

IBM TLS SUBBING-SERVICE OFFERING

AP Log 入住 與 Kibana 說明

Taiwan | Oct 29, 2025

IBM Services



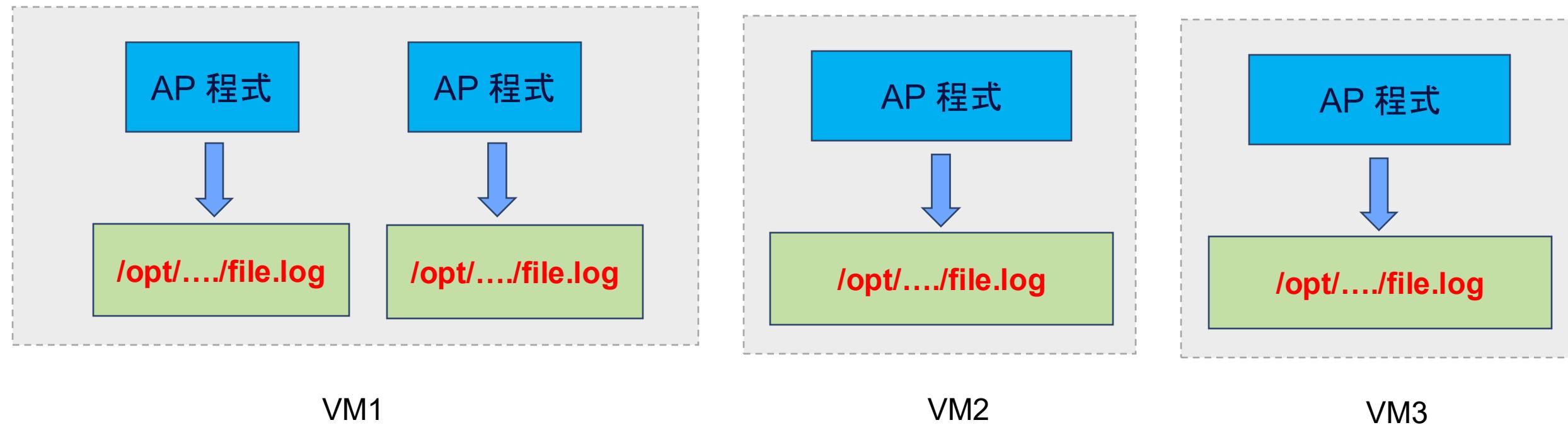
01

AP Log 日誌收集環境

日誌收集環境

關於日誌收集收納基本說明

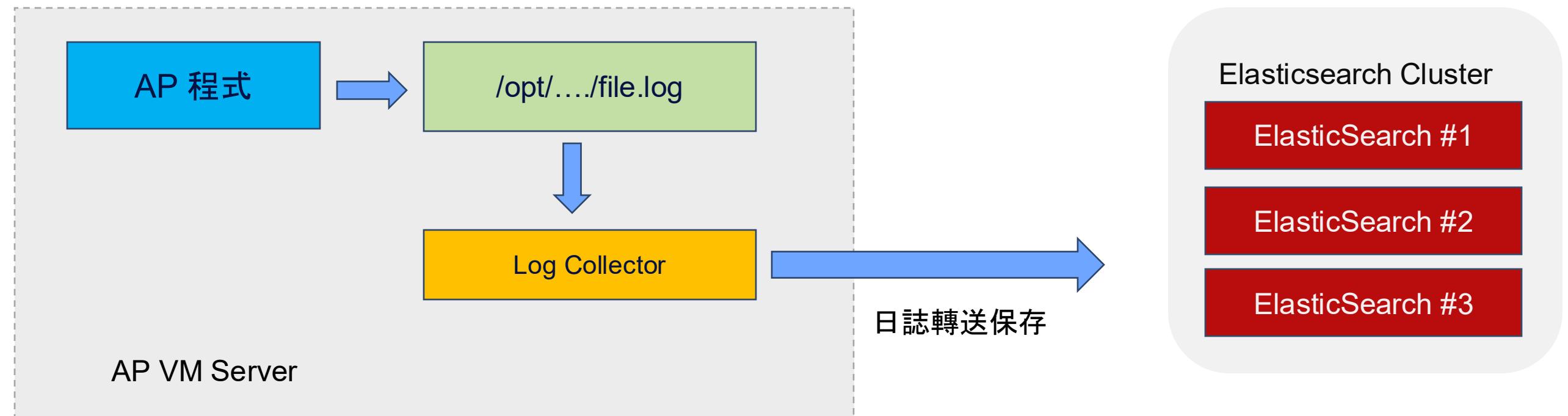
- 傳統 AP 應用程式執行期日誌，可以輸出落地保存於本機的目錄內，後續提供診斷分析。
- 行內有多種不同 AP 系統，許多 AP 系統之間會相互溝通傳遞資料，日誌內會保存相關 trace id 等資訊。
- 不同系統各別獨立於不同機器環境，日誌是分散各自保存，跨越多個追查問題有許多限制。



日誌收集環境

關於日誌收集收納基本說明

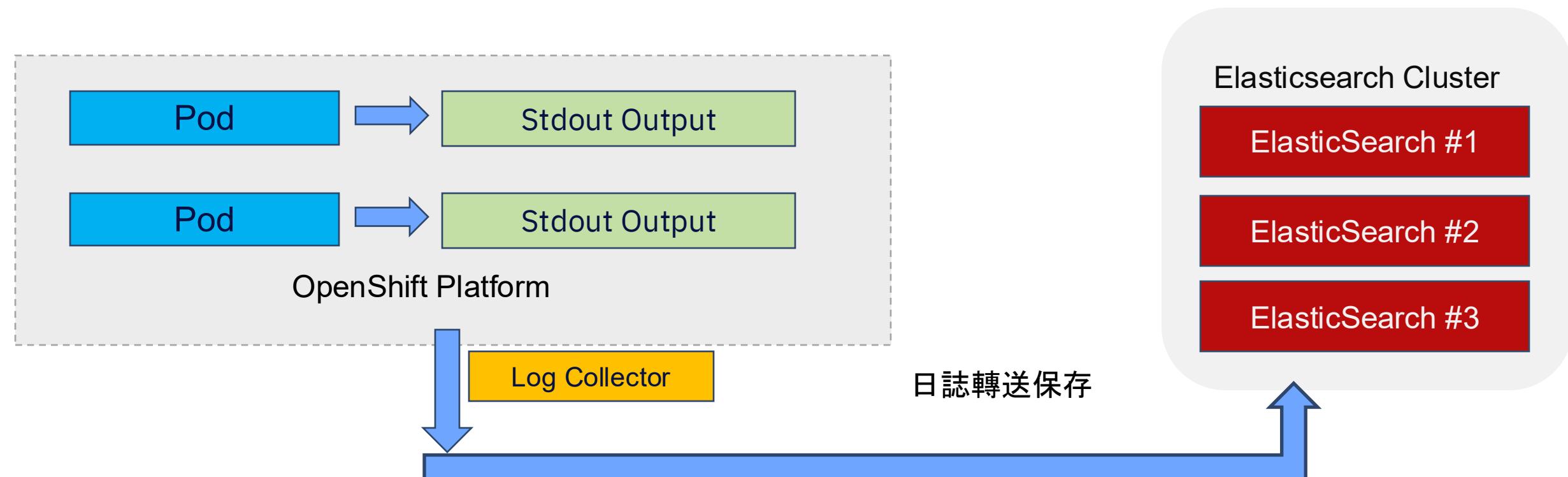
- 透過日誌統一收納到轉送到日誌收集平台統一保存，可以更方便一致方式進行檢視追蹤所需日誌內容。
- AP 主機將執行一個日誌收集器，依據指定的檔案進行收集並轉送保存。



日誌收集環境

關於日誌收集收納基本說明

- 執行於 OpenShift 平台上的 AP 日誌，不直接落地保存於本機目錄。
- 以平台 Container 執行的 Pod 服務，程式透過標註輸出顯示日誌，平台將會自行收集轉送保存。
- AP 主機將執行一個日誌收集器，依據指定的檔案進行收集並轉送保存。





02

AP Log 日誌格式

日誌格式

日誌檔案格式配合

- 日誌收集格式分類項目

編號	項目
1	行內目前 AP 系統討論已制定日誌格式 (JSON 格式)
2	客製化日誌格式

日誌格式

日誌檔案格式配合

- #1 行內目前 AP 系統討論已制定日誌格式
 - JSON 格式，固定 key 與 value 組成，定義不同欄位記錄日誌資訊。

```
1 {"@timestamp":"2024-10-23T15:11:57.409+08:00","caller_class_name":"com.ibm.el.consumer.sampleserver.filter.GlobalExchangeAccessLogFilter","caller_method_name":"doFilterInternal","caller_file_name":"GlobalExchangeAccessLogFilter.java","caller_line_number":53,"app":"sample-application","context_path":"/sample","pid":92437,"thread":"http-nio-8080-exec-5","logger":"com.ibm.el.consumer.sampleserver.filter.GlobalExchangeAccessLogFilter","trace_id":"4bf92f3577b34da6a3ce929d0e0e4736","span_id":"046b85f39e96e242","txnSeqNo":"this_is_txSeqNo_sample","marker":"response","level":"INFO","message":"{\\"header\\":{\\\"clientSeqNo\\\":\\\"this_is_clientSeqNo_sample\\\",\\\"guid\\\":\\\"this_is_guid_sample\\\",\\\"tellerId\\\":\\\"this_is_tellerId_sample\\\",\\\"txSeqNo\\\":\\\"this_is_txSeqNo_sample\\\"},\\\"serviceRq\\\":{\\\"test\\\":null}}","exception":"","clientSeqNo":"this_is_clientSeqNo_sample","guid":"this_is_guid_sample","txSeqNo":"this_is_txSeqNo_sample","tellerId":"this_is_tellerId_sample","extension":null}  
2 {"@timestamp":"2024-10-23T15:11:57.409+08:00","caller_class_name":"com.ibm.el.consumer.sampleserver.filter.GlobalExchangeAccessLogFilter","caller_method_name":"doFilterInternal","caller_file_name":"GlobalExchangeAccessLogFilter.java","caller_line_number":53,"app":"sample-application","context_path":"/sample","pid":92437,"thread":"http-nio-8080-exec-5","logger":"com.ibm.el.consumer.sampleserver.filter.GlobalExchangeAccessLogFilter","trace_id":"4bf92f3577b34da6a3ce929d0e0e4736","span_id":"046b85f39e96e242","txnSeqNo":"this_is_txSeqNo_sample","marker":"response","level":"INFO","message":"{\\"header\\":{\\\"clientSeqNo\\\":\\\"this_is_clientSeqNo_sample\\\",\\\"guid\\\":\\\"this_is_guid_sample\\\",\\\"tellerId\\\":\\\"this_is_tellerId_sample\\\",\\\"txSeqNo\\\":\\\"this_is_txSeqNo_sample\\\"},\\\"serviceRq\\\":{\\\"test\\\":null}}","exception":"","clientSeqNo":"this_is_clientSeqNo_sample","guid":"this_is_guid_sample","txSeqNo":"this_is_txSeqNo_sample","tellerId":"this_is_tellerId_sample","extension":null}
```

JSON 結構日誌格式，且符合已經討論欄位

日誌格式

行內目前系統 AP 日誌內容範例 (結構化)

```
{  
  "@timestamp": "2024-10-23T15:11:57.409+08:00",  
  "caller_class_name": "com.ibm.el.consumer.sampleserver.filter.GlobalExchangeAccessLogFilter",  
  "caller_method_name": "doFilterInternal",  
  "caller_file_name": "GlobalExchangeAccessLogFilter.java",  
  "caller_line_number": 53,  
  "app": "sample-application",  
  "context_path": "/sample",  
  "pid": "92437",  
  "thread": "http-nio-8080-exec-5",  
  "logger": "com.ibm.el.consumer.sampleserver.filter.GlobalExchangeAccessLogFilter",  
  "trace_id": "4bf92f3577b34da6a3ce929d0e0e4736",  
  "span_id": "046b85f39e96e242",  
  "txnSeqNo": "this_is_txSeqNo_sample",  
  "marker": "response",  
  "level": "INFO",  
  "message": "{\"header\":{\"clientSeqNo\":\"this_is_clientSeqNo_sample\",\"guid\":\"this_is_guid_sample\",\"tellerId\":\"this_is_tellerId_sample\",\"txSeqNo\":\"this_is_txSeqNo_sample\"},\"serviceRq\":{\"test\":null}}",  
  "exception": "",  
  "clientSeqNo": "this_is_clientSeqNo_sample",  
  "guid": "this_is_guid_sample",  
  "txSeqNo": "this_is_txSeqNo_sample",  
  "tellerId": "this_is_tellerId_sample",  
  "extension": null  
}
```

