

# Elastic 로깅 워크샵 실습

## 목차

- 1장: Elastic 클러스터 생성
- 2장: Metricbeat 실습
- 3장: Filebeat 실습
- 4장: Alerting 실습
- 5장: Machine Learning 실습

Elastic 로깅 워크샵  
2020.04.17(목)

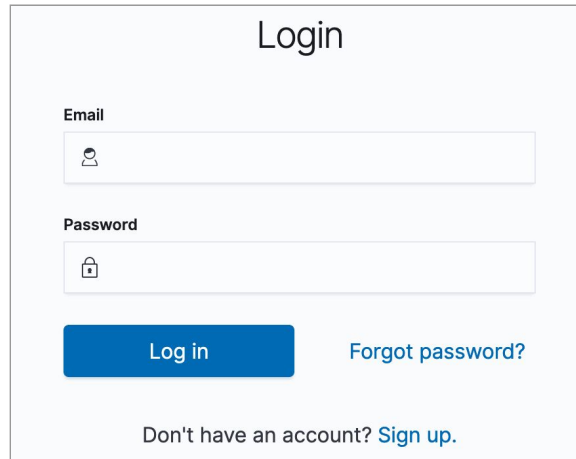
설문: <https://ela.st/loggingkr>  
문의: [kr-mktg@elastic.co](mailto:kr-mktg@elastic.co)

# 1장: Elastic 클러스터 생성

실습 시간: 20분

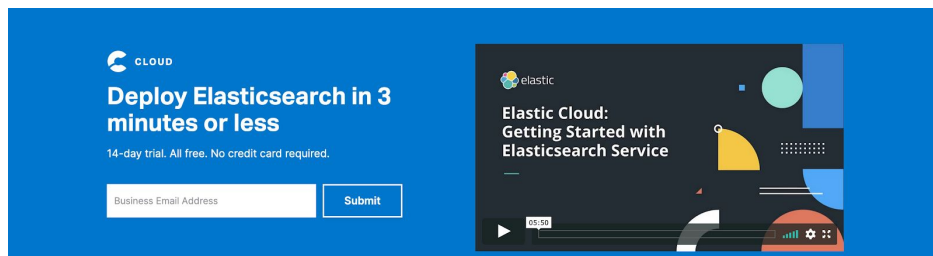
## 1. Elastic Cloud 계정 생성

1. [cloud.elastic.co](https://cloud.elastic.co) 에 접속 후 “Sign up” 링크를 클릭한다.

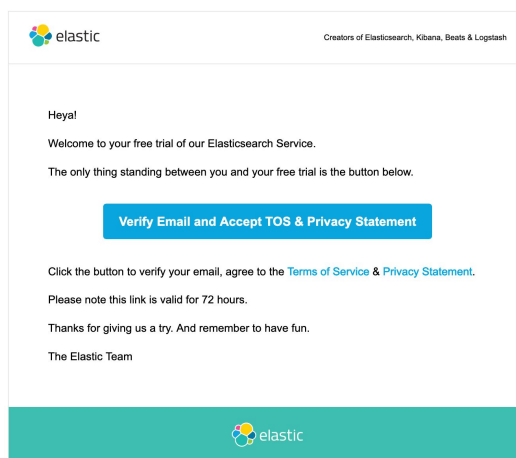


The image shows the Elastic Cloud login page. It has a title "Login" at the top. Below it are two input fields: "Email" with a person icon and "Password" with a lock icon. There is a blue "Log in" button and a link "Forgot password?". At the bottom, it says "Don't have an account? [Sign up.](#)"

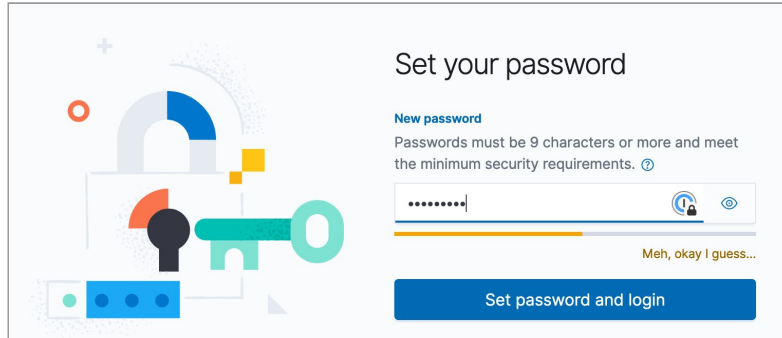
2. 자신의 **회사** 이메일 주소를 입력하고 “Submit” 버튼을 클릭한다. (신용카드 정보 불필요)



3. 메일을 확인한다. “Please verify your email address” 제목의 메일을 받았으면 이메일 검증 진행 버튼을 클릭한다. 미수신시 스팸함도 확인한다.

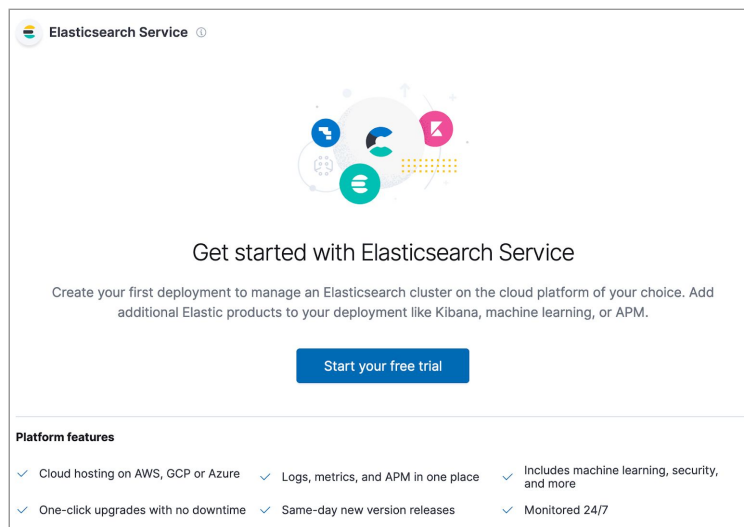


4. 강력한 Elastic Cloud 계정 비밀번호 지정 후 로그인, 팝업 화면에서는 Next > Next > Next > Go to Elastic Cloud



The screenshot shows the 'Set your password' screen in the Elastic Cloud console. On the left, there is a graphic of a key and a lock. On the right, the text 'Set your password' is displayed. Below it, a 'New password' section states: 'Passwords must be 9 characters or more and meet the minimum security requirements. ?'. A password input field shows a masked password '.....'. To the right of the input field are icons for a lock and an eye. Below the input field, a feedback message says 'Meh, okay I guess...'. At the bottom, there is a blue button labeled 'Set password and login'.

5. Elastic Cloud 대시보드에 “Start your free trial” 버튼을 클릭한다.



The screenshot shows the 'Elasticsearch Service' dashboard. At the top, it says 'Elasticsearch Service'. Below that is a graphic with several icons. The main heading is 'Get started with Elasticsearch Service'. Below this, it says: 'Create your first deployment to manage an Elasticsearch cluster on the cloud platform of your choice. Add additional Elastic products to your deployment like Kibana, machine learning, or APM.' At the bottom, there is a blue button labeled 'Start your free trial'. Below the button, there is a section titled 'Platform features' with a list of features: 'Cloud hosting on AWS, GCP or Azure', 'Logs, metrics, and APM in one place', 'Includes machine learning, security, and more', 'One-click upgrades with no downtime', 'Same-day new version releases', and 'Monitored 24/7'.

## 2. Elasticsearch Service(ESS) 생성

1. Name your deployment에 “mlworkshop”을 입력한다.
  - elastic\_workshop

Deployments / Create

### Create deployment

#### 1 Name your deployment

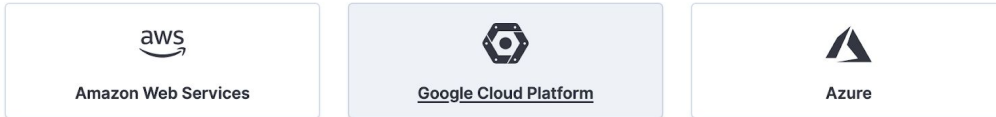
Give your deployment a name

elastic\_workshop

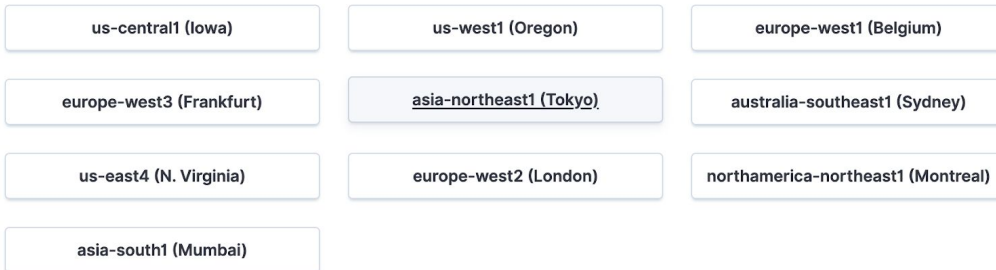
2. 선호하는 클라우드 서비스 제공사(CSP) 선택. 각 CSP를 눌러 어떤 리전이 있는지도 확인한다.

## 2 Select a cloud platform

Pick your cloud and let us handle the rest. No additional accounts required.



