Section : ELK STACK

Documents create date : 21/05/2024

Version : 1.0

Status : initial Version

Document Author : Itsranuwat Chaodon

Document Reviewer : Krittimasak Wangsri (Mentor Engineer)

คำนำ

เอกสารฉบับนี้มีวัตถุประสงค์เพื่อให้ความรู้และข้อมูลเกี่ยวข้องกับการใช้งาน ELK STACK ซึ่งเป็ฯเครื่องมือที่ประกอบด้วย Elastic Search, Logstash, Kibana ซึ่งเป็นเครื่องมือสำคัญในการและสร้างการแสดงข้อมูลด้วยภาพสำหรับการตรวจสอบ การแก้ไขปัญหาอย่างรวดเร็ว การวิเคราะห์ความปลอดภัย และอื่นๆ อีกมากมายให้กับแอปพลิเคชัน

ในเอกสารนี้จะครอบคลุมถึงการติดตั้งและการใช้งานของ ELK STACK การนำเข้าข้อมูลประเภท csv มาทำการวิเคราะห์ข้อมูล และการตั้งค่าเบื้องต้นของ ELK STACK

เราเชื่อว่าเอกสารฉบับนี้จะเป็นประโยชน์สำหรับนักพัฒนาระบบ และหวังเป็ฯอย่างยิ่งว่าจะสามารถช่วยให้ท่านได้นำความรู้ที่ได้รับไปประยุกต์ใช้ในการทำงานได้อย่างมีประสิทธิภาพ

นายอิศรานุวัฒน์ ชาวดร

สารบัญ

Elk Stack คืออะไร

ELK Stack คือตัวย่อที่ใช้แทนสแตกที่ประกอบด้วยสามโปรเจกต์ยอดนิยม ได้แก่ Elasticsearch, Logstash และ Kibana ELK Stack หรือที่มักเรียกกันว่า Elasticsearch จะมอบความสามารถในการรวมข้อมูลบันทึกจากระบบและแอปพลิเคชันทั้งหมดของคุณ วิเคราะห์ข้อมูลบันทึกเหล่านี้ และสร้างการแสดงข้อมูลด้วยภาพสำหรับการตรวจสอบ การแก้ไขปัญหาอย่างรวดเร็ว การวิเคราะห์ความปลอดภัย และอื่นๆ อีกมากมายให้กับแอปพลิเคชันและโครงสร้างพื้นฐาน

1. **Elasticsearch** คือเครื่องมือค้นหาและวิเคราะห์ข้อมูลแบบกระจาย ที่มีพื้นฐานมาจาก Apache Lucene การรองรับภาษาต่างๆ ประสิทธิภาพที่สูง และเอกสาร JSON ที่ปราศจากสคีปมาทำให้ Elasticsearch เป็นตัวเลือกที่เหมาะอย่างยิ่งสำหรับการวิเคราะห์บันทึกและกรณีใช้งานการค้นหาต่างๆ

2. **Logstash** คือเครื่องมือนำเข้าข้อมูลแบบโอเพนซอร์สที่ช่วยในการรวบรวมข้อมูลจากแหล่งต่างๆ ก่อนจะแปลงข้อมูลดังกล่าว แล้วส่งไปยังปลายทางที่ต้องการ Logstash ช่วยให้นำเข้าข้อมูลได้อย่างง่ายดายไม่ว่าจะเป็นแหล่งข้อมูลหรือข้อมูลประเภทใด ด้วยตัวกรองที่สร้างไว้ล่วงหน้าและความสามารถในการรองรับปลั๊กอินมากกว่า 200 รายการ

   Logstash คือไปป์ไลน์การประมวลผลข้อมูลฝั่งเซิร์ฟเวอร์แบบโอเพนซอร์สที่ใช้ทรัพยากรน้อย ซึ่งช่วยให้สามารถรวบรวมข้อมูลจากแหล่งต่างๆ ก่อนจะแปลงข้อมูลดังกล่าวทันที แล้วส่งไปยังปลายทางที่ต้องการได้ โดยมักจะนำไปใช้เป็นไปป์ไลน์ข้อมูลสำหรับเครื่องมือวิเคราะห์และค้นหาแบบโอเพนซอร์สอย่าง Elasticsearch Logstash คือตัวเลือกยอดนิยมในการโหลดข้อมูลไปยัง Elasticsearch เพราะผสานรวมอย่างเหนียวแน่นกับ Elasticsearch, มีคุณสมบัติในการประมวลผลบันทึกที่มีประสิทธิภาพ และมีปลั๊กอินโอเพนซอร์สที่สร้างไว้ล่วงหน้ามากกว่า 200 รายการที่ช่วยให้คุณสร้างดัชนีข้อมูลได้อย่างง่ายดาย Logstash ช่วยให้สามารถนำเข้าข้อมูลที่ไม่มีโครงสร้างจากแหล่งข้อมูลต่าง ๆ ได้อย่างง่ายดาย เช่น บันทึกระบบ บันทึกเว็บไซต์ และบันทึกเซิร์ฟเวอร์แอปพลิเคชัน

   Logstash มีตัวกรองที่สร้างไว้ล่วงหน้า จึงสามารถแปลงประเภทข้อมูลทั่วไป สร้างดัชนีข้อมูลใน Elasticsearch และเริ่มสืบค้นได้อย่างง่ายดายโดยไม่ต้องสร้างไปป์ไลน์การแปลงข้อมูลแบบกำหนดเอง

3. **Kibana** คือเครื่องมือแสดงข้อมูลด้วยภาพและสำรวจข้อมูลที่ใช้สำหรับการวิเคราะห์บันทึกและอนุกรมเวลา การตรวจสอบแอปพลิเคชัน และการใช้งานความอัจฉริยะในการดำเนินการ ซึ่งมีคุณสมบัติประสิทธิภาพสูงแต่ใช้งานง่ายมากมาย เช่น ฮิสโตแกรม กราฟเส้น แผนภูมิวงกลม แผนภูมิความร้อน และการสนับสนุนภูมิสารสนเทศในตัว นอกจากนั้นยังมีการผสานรวมที่เหนียวแน่นกับเครื่องมือวิเคราะห์และค้นหายอดนิยมอย่าง Elasticsearch อีกด้วย ซึ่งทำให้ Kibana กลายเป็นตัวเลือกแรก ๆ ในการแสดงข้อมูลที่อยู่ใน Elasticsearch ด้วยภาพ

ตารางแบบอินเทอร์แอคทีฟ :

Kibana มีตารางและรายงานแบบอินเทอร์แอคทีฟที่สามารถใช้เพื่อดูข้อมูลบันทึกจำนวนมากได้ สามารถเลือกช่วงเวลา ซูมเข้าออกจากชุดข้อมูลย่อยที่ต้องการ และเจาะลึกรายงานเพื่อดึงข้อมูลเชิงลึกที่นำไปใช้ได้จริงจากข้อมูลได้

รองรับการแมป :

Kibana มาพร้อมกับความสามารถด้านภูมิสารสนเทศที่มีประสิทธิภาพ ดังนั้นจึงสามารถจัดเลเยอร์ข้อมูลทางภูมิศาสตร์ที่ด้านบนของข้อมูลได้อย่างราบรื่นและแสดงผลลัพธ์บนแผนที่

การรวบรวมและการคัดกรองที่สร้างไว้ล่วงหน้า :

เมื่อใช้การรวบรวมและตัวกรองที่สร้างไว้ล่วงหน้าของ Kibana สามารถเรียกใช้การวิเคราะห์ต่าง ๆ เช่น ฮิสโตแกรม แบบสอบถาม TOP-N และแนวโน้มได้ในไม่กี่ขั้นตอน

แดชบอร์ดที่เข้าถึงได้อย่างง่ายดาย :

สามารถตั้งค่าแดชบอร์ดและรายงานต่างๆ ได้อย่างง่ายดาย อีกทั้งยังแชร์ให้กับผู้อื่นได้ด้วย เพียงแค่ใช้เบราว์เซอร์เพื่อดูและค้นหาข้อมูลเท่านั้น

โดยทั่วไปแล้ว ELK Stack นั้นใช้สำหรับการวิเคราะห์ข้อมูลจากตัวโปรแกรมอื่นๆ เช่น บันทึกเหตุการณ์ระบบ (system logs), ข้อมูลการใช้งานเว็บ (web usage data), ข้อมูลแอปพลิเคชัน (application logs), หรือแม้กระทั่งข้อมูลเซิร์ฟเวอร์ (server metrics) เพื่อให้ผู้ใช้สามารถทำความเข้าใจและวิเคราะห์ข้อมูลเหล่านี้ได้อย่างมีประสิทธิภาพ

ELK Stack จึงมีความสำคัญ

ELK Stack เติมเต็มความต้องการพื้นที่ในด้านการวิเคราะห์ข้อมูลบันทึก เมื่อโครงสร้างพื้นฐานด้านไอทีจำเป็นต้องย้ายไปยังระบบคลาวด์สาธารณะมากขึ้น ยิ่งทำให้ต้องการการจัดการข้อมูลบันทึกและโซลูชันสำหรับการวิเคราะห์เพื่อตรวจสอบโครงสร้างพื้นฐานนี้รวมถึงการประมวลผลข้อมูลบันทึกเซิร์ฟเวอร์ ข้อมูลบันทึกแอปพลิเคชัน และคลิกสตรีม ELK Stack จะให้โซลูชันการวิเคราะห์ข้อมูลบันทึกที่เรียบง่ายแต่มีประสิทธิภาพแก่นักพัฒนาและวิศวกร DevOps เพื่อรับข้อมูลเชิงลึกอันมีค่าเกี่ยวกับการวินิจฉัยความล้มเหลว ประสิทธิภาพของแอปพลิเคชันและการตรวจสอบโครงสร้างพื้นฐาน โดยมีค่าใช้จ่ายเพียงเล็กน้อยเท่านั้น

ทำไมต้องใช้มัน ?

