



# Elasticsearch AI 與 ML 的說明與運用



講師:陳俊佑  
集先鋒科技有限公司



# Elasticsearch 基礎說明

---

# Elasticsearch 是什麼?

ElasticSearch 是一款非常強大的、基於 Lucene 的開源搜尋及分析引擎，可以幫助你從海量資料中，快速找到相關的資料資訊

分散式儲存

高拓展性

高安全性

高效檢索

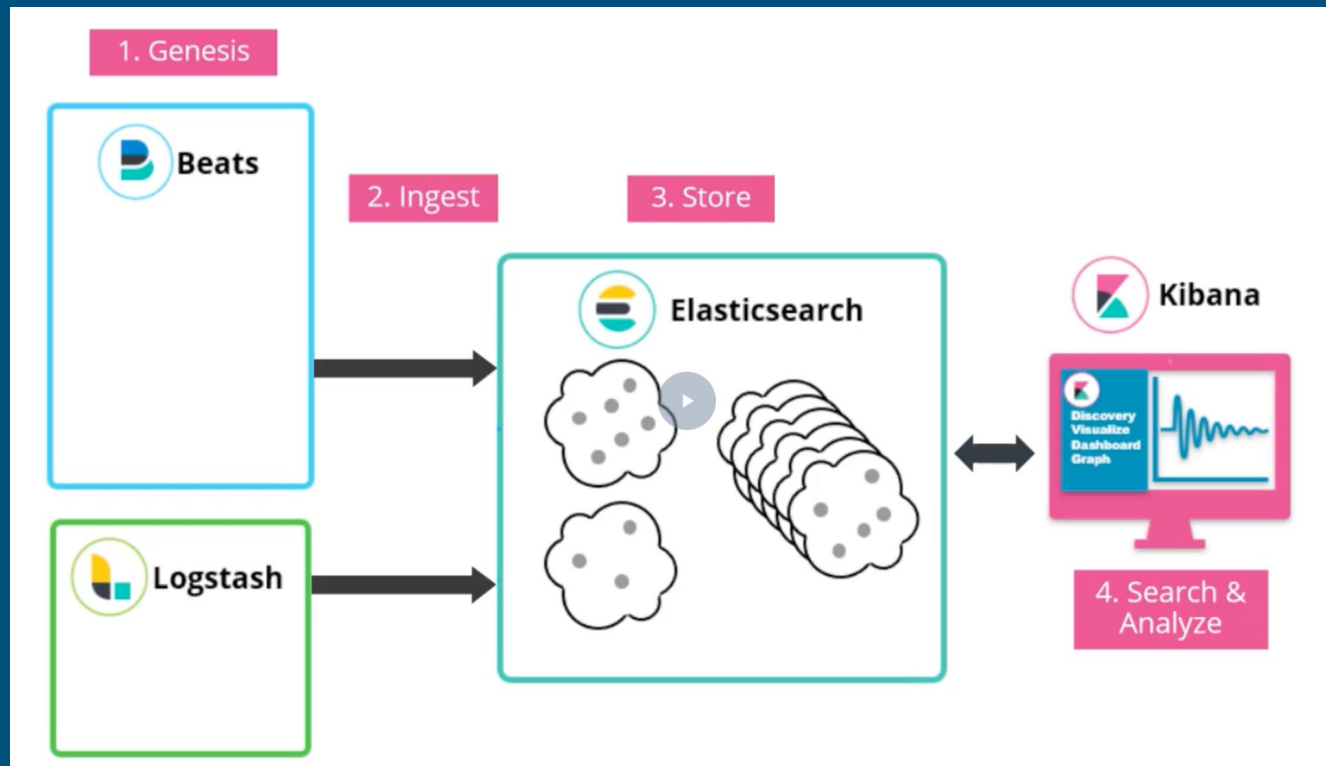
多語種查詢

多租戶技術

Schema Free

RESTful API

# 什麼是 ELK?



# Elasticsearch 排名

include secondary database models

21 systems in ranking, December 2020

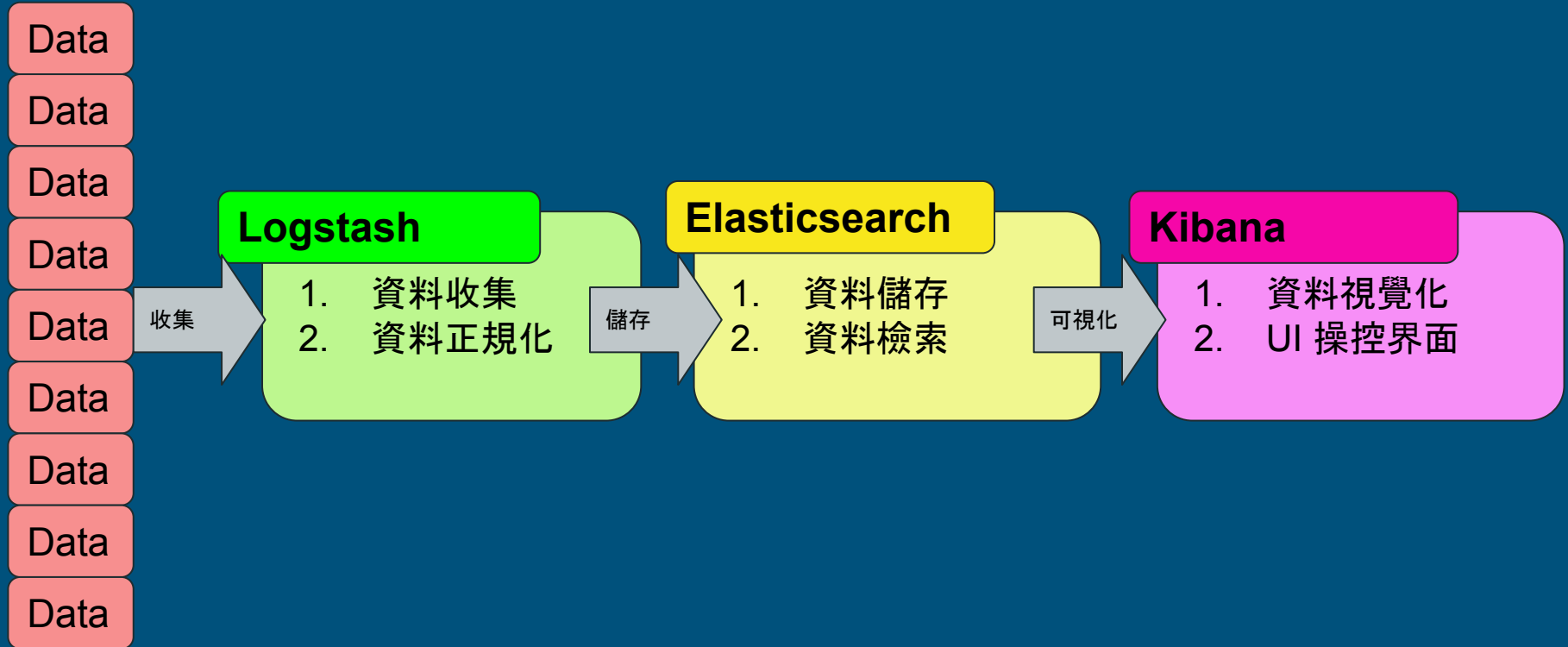
Rank			DBMS	Database Model	Score		
Dec 2020	Nov 2020	Dec 2019			Dec 2020	Nov 2020	Dec 2019
1.	1.	1.	Elasticsearch <span>+</span>	Search engine, Multi-model <span>f</span>	152.49	+0.94	+2.24
2.	2.	2.	Splunk	Search engine	87.00	-2.71	-3.53
3.	3.	3.	Solr	Search engine	51.24	-0.57	-5.98
4.	4.	4.	MarkLogic <span>+</span>	Multi-model <span>f</span>	10.94	-0.16	-1.53
5.	5.	<span>↑</span> 8.	Algolia	Search engine	7.83	+0.45	+3.15
6.	6.	6.	Microsoft Azure Search	Search engine	6.85	+0.05	+0.56
7.	7.	<span>↓</span> 5.	Sphinx	Search engine	6.32	-0.03	-0.30
8.	8.	<span>↓</span> 7.	ArangoDB <span>+</span>	Multi-model <span>f</span>	5.51	+0.14	+0.64
9.	9.	9.	Amazon CloudSearch	Search engine	3.06	+0.29	-0.15
10.	10.	<span>↑</span> 11.	Virtuoso <span>+</span>	Multi-model <span>f</span>	2.58	+0.05	-0.05
11.	11.	<span>↑</span> 12.	Xapian	Search engine	1.01	+0.17	+0.25
12.	12.	<span>↑</span> 13.	CrateDB <span>+</span>	Multi-model <span>f</span>	0.90	+0.08	+0.28
13.	13.	13.	Alibaba Cloud Log Service <span>+</span>	Search engine	0.40	-0.02	
14.	14.	14.	SearchBlox	Search engine	0.40	+0.01	+0.10
15.	15.	<span>↑</span> 16.	Manticore Search	Search engine	0.07	-0.03	+0.01
16.	16.	<span>↑</span> 20.	Weaviate	Search engine	0.05	-0.03	+0.05
17.	<span>↑</span> 18.	17.	Exorbyte	Search engine	0.03	-0.02	-0.03
18.	<span>↑</span> 19.	<span>↑</span> 19.	FinchDB	Multi-model <span>f</span>	0.03	0.00	+0.00
19.	<span>↓</span> 17.	<span>↓</span> 15.	searchxml	Multi-model <span>f</span>	0.01	-0.05	-0.12
20.	20.	<span>↑</span> 21.	Indica	Search engine	0.00	±0.00	±0.00
20.	20.	20.	Rizhiyi	Search engine, Multi-model <span>f</span>	0.00	±0.00	

include secondary database models

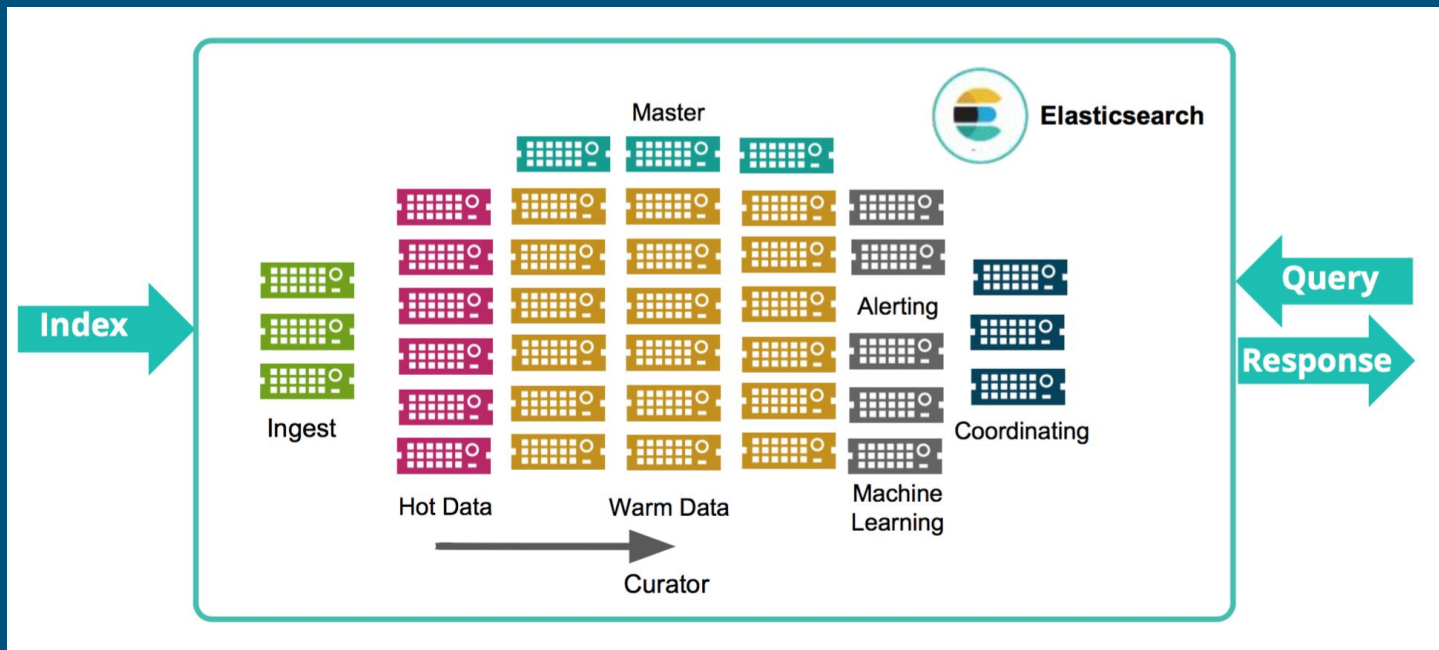
26 systems in ranking, August 2024

Rank			DBMS	Database Model	Score		
Aug 2024	Jul 2024	Aug 2023			Aug 2024	Jul 2024	Aug 2023
1.	1.	1.	Elasticsearch	Search engine, Multi-model <span>f</span>	129.83	-0.99	-10.09
2.	2.	2.	Splunk	Search engine	96.10	+3.18	+7.12
3.	3.	3.	Apache Solr	Search engine, Multi-model <span>f</span>	36.30	-2.58	-11.51
4.	4.	4.	OpenSearch <span>+</span>	Search engine, Multi-model <span>f</span>	16.47	-0.17	+4.03
5.	5.	<span>↑</span> 8.	Sphinx	Search engine	5.97	+0.01	-0.10
6.	<span>↑</span> 7.	6.	Algolia	Search engine	5.77	+0.20	-1.45
7.	<span>↓</span> 6.	7.	Microsoft Azure AI Search	Search engine, Multi-model <span>f</span>	5.73	+0.05	-0.38
8.	8.	<span>↓</span> 5.	MarkLogic	Multi-model <span>f</span>	4.41	-0.02	-4.03
9.	9.	9.	Virtuoso <span>+</span>	Multi-model <span>f</span>	3.85	-0.12	-0.94
10.	10.	10.	ArangoDB <span>+</span>	Multi-model <span>f</span>	3.40	-0.02	-0.97
11.	11.	11.	Coveo	Search engine	2.05	+0.07	-0.50
12.	12.	12.	Amazon CloudSearch	Search engine	1.85	+0.06	-0.32
13.	13.	13.	Meilisearch	Search engine	0.99	+0.02	-0.40
14.	<span>↑</span> 16.	<span>↑</span> 17.	Typesense	Search engine	0.78	+0.08	+0.02
15.	<span>↓</span> 14.	<span>↓</span> 14.	Xapian	Search engine	0.73	-0.02	-0.47
16.	<span>↓</span> 15.	<span>↓</span> 15.	CrateDB	Multi-model <span>f</span>	0.69	-0.03	-0.20
17.	17.	<span>↑</span> 18.	Vespa	Multi-model <span>f</span>	0.59	-0.05	+0.03
18.	18.	<span>↑</span> 20.	Alibaba Cloud Log Service <span>+</span>	Search engine	0.42	+0.05	+0.01
19.	<span>↑</span> 20.	19.	Marqo	Search engine	0.35	+0.05	-0.07
20.	<span>↓</span> 19.	<span>↓</span> 16.	SearchBlox	Search engine	0.32	-0.05	-0.47

