ELK Stack 概覽

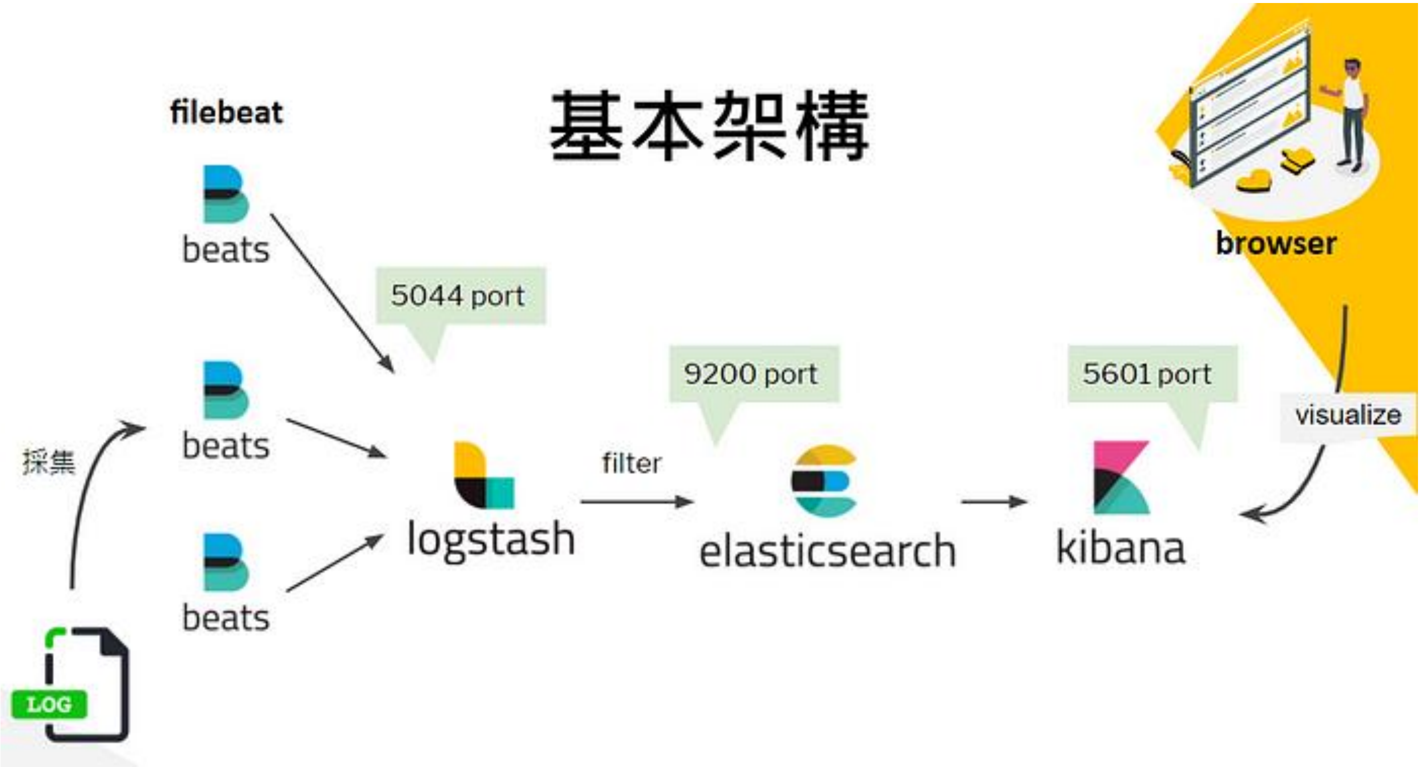
國泰產險-應用開發科

蔡東翰
2024/05/30

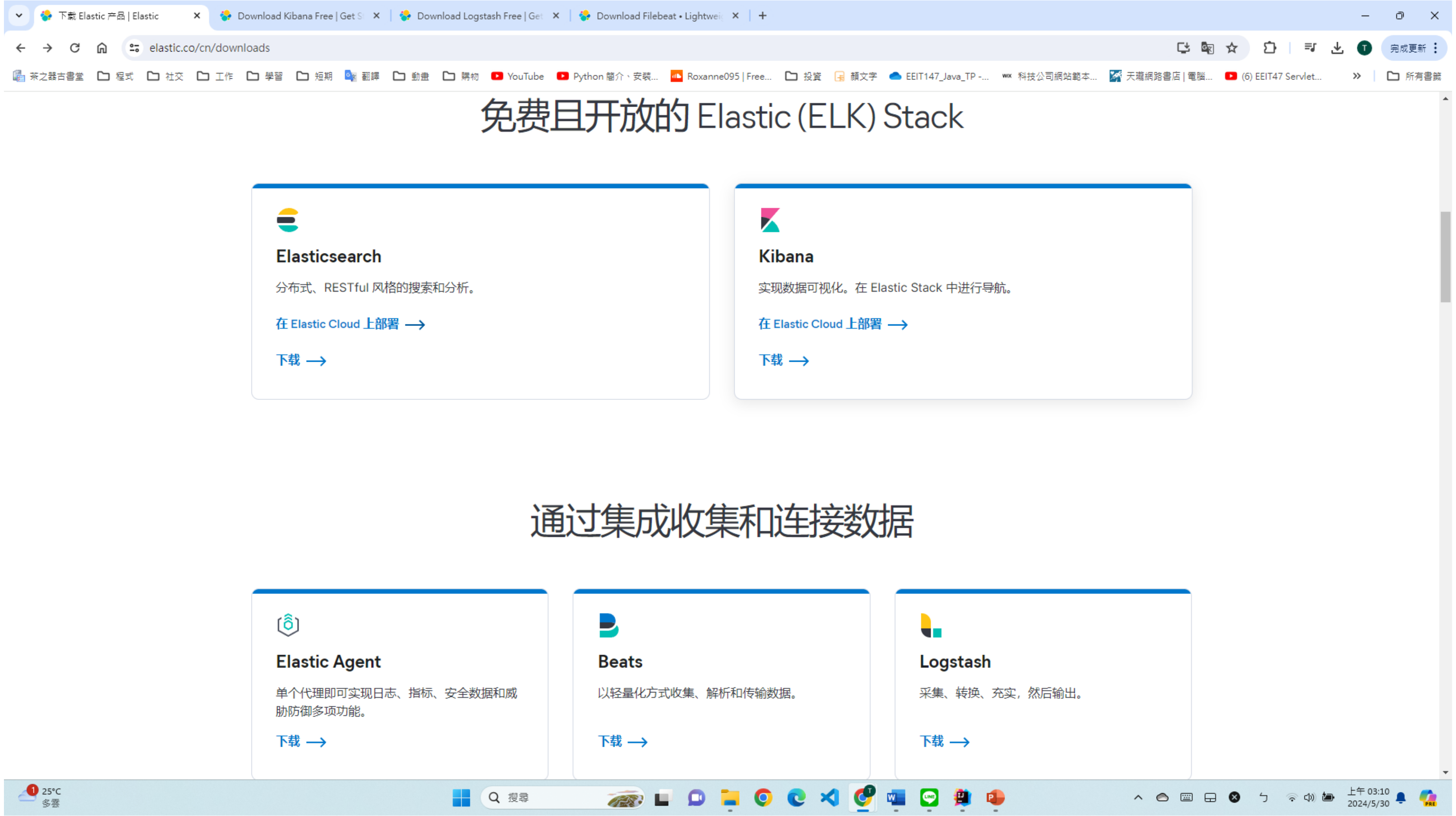
ELK Stack 概覽

什麼是ELK Stack？

- ELK Stack是由Elasticsearch, Logstash, 和 Kibana三個開源項目組成的技術棧，主要用於實時處理大量數據。
- 它允許用戶在所有數據中進行搜索、分析和可視化，廣泛應用於日誌分析、性能監控和數據可視化等領域。



下載連結


下載 Elastic 产品 | Elastic
Download Kibana Free | Get S
Download Logstash Free | Get
Download Filebeat • Lightwei
elastic.co/cn/downloads
完成更新
YouTube
所有書籤
25°C
多雲
搜尋
上午 03:10
2024/5/30