- การใช้ ELK Stack มีประโยชน์มากมายเนื่องจากความสามารถของแต่ละเครื่องมือภายในชุดนี้ที่ช่วยให้ผู้ใช้สามารถจัดการและวิเคราะห์ข้อมูลได้อย่างมีประสิทธิภาพ นี่คือเหตุผลหลักที่ทำให้หลายองค์กรและธุรกิจต่างๆ เลือกที่จะนำ ELK Stack มาใช้:
- การจัดเก็บข้อมูลใหญ่และค้นหาข้อมูลอย่างรวดเร็ว: Elasticsearch เป็นพื้นที่จัดเก็บข้อมูลที่มีประสิทธิภาพสูงและสามารถทำการค้นหาข้อมูลอย่างรวดเร็ว ด้วยระบบการทำ Indexing ที่เชื่อถือได้ ทำให้สามารถค้นหาข้อมูลในข้อมูลใหญ่ๆ ได้อย่างรวดเร็วและมีประสิทธิภาพ
- การประมวลผลข้อมูลแบบท่อน้ำ: Logstash เป็นเครื่องมือที่มีความยืดหยุ่นสูงในการปรับแต่งและจัดการข้อมูลที่มีลักษณะแตกต่างกัน ซึ่งช่วยให้ผู้ใช้สามารถรวบรวมข้อมูลจากแหล่งต่างๆ และนำเข้าสู่ Elasticsearch หรือส่งออกไปยังแหล่งข้อมูลอื่นๆ ได้อย่างมีประสิทธิภาพ
- การแสดงผลข้อมูลและการวิเคราะห์เชิงลึก: Kibana เป็นเครื่องมือที่ใช้สำหรับการแสดงผลข้อมูลและการวิเคราะห์ที่มีความสามารถในการสร้างแผนภูมิ กราฟ และการแสดงข้อมูลอื่นๆ อย่างสวยงามและมีประสิทธิภาพ ช่วยให้ผู้ใช้สามารถทำความเข้าใจและวิเคราะห์ข้อมูลได้อย่างชัดเจน

- ความยืดหยุ่นและปรับแต่ง: ELK Stack มีความยืดหยุ่นสูงในการปรับแต่งตามความต้องการของผู้ใช้ เช่น การสร้างชุดข้อมูลที่แตกต่างกัน การกำหนดเงื่อนไขในการตัดสินใจการวิเคราะห์ข้อมูล หรือการปรับแต่งส่วนต่างๆ ของเครื่องมือ
- ดังนั้น ELK Stack เป็นเครื่องมือที่มีความสามารถในการจัดการและวิเคราะห์ข้อมูลให้กับองค์กรในรูปแบบที่มีประสิทธิภาพและมีประสิทธิภาพสูง โดยเฉพาะองค์กรที่มีความต้องการในการจัดการข้อมูลขนาดใหญ่และการทำความเข้าใจข้อมูลในลักษณะที่หลากหลาย

ยกตัวอย่าง Usecase

การวิเคราะห์และตรวจสอบข้อมูลการโจมตีความปลอดภัย (Security Monitoring and Analysis) ในสถานการณ์ที่ธุรกิจหรือองค์กรต้องการป้องกันตัวเองจากการโจมตีความปลอดภัยในระบบของตน พวกเขาสามารถใช้ ELK Stack เพื่อวิเคราะห์และตรวจสอบกิจกรรมที่เกี่ยวข้องกับความปลอดภัยได้ ตัวอย่างเช่น:

รวบรวมข้อมูลการโจมตี: ใช้ Logstash เพื่อรวบรวมข้อมูลจากเหตุการณ์ระบบและอุปกรณ์เครือข่ายที่เป็นไปได้เกี่ยวข้องกับการโจมตี โดยอาจเป็นการบันทึกเหตุการณ์ของระบบปฏิบัติการหรือการบันทึกการสแกนโครงข่าย (network scans) จากอุปกรณ์ไฟร์วอลล์

จัดเก็บและค้นหาข้อมูล: Elasticsearch จะใช้เก็บข้อมูลที่รวบรวมมาได้อย่างมีประสิทธิภาพ และสามารถค้นหาข้อมูลเหล่านั้นอย่างรวดเร็ว

วิเคราะห์และการแสดงผล: ใช้ Kibana เพื่อสร้างแผนภูมิและกราฟเพื่อวิเคราะห์และแสดงผลข้อมูลการโจมตีอย่างชัดเจน เช่น แผนภูมิการเปลี่ยนแปลงพอร์ต (port changes) หรือการจับกลุ่มของแผนภูมิที่แสดงข้อมูลการเข้าถึงที่มีความเสี่ยงสูง

การใช้ ELK Stack เพื่อการวิเคราะห์และตรวจสอบข้อมูลการโจมตีความปลอดภัยเป็นเพียงตัวอย่างเดียวจากการนำเสนอ การใช้งานอื่นๆ อาจรวมถึงการวิเคราะห์และจัดการข้อมูลเซิร์ฟเวอร์ การวิเคราะห์ข้อมูลการใช้งานแอปพลิเคชัน หรือการวิเคราะห์และจัดการข้อมูลลูกค้า โดยใช้เครื่องมือในชุด ELK Stack อย่างอัตราความสำเร็จและเป็นประสิทธิภาพ

ตัวอย่าง Usecase เพิ่มเติม

Monitoring Infrastructure : ใช้ ELK Stack เพื่อตรวจสอบสถานะและประสิทธิภาพของพื้นฐานของระบบเช่น เซิร์ฟเวอร์, เครือข่าย โดยใช้ Logstash เพื่อเก็บข้อมูล logs จากเซิร์ฟเวอร์และ Kibana เพื่อให้สามารถวิเคราะห์และแสดงข้อมูลได้อย่างสะดวก

Application Performance Monitoring (APM) : ใช้ ELK Stack เพื่อตรวจสอบประสิทธิภาพของแอปพลิเคชัน โดยใช้ Logstash เพื่อรวบรวม logs จากแอปพลิเคชัน และใช้ Elasticsearch เพื่อเก็บข้อมูลนี้ และใช้ Kibana เพื่อสร้างพวกกราฟและรายงานเพื่อวิเคราะห์ประสิทธิภาพของแอปพลิเคชัน

Security Analytics : ใช้ ELK Stack เพื่อตรวจสอบการดำเนินการของระบบและการทำงานของผู้ใช้ โดยใช้ Logstash เพื่อรวบรวมข้อมูลการเข้าถึง และใช้ Elasticsearch เพื่อเก็บข้อมูลนี้ และใช้ Kibana เพื่อสร้างรายงานและกราฟเพื่อวิเคราะห์และตรวจสอบการดำเนินการที่เกิดขึ้นในระบบ

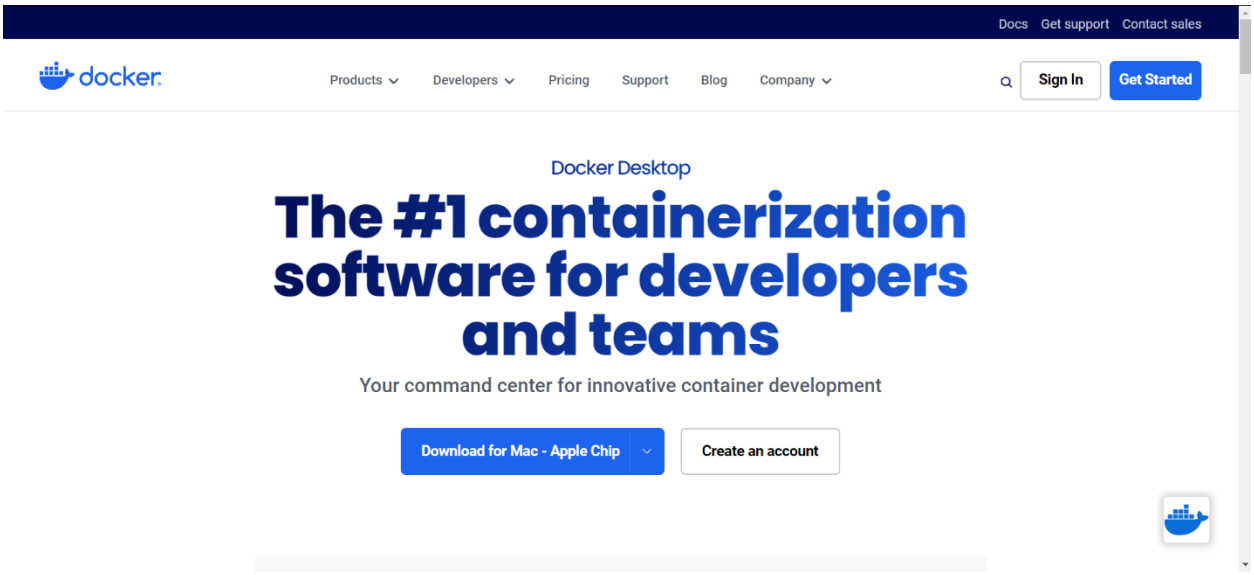
Centralized Logging : ใช้ ELK Stack เพื่อรวบรวม logs จากหลายแหล่งไปยังที่เดียว เพื่อให้ง่ายต่อการค้นหาและวิเคราะห์ข้อมูล ทำให้การตรวจสอบและการแก้ไขปัญหาเป็นไปได้อย่างมีประสิทธิภาพขึ้น

Business Intelligence : ใช้ ELK Stack เพื่อวิเคราะห์ข้อมูลทางธุรกิจ เช่น แสดงข้อมูลการใช้งานของผู้ใช้หรือวิเคราะห์แนวโน้มของการซื้อสินค้า ซึ่งจะช่วยให้ธุรกิจมีข้อมูลที่สำคัญในการตัดสินใจทางธุรกิจ

Demo

ขั้นตอนแรกการเรียกใช้ ELK Stack มีได้ 2 วิธีคือการโหลดไฟล์ จากเว็ปหลักของ ELK Stack และรันผ่านไฟล์ได้เลย แต่ผมจะยกตัวอย่างการเรียกใช้ ELK Stack ผ่าน docker

