BATUHAN TORUK HAFTA 4

IGERIK

GRAYGOL ILE VERI 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 görüntülemesi gerçekleşecektir.



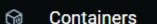


View Configurations









- **Images**
- Volumes
- Builds
- **Docker Scout**
- Extensions

Docker desktop üzerinden graylogu başlatıyoruz



"component": "o.e.l.LicenseService", "cluster.name": "docker-cluster", "node.name": "44f4313b8c2b", "message": "lice nse [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.SecurityStatusChangeListener", "cluster.name": "docker-cluster", "node.name": "44f4313b8c2b" , "message": "Active license is now [BASIC]; Security is disabled", "cluster.uuid": "ZJh-3MRPQZ2iepP4Uzb_ng", "node. id": "GihFJqJKRxW8bp70ghW2uQ" 回 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": "reco vered [3] indices into cluster_state", "cluster.uuid": "ZJh-3MRPQZ2iepP4Uzb_ng", "node.id": "GihFJqJKRxW8bp70ghW2uQ" 2024-11-05 18:38:56,637 INFO : org.hibernate.validator.internal.util.Version 2024-11-05 21:38:56 graylog-1 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": "GihFJqJKRxW8bp7OghW2uQ" }

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 ignor ed, please remove it to avoid potential confusion" [+] Running 3/3 1.0s

√ Container graylog-setup-graylog-1 Started √ Container graylog-setup-mongo-1 Started

√ Container graylog-setup-elasticsearch-1 Started

PS C:\graylog-setup> ||







Engine running





Windo.

Windo...

















0.9s

0.9s



Search Streams Alerts

Dashboards

Enterprise







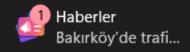


X Dismiss guide

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)



















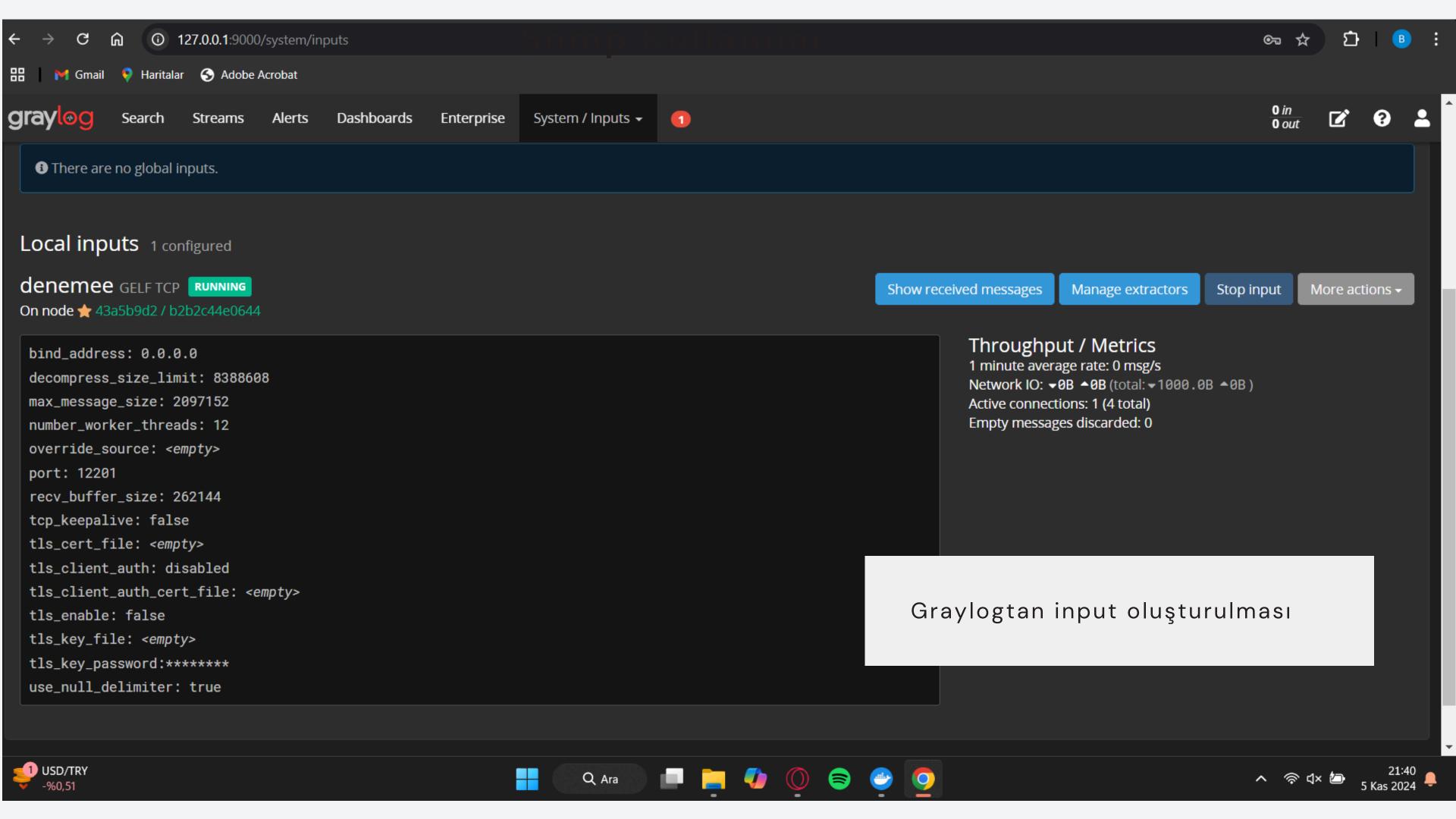












>> CONTAINER ID **IMAGE** COMMAND CREATED **STATUS PORTS** NAMES "tini -- /docker-ent..." 7 minutes ago Up 7 minutes (healthy) 67c1ef349c58 graylog/graylog:4.0 0.0.0.0:9000->9000/tcp, 0.0.0.0:12201->122 graylog-setup-graylog-1 01/tcp 9441822105b9 mongo:4.0 "docker-entrypoint.s..." 15 minutes ago Up 15 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

