İŞLETİM SİSTEMLERİ

ElasticSearch ve Kibana ile MySQL veritabanının

Log takibi ve görselleştirilmesi

Gazi Üniversitesi

Grup Üyeleri: Berke Güneş-181816064 && Selim Savaş-181816070

Özet

Ubuntu sunucusu üzerinde kurulumunu yaptığımız ElasticSearch paketini, ters proxy(nginx) ile kibana eklentisine bağladıktan sonra, Ubuntu üzerinde kurulu olan MySQL veritabanının, Beat ailesinde yaygın olarak kullanılan Filebeat paketi ile toplanmasının ardından Kibana eklentisinde görselleştirilmesi

Anahtar Kelimeler: ElasticSearch, Kibana, Filebeat, MySQL, Log, Proxy, UFW, Nginx

1. GİRİŞ

Daha önce *ELK Yığını* olarak bilinen Elastic Stack , Elastic tarafından üretilen ve herhangi bir biçimde herhangi bir kaynaktan oluşturulan günlükleri aramanıza, analiz etmenize ve görselleştirmenize olanak tanıyan, *merkezi günlük kaydı* olarak bilinen bir uygulama olan açık kaynaklı bir yazılım koleksiyonudur . Merkezi günlük kaydı, sunucularınız veya uygulamalarınızla ilgili sorunları belirlemeye çalışırken çok yararlı olabilir, çünkü tüm günlüklerinizi tek bir yerde aramanıza izin verir. Ayrıca, belirli bir zaman dilimi boyunca günlüklerini ilişkilendirerek birden çok sunucuya yayılan sorunları tanımlamanıza izin verdiği için de kullanışlıdır.

Elastic Stack'in dört ana bileşeni vardır:

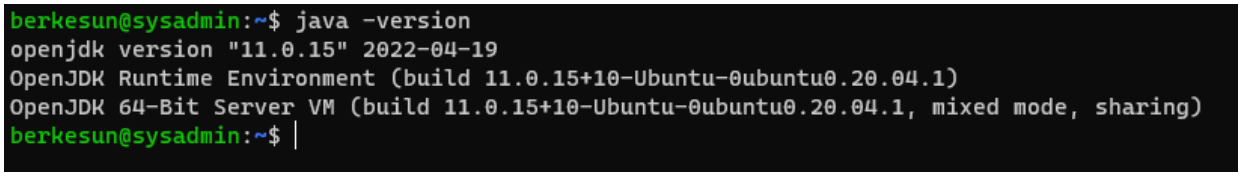
- **Elasticsearch** :toplanan tüm verileri depolayandağıtılmış bir *RESTful* arama motoru.
- **Logstash** : **Elasticsearch'e** gelen verileri gönderen Elastic **Stack'ın** veri işleme bileşeni.
- **Kibana** : günlükleri aramak ve görselleştirmek için bir web arayüzü.
- **Beats** : yüzlerce veya binlerce makineden Logstash veya Elasticsearch'e veri gönderebilen hafif, tek amaçlı veri taşıyıcıları.

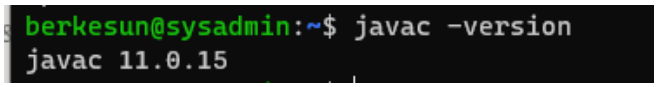
ElasticSearch kurulumu için, sunucunuzda önkoşul olarak Java JRE/SDK kurulması gerekmektedir.

2. JAVA SDK/JRE Kurulumu

```
sudo apt update
sudo apt install default-jre
java -version
```

```
sudo apt install default-jdk
javac -version
```



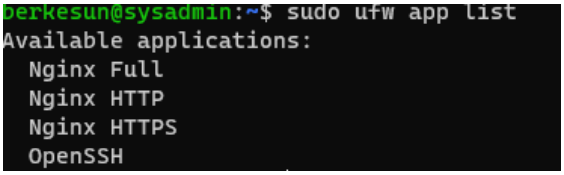


2. Nginx'i Kurmak

```
sudo apt update
sudo apt install nginx
```

Nginx'i test etmeden önce, hizmete erişime izin vermek için güvenlik duvarı yazılımının ayarlanması gerekir. Nginx ufw, kurulumdan sonra kendisini bir hizmet olarak kaydeder ve Nginx erişimine izin vermeyi kolaylaştırır.

```
sudo ufw app list
```