1. ติดตั้งโปรแกรม Docker desktop



เมื่อติดตั้งเสร็จแล้วทำการเปิดโปรแกรม Docker desktop ขึ้นมา

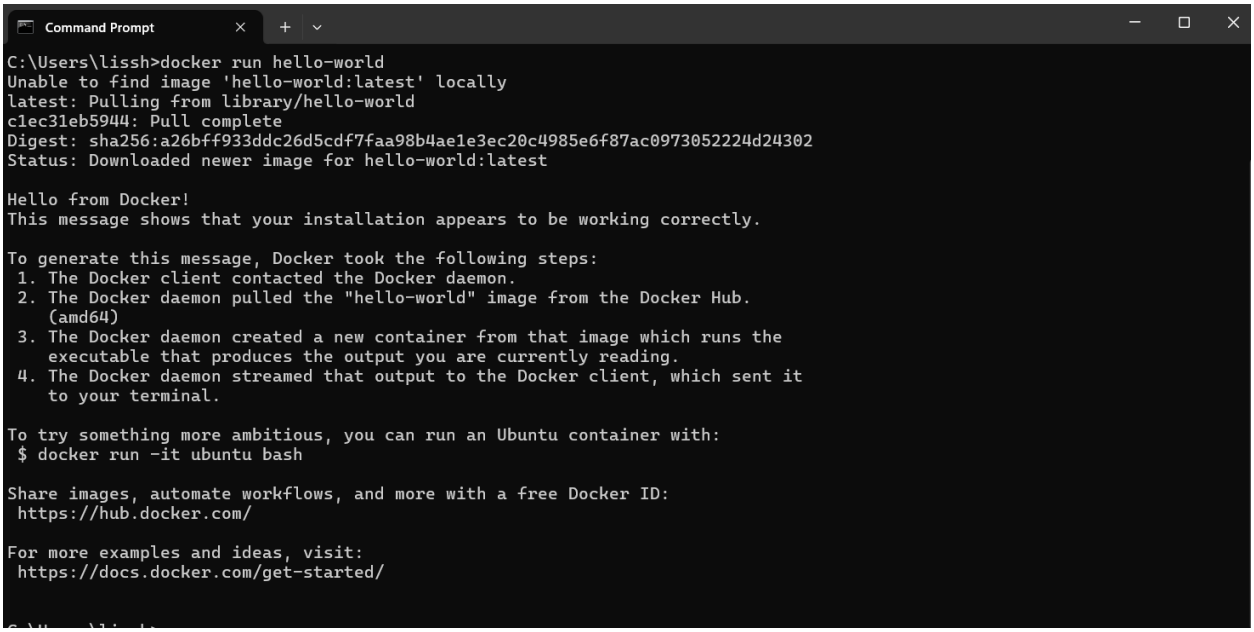
ตรวจสอบการติดตั้ง โดยการรันคำสั่งเช่น

```
docker --version
```

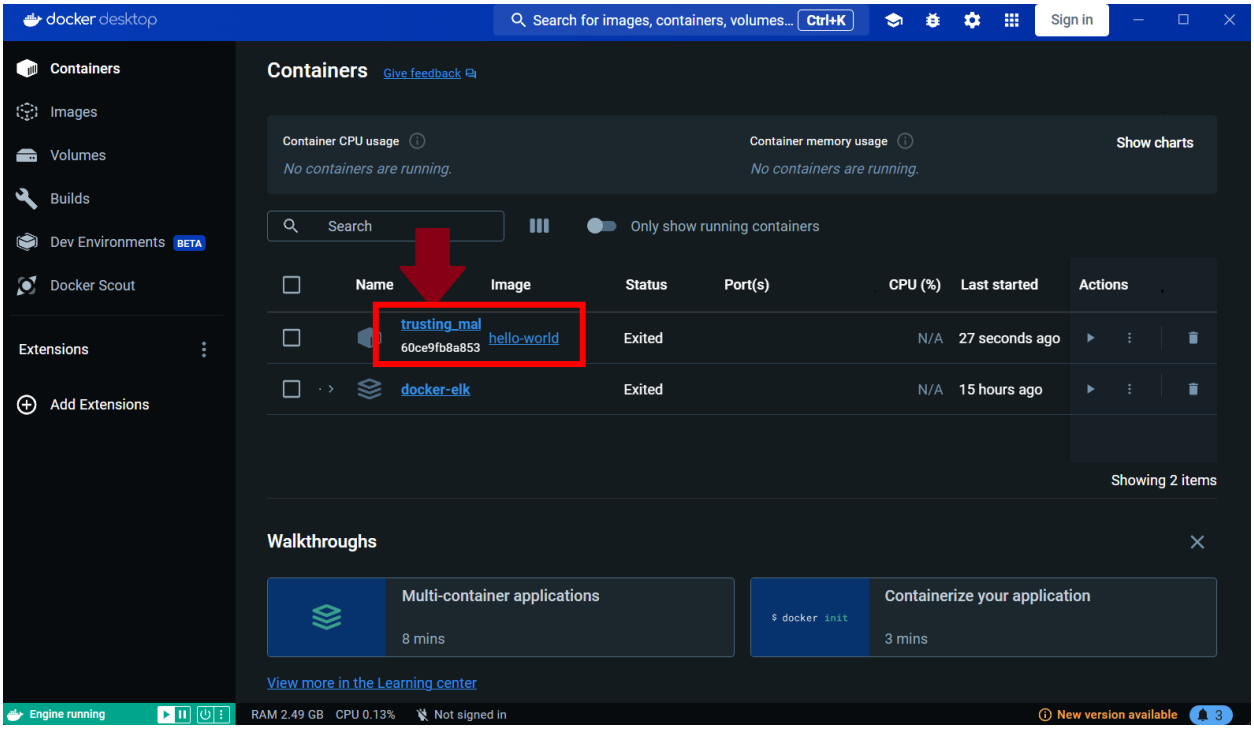
เพื่อตรวจสอบ Docker CLI ทำงานได้อย่างถูกต้อง

ทำการรันคำสั่งเพื่อทดสอบว่า Docker Engine สามารถดาวน์โหลดและรัน Containers ได้อย่างถูกต้อง โดยรันคำสั่ง

