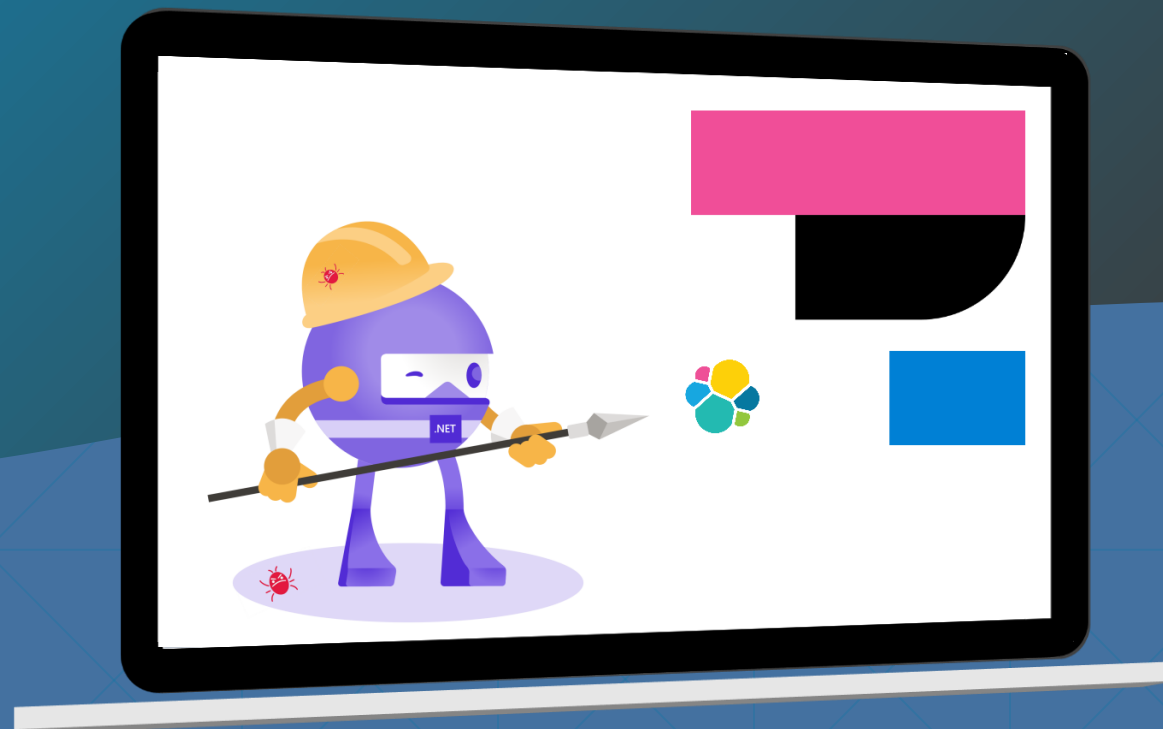


Elastic APM 的兩三事

Roberson Liou



歡迎參加我們的每週四固定聚會



關於我

- Backend / Cloud
- Microsoft MVP (2020-2023)
- twMVC 核心成員
- DevOps Taiwan 志工
- BLOG - 工程良田的小球場



大綱

- Introduction
- Features
- Operations



<https://github.com/robersonliou/ElasticApmNet7>

你的 Elasticsearch 安全嗎？

- 黑暗執行緒 - iRent 個資外洩事件是怎麼一回事？
- 中國笨鳥公司Elasticsearch資料庫配置不當，洩漏全球2.14億人個資
- 這些不是個案！



Elasticsearch 資安小提醒

- 啟用 Security feature
 - 8.x 版後預設啟用
 - SSL/TLS
 - Enrollment Token 機制
- 適當的帳號權限設定
 - 不使用 admin 帳號進行操作
 - 不要設定空密碼
- 開啟 Audit log
 - 預設是 disable
- 網路層防護
 - 架設防火牆
 - IP 白名單管控
 - 搬入內網

Introduction

APM 是什麼？

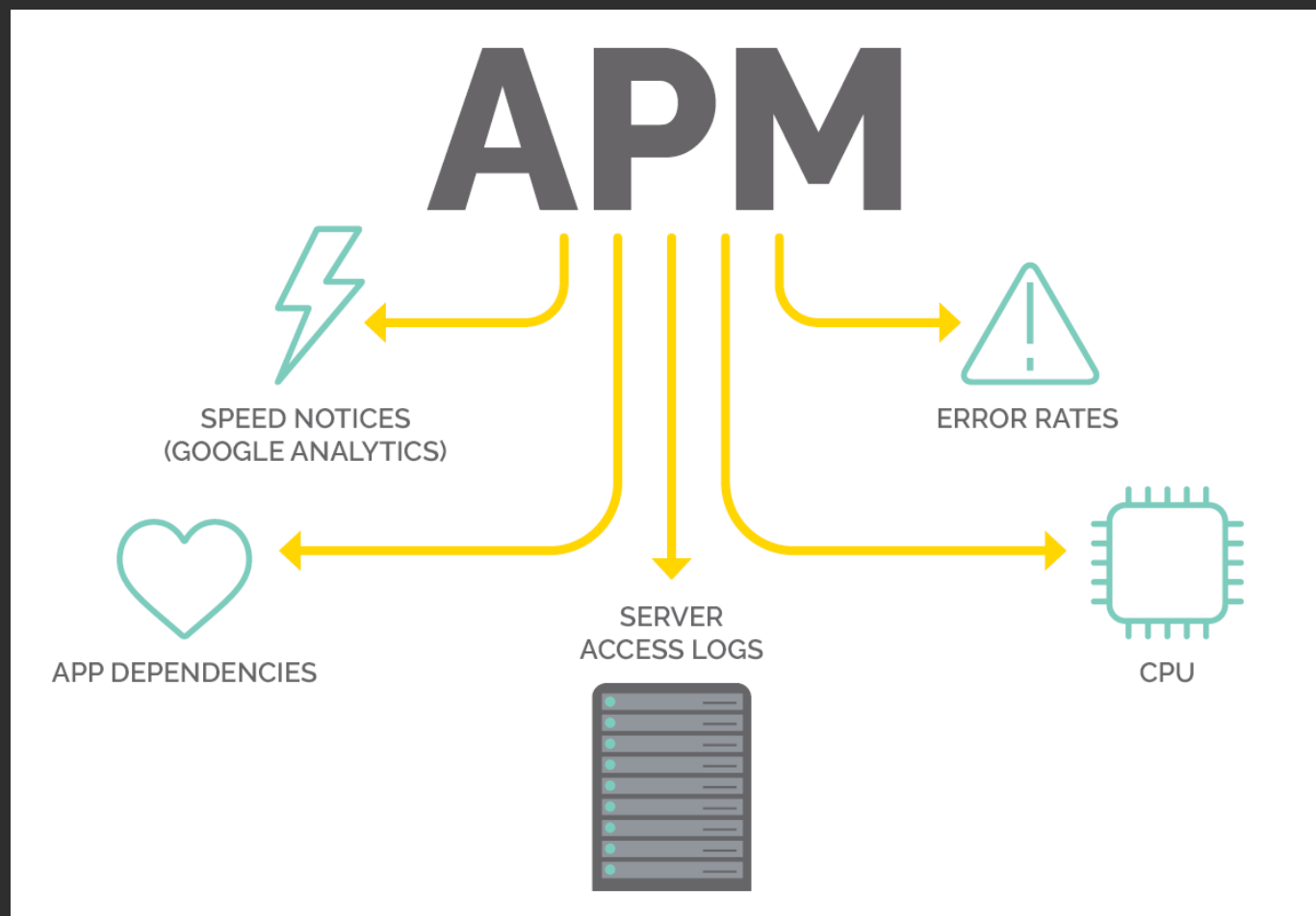
- Application Performance Monitoring(Management)
- 聽聽 ChatGPT 怎麼說