# 常規 Elasticsearch 資料處理流程

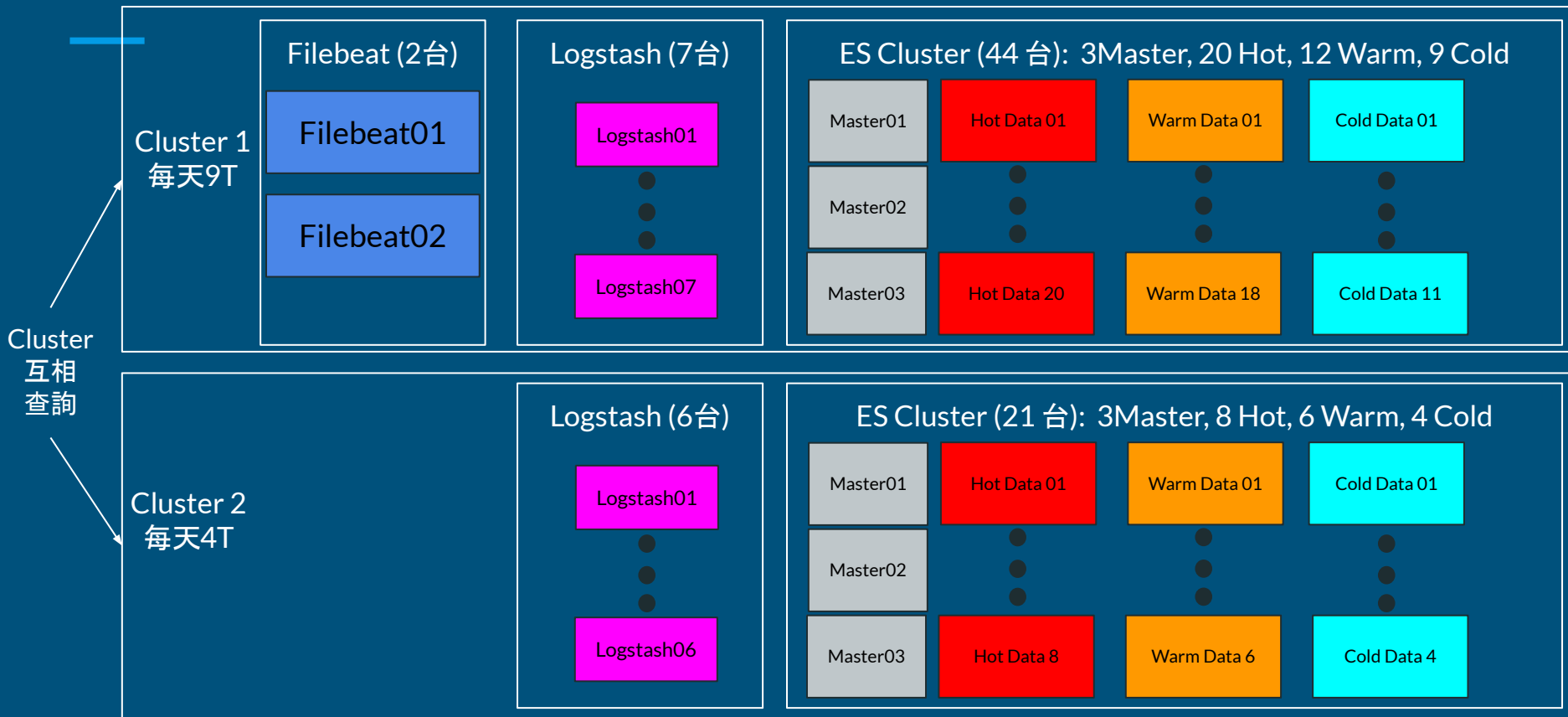


# Elasticsearch 集群架構



# Elasticsearch 集群架構-範例 每天13T的系統架構

Hot 保留30分钟, Warm 保留3天, Cold 保留30天

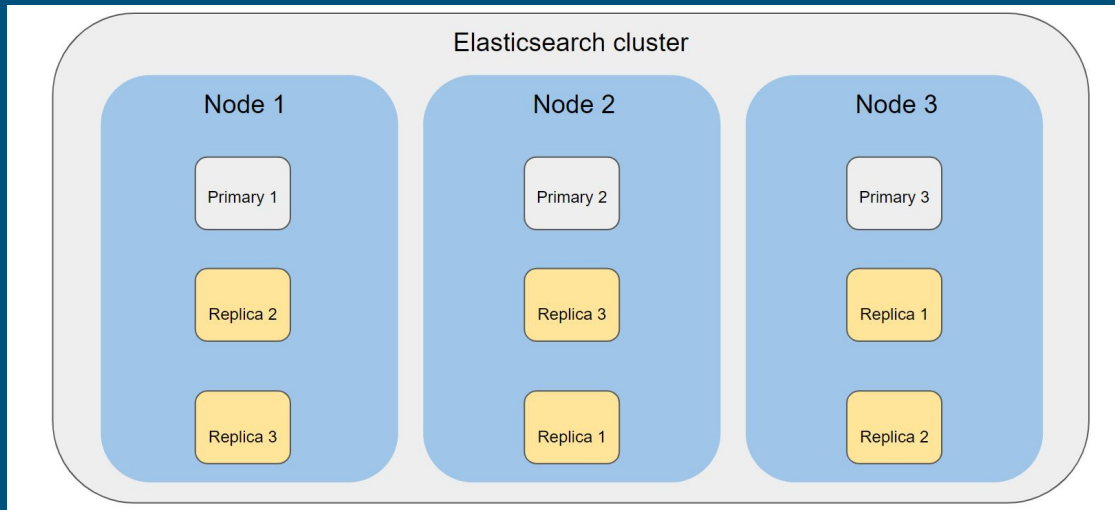




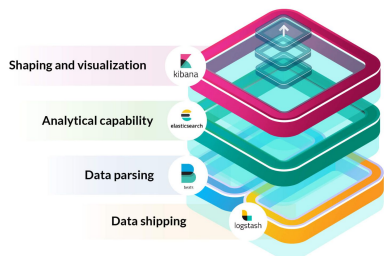
# Elasticsearch 分片與副本

1. 分散式儲存採用了多副本備份機制，其中之一不可用時，可用其他代替
2. primary shard 遺失時，replica shard 就可以被 promote 成 primary shard 來保持資料完整性

範例: 1 Cluster, 3 Node, 3 Primary Shard, 2 Replica



# Elastic stack 中的 beats 大家族



## Beats 系列

全品類採集器，搞定所有數據類型。

### Filebeat

日誌文件



### Metricbeat

指標



### Packetbeat

網絡數據



### Winlogbeat

Windows 事件日誌



### Auditbeat

審計數據



### Heartbeat

運行時間監控



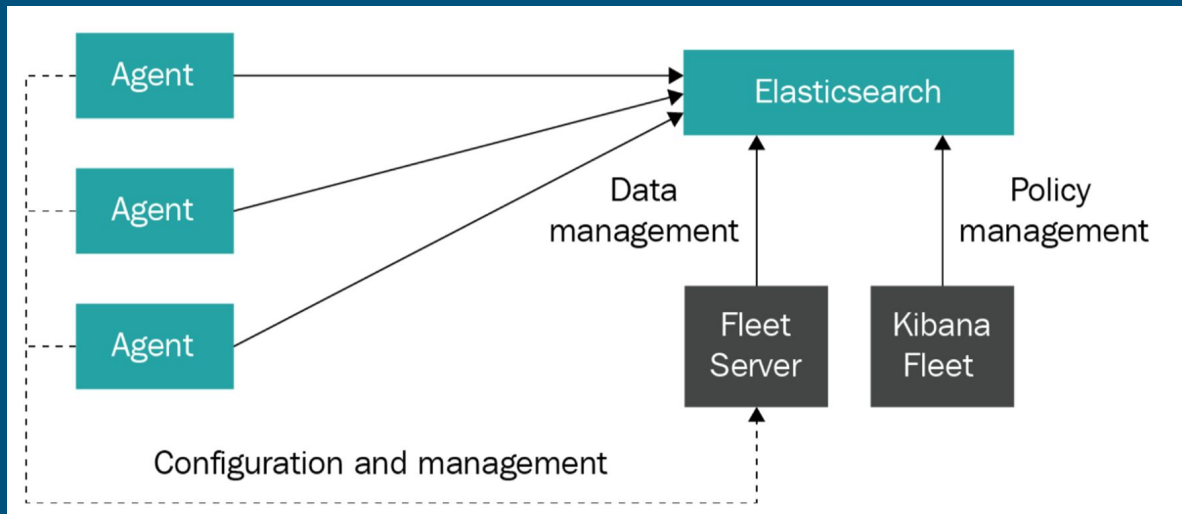
### Functionbeat

無需服務器的採集器



Beats 是一個免費且開放的平台，集合了多種單一用途數據採集器。它們從成百上千或成千上萬台機器和系統向 Logstash 或 Elasticsearch 發送數據

# 通過 Fleet 輕鬆整合資料



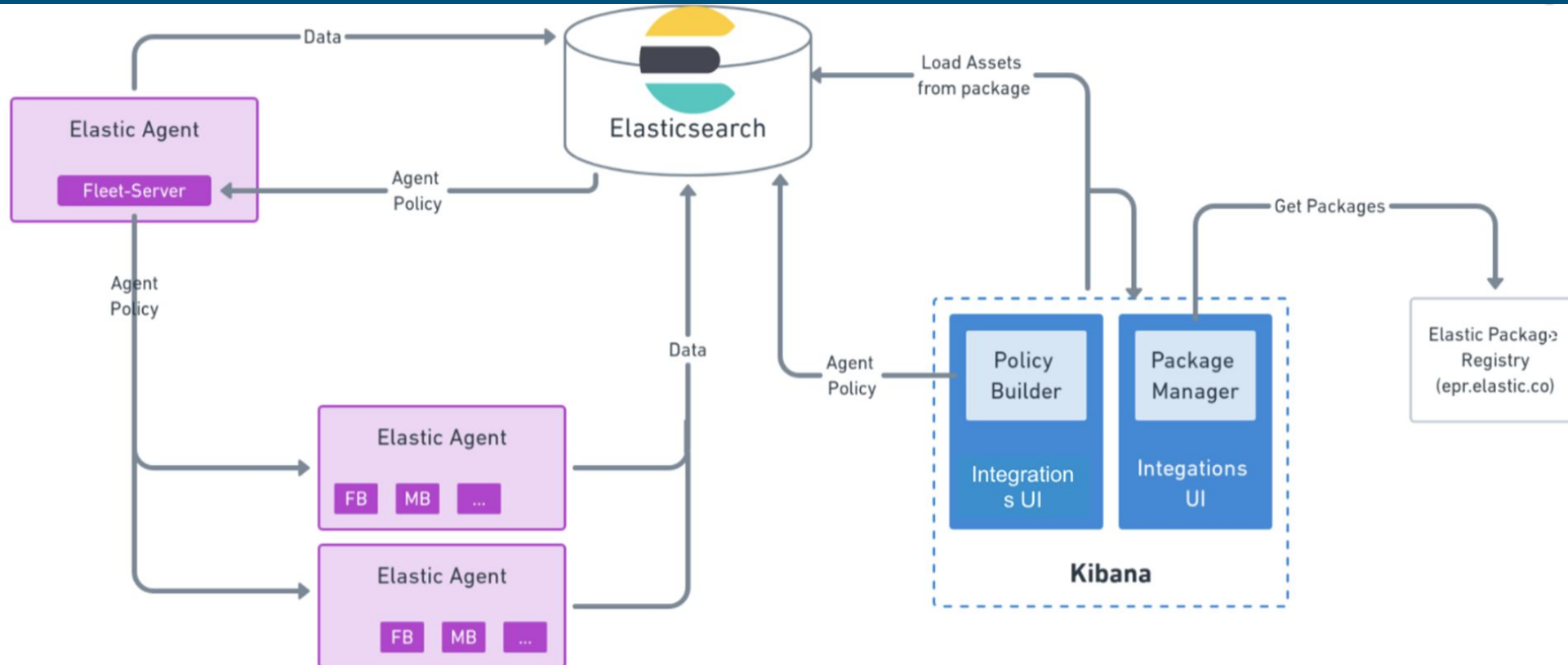
**Fleet:** Agent 的中控平台，負責管理與查看現有環境中的 Elastic Agent 配置，專用的 Elastic Agent 通信主機運行

**Fleet UI:** Kibana 上新的頁面，供使用者載入和配置代理、管理載入資料以及管理整個環境中的代理

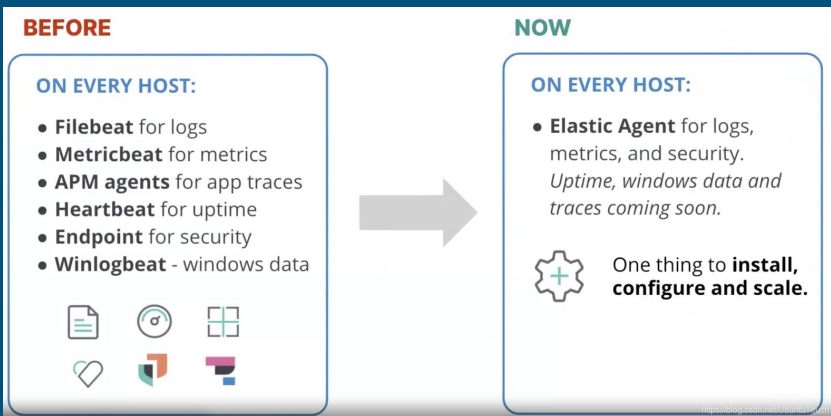
**Fleet Server:** 後端元件，環境中的彈性代理可以連接到該元件，以檢索代理策略、更新和管理命令。

