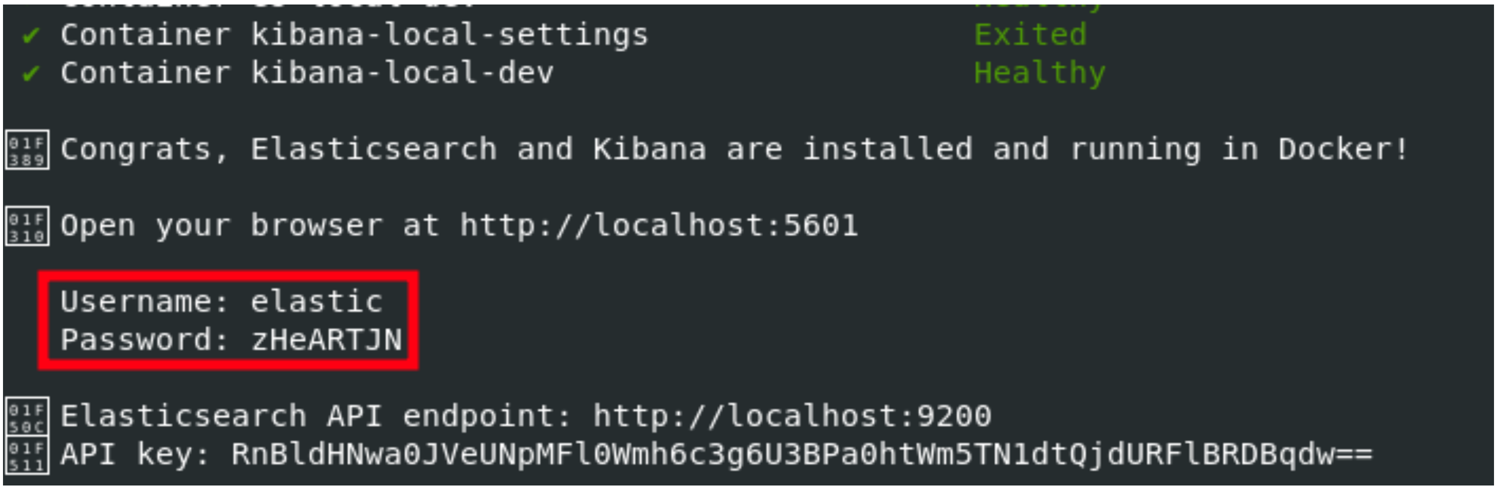
ELK stack for local testing

1. Docker 설치

```
sudo apt update
sudo apt install docker.io docker-compose -y
sudo systemctl enable docker
sudo usermod -aG docker $USER
```

2. elastic search 설치

```
curl -fsSL https://elastic.co/start-local | sh
```



```
✔ Container kibana-local-settings                    Exited
✔ Container kibana-local-dev                         Healthy

🎉 Congrats, Elasticsearch and Kibana are installed and running in Docker!

🌐 Open your browser at http://localhost:5601

   Username: elastic
   Password: zHeARTJN

🔌 Elasticsearch API endpoint: http://localhost:9200
🔑 API key: RnBldHNwa0JVeUNpMFl0Wmh6c3g6U3BPa0htWm5TN1dtQjdURFlBRDBqdw==
```

비밀번호 혹은 API key 메모해두기

3. https://www.elastic.co/downloads/beats/filebeat 에서 deb 파일 다운

4. filebeat 설치

```
sudo dpkg -i <파일 이름.deb>
```

5. system 모듈 활성화

```
sudo filebeat modules enable system
sudo nano /etc/filebeat/modules.d/system.yml
```

6. system.yml 수정

```
- module: system
  syslog:
    enabled: true
    var.paths: ["/var/log/syslog"]
  auth:
    enabled: true
    var.paths: ["/var/log/auth.log"]
```

7. filebeat.yml 수정

```
filebeat.inputs:

# Each - is an input. Most options can be set at the input level, so
# you can use different inputs for various configurations.
# Below are the input-specific configurations.

# filestream is an input for collecting log messages from files.
- type: filestream

  # Unique ID among all inputs, an ID is required.
  id: my-filestream-id

  # Change to true to enable this input configuration.
  enabled: true

  # Paths that should be crawled and fetched. Glob based paths.
  paths:
    - /var/log/*.log
    - /var/log/syslog
```

