

E-7

結合大語言模型的系統監控與自動化平台

AI Powered Monitoring and Automation Platform

指導教授：張瑞紘

專題成員：莊智皓



Chapter 1

背景與動機

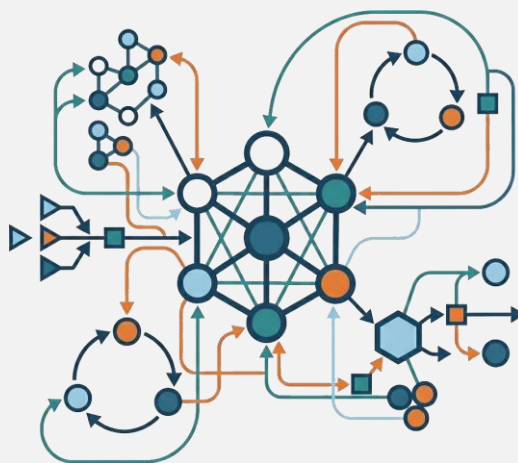
專題的發想過程及製作目的

背景與動機

越來越多的需求與日漸龐大的系統



需求增多



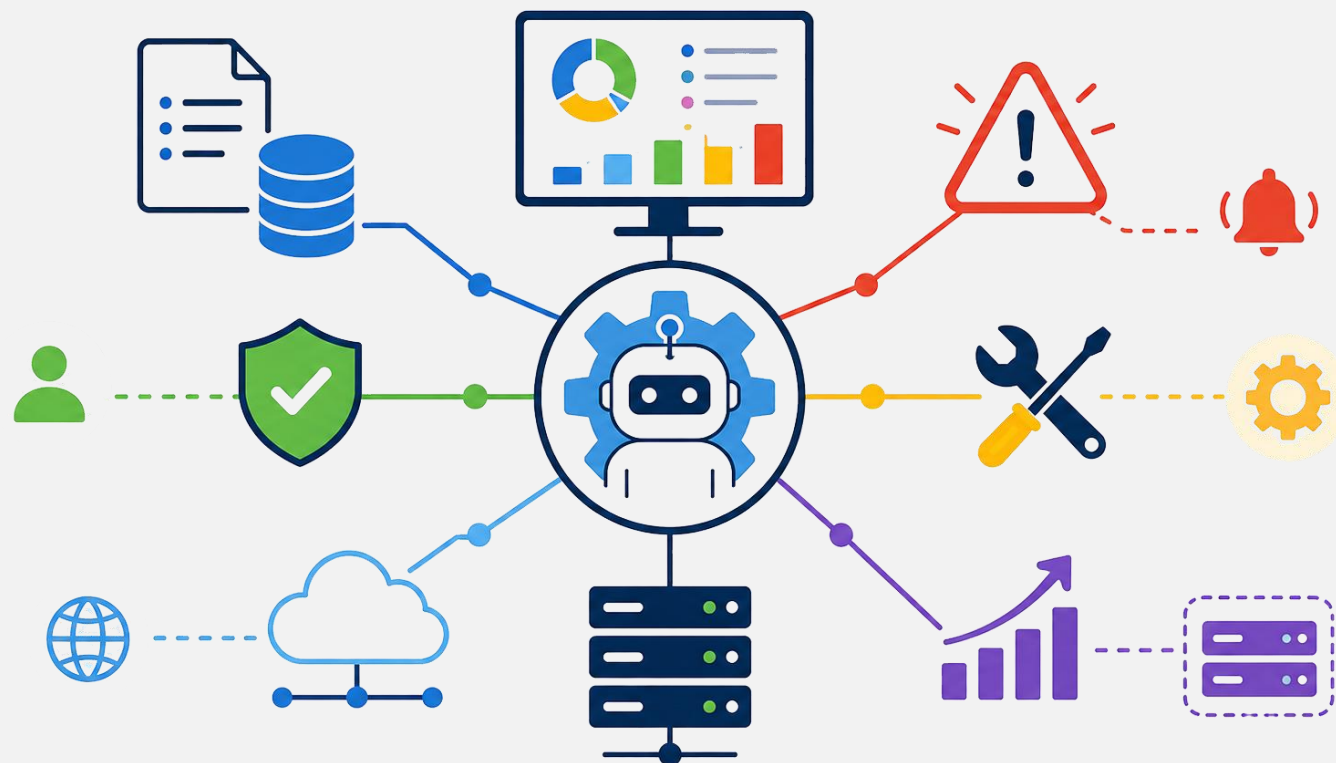