應用程式效能監控 (APM) 是一種軟件工具，用於監控應用程式的效能並提供解決效能問題的資訊。APM 能追蹤應用程式的內部運作，透過分析資料來偵測問題，如異常、漏洞、資源佔用等。APM 的目標是確保應用程式能順利且有效地運行，並發現並修正任何效能問題。

我覺得 APM 是...

- 工具 / 平台？
- 提升可觀測性的方法之一
- Data Driven
 - 收集
 - 分析
 - 監控



APM 存在的目的

- 提升客戶滿意度
- 降低 MTTR
- 識別瓶頸，持續改善

APM Family



Elastic APM

- Open Source
- Gartner APM 榜上 4.5 ★ 評價
- 提供多樣的佈署模式 (雲、地)
- 提供 10+ 語言支援
- 提供 OpenTelemetry 整合





Elastic Observability Reviews

by Elastic in Application Performance Monitoring and Observability

4.5 ★★★★★ 114 Ratings

elastic / apm Public

Fork 94

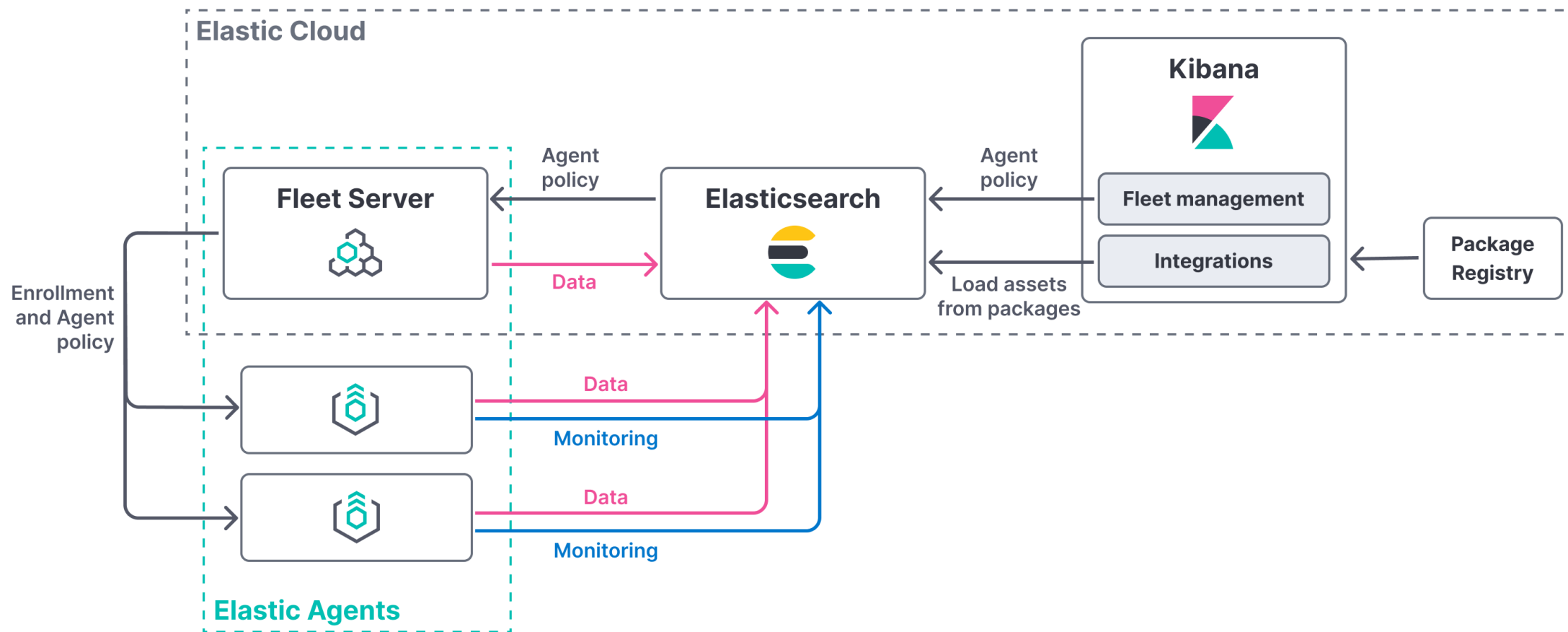
Starred 305

Android Agent (🚧 In Development)	apm-agent-android	elastic.co
Go Agent	apm-agent-go	elastic.co
iOS Agent (🚧 In Development)	apm-agent-ios	elastic.co
Java Agent	apm-agent-java	elastic.co
JavaScript RUM Agent	apm-agent-rum-js	elastic.co
Node.js Agent	apm-agent-nodejs	elastic.co
PHP Agent	apm-agent-php	elastic.co
Python Agent	apm-agent-python	elastic.co
Ruby Agent	apm-agent-ruby	elastic.co
.NET Agent	apm-agent-dotnet	elastic.co