## 3 Select a region



3. 가장 최신 Elastic Stack을 선택한다. (7.6.2)

## 4 Set up your deployment

Elastic Stack version

7.6.2 [Edit](#)

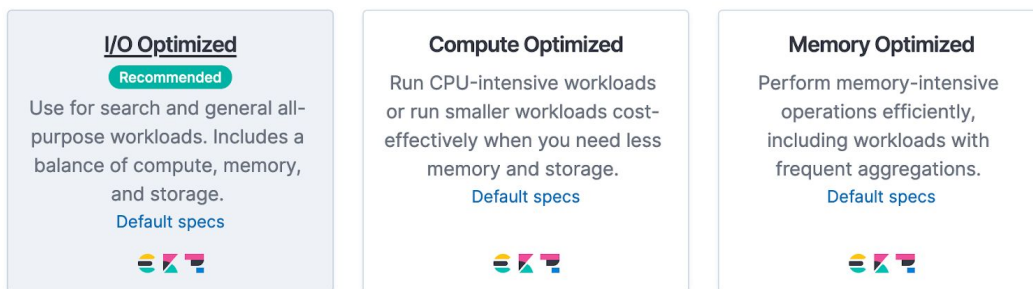
☐ Select a deployment to restore from one of its snapshots

Monitoring

☐ Enable monitoring by shipping metrics to a deployment

4. “I/O optimized” 템플릿을 선택한다.

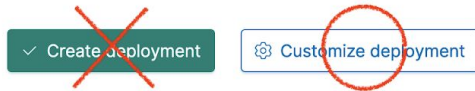
## 5 Optimize your deployment



5. **중요!** 마지막 단계에서 반드시 “Customize deployment” 버튼을 클릭한다.

## ✓ Deployment pricing

Free! As part of your 14-day trial, you can try it out without a credit card. If you want to unleash the full power of Elasticsearch Service now, you can enter your credit card details or contact [sales@elastic.co](mailto:sales@elastic.co).

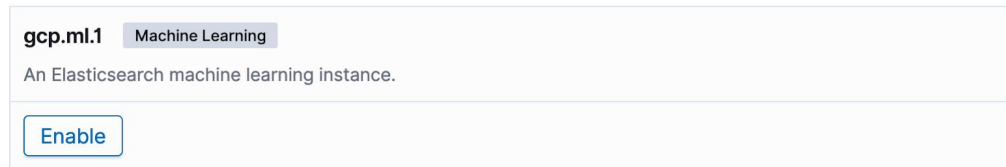


6. “Machine Learning” 섹션에서 “Enable” 버튼을 눌러 ML 노드를 활성화한다.

## Machine Learning 1 configuration

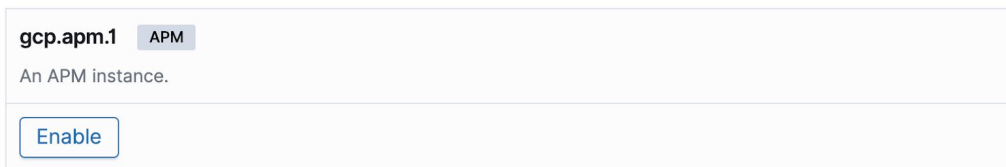
Automatically model the behavior of your Elasticsearch data — trends, periodicity, and more.

[Learn more](#)



7. “APM” 섹션은 Disable 한다.

## APM 1 configuration



8. 우측에 Elastic Cluster 아키텍처를 확인한다.

## Architecture

### Zone 1



### Zone 2



-  **aws.data.highio.i3** (data)  
4 GB RAM x 2, 120 GB storage x 2
-  **aws.kibana.r4** (kibana)  
1 GB RAM x 1
-  **aws.ml.m5** (ml)  
1 GB RAM x 1

9. Elastic Cluster 생성에는 약 3~6분이 소요된다.

mlworkshop  
Activity

✓ Your deployment has been created.  
Now that it's ready, view [your deployment](#).

**Save your Elasticsearch and Kibana password**

These credentials provide superuser access to Elasticsearch and Kibana in this deployment. The password won't be shown again.

Username  
elastic

Password  
j6yi00FrQfeuojrjjSEF4pZQ [COPY](#) [DOWNLOAD](#)

**Change history**  
Here's what's happening under the hood.

Q e.g.: healthy\_configuration: y apm

Successful Unsuccessful Pending Finished System Source ▾

All 2 Elasticsearch 1 Kibana 1 APM

Change	Summary	Actions
⌚ Applied a few seconds ago, took 3 minutes		

10. **중요!!!** Cluster 생성 완료 후 반드시 “Username”과 “Password” 복사하여 메모장 등에 기록.

**Username**  
elastic

**Password**  
j6yi00FrQfeuojrjjSEF4pZQ [COPY](#) [DOWNLOAD](#)

11. 좌측 메뉴에서 “elastic\_workshop”을 클릭하고 아래 정보들을 확인한다.

- Deployment version / Deployment status
- Cloud ID

Kibana 아래 Launch 링크를 클릭하여 Kibana에 접속한다.

Elastic Cloud / Elasticsearch Service

**Deployments**

[elastic\\_workshop](#)

- Edit
- Elasticsearch
  - Logs
  - Snapshots
  - API console
- Kibana
- APM
- Activity
- Security
- Metrics

**Custom plugins**

**Account**

**Help**

Deployments / c5460e3


## elastic\_workshop


**Deployment name**  
elastic\_workshop [Edit](#)

**Deployment status**  
● Healthy

**Deployment version**  
v7.6.2

**Applications**

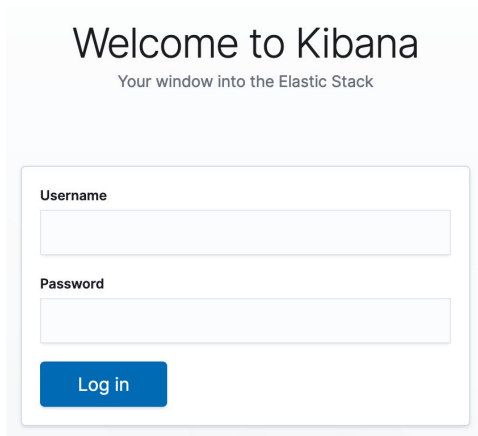
 Elasticsearch [?](#)  
[Launch](#) | [Copy Endpoint URL](#)

 Kibana [?](#)  
[Launch](#) | [Copy Endpoint URL](#)

**Cloud ID** [?](#)

```
elastic_workshop:YXNpYS1ub3J0aGVhc3QxLmdjcC5jbG91ZC51cy5pbyQ3NTU5Y2I2MmJkNWE0MDY1Yjk4MzB1M2E0YmE2YTl2NyQ4Yjh1OWY3ZjQxMDc0NGY2OTI1OGY3MGE0ZTU3YzYxZQ==
```

12. Kibana 로그인 창이 뜨면 앞에서 기록했던 Username과 Password를 이용하여 로그인 한다.



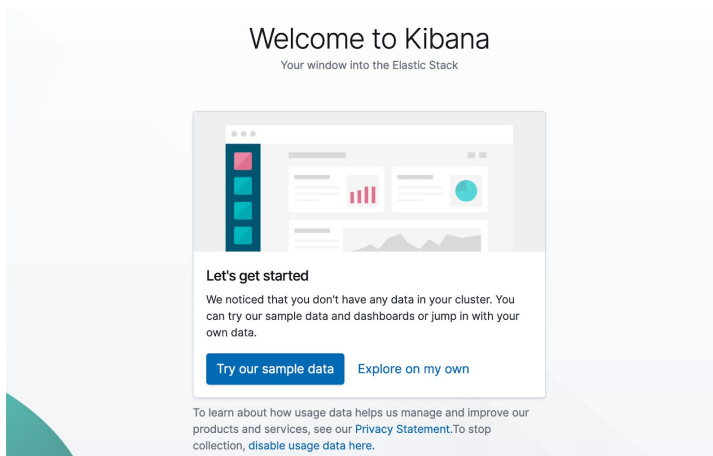
Welcome to Kibana  
Your window into the Elastic Stack

Username

Password

Log in

13. “Try our sample data”를 누르면 자동으로 샘플 인덱스를 생성하고 데이터를 추가해준다.



14. 끝.

## 2장: Metricbeat 실습

이번 장에서는 Metricbeat를 설치하고 “system” 메트릭을 직접 수집합니다.

1. Metricbeat [내려받기](#)

2. Metricbeat 설치

```
$ cd /opt
$ sudo tar xzf metricbeat-7.6.2-darwin-x86_64.tar.gz
$ sudo chown -R <user>:<group> metricbeat-7.6.2-darwin-x86_64.tar.gz
```

3. metricbeat.yml 파일을 수정하여 자신의 Elastic 클러스터 인스턴스를 바라보도록 지정

```
$ sudo vi /opt/metricbeat-7.6.2-darwin-x86_64/metricbeat.yml
```

“Elastic Cloud” 섹션을 찾아 81번째 줄 “cloud.id”의 주석을 제거하고 그 아래 85번째 줄 “cloud.auth”의 주석도 제거한다.