免费且开放的 Elastic (ELK) Stack

Elasticsearch

分布式、RESTful 风格的搜索和分析。

在 Elastic Cloud 上部署 ⟶

下载 ⟶

Kibana

实现数据可视化。在 Elastic Stack 中进行导航。

在 Elastic Cloud 上部署 ⟶

下载 ⟶

通过集成收集和连接数据

Elastic Agent

单个代理即可实现日志、指标、安全数据和威胁防御多项功能。

下载 ⟶

Beats

以轻量化方式收集、解析和传输数据。

下载 ⟶

Logstash

采集、转换、充实，然后输出。

下载 ⟶

https://www.elastic.co/cn/downloads

Elasticsearch

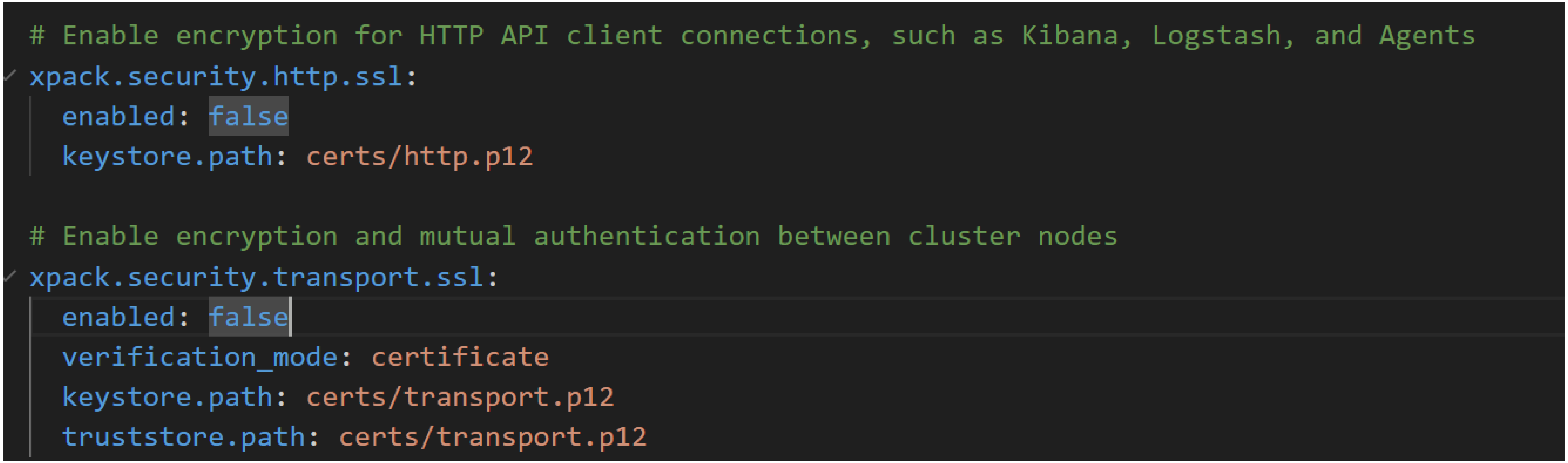
Elasticsearch 簡介

- Elasticsearch是一個高度可擴展的開源全文搜索和分析引擎，允許你快速地存儲、搜索和分析大量數據。
- 主要操作包括建立索引（儲存數據）、執行查詢（檢索數據）、以及使用聚合功能進行數據分析。

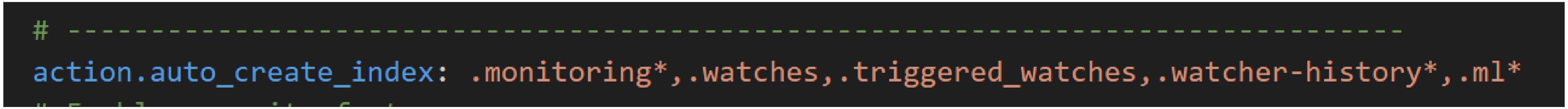
Elasticsearch 的應用案例

- 日誌分析：利用Elasticsearch存儲和分析來自多個來源的日誌數據，以便於快速定位系統問題和性能瓶頸。
- 全文搜索：在網站或應用中實現快速且高度可定制的搜索功能。
- 實時數據分析：對來自業務應用的數據進行即時分析，以支持決策制定。

設定檔調整



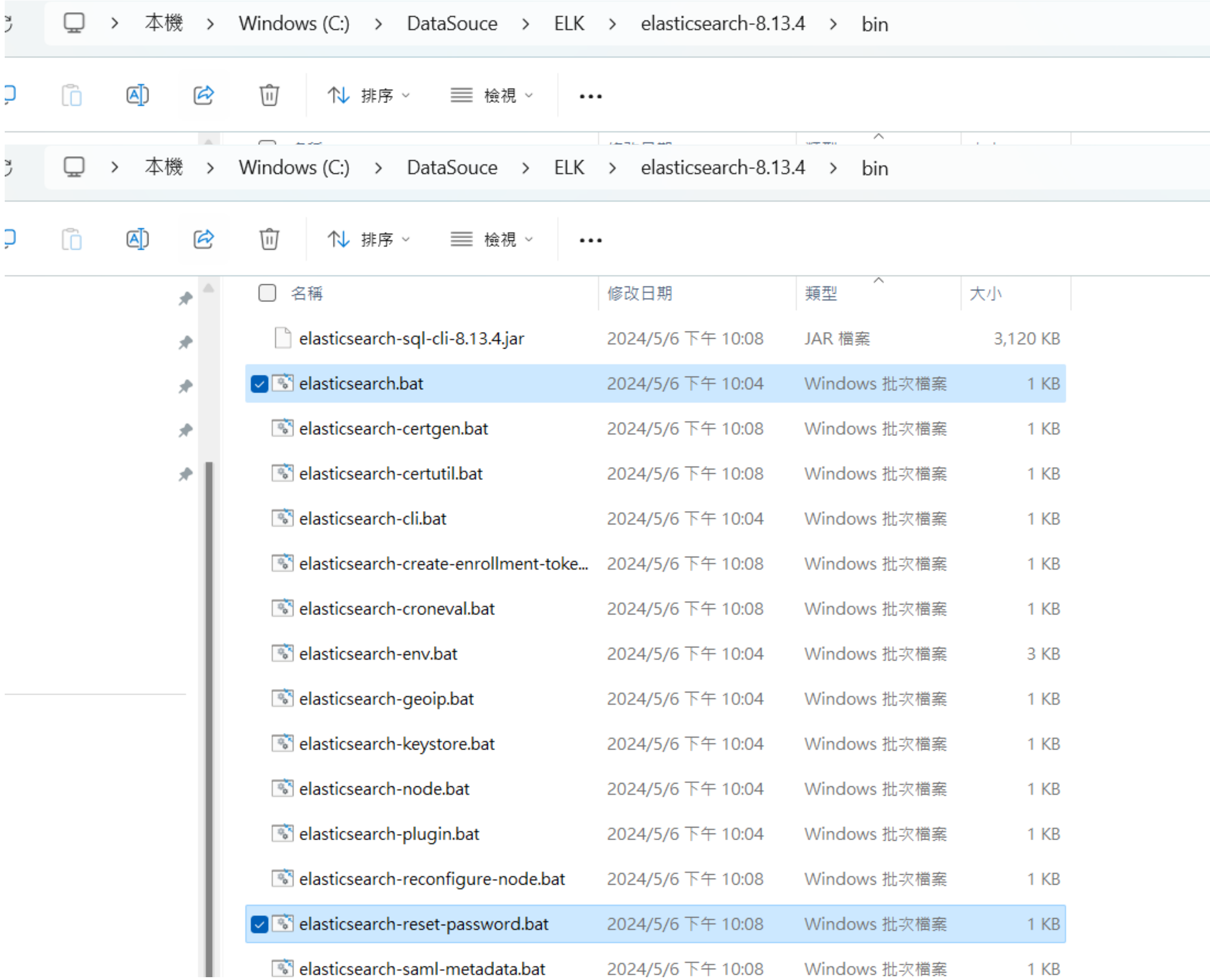
```
# Enable encryption for HTTP API client connections, such as Kibana, Logstash, and Agents
xpack.security.http.ssl:
  enabled: false
  keystore.path: certs/http.p12

# Enable encryption and mutual authentication between cluster nodes
xpack.security.transport.ssl:
  enabled: false
  verification_mode: certificate
  keystore.path: certs/transport.p12
  truststore.path: certs/transport.p12
```



```
# --------------------------------------------------------------------------------
action.auto_create_index: .monitoring*,.watches,.triggered_watches,.watcher-history*,.ml*
```

action.auto_create_index: .monitoring*,.watches,.triggered_watches,.watcher-history*,.ml*