Yapılandırdığınız trafiğe yine de izin verecek en kısıtlayıcı profili etkinleştirmeniz önerilir. Henüz bu kılavuzda sunucumuz için SSL yapılandırmadığımızdan, yalnızca 80 numaralı bağlantı noktasında trafiğe izin vermemiz gerekecek.

```
sudo ufw allow 'Nginx HTTP'
```

3. Elasticsearch Kurulumu ve Yapılandırılması

Elastic Stack'in tüm paketleri, sisteminizi paket sahtekarlığından korumak için Elasticsearch imzalama anahtarı ile imzalanmıştır. Anahtar kullanılarak kimliği doğrulanan paketler, paket yöneticiniz tarafından güvenilir olarak kabul edilecektir. Bu adımda, Elasticsearch'ü kurmak için Elasticsearch genel GPG anahtarını içe aktaracak ve Elastic paket kaynak listesini ekleyeceksiniz.

```
wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -
```

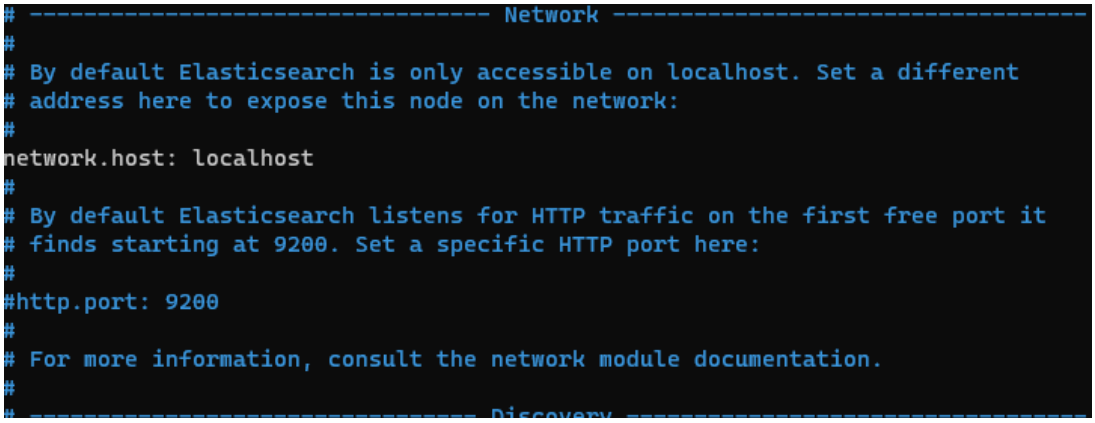
Ardından, Esnek kaynak listesini `sources.list.d`, APT'nin yeni kaynakları arayacağı dizine ekleyin :

```
echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee -a /etc/apt/sources.list.d/elastic-7.x.list
```

```
sudo apt update
sudo apt install elasticsearch
```

Elasticsearch kurulumu tamamlandığında, Elasticsearch'ün ana yapılandırma dosyasını düzenlemek için tercih ettiğiniz metin düzenleyiciyi kullanın `elasticsearch.yml`

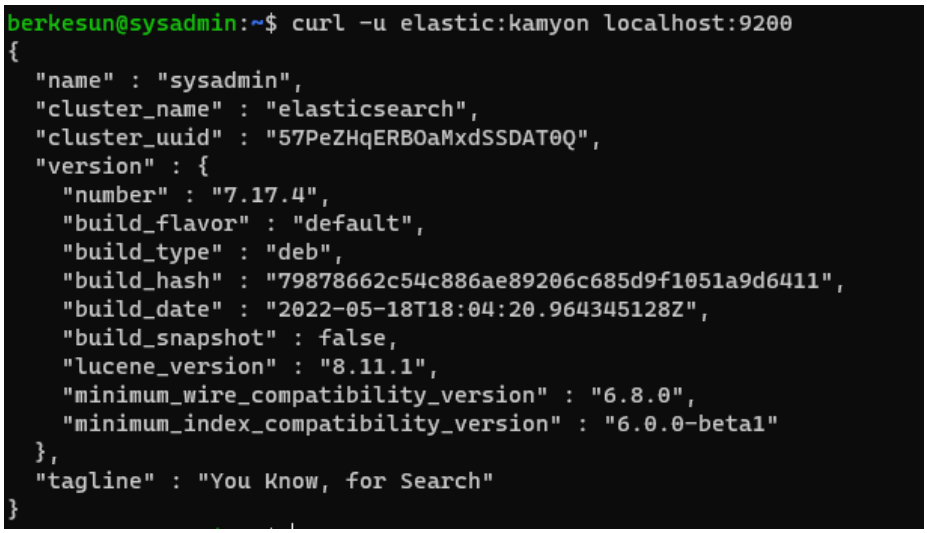
```
sudo nano /etc/elasticsearch/elasticsearch.yml
```




```
sudo systemctl enable elasticsearch
sudo systemctl start elasticsearch
```