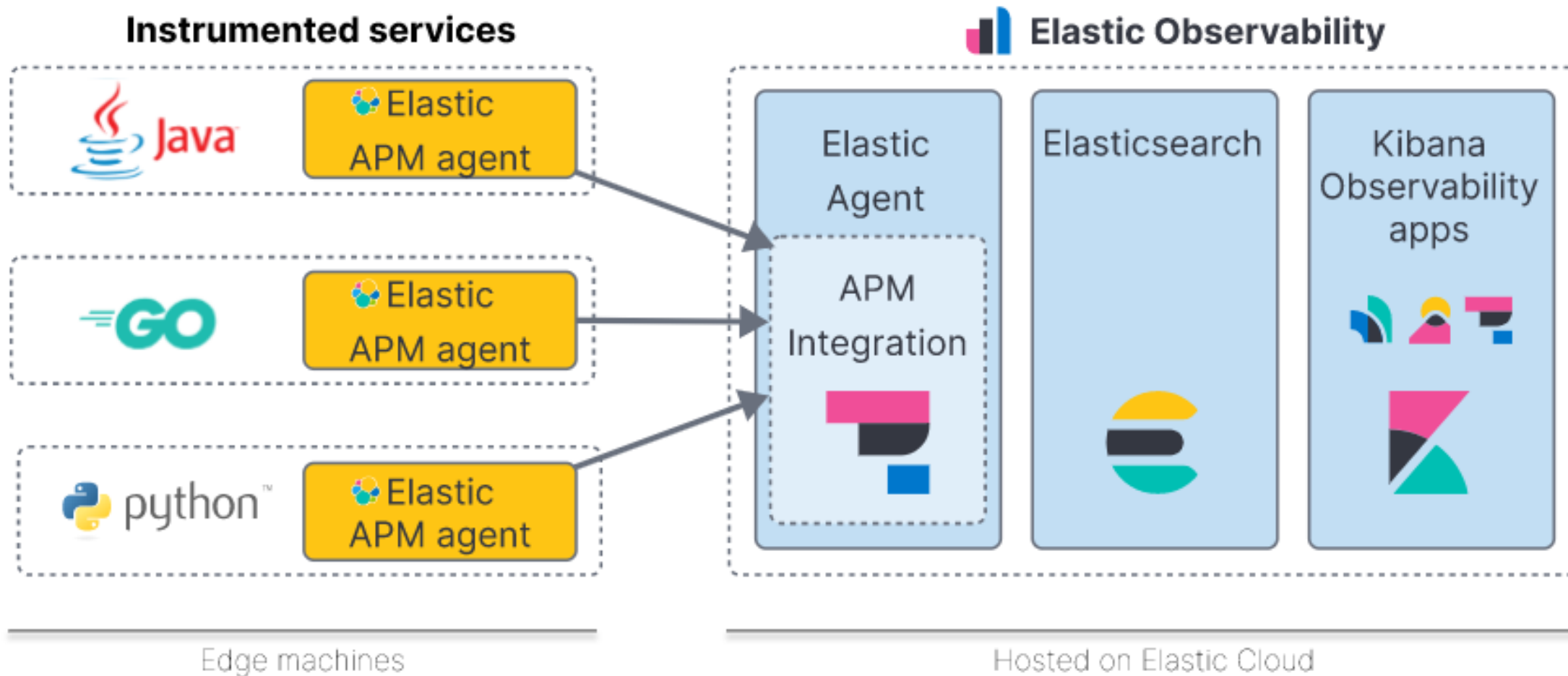
Elastic APM 核心成員

- **Elasticsearch** : 資料儲存
- **Kibana** : UI介面
- **Fleet Server** : 管理 Elastic Agent
- **Elastic Agent** : APM Server , 傳送 APM 資料的媒介
- **Elastic APM Agent** : APM Client , 透過安裝 SDK 形式

Elastic APM 架構流程(1)

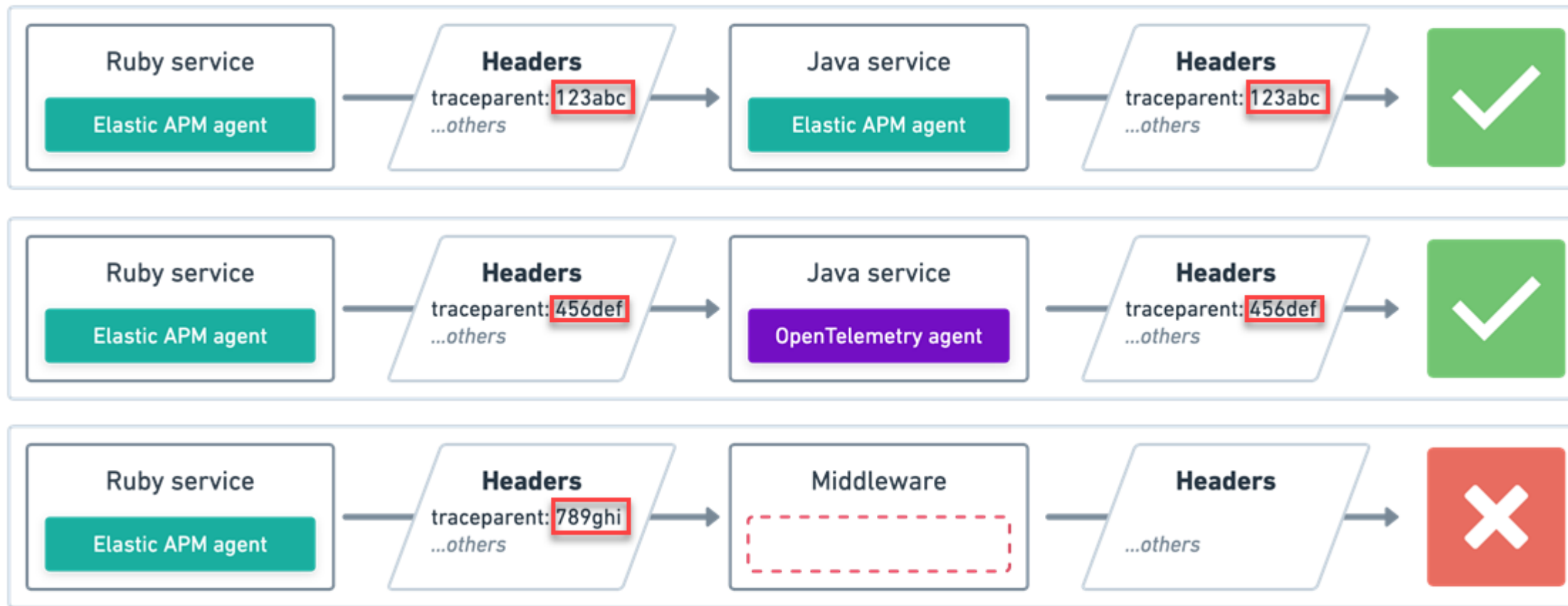


Elastic APM 架構流程(2)



分散式追蹤 (Distributed Tracing)

- 以 **trace.id** 貫穿整段 E2E 交易流程



Features

驗證方式 (Authentication)

- Secret Token
- API Key
 - Kibana 預設產生格式為 Base64
 - 解開才有 APIKey ID & API Key
- Anonymous

Agent authorization

☒ API key for agent authentication Optional
Enable API Key auth between APM Server and APM Agents.

Maximum number of API keys of Agent authentication
Restrict number of unique API keys per minute, used for auth between APM Agents and Server.

Number of keys Optional
100
Might be used for security policy compliance.

Secret token Optional

Settings

General settings Agent Configuration **Agent Keys** Anomaly detection Custom Links Indices

View and delete APM agent keys. An APM agent key sends requests on behalf of a user.

APM agent keys [+ Create APM agent key](#)

Search...