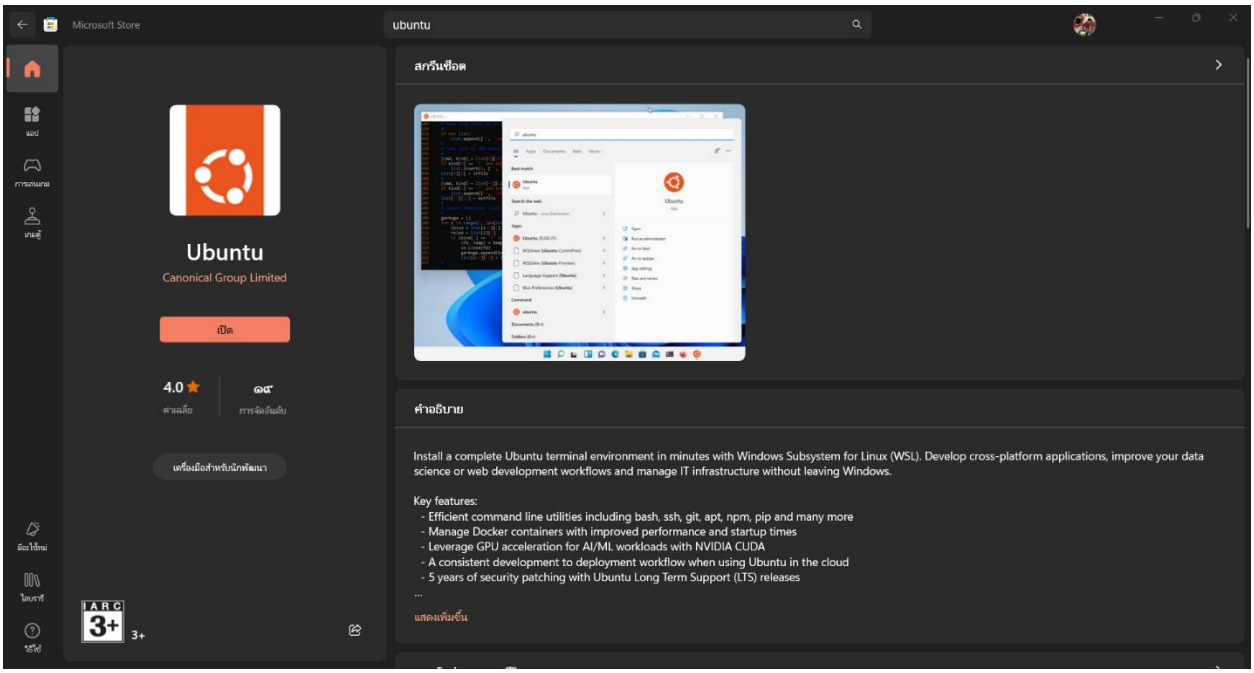
```
docker run hello-world
```



จะได้ ตัว hello world ขึ้นมาใน docker



2. การติดตั้ง Ubuntu



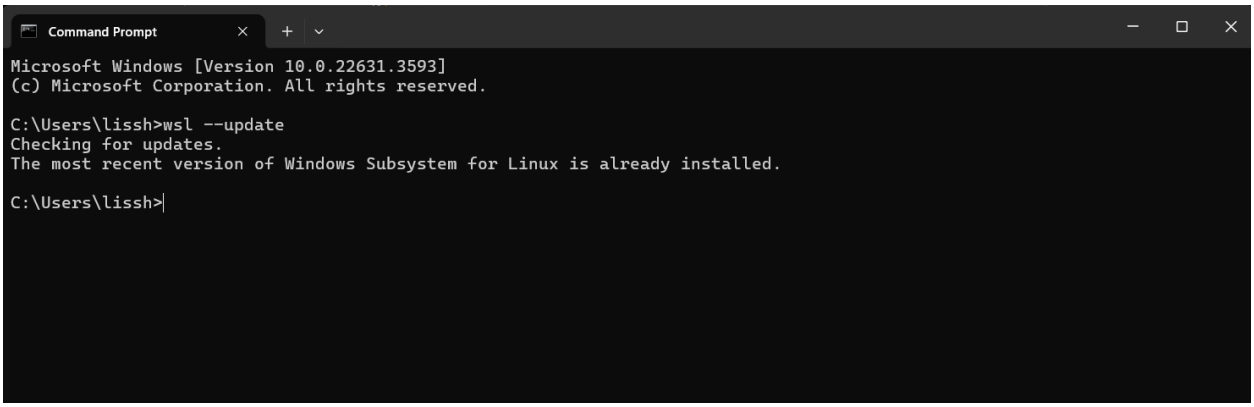
ในที่นี้ผมติดตั้งผ่าน Microsoft store

กดกรอก usename และ password ที่ต้องการจากนั้นรอการติดตั้งจนเสร็จ

จากนั้น เปิด Command Prompt ขึ้นมาแล้วพิมพ์คำสั่ง

```
wsl --update
```

การติดตั้งเสร็จสิ้น



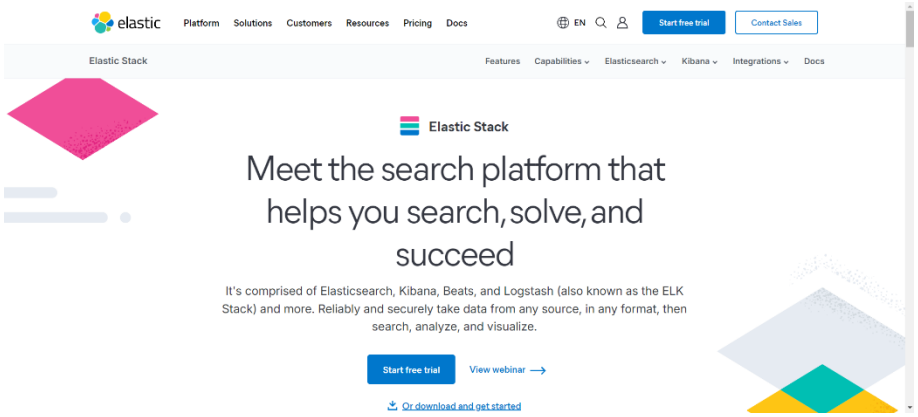
3.ทำการติดตั้ง Elk stack

วิธีที่ 1.)

สามารถเข้าไปที่เว็ปไซต์ทางการของ Elk stack https://www.elastic.co/elastic-stack สามารถเลือกโหลด Elasticsearch Logstash Kibana หรือ สามารถใช้ Docker เพื่อการติดตั้งที่ง่ายต่อการใช้งานมากขึ้น

วิธีที่ 2.)

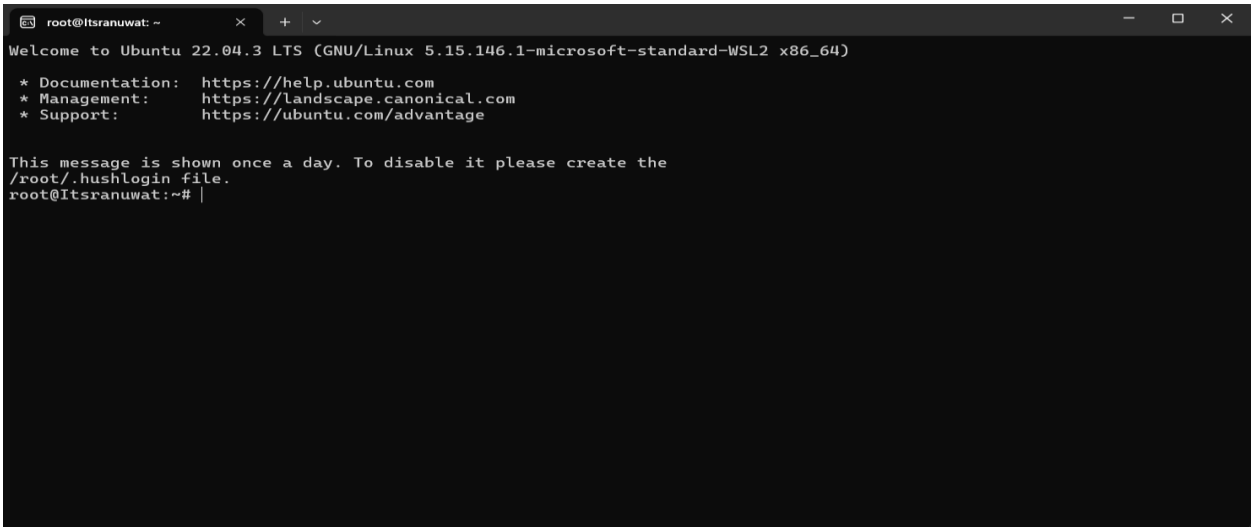
ใช้ Docker สามารถใช้ Docker compose เพื่อเริ่มติดตั้ง Elk stack ได้ง่ายๆ



การใช้งาน Docker ขั้นตอนแรกทำการ gitclone ผ่าน ubuntu ดังนี้

ทำการ gitclone

```
git clone https://github.com/deviantony/docker-elk.git
```



เมื่อทำการ gitclone ผ่าน ubuntu เสร็จจะได้ผลลัพธ์ดังนี้

```
root@Itsranuwat:~# git clone https://github.com/deviantony/docker-elk.git
Cloning into 'docker-elk'...
remote: Enumerating objects: 2984, done.
remote: Counting objects: 100% (208/208), done.
remote: Compressing objects: 100% (94/94), done.
remote: Total 2984 (delta 135), reused 160 (delta 106), pack-reused 2776
Receiving objects: 100% (2984/2984), 778.89 KiB | 105.00 KiB/s, done.
Resolving deltas: 100% (1450/1450), done.
```