日誌內容格式

行內 AP Log 格式欄位說明

編號	欄位名稱	欄位說明	類型	必要	RestAPI	備註
1	@timestamp	日誌時間戳記	Date	Y	Y	ISO 8601 格式
2	caller_class_name	類別名稱	String	N	Y	紀錄此日誌的類別名稱
3	caller_method_name	類別方法	String	N	Y	紀錄此日誌的類別方法
4	caller_file_name	請求內文	String	N	Y	紀錄此日誌的程式檔名
5	caller_line_number	請求內文	String	N	Y	紀錄此日誌的程式行號
6	hostname	主機名稱	String	Y	Y	主機名稱
7	app	系統名稱	String	Y	Y	app 名稱
8	version	系統版本	String	N	Y	pom.xml 的版本號

日誌內容格式

行內 AP Log 格式欄位說明

編號	欄位名稱	欄位說明	類型	必要	RestAPI	備註
9	version_tag	版本標籤	String	N	O	CI/CD包版時的版本號
10	version_timestamp	版本時間	Date	N	Y	Maven包版時間 yyyyMMddHHmmss
11	context_path	上下文路徑	String	N	Y	系統 HTTP 網址根目錄
12	request_uri	HTTP網址	String	N	Y	若為 RestAPI 時，記錄該API的HTTP URL
13	pid	Process ID	Number	N	Y	Process ID 編號
14	thread	執行緒	String	N	Y	執行緒名稱
15	logger	日誌名稱	String	Y	Y	產生日誌 logging 的日誌類別名稱
16	trace_id	Trace ID	String	N	Y	用來追蹤交易的唯一識別碼

日誌內容格式

行內 AP Log 格式欄位說明

編號	欄位名稱	欄位說明	類型	必要	RestAPI	備註
17	span_id	Span ID	String	N	Y	單一服務的唯一識別碼 (64bit, 16 hex 字元)
18	guid	交易序號	String	N	Y	
19	txSeqNo	交易流水號	String	N	O	
20	marker	標記	String	N	O	RQ: request, RS: response, 其他: 空值
21	level	等級	String	Y	Y	
22	message	訊息	String	Y	Y	程式本身額外的訊息資訊
23	exception	錯誤訊息	String	N	O	系統發生異常時的 exception stack trace

日誌內容格式

行內 AP Log 格式欄位說明

編號	欄位名稱	欄位說明	類型	必要	RestAPI	備註
24	clientSeqNo	用戶端交易序號	String	N	O	若為 RestAPI 時紀錄 Header 的用戶端交易序號
25	tellerId	櫃員代號	String	N	O	若為 RestAPI 時紀錄 Header 的櫃員代號
26	extension	擴充欄位	JSON	N	O	各系統自訂擴充欄位，無資料請使用 {}

日誌內容格式

行內 AP Log Timestamp 格式欄位補充說明

- 日誌內 @timestamp 欄位，用來表示程式本身日誌的產生日資訊
- 格式為 ISO 8601 格式，組成：日期 + 時間 (含毫秒 + 時區)

編號	格式範例	備註
1	2025-09-29T12:34:56Z	2025 年 9 月 29 日， UTC 時間
2	2025-09-29T12:34:56	2025 年 9 月 29 日， Local time (時區依據 server 設定)
3	2025-09-29T20:34:56+08:00	2025 年 9 月 29 日 20:34:56， 北京 / 台灣時間 (UTC+8)
4	2025-09-29T12:34:56.789-05:00	2025 年 9 月 29 日 12:34:56.789， 美東時間 (UTC-5)

日誌內容格式

行內 AP Log trace_id 格式欄位補充說明

項目	W3C Trace Context	B3 Propagation
主要 Header	traceparent (+ tracestate)	多個 X-B3-* 或單一 b3
基本格式	version-traceid-parentid-flags	X-B3-Traceld, X-B3-SpanId, X-B3-Sampled, ...
Trace ID 長度	128 bit (32 hex)	64 或 128 bit (16 或 32 hex)
Span ID 長度	64 bit (16 hex)	64 bit (16 hex)
取樣旗標	trace-flags (最低位=sample)	X-B3-Sampled: 1/0, X-B3-Flags: 1
是否多 Header	否 (固定一個)	是 (或 b3 單一合併)
範例	traceparent: 00-4bf92f3577b34da6a3ce929d0e0e4736-00f067aa0ba902b7-01	X-B3-Traceld: 463ac35c9f6413ad48485a3953bb6124 X-B3-SpanId: a2fb4a1d1a96d312 X-B3-Sampled: 1
是否有 Parent Span ID	有 (parent-id 欄位)	有 (X-B3-ParentSpanId 可選)
可攜帶廠商資料	有 (tracestate: rojo=abc,congo=xyz)	無 (需自定義)
常見環境使用	OpenTelemetry, Azure Monitor, Elastic APM, Google Cloud Trace	Zipkin, Jaeger, Spring Cloud Sleuth

日誌格式

日誌檔案格式配合

- **#2 AP 本身自行定義的日誌格式**
 - 用來追蹤分析查詢本身該系統相關日誌資訊，純文字檔案。常見 Nginx, Jboss 標準輸出 Log。
 - 若要被系統收納正規化，以便於後續結構化方式搜尋檢索，需要提供告知格式轉換資訊。
 - 不轉換正規化處理，缺點後續日誌檢索為全文搜尋，檢索效率差。

```

1 2024-12-17 18:31:00,271 [t=ServerService Thread Pool -- 82,p=1274873] DEBUG [UTIL] uuId="cd5a5a115673479ca1d416d1b1acd745",dim="D",level="DEBUG",comp="TEMN-IRIS_dsf-iris-202303.0.17-UTIL",cn="com.temenos.irf.logging.IrisTemenosLogImpl:debug:66",msg="Found a key certificate file path, reading this file and proceeding with this key."
2 2024-12-17 18:31:00,274 [t=ServerService Thread Pool -- 82,p=1274873] WARN [UTIL] uuId="cd5a5a115673479ca1d416d1b1acd745",dim="A",level="WARN",comp="TEMN-IRIS_dsf-iris-202303.0.17-UTIL-RUNTIME",cn="com.temenos.irf.logging.IrisTemenosLogImpl:warn:166",code="00006001",("possibleReason="System Failure",msg="Error Loading the certificate fileC:/share/Share/ws02/wso2is-5.3.0/repository/resources/security/wso2carbon.cer (No such file or directory)",code="00006001"
3 2024-12-17 18:31:01,634 [t=ServerService Thread Pool -- 82,p=1274873] DEBUG [UTIL] uuId="cd5a5a115673479ca1d416d1b1acd745",dim="D",level="DEBUG",comp="TEMN-IRIS_dsf-iris-202303.0.17-UTIL",cn="com.temenos.irf.logging.IrisTemenosLogImpl:debug:66",msg="Checking if config-microservice is enabled"

```

內容有固定結構的資訊，可以解析識別

日誌格式

AP 自定義格式範例

```

1 2024-12-17 18:31:00,271 [t=ServerService Thread Pool -- 82,p=1274873] DEBUG [UTIL] uuId="cd5a5a115673479ca1d416d1b1acd745",dim="D",level="DEBUG",comp="TEMN-IRIS_dsf-iris-202303.0.17-UTIL",cn="com.temenos.irf.logging.IrisTemenosLogImpl:debug:66",msg="Found a key certificate file path, reading this file and proceeding with this key."
2 2024-12-17 18:31:00,274 [t=ServerService Thread Pool -- 82,p=1274873] WARN [UTIL] uuId="cd5a5a115673479ca1d416d1b1acd745",dim="A",level="WARN",comp="TEMN-IRIS_dsf-iris-202303.0.17-UTIL-RUNTIME",cn="com.temenos.irf.logging.IrisTemenosLogImpl:warn:166",code="00006001",("possibleReason="System Failure",msg="Error Loading the certificate fileC:/share/Share/ws02/wso2is-5.3.0/repository/resources/security/wso2carbon.cer (No such file or directory)",code="00006001"
3 2024-12-17 18:31:01,634 [t=ServerService Thread Pool -- 82,p=1274873] DEBUG [UTIL] uuId="cd5a5a115673479ca1d416d1b1acd745",dim="D",level="DEBUG",comp="TEMN-IRIS_dsf-iris-202303.0.17-UTIL",cn="com.temenos.irf.logging.IrisTemenosLogImpl:debug:66",msg="Checking if config-microservice is enabled"
4 2024-12-17 18:31:01,637 [t=ServerService Thread Pool -- 82,p=1274873] DEBUG [UTIL] uuId="cd5a5a115673479ca1d416d1b1acd745",dim="D",level="DEBUG",comp="TEMN-IRIS_dsf-iris-202303.0.17-UTIL",cn="com.temenos.irf.logging.IrisTemenosLogImpl:debug:66",msg="Exited from config ms check"
5 2024-12-17 18:34:08,594 [t=default task-1,p=1274873] INFO [UTIL] uuId="961fee65017c47418fdaf1935223bf23",dim="D",level="INFO",comp="TEMN-IRIS_dsf-iris-202303.0.17-UTIL",cn="com.temenos.irf.logging.IrisTemenosLogImpl:info:124",msg="API request received -POST - /v1.0.0/meta/dsfpackages/deploy"
6 2024-12-17 18:34:08,597 [t=default task-1,p=1274873] DEBUG [UTIL] uuId="961fee65017c47418fdaf1935223bf23",dim="D",level="DEBUG",comp="TEMN-IRIS_dsf-iris-202303.0.17-UTIL",cn="com.temenos.irf.logging.IrisTemenosLogImpl:debug:66",msg="path is /v1.0.0/meta/dsfpackages"
7 2024-12-17 18:34:08,597 [t=default task-1,p=1274873] DEBUG [UTIL] uuId="961fee65017c47418fdaf1935223bf23",dim="D",level="DEBUG",comp="TEMN-IRIS_dsf-iris-202303.0.17-UTIL",cn="com.temenos.irf.logging.IrisTemenosLogImpl:debug:66",msg="domain is : meta"
8 2024-12-17 18:34:08,597 [t=default task-1,p=1274873] DEBUG [UTIL] uuId="961fee65017c47418fdaf1935223bf23",dim="D",level="DEBUG",comp="TEMN-IRIS_dsf-iris-202303.0.17-UTIL",cn="com.temenos.irf.logging.IrisTemenosLogImpl:debug:66",msg="operation Id : deployPackageFromZip"
9 2024-12-17 18:34:08,602 [t=default task-1,p=1274873] WARN [UTIL] uuId="961fee65017c47418fdaf1935223bf23",dim="A",level="WARN",comp="TEMN-IRIS_dsf-iris-202303.0.17-UTIL-RUNTIME",cn="com.temenos.irf.logging.IrisTemenosLogImpl:warn:166",code="00006001",("possibleReason="System Failure",msg="API timeout not configured and hence defaulting to the maximum timeout limit.",code="00006001"

