

Elastic – 最佳企業數據搜索分析工具

Elastic – 整合數據收集、儲存、分析與資安

Elastic 成立於 2012 年，隨著雲計算和物連網的興起，實時搜尋大量結構和非結構數據的需求也隨之而來。由於早期的搜尋工具不易擴展、費用昂貴，Elastic 建立一個開源、分佈式的數據搜尋方案解決問題。

Elastic Stack (ELK) 由全文搜尋引擎 Elasticsearch、資料收集引擎 Logstash、資料視覺化平台 Kibana、輕量資料採集工具 Beats 等開源軟體組成，形成具擴展性、易於管理及即時資料分析的整合解決方案。

其中 Elasticsearch 為實時搜尋與分析引擎，其擴展性可以在任何環境下快速搜索，並即時提供分析結果。Logstash 則是最先接觸日誌資料的系統，為一資料採集管道，再複雜的資料源都能快速轉換、傳送至 Elasticsearch。最後資料交由 Kibana 進行視覺化，客製化的儀表板與圖表提供絕佳的視覺體驗，也有**告警機制 (Alerting)** 能針對特定條件發出告警。

Elastic Stack 解決方案中也包含專為企業打造的 **Elastic Enterprise Search** 以及整合日誌、指標、APM 等資訊於一身的 **Elastic Observability**，僅需一個平台就能觀看所有資訊。

Elastic 是由 32 個國家的員工所組成的團隊，截至目前為止，Elastic 在全球有 3.5 億次下載、5,500 個企業用戶，其相關的社群更橫跨 100 多個國家，擁有超過 10 萬名社群成員。



- 1

FEATURE

架構靈活：基於 REST 和 JSON 的資料儲存方式
- 2

FEATURE

分佈式叢集、易於水平擴展
- 3

FEATURE

依 Apache Lucene 2.0 開源。無須編譯、下載即用
- 4

FEATURE

系統化管理與資安維護
- 5


FEATURE

基於 JVM 平台


探索 Elastic

Elastic 產品資訊


掌握產品新功能、研討會等最新動態！



2025.05.28 [錄下工作坊] Elastic 資安 AI 實戰 — 攻擊偵測 & 威脅狩獵全攻略



什麼是 RAG (檢索增強生成)？




整合 Elastic Security、HashiCorp Vault 與 Elastic APM 的全面防護與效能優化


查看更多

Elastic 成功案例


快來看看哪些企業利用 Elastic 獲得成功，您也可以！



Elastic APM 成功案例 | 阿聯酋杜拜國家銀行確保數十億資產的安全，並提高客戶滿意度和信任度



國家實驗室 Oak Ridge 以 Elastic 優化超級電腦



Elastic 提供如 T-Mobile 和 Netflix 的電信公司和媒體服務商即時洞察方案

查看更多

Elastic Stack 介紹

Elastic Stack - 分散式資料儲存平台

Elastic Stack 為現今最熱門的日誌管理平台，並簡稱為 ELK，是取自於其三個主要產品的字首作為縮寫：Elasticsearch、Logstash 及 Kibana。ELK 使日誌資料收集、儲存及分析能在一套系統之下完成，成為現今開發人員與 DevOps 工程師的首選。


在分散式架構中，資料以索引的方式儲存在**分片 (Shards)**內，在此可將每個分片視為一個 Lucene 索引，而 Elasticsearch 為每個分片建立副本，以確保某些節點故障或中斷連線時，分片副本內的資料仍能維持整個叢集正常運作，使 Elasticsearch 具高可用性。

Elasticsearch 不需徹底維修應用程式即可達成水平擴展，透過自動遷移分片以平衡多節點的集群，實現高擴展性與高可用性，因此支援 PB 等級的資料儲存。

Elastic Stack 可搭配以下插件擴充更多功能：


- Monitoring (監控)：透過 Kibana 輕鬆監控 Elasticsearch，實時檢視資料群集、索引與節點狀況。
- Security (安全)：為資料提供防護，也能執行更多安全管理，如：預防未授權的存取、加密處理等。
- Watcher (告警)：Watcher 能依情況設置執行指令，這對於業務端的資料流分析十分重要。也可以設置閾值警告，監測資料狀況。
- Graph (資料關聯性)：Graph 為基於 API 的 UI 的工具，利用 Elasticsearch 建立索引、查詢等功能，協助了解資料間的關聯性。