啟動服務

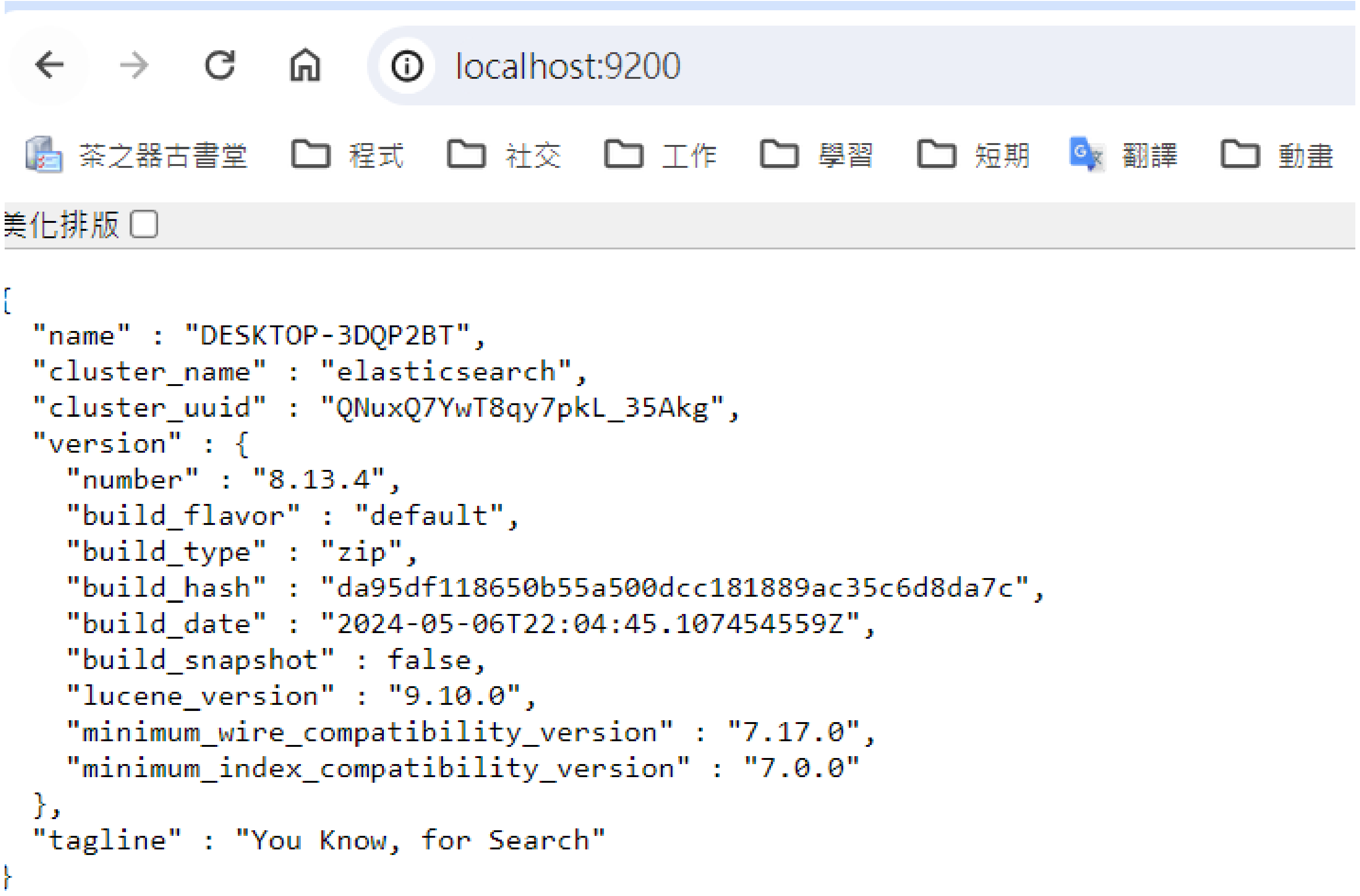


本機 > Windows (C:) > DataSouce > ELK > elasticsearch-8.13.4 > bin

本機 > Windows (C:) > DataSouce > ELK > elasticsearch-8.13.4 > bin

□	名稱	修改日期	類型	大小
	elasticsearch-sql-cli-8.13.4.jar	2024/5/6 下午 10:08	JAR 檔案	3,120 KB
☑	elasticsearch.bat	2024/5/6 下午 10:04	Windows 批次檔案	1 KB
	elasticsearch-certgen.bat	2024/5/6 下午 10:08	Windows 批次檔案	1 KB
	elasticsearch-certutil.bat	2024/5/6 下午 10:08	Windows 批次檔案	1 KB
	elasticsearch-cli.bat	2024/5/6 下午 10:04	Windows 批次檔案	1 KB
	elasticsearch-create-enrollment-toke...	2024/5/6 下午 10:08	Windows 批次檔案	1 KB
	elasticsearch-croneval.bat	2024/5/6 下午 10:08	Windows 批次檔案	1 KB
	elasticsearch-env.bat	2024/5/6 下午 10:04	Windows 批次檔案	3 KB
	elasticsearch-geoip.bat	2024/5/6 下午 10:04	Windows 批次檔案	1 KB
	elasticsearch-keystore.bat	2024/5/6 下午 10:04	Windows 批次檔案	1 KB
	elasticsearch-node.bat	2024/5/6 下午 10:04	Windows 批次檔案	1 KB
	elasticsearch-plugin.bat	2024/5/6 下午 10:04	Windows 批次檔案	1 KB
	elasticsearch-reconfigure-node.bat	2024/5/6 下午 10:08	Windows 批次檔案	1 KB
☑	elasticsearch-reset-password.bat	2024/5/6 下午 10:08	Windows 批次檔案	1 KB
	elasticsearch-saml-metadata.bat	2024/5/6 下午 10:08	Windows 批次檔案	1 KB

啟動成功



美化排版 □

```
{
  "name" : "DESKTOP-3DQP2BT",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "QNuxQ7YwT8qy7pkL_35Akg",
  "version" : {
    "number" : "8.13.4",
    "build_flavor" : "default",
    "build_type" : "zip",
    "build_hash" : "da95df118650b55a500dcc181889ac35c6d8da7c",
    "build_date" : "2024-05-06T22:04:45.107454559Z",
    "build_snapshot" : false,
    "lucene_version" : "9.10.0",
    "minimum_wire_compatibility_version" : "7.17.0",
    "minimum_index_compatibility_version" : "7.0.0"
  },
  "tagline" : "You Know, for Search"
}
```

Logstash

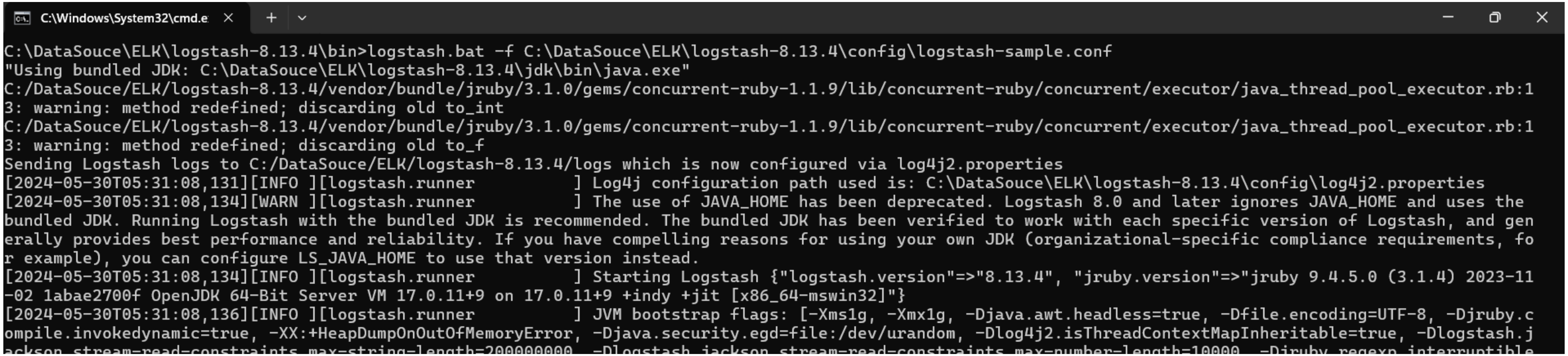
Logstash 簡介

- Logstash是一個開源的服務器端數據處理管道，可以同時從多個來源攝取數據，轉換數據，然後將數據發送到你指定的存儲庫。
- 主要用於數據收集、數據轉換（如格式化、添加字段）、以及數據輸出到Elasticsearch或其他存儲系統。