Name	User	Realm	Created
demo-apm-key	2715104963	cloud-saml-kibana	31 minutes ago

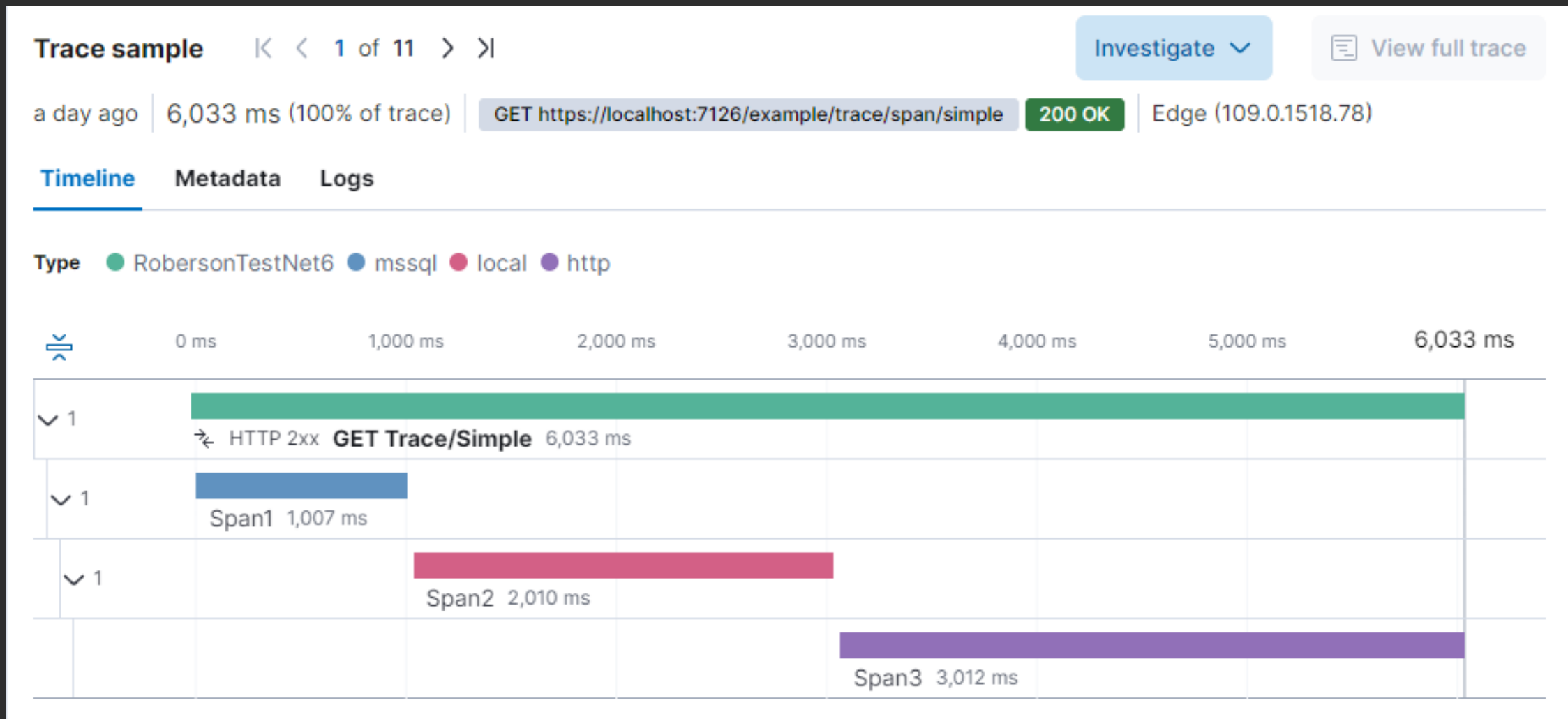
資料模型 (Data Model)

- Traces
 - Spans
 - Transactions
- Errors
- Metrics

Traces

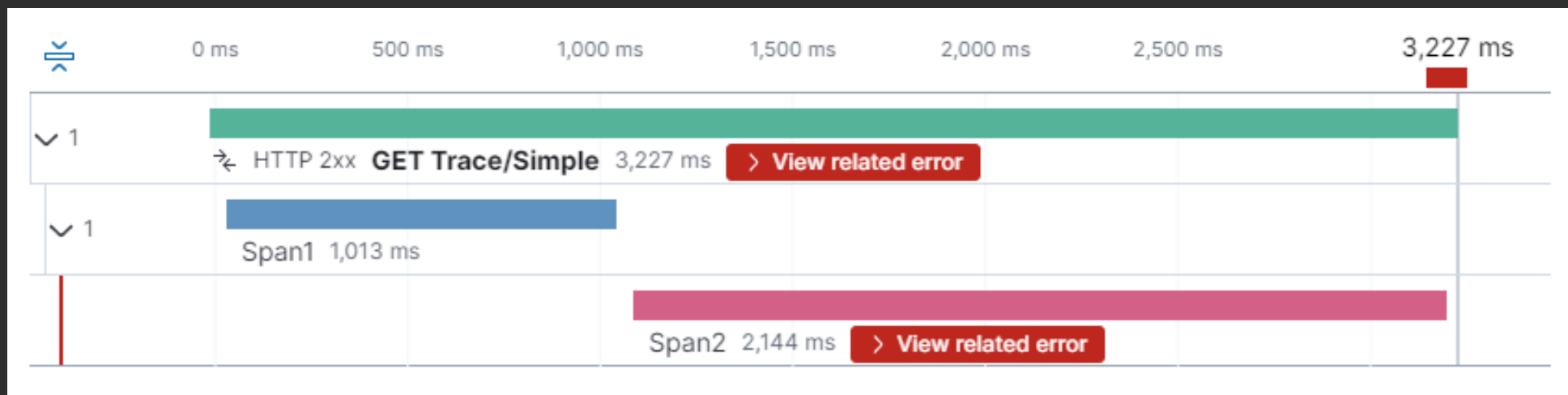
- Span：量測一段時間的最小單位
 - 某段 LINQ 語法的執行時間
 - 某段 SQL 語法的執行時間
- Transaction：最高維度的量測單位，可由數個 Span 組成
 - 發送一個 HTTP 請求的執行時間
 - 觸發一次排程的執行時間

Traces - Kibana



Errors

- 原始的例外錯誤
- 從底層 CLR 自動捕捉例外，也可手動回傳
- 搭配 **span** 可更快速定位錯誤可能原因





要來寫扣啦

.NET

Elastic APM x .NET

- 支援 .NET Framework 及 .NET Core
 - .NET Core >= 2.1 / .NET Framework >= 4.6.1
 - 本議程會以 .NET 7 作為範例介紹
- APM 套件
 - ASP.NET Core : [Elastic.Apm.NetCoreAll](#)
 - ASP.NET : [Elastic.Apm.AspNetFullFramework](#)

設定方式

- 組態設定

- 透過環境變數及 `IConfiguration` 方式設定
- 要特別留意預設值

- 程式碼

- 以 `Middleware` 方式設定
- APM Client 會自動從有註冊的 `IDiagnosticsSubscriber` 收集資料
- 細部調整可參考 [Public API](#)

常用組態設定 (Configuration)