為何您需要 Elastic Stack



複雜的資料

隨著科技發展，許多企業面臨非結構化資料收集與統整的困境。Elastic Stack 能輕鬆處理不同來源的複雜資料，如：社群網站、地圖資訊、各式文件、機器設備等。其中 Logstash 備有許多針對特定資料源的插件以及插件編輯器，使 ELK 能讀取各類資料 (如：日誌、指標、應用程式、資料庫及雲端服務) 並進行轉換、輸出，解決了資料收集的難題。



多變的需求

如何有效率地處理巨量資料已被眾多企業所重視，要同時兼顧處理速度與完整度並非易事。


現今常見的資料處理需求如下：

- 不同的資料來源
- 監控系統與應用程式效能品質
- 管理巨量的資料與不同使用者
- 快速處理資料
- 要求資料品質與完整性

Elastic Stack 強大的功能可以解決一切


在競爭的環境下，現今企業更講求應用程式的監控與效率，如何自應用程式中提取複雜的日誌並做有效控管，是許多企業所重視的問題。

幸運的是，Elastic Stack 提供集中日誌管理的解決方案，如：從複雜資料源中傳送日誌，並轉換為結構化資料以供即時分析。ELK 提供針對資料叢集、節點、應用程式效能的監控儀表板，清楚呈現資料的狀態以做即時控管。其中 Elasticsearch 將資料儲存成 JSON 格式，並利用反向檢索 (Inverted Index) 以實時搜索文件，大幅提升檢索速度。此外，Kibana 集結圖表、地圖與篩選器，提升資料的品質與可視性，以達到資料完整性的需求。




日誌監控與分析
Logs Monitoring

透過機器學習，偵測異常的日誌資料並發出警告，隨時監控資料狀況




水平擴展
Horizontal Scale

Elastic Stack 無需終止應用程式，就能依照節點數量擴展展現視範圍




實時可用性
Real-Time Availability

Elastic Stack 最方便之處在於實時可用，能實時搜索、分析與創建圖表



彈性資料模組
Flexible Data Model

Elastic Stack 支援各種資料模組，便於資料儲存



快速查詢
Rapid Query

利用反向檢索 (Inverted Indices) 功能快速查找資料並即時獲得結果

Elastic 產品組合

Logstash

最佳日誌收集與轉換工具

Logstash 是 Elastic Stack 中重要的資料收集工具，負責日誌的接收 (Inputs)、過濾 (Filters) 與輸出 (Outputs)。即使資料複雜多元，Logstash 皆能靈活運用動態過濾器以找到正確資料，並即時轉換、傳送到指定之處，不受資料源格式、架構影響，解決了資料來源複雜的問題。

Logstash 擁有許多插件的可插拔架構，使其能混合與編排各種輸入方式，可以從特定的應用程式中獲取資料，無需額外繁瑣的程序，也有插件編輯器以支援多種資料源。憑藉大量吞吐資料的能力，Logstash 無需使用外部佇列層 (External Queueing Layer) 就能應付資料收取的高峰 (Ingestion Spikes) 以進行擴展。

Elasticsearch

Elastic Stack 的核心

作為 Elastic Stack 的核心，**Elasticsearch** 是基於 Apache Lucene 的分佈式、開源的搜尋引擎，主要用於全文搜索、分析與儲存資料。Elasticsearch 具備高度的擴展性，即使在上百個節點的環境，Elasticsearch 也能依您的需求自動擴展，高擴展性使您能輕鬆部署，進行大量的資料搜索。