```



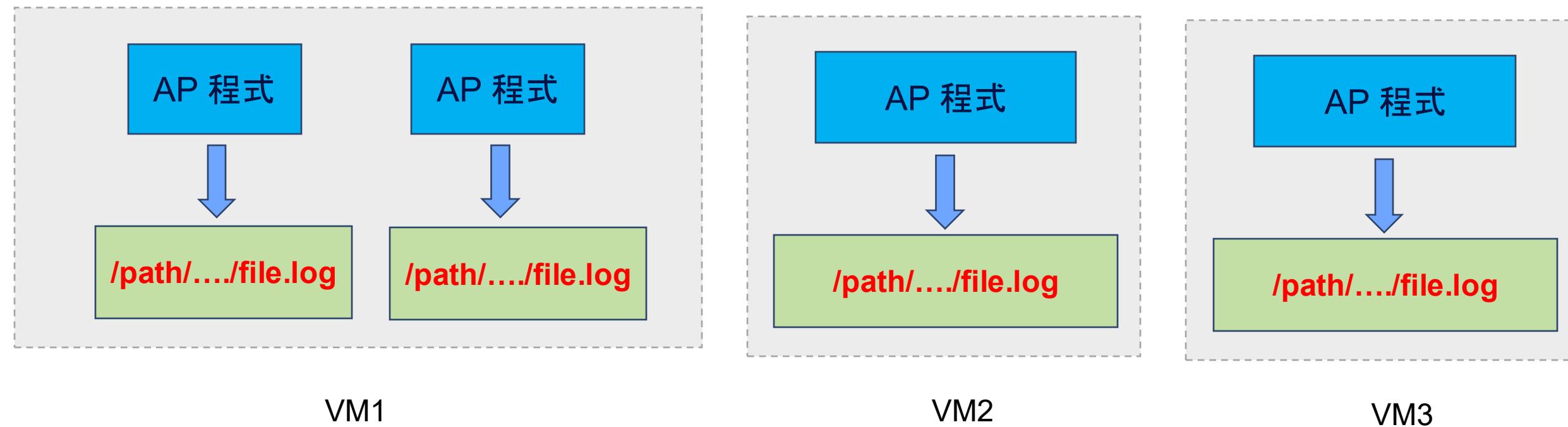
03

AP Log 日誌放置配合

AP Log 日誌放置配合

AP Log 日誌檔案放置配合

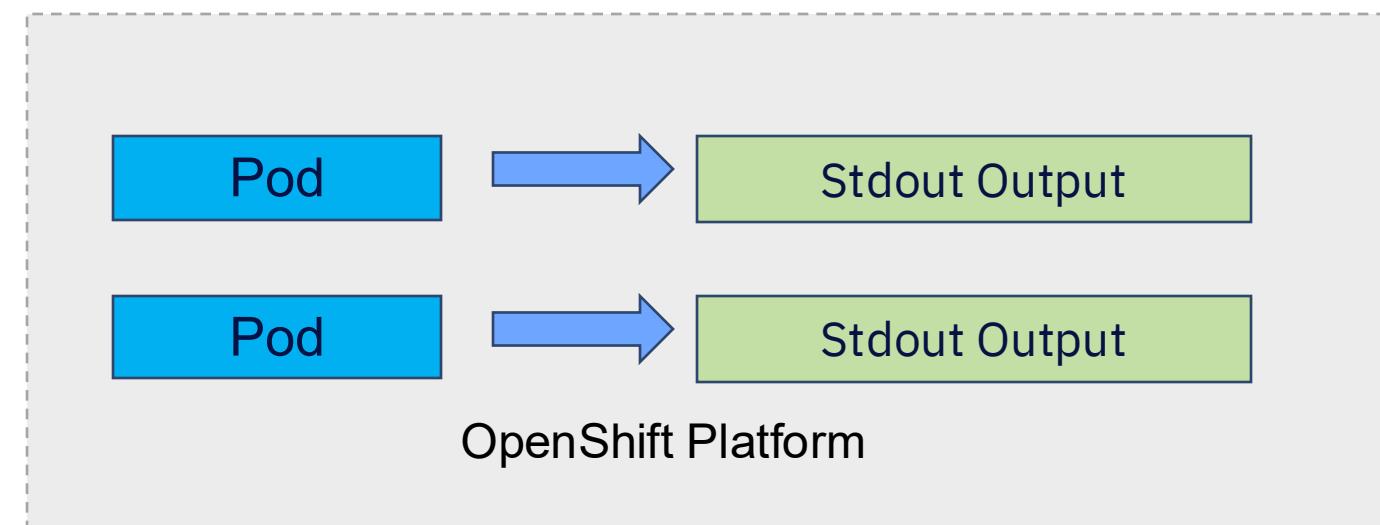
- VM 或是實體機器上 AP 日誌
 - 確認日誌記錄檔案輸出的路徑規則。
 - 後續填寫 AP 日誌入住表註明收集的路徑資訊。



AP Log 日誌放置配合

AP Log 日誌檔案放置配合

- OpenShift 上 AP 日誌
 - 程式使用標準輸出顯示日誌內容，平台會自動保存。
 - 可以透過 oc / kubectl 等命令傳入 logs 查看指定 Pod 可以檢視訊息輸出內容。

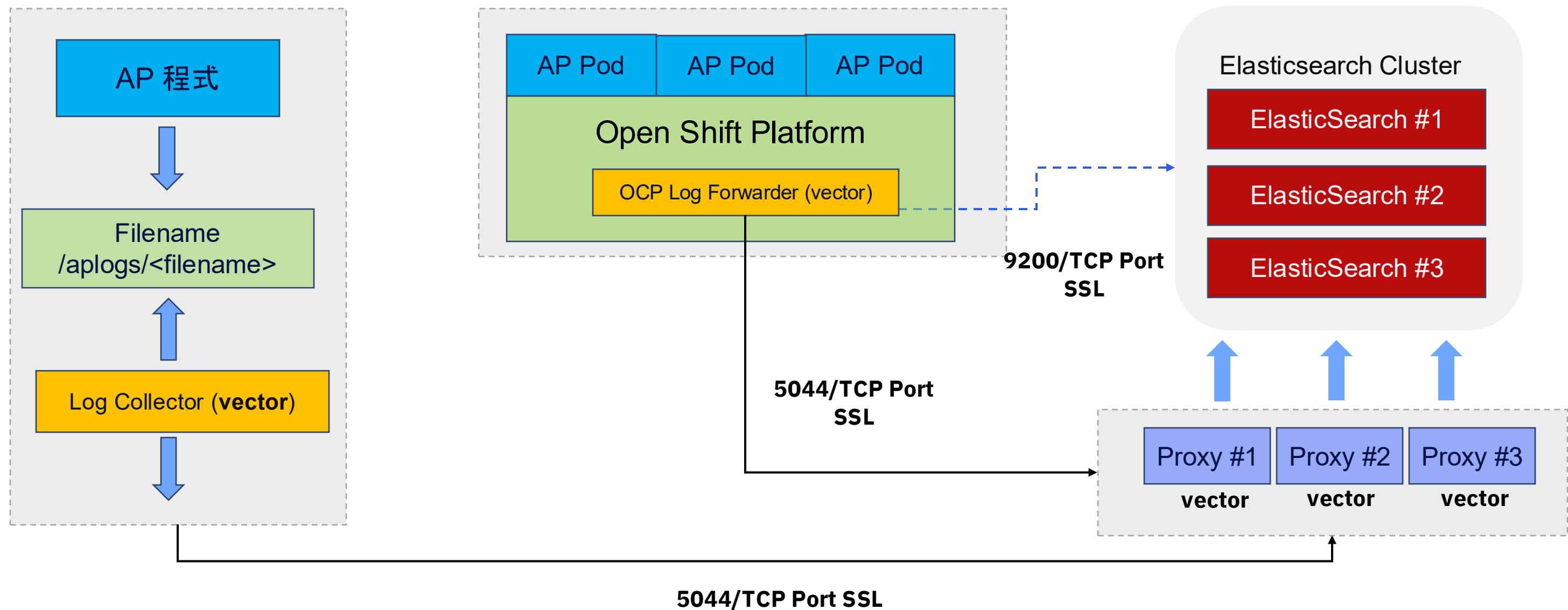


AP Log 日誌放置配合

日誌收集工具

- 位於 AP Server 上安裝日誌收集器程式進行日誌的處理支援
 - 主機將會安裝 vector，提供日誌收集的功能。
 - 透過指定讀取來源日誌，格式化轉換與處理，最後轉送到最後目的進行保存。

AP Log 日誌放置配合



04

關於 Elasticsearch 與 Kibana

關於 Elasticsearch 與 Kibana

Elasticsearch

- Elasticsearch 是一個開源的分散式搜尋與分析引擎，提供高效能且即時的全文搜尋、分析與資料視覺化功能，廣泛用於日誌分析、資料檢索、系統監控與商業智慧等場景。
 - 分散式全文搜尋引擎 (Distributed Full-Text Search Engine)
 - 提供 HTTP 介面，方便程式或應用程式進行存取和管理
 - 高度可擴展性 (Scalability)，可輕鬆橫向擴展，多節點間自動分配資料，確保搜尋性能及高可用性
 - 資料均以 JSON 格式儲存，結構靈活，便於調整及擴展
 - 支援即時分析及聚合統計，例如即時圖表、監控、報表生成等，常用於日誌分析、資料視覺化



關於 Elasticsearch 與 Kibana

Kibana

- Kibana 是 Elasticsearch 官方提供的開源視覺化與管理工具，直觀地分析與呈現 Elasticsearch 中的資料。
 - 數據視覺化 (Data Visualization) ， 快速將 Elasticsearch 中的資料製作成圖表
 - 提供儀表板 (Dashboard) ， 透過多種視覺化元件（圖表、地圖、表格）重新資料趨勢與關鍵指標
 - 透過直觀的查詢界面 (KQL, Lucene 語法)， 輕鬆篩選和分析日誌資料，快速識別異常事件
 - 提供叢集、索引、索引模板、使用者與角色權限管理的便利介面。
 - 結合 Elasticsearch Alerts 及 Watcher 功能， 設定條件與警報，隨時掌握重要事件



05

Elasticsearch 與 Kibana 名詞說明

Elasticsearch 與 Kibana 名詞說明

相關名詞

編號	項目	說明
1	Index	<ul style="list-style-type: none"> ■ Elasticsearch 中的一個單一資料數據集合，類似於資料庫中的資料表 ■ 海銀入住環境，每個 VM AP 入住的系統，會應對一個 Index 名稱
2	Data View	<ul style="list-style-type: none"> ■ Kibana 提供使用者指定一到多個索引，可查詢和視覺呈現 Elasticsearch 中的數據 ■ 提供用於定義一組索引，指向多個 Index 項目 ■ 海銀入住環境，管理者會自行建立一組 Data View 應對到所屬 APID 系統的 Index ■ 比方 view 名稱為 app-apic-all，應對到 apic-apic-* 開頭的 index 列表

Elasticsearch 與 Kibana 名詞

行內目前規範 Elasticsearch 上不同 Index Name 規則

編號	系統別/環境	描述	名稱範例
1	OpenShift 環境	<ul style="list-style-type: none"> 使用 container_name 當識別 container name 包含行內的 apic 名稱組成 	<ul style="list-style-type: none"> app-mid-cbr-app-write
2	VM 環境	<ul style="list-style-type: none"> 依據 APID 當識別 相同的 APID 系統的 index 名稱獨立 可以依據 subname 指定不同分類 	<ul style="list-style-type: none"> app-brh-write app-brh-service-write

Elasticsearch 與 Kibana 名詞

Elasticsearch Index

The screenshot shows the Elasticsearch Index Management interface. The left sidebar has sections for Management, Ingest, Data, and Index Management. The main area is titled "Index Management" and contains tabs for Indices, Data Streams, Index Templates, Component Templates, and Enrich Policies. The Indices tab is selected. A search bar and filters for Lifecycle status and phase are available. The table lists three indices:

Name	Health	Status	Primaries	Replicas	Docs count	Storage size	Data stream
app-mid-write	green	open	1	1	90,133	51.49mb	
app-vm-write	green	open	1	1	3,501	1.36mb	
app-write	green	open	1	1	27,103	20.06mb	

A red box highlights the "Name" column header and the first three rows of the table.

Elasticsearch 與 Kibana 名詞說明

Elasticsearch Data Views

The screenshot shows the Elasticsearch Data Views interface. The top navigation bar includes the elastic logo, a search bar with placeholder text 'Find apps, content, and more.', and user icons. The left sidebar contains links for Stack Management (selected), Data views, Snapshot and Restore, Rollup Jobs, Transforms, Remote Clusters, Migrate, Alerts and Insights (with sub-links for Alerts, Rules, Cases, Connectors, Reporting, Machine Learning, and Maintenance Windows), and Security (with sub-links for Users). The main content area is titled 'Data Views' and displays a list of data views. A red box highlights the first four items in the list:

Name	Spaces	Actions
<input type="checkbox"/> Name ↑		
<input type="checkbox"/> app-mid-write ⓘ Default	D	
<input type="checkbox"/> app-all ⓘ	D	
<input type="checkbox"/> app-vm-write ⓘ	D	

Below the list, there is a 'Search...' input field and pagination controls showing 'Rows per page: 10' and page '1'.