名稱	說明	預設值
<u>ServerUrl</u>	Elastic Agent 網址	<none>
<u>ServiceName</u>	服務名稱	<none>
<u>Environment</u>	應用程式環境	<none>
<u>SecretToken</u>	驗證	<none>
<u>ApiKey</u>	驗證	<none>
<u>Enabled</u>	功能開關	true
<u>TransactionSampleRate</u>	取樣比率	1.0
<u>FlushInterval</u>	APM Event Queue 清除週期	10s
<u>MaxBatchEventCount</u>	單筆請求最大的 Event 數量	10

範例 - 設定 APM 整合

■ appsettings.json

```
{  
  "ElasticApm": {  
    "ServerUrl": "YOUR_ELASTIC_APM_HOST",  
    "ServiceName": "YOUR_SERVICE_NAME",  
    "SecretToken": "YOUR_SECRET_TOKEN",  
    "Environment": "YOUR_ENVIRONMENT"  
  }  
}
```

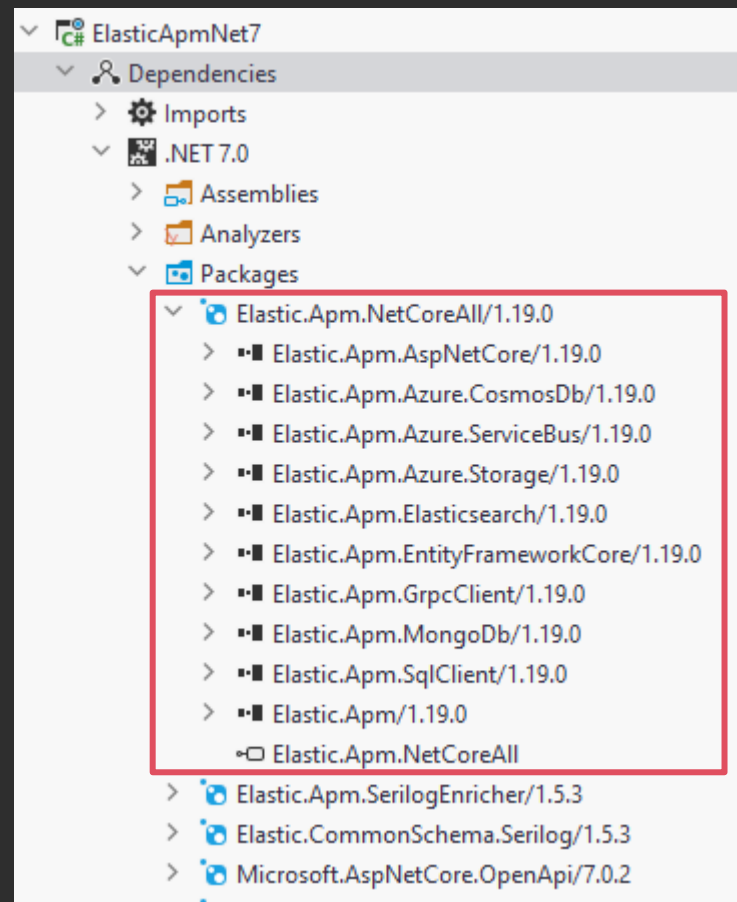
■ Program.cs

```
var builder = WebApplication.CreateBuilder(args);  
//...  
var app = builder.Build();  
app.UseAllElasticApm(app.Configuration);  
//...
```

UseAllElasticApm 實作

- 預設實作多個 IDiagnosticSubscriber

```
public static IApplicationBuilder UseAllElasticApm(
    this IApplicationBuilder builder,
    IConfiguration configuration = null
) => AspNetCore.ApmMiddlewareExtension
    .UseElasticApm(builder, configuration,
        new HttpDiagnosticsSubscriber(),
        new EfCoreDiagnosticsSubscriber(),
        new SqlClientDiagnosticSubscriber(),
        new ElasticsearchDiagnosticsSubscriber(),
        new GrpcClientDiagnosticSubscriber(),
        new AzureMessagingServiceBusDiagnosticsSubscriber(),
        new MicrosoftAzureServiceBusDiagnosticsSubscriber(),
        new AzureBlobStorageDiagnosticsSubscriber(),
        new AzureQueueStorageDiagnosticsSubscriber(),
        new AzureFileShareStorageDiagnosticsSubscriber(),
        new AzureCosmosDbDiagnosticsSubscriber(),
        new MongoDBDiagnosticsSubscriber());
```

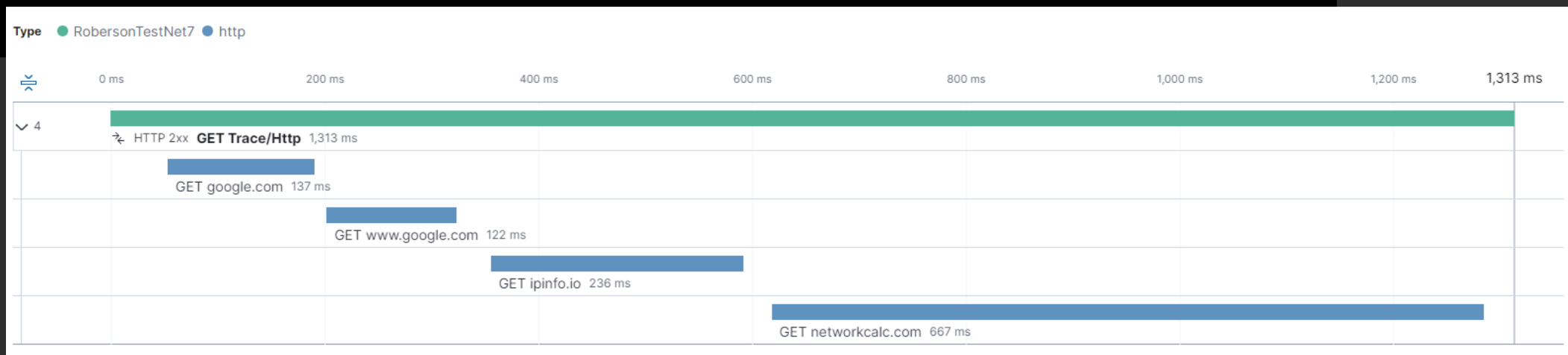


範例 - HTTP Trace

```
[HttpGet("http")]
public async Task<IActionResult> Http()
{
    var client = _factory.CreateClient();

    await client.GetAsync("https://google.com");
    await client.GetAsync("https://ipinfo.io");
    await client.GetAsync("https://networkcalc.com/api/ip/192.168.1.1/24");

    return Ok(new
    {
        Message = "http client tracing sample"
    });
}
```



APM 如何與 Log 整合?