Elasticsearch 對於資料儲存也十分彈性，無論是結構化或非結構性的資料、數位或地理資料，Elasticsearch 先進的資料庫技術讓您能針對各種格式的資料做檢索與儲存。(支援的資料類型包含：文字、數字、圖形、時間序列、地理數據、非結構化資料等)。

除了收集資料，Elasticsearch 備有完整的分析功能，能進一步整理並洞察資料。Elasticsearch 利用 **Aggregation** 模組將資料聚合並進行多種統計歸納，依您的需求客製化分析結果。常見的聚合有：指數型聚合 (Metric Aggregation)、桶型聚合 (Bucket Aggregation)、管道型聚合 (Pipeline Aggregation)、矩陣型聚合 (Matrix Aggregation) 等。

Kibana

最佳資料視覺化工具

Kibana 是開源的資料視覺化工具，強大的交互視覺化功能可以將匯集好的資料以圖表呈現。Kibana 提供多種圖表的預覽，運用預覽模式能找到最適合的資料呈現方式。

另一個 Kibana 的重點功能，是能即時集結圖表、地圖與篩選器形成儀表板，使用者能自行編輯，讓數據更為清晰生動，對於需進一步監測與分析應用程式的用戶提供完整的資訊。Kibana 也能對複雜的時間序列進行分析、轉換，直觀地將數據視覺化。Kibana 完整呈現資料，降低資料管理、分析的成本，且能即時偵測並於危機時發起警報，易於資料的控管。

Beats

完美的輕量資料採集工具

Beats 為 Elastic Stack 中開源的資料採集工具，主要用於輕量資料的收集，再發送至 Elasticsearch 及 Logstash 進行下一步的處理。Beats 的特點在於輕便，能以較少的資源處理資料，直接從伺服器上快速收錄輕量數據，無論是雲端、容器與各類系統上的資訊都能使用 Beats 來收集。

此外，Beats 透過無伺服器架構 (**Serverless Architectures**)，收集主機、容器平台與雲端環境的日誌及指標數據，以達到監控 Docker、K8s 等容器 (**Container Monitoring**) 和傳輸數據的目的。最新版本的 Beats 家族涵蓋各種客製化的輸送管道：

- Filebeat**：收集與傳送日誌文件
- Metricbeat**：收集與傳送指標資料
- Packetbeat**：收集與傳送網路資料
- Winlogbeat**：收集與傳送 Windows 事件
- Auditbeat**：收集與傳送系統數據
- Heartbeat**：收集與傳送網站運作資料
- Functionbeat**：收集與傳送雲端資料

Elastic Cloud

高效管理 Elastic Stack

Elastic Cloud 為 Elastic Stack 所提供的 SaaS 平台，主要特色是能快速部署並擴展專屬的 Elastic 產品叢集。有了 Elastic Cloud，即能獲得各類部署模板，在特定的環境下管理及監控 Elastic Stack 與 Kibana 等產品。

Elastic Cloud 也集各大功能於一身，在同一部裝置上即可匯入日誌資料、運用 Beats 從容器內傳送數據，也能使用 Elastic APM 控管程式碼，無需另外部署。Elastic Cloud 輕鬆建立集群的特色，使其成為現今開發人員優質的解決方案。

Elastic 帶來的資料安全

Elastic Security 能提供防範安全防護、檢測並排除惡意軟體的威脅。無論 Windows、MacOS、Linux 皆在保護範圍。其中 Elastic Agent 更快速地導入日誌並作安全監控，讓資料輸入或處理更簡便，另外 Limitless XDR 整合 SIEM 及 Endpoint 安全功能，即時導入日誌並排除威脅。

Elastic Agent – 易於部署與管理


自 7.14 版本 Elastic 正式推出了 **Elastic Agent**，幫助用戶更快設定日誌的導入。未來，Elastic Agent 將成為為每個主機添加日誌、指標和其他類型數據監控的單一方式。為了配合 Elastic Agent，Elastic Stack 同時也推出了 Fleet Server 幫客戶進行集中管理。Fleet 會在 Kibana 提供 Web 介面，讓客戶輕鬆群組監控系統，以大规模添加和管理 Elastic Agent 中的資訊。