พิมพ์คำสั่ง

```
ls
```

เพื่อเช็คว่าเราลง docker เสร็จสิ้นแล้ว

ขั้นตอนต่อไป คือ การ setup docker ลงไปที่โปรแกรม docker desktop

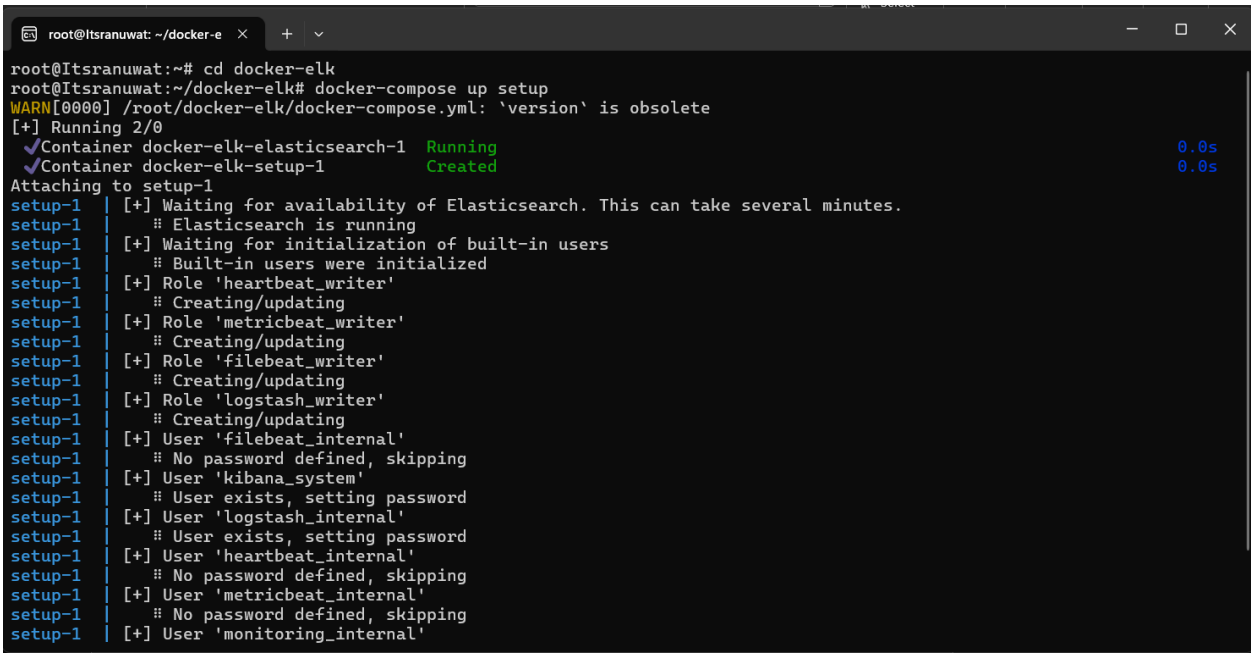
โดยการพิมพ์คำสั่งดังนี้

1. ทำการพิมพ์คำส่ง

```
cd docker-elk
```

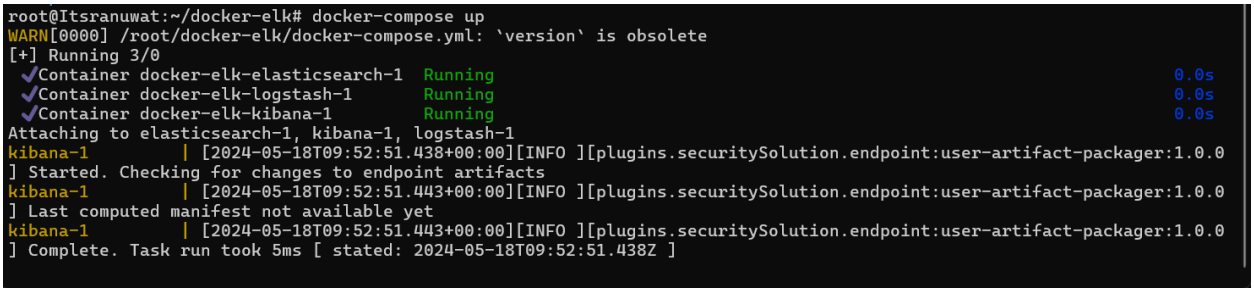
2. ทำการพิมพ์คำสั่ง

ทำการพิมพ์คำสั่ง docker-compose up setup

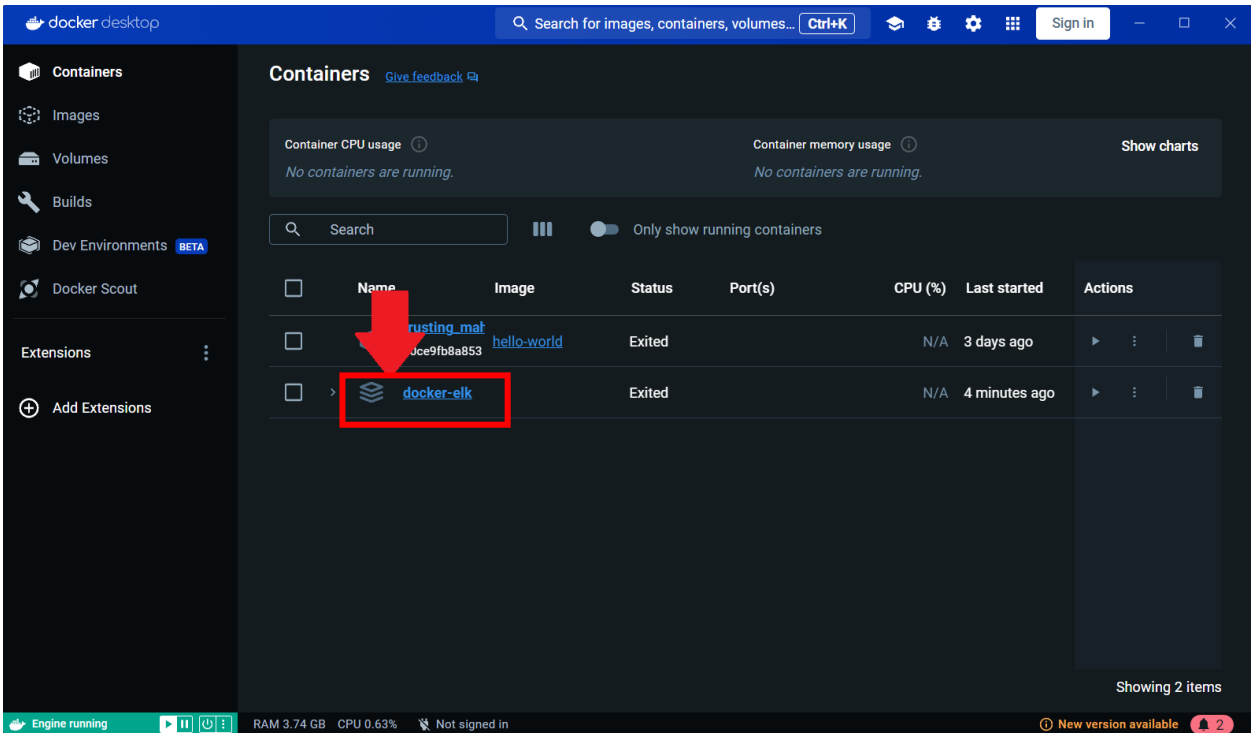


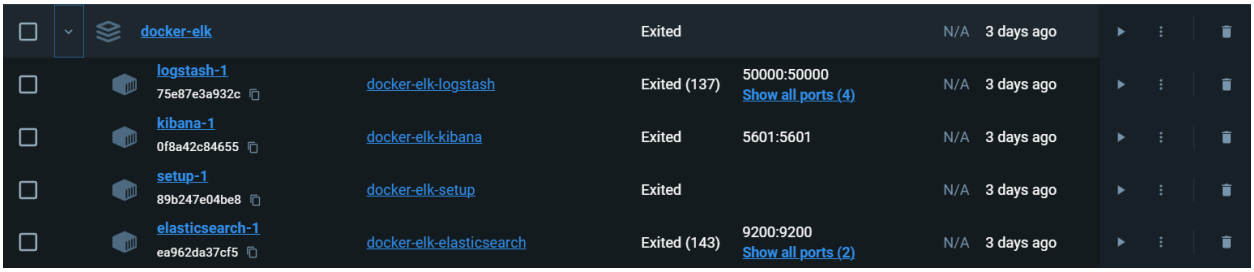
3. ทำการพิมพ์คำสั่ง

docker-compose up



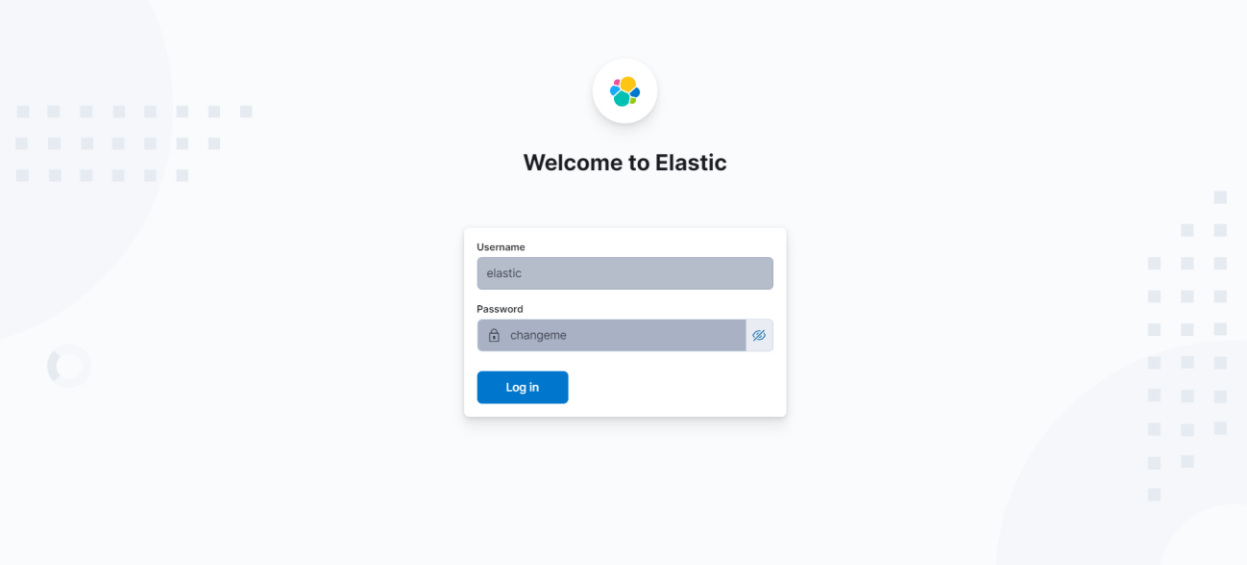
เมื่อทำสองวิธีข้างต้นแล้วเช็คโปรแกรม docker desktop



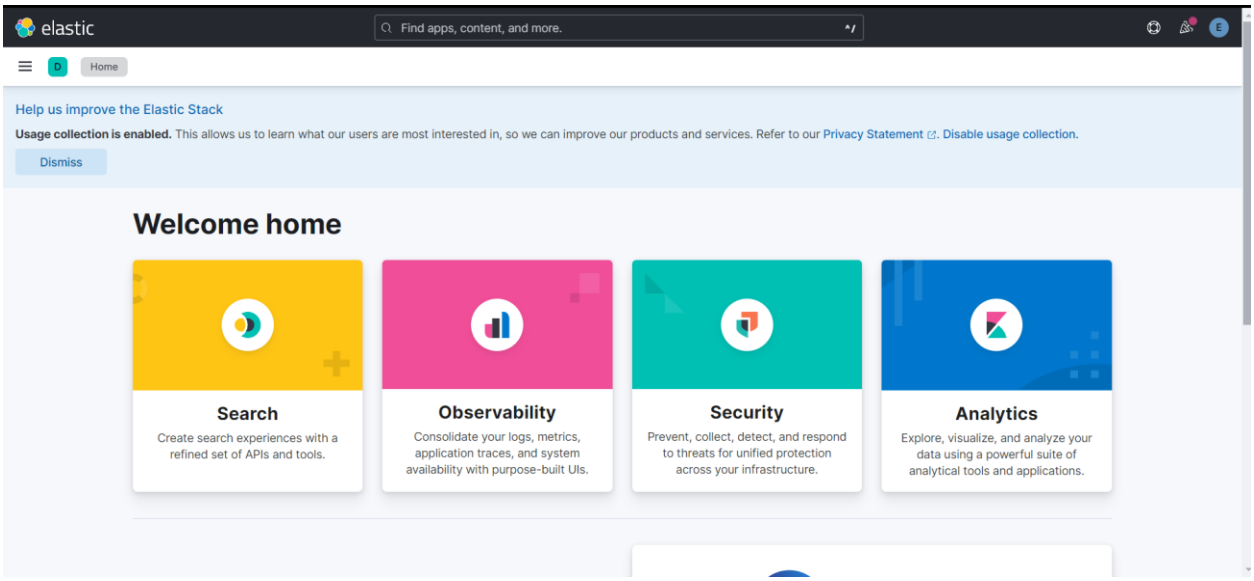


จะเห็นได้ว่ามี elk stack ขึ้นมาแล้ว กดลูกศรลงจะเห็นได้ว่ามี เครื่องมืออยู่ 3 ตัวคือ Elastic search , Logstash , Kibana จะเห็นได้ว่า Kibana จะรันอยู่ที่ port 5601:5601 ทำการคลิกเพื่อเข้าหน้า interface ของ Elk stack