Logstash 配置與實戰

- 配置文件通常包括input、filter和output三部分。通過不同的插件可以定制處理的流程。
- 實例：設置Logstash來分析Apache服務器的日誌，並將處理過的數據輸出到Elasticsearch。

啟動服務

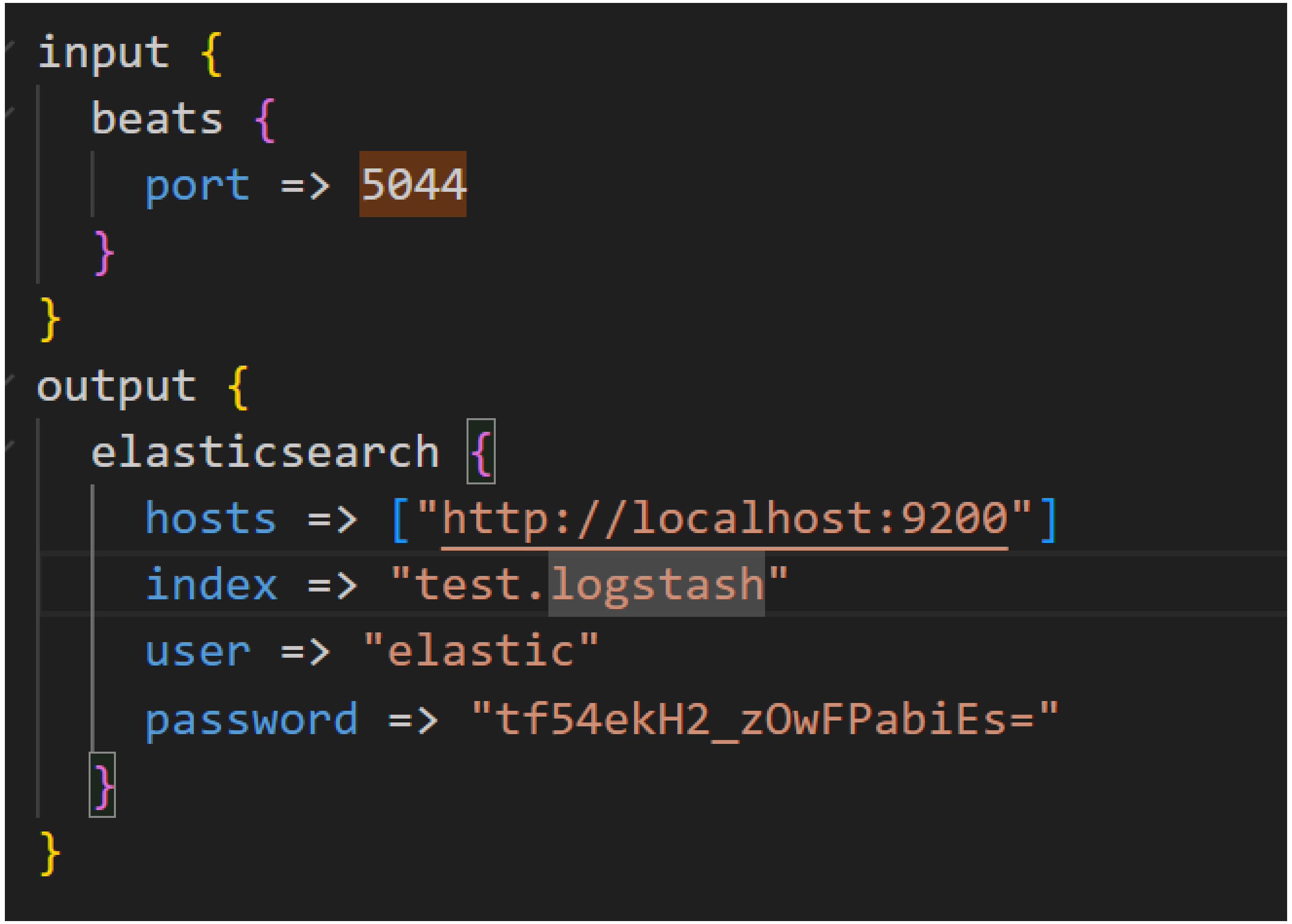


```
C:\DataSouce\ELK\logstash-8.13.4\bin>logstash.bat -f C:\DataSouce\ELK\logstash-8.13.4\config\logstash-sample.conf
"Using bundled JDK: C:\DataSouce\ELK\logstash-8.13.4\jdk\bin\java.exe"
C:/DataSouce/ELK/logstash-8.13.4/vendor/bundle/jruby/3.1.0/gems/concurrent-ruby-1.1.9/lib/concurrent-ruby/concurrent/executor/java_thread_pool_executor.rb:1
3: warning: method redefined; discarding old to_int
C:/DataSouce/ELK/logstash-8.13.4/vendor/bundle/jruby/3.1.0/gems/concurrent-ruby-1.1.9/lib/concurrent-ruby/concurrent/executor/java_thread_pool_executor.rb:1
3: warning: method redefined; discarding old to_f
Sending Logstash logs to C:/DataSouce/ELK/logstash-8.13.4/logs which is now configured via log4j2.properties
[2024-05-30T05:31:08,131][INFO ][logstash.runner          ] Log4j configuration path used is: C:\DataSouce\ELK\logstash-8.13.4\config\log4j2.properties
[2024-05-30T05:31:08,134][WARN ][logstash.runner          ] The use of JAVA_HOME has been deprecated. Logstash 8.0 and later ignores JAVA_HOME and uses the
bundled JDK. Running Logstash with the bundled JDK is recommended. The bundled JDK has been verified to work with each specific version of Logstash, and gen
erally provides best performance and reliability. If you have compelling reasons for using your own JDK (organizational-specific compliance requirements, fo
r example), you can configure LS_JAVA_HOME to use that version instead.
[2024-05-30T05:31:08,134][INFO ][logstash.runner          ] Starting Logstash {"logstash.version"=>"8.13.4", "jruby.version"=>"jruby 9.4.5.0 (3.1.4) 2023-11
-02 1abae2700f OpenJDK 64-Bit Server VM 17.0.11+9 on 17.0.11+9 +indy +jit [x86_64-mswin32]"}
[2024-05-30T05:31:08,136][INFO ][logstash.runner          ] JVM bootstrap flags: [-Xms1g, -Xmx1g, -Djava.awt.headless=true, -Dfile.encoding=UTF-8, -Djruby.c
ompile.invokedynamic=true, -XX:+HeapDumpOnOutOfMemoryError, -Djava.security.egd=file:/dev/urandom, -Dlog4j2.isThreadContextMapInheritable=true, -Dlogstash.j
ackson.stream-read-constraints.max-string-length=200000000, -Dlogstash.jackson.stream-read-constraints.max-number-length=10000, -Djruby.regexp.interruptible
```