자신의 Cloud ID와 사용자 ID와 비밀번호를 입력한다.

```
#===== Elastic Cloud

# You can find the `cloud.id` in the Elastic Cloud web UI.
cloud.id: your_cloud_id

# The format is `<user>:<pass>`.
cloud.auth: elastic:your_cluster_password
```

4. 인덱스 템플릿과 데시보드 적재

```
$ ./metricbeat setup
```

아래와 같은 결과가 나올 때 까지 잠시 기다린다. (약 20초)

```
Index setup finished.
Loading dashboards (Kibana must be running and reachable)
Loaded dashboards
```

5. 부팅시 metricbeat가 자동으로 시작할 수 있도록 설정한다.

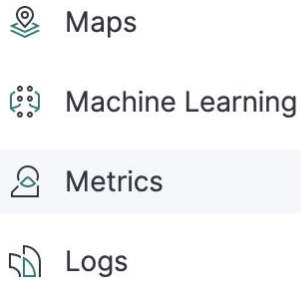
```
$ sudo systemctl enable metricbeat
```

6. metricbeat를 시작한다.

```
$ sudo service metricbeat run
```



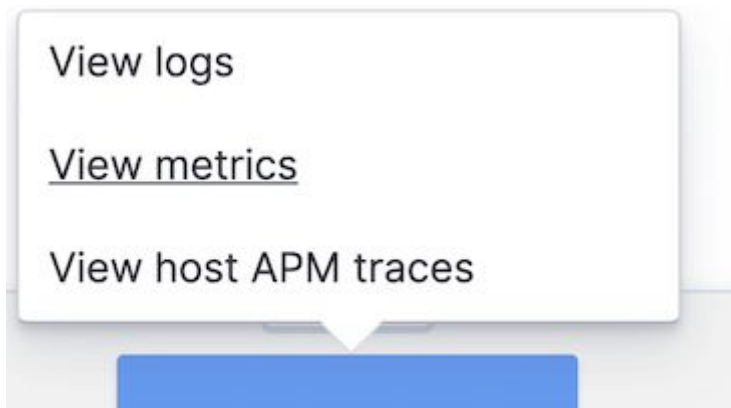
6. 키바나 인스턴스로 가서 좌측 앱 메뉴에서 “Metrics” 메뉴를 선택한다.



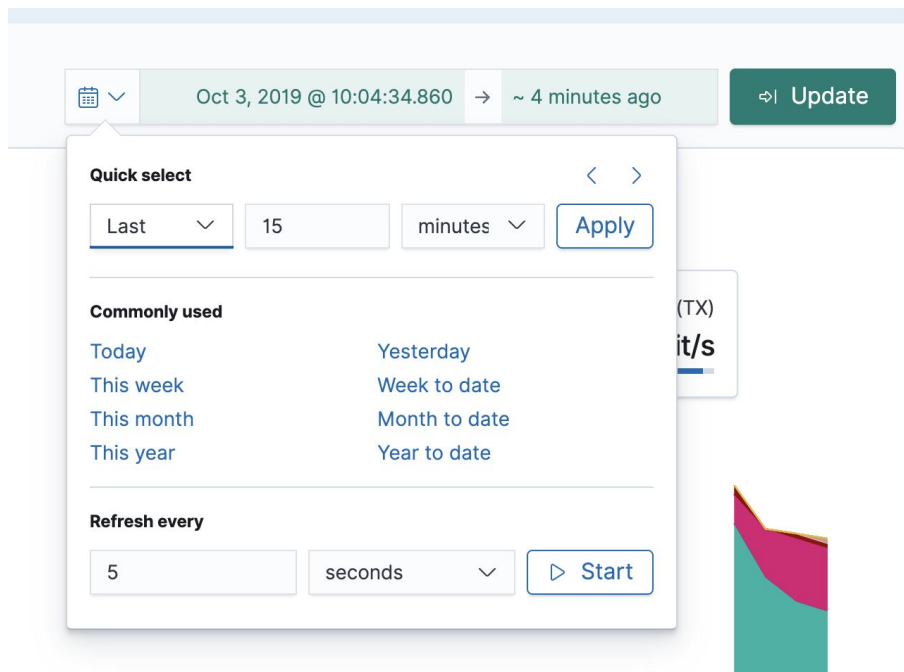
아래와 같이 자신의 호스트 상태를 볼 수 있다.



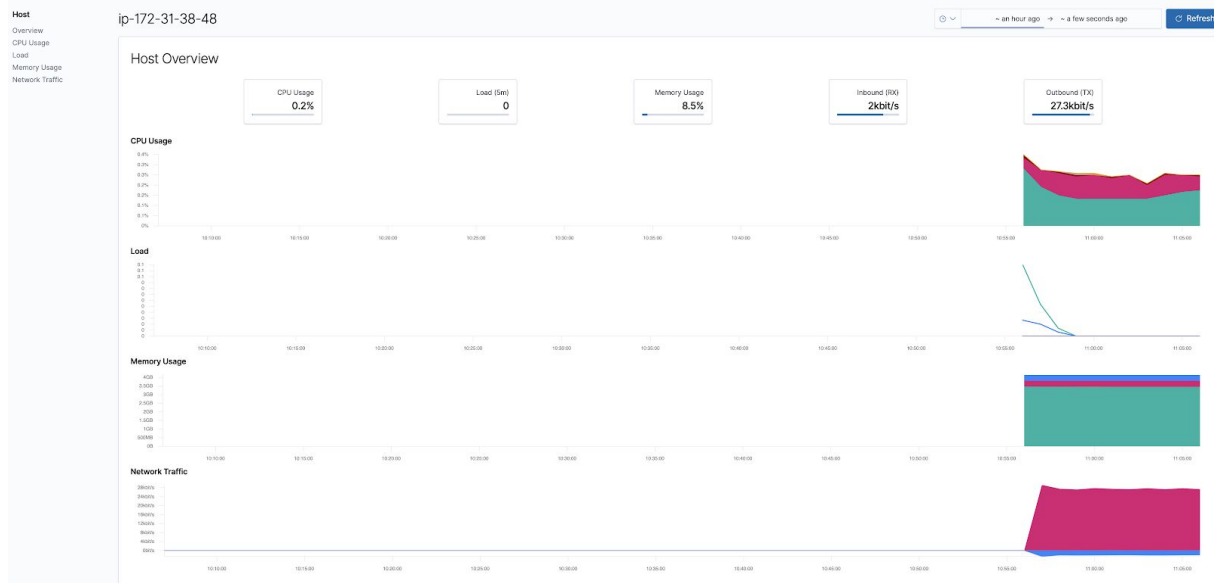
7. 호스트를 클릭하고 “View metrics”를 클릭한다.



8. 시간 선택기를 눌러 5초마다 갱신되도록 설정한 후 Start 버튼을 클릭한다.



9. 아래와 같이 메트릭이 변화하는 것을 볼 수 있다.



10. 끝.

## 3장: Filebeat 실습

이번 장에서는 Filebeat를 설치하고 /var/log/\*.log 로그 데이터를 수집합니다.

### 1. Filebeat [내려받기](#)

### 2. Filebeat 설치

```
$ cd /opt
$ sudo tar xzf filebeat-7.6.2-darwin-x86_64.tar.gz
$ sudo chown -R <user>:<group> filebeat-7.6.2-darwin-x86_64.tar.gz
```

### 3. filebeat.yml 파일을 수정하여 자신의 Elastic 클러스터 인스턴스를 바라보도록 지정

```
$ sudo vi /opt/filebeat-7.6.2-darwin-x86_64/filebeat.yml
```

“Elastic Cloud” 섹션을 찾아 137번째 줄 “cloud.id”의 주석을 제거하고 그 아래 141번째 줄 “cloud.auth”의 주석도 제거한다.

자신의 Cloud ID와 사용자 ID와 비밀번호를 입력한다.

```
#===== Elastic Cloud

# You can find the `cloud.id` in the Elastic Cloud web UI.
cloud.id: your_cloud_id

# The format is `
```

### 4. Filebeat 모듈 목록 조회. 활성화된 모듈이 아직 없다!

```
$ sudo filebeat modules list
Enabled:

Disabled:
apache
auditd
aws
cef
cisco
coredns
elasticsearch
envoyproxy
googlecloud
haproxy
ibmmq
icinga
```

```
iis
iptables
kafka
kibana
logstash
mongodb
mssql
mysql
nats
netflow
nginx
osquery
panw
postgresql
rabbitmq
redis
santa
suricata
system
traefik
zeek
```

#### 5. “system” 모듈 활성화

```
$ ./filebeat modules enable system
Enabled system
```

다시 모듈 목록을 조회한다.

```
$ ./filebeat modules list
Enabled:
system
```

#### 6. 인덱스 템플릿과 대시보드 적재

```
$ ./filebeat setup
```

아래와 같은 결과가 나올 때 까지 잠시 기다린다. (약 20초)

```
Index setup finished.
Loading dashboards (Kibana must be running and reachable)
Loaded dashboards
Loaded machine learning job configurations
Loaded Ingest pipelines
```

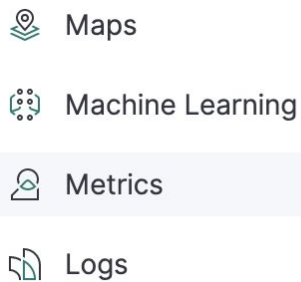
#### 7. 부팅시 metricbeat가 자동으로 시작할 수 있도록 설정한다.

```
$ sudo systemctl enable filebeat
```