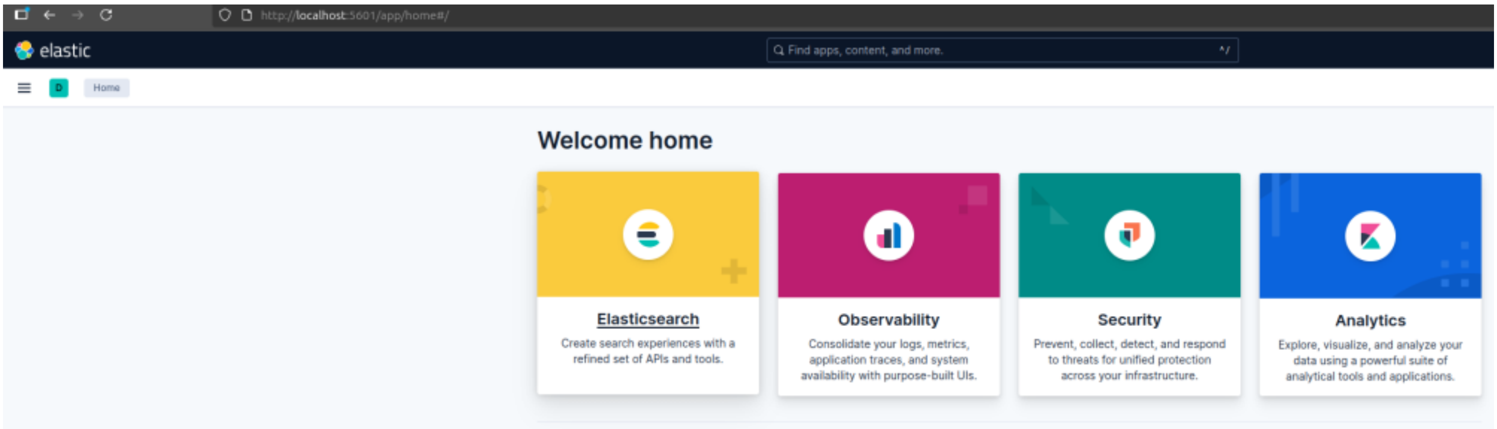
```
# ---------------------------- Elasticsearch Output
----------------------------
output.elasticsearch:
  # Array of hosts to connect to.
  hosts: ["localhost:9200"]

  # Performance preset - one of "balanced", "throughput", "scale",
  # "latency", or "custom".
  preset: balanced

  # Protocol - either `http` (default) or `https`.
  #protocol: "https"

  # Authentication credentials - either API key or username/password.
  #api_key: "id:api_key"
  username: "elastic"
  password: "zHeARTJN"
```

로그 위치 설정, 비밀번호 설정

8. filebeat 실행

```
sudo filebeat setup
sudo systemctl enable filebeat
sudo systemctl start filebeat
```

9. http://localhost:5601 을 가면 실행을 확인할 수 있다



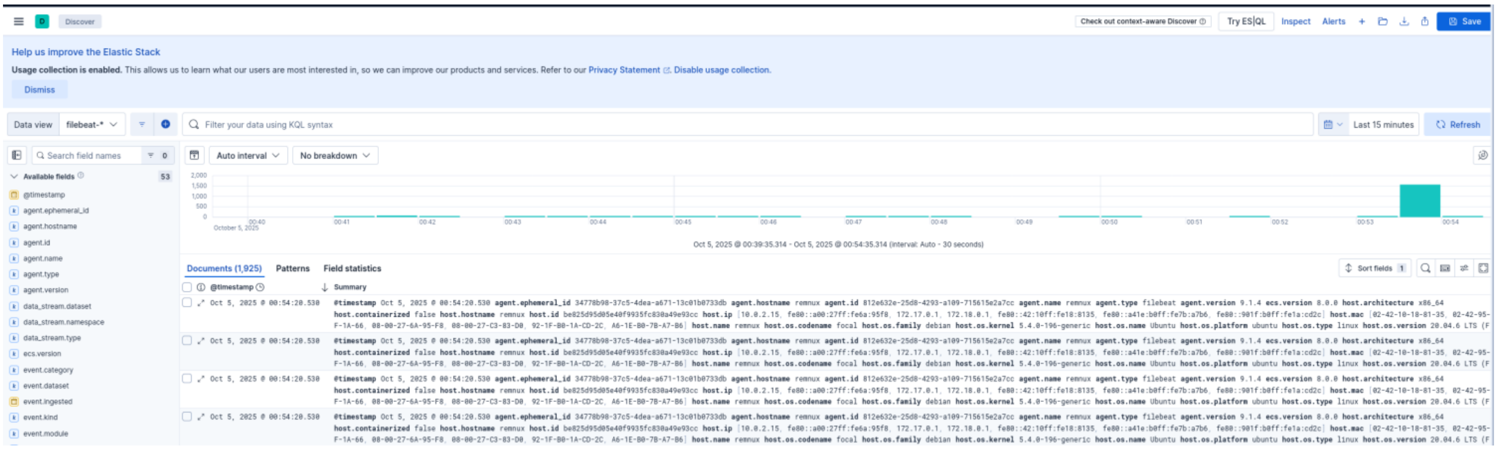
Create search experiences with a refined set of APIs and tools.

Consolidate your logs, metrics, application traces, and system availability with purpose-built UIs.

Prevent, collect, detect, and respond to threats for unified protection across your infrastructure.

Explore, visualize, and analyze your data using a powerful suite of analytical tools and applications.

10. discover에서 로그가 보이면 설치 완료



Help us improve the Elastic Stack

Usage collection is enabled. This allows us to learn what our users are most interested in, so we can improve our products and services. Refer to our Privacy Statement. Disable usage collection.