CMD :
logstash.bat -f C:\DataSouce\ELK\logstash-.13.4\config\logstash-sample.conf

logstash.bat -f C:\DataSouce\ELK\logstash-.13.4\config\logstash-sample.conf

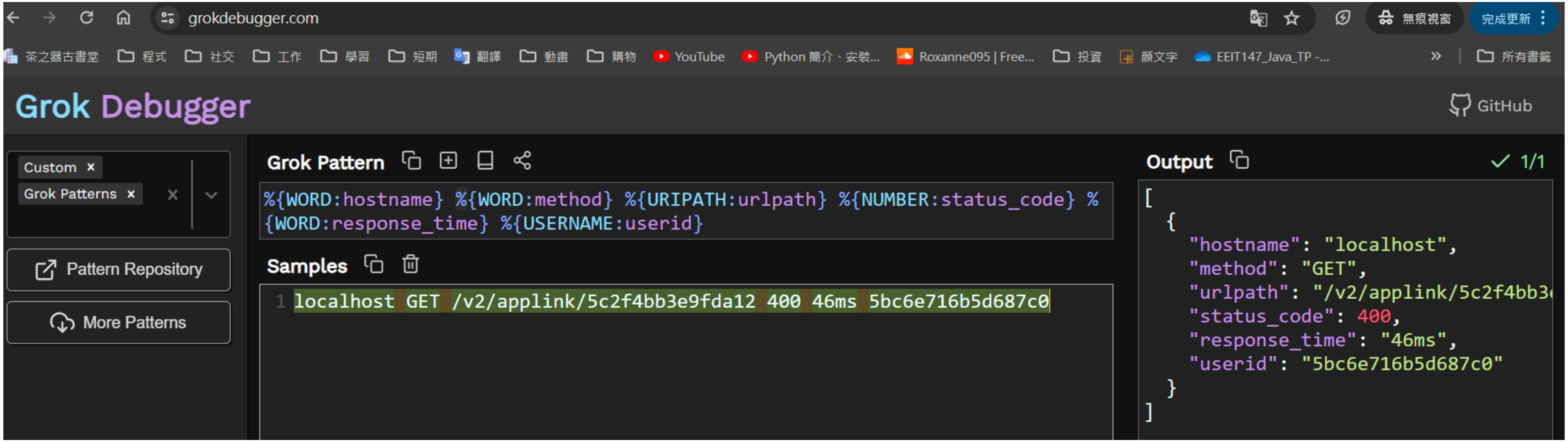
設定檔調整



```
input {
  beats {
    port => 5044
  }
}
output {
  elasticsearch {
    hosts => ["http://localhost:9200"]
    index => "test.logstash"
    user => "elastic"
    password => "tf54ekH2_zOwFPabiEs="
  }
}
```

https://grokdebugger.com/

Grok_debugger

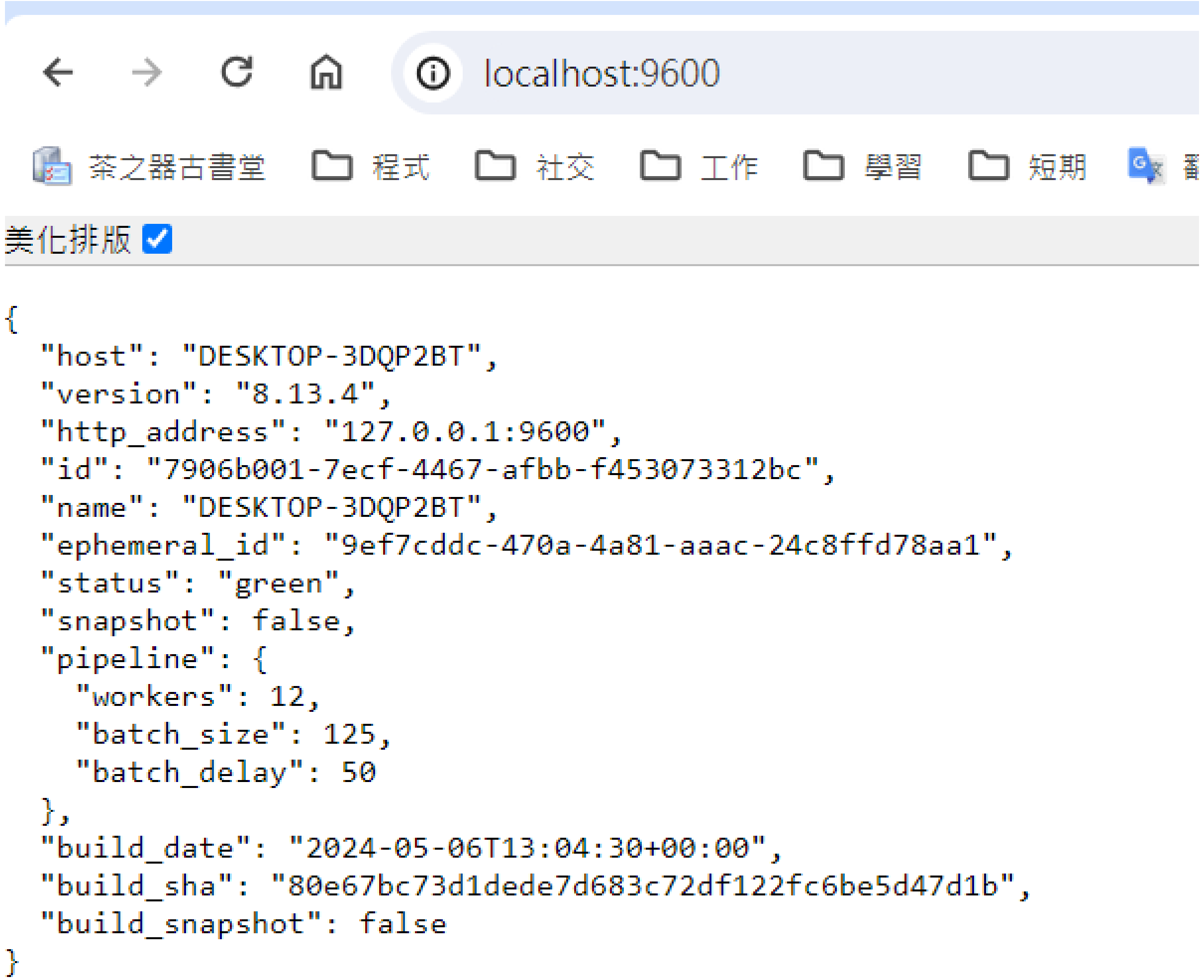


```
%{WORD:hostname} %{WORD:method} %{URIPATH:urlpath} %{NUMBER:status_code} %
{WORD:response_time} %{USERNAME:userid}
```

```
localhost GET /v2/applink/5c2f4bb3e9fda12 400 46ms 5bc6e716b5d687c0
```

```
[
  {
    "hostname": "localhost",
    "method": "GET",
    "urlpath": "/v2/applink/5c2f4bb3
    "status_code": 400,
    "response_time": "46ms",
    "userid": "5bc6e716b5d687c0"
  }
]
```

啟動成功



美化排版 ☑

```
{
  "host": "DESKTOP-3DQP2BT",
  "version": "8.13.4",
  "http_address": "127.0.0.1:9600",
  "id": "7906b001-7ecf-4467-afbb-f453073312bc",
  "name": "DESKTOP-3DQP2BT",
  "ephemeral_id": "9ef7cddc-470a-4a81-aaac-24c8ffd78aa1",
  "status": "green",
  "snapshot": false,
  "pipeline": {
    "workers": 12,
    "batch_size": 125,
    "batch_delay": 50
  },
  "build_date": "2024-05-06T13:04:30+00:00",
  "build_sha": "80e67bc73d1dede7d683c72df122fc6be5d47d1b",
  "build_snapshot": false
}
```

Kibana

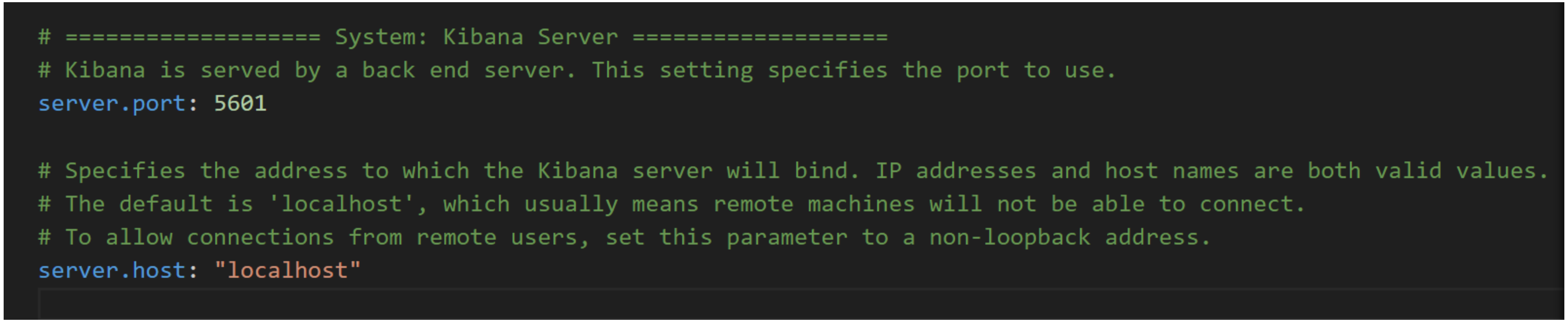
Kibana 簡介

- Kibana是一個開源的數據可視化平台，專為Elasticsearch設計。用戶可以通過Kibana來創建圖表、地圖和儀表板。
- Kibana使數據探索、可視化和分析變得直觀易懂，支持從基本的圖表到複雜的地理空間數據分析。