**Elastic Agent:** 將資料直接發送到目標 Elasticsearch 集群

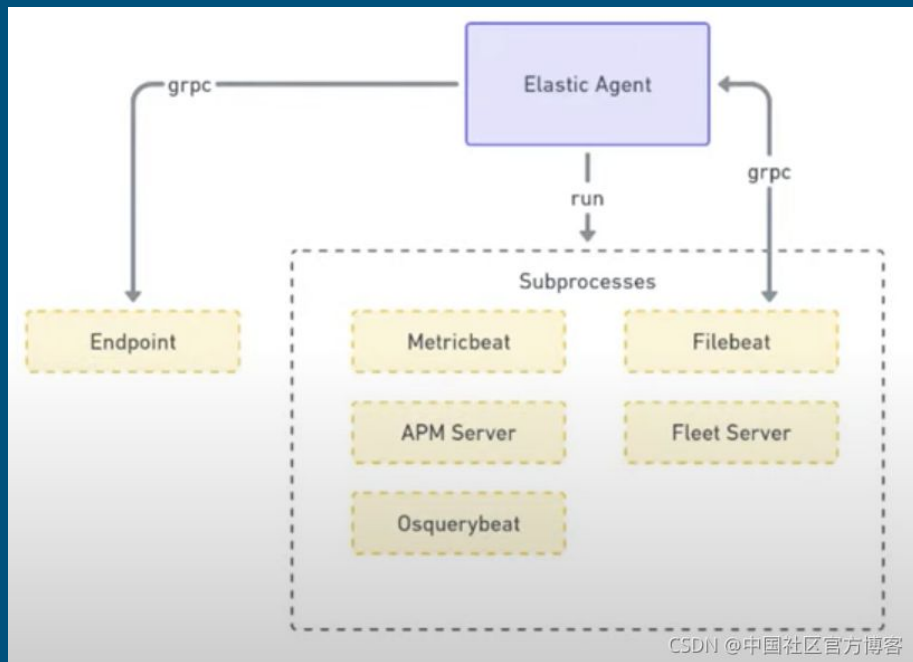
# Fleet & Elastic Agent 組件說明



# Fleet&Elastic Agent 與 Beat 的區別



1. beat現在被統稱為 Elastic Agents
2. Elastic Agent 本質為 beat 的主管



# Fleet & Elastic Agent 的優點

---

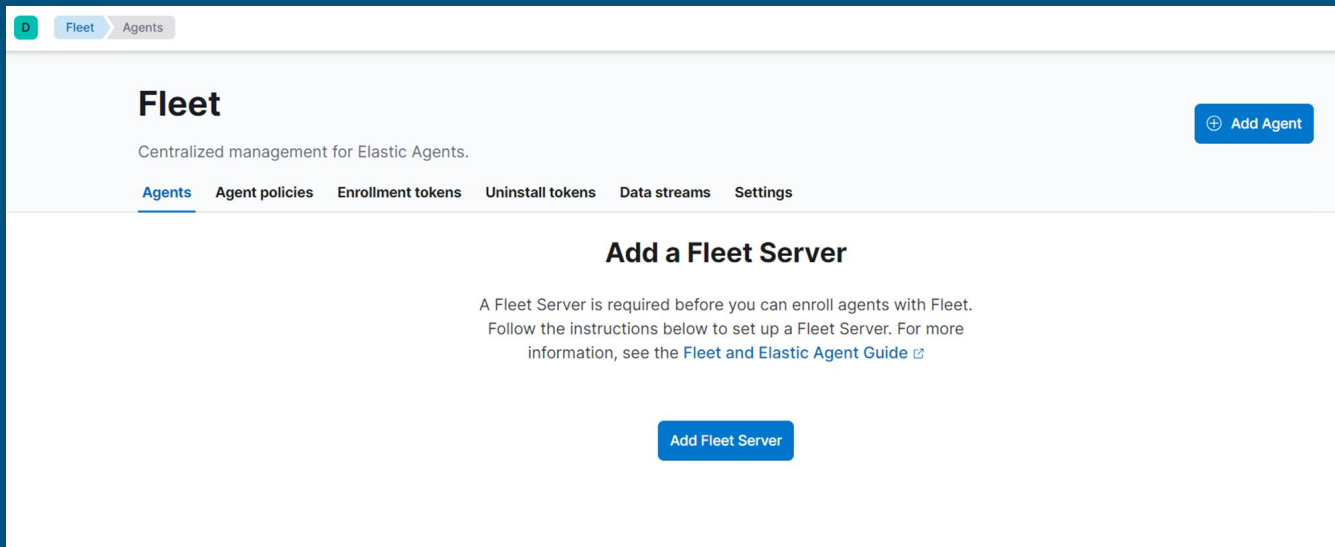
大量部署: 隨著原本 Elastic Agents 的數量增加, 越來越需要一個中控平台對 Elastic Agents 進行統一管理與配置

安全性: 相對 beat 所需的權限更少

靈活性: 部署方便快捷

簡便性: 有著大量已經預先處理好的模版, 目前以有超過300種資料的模版, 收取特定資料時可直接以 elastic common schema (ecs) 格式進行儲存

# Fleet 安裝



The screenshot shows a web interface for Fleet management. At the top left, there is a breadcrumb trail: 'D' (a small green square with a white 'D') followed by 'Fleet' and 'Agents' (with a right-pointing arrow). Below this, the main heading is 'Fleet' in a large, bold font. Underneath the heading is the text 'Centralized management for Elastic Agents.' To the right of this text is a blue button with a white plus sign and the text 'Add Agent'. Below the heading and text is a horizontal navigation menu with several items: 'Agents' (underlined), 'Agent policies', 'Enrollment tokens', 'Uninstall tokens', 'Data streams', and 'Settings'. The main content area has a heading 'Add a Fleet Server' in bold. Below this heading is a paragraph of text: 'A Fleet Server is required before you can enroll agents with Fleet. Follow the instructions below to set up a Fleet Server. For more information, see the [Fleet and Elastic Agent Guide](#) with an external link icon.' At the bottom center of the main content area is a blue button with the text 'Add Fleet Server'.





# Fleet 離線安裝與 Beats

```
downloads/
├─ apm-server
│  ├── apm-server-8.5.0-linux-x86_64.tar.gz
│  ├── apm-server-8.5.0-linux-x86_64.tar.gz.asc
│  └─ apm-server-8.5.0-linux-x86_64.tar.gz.sha512
├─ beats
│  ├── auditbeat
│  │  ├── auditbeat-8.5.0-linux-x86_64.tar.gz
│  │  ├── auditbeat-8.5.0-linux-x86_64.tar.gz.asc
│  │  └─ auditbeat-8.5.0-linux-x86_64.tar.gz.sha512
│  ├── elastic-agent
│  │  ├── elastic-agent-8.5.0-linux-x86_64.tar.gz
│  │  ├── elastic-agent-8.5.0-linux-x86_64.tar.gz.asc
│  │  └─ elastic-agent-8.5.0-linux-x86_64.tar.gz.sha512
│  ├── filebeat
│  │  ├── filebeat-8.5.0-linux-x86_64.tar.gz
│  │  ├── filebeat-8.5.0-linux-x86_64.tar.gz.asc
│  │  └─ filebeat-8.5.0-linux-x86_64.tar.gz.sha512
│  ├── heartbeat
│  │  ├── heartbeat-8.5.0-linux-x86_64.tar.gz
│  │  ├── heartbeat-8.5.0-linux-x86_64.tar.gz.asc
│  │  └─ heartbeat-8.5.0-linux-x86_64.tar.gz.sha512
│  ├── metricbeat
│  │  ├── metricbeat-8.5.0-linux-x86_64.tar.gz
│  │  ├── metricbeat-8.5.0-linux-x86_64.tar.gz.asc
│  │  └─ metricbeat-8.5.0-linux-x86_64.tar.gz.sha512
│  ├── osquerybeat
│  │  ├── osquerybeat-8.5.0-linux-x86_64.tar.gz
│  │  ├── osquerybeat-8.5.0-linux-x86_64.tar.gz.asc
│  │  └─ osquerybeat-8.5.0-linux-x86_64.tar.gz.sha512
│  └─ packetbeat
│     ├── packetbeat-8.5.0-linux-x86_64.tar.gz
│     ├── packetbeat-8.5.0-linux-x86_64.tar.gz.asc
│     └─ packetbeat-8.5.0-linux-x86_64.tar.gz.sha512
```

```
├─ cloudbeat
│  ├── cloudbeat-8.5.0-linux-x86_64.tar.gz
│  ├── cloudbeat-8.5.0-linux-x86_64.tar.gz.asc
│  └─ cloudbeat-8.5.0-linux-x86_64.tar.gz.sha512
├─ endpoint-dev
│  ├── endpoint-security-8.5.0-linux-x86_64.tar.gz
│  ├── endpoint-security-8.5.0-linux-x86_64.tar.gz.asc
│  └─ endpoint-security-8.5.0-linux-x86_64.tar.gz.sha512
├─ fleet-server
│  ├── fleet-server-8.5.0-linux-x86_64.tar.gz
│  ├── fleet-server-8.5.0-linux-x86_64.tar.gz.asc
│  └─ fleet-server-8.5.0-linux-x86_64.tar.gz.sha512
└─ pull-bin.sh
```

1. 離線安裝 Fleet Server 時需將所有相關組件提前下載
2. 內容包含全部的 beats

# 檢查 Fleet Settings

## Fleet

Centralized management for Elastic Agents.

[Agents](#) [Agent policies](#) [Enrollment tokens](#) [Uninstall tokens](#) [Data streams](#) [Settings](#)

### Fleet server hosts

Specify the URLs that your agents will use to connect to a Fleet Server. If multiple URLs exist, Fleet will show the first provided URL for enrollment purposes. For more information, see the [Fleet and Elastic Agent Guide](#).

Name	Host URLs	Default	Actions
FleetServer	https://10.99.1.69:8220	✓	

[Add Fleet Server](#)

### Outputs

Specify where agents will send data.

Name	Type	Hosts	Status	Default	Actions
default	Elasticsearch	https://10.99.1.69:9200		<a href="#">Agent integrations</a> <a href="#">Agent monitoring</a>	

[Add output](#)

### Agent Binary Download

Specify where the agents will download their binary from. Checked default will apply to all policies unless overwritten.

Name	Host	Default	Actions
Elastic Artifacts	https://artifacts.elastic.co/downloads/	✓	

[Add agent binary source](#)

1. Fleet Server 的 host
2. 輸出的 Elasticsearch
3. 下載路徑 (非離線下載不需要)

# 種類繁多的 Elastic Agents

The screenshot displays the Elastic Agent integrations page. On the left, a sidebar lists 384 categories with counts: APM (1), AWS (41), Azure (25), Cloud (9), Containers (15), Custom (44), Database (39), Elastic Stack (51), Elasticsearch SDK (9), Search (37), Google Cloud (20), Network (56), and Observability (124). Below the sidebar, there are filters for 'Display beta integrations' and a note about 'Elastic Agent and Beats' integration. The main content area is a grid of integration cards, each with an icon, name, and description of what it collects or monitors.

Category	Count
APM	1
AWS	41
Azure	25
Cloud	9
Containers	15
Custom	44
Database	39
Elastic Stack	51
Elasticsearch SDK	9
Search	37
Google Cloud	20
Network	56
Observability	124

Display beta integrations

If an integration is available for [Elastic Agent and Beats](#), show:

- Recommended @
- Elastic Agent only
- Beats only

Integration Name	Description
APM	Collect performance metrics from your applications with Elastic APM.
Elastic Defend	Protect your hosts and cloud workloads with threat prevention, detection, and deep security data visibility.
Web crawler	Add search to your website with the web crawler.
1Password	Collect logs from 1Password with Elastic Agent.
AbuseCH	Ingest threat intelligence indicators from URL Haus, Malware Bazaar, and Threat Fox feeds with Elastic Agent.
ActiveMQ	Collect logs and metrics from ActiveMQ instances with Elastic Agent.
Aerospike Metrics	Collect metrics from Aerospike servers with Metricbeat.
Akamai	Collect logs from Akamai with Elastic Agent.
AlienVault OTX	Ingest threat intelligence indicators from AlienVault Open Threat Exchange (OTX) with Elastic Agent.
Amazon CloudFront	Collect Amazon CloudFront logs with Elastic Agent
Amazon Data Firehose	Stream logs and metrics from Amazon Data Firehose into Elastic Cloud.
Amazon DynamoDB	Collect Amazon DynamoDB metrics with Elastic Agent
Amazon EBS	Collect Amazon Elastic Block Storage metrics with Elastic Agent
Amazon EC2	Collect logs and metrics for Amazon Elastic Compute Cloud service with Elastic Agent
Amazon ECS	Collect metrics for Amazon Elastic Container Service with Elastic Agent

1. 通過 integration 界面輕鬆選擇查看所有的可採集資料
2. 目前 Elastic Agent 已對384種資料進行預處理

# 通過 Intergration 輕鬆整合資料 - Apache 為例

The screenshot shows the 'Integrations' page in the Elastic Agent console. The page title is 'Integrations' with a subtitle 'Choose an integration to start collecting and analyzing your data.' There are two tabs: 'Browse integrations' and 'Installed integrations'. A search bar contains the text 'apache'. On the left, a category list shows 'All categories' with 384 items, and various categories like APM, AWS, Azure, etc. The main content area displays six integration cards:

- Amazon Managed Streaming for Apache Kafka (MSK)**: Collect Amazon MSK metrics with Elastic Agent.
- Apache HTTP Server**: Collect logs and metrics from Apache servers with Elastic Agent.
- Apache Spark**: Collect metrics from Apache Spark with Elastic Agent.
- Apache Tomcat**: Collect and parse logs and metrics from Apache Tomcat servers with Elastic Agent.
- Hadoop**: Collect metrics from Apache Hadoop with Elastic Agent.
- Tomcat NetWitness Logs**: Collect and parse logs from Apache Tomcat servers with Elastic Agent.

1. 選擇 Apache HTTP Server 來抓取 Apache 日誌

# 修改設定

針對 Apache Log 僅需修改文件路徑即可  
可針對 access 和 error log 進行拆解

Collect logs from Apache instances [Change defaults](#) ^

### Settings

The following settings are applicable to all inputs below. [Advanced options](#)

Apache access logs  
Collect Apache access logs

**Paths**

- X
- X
- X

[+ Add row](#)

Preserve original event  
Preserves a raw copy of the original event, added to the field event.original

[Advanced options](#)

Apache error logs  
Collect Apache error logs

**Paths**

- X
- X

[+ Add row](#)

# Elastic Agent 安裝

## Add agent

Add Elastic Agents to your hosts to collect data and send it to the Elastic Stack.

### 1 Select enrollment token

Apache has been selected. Select which enrollment token to use when enrolling agents.

#### Authentication settings

Enrollment token Default (d767d015-eabd-4920-b6a6-afb0f3ff4b17)

### 2 Enroll in Fleet?

- Enroll in Fleet (recommended)** – Enroll in Elastic Agent in Fleet to automatically deploy updates and centrally manage the agent.
- Run standalone** – Run an Elastic Agent standalone to configure and update the agent manually on the host where the agent is installed.

### 3 Install Elastic Agent on your host

Select the appropriate platform and run commands to install, enroll, and start Elastic Agent. Reuse commands to set up agents on more than one host. For aarch64, see our [downloads page](#). This guidance is for AMD but you can adapt it to your device architecture. For additional guidance, see our [installation docs](#).

Linux Tar Mac Windows RPM DEB Kubernetes

```
curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.14.3-linux-x86_64.tar.gz
tar xzvf elastic-agent-8.14.3-linux-x86_64.tar.gz
cd elastic-agent-8.14.3-linux-x86_64
sudo ./elastic-agent install --url=https://10.99.1.69:8220 --enrollment-token=NGp30VJwRUJsaFpuX2pUSHNZMmg6WnIZuU1NY
```

1. 按照步驟安裝即可
2. 最後一步安裝時，如無憑證可加入 `--insecure`

### Agent enrollment confirmed

✓ 1 agent has been enrolled.

[View enrolled agents](#)

### Incoming data confirmed

✓ Incoming data received from 1 of 1 recently enrolled agent.

# 資料寫入查看-data stream

## Index Management

[Index Management docs](#)

Indices **Data Streams** Index Templates Component Templates Enrich Policies

Data streams store time-series data across multiple indices and can be created from index templates. [Learn more.](#)

Include stats [?](#)

View 1 [v](#)

Q apache

Reload

<input type="checkbox"/> Name <a href="#">↑</a>	Health	Indices	Data retention <a href="#">ⓘ</a>	Actions
<input type="checkbox"/> logs-apache.access-default <span>Managed</span>	<span>●</span> yellow	1	Disabled	<a href="#">🗑️</a>
<input type="checkbox"/> logs-apache.error-default <span>Managed</span>	<span>●</span> yellow	1	Disabled	<a href="#">🗑️</a>

Rows per page: 20 [v](#)

< 1 >

通過 agent 直接寫入的資料並不顯示在普通的 Indices 中，而是以 data stream 的方式儲存

# 通過製作 Data View 查看 Apache 資料

## Create data view

Name

Apache Access

Index pattern

logs-apache.access\*



Timestamp field

@timestamp



Select a timestamp field for use with the global time filter.

[Show advanced settings](#)

✓ Your index pattern matches 1 source.