- Log 需包含以下屬性
 - `service.name`
 - `trace.id`
 - `transaction.id`
- 可透過 Log 套件整合
 - [Serilog](#)
 - [NLog](#)

Log 整合 - Serilog

- 安裝套件
 - [Elastic.Apm.SerilogEnricher](#)
 - [Serilog.Sinks.Elasticsearch](#)
 - [Elastic.CommonSchema.Serilog](#)
 - [Serilog.AspNetCore](#)
- 在 **WebApplicationBuilder** 階段註冊

Log 整合 - Serilog 設定

```
var formatter = new EcsTextFormatter(new EcsTextFormatterConfiguration()
    .MapCustom((ecsDoc, log) =>
    {
        ecsDoc.Service = new Service { Name = "ELASTIC_SERVICE_NAME" };
        return ecsDoc;
    }));

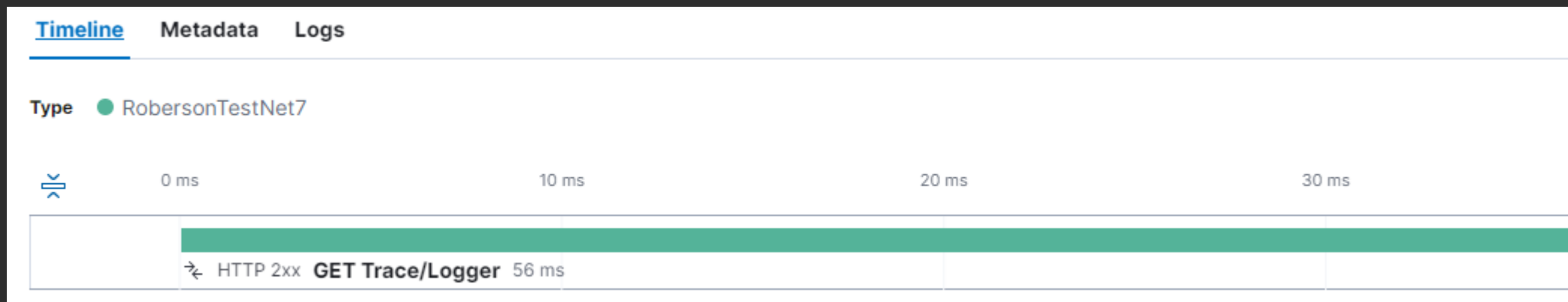
builder.Host.UseSerilog((context, services, config) =>
    config
        .Enrich.WithElasticApmCorrelationInfo()
        .WriteTo.Elasticsearch(new ElasticsearchSinkOptions(
            new Uri("ELASTIC_SERVER_URL"))
            {
                IndexFormat = "ELASTIC_INDEX_FORMAT",
                CustomFormatter = formatter,
                ModifyConnectionSettings = x => x
                    .ApiKeyAuthentication("ELASTIC_APIKEY_ID", "ELASTIC_APIKEY")
                    .ConnectionLimit(-1)
            }
        )
        .WriteTo.Console(formatter)
    );
```

Log 整合 - 範例

```
[HttpGet("logger")]
public async Task<IActionResult> Logger()
{
    _logger.Information("log info in trace...");
    _logger.Warning("log warning in trace...");
    _logger.Error("log error in trace...");

    return Ok(new
    {
        Message = "Trace & Logger"
    });
}
```


Log 整合 - Kibana



Timeline Metadata Logs

Timestamp	Service Name	Message
Showing entries from Feb 10, 15:58:35		
15:58:35.000	RobersonTestNet7	[Information] log info in trace...
15:58:35.009	RobersonTestNet7	[Warning] log warning in trace...
15:58:35.015	RobersonTestNet7	[Error] log error in trace...

SeriLog - RequestLoggingMiddleware

Message

```
[Information] Request finished HTTP/2 GET https://localhost:7205/swagger/v1/swagger.json - - - 200 - application/json; charset=utf-8 102.9544ms
[Information] Request starting HTTP/2 GET https://localhost:7205/example/trace/logger - -
[Information] Executing endpoint '"ElasticApmNet7.Controllers.TraceController.Logger (ElasticApmNet7)"'
[Information] Route matched with "{action = \"Logger\", controller = \"Trace\"}". Executing controller action with signature "System.Threading.Tasks.Task`1[Microsoft.AspNetCore.Mvc.IActionResult] Logger()" on controller "ElasticApmNet7.Controllers.TraceController" ("ElasticApmNet7").
[Information] Executing action method "ElasticApmNet7.Controllers.TraceController.Logger (ElasticApmNet7)" - Validation state: Valid
[Information] log info in trace...
[Warning] log warning in trace...
[Error] log error in trace...
[Information] Executed action method "ElasticApmNet7.Controllers.TraceController.Logger (ElasticApmNet7)", returned result "Microsoft.AspNetCore.Mvc.OkObjectResult" in 22.998ms.
[Information] Executing "OkObjectResult", writing value of type '"<>f__AnonymousType0`1[[System.String, System.Private.CoreLib, Version=7.0.0.0, Culture=neutral, PublicKeyToken=7cec85d7bea7798e]]"''.
[Information] Executed action "ElasticApmNet7.Controllers.TraceController.Logger (ElasticApmNet7)" in 93.874ms
[Information] Executed endpoint '"ElasticApmNet7.Controllers.TraceController.Logger (ElasticApmNet7)"'
[Information] Request finished HTTP/2 GET https://localhost:7205/example/trace/logger - - - 200 - application/json; charset=utf-8 184.2800ms
```

Serilog - 如何過濾預設的 Request Log

■ 調整 LogLevel

```
builder.Host.UseSerilog((context, services, config) =>
    config
        .MinimumLevel.Override("Microsoft", LogEventLevel.Warning)
        .MinimumLevel.Override("Microsoft.AspNetCore", LogEventLevel.Warning)
        .Enrich.WithElasticApmCorrelationInfo()
        //...
)
```

Message

```
[Information] log info in trace...
[Warning] log warning in trace...
[Error] log error in trace...
[Information] log info in trace...
[Warning] log warning in trace...
[Error] log error in trace...
```

敏感的資料怎麼辦？

- 資料遮罩(data filter)
 - 有提供預設值
- 調整方式
 - 程式碼：SanitizeFieldNames 組態
 - Kibana：Agent configuration

Environment variable name	IConfiguration key
ELASTIC_APM_SANITIZE_FIELD_NAMES	ElasticApm:SanitizeFieldNames

Sanitize field names

Sometimes it is necessary to sanitize, i.e., remove, sensitive data sent to Elastic APM. This config accepts a list of wildcard patterns of field names which should be sanitized. These apply to HTTP headers (including cookies) and `application/x-www-form-urlencoded` data (POST form fields). The query string and the captured request body (such as `application/json` data) will not get sanitized.

Default: password, passwd, pwd, secret, *key, *token*, *session*, *credit*, *card*, authorization, set-cookie

sanitize_field_names

Operations



服務架設

- Elastic Cloud

- 要錢，但方便省事（30 天免費試用）
- 三朵雲都有，可自動版更

- Self Hosting

- 平台維護需有專員管理（資料、憑證、內網）
- 部分功能需購買授權（ex: Alert / Service Map）

APM 資料預設保留幾天呢?