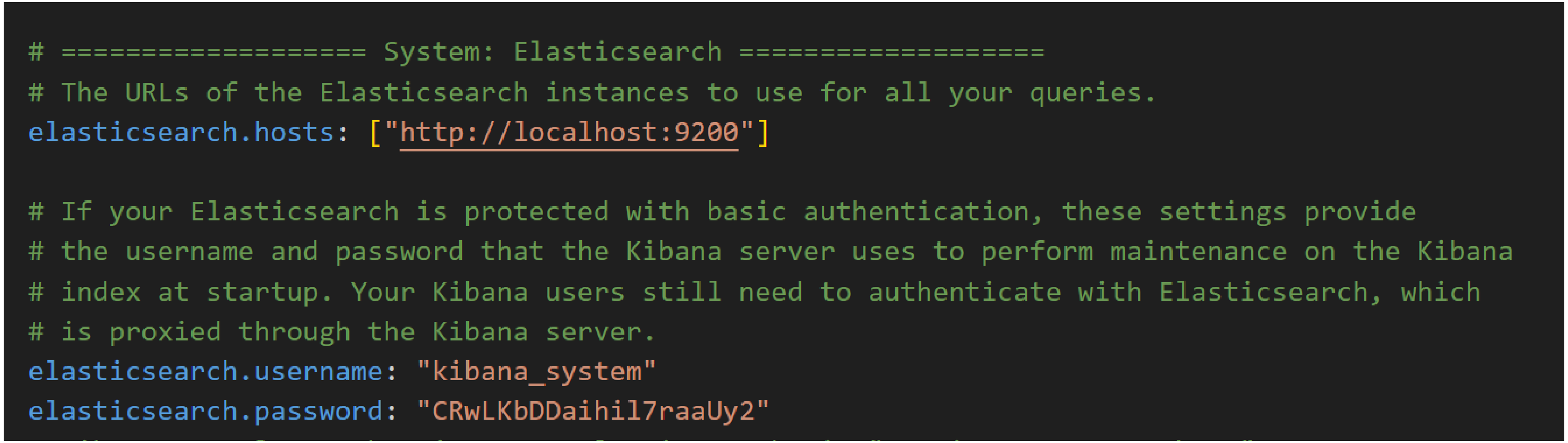
Kibana 的實用技巧

- 建立儀表板：選擇適當的視覺化組件，配置數據源，設計互動和實時更新的儀表板。
- 數據探索與視覺化案例：使用Kibana來分析銷售數據，展示不同地區的銷

設定檔調整

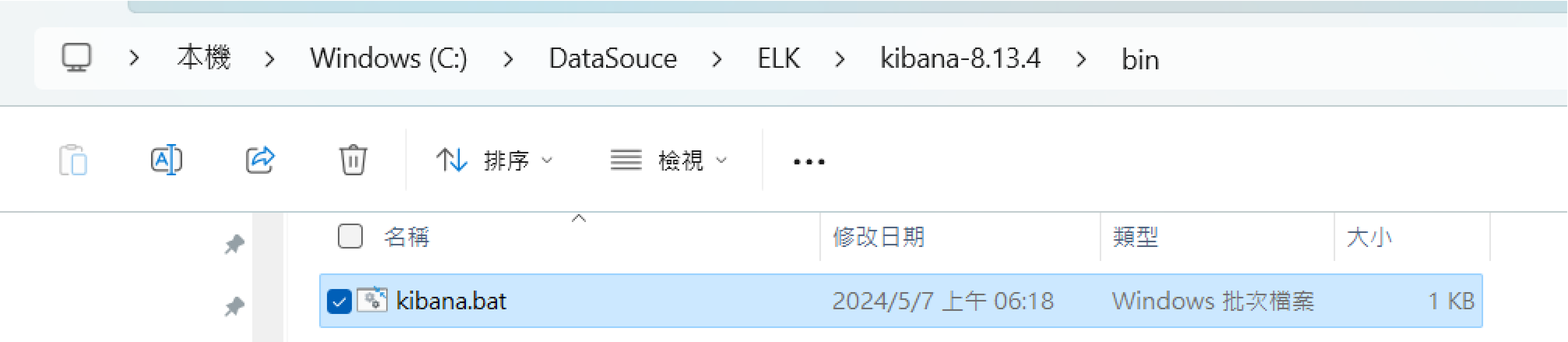


```
# ================== System: Kibana Server ===================
# Kibana is served by a back end server. This setting specifies the port to use.
server.port: 5601

# Specifies the address to which the Kibana server will bind. IP addresses and host names are both valid values.
# The default is 'localhost', which usually means remote machines will not be able to connect.
# To allow connections from remote users, set this parameter to a non-loopback address.
server.host: "localhost"
```



```
# =================== System: Elasticsearch ===================
# The URLs of the Elasticsearch instances to use for all your queries.
elasticsearch.hosts: ["http://localhost:9200"]

# 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: "kibana_system"
elasticsearch.password: "CRwLKbDDaihil7raaUy2"
```

