# Graylog

## Docker

* Install Docker

## Setup Graylog

* Create a docker-compose.yml

version: '2'

services:

# MongoDB: https://hub.docker.com/\_/mongo/

mongodb:

image: mongo:3

# Elasticsearch: https://www.elastic.co/guide/en/elasticsearch/reference/5.6/docker.html

elasticsearch:

image: docker.elastic.co/elasticsearch/elasticsearch:5.6.3

environment:

- http.host=0.0.0.0

- transport.host=localhost

- network.host=0.0.0.0

# Disable X-Pack security: https://www.elastic.co/guide/en/elasticsearch/reference/5.6/security-settings.html#general-security-settings

- xpack.security.enabled=false

- "ES\_JAVA\_OPTS=-Xms512m -Xmx512m"

ulimits:

memlock:

soft: -1

hard: -1

mem\_limit: 1g

# Graylog: https://hub.docker.com/r/graylog/graylog/

graylog:

image: graylog/graylog:2.4.0-1

environment:

# CHANGE ME!

- GRAYLOG\_PASSWORD\_SECRET=somepasswordpepper

# Password: admin

- GRAYLOG\_ROOT\_PASSWORD\_SHA2=8c6976e5b5410415bde908bd4dee15dfb167a9c873fc4bb8a81f6f2ab448a918

- GRAYLOG\_WEB\_ENDPOINT\_URI=http://127.0.0.1:9000/api

links:

- mongodb:mongo

- elasticsearch

depends\_on:

- mongodb

- elasticsearch

ports:

# Graylog web interface and REST API

- 9000:9000

# Syslog TCP

- 514:514

# Syslog UDP

- 514:514/udp

# GELF TCP

- 12201:12201

# GELF UDP

- 12201:12201/udp

* Execute the file

docker-compose up

* You can open the URL http://127.0.0.1:9000 in a web browser and log in with username admin and password admin
* Set a input for your app

## For normal log

* Install graylog2

npm install graylog2

* Import and set graylog2

var graylog2 **=** require("graylog2");

var logger **=** **new** graylog2.graylog({

    servers**:** [

        { 'host'**:** '127.0.0.1', port**:** 12201 },

        { 'host'**:** '127.0.0.2', port**:** 12201 }

    ],

    hostname**:** 'server.name', *// the name of this host*

*// (optional, default: os.hostname())*

    facility**:** 'Node.js',     *// the facility for these log messages*

*// (optional, default: "Node.js")*

    bufferSize**:** 1350         *// max UDP packet size, should never exceed the*

*// MTU of your system (optional, default: 1400)*

});

logger.on('error', function (error) {

    console.error('Error while trying to write to graylog2:', error);

});

* Log message exemple:

logger.log("What we've got here is...failure to communicate");

* Check your log on http://127.0.0.1:9000 in Inputs/Show received messages

## Http middleware log

npm install graylog-loging --save

var graylog = require('graylog-loging');

graylog.init({

graylogPort: 12201,

graylogHostname: '192.0.0.1'

});

app.use(graylog.logRequest);

app.use(graylog.logResponse);

app.use(graylog.handleErrors)

Source:

* http://docs.graylog.org/en/latest/pages/installation/docker.html
* https://www.npmjs.com/package/graylog-loging