Elasticsearch hizmetinizin çalışıp çalışmadığını bir HTTP isteği göndererek test edebilirsiniz:

```
curl -u elastic:kamyon localhost:9200
```



4. Kibana Dashboard'u Kurma ve Yapılandırması

```
sudo apt install kibana
sudo systemctl enable kibana
sudo systemctl start kibana
```

Kibana yalnızca dinleyecek şekilde yapılandırıldığından `localhost`, ona harici erişime izin vermek için bir ters proxy kurmalıyız . Bu amaçla sunucunuza zaten kurulu olması gereken Nginx'i kullanacağız.

İlk olarak, `openssh`, SSH Key kullanarak Kibana için güçlü bir parola oluşturacağız.

```
echo "kibanaadmin:`openssh passwd -apr1`" | sudo tee -a /etc/nginx/htpasswd.users
```

Ardından, bir Nginx sunucu blok dosyası oluşturacağız. Örnek olarak bu dosyaya şu şekilde adlandıralım. `example.com`

```
sudo nano /etc/nginx/sites-available/example.com
```

Nginx'i sunucunuzun HTTP trafiğini dinleyen Kibana uygulamasına yönlendirecek şekilde yapılandıralım ve güvenliği az önce oluşturduğumuz htpasswd prensibine göre düzenleyelim.

```
  GNU nano 4.8
server {
    listen 80;

    server_name example.com;

    auth_basic "Restricted Access";
    auth_basic_user_file /etc/nginx/htpasswd.users;

    location / {
        proxy_pass http://192.168.43.35:5601;
        proxy_http_version 1.1;
        proxy_set_header Upgrade $http_upgrade;
        proxy_set_header Connection 'upgrade';
        proxy_set_header Host $host;
        proxy_cache_bypass $http_upgrade;
    }
}
```

Ardından, `sites-enabled` dizine sembolik bir bağlantı oluşturarak yeni yapılandırmayı etkinleştirelim.

```
sudo ln -s /etc/nginx/sites-available/example.com /etc/nginx/sites-enabled/example.com
sudo nginx -t
```

```
berkesun@sysadmin:~$ sudo nginx -t
nginx: the configuration file /etc/nginx/nginx.conf syntax is ok
nginx: configuration file /etc/nginx/nginx.conf test is successful
```

```
sudo systemctl restart nginx
sudo ufw allow 'Nginx Full'
```

5. Elasticsearch ve Kibana’yı tam yetkili hale getirme

Tanımlı olarak yüklendiğinde bize sınırlı yetkisi olan bu eklenti paketine Log takibinin yapılabilmesi için .yml dosyalarında bir kaç düzenleme ve yeni parola oluşturulması gerekir.

xpack güvenlik aşamasını elasticsearch.yml dosyasına ekleyelim.

```
sudo nano /etc/elasticsearch/elasticsearch.yml

xpack.security.enabled: true
```

```
berkesun@sysadmin: ~
  GNU nano 4.8                                  /etc/elasticsearch/elasticsearch.yml
xpack.security.enabled: true
discovery.type: single-node

# ======================== Elasticsearch Configuration =========================
#
```

Daha sonra tanımlı olan kullanıcı ve şifreleri değiştirip bunu kibana.yml dosyasına tanımlamamız gerekiyor.

```
cd /usr/share/elasticsearch

./bin/elasticsearch-setup-passwords interactive
```

Bu işlemi yaptıktan sonra bize her eklenti için şifre belirlememizi isteyecektir.

```
sudo nano /etc/kibana/kibana.yml
```

```
# The default application to load.
#kibana.defaultAppId: "home"

# If your Elasticsearch is protected with basic authentication, these settings provide
# the username and password that the Kibana server uses to perform maintenance on the Kibana
# index at startup. Your Kibana users still need to authenticate with Elasticsearch, which
# is proxied through the Kibana server.
elasticsearch.username: "elastic"
elasticsearch.password: "kamyon"
```

Tanımladıktan sonra artık kibana üzerinde tam yetkiye sahip olmuş olduk ve MySQL eklentisini tanımlayabiliriz.