AP Log 收集儲存於 Elasticsearch 上格式

VM AP Log 檔案日誌檔案內容收集處理

編號	欄位名稱	描述
1	source_type	讀取日誌的來源類型名稱
2	file	讀取日誌檔案名稱
3	host	執行 vector 收集日誌所在設備主機名稱
4	timestamp	vector 處理收集時間記錄
5	message	實際的日誌內容 內容 (程式時間 stdout 輸出內容在此區段)
6	structured	為 message 內容是 JSON 格式的物件結構放置
7	@timestamp	structured 內 @timestamp 欄位解析放置提供該欄位 (內部客製)

Kibana 後端系統使用檢視日誌

OpenShift 內 AP 透過標準輸出日誌檔案內容收集處理

編號	欄位名稱	描述
1	kubernetes	物件結構，記錄執行 kubernetes 相關資訊
2	openshift	物件結構，記錄 openshift 相關資訊
3	@timestamp	日誌時間資訊 (openshift 將 structured 內 @timestamp 複製)
4	hostname	產生日誌的執行的節點主機名稱
5	log_type	日誌類型 (application, infra, audit)
6	level	日誌級別 (info, debug, error)
7	message	實際的日誌內容 (程式時間 stdout 輸出內容在此區段)
8	structured	僅出現於啟用設定使用 JSON 解析環境 為 message 內容是 JSON 格式的物件結構

Kibana 後端系統使用檢視日誌

VM AP Log 檔案日誌檔案內容收集處理

Field	Value
k _id	79yNh5QBvIYwfrysQ5pn
k _ignored	-
k _index	app-brh-write
# _score	-
calendar @timestamp	Jan 21, 2025 @ 14:29:25.899
t apid_name	brh
t file	/opt/SIT/jboss-eap-8.0/standalone/log/server.log
t host	DBRH001
t source_type	file
calendar structured.@timestamp	Jan 21, 2025 @ 14:29:25.899
t structured.app	brh-brh
t structured.caller_class_name	mds.com.scsb_s.Service.Tools.SyncDesktopService
t structured.caller_file_name	SyncDesktopService.java
# structured.caller_line	191

Rows per page: 500 ▾

< 1 >

Kibana 後端系統使用檢視日誌

OpenShift 日誌檔案內容收集處理

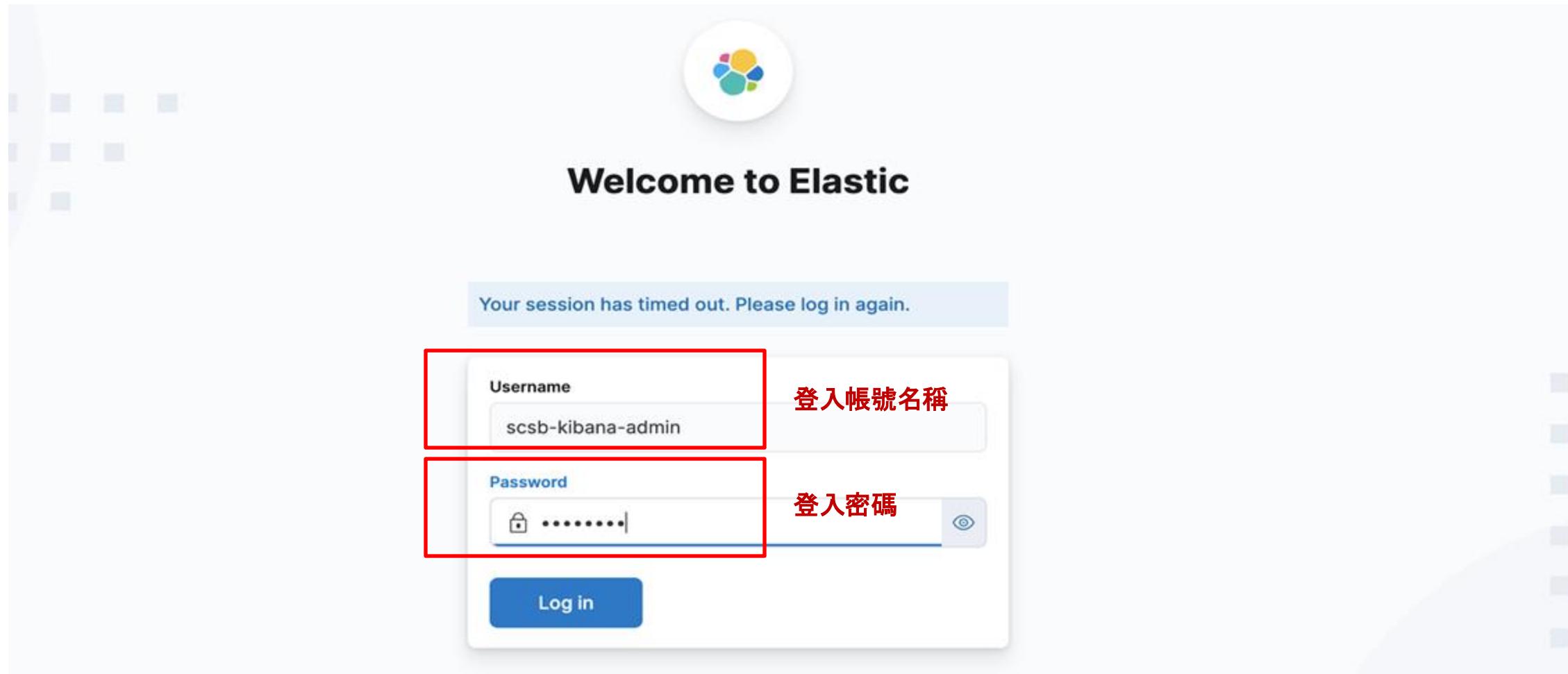
Field	Value	Field	Value
<code>k _id</code>	YTMzYzlhZDQtZDk5Zi00ZDk1	<code>t kubernetes.container_id</code>	cri-o://bf504f0f7e9d32a2507e265f7f550953f7cb33cb565ab6
<code>k _ignored</code>	-	<code>t kubernetes.container_image</code>	python:3.9-slim
<code>k _index</code>	app-mid-write	<code>t kubernetes.container_image_id</code>	docker.io/library/python@sha256:7a9cc80ab9ae3b6551323a7ddbc2a89ad6e3
<code># _score</code>	-	<code>t kubernetes.container_name</code>	app-log-demo1
<code>calendar @timestamp</code>	Nov 6, 2024 @ 10:59:58.486	<code>t kubernetes.flat_labels</code>	app=app-log-demo1, pod-template-ha
<code>t hostname</code>	infra1.oc4.k8sbridge.com	<code>t kubernetes.namespace_id</code>	36898e27-f04d-44da-aed3-8e18659
<code>t kubernetes.annotations.k8s.v1.cni.cncf.io/network-status</code>	[{"name": "openshift-sdn", "interface": "eth0", "ips": [{"ip": "10.129.3.53"}], "default": true, "dns": {}}]	<code>t kubernetes.namespace_labels.kubernetes_io_metadata_name</code>	mid
<code>t kubernetes.annotations.openshift.io/scc</code>	restricted-v2	<code>t kubernetes.namespace_labels.pod-security_kubernetes_io_audit</code>	baseline
<code>t kubernetes.annotations.seccomp.security.alpha.kubernetes.io/</code>	runtime/default	<code>t kubernetes.namespace_labels.pod-security</code>	v1.24
		<code>t level</code>	info
		<code>t log_type</code>	application
		<code>t openshift.cluster_id</code>	c32779a8-cdef-4ab4-8af9-3f7649646a0e
		<code># openshift.sequence</code>	1,730,861,999,727,075,584
		<code>calendar structured.@timestamp</code>	Sep 27, 2024 @ 15:03:10.654
		<code>t structured.app</code>	sample-application
		<code>t structured.caller_class_name</code>	com.ibm.logging.server.service.LoggingService
		<code>t structured.caller_file_name</code>	LoggingService.java
		<code># structured.caller_line_number</code>	25
		<code>t structured.caller_method_name</code>	log
		<code>t structured.clientSeqNo</code>	(empty)
		<code>t structured.context_path</code>	/

06

Kibana Dashboard 內資料檢索使用

Use Kibana for Elasticsearch Log

Kibana Login



Use Kibana for Elasticsearch Log

Kibana Main Page

The screenshot shows the Kibana main page with a red box highlighting the top-left navigation area. The navigation bar includes the elastic logo, a search bar, and a menu icon labeled "選單". Below the navigation bar, the page features a "Welcome home" header and four service cards: Search, Observability, Security, and Analytics. Each card has an icon and a brief description. At the bottom, there's a section for adding integrations and a callout for trying managed Elastic Cloud.

選單

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.

[Move to Elastic Cloud](#)

[+ Add integrations](#) [Try sample data](#) [Upload a file](#)

Use Kibana for Elasticsearch Log

Kibana Left Side Menu

The screenshot shows the Kibana interface with the left sidebar expanded. The 'Management' section is selected, and the 'Stack Management' item is highlighted with a red box. Below it, there is a button labeled '+ Add integrations' and a URL 'https://localhost:10000/app/management'. The main content area displays a dashboard titled 'e home' with four cards: 'Search', 'Observability', 'Security', and 'Analytics'. A section below the cards is titled 'Try adding integrations' with instructions and buttons for 'Try sample data' and 'Upload a file'. To the right, there is a 'Try managed Elastic' section with an illustration of clouds and a 'Move to Elastic Cloud' button. At the bottom of the sidebar, there are links for 'Dev Tools' and 'Stack Management'.

Use Kibana for Elasticsearch Log

Kibana Users

The screenshot shows the Kibana Management interface with the 'Users' page selected. The left sidebar contains navigation links for Management, Ingest, Data, Alerts and Insights, and Security. The 'Users' link under Security is highlighted with a red box. The main area displays a table of users with columns for User Name, Full Name, Email Address, Roles, and Status. A search bar at the top is set to 'viewer'. A 'Create user' button is in the top right. A 'Show reserved users' toggle is checked. The user list table is highlighted with a red border.

User Name	Full Name	Email Address	Roles	Status
ach-viewer			viewer	
apc-viewer	apc-viewer		viewer	
baw-viewer			viewer	
brh-viewer			viewer	
fep-viewer			viewer	
mid-viewer			viewer	
tbc-viewer			viewer	

Use Kibana for Elasticsearch Log

Kibana Index

The screenshot shows the Elasticsearch Stack Management interface with the 'Index Management' tab selected. The left sidebar has a red box around the 'Data' section, and the 'Index Management' sub-section is also highlighted with a red box. The main area displays a table of indices with columns for Name, Health, Status, Primaries, Replicas, Docs count, Storage size, and Data stream. Each index entry is preceded by a checkbox. The table lists ten indices, all of which are green (healthy) and open. The first index, 'app-apc-write', has the highest document count at 2,434,986.

Name	Health	Status	Primaries	Replicas	Docs count	Storage size	Data stream
app-apc-write	green	open	1	1	2,434,986	2.24gb	
app-brh-write	green	open	1	1	9,449,142	9.06gb	
app-mid-cbr-app-write	green	open	1	1	19,433	22.04mb	
app-mid-cmn-app-write	green	open	1	1	64,597	90.68mb	
app-mid-dep-app-write	green	open	1	1	65,604	106.28mb	
app-mid-gla-app-write	green	open	1	1	10,436	13.26mb	
app-mid-len-app-write	green	open	1	1	25,872	28.52mb	
app-mid-rem-app-write	green	open	1	1	8,534	11.82mb	
app-mid-remb-app-write	green	open	1	1	19,565	21.67mb	
app-mid-remm-app-write	green	open	1	1	666	2.07mb	

Use Kibana for Elasticsearch Log

Kibana Index Detail

The screenshot shows the Kibana interface for managing indices. The top navigation bar includes the elastic logo, a search bar, and user authentication information. The main navigation on the left is under 'Stack Management' and 'Index Management'. The current view is 'Indices > Index details > Overview' for the 'app-apc-write' index.

The 'app-apc-write' index details page displays the following information:

- Storage:** 1.1gb Primary, 2.24gb Total
- Status:** Open, Healthy
- Shards:** 1 Primary / 1 Replica
- Documents:** 2,434,986 Documents / 0 Deleted

On the right side, there are buttons for 'Manage index' and 'Discover index'. The 'Discover index' button is highlighted with a red box.

Below the index details, there is a section titled 'Add data to this index' with a note about using the bulk API. A 'curl' command is provided for adding data:

```
curl -X POST https://your_deployment_url/_bulk?pretty \
-H "Authorization: ApiKey your_api_key" \
-H "Content-Type: application/json" \
-d'
{ "index" : { "_index" : "app-apc-write" } }
{"name": "foo", "title": "bar"}'
```

At the bottom, there are links for 'Console' and 'Notebooks'.

Use Kibana for Elasticsearch Log

Kibana index Mappings

The screenshot shows the Elasticsearch Stack Management interface. The left sidebar has sections for Ingest, Data, Index Management, Alerts and Insights, Security, and Kibana. The 'Data' and 'Index Management' sections are highlighted with red boxes. The main content area shows the 'Indices' section with 'app-apc-write' selected. The 'Mappings' tab is active. The page displays field mappings for the 'structured' object type, including @timestamp, apid_name, file, host, source_type, and structured. A tooltip about index mappings is visible.

Use Kibana for Elasticsearch Log

Kibana Data Views

The screenshot shows the Kibana Data Views interface. On the left, there is a sidebar with various navigation options: Remote Clusters, Migrate, Alerts and Insights (Alerts, Rules, Cases, Connectors, Reporting), Machine Learning, Maintenance Windows, Security (Users, Roles, API keys), Kibana (Data Views, highlighted with a red box), Files, AI Assistant (Data Views, highlighted with a red box), Saved Objects, Tags, Search Sessions, Spaces, Advanced Settings, and Stack. The main area is titled "Data Views" and contains a sub-instruction: "Create and manage the data views that help you retrieve your data from Elasticsearch." Below this is a search bar and a table listing data views. The table has columns for Name, Spaces, and Actions. The data views listed are:

Name	Spaces	Actions
app-mid-dep-app-write ⓘ Default	D	trash
.alerts-security.alerts-default,apm-*~transaction*,auditbeat-*~endgame*,filebeat-*~logs*,packetbeat-*~traces~,apm*,winlogbeat*~elastic-cloud-logs* ⓘ Security Data View	D	trash
.kibana-event-log-* ⓘ	D	trash
app-all-ap-log ⓘ	D	trash
app-brh-write ⓘ	D	trash
app-mid-write* ⓘ	D	trash
logs-*	D	trash
metrics-*	D	trash

At the bottom, there is a "Rows per page: 10" dropdown and a page navigation section with arrows and a page number "1". The URL at the bottom of the browser window is <https://localhost:10000/app/management/kibana/dataViews>.