- 依資料類型區分

- Traces : 10 天

- Metrics : 90天

- Errors : 10 天

- Rollover

- 30 天

- 50 GB

Data stream	Rollover after	Delete after
traces-apm	30 days / 50 GB	10 days
traces-apm.rum	30 days / 50 GB	90 days
metrics-apm.internal	30 days / 50 GB	90 days
metrics-apm.app	30 days / 50 GB	90 days
logs-apm.error	30 days / 50 GB	10 days

調整 APM 資料保留天數

- 調整 APM 的 **ILM** (Index Lifecycle Management)

The screenshot shows the 'Index Lifecycle Policies' page in the Elasticsearch Management UI. The left sidebar contains navigation links for Management, Ingest, Data, Alerts and Insights, and Security. The 'Index Lifecycle Policies' link under the Data section is highlighted. The main content area shows a search bar with 'apm' entered and a toggle switch for 'Include managed system policies' which is turned on. Below this is a table listing several policies, each with a 'Managed' status tag, a count of linked index templates, a count of linked indices, a modified date, and action icons.

Name ↑	Linked index templates	Linked indices	Modified date	Actions
logs-apm.app_logs-default_policy Managed	1	0	Jan 25, 2023	+ 🗑️
logs-apm.error_logs-default_policy Managed	1	1	Jan 25, 2023	+ 🗑️
metrics-apm.app_metrics-default_policy Managed	1	0	Jan 25, 2023	+ 🗑️
metrics-apm.internal_metrics-default_policy Managed	1	1	Jan 25, 2023	+ 🗑️
traces-apm.rum_traces-default_policy Managed	1	0	Jan 25, 2023	+ 🗑️
traces-apm.sampled_traces-default_policy Managed	1	0	Jan 25, 2023	+ 🗑️
traces-apm.traces-default_policy Managed	1	1	Jan 25, 2023	+ 🗑️

冷知識 - APM 資料存在哪裡?

- 存放在 Elasticsearch 中
- Index pattern : `<type>-<dataset>-<namespace>`
 - Traces: `traces-apm-<namespace>`
 - Errors: `<namespace>`
 - Metrics: `metrics-apm.*-<namespace>`

情境題 – 多產品團隊的資料管理

- 假設有兩個產品團隊，分別使用以下的 space
 - abc
 - def
- 如何讓各團隊只看自己的 APM 資料?
 1. 調整 APM 寫入的 space
 2. 設定 **filtered alias**

1. 修改 APM 寫入的 space

- 可在 Elastic Agent Policy 調整
- 優點：操作方便
- 缺點：Elastic Agent 僅能提供單一產品團隊使用

The screenshot shows the 'Elastic Cloud agent policy' settings page. At the top, there's a header with the title 'Elastic Cloud agent policy' and a lock icon. To the right of the title are statistics: 'Revision 4', 'Integrations 2', 'Agents 1 agent', and 'Last updated on Jan 25, 2023'. An 'Actions' dropdown menu is on the far right. Below the header, there's a sub-header 'Default agent policy for agents hosted on Elastic Cloud'. The main content area has two tabs: 'Integrations' and 'Settings', with 'Settings' being the active tab. Under 'Settings', there are three sections: 'General settings' with a 'Name' field containing 'Elastic Cloud agent policy'; 'Description' with a text area containing 'Default agent policy for agents hosted on Elastic Cloud'; and 'Default namespace' with a dropdown menu showing 'default' and a 'Learn more' link.

Elastic Cloud agent policy

Revision **4** | Integrations **2** | Agents **1 agent** | Last updated on **Jan 25, 2023** | [Actions](#)

Default agent policy for agents hosted on Elastic Cloud

[Integrations](#) [Settings](#)

General settings

Choose a name and description for your agent policy.

Name

Elastic Cloud agent policy

Description

Add a description of how this policy will be used.

Default agent policy for agents hosted on Elastic Cloud

Default namespace

Namespaces are a user-configurable arbitrary grouping that makes it easier to search for data and manage user permissions. A policy namespace is used to name its integration's data streams. [Learn more](#)

default

2. 設定 filtered alias

- Alias 提供 filter 語法
- 三種資料模型都要設定
 - Traces / Metrics / Errors
- 服務名稱要經過設計
 - {space}-{application}
 - abc-myweb-1

```
POST /_aliases?pretty
{
  "actions": [
    {
      "add": {
        "index": "traces-apm*",
        "alias": "{space}-traces-apm",
        "filter": {
          "wildcard": {
            "service.name": {
              "value": "{space}-*"
            }
          }
        }
      }
    }
  ]
}
```

```
GET traces-apm*/_alias
```

abc space

```
POST /_aliases?pretty
{
  "actions": [
    {
      "add": {
        "index": "traces-apm*",
        "alias": "abc-traces-apm",
        "filter": {
          "wildcard": {
            "service.name": {
              "value": "abc-*"
            }
          }
        }
      }
    }
  ]
}
```


def space

```
POST /_aliases?pretty
{
  "actions": [
    {
      "add": {
        "index": "traces-apm*",
        "alias": "def-traces-apm",
        "filter": {
          "wildcard": {
            "service.name": {
              "value": "def-*"
            }
          }
        }
      }
    }
  ]
}
```

修改 APM Index setting

- 每個 space 有各自的 APM 設定
- 將 filtered alias 套用上去

Indices

 The index settings apply to the **abc** space.