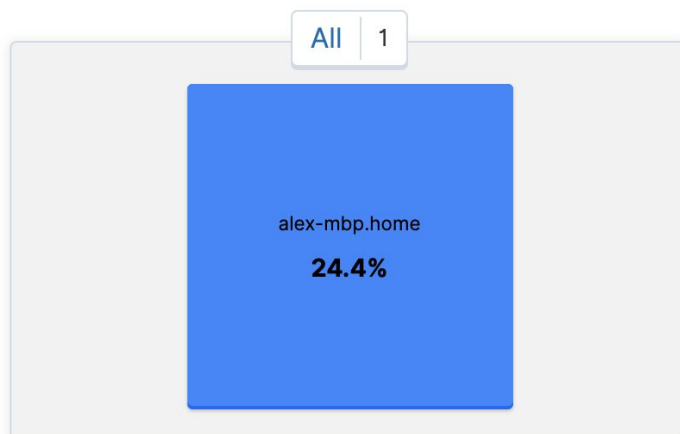
8. filebeat를 시작한다.

```
$ sudo service filebeat run
```

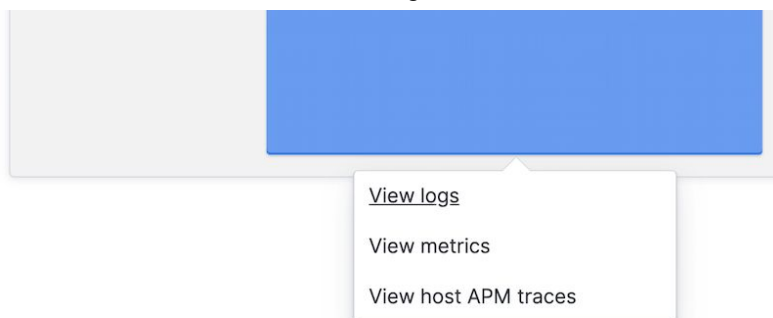
9. 키바나 인스턴스로 가서 좌측 앱 메뉴에서 “Metrics” 메뉴를 선택한다.



아래와 같이 자신의 호스트 상태를 볼 수 있다.



10. 호스트를 클릭하고 “View Logs”를 클릭한다.



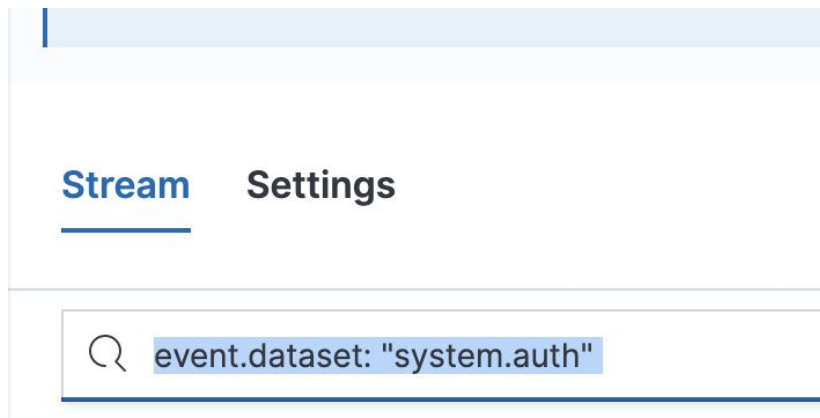
11. “Stream live”를 클릭한다.

 Stream live

로그 데이터가 실시간으로 수집되는 것을 볼 수 있다. 수집된 로그에는 system과 auth 두가지 로그 파일이 있다. 하나씩 볼 수 있도록 필터를 걸어본다.

12. auth 로그만 볼 수 있도록 검색창에 필터 적용

```
event.dataset: "system.auth"
```



13. 터미널로 가서 자신의 공인 IP주소를 확인한다.

```
$ curl https://ipinfo.io/ip
```

14. 확인한 IP로 SSH 접속을 시도하여 auth.log에 기록되도록 한다.

```
$ ssh hAx0R@IP_ADDRESS
...
Are you sure you want to continue connecting (yes/no)? yes
```

15. Kibana로 돌아와서 SSH 로그인 시도 기록을 확인한다.

Oct 3, 2019 @ 11:29:18.000	system.auth	[System][auth][ssh] Invalid user undefined from undefined
Oct 3, 2019 @ 11:29:18.000	system.auth	input_userauth_request: invalid user hAx0R [preauth]
Oct 3, 2019 @ 11:29:18.000	system.auth	Connection closed by 18.184.162.251 port 34040 [preauth]

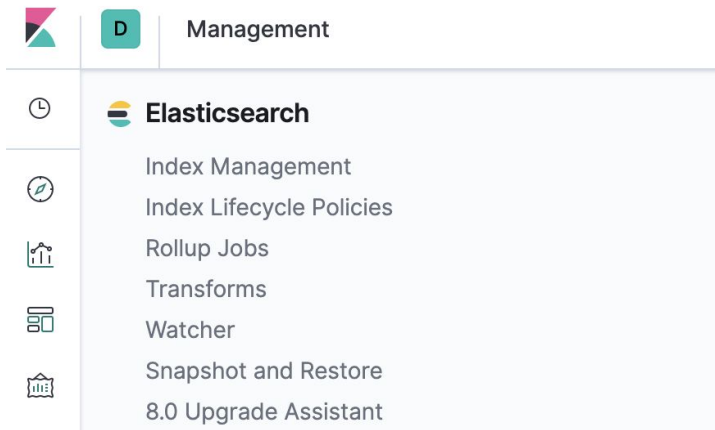
16. 끝.

## 4장: Alerting 실습

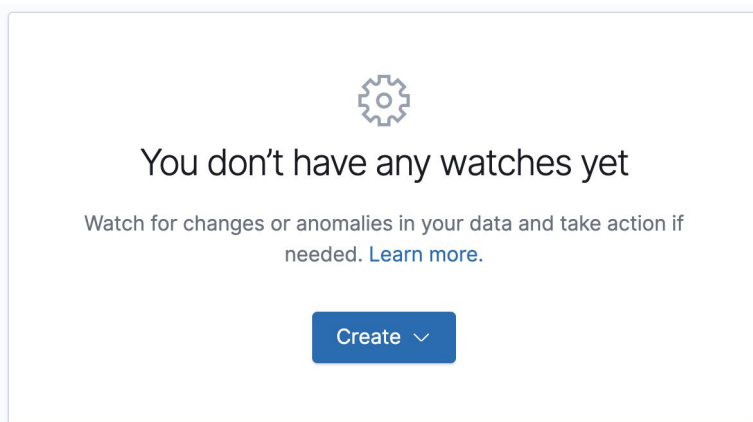
이번장에서는 로그와 메트릭 스트림을 받아 서버에 어떤 문제가 발생했을 때 경고를 발생시키는 과정을 실습한다.

임계치 경고(Threshold Alert)를 생성한다.

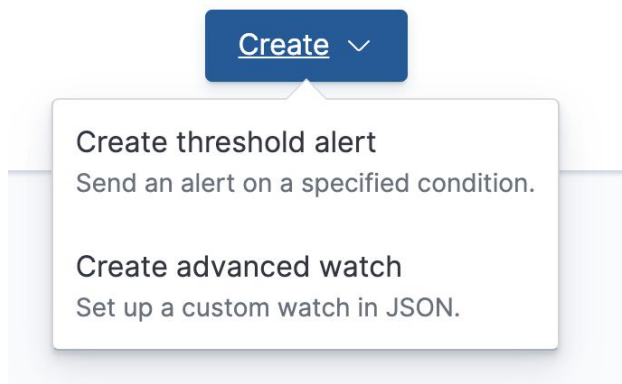
1. Kibana의 앱 메뉴에서 “Management” 앱을 클릭하고 “Watcher” 메뉴로 들어간다.



2. 아래와 같은 화면을 볼 수 있다.

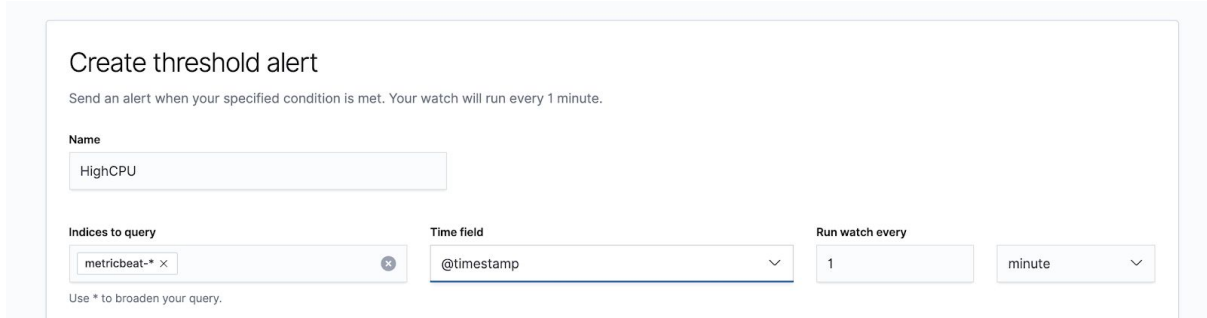


3. “Create” 버튼을 클릭하고 “Create threshold alert” 항목을 선택한다.



4. 아래와 같이 내용을 입력한다.

- HighCPU
- metricbeat-\*
- @timestamp
- 1 minutes



Create threshold alert

Send an alert when your specified condition is met. Your watch will run every 1 minute.