Use Kibana for Elasticsearch Log

Kibana Data View Matches

View 可以指定多一給 Index

Name: app-all-ap-log

Index pattern: app-*-write

Matching sources:

- app-apc-write
- app-brh-write
- app-mid-cbr-app-write
- app-mid-cmn-app-write
- app-mid-dep-app-write
- app-mid-gla-app-write
- app-mid-len-app-write
- app-mid-rem-app-write
- app-mid-remb-app-write
- app-mid-remm-app-write

Use Kibana for Elasticsearch Log

Kibana Discover

The screenshot shows the Kibana Discover interface. The left sidebar has a red box around the 'Discover' item under the 'Analytics' section. The main area features four cards: 'Search' (yellow), 'Observability' (pink), 'Security' (teal), and 'Analytics' (blue). Below these are sections for 'Try adding integrations' and 'Try managed Elastic'. At the bottom, there's a 'Dev Tools' and 'Stack Management' link, and the URL 'https://localhost:10000/app/discover#/_g=(filters:(),refreshInterval:(pause:lt,value:60000),time:(from:now-15m,to:now))&_a=(columns:(),dataSource:(dataViewId:'7ec22c3d-48a5-444c-bb7d-d436a98a03ea',type:dataView),filters:(),interval:())'.

Use Kibana for Elasticsearch Log

Kibana Discover

內容搜尋輸入區

時間選擇

日誌內容

The screenshot shows the Kibana Discover interface with several key components highlighted by red boxes:

- Top Bar:** Includes the elastic logo, a search bar ("Find apps, content, and more."), and navigation links (New, Open, Share, Alerts, Inspect, Save).
- Left Sidebar:** A tree view titled "Available fields" containing 66 items, including "_partial", "@timestamp", "app", "exception", "guid", "hostname", and various Kubernetes-related annotations.
- Central Histogram:** A chart showing event counts over time from October 21, 2025, at 17:54 to 18:09. The x-axis represents time intervals of 30 seconds, and the y-axis represents the count of events, ranging from 0 to 500.
- Field Statistics:** A table titled "Field statistics" showing document counts and details for the "@timestamp" field. It lists five log entries with their timestamps and raw log data.

Use Kibana for Elasticsearch Log

Kibana Discover Data Views

切換選擇 view

The screenshot shows the Kibana Discover interface. On the left, there's a sidebar titled "Data views" with a search bar and a list of available data views. One view, "app-mid-dep-app-write", is selected and expanded, showing its fields. The main area displays a timeline from Jan 21, 2025, at 14:10 to 14:25, with a green bar indicating activity between 14:15 and 14:23. Below the timeline, a "Document" section shows log entries. The first entry is:

```
_partial true @timestamp Jan 21, 2025 @ 14:23:18.970 hostname docpw01.cbsd.sczb.com.t
w kubernetes.annotations.cni.projectcalico.org/containerID 435538ea7cf0c5256e05eaef992d44ad99366dae7fd0048a40f51b3009
cc3f82 kubernetes.annotations.cni.projectcalico.org/podIP 172.30.79.199/3...
```

Below this, there are five more log entries, each with a timestamp and log details. At the bottom of the page, there are buttons for "Add a field" and "Rows per page: 100".

Use Kibana for Elasticsearch Log

Kibana Discover View Log Detail

The screenshot shows the Kibana Discover interface. On the left, there's a sidebar with 'Selected fields' (structured.trace_id, structured.span_id), 'Popular fields' (structured.marker), and 'Available fields' (including @timestamp, apid_name, file, host, message, source_type, structured.@timestamp, structured.app, structured.caller_class_name, structured.caller_file_name, structured.caller_line_number, structured.caller_method_name, structured.clientSeqNo, structured.context_path, structured.exception, structured.guid, structured.level). A red box highlights the 'Available fields' section. The main area shows a histogram from 14:15 to 14:25 on January 21, 2025, with a peak around 14:20. Below it, a table lists 11,131 documents with columns: @timestamp, structured.trace_id, and structured.span_id. Another red box highlights this table. To the right, a 'Document' modal is open, showing 1 of 500 results. The modal has tabs for 'Table' and 'JSON'. The 'Table' tab shows a list of fields and values. The 'JSON' tab shows the full JSON document.

Field	Value
structured.caller_line_number	191
structured.caller_method_name	getToDoBadgeNumber
structured.clientSeqNo	(empty)
structured.context_path	(empty)
structured.exception	(empty)
structured.guid	(empty)
structured.level	INFO
structured.logger	Common
structured.marker	(empty)
structured.message	resObj={"toDoSum":0,"checkToken":"true"}
structured.pid	3187569
structured.span_id	b00b9c88bde7b92a

點擊展開查看 Document 結構內容

Use Kibana for Elasticsearch Log

Kibana Discover Add Field Column

The screenshot shows the Kibana Discover interface. At the top, there's a search bar with 'Find apps, content, and more.' and a date range selector 'Last 15 minutes'. Below the search bar, there's a sidebar with a list of fields: structured.foundation_version, structured.foundation_version_time stamp, structured.guid, structured.hostname, structured.level, structured.logger, structured.marker, structured.message, structured.pid, structured.request_uri, structured.span_id, structured.tellerId, structured.thread, structured.trace_id, and structured.txSeqNo. The 'structured.trace_id' field is highlighted with a red box. A callout bubble from a button labeled 'Add field as column' points to this red box. The main area displays a timeline from January 21, 2025, at 14:13 to 14:28, with several green bars indicating document intervals. Below the timeline, a table shows 'Documents (148)'. The first row of the table has two columns: 'structured.@timestamp' and 'structured.trace_id'. The second row shows 'Jan 21, 2025 @ 14:23:18.970' and '46d5b05aca32bc7e4f1e5725c8acd240'. The third row shows 'Jan 21, 2025 @ 14:23:18.968' and '46d5b05aca32bc7e4f1e5725c8acd240'. The fourth row shows 'Jan 21, 2025 @ 14:23:18.961' and '46d5b05aca32bc7e4f1e5725c8acd240'. There are also 'Columns' and 'Sort fields' buttons at the bottom of the table.

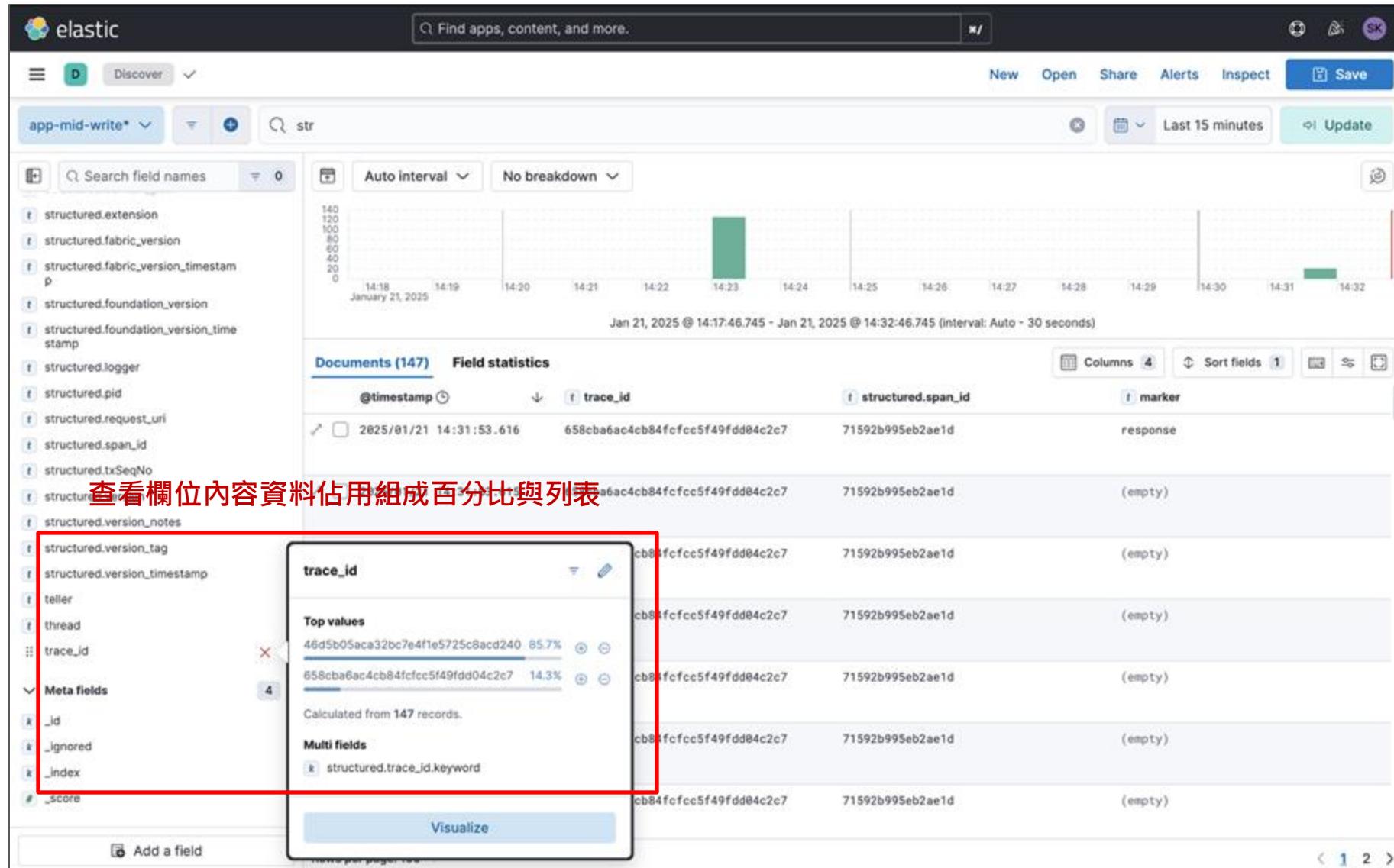
增加自定義顯示欄位內容

Add field as column

structured.@timestamp	structured.trace_id
Jan 21, 2025 @ 14:23:18.970	46d5b05aca32bc7e4f1e5725c8acd240
Jan 21, 2025 @ 14:23:18.968	46d5b05aca32bc7e4f1e5725c8acd240
Jan 21, 2025 @ 14:23:18.961	46d5b05aca32bc7e4f1e5725c8acd240

Use Kibana for Elasticsearch Log

Kibana Discover View Column



Use Kibana for Elasticsearch Log

Kibana Discover Search

The screenshot shows the Kibana Discover interface. At the top, there is a search bar with the query: structured.tellerId : 06801179 and structured.trace_id.keyword : f1114267382ca1b5d74e0fa3f14966b2. Below the search bar, there is a red box highlighting the search bar and the text "查詢指定資料語法" (Query specified data syntax) which is overlaid on the interface. On the left, there is a sidebar with sections for Selected fields, Popular fields, and Available fields. The main area displays a timeline from 18:04 to 18:18 on October 21, 2025. A green bar highlights a specific event at 18:11. Below the timeline, a table shows 8 documents with columns for @timestamp, structured.caller_line_number, structured.trace_id, and teller. The teller column values are highlighted in yellow: 06801179, 06801179, 06801179, 06801179, 06801179, 06801179, 06801179, and 06801179.

Document ID	@timestamp	structured.caller_line_number	structured.trace_id	teller
1	2025/10/21 18:11:35.027		f1114267382ca1b5d74e0fa3f14966b2	06801179
2	2025/10/21 18:11:35.026		f1114267382ca1b5d74e0fa3f14966b2	06801179
3	2025/10/21 18:11:35.023		f1114267382ca1b5d74e0fa3f14966b2	06801179
4	2025/10/21 18:11:35.019		f1114267382ca1b5d74e0fa3f14966b2	06801179
5				
6				
7				
8				

Use Kibana for Elasticsearch Log

Kibana Discover Search

Documents (52) Field statistics

Get the best look at your search results

Add relevant fields, reorder and sort columns, resize rows, and more in the document table.