Sourcemap Indices

apm-*

Overrides xpack.apm.indices.sourcemap: apm-*

Error Indices

abc-logs-apm*

Overrides xpack.apm.indices.error: logs-apm*,apm-*

Onboarding Indices

apm-*

Overrides xpack.apm.indices.onboarding: apm-*

Span Indices

abc-traces-apm*

Overrides xpack.apm.indices.span: traces-apm*,apm-*

Transaction Indices

abc-traces-apm*

Overrides xpack.apm.indices.transaction: traces-apm*,apm-*

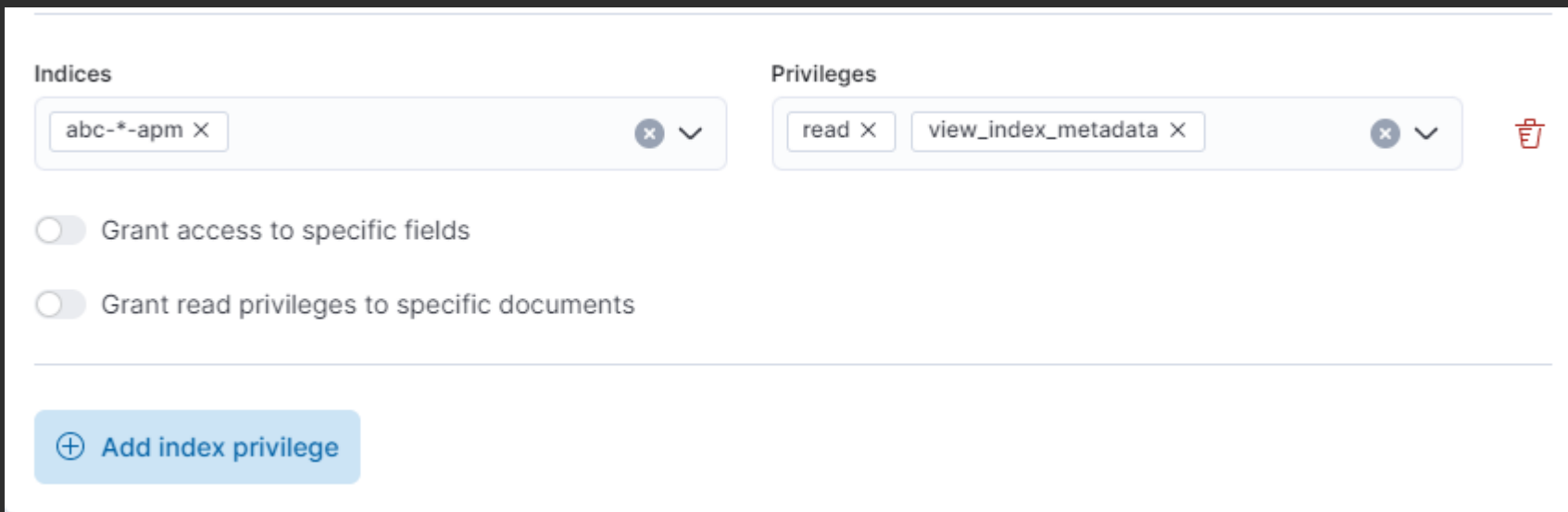
Metrics Indices

abc-metrics-apm*

Overrides xpack.apm.indices.metric: metrics-apm*,apm-*

設定角色檢視權限

- 讓成員能夠檢視 APM 的索引資料
- 須賦予 read / view_index_metadata 權限



The screenshot displays the Elasticsearch Privileges configuration interface. It is divided into two main sections: 'Indices' and 'Privileges'. In the 'Indices' section, a text box contains the pattern 'abc-*-apm' with a close button (x) and a dropdown arrow (v). In the 'Privileges' section, two text boxes contain 'read' and 'view_index_metadata', each with a close button (x) and a dropdown arrow (v). To the right of these sections is a red trash icon. Below the sections are two toggle switches, both of which are turned off: 'Grant access to specific fields' and 'Grant read privileges to specific documents'. At the bottom left, there is a blue button with a plus icon and the text 'Add index privilege'.

補充



自架 Lab 環境 - Docker

- 參考官方提供 [docker-compose.yml](#)
- 預設會安裝以下元件
 - Elasticsearch
 - Kibana
 - Fleet-server
 - Metricbeat
- 少了 Elastic Agent !

補上 Elastic Agent

```
# ...
elastic-agent:
  image: docker.elastic.co/beats/elastic-agent:8.7.0-909f3a86-SNAPSHOT
  environment:
    FLEET_ENROLLMENT_TOKEN: "paste_token_after_fleet_init"
    FLEET_ENROLL: 1
    FLEET_URL: "https://fleet-server:8220"
    FLEET_INSECURE: "true"
    KIBANA_FLEET_SETUP: "false"
  ports:
    - 8200:8200
  depends_on:
    fleet-server:
      condition: service_healthy
# ...
```



使用機器規格

- Azure VM
 - Standard B2ms
 - 2 Core, 8G
 - Ubuntu 20.04

- Ports

- 5601 / 9200 / 8200

OS/Software:
CentOS or Ubuntu Linux

Category:
All

VM series:
All

Region:
Japan East

Currency:
Taiwan – Dollar (NT\$) TWD

Display pricing by:
Hour

Pricing model & comparison: ⓘ
Savings plan (1 & 3 year)

1 USD = 30 TWD.
Showing 89 applicable virtual machine series.

B2ms	2	8 GiB	16 GiB	NT\$3.3102/hour	NT\$2.4283/hour ~26% savings	NT\$1.7058/hour ~48% savings	--	+
------	---	----------	--------	-----------------	---------------------------------	---------------------------------	----	---

操作步驟

1. 下載 apm-server

```
> git clone https://github.com/elastic/apm-server.git
```

2. cd & docker compose up

```
> cd apm-server
```

```
> docker compose up
```

3. 登入及建立 Elastic Agent

4. 複製 Elastic Agent 的 enrollment token

5. 修改 docker-compose elastic-agent 的 FLEET_ENROLLMENT_TOKEN 參數

6. 重啟 elastic-agent

```
> docker compose up --force-recreate elastic-agent
```

好了，要結束了！

結語

- Elastic APM 是一個很不錯的產品
 - 統整 Trace, Error, Log 於單一平台
 - 各元件可雲、地混合架設
- 如果你還沒開始導入 APM
 - 不管用哪套都好，用下去就對了

推薦閱讀 & 參考

- [喬叔 - 探索與實踐 Observability 系列](#)
- [Marcus - 再不使用 APM 就芭比Q 了](#)
- [Elastic APM 官方文件](#)
- [Elastic APM .NET 官方文件](#)
- [Elastic Fleet 官方文件](#)

Thanks

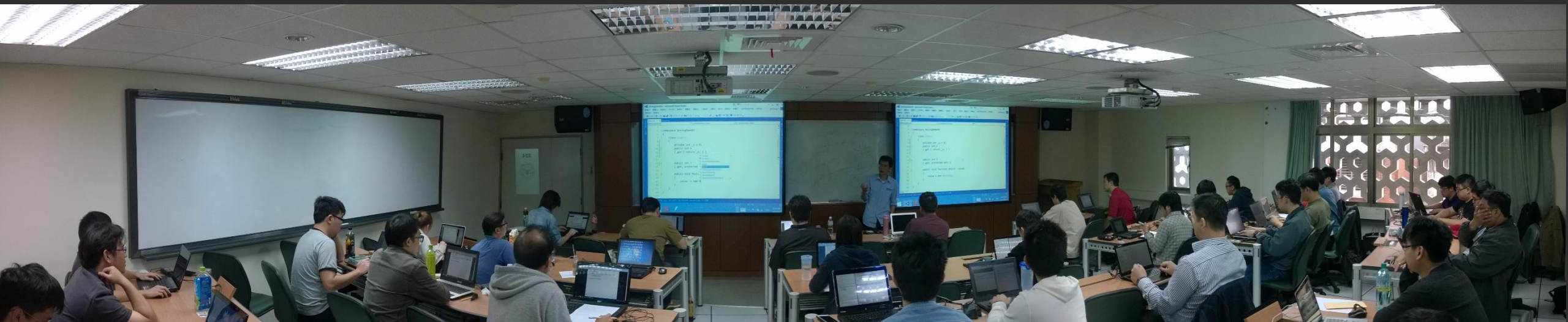


Blog 是記錄知識的最佳平台



<https://dotblogs.com.tw>

SkillTree 為了確保內容與實務不會脫節，我們都是聘請企業顧問等級並且目前依然在職場的**業界講師**，我們不把時間浪費在述說歷史與沿革，我們並不是教您考取證照，而是教您如何上場殺敵，**拳拳到肉**的內容才是您花錢想要聽到的，而這也剛好是我們擅長的。



<https://skilltree.my>

天瓏資訊圖書