Name  
HighCPU

Indices to query  
metricbeat-\*

Time field  
@timestamp

Run watch every  
1 minute

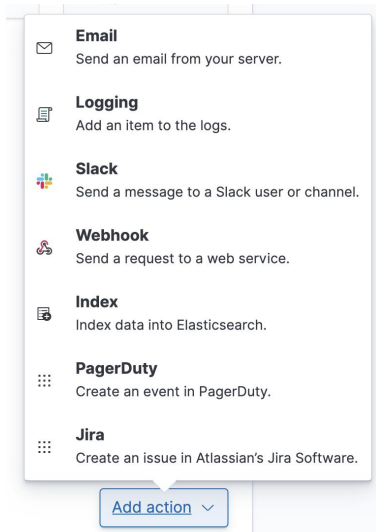
Use \* to broaden your query.

Match the following condition

WHEN average() OF system.cpu.total.pct OVER all documents IS ABOVE 0.8 FOR THE LAST 1 minute



5. “Add Action” 버튼을 누르고 “Email”을 선택한다.



Dropdown menu options:

- Email: Send an email from your server.
- Logging: Add an item to the logs.
- Slack: Send a message to a Slack user or channel.
- Webhook: Send a request to a web service.
- Index: Index data into Elasticsearch.
- PagerDuty: Create an event in PagerDuty.
- Jira: Create an issue in Atlassian's Jira Software.

Add action



6. 자신의 이메일 주소를 입력한 후 “Send test email” 버튼을 클릭하여 검증한다.

✕ Email

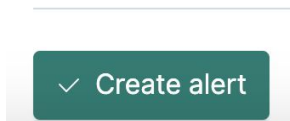
To email address  
YOUR\_EMAIL\_ADDRESS ✕

Subject (optional)  
Watch [{{ctx.metadata.name}}] has exceeded the threshold

Body  
HIGH\_CPU

Send test email

7. 이메일 설정이 완료되었으면 “Create Alert” 버튼을 클릭한다.



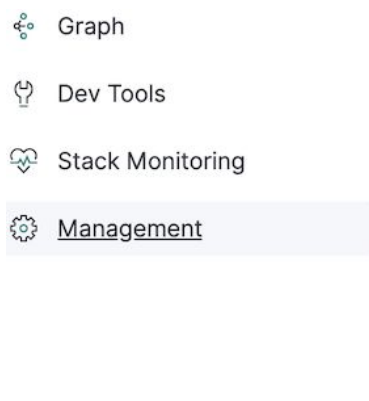
4. 이제는 실제로 부하를 발생시켜 경고를 띄워본다.

5. 리눅스 호스트로 이동하여 아래 명령어를 실행한다.

```
$ dd if=/dev/zero of=/dev/null
```

이 명령어는 리눅스 호스트에 많은 부하를 준다. 2~3분 가량 실행되도록 둔다. 기다리는 동안 CPU 부하가 높다는 경고 이메일을 몇개 받을것이다.

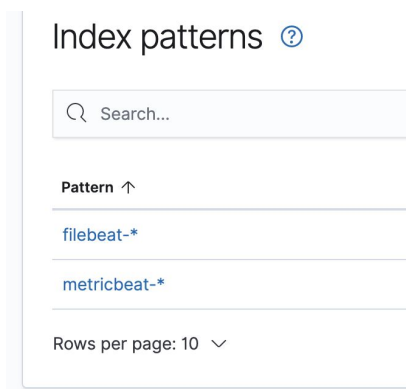
6. 다시 Kibana로 돌아가서 “Management” 앱으로 이동한다.



7. Kibana 색면에서 “Index Patterns” 메뉴를 클릭한다.



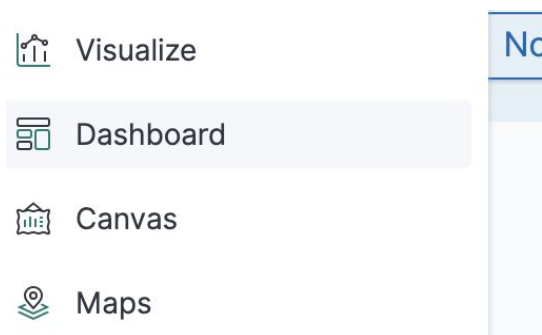
8. “metricbeat-\*” 인덱스 패턴을 선택한다.



9. 별 아이콘을 클릭하여 기본 인덱스 패턴으로 선택한다.



10. Kibana 앱 메뉴에서 “Dashboard” 앱을 클릭한다.



11. 대시보드 목록 상단의 검색창에 “host”를 입력하고 “[Metricbeat System] Host overview ECS”를 클릭한다.

## Dashboards

🔍 host

<input type="checkbox"/> Title	Description
<input type="checkbox"/> [Metricbeat System] Host Services Overview	Overview of services on an individual host.
<input type="checkbox"/> [Metricbeat System] Host overview ECS	Overview of host metrics

12. 시간 선택기에서 갱신 주기를 5초로 맞춘 후 “Start” 버튼을 클릭한다.

📅 Oct 3, 2019 @ 10:04:34.860 → ~ 4 minutes ago ↻ Update

**Quick select**

Last 15 minutes Apply

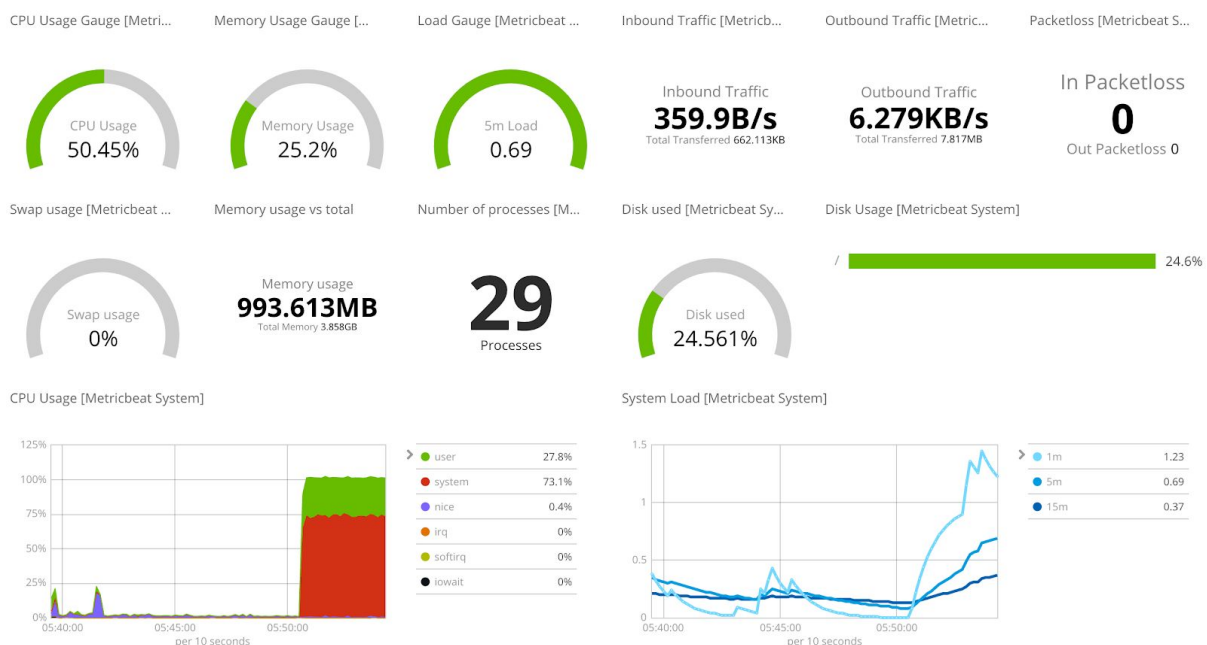
**Commonly used**

Today Yesterday  
This week Week to date  
This month Month to date  
This year Year to date

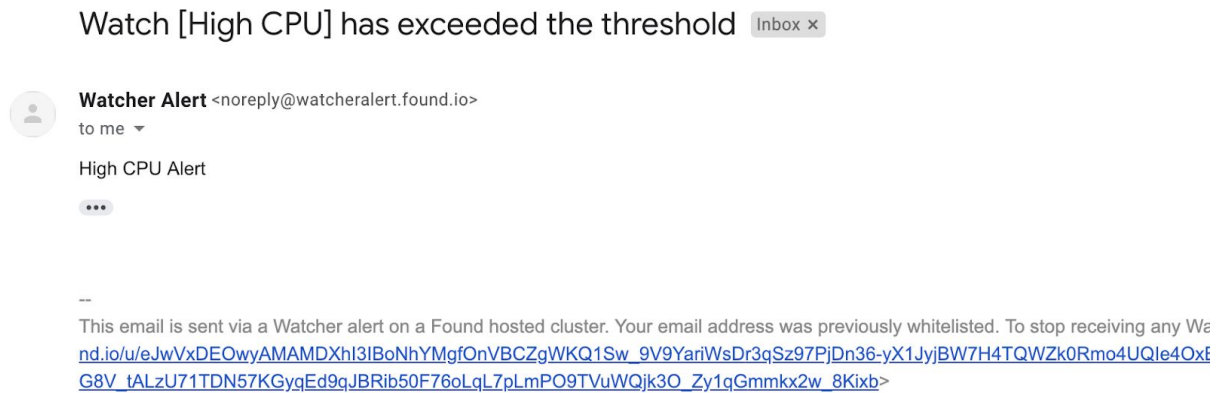
**Refresh every**

5 seconds ▶ Start

13. CPU 부하가 증가했음을 확인한다.



15. 이메일 내용도 확인한다.