All sources

Matching sources

logs-apache.access-default

Data stream

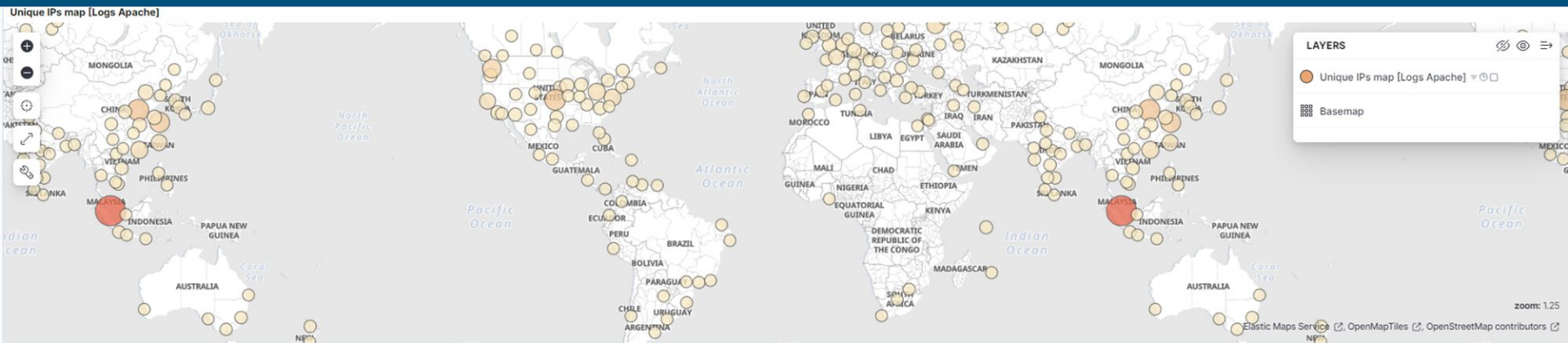
Rows per page: 10

1. 新資料必須通過建設 Data view 才可查看
2. 以Agent寫入的資料皆以 logs- 開頭



# 查看 Apache Default 儀表板

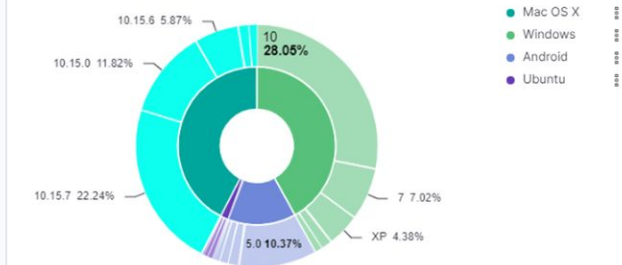
通過 Dashboards → [Logs Apache] Access and error logs 可查看默認儀表板



Response codes over time [Logs Apache]



Operating systems breakdown [Logs Apache]



# Elasticsearch Security 説明

---

# 大量的 Pre-built in rule

The screenshot displays the 'Add Elastic Rules' page in the Microsoft Defender Security Center. The interface includes a navigation sidebar on the left with categories like Dashboards, Rules, Alerts, Attack discovery, Findings, Cases, Timelines, Intelligence, Explore, Get started, and Manage. The main content area features a search bar, a 'Tags 108' dropdown, and a table of rules. Each rule entry includes a checkbox, the rule name, a button for integrations, a risk score icon, the risk score value, the severity level, and an 'Install rule' button.

<input type="checkbox"/>	Rule	Integrations	Risk score icon	Risk score	Severity	Install rule
<input type="checkbox"/>	Microsoft IIS Service Account Password Dumped	1/3 integrations	7	21	Low	Install rule
<input type="checkbox"/>	Local Account TokenFilter Policy Disabled	0/4 integrations	10	47	Medium	Install rule
<input type="checkbox"/>	Potential Persistence via Time Provider Modification	0/1 integrations	8	47	Medium	Install rule
<input type="checkbox"/>	Component Object Model Hijacking	0/1 integrations	9	47	Medium	Install rule
<input type="checkbox"/>	Creation or Modification of Root Certificate	0/2 integrations	8	21	Low	Install rule
<input type="checkbox"/>	Potential Suspicious DebugFS Root Device Access	0/1 integrations	5	21	Low	Install rule
<input type="checkbox"/>	Creation of a Hidden Local User Account	0/2 integrations	8	73	High	Install rule
<input type="checkbox"/>	Windows Defender Disabled via Registry Modification	0/1 integrations	8	21	Low	Install rule

1. 超過1000條的 Pre-built rule, 點擊 install rule 即可安裝
2. 需要安裝相應的 intergration 進行配合
3. Pre-built in rule 的安裝不需要開啟 License

# 可通過查看 Tags 確認所屬 Mitre ATT&CK 類型

## Tags

Domain: Endpoint

OS: Windows

Use Case: Threat Detection

Tactic: Collection

Data Source: Elastic Defend

Rule Type: BBR

Data Source: Sysmon

Data Source: Elastic Endgame

Tactic 便為 Mitre ATT&CK 類型

# Mitre ATT&CK 页面 Sample

## MITRE ATT&CK® coverage

Your current coverage of MITRE ATT&CK® tactics and techniques, based on installed rules. Click a cell to view and enable a technique's rules. Rules must be mapped to the MITRE ATT&CK® framework to be displayed. [Learn more.](#)

Installed rule status **1**  Installed rule type **2**

Search for the tactic, technique (e.g., "defense evasion" or "TA0005") or rule name

[Collapse cells](#) [Expand cells](#)

**Legend** (count will include all rules selected)

- >10 rules
- 7-10 rules
- 3-7 rules
- 1-3 rules
- 0 rules

<b>Reconnaissance</b> 1/10 techniques Disabled Rules: 0 Enabled Rules: 4	<b>Resource Development</b> 1/7 techniques Disabled Rules: 0 Enabled Rules: 1	<b>Initial Access</b> 7/12 techniques Disabled Rules: 0 Enabled Rules: 66	<b>Execution</b> 11/35 techniques Disabled Rules: 0 Enabled Rules: 116	<b>Persistence</b> 15/70 techniques Disabled Rules: 0 Enabled Rules: 178	<b>Privilege Escalation</b> 13/40 techniques Disabled Rules: 0 Enabled Rules: 100	<b>Defense Evasion</b> 29/88 techniques Disabled Rules: 0 Enabled Rules: 219	<b>Credential Access</b> 12/30 techniques Disabled Rules: 0 Enabled Rules: 100
<b>Active Scanning</b> Sub-techniques 1/3	<b>Acquire Infrastructure</b> Sub-techniques 0/7	<b>Drive-by Compromise</b> Sub-techniques 0/0	<b>AppleScript</b> Sub-techniques 0/0	<b>Accessibility Features</b> Sub-techniques 0/0	<b>Abuse Elevation Control Mechanism</b> Sub-techniques 4/4	<b>Abuse Elevation Control Mechanism</b> Sub-techniques 4/4	<b>Adversary Operations</b> Sub-techniques 0/0
<b>Gather Victim Host Information</b> Sub-techniques 0/4	<b>Compromise Accounts</b> Sub-techniques 0/3	<b>Exploit Public-Facing Application</b> Sub-techniques 0/0	<b>CMSTP</b> Sub-techniques 0/0	<b>Account Manipulation</b> Sub-techniques 3/5	<b>Access Token Manipulation</b> Sub-techniques 3/5	<b>Access Token Manipulation</b> Sub-techniques 3/5	<b>Adversary Operations</b> Sub-techniques 0/0
<b>Gather Victim Identity Information</b> Sub-techniques 0/3	<b>Compromise Infrastructure</b> Sub-techniques 0/7	<b>External Remote Services</b> Sub-techniques 0/0	<b>Command and Scripting Interpreter</b> Sub-techniques 6/8	<b>AppCert DLLs</b> Sub-techniques 0/0	<b>Access Token Manipulation</b> Sub-techniques 3/5	<b>Access Token Manipulation</b> Sub-techniques 3/5	<b>Adversary Operations</b> Sub-techniques 0/0
<b>Gather Victim Network Information</b> Sub-techniques 0/6	<b>Develop Capabilities</b> Sub-techniques 0/4	<b>Hardware Additions</b> Sub-techniques 0/0	<b>Compiled HTML File</b> Sub-techniques 0/0	<b>Appinit DLLs</b> Sub-techniques 0/0	<b>Accessibility Features</b> Sub-techniques 0/0	<b>Application Access Token</b> Sub-techniques 0/0	<b>Adversary Operations</b> Sub-techniques 0/0
<b>Gather Victim Org Information</b> Sub-techniques 0/4	<b>Establish Accounts</b> Sub-techniques 0/3	<b>Phishing</b> Sub-techniques 2/3	<b>Component Object Model and Distributed COM</b> Sub-techniques 0/0	<b>Application Shimming</b> Sub-techniques 0/0	<b>AppCert DLLs</b> Sub-techniques 0/0	<b>Application Access Token</b> Sub-techniques 0/0	<b>Adversary Operations</b> Sub-techniques 0/0
<b>Phishing for Information</b> Sub-techniques 0/3	<b>Obtain Capabilities</b> Sub-techniques 1/6	<b>Replication Through Removable Media</b> Sub-techniques 0/0	<b>Container Administration Command</b> Sub-techniques 0/0	<b>Authentication Package</b> Sub-techniques 0/0	<b>Appinit DLLs</b> Sub-techniques 0/0	<b>Application Access Token</b> Sub-techniques 0/0	<b>Adversary Operations</b> Sub-techniques 0/0
<b>Search Closed Sources</b> Sub-techniques 0/2	<b>Stage Capabilities</b> Sub-techniques 0/6	<b>Spearphishing Attachment</b> Sub-techniques 0/0	<b>Control Panel Items</b> Sub-techniques 0/0	<b>BITS Jobs</b> Sub-techniques 0/0	<b>Application Shimming</b> Sub-techniques 0/0	<b>Application Access Token</b> Sub-techniques 0/0	<b>Adversary Operations</b> Sub-techniques 0/0
		<b>Spearphishing Link</b> Sub-techniques 0/0		<b>Boot or Logon Autostart Execution</b> Sub-techniques 6/15	<b>Appinit DLLs</b> Sub-techniques 0/0	<b>Application Access Token</b> Sub-techniques 0/0	<b>Adversary Operations</b> Sub-techniques 0/0
				<b>Boot or Logon Autostart Execution</b> Sub-techniques 6/15	<b>Appinit DLLs</b> Sub-techniques 0/0	<b>Application Access Token</b> Sub-techniques 0/0	<b>Adversary Operations</b> Sub-techniques 0/0
				<b>Boot or Logon Autostart Execution</b> Sub-techniques 6/15	<b>Appinit DLLs</b> Sub-techniques 0/0	<b>Application Access Token</b> Sub-techniques 0/0	<b>Adversary Operations</b> Sub-techniques 0/0

整合生成式AI輕鬆處理解資料

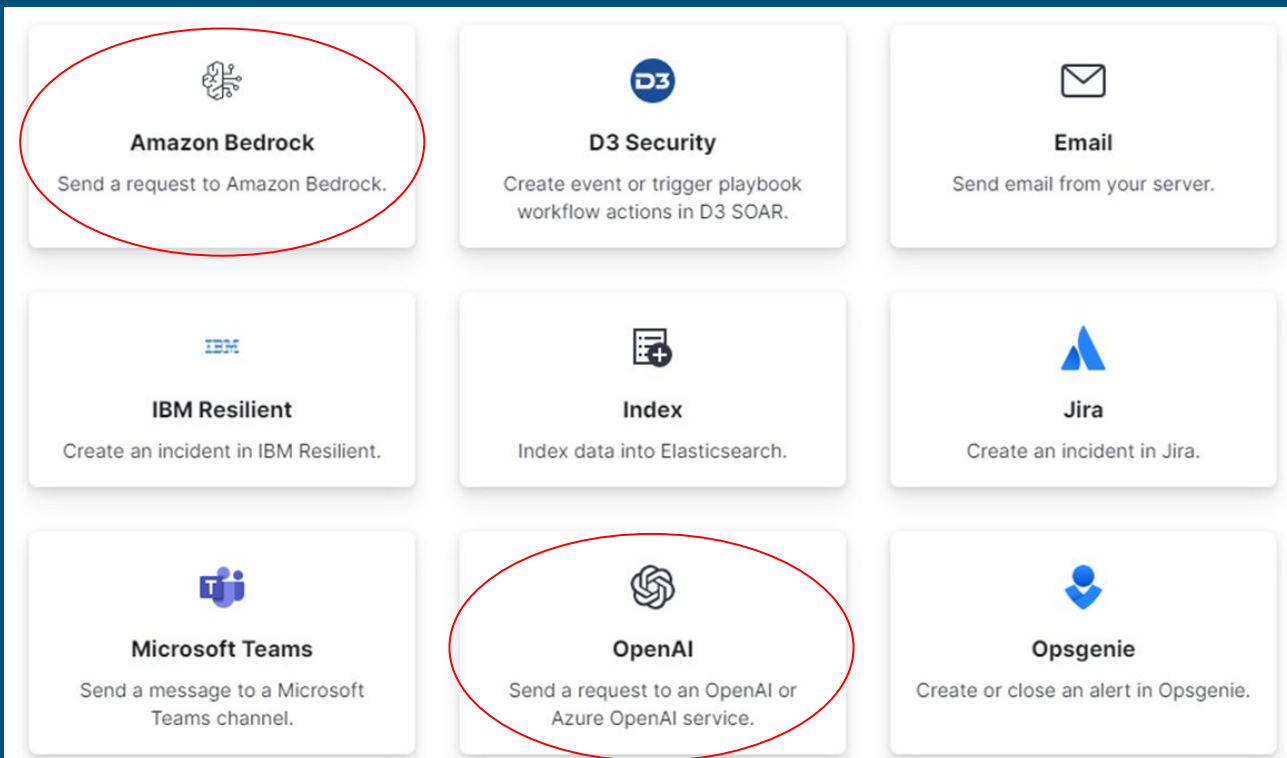
---

# Elasticsearch 整合 AI 計費模式

	Free and open - Basic <sup>1,2</sup>	Platinum	Enterprise
DATA EXPLORATION & VISUALIZATION			
ELASTIC OBSERVABILITY			
Observability overview	✓	✓	✓
User Experience overview	✓	✓	✓
Curated ad hoc data exploration	✓	✓	✓
Service Level Objectives (SLOs)	—	✓	✓
Kibana alerting and actions <sup>5</sup>	✓	✓	✓
Elastic AI Assistant	—	—	✓

1. 要串聯第三方 AI 程式必須購買 Enterprise 版本
2. 第三方程式使用的 Token 需額外付費

# Elasticsearch 串聯第三方 LLM



當前可用第三方 LLM 有 Amazon Bedrock 與 OpenAI



# 生成式 AI 當前面臨問題

---

1. 資料訓練截止到 2021年9月，造成資料可能過時或不準確
2. 對特定領域內容知識不足
3. 當問題不夠準確時會提供不正確答案

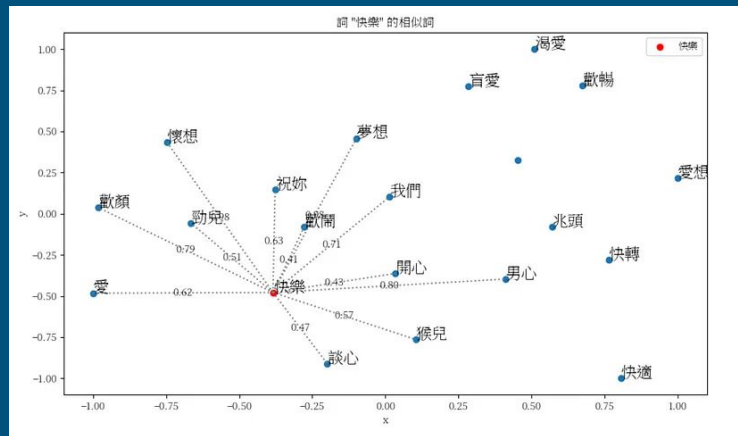
# Elasticsearch 串聯生成式 AI 的優勢

---

1. Elasticsearch 是一個可大量儲存資料、文本、向量的資料庫。可以非常快速的提供準確的查詢結果
2. 提供混合搜索能力 (BM25 & kNN)
  - a. BM25 為傳統文本搜索
  - b. kNN (k-Nearest Neighbor) 為可供 AI 使用的向量搜索 (vector search)
3. 提供豐富的 API 及資料串聯能力