Limitless XDR

Limitless XDR 代表著 Elastic 提供單一方案就實現 SIEM 跟 Endpoint Security。Elastic Security 能夠幫助客戶對所有數據進行分析，自動執行關鍵流程，並將原生的 Endpoint Security 引入每台主機。


- Limitless Visibility**
通過一個 Agent 就能添加不同的方案及導入日誌到 Elastic。
- Limitless Data**
客戶可以利用 Frozen Storage Data 儲存以年計算的歷史數據、威脅情報、報告等，將資料減到最低。
- Limitless Prevention And Detection**
Elastic Security 預設了五百多條安全檢測規則，無需複雜的設定即可使用。客戶亦可以創建適合自己環境的檢測規則，使用 Adaptive ML 模型發現威脅並降低告警疲勞、排檢並匹配檔案中的威脅情報，以找出新的漏洞攻擊標記。Elastic Security 亦支持通過將分析方案與 MITRE ATT&CK® 保持同步來提高計劃成熟度。
- Limitless Analysis**
客戶能透過 Elastic Security 去搜尋、關聯化安全日誌，以及利用機器學習尋找異常值。Security Analyst 亦可以使用靈活的 UI、內置案例管理和一系列新興的外部自動化功能，快速做出響應。
- Limitless Value**
Elastic Security 跟 Elastic Stack 的訂閱模式一樣，不會按 Agent 數目或數據量來收費。如果用戶已經訂閱 Elastic Stack，更新後就可以使用新版本的功能。

Elastic 內建功能




Elasticsearch For Apache Hadoop (ES-Hadoop)

Elasticsearch 被譽為雙向連接器，在 Map/Reduce 上運行的 ES-Hadoop 能讀取和寫入數據到 Elasticsearch、Hadoop，並實時查詢。ES-Hadoop 透過 REST 介面來運作，藉由降低伺服器所需的資源，以達到靈活部署。




Watcher

Watcher 是 Elasticsearch 的告警和通知的功能，它的設計宗旨是：如果可以查詢，就可以告警。Watcher 作為 Elasticsearch 的守門員，當有應用程式無回應、日誌受威脅等狀況，Watcher 即發出警告，讓您根據數據變化來採取行動。



Security

Security 為 Elasticsearch 帶來了企業級的安全性，保護 Elastic 插件間的加密通信、身份認證、基於角色的存取控制和權限。Security 強大的防護功能用來解決不斷增長的業務安全需求，提供 Elasticsearch 安全的數據環境。



Monitoring

Monitoring 為 Kibana 內建監控功能，為 Elasticsearch 的部署內容達到資料透明化，隨時監控 Elasticsearch 集群活動、快速診斷問題、微調和優化性能，將 Elasticsearch 的效益最大化。

關於 Elastic 你可能想問

為何企業喜歡使用 Elasticsearch?

➤

Kibana 是什麼?

➤

為什麼要使用 Kibana?

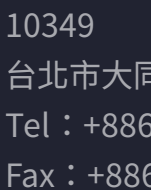
➤

Logstash 的用途為何?

➤

想了解更多 Elastic 資訊嗎？
歡迎與我們聯繫，由專人為您服務

免費諮詢



歐立威科技

歐立威科技股份有限公司
Omniwaresoft Technology Inc.
開源軟體解決方案代理商

◎ 台北總公司
10349
台北市大同區鄭州路 87 號 11 樓之 1
Tel：+886-2-2558-2656
Fax：+886-2-2558-5559

關於我們

關於歐立威
服務項目
加入我們
聯絡我們

追蹤我們

- 歐立威 Facebook 粉專
- 歐立威 LINE 官方帳號
- 歐立威 Youtube 頻道
- 歐立威 Accupass 活動列表
- 歐立威 LinkedIn

訂閱電子報

掌握活動資訊 & 產業動向

電子信箱 *

訂閱

Copyright © Omniwaresoft Tech Inc. All Rights Reserved. | Privacy Policy