กรอก Username : elastic , Password : changeme

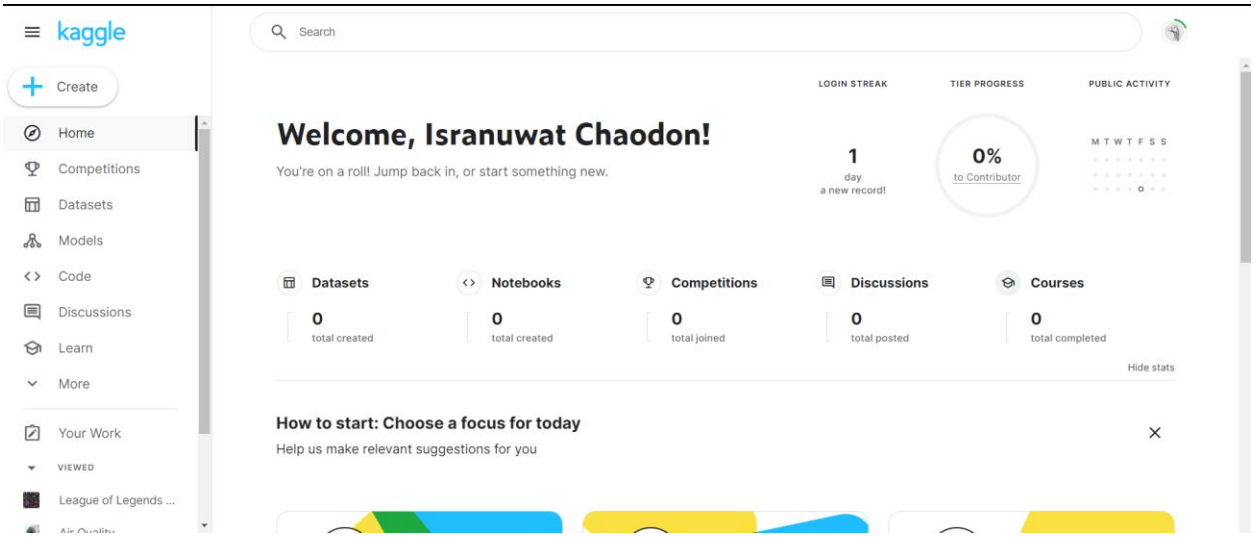


ก็จะเข้าสู่ หน้าหลักของ Elk stack เป็นที่เรียบร้อยแล้ว



ตัวอย่างการใช้งาน Elk stack

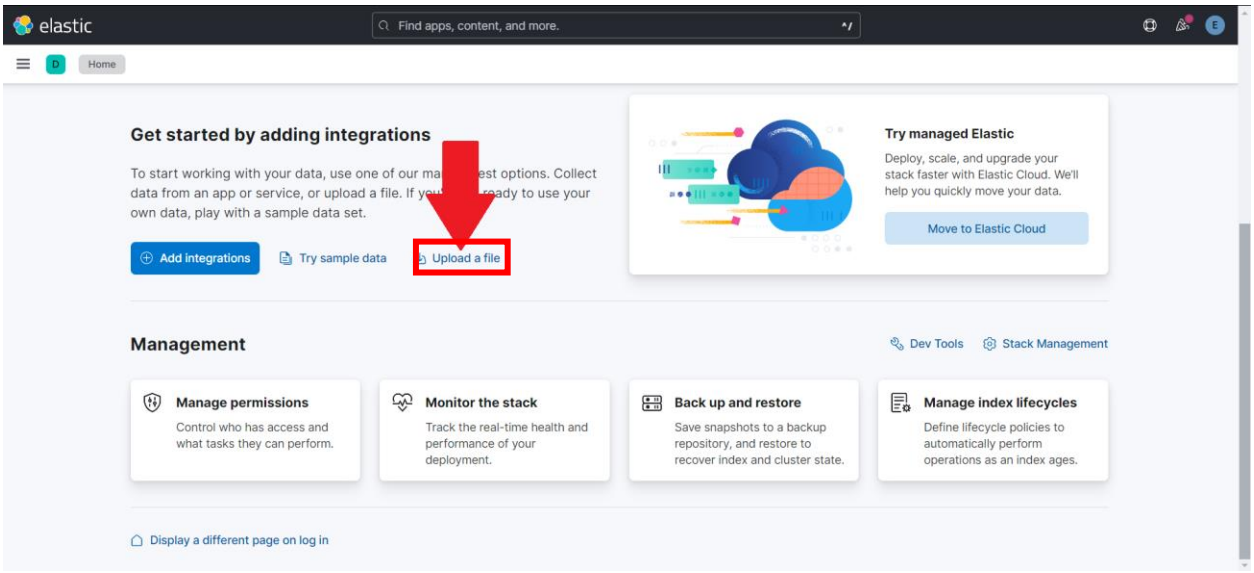
ขั้นตอนนี้ผมทดลองโดยการโหลดตัวอย่างข้อมูลประเภท csv จากเว็ป https://www.kaggle.com/ ทำการเลือกตัวอย่างข้อมูลไฟล์ csv ตามความสนใจของเรา จากตรง Datasets



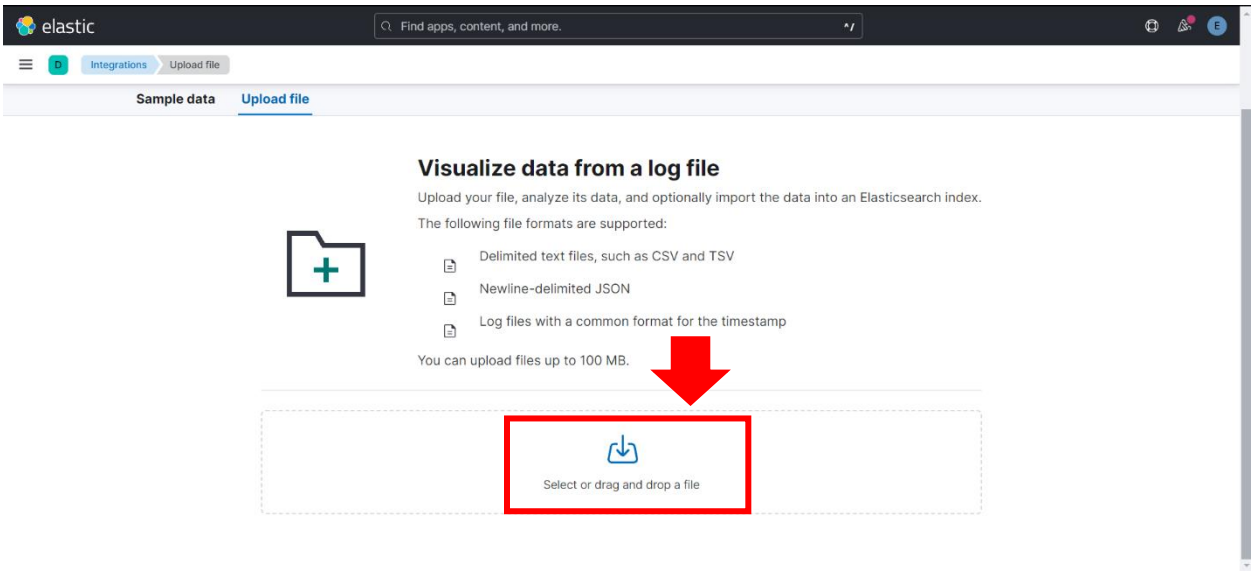
เพื่อนำเข้าไฟล์ csv ไปยัง Elasticsearch โดยแสดงผลผ่านทาง Kibana

1. เข้าหน้าหลักของ Elk stack ผ่าน Docker ที่เราทำการติดตั้งไว้

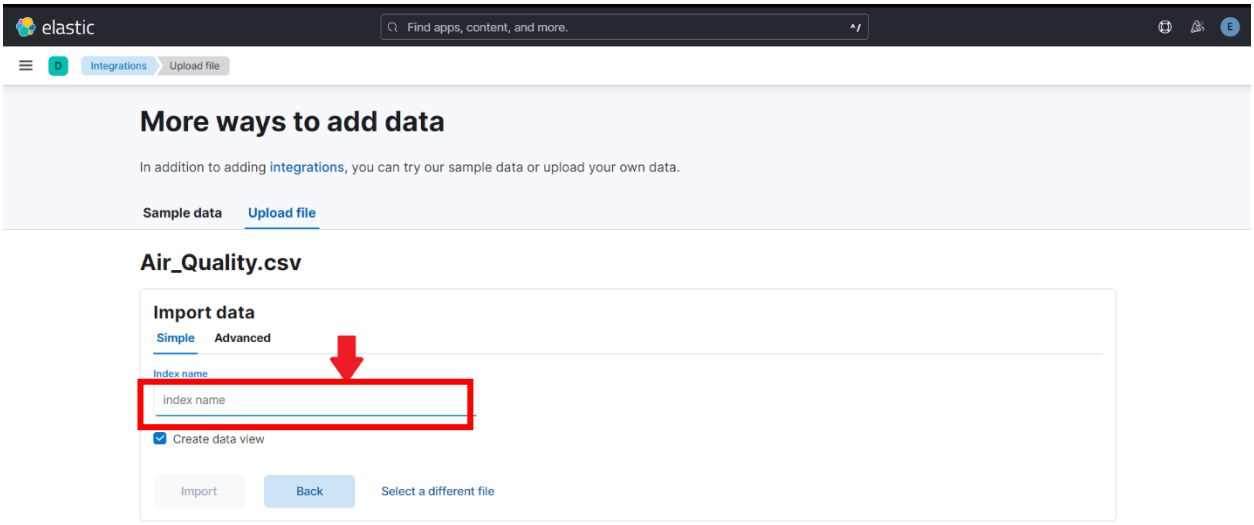
กด Upload a file



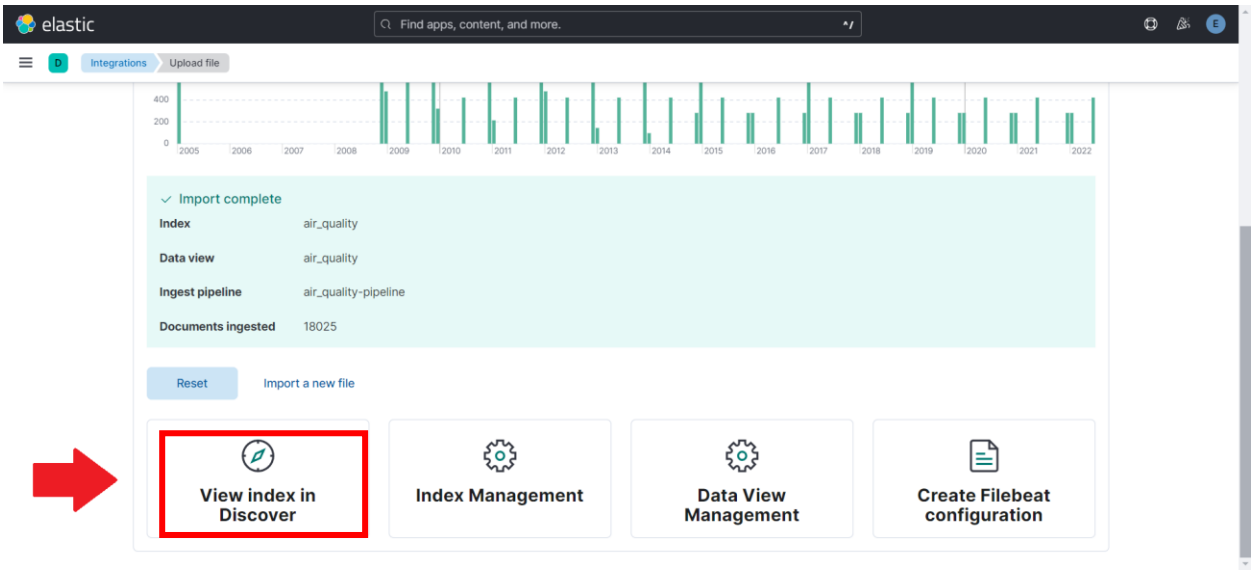
กดไปที่ select or drag and drop a file



เมื่อทำการ Upload ตัวอย่างไฟล์ csv เสร็จแล้ว ทำการตั้ง index name เป็นชื่อของไฟล์ csv ของเรา