# 簡單的向量化數據庫說明

1. 數據 (文本、圖像、影音) 會被轉換為向量
  - a. 例如 "Hello World!" 會被轉換為 [72, 101, 108, 108, 111, 32, 87, 111, 114, 108, 100, 33]
2. 資料可以類似 Cosine similarity 的方式查詢相似性
3. 優點:
  - a. 可以通過關鍵字或語義 查詢查找相關文檔
  - b. 可以查找複雜的資料 (圖像, 影音)
  - c. 自然語言處理 (NLP) 的必要前置條件
  - d. 不需像傳統 DB 一樣手動定義同義字等



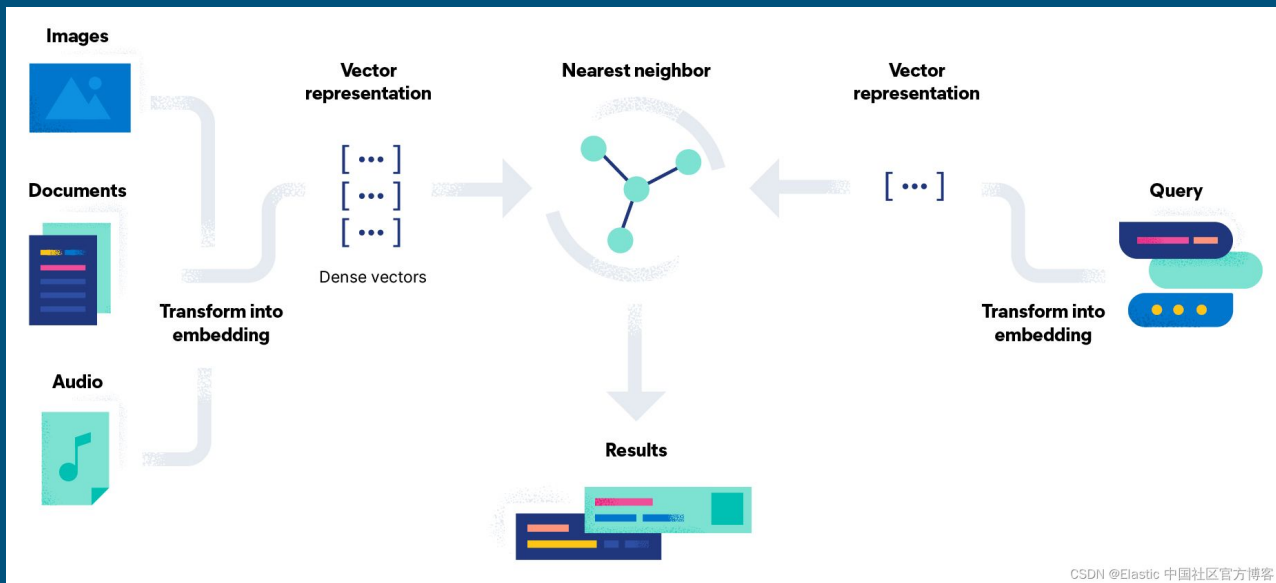
# 簡單的向量搜索 Sample

1. “Cat” 會被轉換為 [ 0.49671415, -0.1382643 , 0.64768854, 1.52302986, -0.23415337, -0.23413696, 1.57921282, ...]
2. “Dog” 會被轉換為 [1.69052570, -0.46593737, 0.03282016, 0.40751628, -0.78892303, 0.00206557, -0.00089039, ...]
3. “Kitten” 會被轉換為 [-0.05196425, -0.11119605, 1.0417968, -1.25673929, 0.74538768, -1.71105376, -0.20586438, ...]
4. 從結果來看 Cat 與 Kitten 的 cosine distance

更接近所以 Kitten 和 Cat 相似

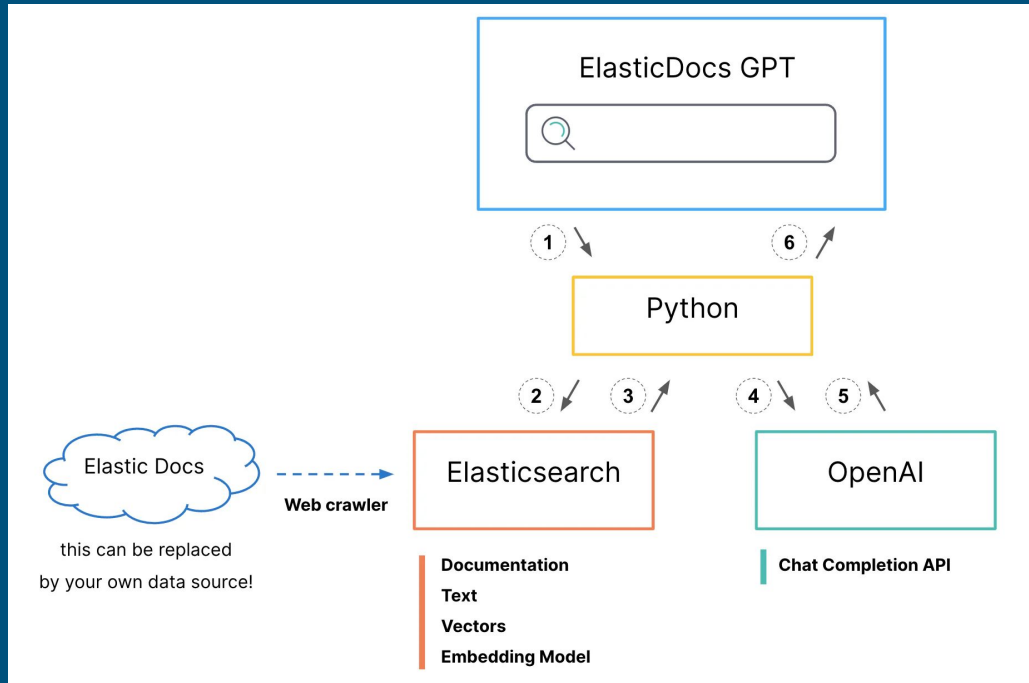


# Elasticsearch 簡單的向量搜索說明



通過儲存時將資料轉換為陣列後儲存如Elasticsearch，用戶查詢時將查詢語句也轉換為陣列，在通過 kNN 查詢後返回最相似的結果

# Elasticsearch 與 第三方 AI 串聯方法



1. 用戶通過主頁面輸入問題給後台 Python
2. 通過生成 BM25 與 kNN 搜索查詢 Elasticsearch
3. 將最終唯一結果返回給 Python 頁面
4. 調用 OpenAI API 重新匯整問題。要求 OpenAI 回答問題是必須採用 Elasticsearch 的查詢結果
5. 查詢結果返回給 Python 程式
6. Python 將 OpenAI 結果與 Elasticsearch 查詢結果一併返回

# Retrieval-Augmented Generation (RAG)- 檢索增強生成

---

## 大型語言模型優點:

1. 可以理解人類上下文和意圖
2. 可與人類進行互動
3. 多語種支援

## 大型語言模型缺點:

1. 無法持續更新資料, 不會因為資料更新而重新訓練Model
2. 因缺乏特定行業資料, 對特定行業認知有限, 可能回答錯誤內容
3. 對問題的輸入方式很敏感, 同樣的問題, 不同的輸入方式可能有不同的答案
4. 消耗大量資源無法大量遠程部署

# Retrieval-Augmented Generation (RAG)- 檢索增強生成

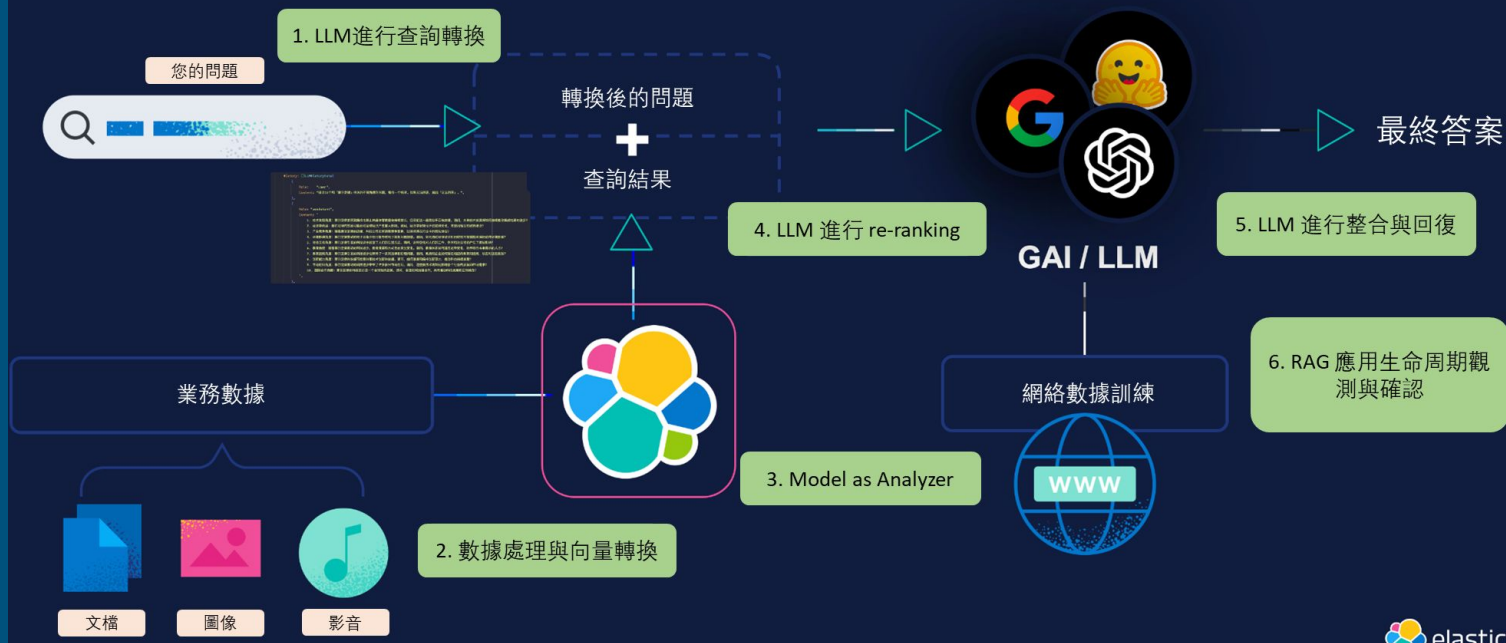
---

1. 結合“搜尋檢索”和“生成能力”的自然語言處理架構。
2. 執行步驟:
  - a. 從外部資料庫搜索相關信息
  - b. 整合相關信息後生成問題後交給 大語言模型 (LLM)
  - c. 由大語言模型進行回復完成特定 NLP 任務
3. RAG 基本架構:
  - a. Retriever (檢索器): 負責提供儲存與資訊 - Elasticsearch
  - b. Generator (生成器): 語言生成模型 - ChatGPT
  - c. Integration and Adjustment (整合與調整): 負責將問題發送至檢索器, 後基於特定資訊生成問題後交給生成器, 最終將結果返回 - Python



# Elasticsearch 與 生成式 AI 的整合

## RAG 領域 – Elasticsearch 的應用



# Elasticsearch 整合生成式 AI 是否會造成隱私洩露?

---

1. 大語言模型必須有對外
2. 資料會經過 Elasticsearch 加工後送出, 且僅送出最相關的1筆資料, 不是直接寄送給 ChatGPT
3. 機密資料或欄位可預先處理, 僅送出特定欄位

# Elasticsearch 與常見 RAG 系統比對

---

其他 RAG 系統常見問題:

1. 高度依賴檢索能力
2. 計算資源需求高
3. 長文本檢索困難效率低下

Elasticsearch 優勢:

1. 檢索效率高效
2. 長期優化檢索算法, 資源耗費較少

# Elasticsearch 結合生成式 AI 結果展示 - Nginx

---



# OpenAI connector

## OpenAI connector

Send a request to an OpenAI or Azure OpenAI service.

Compatibility: Generative AI for Security Generative AI for Observability Generative AI for Search Playground

### Connector settings

Select an OpenAI provider

OpenAI ▼

URL

The OpenAI API endpoint URL. For more information on the URL, refer to the [OpenAI documentation](#).

Default model

If a request does not include a model, it uses the default.

### Authentication

API key

The OpenAI API authentication key for HTTP Basic authentication. For more details about generating OpenAI API keys, refer to the [OpenAI documentation](#).

① Remember your API key value. You must reenter it each time you edit the connector.

Save & test Save

[Back](#)

輸入 API key 即可串聯至  
OpenAI

# Elasticsearch AI 案例1 - Cisco

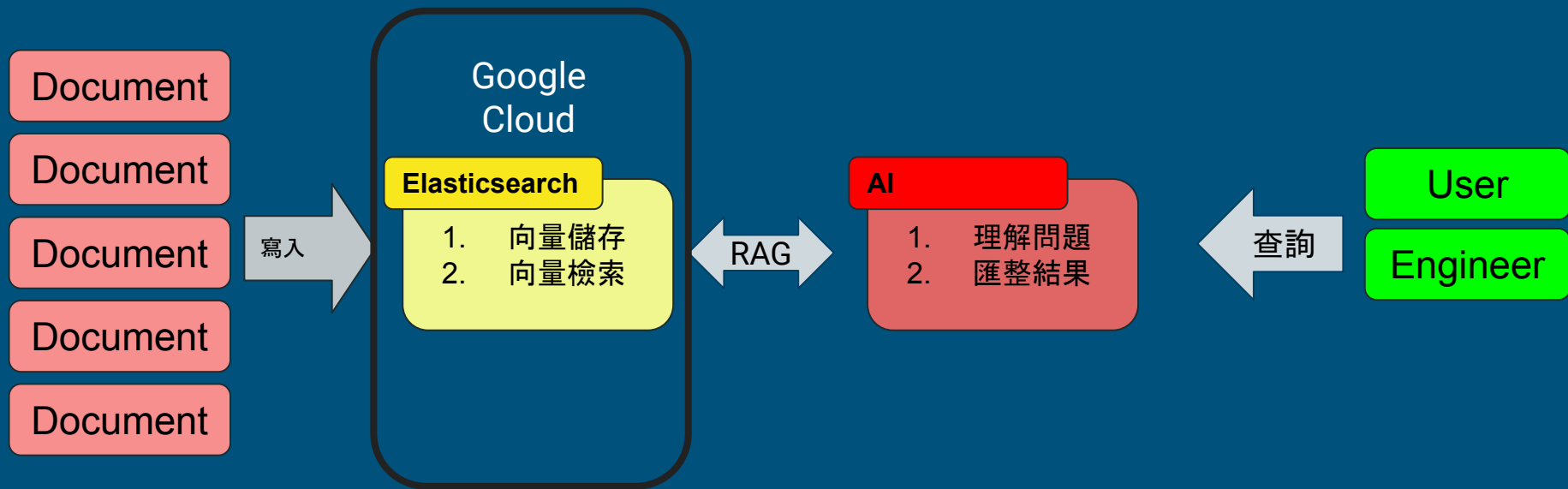
---

Cisco 面臨問題:

1. 歷史資料技術文件太多, 且放置位置過多, 搜索困難且耗時
2. 工程師要尋找文件尋要從上百萬文件中撈取, 耗時且效果差
3. 維護人員處理維護案件時, 無法及時的取得常見問題處理方式
4. 客戶無法從官網順利找到自己希望的文件

# Elasticsearch AI 案例1 - Cisco

處理方式:





# Elasticsearch AI 案例1 - Cisco

---

結果:

1. 工程師回應時間加快 73%
2. 新系統解決了90% 的 支援請求
3. 每月減少 5000 工程師工時

# Elasticsearch AI 官方案例2 - Stack overflow

---

Stack overflow 遭遇問題:

1. 查詢時間過長: 隨著時間不斷快速增長, 預期每項科技產品超過 6000萬個問題
2. 順利找出有價值的答案: 問題中有大量重複問題且價值有限
3. 結果讀取緩慢: 查詢頻率不斷提升, 導致查詢時間緩慢
4. 希望導入 AI 查詢, 但是資料過大查詢緩慢且準確率僅有 42%

# Elasticsearch AI 案例2 - Stack overflow

---

Stack overflow 基於 AI 解決問題:

1. 建立高可信的用戶資料庫: 優先提供高可信度用戶的回復 (Stack overflow 自行解決)
2. 縮短查詢時間和頻率: 通過 AI 優化查詢問題, 使查詢更準確答案更符合需求, 降低重複查詢頻率

# Elasticsearch AI 案例3 - HSE retail

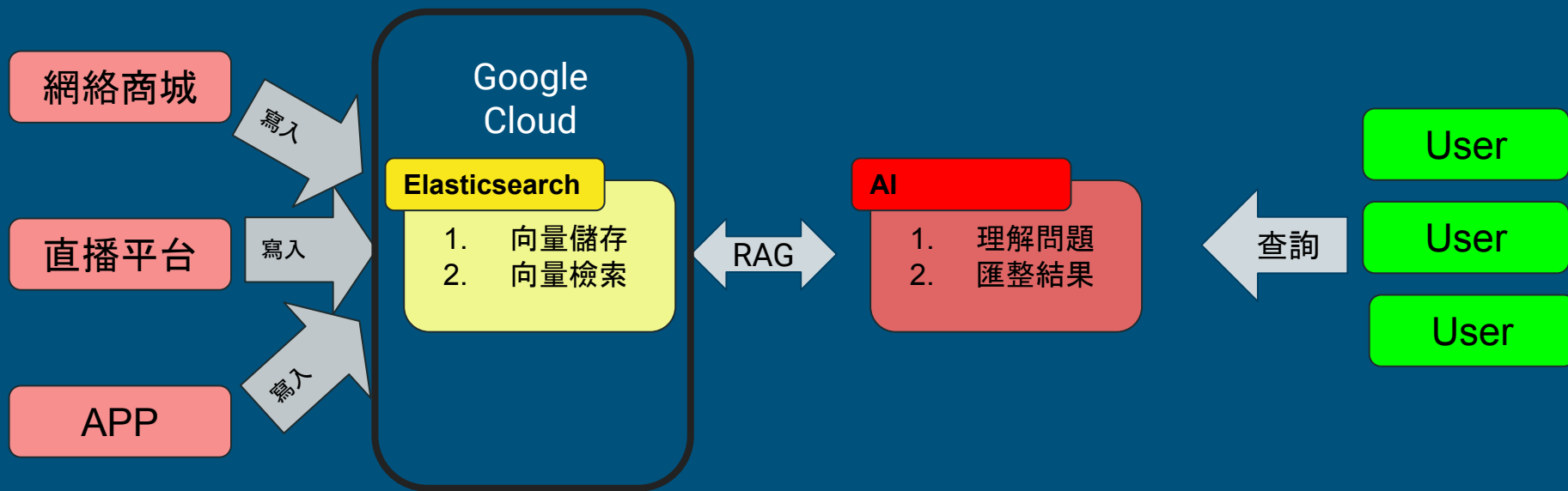
---

HSE 遭遇問題:

1. 客戶查詢條件不準確
2. 有3個通路: 網絡商城, 直播平台, APP 導致資料無法順利整合
3. 查詢結果不佳, 客戶反饋差, 購買意願低

# Elasticsearch AI 案例1 - Cisco

處理方式:



# Elasticsearch AI 案例3 - HSE retail

---

HSE 基於 Elasticsearch AI 解決問題:

1. 使用 Vector search 使客戶更容易查詢到希望的商品, 使點擊購買率增加 4%
2. 減少42%設備的維護時間
3. 減少客戶查詢時的等待時間, 客戶滿意度提升 8%

# 使用 Machine Learning 進行異常偵測

---

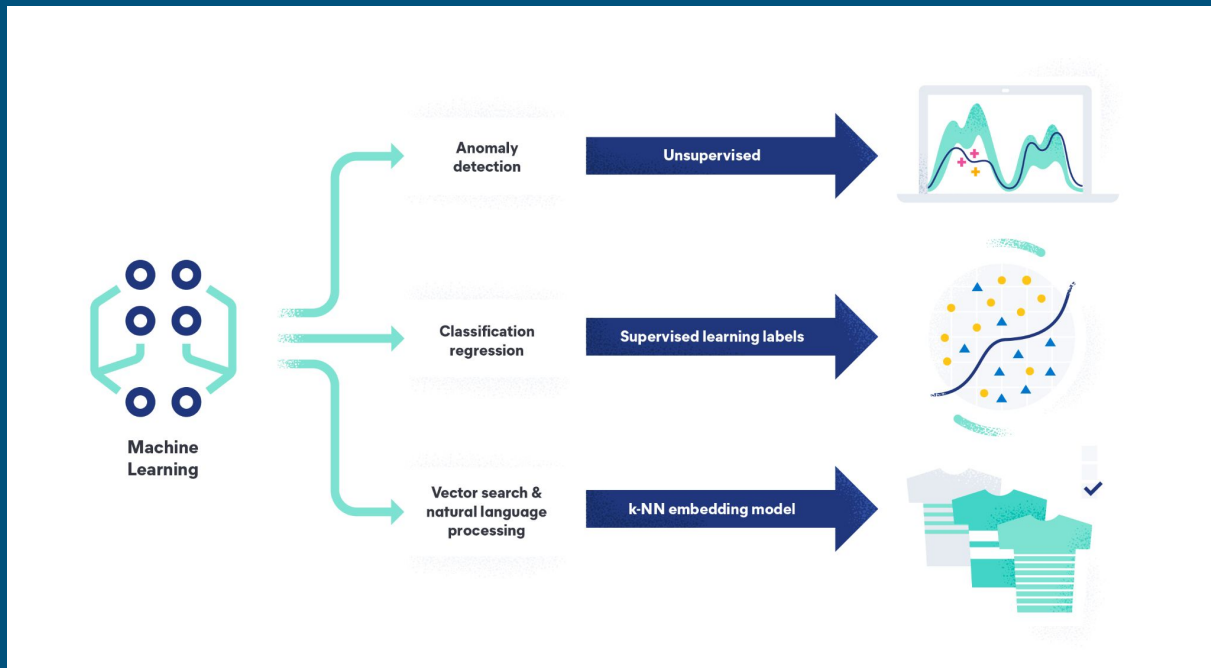
# Elasticsearch Machine Learning 優勢

---

1. 可儲存大量資料: 大量資料是 Machine learning 的前提, 而 elasticsearch 正好是儲存大資料的專家
2. 高靈活性: 可簡單擴容, 即使資料越來越大, 也可輕鬆應對
3. 查詢快速: 通過倒排索引可快速查詢
4. 方便後續排查: Machine learning 後的結果依然需要人為確認, Kibana 可以很簡單的排查問題



# Elasticsearch Machine Learning 分類



Elasticsearch 的 ML  
分為3部分:

1. 異常偵測
2. 分類預測
3. 向量搜索

# 資安常用 Machine Learning

## Unsupervised

- **Outlier Detection**
- Anomaly Detection

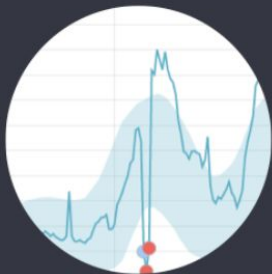
## Supervised

- **Classification**
- **Regression**

1. 資安中僅有 Unsupervised 和 Supervised learning 常用
2. Unsupervised Model 不需額外加工因此絕大部分客戶都使用這個
3. Supervised Model 需要將資料加工成 Panel Data 樣式所以使用率較低

# 機器學習分類

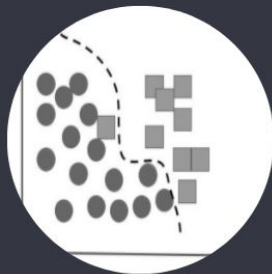
Unsupervised



**Time-series analysis**

Anomaly Detection  
Forecasting

Supervised



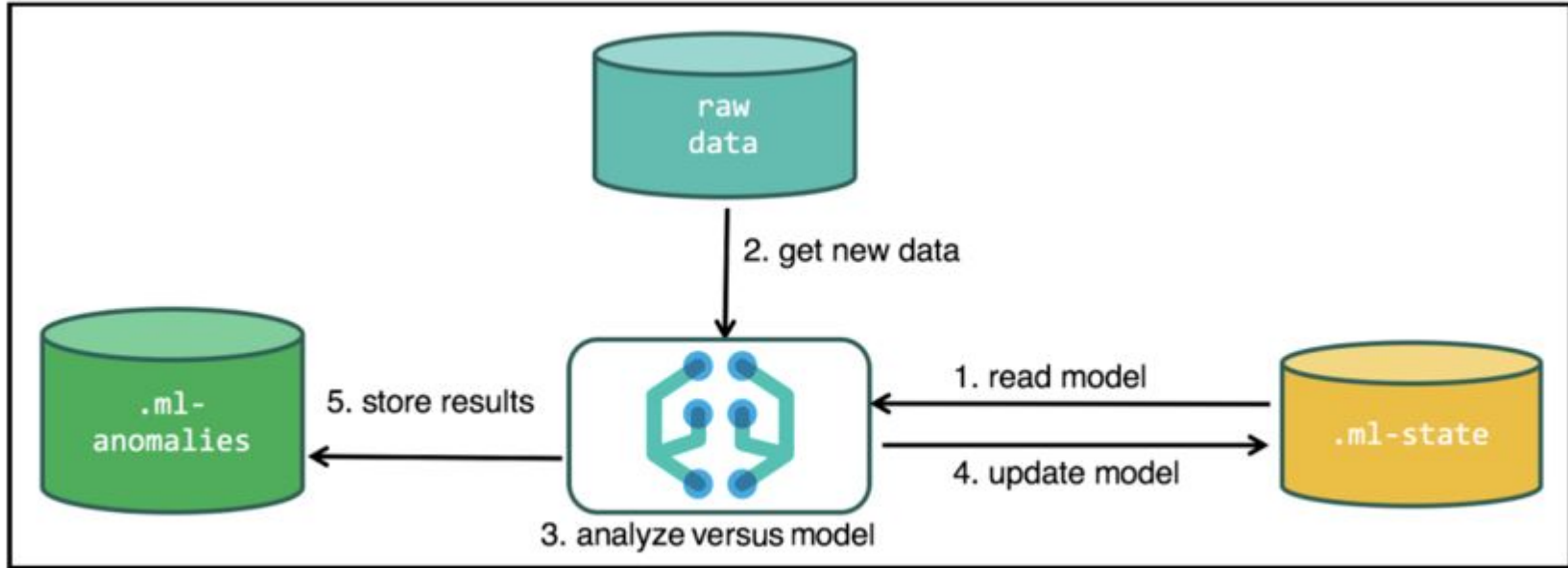
**Data frame analytics**

Classification  
Regression

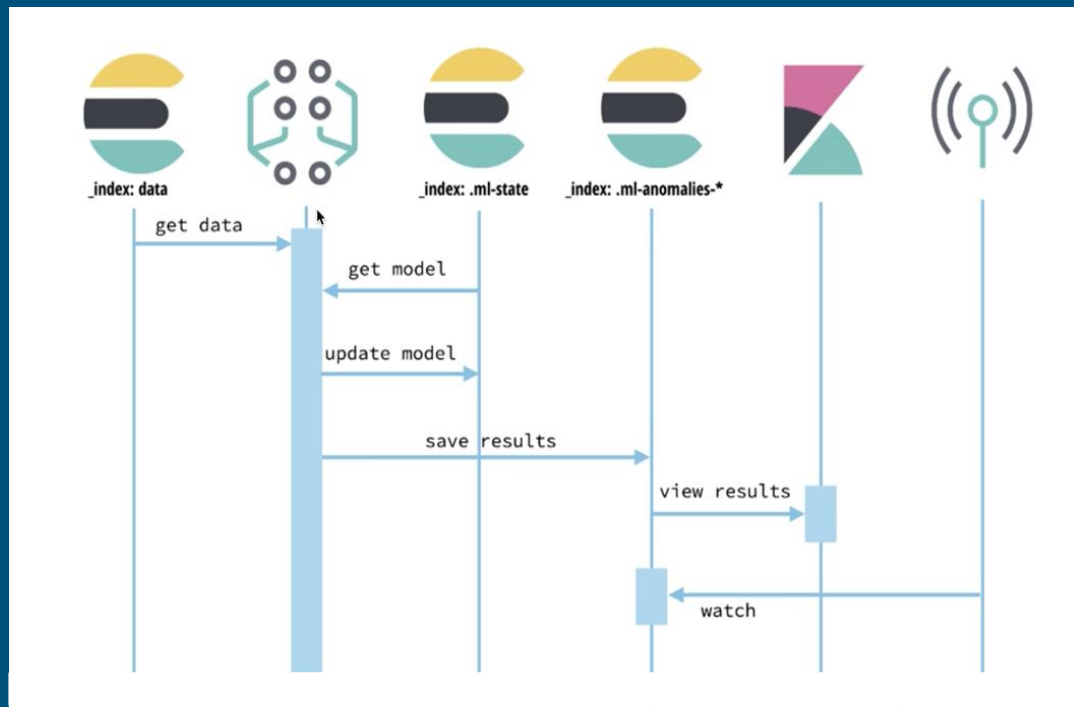
Unsupervised machine learning 作用於 Time series data 資料

Supervised machine learning 作用於 Panel data 資料

# Elasticsearch 機械學習說明



# Elasticsearch 機械學習說明



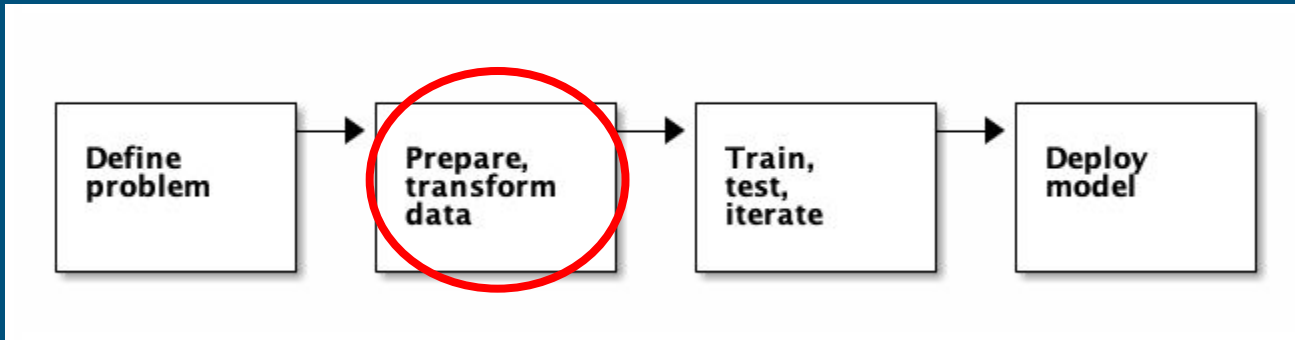
`.ml-state`: 負責儲存模型

`.ml-anomalies`: 負責儲存異常

`data`: 為原始資料

# 監督式機械學習過程

---



1. 資料需要經過額外處理才可以使用，基本不能以 raw data 進行學習，且 Model 需要反復測試
2. 需將 Timeseries 資料整理轉換為 Panel Data 格式