6. Filebeat kurulumu ve MySQL konfigürasyonu

MySQL tarafında kaydedilen logları, Filebeat aracılığıyla ElasticSearch sunucusuna yerleştirmemiz gerekmekte. Gerekli ayarlardan önce Filebeat kurulumuna bakalım.

```
wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -
sudo apt-get install apt-transport-https
echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee -a /etc/apt/sources.list.d/elastic-7.x.list
sudo apt-get update && sudo apt-get install filebeat
sudo update-rc.d filebeat defaults 95 10
```

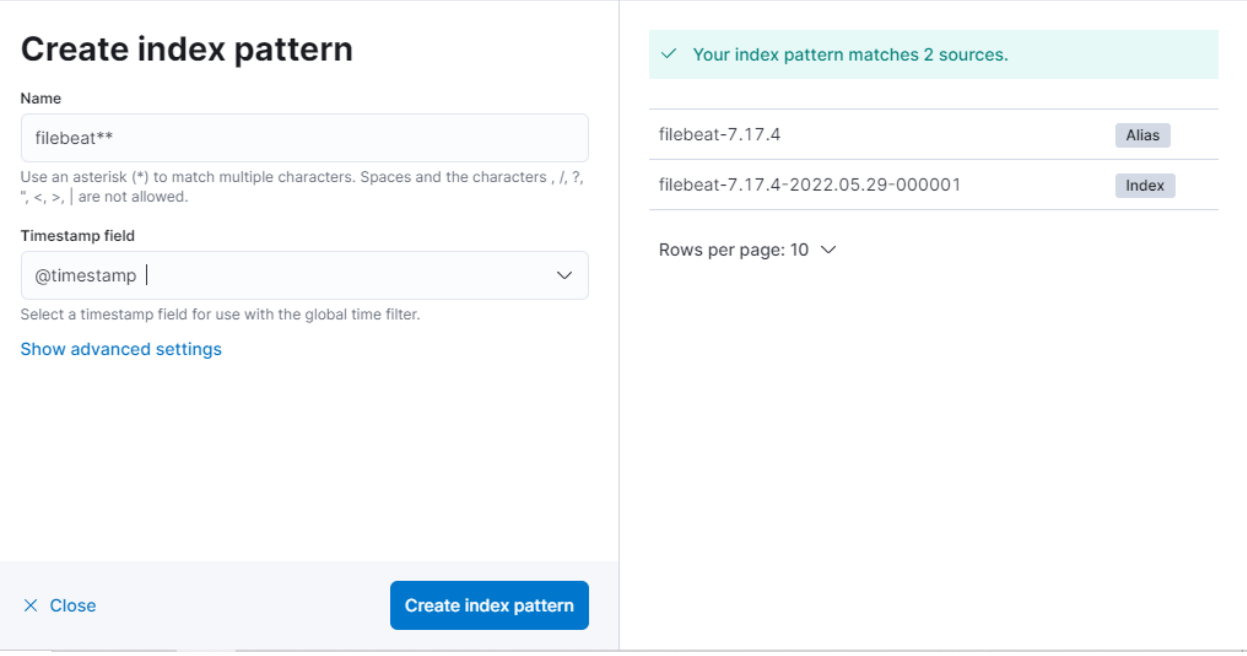
Kurulumun ardından Filebeat için MySQL modülünü aktif hale getirmemiz gerekmekte.

```
filebeat modules enable mysql
filebeat modules list
```

```
berkesun@sysadmin:~$ sudo filebeat modules list
Enabled:
mysql
nginx
system
```

Daha sonra Kibana ayarlarında üzerinden Filebeat bağlantısının onaylandığını görmemiz ve tanımlamamız için bir index-pattern oluşturmamız gerekiyor.