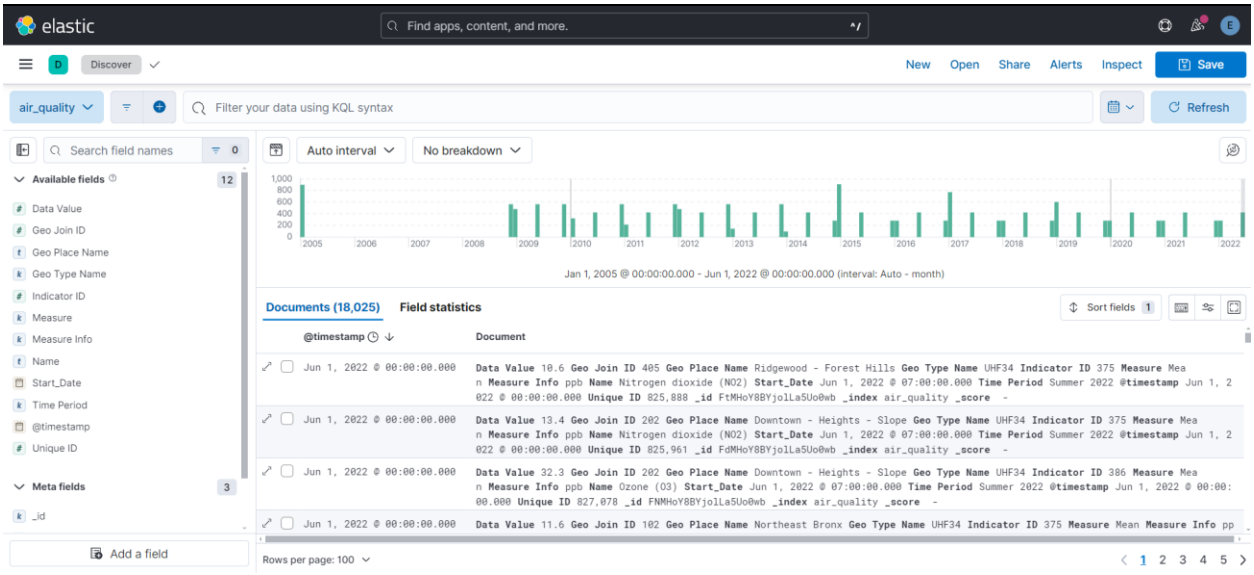


เมื่อ import เสร็จแล้ว ให้ทำการกด View index in Discover เพื่อจัดการไฟล์ข้อมูลไฟล์ csv ต่อไป

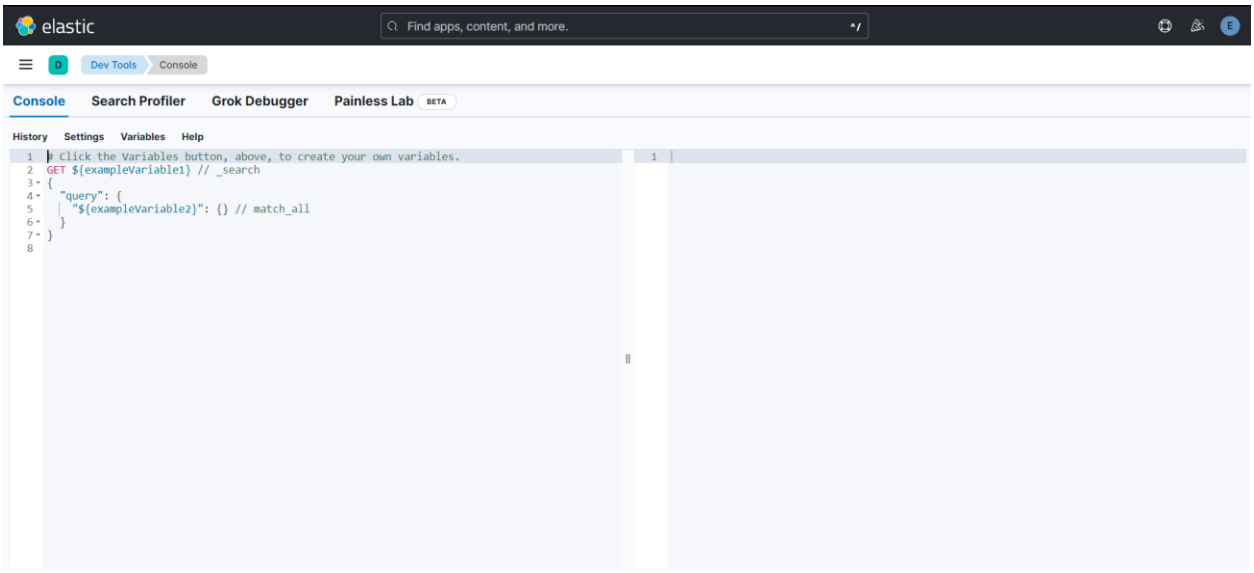


ดูข้อมูลที่เรามีใน Elasticsearch ผ่านหน้า Discover

ซึ่งเราสามารถตรวจสอบ วิเคราะห์ข้อมูล บันทึก หรือค้นหาข้อมูลต่างๆได้จากทาง Elasticsearch และแสดงผลข้อมูลผ่านทาง Kibana

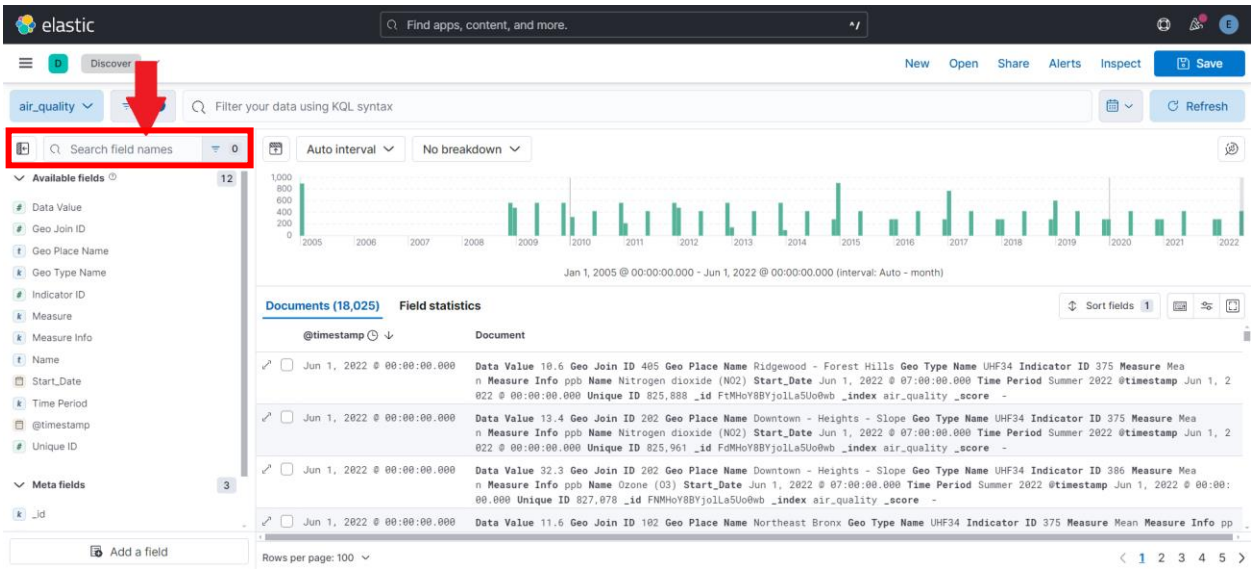


เราสามารถ เพิ่ม ลบ หรือเรียกดูข้อมูลบน Elasticsearch ได้ผ่านหน้า Dev Tools โดยใช้ คำสั่งต่างๆ

