth\_username = you@example.com

#transport\_email\_auth\_password = secret

#transport\_email\_subject\_prefix = [graylog]

#transport\_email\_from\_email = graylog@example.com

# Specify and uncomment this if you want to include links to the stream in your stream alert mails.

# This should define the fully qualified base url to your web interface exactly the same way as it is accessed by your users.

#transport\_email\_web\_interface\_url = https://graylog.example.com

# The default connect timeout for outgoing HTTP connections.

# Values must be a positive duration (and between 1 and 2147483647 when converted to milliseconds).

# Default: 5s

#http\_connect\_timeout = 5s

# The default read timeout for outgoing HTTP connections.

# Values must be a positive duration (and between 1 and 2147483647 when converted to milliseconds).

# Default: 10s

#http\_read\_timeout = 10s

# The default write timeout for outgoing HTTP connections.

# Values must be a positive duration (and between 1 and 2147483647 when converted to milliseconds).

# Default: 10s

#http\_write\_timeout = 10s

# HTTP proxy for outgoing HTTP connections

#http\_proxy\_uri =

# The threshold of the garbage collection runs. If GC runs take longer than this threshold, a system notification

# will be generated to warn the administrator about possible problems with the system. Default is 1 second.

#gc\_warning\_threshold = 1s

# Connection timeout for a configured LDAP server (e. g. ActiveDirectory) in milliseconds.

#ldap\_connection\_timeout = 2000

# Disable the use of SIGAR for collecting system stats

#disable\_sigar = false

# The default cache time for dashboard widgets. (Default: 10 seconds, minimum: 1 second)

#dashboard\_widget\_default\_cache\_time = 10s

# Automatically load content packs in "content\_packs\_dir" on the first start of Graylog.

content\_packs\_loader\_enabled = true

# The directory which contains content packs which should be loaded on the first start of Graylog.

content\_packs\_dir = /usr/share/graylog/data/contentpacks

# A comma-separated list of content packs (files in "content\_packs\_dir") which should be applied on

# the first start of Graylog.

# Default: empty

content\_packs\_auto\_load = grok-patterns.json

# For some cluster-related REST requests, the node must query all other nodes in the cluster. This is the maximum number

# of threads available for this. Increase it, if '/cluster/\*' requests take long to complete.

# Should be http\_thread\_pool\_size \* average\_cluster\_size if you have a high number of concurrent users.

proxied\_requests\_thread\_pool\_size = 32