Take the tour **Dismiss**

@timestamp	Document
Oct 8, 2025 @ 11:44:36.271	apid_name t24 structured.trace_id d3e347581c961b1c7bda7216df214ccf @timestamp Oct 8, 2025 @ 11:44:36.271 file /opt/SIT/SIT1/logs/irisLogs/iris-api-container/iris-api-container.log host DT24001 level TRACE message Transact response received: 100147/EXTERNALUUID00-d3e347581c961b1c7bda7216df214ccf-f02f176a1d385e6e-01/1, MNEMONIC:1:1=A193463605, SHORT.NAME:1:1=TEST, NAME.1:1:1=CHEN TEST, STREET:1:1=TAMSUI TEST, TOWN.COUNTRY:1:1=NEW TAIPEI CITY, COUNTRY:1:1=TW, SECTOR:1:1=1101, ACCOUN...
Oct 8, 2025 @ 11:44:31.759	apid_name apc structured.trace_id d3e347581c961b1c7bda7216df214ccf @timestamp Oct 8, 2025 @ 11:44:31.759 file /opt/jbosss/jboss-eap-7.4/standalone/log/aplog/apic-ap.log host DAPCN01 proxy_hostname DELSP01 source_type file structured.@timestamp Oct 8, 2025 @ 11:44:31.759 structured.app apic-dapcg01-ap p structured.caller_class_name com.ibm.logging.server.service.LoggingService structured.caller_file_name LoggingService.java structured.caller_line_number 3...
Oct 8, 2025 @ 11:44:31.759	apid_name apc structured.trace_id d3e347581c961b1c7bda7216df214ccf @timestamp Oct 8, 2025 @ 11:44:31.759 file /opt/jbosss/jboss-eap-7.4/standalone/log/aplog/apic-ap.log host DAPCN01 proxy_hostname DELSP01 source_type file structured.@timestamp Oct 8, 2025 @ 11:44:31.759 structured.app apic-dapcg01-ap p structured.caller_class_name com.ibm.logging.server.service.LoggingService structured.caller_file_name LoggingService.java structured.caller_line_number 2...
Oct 8, 2025 @ 11:44:31.033	apid_name brh structured.trace_id d3e347581c961b1c7bda7216df214ccf @timestamp Oct 8, 2025 @ 11:44:31.033 file /opt/SIT/jboss-eap-8.0/standalone/log/server.log host DBRH001 proxy_hostname DELSP01 source_type file structured.@timestamp Oct 8, 2025 @ 11:44:31.033 structured.app brh-brh structured.caller_class_name md s.com.scsb_s.Service.Transaction.ServerQueryService structured.caller_file_name ServerQueryService.java structured.caller_line_number 12...
Oct 8, 2025 @ 11:44:31.033	apid_name brh structured.trace_id d3e347581c961b1c7bda7216df214ccf @timestamp Oct 8, 2025 @ 11:44:31.033 file /opt/SIT/jboss-eap-8.0/standalone/log/server.log host DBRH001 proxy_hostname DELSP01 source_type file structured.@timestamp Oct 8, 2025 @ 11:44:31.033 structured.app brh-brh structured.caller_class_name md s.com.scsb_s.Service.Transaction.ServerQuery.SQCustInfo structured.caller_file_name SQCustInfo.java structured.caller_line_number 6...
Oct 8, 2025 @ 11:44:31.032	apid_name brh structured.trace_id d3e347581c961b1c7bda7216df214ccf @timestamp Oct 8, 2025 @ 11:44:31.032 file /opt/SIT/jboss-eap-8.0/standalone/log/server.log host DBRH001 proxy_hostname DELSP01 source_type file structured.@timestamp Oct 8, 2025 @ 11:44:31.032 structured.app brh-brh structured.caller_class_name md s.com.scsb_s.Service.Tools.CommonFnService structured.caller_file_name CommonFnService.java structured.caller_line_number 2584 structured.caller_method_name p...
Oct 8, 2025 @ 11:44:31.032	apid_name brh structured.trace_id d3e347581c961b1c7bda7216df214ccf @timestamp Oct 8, 2025 @ 11:44:31.032 file /opt/SIT/jboss-eap-8.0/standalone/log/server.log host DBRH001 proxy_hostname DELSP01 source_type file structured.@timestamp Oct 8, 2025 @ 11:44:31.032 structured.app brh-brh structured.caller_class_name md s.com.scsb_s.Service.Transaction.Common.OutputProcess structured.caller_file_name OutputProcess.java structured.caller_line_number 63...
Oct 8, 2025 @ 11:44:31.031	apid_name brh structured.trace_id d3e347581c961b1c7bda7216df214ccf @timestamp Oct 8, 2025 @ 11:44:31.031 file /opt/SIT/jboss-eap-8.0/standalone/log/server.log host DBRH001 proxy_hostname DELSP01 source_type file structured.@timestamp Oct 8, 2025 @ 11:44:31.031 structured.app brh-brh structured.caller_class_name md

Use Kibana for Elasticsearch Log

Kibana Dashboard Search

The screenshot shows the Kibana interface with a dark header bar. The header includes the elastic logo, a search bar with the placeholder "Find apps, content, and more.", and user profile icons.

The main navigation bar has tabs for Home, Analytics, Search, and Observability. The Analytics tab is currently selected, indicated by a green background and a blue border around the "Discover" and "Dashboards" sub-options. The "Dashboards" option is underlined, indicating it is active.

A sidebar on the left is titled "選擇 Dashboard" (Select Dashboard) and contains links for Machine Learning, Visualize Library, Overview, Content, Elasticsearch, Vector Search, Semantic Search, Playground, Behavioral Analytics, and Observability. The Observability link is also underlined.

The main content area features a "Welcome home" banner with four cards: "Search" (yellow), "Observability" (pink), "Security" (teal), and "Analytics" (blue). Below this is a section titled "Get started by adding integrations" with instructions to collect data from an app or service or upload a file. It includes buttons for "Add integrations", "Try sample data", and "Upload a file".

At the bottom right, there is a "Try managed Elastic" section with an illustration of a cloud and a "Move to Elastic Cloud" button.

Use Kibana for Elasticsearch Log

Kibana Dashboard Search

The screenshot shows the Kibana interface with a red border around the main content area. At the top, there is a header with the elastic logo, a search bar containing 'Find apps, content, and more.', and a user icon. Below the header, a navigation bar has a 'Dashboards' tab selected. The main section is titled 'Dashboards'. It includes a search bar, filter buttons for 'Recently updated', 'Tags', and 'Created by', and a blue 'Create dashboard' button. A red box highlights the first two items in a list of dashboards:

- Name, description, tags
- [SCSB] AP Log Dashboard

Next to the second item, the text '選擇指定 dashboard' is overlaid in red. The list continues with other dashboards:

- [Elastic Security] Detection rule monitoring
- This dashboard helps you monitor the health and performance of detection rules.

At the bottom of the list, there are 'Managed' and 'Security Solution' tags.

Use Kibana for Elasticsearch Log

Kibana Dashboard Search

The screenshot shows the Kibana interface for searching logs. A red box highlights the search bar at the top, which contains the placeholder text "Filter your data using KQL syntax" and the Chinese text "查詢指定資料語法". Another red box highlights the filter section below the search bar, containing fields for APID, Trace ID, TellerID, Extension Stan (FEP), Extension Marker (FEP), Extension ATM NO (BRH), and Extension Message ID (FEP). A third red box highlights the main results table, which displays log entries with columns for @timestamp, structured.message, structured.trace_id, apid_name, structured.tellerId, structured.app, and structured.guid. The table shows several log entries from October 20, 2025, such as FISCService Empty FISC Response and FEP server logs. A red callout box points to the filter section with the text "下列選擇常見的欄位進行篩選".

查詢指定資料語法

APID Any

Trace ID Exists

TellerID Any

Extension Stan (FEP) Any

Extension Marker (FEP) Any

Extension ATM NO (BRH) Any

Extension Message ID (FEP) Exists

下列選擇常見的欄位進行篩選

@timestamp	structured.message	structured.trace_id	apid_name	structured.tellerId	structured.app	structured.guid
Oct 20, 2025 @ 17:22:59.503	FISCService Empty FISC Response STAN=800CBBE	8e5390ce20244a77aa24e16c8f568d 6c	fep	(empty)	fep-server-fisc	(empty)
Oct 20, 2025 @ 17:22:59.502	(empty)	8e5390ce20244a77aa24e16c8f568d 6c	fep	(empty)	fep-server-fisc	(empty)
Oct 20, 2025 @ 17:22:59.499	(empty)	8e5390ce20244a77aa24e16c8f568d 6c	fep	(empty)	fep-server-fisc	(empty)
Oct 20, 2025 @ 17:22:59.490	(empty)	8e5390ce20244a77aa24e16c8f568d 6c	fep	(empty)	fep-server-fisc	(empty)

Rows per page: 500

Search results are limited to 500 documents. Add more search terms to narrow your search.

Default All DataView

@timestamp	Document
Oct 20, 2025 @ 17:22:59.503	@timestamp Oct 20, 2025 @ 17:22:59.503 apid_name fep file /opt/P2/Logs/2025-10-20/fep-server-fisc/fep-server-fisc-FISCService-elk-2025-10-20-0.log host DFEPA01 proxy_hostname DELSP01 source_type file structured.@timestamp Oct 20, 2025 @ 17:22:59.503 structured.app fep-server-fisc structured.clientSeqNo (empty) structured.context_path /server/fisc structured.exception (empty) structured.guid (empty) structured.hostname DFEPA01 structured.level INFO structured.logger OTELMessageLogger structured.marker (empty) structured.message FISCService Empty FISC Response S...



07

Kibana 查詢使用語法

Use Kibana for Elasticsearch Log

Kibana Query DSL 查詢

編號	比較項目	使用 field	使用 field.keyword
1	型別	text	keyword
2	是否分詞	是	否
3	查詢方式	支援模糊搜尋、全文搜尋 (match)	精確比對 (term / exact match)
4	可否用於聚合	不支援	可 (terms、count、group by)
5	常見用途	搜尋內容包含某詞	_exists_: user
6	使用範例	message: error → 找出包含 "error" 的訊息	message.keyword: "error" → 找欄位完全等於 "error" message.keyword: error* → 找開頭為 "error" 的字串
7	重要差異說明	<ul style="list-style-type: none"> message: error 找不到 "erroraaa" (因為 token 是 "erroraaa" 不是 "error") message: error* 找得到 "erroraaa" (wildcard 不經 analyzer) 	<ul style="list-style-type: none"> 不分詞 error* 或 "error" 都以原始字串比對搜尋，表示內容完全等於 "error*" 或 "error"
8	最佳使用範例	<ul style="list-style-type: none"> 搜尋 log message: message: timeout 模糊搜尋內容 : message: fail~ 	<ul style="list-style-type: none"> 聚合統計 : terms(field="host.keyword") 篩選 : status.keyword: "FAILED"

Use Kibana for Elasticsearch Log

Kibana Query DSL 查詢

編號	查詢語法	查詢類型	是否分詞	搜尋邏輯	範例符合結果
1	name: error	Term Query (單詞搜尋)	是	搜尋欄位中包含單詞 "error"	system error occurred error in system unexpected system failure
2	name: "error"	Phrase Query (連續出現，順序相同搜尋)	是	搜尋欄位內容中整段等於 "error"	error system error occurred
3	name: error*	Wildcard Query (前綴搜尋)	否	搜尋欄位中以 "error" 開頭的字串	"erroraaa" "error_log" "system error"
4	name: "system error"	Phrase Query (連續出現，順序相同搜尋)	是	搜尋欄位中詞組連續且順序一致	system error occurred error in system
5	name.keyword: "error"	Exact Match (精確比對)	否	欄位整體值必須完全等於 "error"	error system error

Use Kibana for Elasticsearch Log

Kibana Query DSL 使用範例

編號	項目	說明
1	尋找特定欄位的值	status: "error"
2	多個欄位的比對	status: "error" AND user: "john.doe"
3	使用 OR 條件	status: "error" OR status: "warning"
4	範圍查詢	@timestamp >= "2024-11-01T00:00:00" AND @timestamp <= "2024-11-13T23:59:59"
5	存在查詢	_exists_: user
6	通配字元查詢	user: "john*"
7	反向查詢	NOT status: "success"
8	複合查詢	status: "error" AND (user: "john.doe" OR user: "jane.doe")

Use Kibana for Elasticsearch Log

Kibana Query DSL 使用範例

編號	項目	說明
9	搜尋包含空白的值	"user.name.keyword": "John Doe"
10	搜尋特定範圍內的數值	response_time > 100 AND response_time < 500
11	搜尋多個值中的任一個	status: ("error" OR "warning" OR "critical")
12	搜尋多個欄位中任一欄位的值	message: "failed" OR details: "failed"
13	搜尋特定詞語但區分大小寫	status.keyword: "ERROR"
14	不等於指定值	status != "success" Kibana 設定為 Lucene 模式，應改: NOT status:"success" 或 !status:"success"
15	搜尋多個欄位皆存在	_exists_: status AND _exists_: user
16	使用 Regexp	<ul style="list-style-type: none"> • user.keyword:/^j.*n\.doe\$/ 注意 KQL 僅 keyword 下使用 regexp • user:/j.*n.doe/ 注意 Lucene Query 才支援

Use Kibana for Elasticsearch Log

Kibana Query DSL 使用範例

編號	項目	說明
17	字串包含部分內容但不使用通配字元	message: "database connection"
18	結合 AND 和 OR 進行複合查詢	(status: "error" AND user: "admin") OR status: "critical"
19	搜尋具有非空值的欄位	status: *
20	排除特定欄位的存在	NOT _exists_ : error_details
21	搜尋欄位值包含某子字串	file_path: "/var/log/*"
22	搜尋日期欄位中一個特定日期	@timestamp: "2024-11-13"
23	搜尋在特定欄位中包含詞語的數字範圍查詢	memory_usage >= 50 AND memory_usage <= 100
24	查詢時包括空白字元的欄位名稱	"user full name": "Alice Smith"
25	混合布林查詢和通配字元	status: ("error*" AND NOT "success*")