# Elasticsearch ML 案例1 - 沃爾瑪

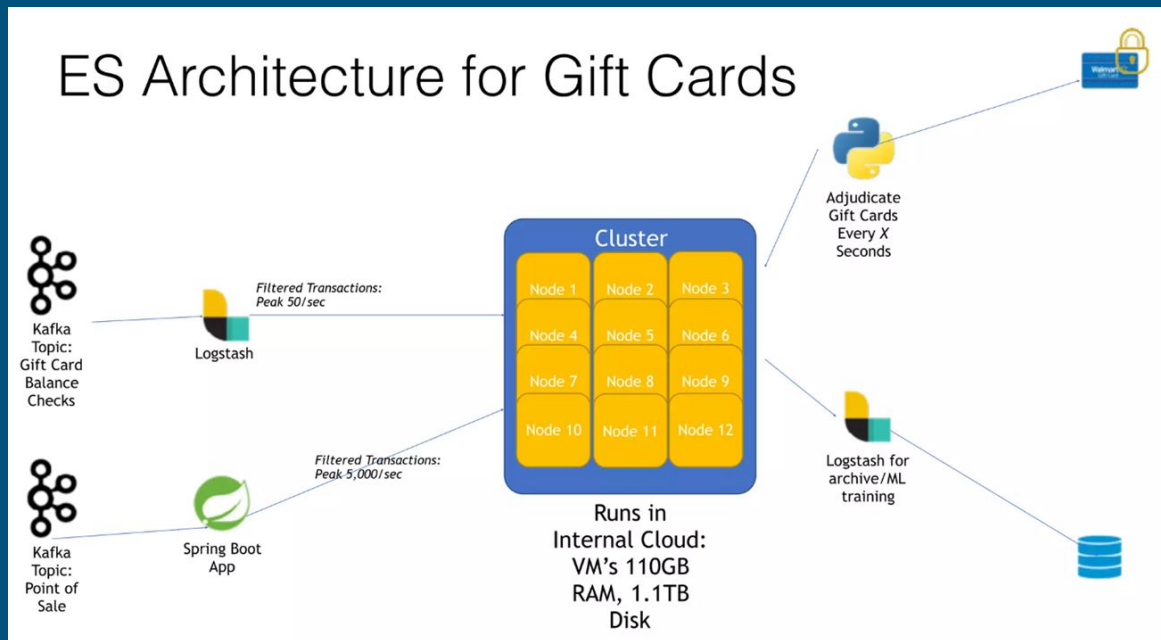
---

沃爾瑪面臨問題:

電信詐騙誘導受害者通過沃爾瑪購買點數卡轉移現金，避開銀行和監管平台

# Elasticsearch ML 案例1 - 沃爾瑪

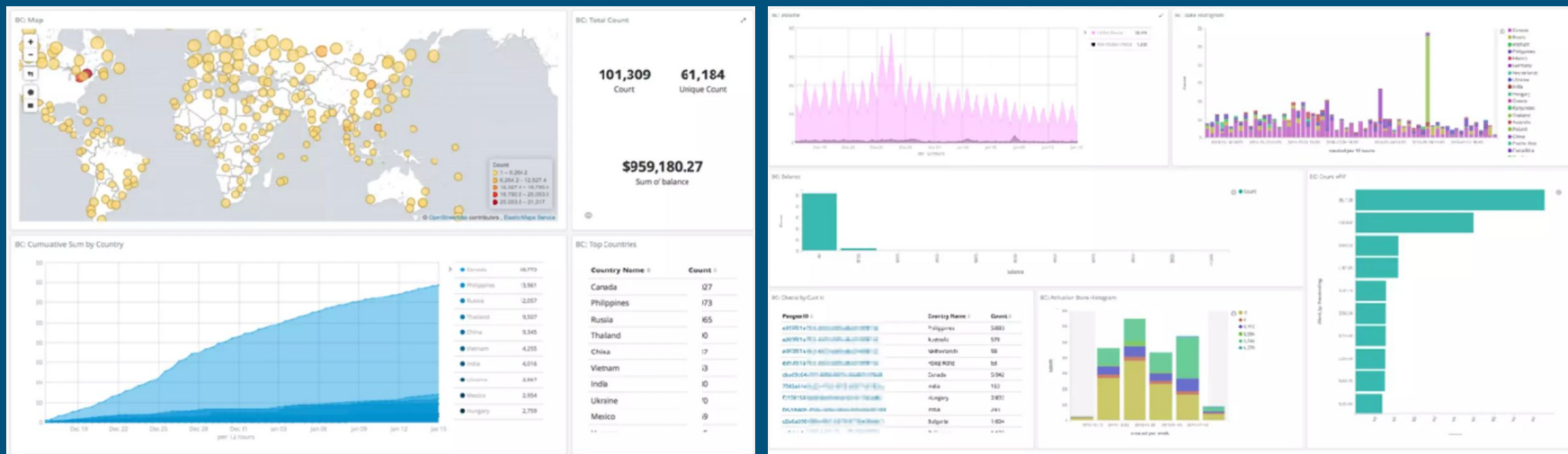
## Elasticsearch 架構





# Elasticsearch ML 案例1 - 沃爾瑪

通過導入信用卡資料, IP, 銷售金額的 AP 日誌後, 同時進行人工與 ML 作業, 保證用戶不被電信詐騙騙走財產



# Elasticsearch ML 案例2 - 歐洲電信警察

---

面臨問題:

1. 需收集超過250套 IT 系統, 超過3500 台 Endpoint 的資安日誌記錄, 資料太大太多且增長迅速
2. 黑客行為不斷增加, 對警力的需求不斷上升

# Elasticsearch ML 案例2 - 歐洲電信警察

---

結果:

1. Elasticsearch 收取了上一個 SIEM 10倍量的資安資料
2. Endpoint 從 3500 台增加到 35000 台
3. 通過 Elasticsearch 異常偵測自動判斷黑客攻擊, 降低警務勞力

# Elasticsearch ML 案例2 - 歐洲電信警察

---

結果:

1. Elasticsearch 收取了上一個 SIEM 10倍量的資安資料
2. Endpoint 從 3500 台增加到 35000 台
3. 通過 Elasticsearch 異常偵測自動判斷黑客攻擊, 降低警務勞力

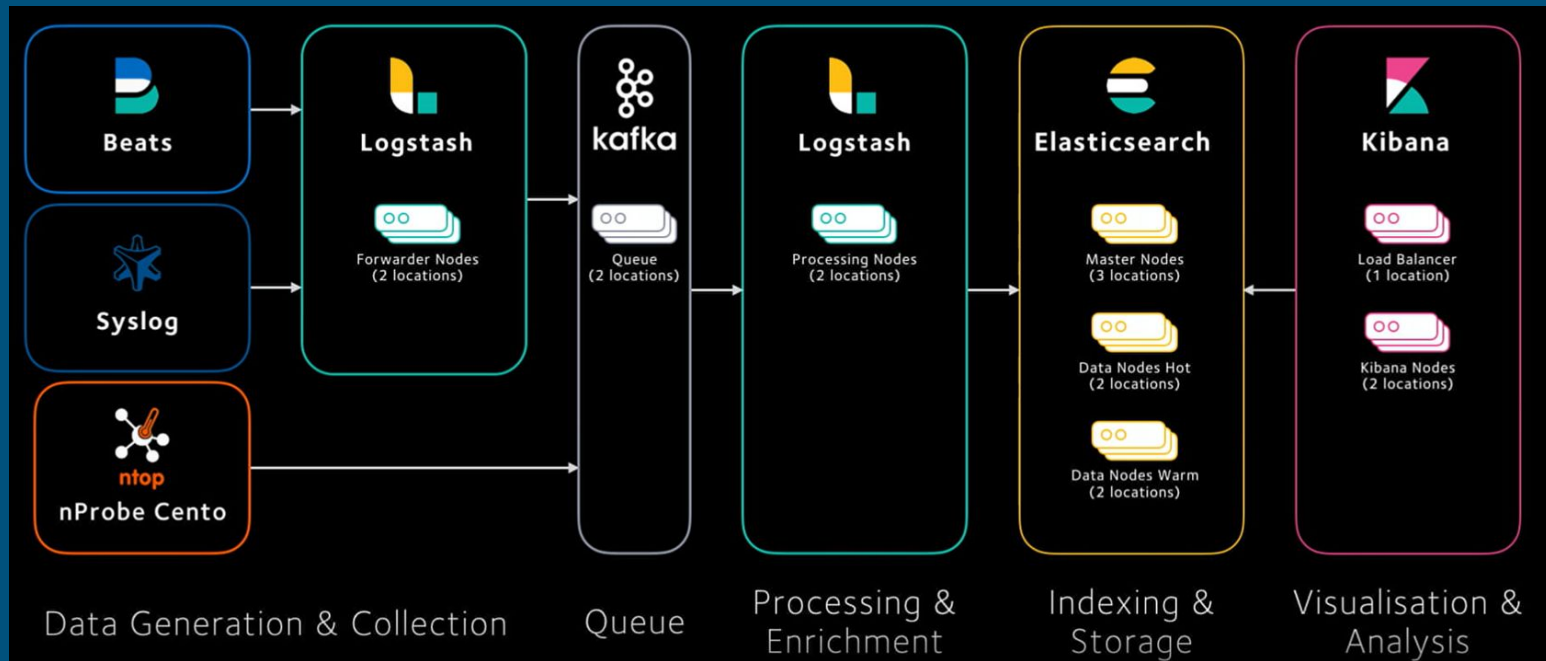
# Elasticsearch ML 案例3 - 哈佛大學開發新一代 SIEM

欄位統一:

Codec nProbe Cento	Logstash Module	FileBeat Module	Elastic Common Schema
netflow.ipv4_src_addr	netflow.src_addr	netflow.source_ipv4_address	source.ip
netflow.l4_src_port	netflow.src_port	netflow.tcp_source_port netflow.udp_source_port	source.port
netflow.in_pkts	netflow.packets	netflow.packet_total_count [ and many others ]	source.packets network.packets

# Elasticsearch ML 案例3 - 哈佛大學開發新一代 SIEM

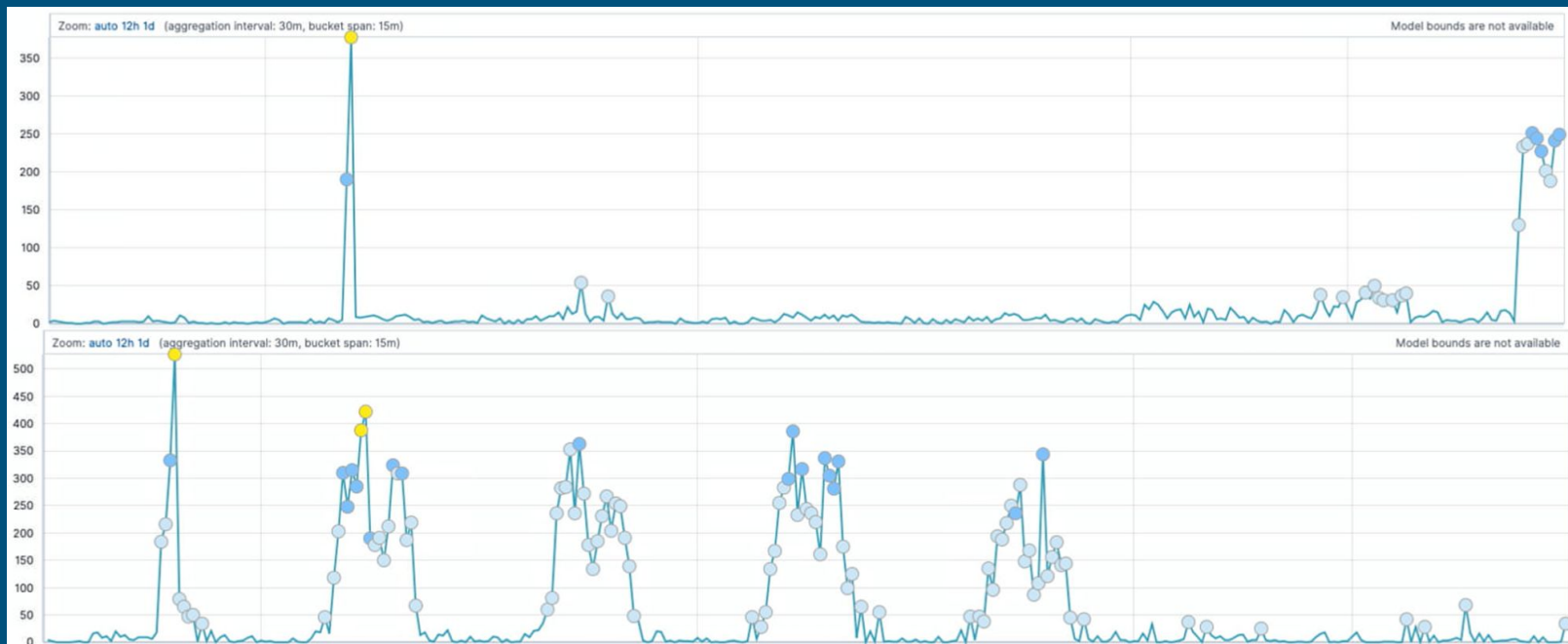
系統架構:





# Elasticsearch ML 案例3 - 哈佛大學開發新一代 SIEM

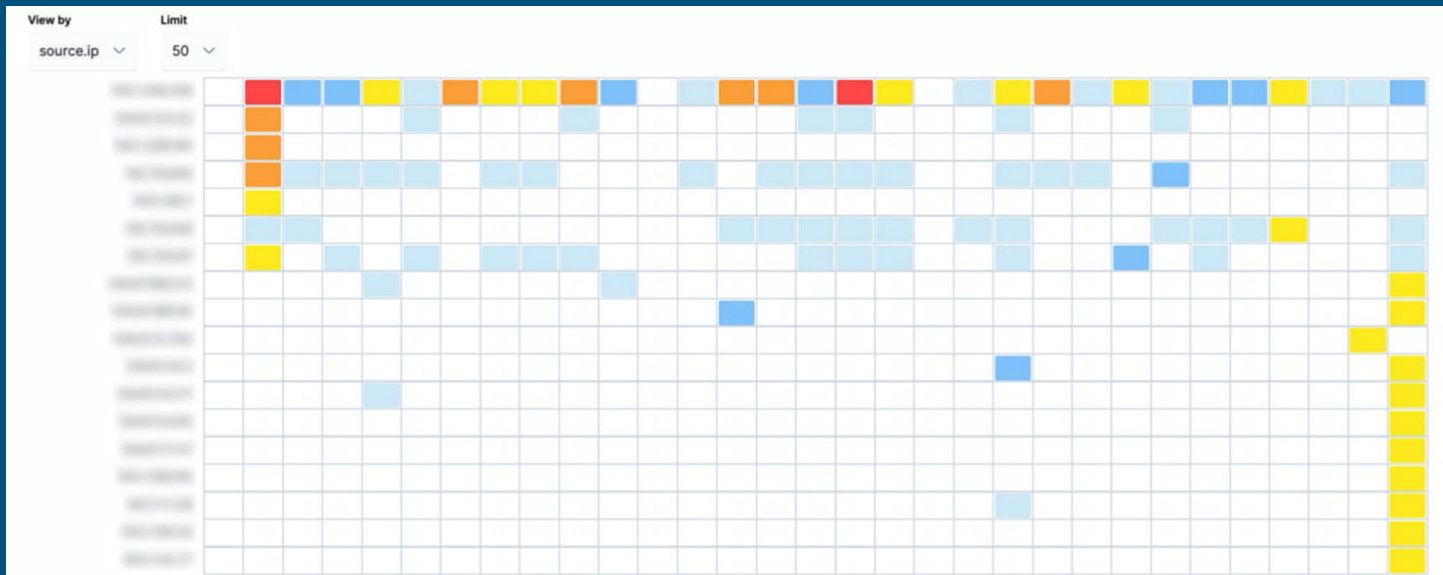
## ML 發現展示:





# Elasticsearch ML 案例3 - 哈佛大學開發新一代 SIEM

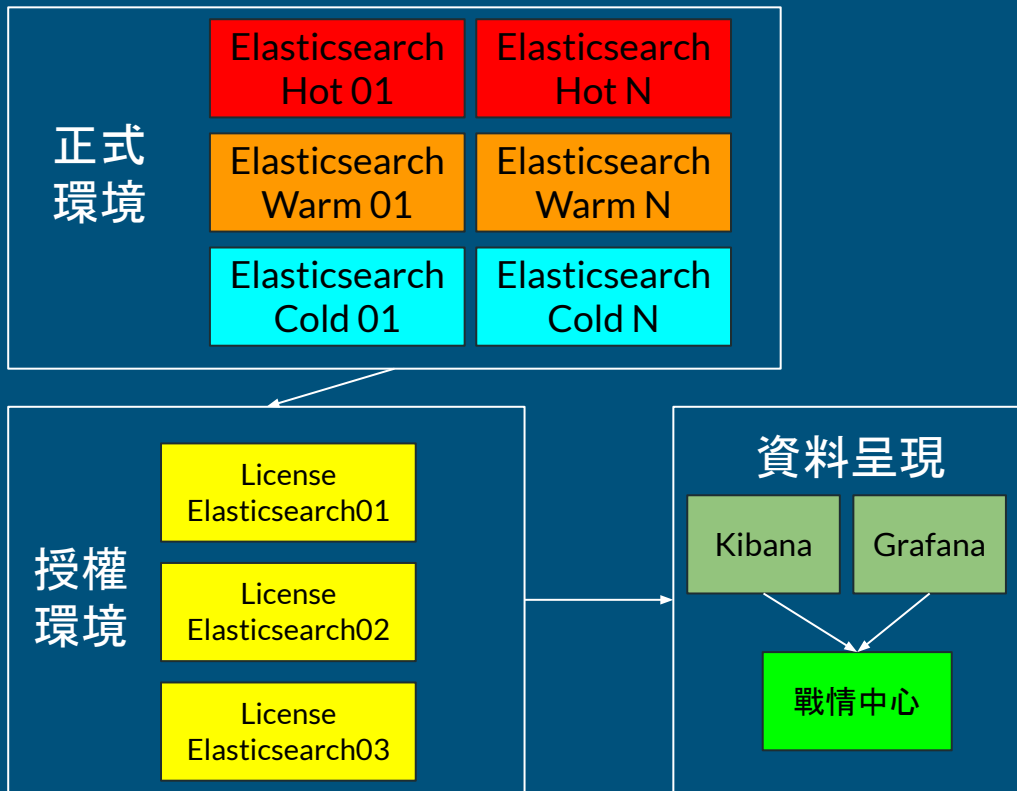
ML 發現展示:



# Elasticsearch ML 案例4 - 台灣中 X

系統規劃架構:


因預算有限, 將大部分資料儲存在正式環境中, 定時將處理後的資料寫入授權環境進行 Machine Learning 作業





# Elasticsearch ML Unsupervise Model 類型總覽


## Create a job from the data view Kibana Sample Data Flights


### Use a wizard


 **Single metric**  
Detect anomalies in a single time series.


 **Multi-metric**  
Detect anomalies with one or more metrics and optionally split the analysis.

 **Population**  
Detect unusual activity in a population. Recommended for high cardinality data.

 **Advanced**  
Use the full range of options to create a job for more advanced use cases.

 **Categorization**  
Group log messages into categories and detect anomalies within them.

 **Rare**  
Detect rare values in time series data.

 **Geo**  
Detect anomalies in the geographic location of the data.

### Learn more about your data

If you're not sure what type of job to create, first explore the fields and metrics in your data.

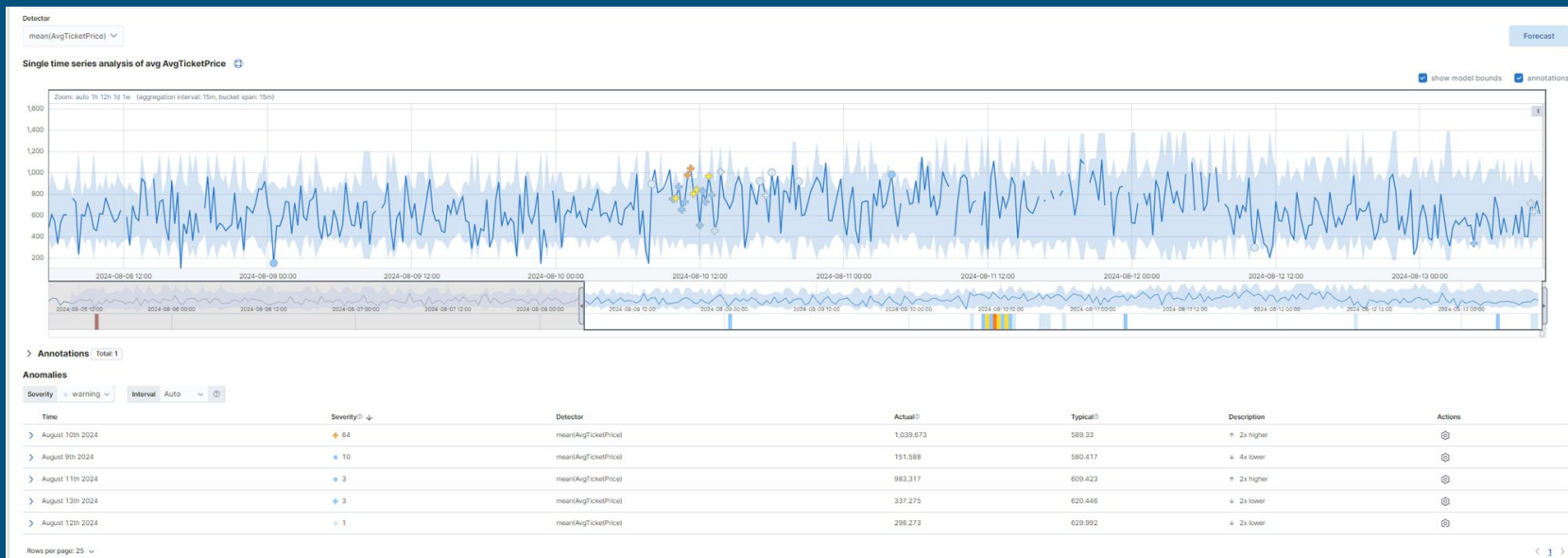
 **Data Visualizer**  
Learn more about the characteristics of your data and identify the fields for analysis with machine learning.

## Anomaly Detection:

1. Single metric: 單一維度基於時間的異常偵測
2. Multi metric: 多維度基於時間的異常偵測
3. Advanced: Single 和 Multi 的結合
4. Population: 單一維度基於同欄位其他值的異常偵測
5. Categorization: 單一維度基於分組的異常偵測，分組不能太多，一般用於系統 AP 日誌
6. Rare: 異常值出現頻率
7. Geo: 基於地理位置的異常偵測

# Elasticsearch ML 實際操作 - Unsupervised

## Single metrics: Averaged ticket price



# Elasticsearch ML 實際操作 - Unsupervised

## Single metrics: Averaged ticket price

### Description

Major anomaly in mean(AvgTicketPrice)

### Details on highest severity anomaly

Time	August 10th 2024, 11:15:00 to August 10th 2024, 11:30:00
Function	mean
Field name	AvgTicketPrice
Actual	1039.7
Typical	589.3
Job ID	flight001
Record score <sup>Ⓢ</sup>	64.433
Initial record score <sup>Ⓢ</sup>	64.433
Probability	0.00102


### Anomaly explanation [Learn more](#)

Anomaly type Spike over 7 buckets

#### Impact on initial score

Anomaly characteristics impact<sup>Ⓢ</sup> 

Single bucket impact<sup>Ⓢ</sup> 

Multi bucket impact<sup>Ⓢ</sup> 

Incomplete bucket<sup>Ⓢ</sup> Yes

結果說明: 在 8月10日 11:15:00 - 8月10日 11:30:00 間平均票價超過正常值兩倍

# Elasticsearch ML 實際操作 - Unsupervised

Mutli metrics: 通過分析 delayed flight minute 找出延遲異常的來源國家



# Elasticsearch ML 實際操作 - Unsupervised

Mutli metrics: 通過分析 delayed flight minute 找出延遲異常的來源國家

Anomalies

Severity warning Interval Auto

Time	Severity	Detector	Found for	Influenced by	Actual	Typical	Description	Actions
> August 7th 2024	97	mean(FlightDelayMin) partitionfield=OriginCountry	ZA	OriginCountry: ZA	105	0.149	↑ More than 100x higher	
> August 6th 2024	91	mean(FlightDelayMin) partitionfield=OriginCountry	CN	OriginCountry: CN	70	0.155	↑ More than 100x higher	
> August 7th 2024	80	mean(FlightDelayMin) partitionfield=OriginCountry	IT	OriginCountry: IT	345	35.532	↑ 10x higher	
> August 8th 2024	42	mean(FlightDelayMin) partitionfield=OriginCountry	AR	OriginCountry: AR	315	4.934	↑ 64x higher	
> August 12th 2024	38	mean(FlightDelayMin) partitionfield=OriginCountry	PL	OriginCountry: PL	270	4.37	↑ 62x higher	
> August 8th 2024	21	mean(FlightDelayMin) partitionfield=OriginCountry	DK	OriginCountry: DK	300	7.254	↑ 41x higher	
> August 7th 2024	17	mean(FlightDelayMin) partitionfield=OriginCountry	KR	OriginCountry: KR	40	0.521	↑ 77x higher	
> August 8th 2024	15	mean(FlightDelayMin) partitionfield=OriginCountry	KR	OriginCountry: KR	345	1.117	↑ More than 100x higher	
> August 11th 2024	13	mean(FlightDelayMin) partitionfield=OriginCountry	US	OriginCountry: US	360	12.08	↑ 30x higher	
> August 13th 2024	12	mean(FlightDelayMin) partitionfield=OriginCountry	CA	OriginCountry: CA	360	3.9	↑ 92x higher	
> August 6th 2024	11	mean(FlightDelayMin) partitionfield=OriginCountry	DE	OriginCountry: DE	360	0.622	↑ More than 100x higher	
> August 11th 2024	10	mean(FlightDelayMin) partitionfield=OriginCountry	AE	OriginCountry: AE	360	60.255	↑ 6x higher	
> August 8th 2024	8	mean(FlightDelayMin) partitionfield=OriginCountry	ZA	OriginCountry: ZA	315	0.456	↑ More than 100x higher	
> August 11th 2024	1	mean(FlightDelayMin) partitionfield=OriginCountry	IT	OriginCountry: IT	330	42.21	↑ 8x higher	
> August 11th 2024	< 1	mean(FlightDelayMin) partitionfield=OriginCountry	ZA	OriginCountry: ZA	285	3.123	↑ 91x higher	
> August 9th 2024	< 1	mean(FlightDelayMin) partitionfield=OriginCountry	ZA	OriginCountry: ZA	255	0.979	↑ More than 100x higher	

# Elasticsearch ML Supervise Model 類型總覽

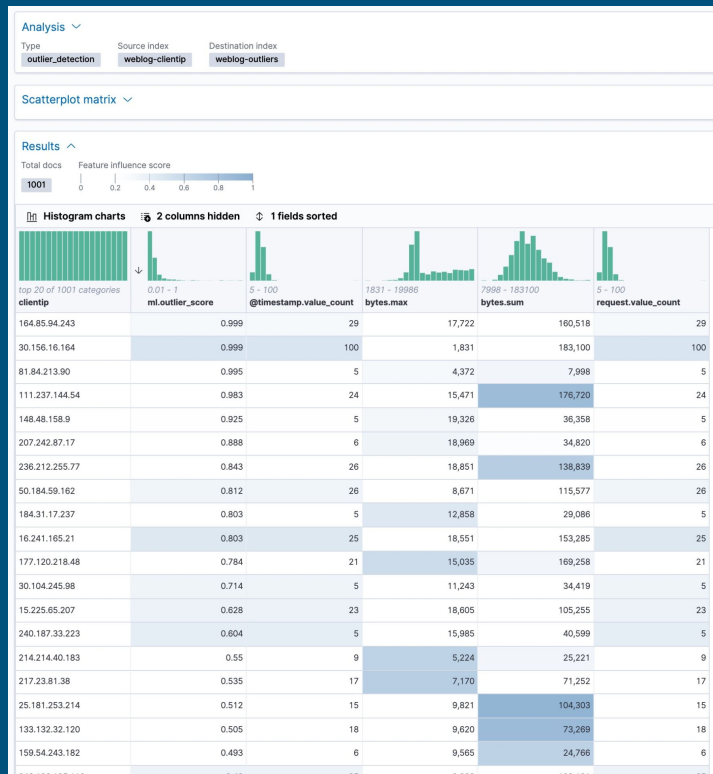
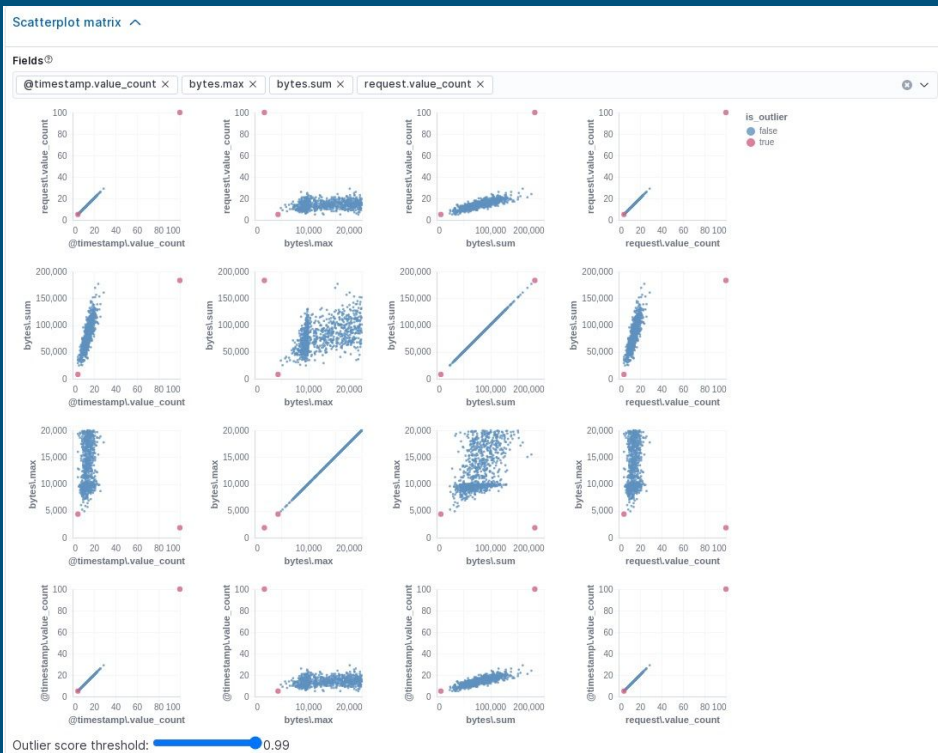
1 Configuration

## Data Frame Analytics:

1. Outlier detection: 異常政策
2. Regression: 預測
3. Classification: 資料分組



# Outlier - Supervised 結果展示



# Elasticsearch ML 實際操作 - Supervised 結果展示