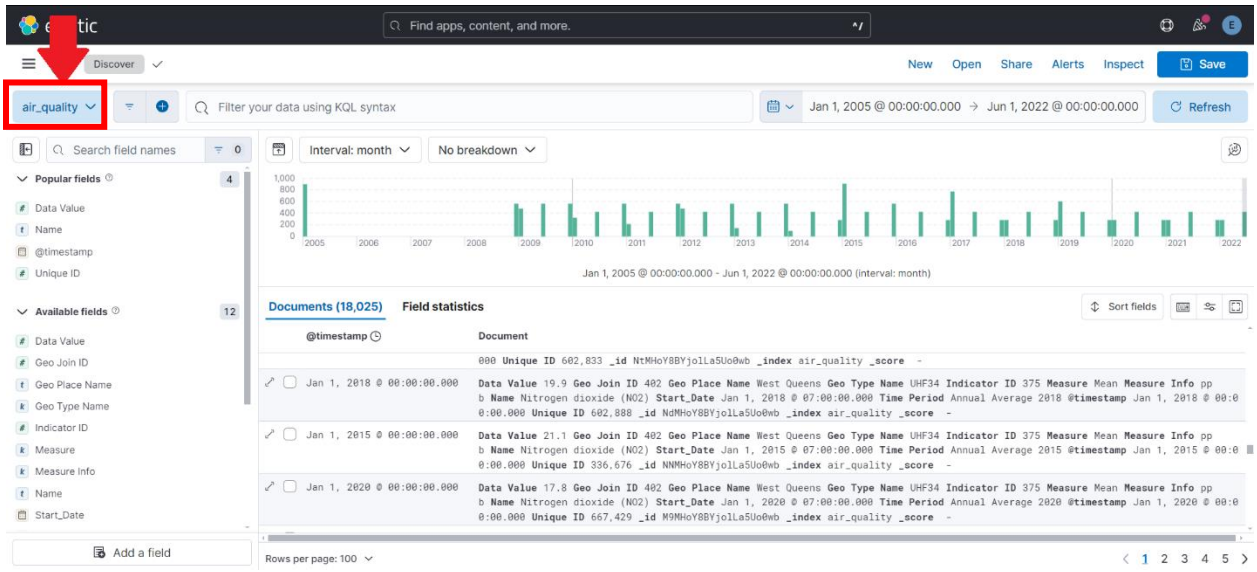


ตัวอย่างหน้าเมนูของ Kibana

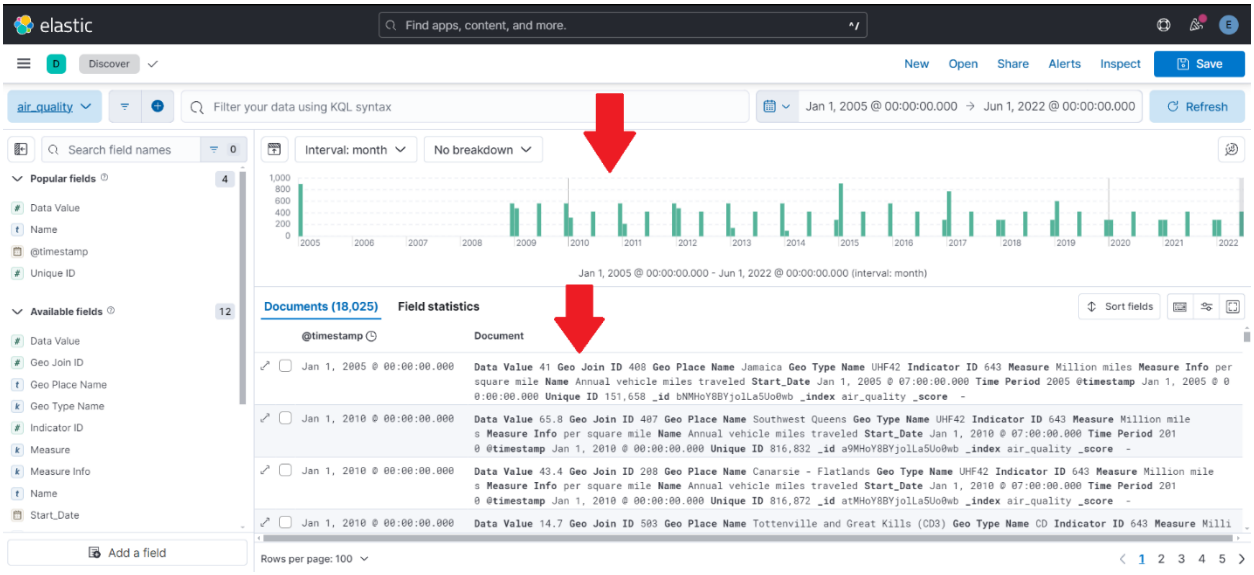
ในส่วนนี้เราสามารถใช้ค้นหา filter field name เพื่อหาหรือดูข้อมูลที่อยู่ใน filter field name นั้นได้



ในส่วนนี้จะเป็นการเลือกข้อมูลจากไฟล์ csv หรือฐานข้อมูลที่เราทำการ Import ลงมา

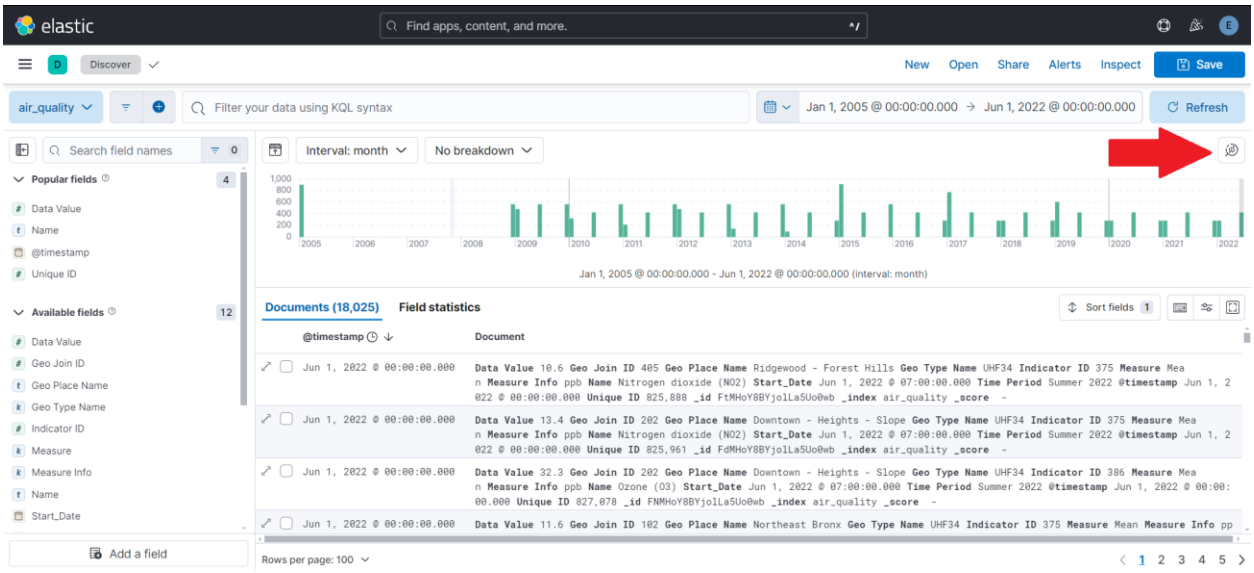


ในส่วนนี้จะเป็นหน้าแสดงผลข้อมูลประเภทต่างๆ เช่น กราฟ วันที่ เป็นต้น

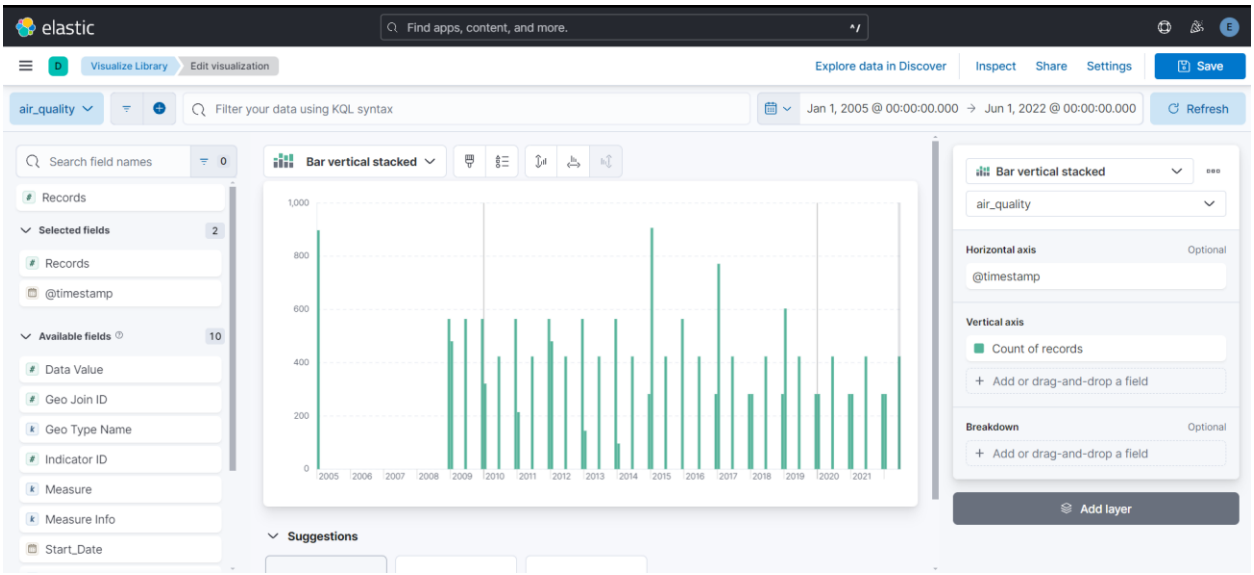


เราสามารถดูข้อมูล กราฟ เป็นแบบช่วงเวลาได้โดยการกดเลือกช่วงเวลาในช่องเลือกช่วงเวลา(Interval month)

และเราสามารถปรับเปลี่ยน กราฟ สีของกราฟ เป็นไปตามรูปแบบที่เราต้องการได้โดยกดไปที่การตั้งค่าแก้ไขการจำลอง(Edit visualization)



เราสามารถตั้งค่าตามที่เราต้องการได้เลย



นี่เป็นตัวอย่าเมนูที่ยกตัวอย่างของ การจัดการข้อมูล ด้วย Elk stack แค่บางส่วนซึ่งอาจต้องศึกษาเพิ่มเติมเพื่อเรียนรู้เครื่องมือ Elk stack สำหรับใช้งานสำหรับโปรเจกต์งานที่ใหญ่ขึ้นและ ELK Stack จะช่วยให้ผู้ใช้งานสามารถมองเห็นภาพรวมของข้อมูล log ที่ได้เก็บรวบรวมและวิเคราะห์ ทำให้สามารถตัดสินใจในการดำเนินการปรับปรุงระบบอย่างมีประสิทธิภาพ