08

AP 入住表申請與填寫

入住流程說明

1. 新核心系統廠商：

- 向服務處索取AP入住表。
- 填寫 AP入住申請表內的ELK入住表與提供日誌範例。
- 將填寫好的申請表提交給 研發處窗口。

2. 研發處窗口：

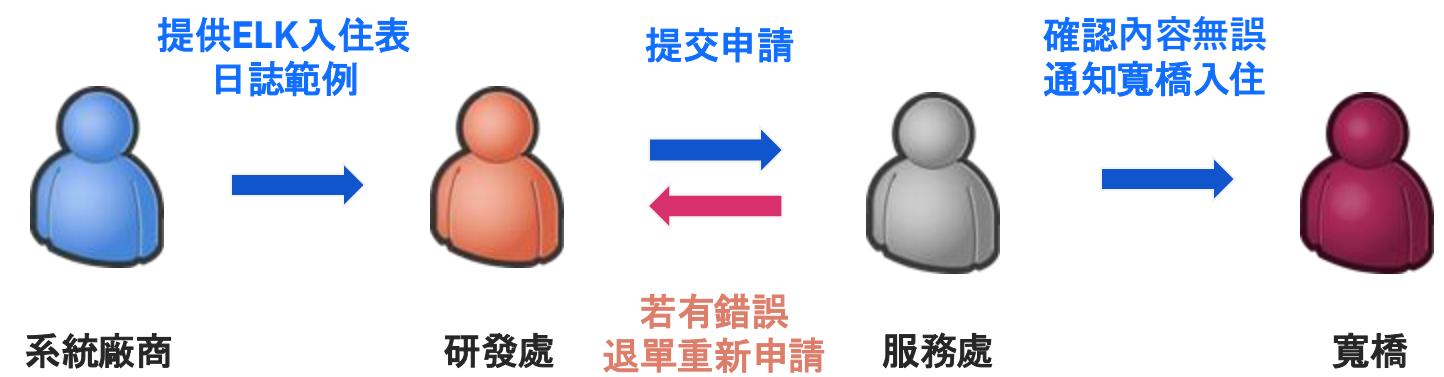
- 將填寫好的申請表與日誌範例提交 服務處窗口。

3. 服務處窗口：

- 接收研發處窗口提供的入住申請。
- 確認填寫資訊無誤（若有錯誤退單重新申請）
- 通知寬橋進行入住。

4. 寬橋人員：

- 收到研發處窗口的入住通知後分析日誌範例是否符合規範。
(若有錯誤聯繫系統廠商進行修正)
- 到場確認系統時實際產出日誌內容（若有錯誤聯繫系統廠商進行修正）
- 設定ELK與建立Kibana帳號。
- 完成入住後通知服務處確認。



AP Log 申請入住表格

VM AP Log 申請入住表格組成

- 申請人資訊表
- VM AP 日誌申請表
- Kibana 登入帳號申請表
- OCP AP 日誌申請表
- 自訂日誌解析申請表

ELK 申請表							說明																																																	
編號	表格申請項目																																																							
1	VM AP Log 收集申請表			VM 或是實體機器 AP 的日誌收集申請表格																																																				
2	Kibana 帳號申請			登入後台 Kibana 帳號申請表格																																																				
3	OCP ONLY			OCP 環境的 AP 日誌收集申請表格																																																				
	申請人	申請人email	申請日期	附註																																																				
	User	XXX@sssh.com.tw																																																						
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th colspan="7">1. VM AP LOG 收集申請表</th> <th>AP 記錄檔案路徑與名稱規則 (請填寫)</th> </tr> <tr> <th>Request (新增/修改/ 刪除)</th> <th>環境 (DEV/UAT/Prod)</th> <th>專案/系統名 稱 (請填寫)</th> <th>APID 名 稱 (請填 寫)</th> <th>Sub-Service Name (識別子服務名稱 - 沒有請填 入None)</th> <th>主機名稱 (請填寫)</th> <th>主機 IP (請填寫)</th> </tr> </thead> <tbody> <tr> <td>新增</td> <td>DEV</td> <td>BAW</td> <td>BAW</td> <td>none</td> <td>DBAWC01</td> <td>10.21.106.111</td> <td>/opt/DEV/TWCtlLogs/{YYYY-MM-DD}/bawctl-{YYYY-MM-DD}*</td> </tr> <tr> <td>新增</td> <td>DEV</td> <td>BAW</td> <td>BAW</td> <td>none</td> <td>DBAWC01</td> <td>10.21.106.111</td> <td>/opt/SIT/TWCtlLogs/{YYYY-MM-DD}/bawctl-{YYYY-MM-DD}*</td> </tr> </tbody> </table>								1. VM AP LOG 收集申請表							AP 記錄檔案路徑與名稱規則 (請填寫)	Request (新增/修改/ 刪除)	環境 (DEV/UAT/Prod)	專案/系統名 稱 (請填寫)	APID 名 稱 (請填 寫)	Sub-Service Name (識別子服務名稱 - 沒有請填 入None)	主機名稱 (請填寫)	主機 IP (請填寫)	新增	DEV	BAW	BAW	none	DBAWC01	10.21.106.111	/opt/DEV/TWCtlLogs/{YYYY-MM-DD}/bawctl-{YYYY-MM-DD}*	新增	DEV	BAW	BAW	none	DBAWC01	10.21.106.111	/opt/SIT/TWCtlLogs/{YYYY-MM-DD}/bawctl-{YYYY-MM-DD}*																		
1. VM AP LOG 收集申請表							AP 記錄檔案路徑與名稱規則 (請填寫)																																																	
Request (新增/修改/ 刪除)	環境 (DEV/UAT/Prod)	專案/系統名 稱 (請填寫)	APID 名 稱 (請填 寫)	Sub-Service Name (識別子服務名稱 - 沒有請填 入None)	主機名稱 (請填寫)	主機 IP (請填寫)																																																		
新增	DEV	BAW	BAW	none	DBAWC01	10.21.106.111	/opt/DEV/TWCtlLogs/{YYYY-MM-DD}/bawctl-{YYYY-MM-DD}*																																																	
新增	DEV	BAW	BAW	none	DBAWC01	10.21.106.111	/opt/SIT/TWCtlLogs/{YYYY-MM-DD}/bawctl-{YYYY-MM-DD}*																																																	
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th colspan="4">2. Kibana 帳號申請</th> <th colspan="4">1.</th> </tr> <tr> <th>Request (新增/修改/ 刪除)</th> <th>環境</th> <th>帳號名稱</th> <th>密碼</th> <th colspan="4">1. 登入帳號名稱必須為 <apid>-viewer，其中 apid 請代換實際的 apid 名稱。 2. 登入帳號預設給的權限都是僅檢視 - 無管理權限。 3. 登入的密碼至少要 12 個字元。請盡量符合密碼要求常見規範： 須包含以下四種類型中的至少三種： 大寫英文字母 (A-Z) 小寫英文字母 (a-z) 數字 (0-9) 特殊符號 (!@#\$%^&*()_-+=[]{}<>?/)</th> </tr> </thead> <tbody> <tr> <td>新增</td> <td>DEV</td> <td>baw-viewer</td> <td></td> <td colspan="4"></td> </tr> <tr> <td></td> <td></td> <td></td> <td></td> <td colspan="4"></td> </tr> <tr> <td></td> <td></td> <td></td> <td></td> <td colspan="4"></td> </tr> <tr> <td></td> <td></td> <td></td> <td></td> <td colspan="4"></td> </tr> </tbody> </table>								2. Kibana 帳號申請				1.				Request (新增/修改/ 刪除)	環境	帳號名稱	密碼	1. 登入帳號名稱必須為 <apid>-viewer，其中 apid 請代換實際的 apid 名稱。 2. 登入帳號預設給的權限都是僅檢視 - 無管理權限。 3. 登入的密碼至少要 12 個字元。請盡量符合密碼要求常見規範： 須包含以下四種類型中的至少三種： 大寫英文字母 (A-Z) 小寫英文字母 (a-z) 數字 (0-9) 特殊符號 (!@#\$%^&*()_-+=[]{}<>?/)				新增	DEV	baw-viewer																														
2. Kibana 帳號申請				1.																																																				
Request (新增/修改/ 刪除)	環境	帳號名稱	密碼	1. 登入帳號名稱必須為 <apid>-viewer，其中 apid 請代換實際的 apid 名稱。 2. 登入帳號預設給的權限都是僅檢視 - 無管理權限。 3. 登入的密碼至少要 12 個字元。請盡量符合密碼要求常見規範： 須包含以下四種類型中的至少三種： 大寫英文字母 (A-Z) 小寫英文字母 (a-z) 數字 (0-9) 特殊符號 (!@#\$%^&*()_-+=[]{}<>?/)																																																				
新增	DEV	baw-viewer																																																						
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th colspan="4">3. OCP ONLY</th> <th colspan="4"></th> </tr> <tr> <th>Request (新增/修改/ 刪除)</th> <th>環境 (DEV/UAT/Prod)</th> <th>APID (請填寫)</th> <th>Project Name (請填 寫)</th> <th colspan="4">Container 名稱 (請填寫)</th> </tr> </thead> <tbody> <tr> <td>新增</td> <td></td> <td></td> <td></td> <td colspan="4"></td> </tr> <tr> <td></td> <td></td> <td></td> <td></td> <td colspan="4"></td> </tr> <tr> <td></td> <td></td> <td></td> <td></td> <td colspan="4"></td> </tr> <tr> <td></td> <td></td> <td></td> <td></td> <td colspan="4"></td> </tr> </tbody> </table>								3. OCP ONLY								Request (新增/修改/ 刪除)	環境 (DEV/UAT/Prod)	APID (請填寫)	Project Name (請填 寫)	Container 名稱 (請填寫)				新增																																
3. OCP ONLY																																																								
Request (新增/修改/ 刪除)	環境 (DEV/UAT/Prod)	APID (請填寫)	Project Name (請填 寫)	Container 名稱 (請填寫)																																																				
新增																																																								
								8. OMS Request																																																
								7. ELK Request																																																
								6.1 CICD Reference																																																
<div style="text-align: center; margin-top: 10px;"> 申請入住流程圖 入住申請流程 1. VM Request 1.1 VM Reference 2. IP申請表 3. F5-FQDN Request 3.1 F5-FQDN Reference 4. Firewall Request 4.1 Firewall Reference 5 OCP Request 6. CICD Request ≡ </div>																																																								

此申請單向服務處窗口索取

AP Log 申請入住表格

申請入住表格主要項目

編號	表格申請項目	說明
1	申請人資訊表	填寫申請人與郵件與日期
2	VM AP Log 申請表	VM 或是實體機器 AP 的日誌收集申請表格
3	Kibana 帳號申請	登入後台 Kibana 帳號申請表格
4	OCP AP Log 申請表	OCP 環境的 AP 日誌收集申請表格
5	自訂日誌解析申請表	VM 或是實體機器 AP 的日誌非標準格式申請解析轉換申請表

AP Log 申請入住表格

申請人資訊表內容

申請人	申請人email	申請日期	附註
User	XXX@scsh.com.tw		

- 1.申請人：負責專案的聯絡人，請填寫全名。
- 2.申請人 email：負責專案的 email。
- 3.申請日期：申請的日期資訊。

AP Log 申請入住表格

VM AP Log 申請入住表格內容

1. VM AP LOG 收集申請表							
Request (新增/修改/ 刪除)	環境 (DEV/UAT/Prod)	專案/系統名 稱 (請填寫)	APID 名 稱 (請填 寫)	Sub-Service Name (識別子服務名稱 · 沒有請填 入None)	主機名稱 (請填寫)	主機 IP (請填寫)	AP 記錄檔案路徑與名稱規則 (請填寫)
新增	DEV	BAW	BAW	none	DBAWC01	10.21.106.111	/opt/DEV/TWCtlLogs/{YYYY-MM-DD}/bawctl-{YYYY-MM-DD}*
新增	DEV	BAW	BAW	none	DBAWC01	10.21.106.111	/opt/SIT/TWCtlLogs/{YYYY-MM-DD}/bawctl-{YYYY-MM-DD}*

1. 申請需求(Request)：新增/修改/刪除
2. 申請環境：申請使用的環境，請填寫 DEV、UAT、或 PROD 等。
3. 專案名稱：對應專案名稱。
4. APID 名稱：對應專案所屬 APID 代碼名稱。
5. Sub-Service Name：對應專案子項服務分類名稱，若是無請填入「無」。
6. 主機名稱 (Host Name)：申請 AP LOG 日誌收取主機的名稱。
7. 主機 IP：申請主機的 IP 位址。
8. AP 記錄檔案路徑與名稱規則：指定記錄檔案的完整路徑包含檔案名稱。