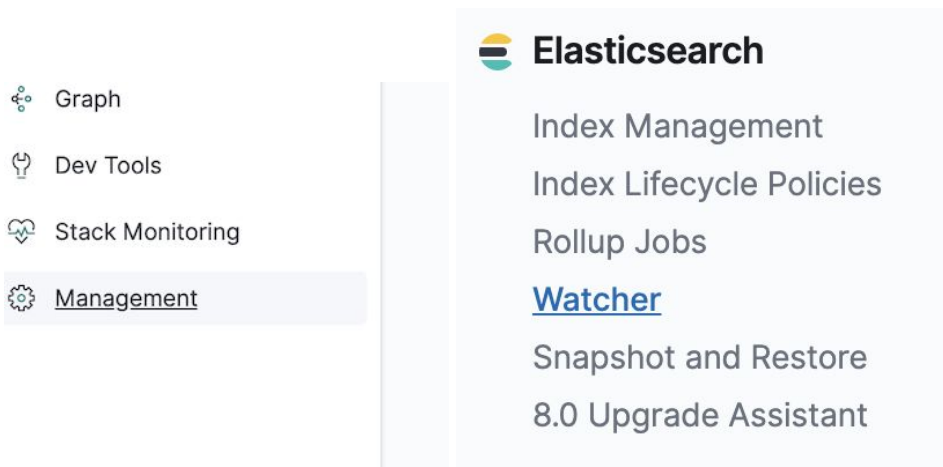
16. 앞서 실행했던 “dd” 명령어를 중지한다. (ctrl-c)

```
$ dd if=/dev/zero of=/dev/null  
^C  
12651700+0 records in  
12651699+0 records out  
6477669888 bytes (6.5 GB, 6.0 GiB) copied, 3.73029 s, 1.7 GB/s
```

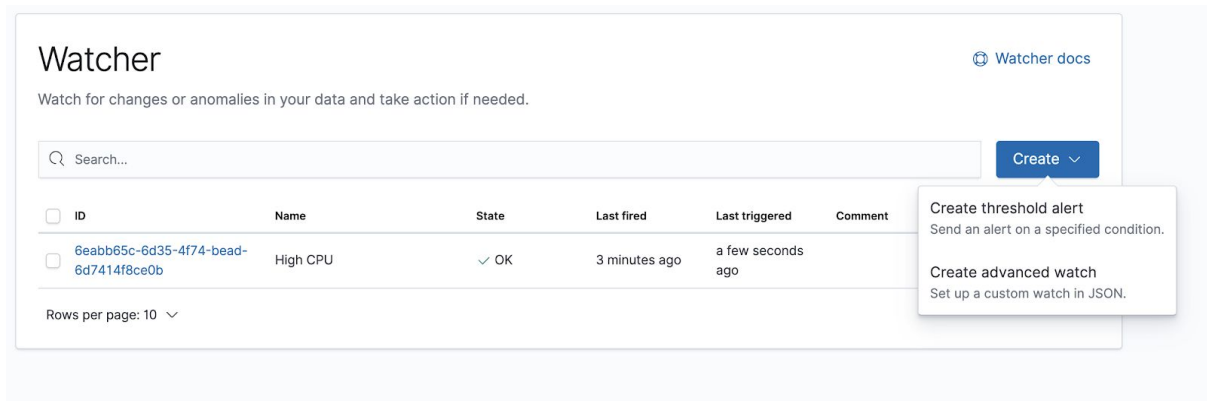
이와 같이 임계치 경고(Threshold Alert)는 디스크 공간 부족, 네트워크 전송량 증가/감소, 업타임 확인 지연 등과 같은 특정 메트릭 정보를 지속적으로 지켜볼 때 효과가 크다.

다음으로, SSH를 이용한 로그인 시도를 탐지하는 경고를 설정해보자.

17. Kibana 앱 메뉴에서 “Management” 앱을 클릭하고 “Watcher” 메뉴로 들어간다.

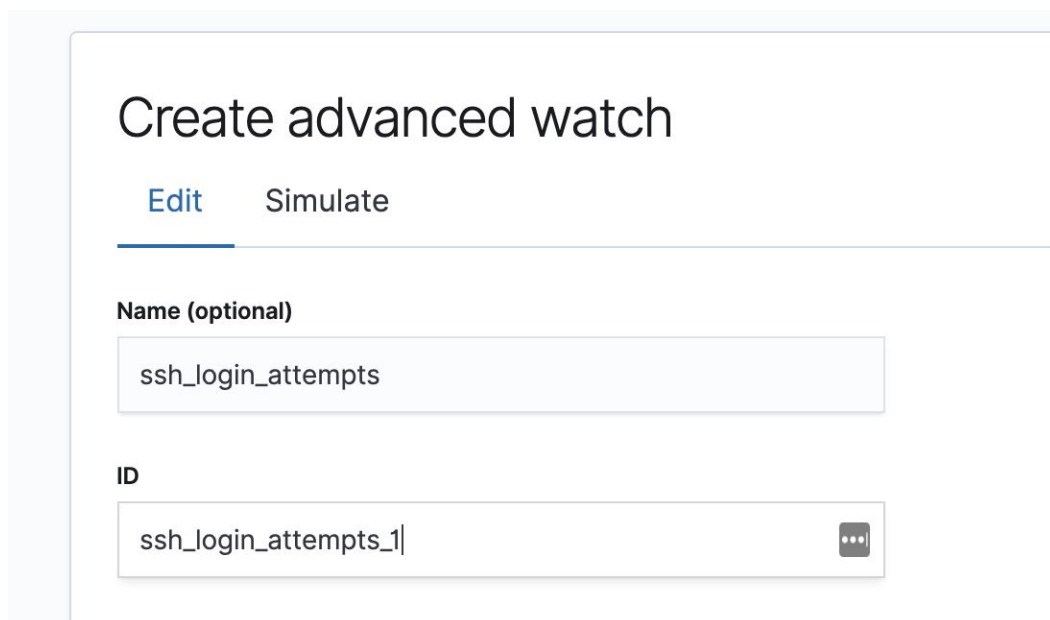


18. “Create” 버튼을 클릭하고 이번에는 Create advanced watch”를 선택한다.



여기서는 SSH 로그인 시도를 찾기 위해 쿼리를 작성할 것이다.

19. 아래와 같이 Name과 ID를 입력한다.



20. 다음 JSON 구문을 “Watch JSON”에 복사하여 붙여넣는다.

Elasticsearch를 통해 쿼리할 수 있는 것은 경고로 만들 수 있다. 따라서 SSH 로그인에 실패한 로그 항목을 찾는 검색 쿼리를 먼저 작성한 후 검색 결과가 중복해서 발생되지 않도록 시간 윈도우를 조정할 것이다. 매 1분마다 실행하도록 설정한 후 발견된 것이 있으면 이메일을 보내도록 설정할 것이다.

JSON 구분을 찬찬히 읽어본다. 4개 영역으로 구성된다:

- Schedule
- Query
- Condition
- Actions

```
{
  "trigger": {
    "schedule": {
      "interval": "1m"
    }
  },
  "input": {
    "search": {
      "request": {
        "search_type": "query_then_fetch",
        "indices": [
          "filebeat-*"
        ],
        "types": [],
        "body": {
          "query": {
            "bool": {
              "must": [
                {
                  "query_string": {
                    "query": "input_userauth_request"
                  }
                },
                {
                  "range": {
                    "@timestamp": {
                      "gte": "now-1m"
                    }
                  }
                }
              ]
            }
          },
          "_source": [
            "message"
          ],
          "sort": [
            {
              "@timestamp": {
                "order": "desc"
              }
            }
          ]
        }
      }
    }
  }
}
```

```
    }
  },
  "condition": {
    "compare": {
      "ctx.payload.hits.total": {
        "gt": 0
      }
    }
  },
  "actions": {
    "send_email": {
      "email": {
        "profile": "standard",
        "to": [
          "YOUR_EMAIL_ADDRESS"
        ],
        "subject": "[Elastic Alert] SSH Login Attempt",
        "body": {
          "text": "{{ctx.payload.hits.total}} SSH login attempts have failed: {{ctx.payload.hits.hits}}[{{_id}}]:{{ctx.payload.hits.hits}}"
        }
      }
    }
  },
  "throttle_period_in_millis": 60000
}
```

21. YOUR\_EMAIL\_ADDRESS 부분에 자신의 이메일을 넣는다.

22. “Create watch” 버튼을 클릭한다.

✓ Create watch Cancel

23. 리눅스 호스트에 SSH 접속을 시도한다.

```
$ curl -s https://ipinfo.io/ip | xargs -Ix ssh foo@x
```

24. 이메일을 확인한다.

## [Elastic Alert] SSH Login Attempt Inbox x



**Watcher Alert** <noreply@watcheralert.found.io>

to me ▾

1 SSH login attempts have failed: {0={\_index=filebeat-6.5.4-2018.12.27, \_type=doc, \_source={message=Dec 27 12:14:27 ip-172-31-25-1: [preauth]], \_id=O-WW72cBjPy1\_ozUd5SJ, sort=[1545912872608], \_score=null}};{0={\_index=filebeat-6.5.4-2018.12.27, \_type=doc, \_source={message=Dec 27 12:14:27 ip-172-31-25-1: sshd[8140]: input\_userauth\_request: invalid user foo [preauth]], \_id=O-WW72cBjPy1\_ozUd5SJ, sort=[1545912872608], \_score=null}}

...