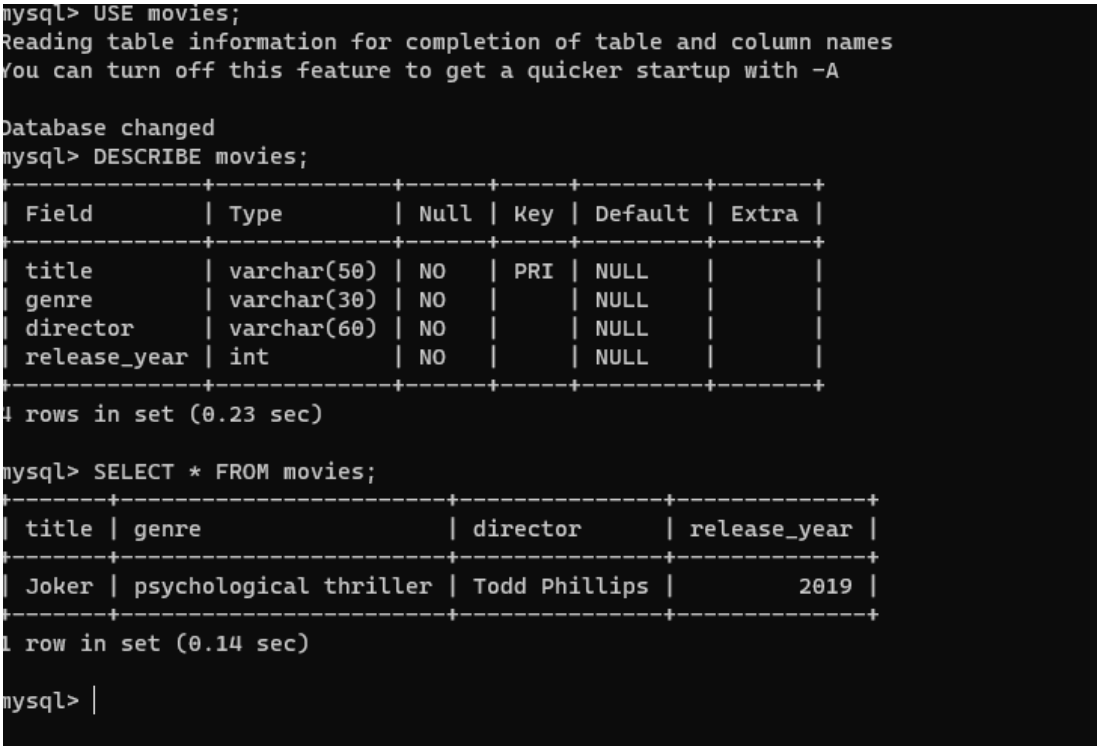
Management → Stack Management → Index Patterns



Ayarlamaları gerçekleştirdikten sırada filebeat.yml dosyasına elasticsearch ve kibana için belirlediğimiz kullanıcı adı ve şifreleri tanımlamamız gerekiyor.

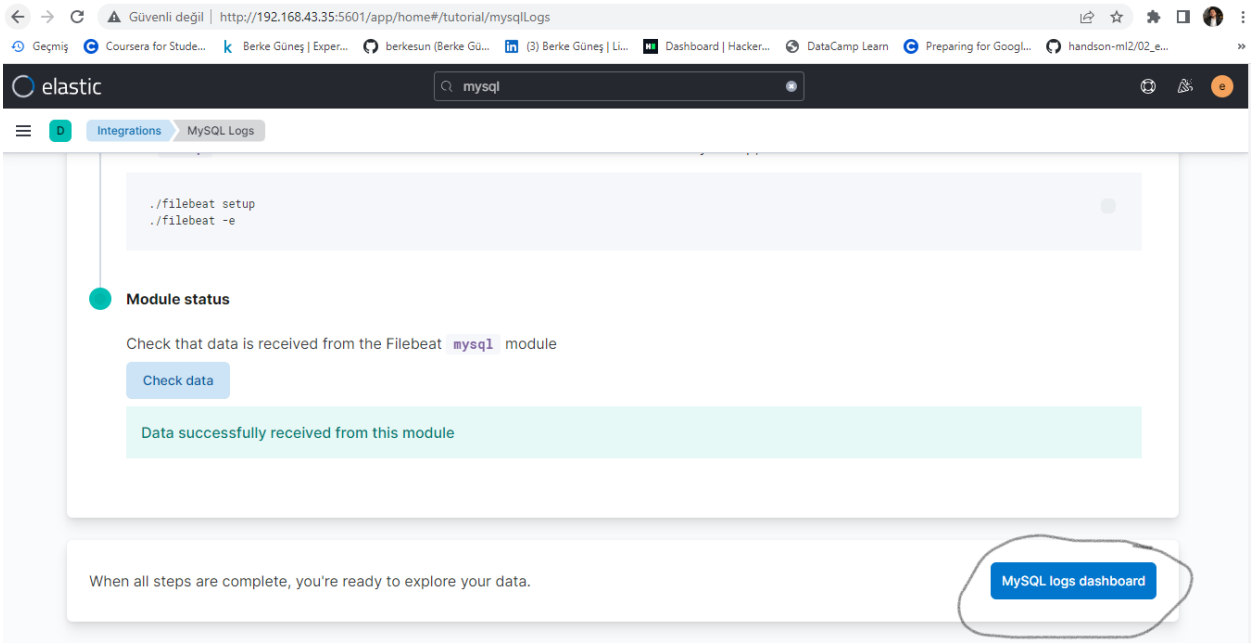
```
  GNU nano 4.8                                                /etc/filebeat/filebeat.yml
  # IPv6 addresses should always be defined as: https://[2001:db8::1]:5601
  host: "192.168.43.35:5601"
  username: "elastic"
  password: "kamyon"

  # Kibana Space ID
  # ID of the Kibana Space into which the dashboards should be loaded. By default,
  # the Default Space will be used.
  #space.id:

# ============================== Elastic Cloud ==============================

# These settings simplify using Filebeat with the Elastic Cloud (https://cloud.elastic.co/).

# The cloud.id setting overwrites the `output.elasticsearch.hosts` and
# `setup.kibana.host` options.
# You can find the `cloud.id` in the Elastic Cloud web UI.
#cloud.id:

# The cloud.auth setting overwrites the `output.elasticsearch.username` and
# `output.elasticsearch.password` settings. The format is `<user>:<pass>`.
#cloud.auth:

# ================================== Outputs ===================================

# Configure what output to use when sending the data collected by the beat.

# ---------------------------- Elasticsearch Output ----------------------------
output.elasticsearch:
  # Array of hosts to connect to.
  hosts: ["localhost:9200"]
```