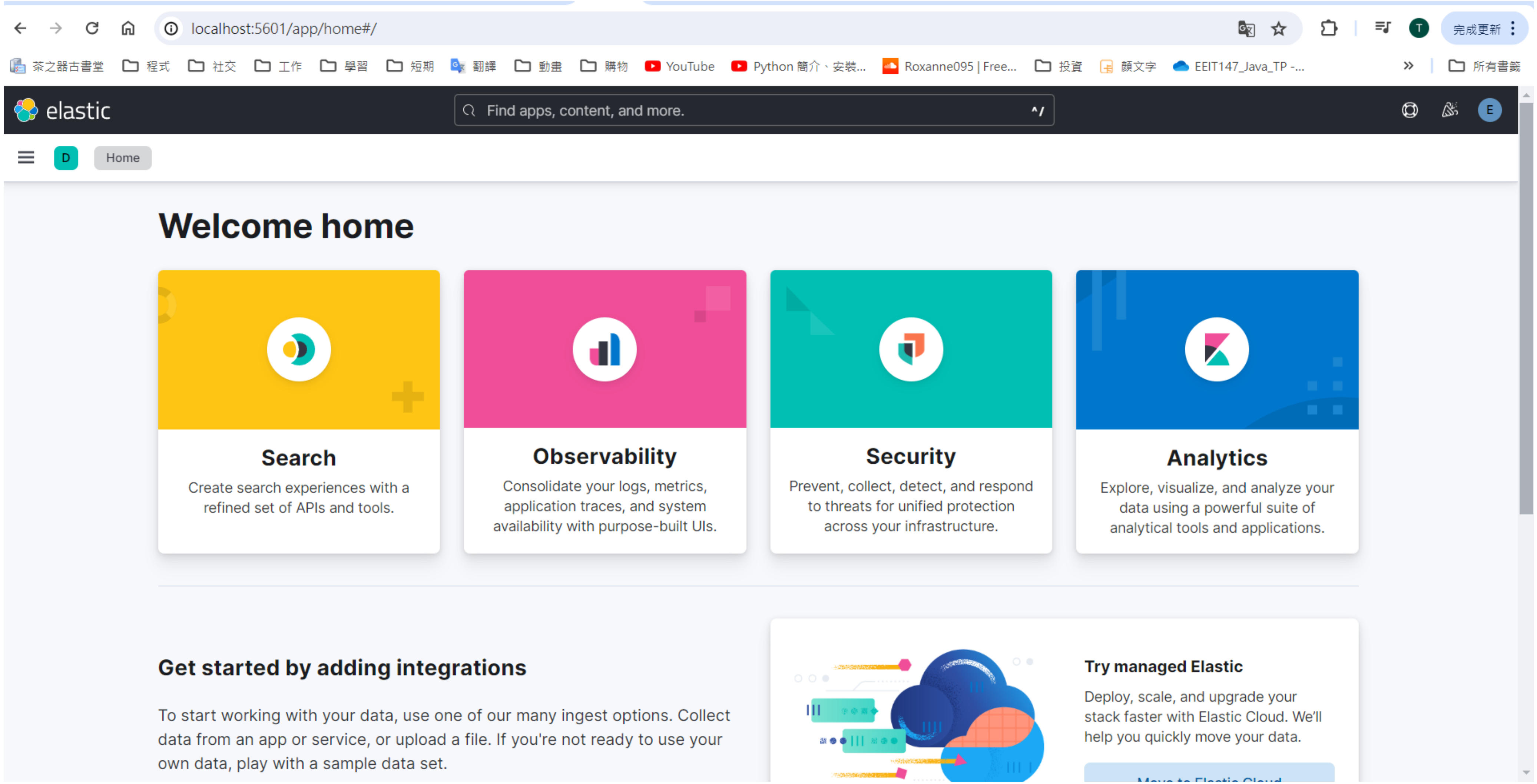
啟動服務



本機 > Windows (C:) > DataSouce > ELK > kibana-8.13.4 > bin

名稱	修改日期	類型	大小
☑ kibana.bat	2024/5/7 上午 06:18	Windows 批次檔案	1 KB

啟動成功



Welcome home

Search

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

Observability

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

Security

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

Analytics

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

Get started by adding integrations

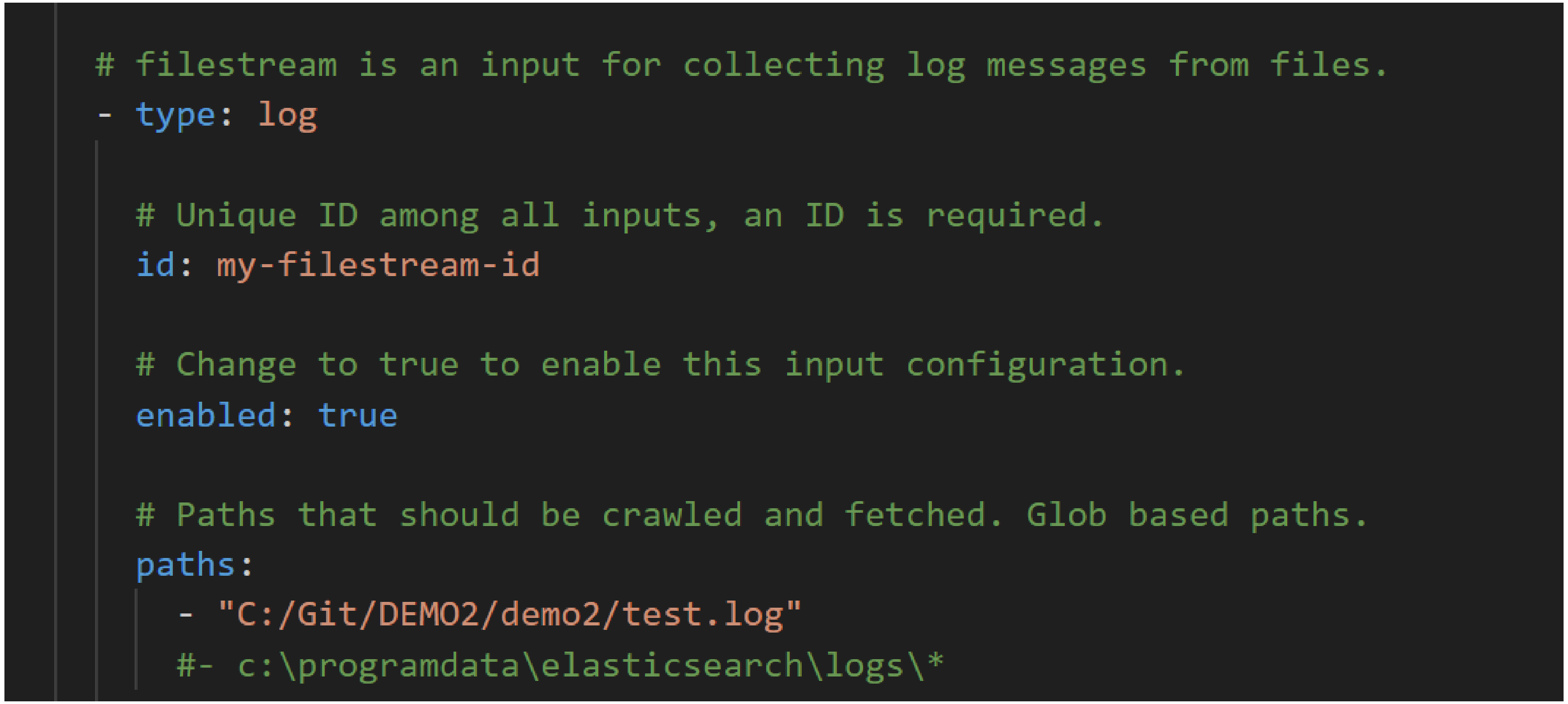
To start working with your data, use one of our many ingest options. Collect data from an app or service, or upload a file. If you're not ready to use your own data, play with a sample data set.

Try managed Elastic

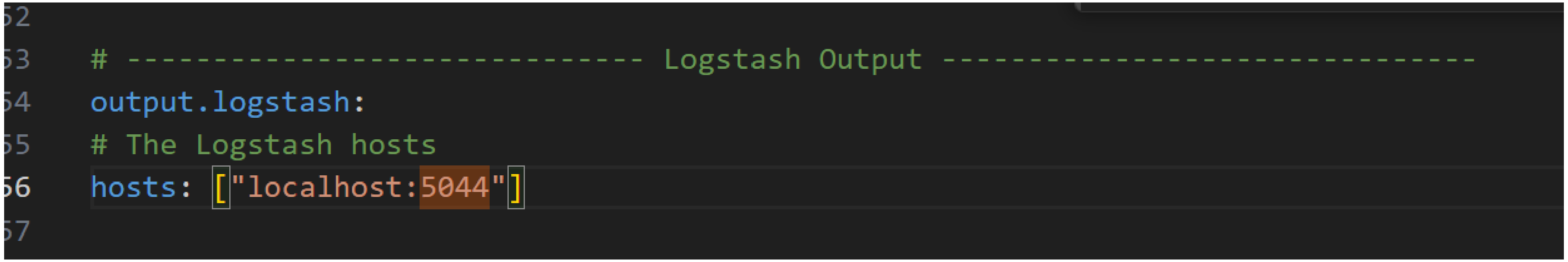
Deploy, scale, and upgrade your stack faster with Elastic Cloud. We'll help you quickly move your data.

Beats

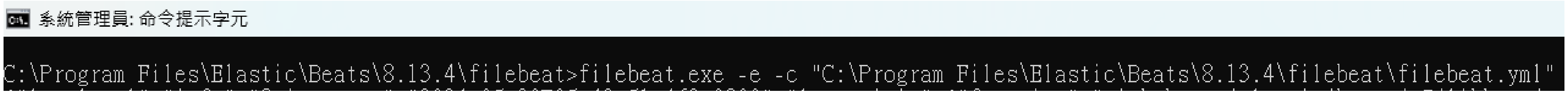
- 在 Elastic Stack 中，Beats 是一組輕量級的單一用途數據收集器。它們主要用於將各種類型的數據發送到 Elasticsearch。
  - Filebeat：專門用於收集和轉發日誌文件。
  - Metricbeat：用於定期收集系統和服務的度量數據。
  - Packetbeat：是一個網絡數據包分析器
  - Heartbeat：用於定期檢查系統服務的可用性。
  - Auditbeat：專注於安全審計，可以收集和報告機器上的文件完整性信息和安全相關的事件，如用戶登錄和新進程的創建。
  - Winlogbeat：針對 Windows 平台，用於收集 Windows 事件日誌。Functionbeat：專門用於在服務器無環境（如 AWS Lambda）中運行，收集和轉發來自雲原生服務（例如，AWS、Azure 或 GCP 中的日誌和事件）的數據。