AP Log 申請入住表格

Kibana 登入帳號申請表格內容

2. Kibana 帳號申請			
Request (新增/修改/刪 除)	環境	帳號名稱	密碼
新增	DEV	baw-viewer	1. 登入帳號名稱必須為 <apid>-viewer，其中 apid 請代換實際的 apid 名稱。 2. 登入帳號預設給的權限都是僅檢視，無管理權限。 3. 登入的密碼至少要 12 個字元，請盡量符合密碼要求常見規範： 須包含以下四種類型中的至少三種： 大寫英文字母 (A-Z) 小寫英文字母 (a-z) 數字 (0-9) 特殊符號 (!@#\$%^&*()_-+=+[]{} ;:,.<>?/)

說明：

1. 需要申請連線到 Kibana 後端管理網址，需要申請一組登入帳號提供檢視使用。
2. 填寫輸入應對的帳號名稱，比方 fep 帳號維 fep-viewer，密碼請依據上述要求填入提供設定。
3. Kibana 帳號名稱自訂，可以另外提出提交，帳號長度請勿超過 32 字元。
4. **若僅有查詢檢視日誌需求只需填寫此部分**

AP Log 申請入住表格

OCP AP Log 申請入住表格內容

3. OCP ONLY				
Request (新增/修改/刪 除)	環境 (DEV/UAT/Prod)	APID (請填寫)	Project Name (請填 寫)	Container 名稱 (請填寫)
新增				

1. 申請需求(Request) : 新增/修改/刪除

2. 申請環境 : 申請使用的環境, 請填寫 DEV、UAT、或 PROD 等。

3. APID : 對應專案所屬 APID 代碼名稱。

4. Project Name : 請填寫在OCP上的 namespace名稱。

5. Container 名稱 : 請填寫部署AP 的 Container Name。

AP Log 申請入住表格

額外補充資訊

4. 其他補充說明			
項目	環境	ELK 提供查詢 Kibana 網址	IP 位址
Kibana 連線資訊	Dev	https://delsk01.cbsd.scsb.com.tw:5601	10.21.104.167
	Stage	https://selsk01.cbss.scsb.com.tw:5601	10.22.104.167
	Prod	https://pelsk01.cbsp.scsb.com.tw:5601	10.23.104.167
項目	環境	日誌收集轉送目的	IP 位址
vector 日誌收集器 (安裝於被收集日誌的本機)	Dev	delsp01.cbsd.scsb.com.tw:5044 delsp02.cbsd.scsb.com.tw:5044 delsp03.cbsd.scsb.com.tw:5044	10.21.104.164 10.21.104.165 10.21.104.166
	Stage	selsp01.cbss.scsb.com.tw:5044 selsp02.cbss.scsb.com.tw:5044 selsp03.cbss.scsb.com.tw:5044	10.22.104.164 10.22.104.165 10.22.104.166
	Prod	pelsp01.cbsp.scsb.com.tw:5044 pelsp02.cbsp.scsb.com.tw:5044 pelsp03.cbsp.scsb.com.tw:5044	10.23.104.164 10.23.104.165 10.23.104.166

1. Kibana 部分， Dev 環境請自行提交開通本機電腦連線到目的 Kibana 主機 Firewall 申請

2. vector 日誌收集部分， 被收集的 Server 本身不需要申請開通 Firewall 允許連線到目的主機， 行內會統一申請允許連線

AP Log 申請入住表格

自定義日誌解析申請表格內容

A	B	C	D	E
說明	1. 行內規範一般的 AP 日誌需要為 JSON 的格式，結構組成已經有規範。 2. 日誌需要自訂解析格式，請提交要解析日誌的檔案名稱範例內容，與內容格式組成的欄位說明。 3. 日誌結構說明，請包含完整檔案的格式、欄位應對說明，與欄位的資料類型、欄位是否可省略。 4. 勿必於申請一併請提交日誌檔案範例與格式說明附件。			
日誌附件檔案名稱	日誌說明檔案名稱	備註		
請填寫附件檔名	請填寫說明文件檔名 (txt 或是 excel 等檔案)	額外備註內容		
範例：server.log	範例：server.xlsx	說明範例可以參考分頁內容		

說明：

1. 自定義解析的日誌，請檢附要解析的日誌檔案名稱列表，與 excel 檔案內要解析處理的說明。

AP Log 申請入住表格

自定義日誌解析申請說明表格內容

鍵名稱 (Key Name)	值 (Value)	資料型別 (Data Type)	說明 (Description)	是否解析 (Parse?)	應對目的產生的欄位
timestamp	2024-12-17 18:34:26,528	string	記錄時間，格式為 yyyy-MM-dd HH:mm:ss,SSS	是 (YES)	timestamp
thread	pool-27-thread-30	string	執行緒名稱或執行緒池的標識符	否 (NO)	thread
processId	1274873	integer	記錄此日誌的進程 ID	是 (YES)	pid
logLevel	DEBUG	string	日誌的等級，例如 DEBUG、INFO、ERROR 等	是 (YES)	loglevel
module	UTIL	string	日誌來自的模組名稱	否 (NO)	caller_method_name
uuld	be5c991b0c52473eba272faa1ec83754	string	唯一識別碼，用於追蹤相關操作	是 (YES)	
dimension	D	string	代表日誌的維度類型	否 (NO)	
level	DEBUG	string	與 logLevel 欄位一致，可能重複記錄	否 (NO)	刪除
component	TEMN-IRIS_dsf-iris-202303.0.17-UTIL	string	系統元件名稱或版本	否 (NO)	caller_class_name
className	com.temenos.irf.logging.IrisTemenosLogImpl:deb	string	Java 類別名稱及方法（行號為 66）	是 (YES)	caller_line_number
message	Time taken to retrieve from Transact(ms): 10 或 Tr	string	實際的日誌訊息內容	是 (YES)	message

檔案內容內容範例

```
2024-12-17 18:34:26,415 [t=pool-27-thread-30,p=1274873] INFO [UTIL] uuld="be5c991b0c52473eba272faa1ec83754",dim="D",level="INFO",comp="TEMN-IRIS_dsf-iris-202303.0.17-UTIL",cn="com.temenos.irf.logging.IrisTemenosLogImpl:debug"
2024-12-17 18:34:26,527 [t=pool-27-thread-30,p=1274873] INFO [UTIL] uuld="be5c991b0c52473eba272faa1ec83754",dim="D",level="INFO",comp="TEMN-IRIS_dsf-iris-202303.0.17-UTIL",cn="com.temenos.irf.logging.IrisTemenosLogImpl:debug
```

1. 自定義解析的日誌，說明日誌組成結構欄位與資訊說明，並告知是否解析與最終產生應對使用實際的欄位名稱。
2. 最終應對欄位名稱，請參考先前討論上述行內 AP 日誌已經定義的格式，若允許請盡量相同名稱應對。

研發處Kibana帳號申請流程說明

1. 研發處：

- 向服務處索取AP入住表。
- 填寫 AP入住申請表內的ELK入住表的Kibana帳號申請欄位。
- 將填寫好的申請表提交給 服務處窗口。

2. 服務處窗口：

- 接收研發處窗口提供的入住申請。
- 確認填寫資訊無誤（若有錯誤退單重新申請）。
- 建立Kibana帳號並通知研發處人員。



2. Kibana 帳號申請						
Request (新增/修改/刪 除)	環境	帳號名稱	密碼	規範		
新增	DEV	baw-viewer		1. 登入帳號名稱必須為 <apid>-viewer，其中 apid 請代換實際的 apid 名稱。 2. 登入帳號預設給的權限都是僅檢視，無管理權限。 3. 登入的密碼至少要 12 個字元，請盡量符合密碼要求常見規範： 須包含以下四種類型中的至少三種： 大寫英文字母 (A-Z) 小寫英文字母 (a-z) 數字 (0-9) 特殊符號 (!@#\$%^&*()_-+=[]{} ;:,.<>?/)		

AP Log 申請入住表格

3 入住申請提交

- 填寫文件完畢，將內容提交給該行內系統的窗口人員，進行內容確認
- 行內窗口人員審視完畢，建立 Notes 單內容，提交完成申請資訊表示提交完成
- 建立的申請單，行內流程將有適當窗口審視進行確認，並完成設定
- 申請單內文件有任何異常會退回申請單，原窗口收到退件狀態再行通知原申請人員

9

Redmine 帳號申請

流程說明

1. 研發處人員：

- 填寫 Redmine 帳號申請表（包含姓名、部門、電子郵件、申請類型、需要加入的專案），密碼由 IBM 設定。
- 將填寫好的申請表提交給 寬橋窗口。



2. 寬橋窗口：

- 接收研發處窗口提供的帳號申請清單。
- 確認填寫資訊無誤。
- 將清單提交給 IBM Redmine 管理員。

3. IBM Redmine 管理員：

- 接收寬橋窗口的申請清單。
- 在 Redmine 系統中為申請人建立帳號。
- 帳號建立完成後，知會寬橋窗口。

4. 帳號開立完成通知：

- 寬橋窗口通知研發處窗口，表示帳號已成功開立。

A	B	C	D	E	F
申請日期	姓名	所屬部門	電子郵件地址	申請類型	需要加入的專案名稱
2025/1/1	XXX(範例)	研發處	xxxxx@gmail.com	新增帳號	SCSB-NCBS-ELK
				新增帳號	
				已有帳號	
				停用帳號	

10

Redmine 檢視與新增議題

流程說明

1. 使用者連線至 Redmine 網址：

- 開啟瀏覽器，輸入Redmine 網址：

<https://128.168.142.185/login>

2. 登入系統：

- 在 Redmine 登入頁面，輸入您的帳號和密碼。



流程說明

3. 選擇專案：

- 登入後，在首頁或透過導覽列，找到 SCSB-NCBS-ELK 專案並點選進入。

The screenshot shows the homepage of the 'NCBS 系統建置專案'. On the right side, there is a sidebar with a dropdown menu titled '選擇欲前往的專案...'. A red arrow points to the 'SCSB-NCBS-ELK' option in this menu. The main content area displays 'Issue tags' (Amount tags: 26, Amount 議題清單 with tags: 56), a 'Activities' section for 'Today' showing a meeting log, and a footer with the date '2025-09-24'.

流程說明

4. 新增議題：

- 進入專案頁面後，點選左上角「+」，並點選「新增議題」。

The screenshot shows the Redmine project dashboard for the 'SCSB-NCBS-INFRA' project, specifically the 'SCSB-NCBS-ELK' instance. The header includes a search bar and a dropdown menu set to 'SCSB-NCBS-ELK'. Below the header, there's a navigation bar with tabs: '+', 概觀 (Overview), 活動 (Activities), 議題清單 (Issues), 時用工時 (Time Tracking), 甘特圖 (Gantt Chart), 日曆 (Calendar), 文件 (Documents), and 檔案清單 (Attachments). The '+’ tab is highlighted. On the left, there are two main sections: '議題追蹤' (Issue Tracking) and '工時追蹤' (Time Tracking). The '議題追蹤' section contains a table with counts for '文件交付(Delivery)', '議題管理(Issue)', and '工作項目(Task)'. The '工時追蹤' section lists '預估工時: 0:00 小時' and '耗用工時: 0:00 小時'. On the right, there's a 'Shared dashboards' sidebar with a 'Project dashboard' link. At the bottom, the URL is https://128.168.142.185/projects/scsb-ncbs-elk/issues/new and it says 'Powered by Redmine © 2006-2022 Jean-Philippe Lang'.

流程說明

5. 新增議題表單：

- **追蹤標籤**：選擇議題管理（issue）。
- **主旨**：簡潔扼要地描述問題或需求。
- **概述**：說明問題或需求內容細節。
- **優先順序**：根據議題的緊急性和重要性等級。
- **負責人**：指定該議題的負責人（寬橋PM）
- **開始及完成日期**：填入開始及完成日期。
- **附件**：上傳相關的截圖、文件或日誌檔。

6. 提交議題：

- 確認表單內容無誤後，點擊「新增」或「建立」按鈕。

7. 議題新增完成：

- 系統將自動導向至新創建的議題頁面，表示議題已成功新增。此時負責人及相關人員會收到通知。

The screenshot shows a detailed view of a software interface for creating a new issue. At the top, it displays the project name 'SCSB-NCBS-ELK' and the tracking label '議題管理(Issue)'. Below this is a rich text editor toolbar. The main body of the form contains several input fields: 'Status' (status) is set to 'Open'; 'Priority' (优先权) is set to 'Medium'; and there is a dropdown for 'Assignee' (被分配者) which has '分派給我' (Assign to me) selected. To the right, there are date and time fields for 'Start Date' (開始日期) and 'End Date' (完成日期), along with a 'Estimated Hours' (預估工時) field and a 'Completion Percentage' (完成百分比) set to '0 %'. At the bottom, there are sections for 'Tags' (Tags) and 'Attachments' (檔案), with a note indicating a maximum file size of 400 MB.