

BATUHAN TORUK


HAFTA 4



İÇERİK

GRAYGOL İLE VERİ GÖRÜNTÜLEME





Graylog windows üzerinden kullanıma uygun olmadığı için docker desktop uygulamasını kullanarak graylog'u konfigüre edeceğiz öncelikle bir klasör açıp graylog-setup adını verdim ve içine birkeç kod yazarak konfigüre işlemini tamamladım tamamlanan konfigüre işleminden sonra docker desktop üzerinden dockerın kendi terminalini açıyoruz ve açılan terminalde klasöre giriş yapıyoruz sonrasında compose up komutu ile graylog ve çalışması için yüklediğimiz öbür bileşenleri aktif hale getiriyoruz(elastisearch-mongo-graylog).Aktif hale getirdikten sonra tarayıcıdan <http://127.0.0.1:9000> adresine giderek graylog arayüzüne belirlediğimiz kullanıcı adı ve şifre ile giriş yapıyoruz.Giriş yaptıktan sonra graylogtan kendimize bir input oluşturuyoruz. Graylogtan log takibi yapabilmek için log göndermemiz gerekmekte bu işlem için ise NXlog uygulamasını kurmamız yada sanal bir makine oluşturup kendi ip adresimize log göndermemiz gerekmekte. Tüm bu işlemler tamamlandıktan sonra log görüntülenmesi gerçekleşecektir.



- Containers
- Images
- Volumes
- Builds
- Docker Scout
- Extensions

graylog-setup

C:\graylog-setup

[View Configurations](#)

graylog-setup-elast...
elasticsearch/elastics
9200:9200

graylog-setup-mon...
mongo:4.0

graylog-setup-grayl...
graylog/graylog:4.0
12201:12201
Show all ports (2)

```
"component": "o.e.l.LicenseService", "cluster.name": "docker-cluster", "node.name": "44f4313b8c2b", "message": "license [eca59574-aca5-44cb-8a48-9fca6502e02f] mode [basic] - valid", "cluster.uuid": "ZJh-3MRPQZ2iepP4Uzb_ng", "node.id": "GihFJqJKRxW8bp70ghW2uQ" }
2024-11-05 21:38:56 elasticsearch-1 | {"type": "server", "timestamp": "2024-11-05T18:38:56,544Z", "level": "INFO", "component": "o.e.x.s.s.SecurityChangeListener", "cluster.name": "docker-cluster", "node.name": "44f4313b8c2b", "message": "Active license is now [BASIC]; Security is disabled", "cluster.uuid": "ZJh-3MRPQZ2iepP4Uzb_ng", "node.id": "GihFJqJKRxW8bp70ghW2uQ" }
2024-11-05 21:38:56 elasticsearch-1 | {"type": "server", "timestamp": "2024-11-05T18:38:56,549Z", "level": "INFO", "component": "o.e.g.GatewayService", "cluster.name": "docker-cluster", "node.name": "44f4313b8c2b", "message": "recovered [3] indices into cluster_state", "cluster.uuid": "ZJh-3MRPQZ2iepP4Uzb_ng", "node.id": "GihFJqJKRxW8bp70ghW2uQ" }
2024-11-05 21:38:56 graylog-1 | 2024-11-05 18:38:56,637 INFO : org.hibernate.validator.internal.util.Version - HV000001: Hibernate Validator null
2024-11-05 21:38:56 elasticsearch-1 | {"type": "server", "timestamp": "2024-11-05T18:38:56,930Z", "level": "INFO", "component": "o.e.c.r.a.AllocationService", "cluster.name": "docker-cluster", "node.name": "44f4313b8c2b", "message": "Cluster health status changed from [RED] to [GREEN] (reason: [shards started [[gl-events_0][0], [gl-system-events_0][0], [graylog_0][0]]).", "cluster.uuid": "ZJh-3MRPQZ2iepP4Uzb_ng", "node.id": "GihFJqJKRxW8bp70ghW2uQ" }
```

Terminal

```
PS C:\graylog-setup> docker-compose up -d
time="2024-11-05T21:38:43+03:00" level=warning msg="C:\\graylog-setup\\docker-compose.yml: the attribute `version` is obsolete, it will be ignored, please remove it to avoid potential confusion"
[+] Running 3/3
 ✓ Container graylog-setup-graylog-1      Started      1.0s
 ✓ Container graylog-setup-mongo-1        Started      0.9s
 ✓ Container graylog-setup-elasticsearch-1 Started      0.9s
PS C:\graylog-setup>
```

Docker
desktop
üzerinden
graylogu
başlatıyoruz



We could not load the [Graylog Getting Started Guide](#). Please open it directly with a browser that can access the public internet.

Graylog arayüzüne giriş yapıyoruz

Graylog 4.0.17+d0c5b22 on ad5a2ee54d52 (Oracle Corporation 1.8.0_332 on Linux 5.15.153.1-microsoft-standard-WSL2)

There are no global inputs.

Local inputs 1 configured

denemee GELF TCP RUNNING

Show received messages Manage extractors Stop input More actions

On node 43a5b9d2 / b2b2c44e0644

```
bind_address: 0.0.0.0
decompress_size_limit: 8388608
max_message_size: 2097152
number_worker_threads: 12
override_source: <empty>
port: 12201
recv_buffer_size: 262144
tcp_keepalive: false
tls_cert_file: <empty>
tls_client_auth: disabled
tls_client_auth_cert_file: <empty>
tls_enable: false
tls_key_file: <empty>
tls_key_password:*****
use_null_delimiter: true
```

Throughput / Metrics
1 minute average rate: 0 msg/s
Network IO: 0B 0B (total: 1000.0B 0B)
Active connections: 1 (4 total)
Empty messages discarded: 0

Graylogtan input oluřturulması

```
>>
CONTAINER ID   IMAGE                                COMMAND                                  CREATED        STATUS              PORTS
NAMES
67c1ef349c58   graylog/graylog:4.0                "tini -- /docker-ent..."             7 minutes ago   Up 7 minutes (healthy)   0.0.0.0:9000->9000/tcp, 0.0.0.0:12201->122
01/tcp   graylog-setup-graylog-1
9441822105b9   mongo:4.0                          "docker-entrypoint.s..."             15 minutes ago   Up 15 minutes           27017/tcp
                                graylog-setup-mongo-1
fe784a58b42a   elasticsearch:7.9.3                "/tini -- /usr/local..."             15 minutes ago   Up 15 minutes           9200/tcp, 9300/tcp
                                graylog-setup-elasticsearch-1
PS C:\Users\toruk>
```

Graylog bileşenlerinin çalışıp çalışmadığının kontrolü

inputların davranışlarının
kontrol edilmesi



timestamp

source

2024-11-05 19:01:04.977 +00:00

Batuhan

Batuhan TORUK_Test mesajı.

4ec10ba0-9ba8-11ef-8e3b-0242ac120004

Timestamp

2024-11-05 19:01:04.977

Received by

denemee on 43a5b9d2 / b2b2c44e0644

Stored in index

graylog_0

Routed into streams

All messages

facility

my_logger

file

C:\graylog-setup\send_graylog.py

function

<module>

level

6

line

11

message

Batuhan TORUK_Test mesajı.

pid

133576

process_name

MainProcess

source

Batuhan

thread name

Permalink

Copy ID

Show surrounding messages

Test against stream

Logların detayı