Data view filebeat-*

Last 15 minutes

Auto interval

Oct 5, 2025 @ 00:39:35.314 - Oct 5, 2025 @ 00:54:35.314 (interval: Auto - 30 seconds)

```
Oct 5, 2025 @ 00:54:20.530   @timestamp Oct 5, 2025 @ 00:54:20.530 agent.ephemeral_id 34778b98-37c5-4dea-a671-13c01b0733db agent.hostname remnux agent.id 812e632e-25d8-4293-a109-715615e2a7cc agent.name remnux agent.type filebeat agent.version 9.1.4 ecs.version 8.0.0 host.architecture x86_64
                             host.containerized false host.hostname remnux host.id be825d95d05e40f9935fc830a49e93cc host.ip [10.0.2.15, fe80::a00:27ff:fe6a:95f8, 172.17.0.1, 172.18.0.1, fe80::42:10ff:fe18:8135, fe80::a41e:b0ff:fe7b:a7b6, fe80::901f:b0ff:fe1a:cd2c] host.mac [02-42-10-18-81-35, 02-42-95-
                             F-1A-66, 08-00-27-6A-95-F8, 08-00-27-C3-83-D0, 92-1F-B0-1A-CD-2C, A6-1E-B0-7B-A7-B6] host.name remnux host.os.codename focal host.os.family debian host.os.kernel 5.4.0-196-generic host.os.name Ubuntu host.os.platform ubuntu host.os.type linux host.os.version 20.04.6 LTS (F
Oct 5, 2025 @ 00:54:20.530   @timestamp Oct 5, 2025 @ 00:54:20.530 agent.ephemeral_id 34778b98-37c5-4dea-a671-13c01b0733db agent.hostname remnux agent.id 812e632e-25d8-4293-a109-715615e2a7cc agent.name remnux agent.type filebeat agent.version 9.1.4 ecs.version 8.0.0 host.architecture x86_64
                             host.containerized false host.hostname remnux host.id be825d95d05e40f9935fc830a49e93cc host.ip [10.0.2.15, fe80::a00:27ff:fe6a:95f8, 172.17.0.1, 172.18.0.1, fe80::42:10ff:fe18:8135, fe80::a41e:b0ff:fe7b:a7b6, fe80::901f:b0ff:fe1a:cd2c] host.mac [02-42-10-18-81-35, 02-42-95-
                             F-1A-66, 08-00-27-6A-95-F8, 08-00-27-C3-83-D0, 92-1F-B0-1A-CD-2C, A6-1E-B0-7B-A7-B6] host.name remnux host.os.codename focal host.os.family debian host.os.kernel 5.4.0-196-generic host.os.name Ubuntu host.os.platform ubuntu host.os.type linux host.os.version 20.04.6 LTS (F
Oct 5, 2025 @ 00:54:20.530   @timestamp Oct 5, 2025 @ 00:54:20.530 agent.ephemeral_id 34778b98-37c5-4dea-a671-13c01b0733db agent.hostname remnux agent.id 812e632e-25d8-4293-a109-715615e2a7cc agent.name remnux agent.type filebeat agent.version 9.1.4 ecs.version 8.0.0 host.architecture x86_64
                             host.containerized false host.hostname remnux host.id be825d95d05e40f9935fc830a49e93cc host.ip [10.0.2.15, fe80::a00:27ff:fe6a:95f8, 172.17.0.1, 172.18.0.1, fe80::42:10ff:fe18:8135, fe80::a41e:b0ff:fe7b:a7b6, fe80::901f:b0ff:fe1a:cd2c] host.mac [02-42-10-18-81-35, 02-42-95-
                             F-1A-66, 08-00-27-6A-95-F8, 08-00-27-C3-83-D0, 92-1F-B0-1A-CD-2C, A6-1E-B0-7B-A7-B6] host.name remnux host.os.codename focal host.os.family debian host.os.kernel 5.4.0-196-generic host.os.name Ubuntu host.os.platform ubuntu host.os.type linux host.os.version 20.04.6 LTS (F
Oct 5, 2025 @ 00:54:20.530   @timestamp Oct 5, 2025 @ 00:54:20.530 agent.ephemeral_id 34778b98-37c5-4dea-a671-13c01b0733db agent.hostname remnux agent.id 812e632e-25d8-4293-a109-715615e2a7cc agent.name remnux agent.type filebeat agent.version 9.1.4 ecs.version 8.0.0 host.architecture x86_64
                             host.containerized false host.hostname remnux host.id be825d95d05e40f9935fc830a49e93cc host.ip [10.0.2.15, fe80::a00:27ff:fe6a:95f8, 172.17.0.1, 172.18.0.1, fe80::42:10ff:fe18:8135, fe80::a41e:b0ff:fe7b:a7b6, fe80::901f:b0ff:fe1a:cd2c] host.mac [02-42-10-18-81-35, 02-42-95-
                             F-1A-66, 08-00-27-6A-95-F8, 08-00-27-C3-83-D0, 92-1F-B0-1A-CD-2C, A6-1E-B0-7B-A7-B6] host.name remnux host.os.codename focal host.os.family debian host.os.kernel 5.4.0-196-generic host.os.name Ubuntu host.os.platform ubuntu host.os.type linux host.os.version 20.04.6 LTS (F
```