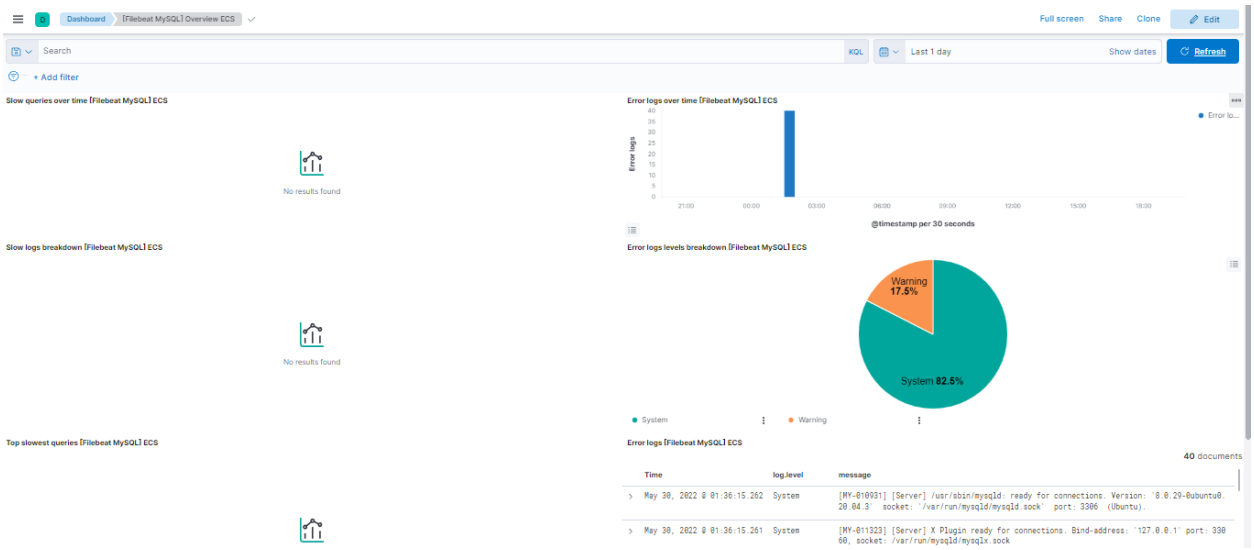
Daha önceden kurmuş olduğumuz ve tanımladığımız MySQL;



Artık filebeat kuruluma ve başlatılmaya hazır.

```
filebeat setup -e
sudo service filebeat start
```





7. KAYNAKÇA

https://stackoverflow.com/

https://www.elastic.co/

https://forum.search-guard.com/