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

  # 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:
    - "C:/Git/DEMO2/demo2/test.log"
    #- c:\programdata\elasticsearch\logs\*
```



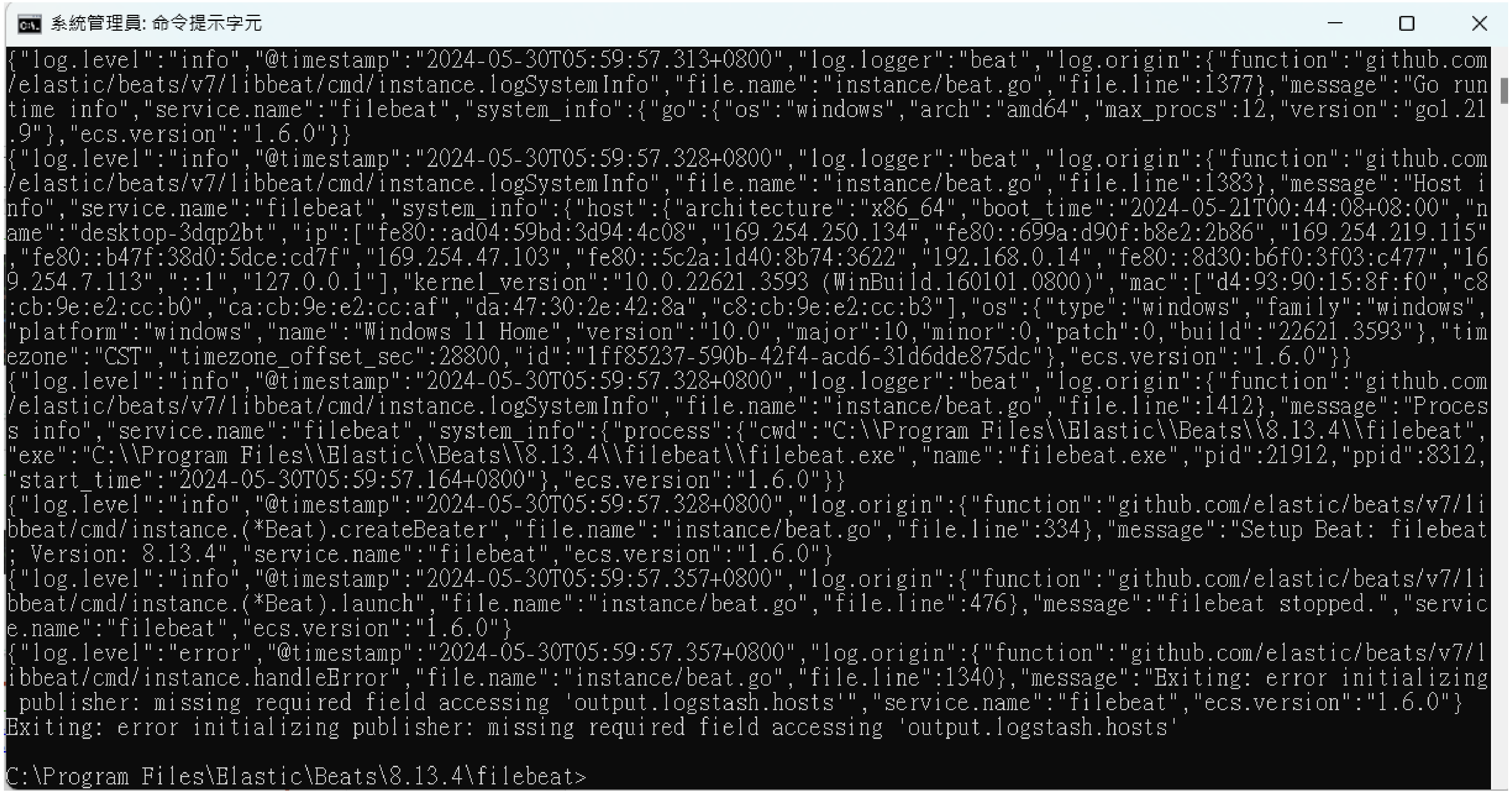
```
# ------------------------------ Logstash Output -------------------------------
output.logstash:
# The Logstash hosts
hosts: ["localhost:5044"]
```



```
C:\Program Files\Elastic\Beats\8.13.4\filebeat>filebeat.exe -e -c "C:\Program Files\Elastic\Beats\8.13.4\filebeat\filebeat.yml"
```

```
C:\Program Files\Elastic\Beats\8.13.4\filebeat>filebeat.exe -e –c "C:\ProgramFiles\Elastic\Beats\8.13.4\filebeat\filebeat.yml"
```

爬 LOG 生效



```
{"log.level":"info","@timestamp":"2024-05-30T05:59:57.313+0800","log.logger":"beat","log.origin":{"function":"github.com
/elastic/beats/v7/libbeat/cmd/instance.logSystemInfo","file.name":"instance/beat.go","file.line":1377},"message":"Go run
time info","service.name":"filebeat","system_info":{"go":{"os":"windows","arch":"amd64","max_procs":12,"version":"go1.21
.9"},"ecs.version":"1.6.0"}}
{"log.level":"info","@timestamp":"2024-05-30T05:59:57.328+0800","log.logger":"beat","log.origin":{"function":"github.com
/elastic/beats/v7/libbeat/cmd/instance.logSystemInfo","file.name":"instance/beat.go","file.line":1383},"message":"Host i
nfo","service.name":"filebeat","system_info":{"host":{"architecture":"x86_64","boot_time":"2024-05-21T00:44:08+08:00","n
ame":"desktop-3dqp2bt","ip":["fe80::ad04:59bd:3d94:4c08","169.254.250.134","fe80::699a:d90f:b8e2:2b86","169.254.219.115"
,"fe80::b47f:38d0:5dce:cd7f","169.254.47.103","fe80::5c2a:1d40:8b74:3622","192.168.0.14","fe80::8d30:b6f0:3f03:c477","16
9.254.7.113","::1","127.0.0.1"],"kernel_version":"10.0.22621.3593 (WinBuild.160101.0800)","mac":["d4:93:90:15:8f:f0","c8
:cb:9e:e2:cc:b0","ca:cb:9e:e2:cc:af","da:47:30:2e:42:8a","c8:cb:9e:e2:cc:b3"],"os":{"type":"windows","family":"windows",
"platform":"windows","name":"Windows 11 Home","version":"10.0","major":10,"minor":0,"patch":0,"build":"22621.3593"},"tim
ezone":"CST","timezone_offset_sec":28800,"id":"1ff85237-590b-42f4-acd6-31d6dde875dc"},"ecs.version":"1.6.0"}}
{"log.level":"info","@timestamp":"2024-05-30T05:59:57.328+0800","log.logger":"beat","log.origin":{"function":"github.com
/elastic/beats/v7/libbeat/cmd/instance.logSystemInfo","file.name":"instance/beat.go","file.line":1412},"message":"Proces
s info","service.name":"filebeat","system_info":{"process":{"cwd":"C:\\Program Files\\Elastic\\Beats\\8.13.4\\filebeat",
"exe":"C:\\Program Files\\Elastic\\Beats\\8.13.4\\filebeat\\filebeat.exe","name":"filebeat.exe","pid":21912,"ppid":8312,
"start_time":"2024-05-30T05:59:57.164+0800"},"ecs.version":"1.6.0"}}
{"log.level":"info","@timestamp":"2024-05-30T05:59:57.328+0800","log.origin":{"function":"github.com/elastic/beats/v7/li
bbeat/cmd/instance.(*Beat).createBeater","file.name":"instance/beat.go","file.line":334},"message":"Setup Beat: filebeat
; Version: 8.13.4","service.name":"filebeat","ecs.version":"1.6.0"}
{"log.level":"info","@timestamp":"2024-05-30T05:59:57.357+0800","log.origin":{"function":"github.com/elastic/beats/v7/li
bbeat/cmd/instance.(*Beat).launch","file.name":"instance/beat.go","file.line":476},"message":"filebeat stopped.","servic
e.name":"filebeat","ecs.version":"1.6.0"}
{"log.level":"error","@timestamp":"2024-05-30T05:59:57.357+0800","log.origin":{"function":"github.com/elastic/beats/v7/l
ibbeat/cmd/instance.handleError","file.name":"instance/beat.go","file.line":1340},"message":"Exiting: error initializing
 publisher: missing required field accessing 'output.logstash.hosts'","service.name":"filebeat","ecs.version":"1.6.0"}
Exiting: error initializing publisher: missing required field accessing 'output.logstash.hosts'

C:\Program Files\Elastic\Beats\8.13.4\filebeat>
```

參考資源

- 【日志&运维】ELK日志采集系统介绍
- Easy Step by Step guide on how to Install Elastic, Kibana, and Log stash Stack 8.3 on Windows 10