25. 끝.

Watcher를 통한 경고 설정 예제

<https://github.com/elastic/examples/tree/master/Alerting/Sample%20Watches>

Watcher 개요

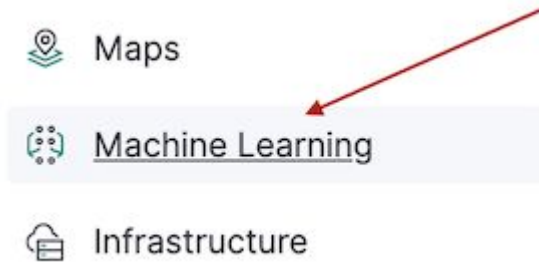
<https://www.elastic.co/guide/en/elastic-stack-overview/6.5/xpack-alerting.html>



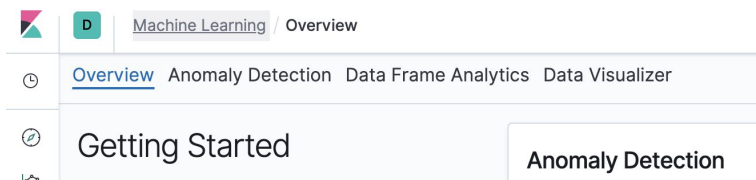
## 5장: Machine Learning 실습

이번장에서는 Machine Learning을 실습한다. Kibana의 “Data Visualizer”를 이용하여 데이터를 특정 인덱스에 넣고 이를 분석한다.

1. Kibana의 앱 메뉴에서 Machine Learning 앱을 선택한다.



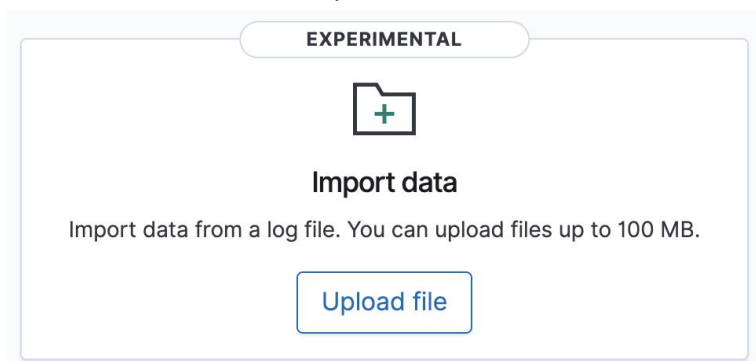
2. “Data Visualizer” 탭을 선택한다.



3. 아래 링크를 클릭하여 “flights.csv” CSV 파일(33MB)을 내려받는다. 이 데이터는 2017년 10월~11월(2개월) 사이의 미국 민항기 운항 정보를 담고 있다.

<https://bit.ly/elastic-data>

4. Data Visualizer에서 “Upload file” 버튼을 클릭한다.

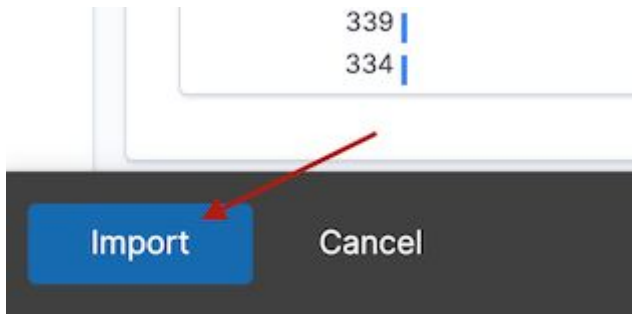


5. 파일 선택기 위로 드래그앤드롭으로 올리면 된다.

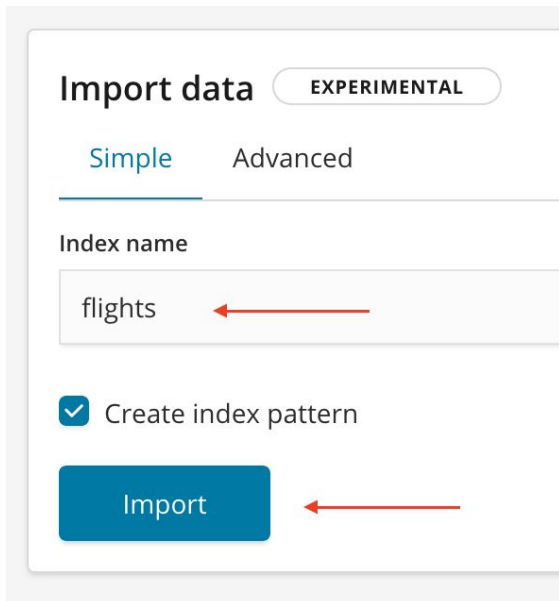


Select or drag and drop a file

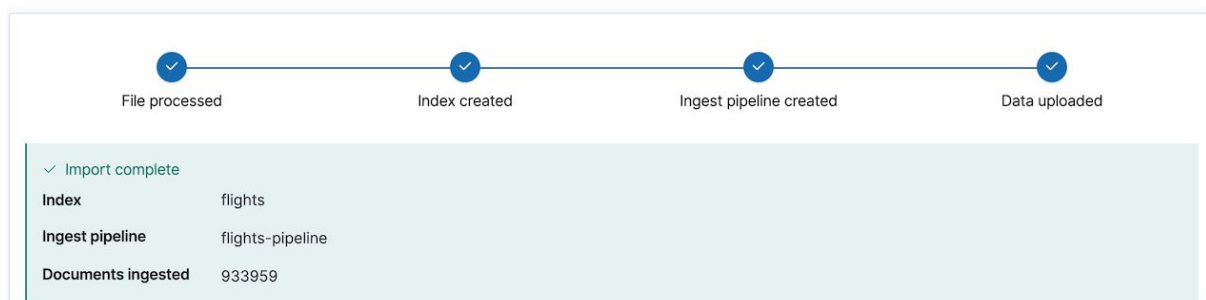
6. 화면 좌측 하단에 “Import” 버튼을 클릭한다.



7. Index name에 “flights”라고 입력한다. “Create index pattern”은 선택 상태로 둔다.



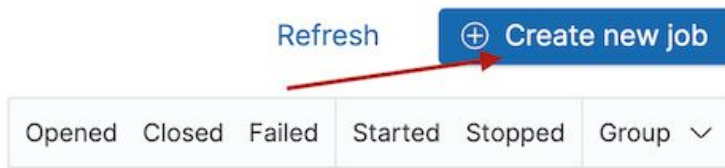
8. “Import” 버튼을 누른 후 “Import complete” 메시지가 나와야 한다.



9. 화면 상단의 “Machine Learning” 링크를 누르고 “Anomaly Detection” 탭을 클릭한다.



10. “Create new job” 버튼을 클릭한다.

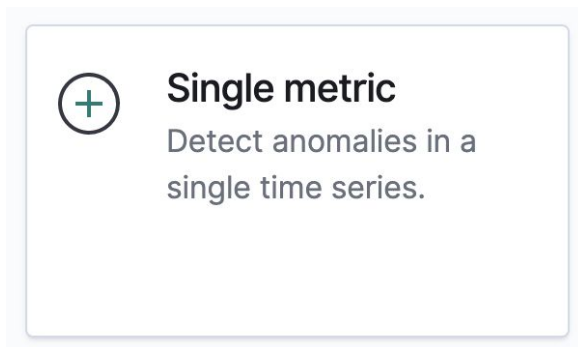


11. 검색창에 “flights”를 입력하고 flights 인덱스를 선택한다.

## From a New Search, Select Index

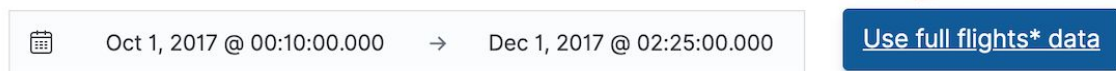


12. “Single metric” 버튼을 클릭한다.



13. 우측의 “Use full flights data”를 클릭한다.

## Time range



14. “Next” 버튼 클릭.



