一致性选择：如何实现数据一致性与事务一致性

存储数据结构：在写入与读取操作上选择了什么数据结构

读写性能：读写操作的效率

事务支持：是否支持分布式事务，支持什么级别

数据正确性：如何保证数据不丢失

内存管理：如何使用内存提高效率，如何回收内存

锁的实现

任务队列

网络框架

压缩与解压缩

多表操作

```
# This is the folder that contains the rule yaml files
# Any .yaml file will be loaded as a rule
rules_folder: example_rules

# How often ElastAlert will query Elasticsearch
# The unit can be anything from weeks to seconds
run_every:
 minutes: 1

# ElastAlert will buffer results from the most recent
# period of time, in case some log sources are not in real time
buffer_time:
 minutes: 15

# The Elasticsearch hostname for metadata writeback
# Note that every rule can have its own Elasticsearch host
es_host: es1

# The Elasticsearch portsss
es_port: 9200

# The AWS region to use. Set this when using AWS-managed elasticsearch
#aws_region: us-east-1

# The AWS profile to use. Use this if you are using an aws-cli profile.
# See http://docs.aws.amazon.com/cli/latest/userguide/cli-chap-getting-started.html
# for details
#profile: test

# Optional URL prefix for Elasticsearch
#es_url_prefix: elasticsearch

# Connect with TLS to Elasticsearch
#use_ssl: True

# Verify TLS certificates
#verify_certs: True

# GET request with body is the default option for Elasticsearch.
# If it fails for some reason, you can pass 'GET', 'POST' or 'source'.
# See http://elasticsearch-py.readthedocs.io/en/master/connection.html?highlight=send_get_body_as#transport
# for details
#es_send_get_body_as: GET

# Option basic-auth username and password for Elasticsearch
es_username: elastic
es_password: elastic

# Use SSL authentication with client certificates client_cert must be
# a pem file containing both cert and key for client
#verify_certs: True
#ca_certs: /path/to/cacert.pem
#client_cert: /path/to/client_cert.pem
#client_key: /path/to/client_key.key

# The index on es_host which is used for metadata storage
# This can be a unmapped index, but it is recommended that you run
# elastalert-create-index to set a mapping
writeback_index: elastalert_status

# If an alert fails for some reason, ElastAlert will retry
# sending the alert until this time period has elapsed
alert_time_limit:
  days: 2
```

```

# Custom logging configuration
# If you want to setup your own logging configuration to log into
# files as well or to Logstash and/or modify log levels, use
# the configuration below and adjust to your needs.
# Note: if you run ElastAlert with --verbose/--debug, the log level of
# the "elastalert" logger is changed to INFO, if not already INFO/DEBUG.
#logging:
# version: 1
# incremental: false
# disable_existing_loggers: false
# formatters:
# logline:
# format: '%(asctime)s %(levelname)+8s %(name)+20s %(message)s'
#
# handlers:
# console:
# class: logging.StreamHandler
# formatter: logline
# level: DEBUG
# stream: ext://sys.stderr
#
# file:
# class : logging.FileHandler
# formatter: logline
# level: DEBUG
# filename: elastalert.log
#
# loggers:
# elastalert:
# level: WARN
# handlers: []
# propagate: true
#
# elasticsearch:
# level: WARN
# handlers: []
# propagate: true
#
# elasticsearch.trace:
```

```
# level: WARN
# handlers: []
# propagate: true
#
# '': # root logger
# level: WARN
# handlers:
# - console
# - file
# propagate: false
```