15. “Pick Fields”에서 “Count(Event rate)” 선택

## Pick fields



**Event rate**

- Count(Event rate)
- High count(Event rate)
- Low count(Event rate)

**airline**

- Distinct count(airline)

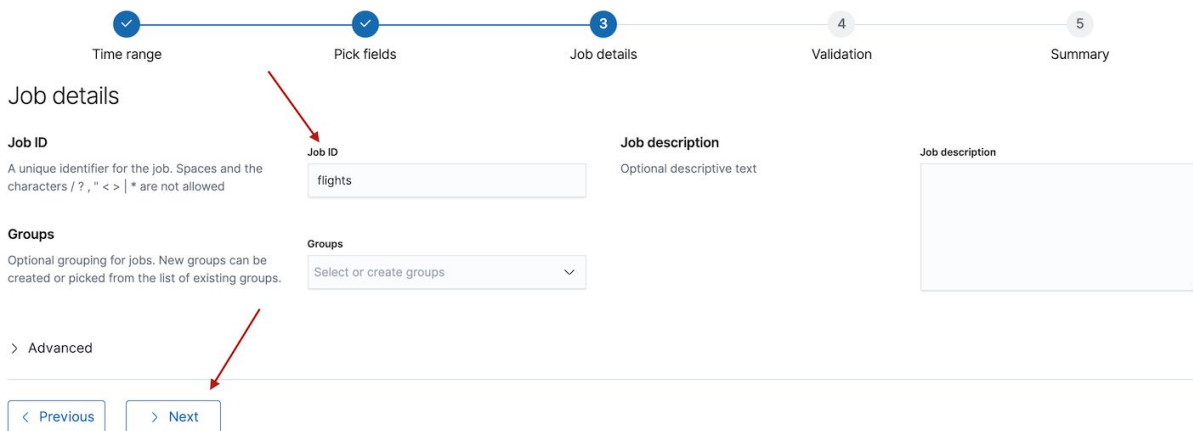
**destination**

노트: 나머지 설정들은 처음 그대로 둔다. default

16. “Next” 버튼 클릭



17. Job ID 필드에 “flights”를 입력하고 “Next” 버튼을 누른다.



Time range Pick fields Job details Validation Summary

**Job ID**  
A unique identifier for the job. Spaces and the characters / ?, " < > \* are not allowed

**Job ID**  
flights

**Job description**  
Optional descriptive text

**Job description**

**Groups**  
Optional grouping for jobs. New groups can be created or picked from the list of existing groups.

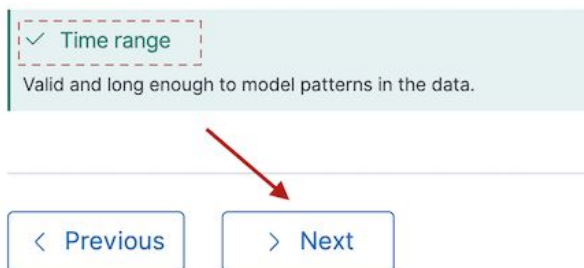
**Groups**  
Select or create groups

> Advanced

< Previous > Next

18. “Time range” 사자가 초록색이어야 한다. “Next” 버튼을 클릭한다.

## Validation



✓ Time range

Valid and long enough to model patterns in the data.

< Previous > Next

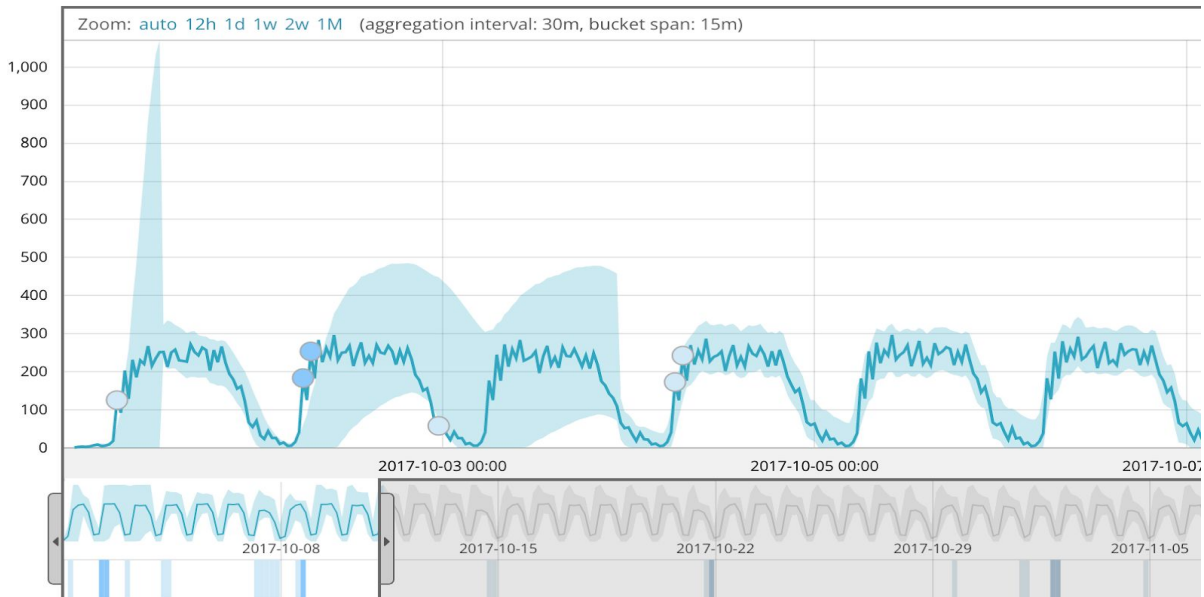
19. “Create job” 버튼을 클릭하여 모델 생성을 시작한다.



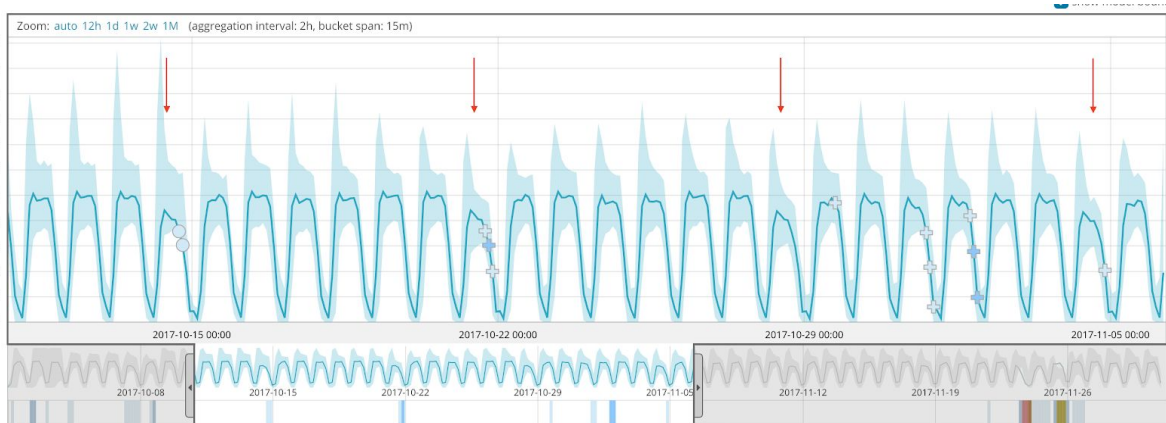
20. 작업이 끝나면, 원본 데이터 스트림 위에 데이터 모델이 겹쳐져 있는 것을 볼 수 있다. “View results” 버튼을 클릭한다.



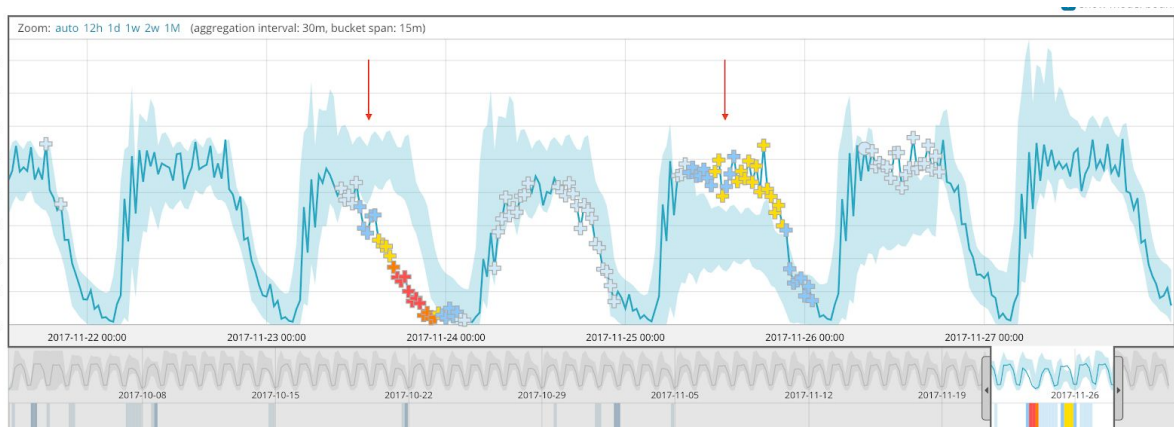
21. 새창이 열리고 “Single Metric Viewer” 화면이 보일것이다. 시간 윈도우를 왼쪽으로 끌어서 데이터의 처음 첫 주 정도만 선택되도록 한다. 데이터 모델이 대략 3일 이후에 정확한 패턴을 찾았음을 알 수 있다.



22. 다시 시간 윈도우를 조정하여 이후 약 4주정도를 선택하도록 한다. 미국 민항기 운항 데이터에서 주간 패턴을 찾을 수 있는가? 주중 어느 요일이 다른 요일에 비해 비행이 적은가?



18. 시간 윈도우를 조정하여 11월 22일이 시작하는 주는 선택한다. Detector는 왜 11/23일 목요일에 높은 점수의 이상치들을 찾은 것일까? 또, 11월 25일 토요일에는 왜 이상치를 탐지했을까?



Elastic Machine Learning은 수백 수천의 데이터 스트림에서 이상치를 찾을 수 있도록 해준다. 이 각각에 대해 데이터 모델을 생성하고 주어진 데이터 스트림이 과거의 행동과 다르게 행동하기 시작하면 이를 알려준다.

16. 끝.

Elastic 워크샵에 참석해주셔서 감사합니다.