系統變複雜



維護成本增高

背景與動機

結合 LLM 協助進行管理





Chapter 2

內容與特色

專題的運作原理與特色過程

內容與特色

結合了監控與自動化的平台

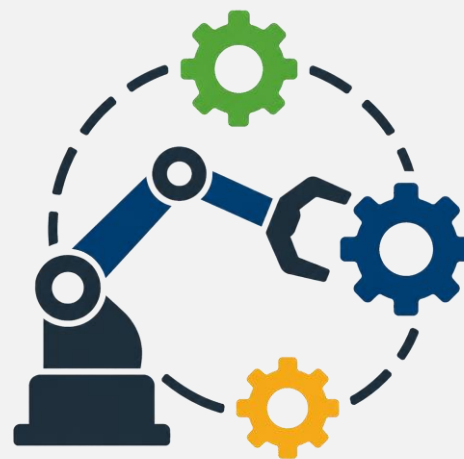
■ 監控

- 蒐集系統的各項資訊
- 為自動化提供判斷資料



■ 自動化

- 將原本手動執行的流程自動化
- 更加靈活的組合與應用



內容與特色

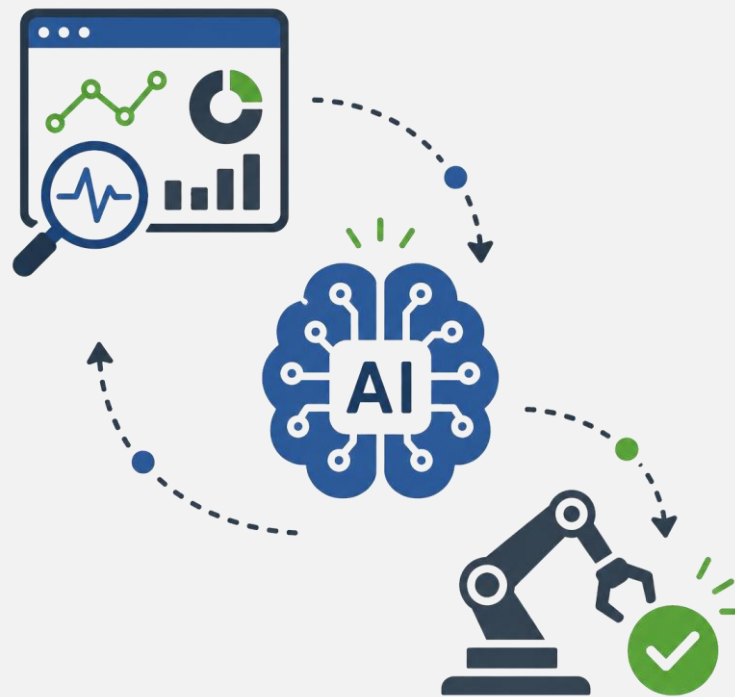
由 LLM 驅動的分析與決策系統

結合 LLM

- 將監控與自動化進行整合
- 自動分析資訊，產生適合的對策
- 提供應對方向
- 協同使用者進行規劃

圖形化介面

- Low Code 開發，使用門檻低





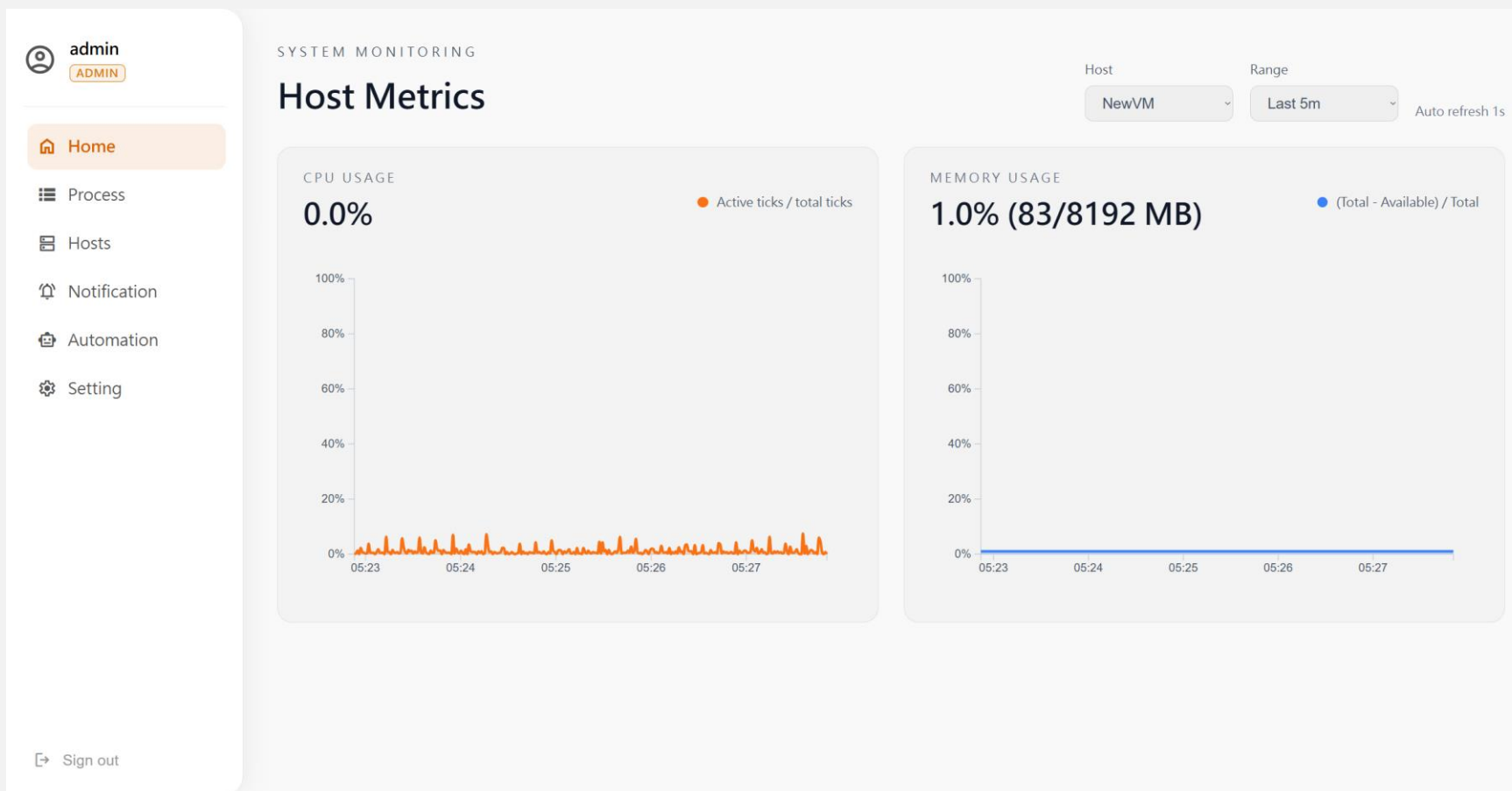
Chapter 3

成果與展示

專題的實際運作畫面

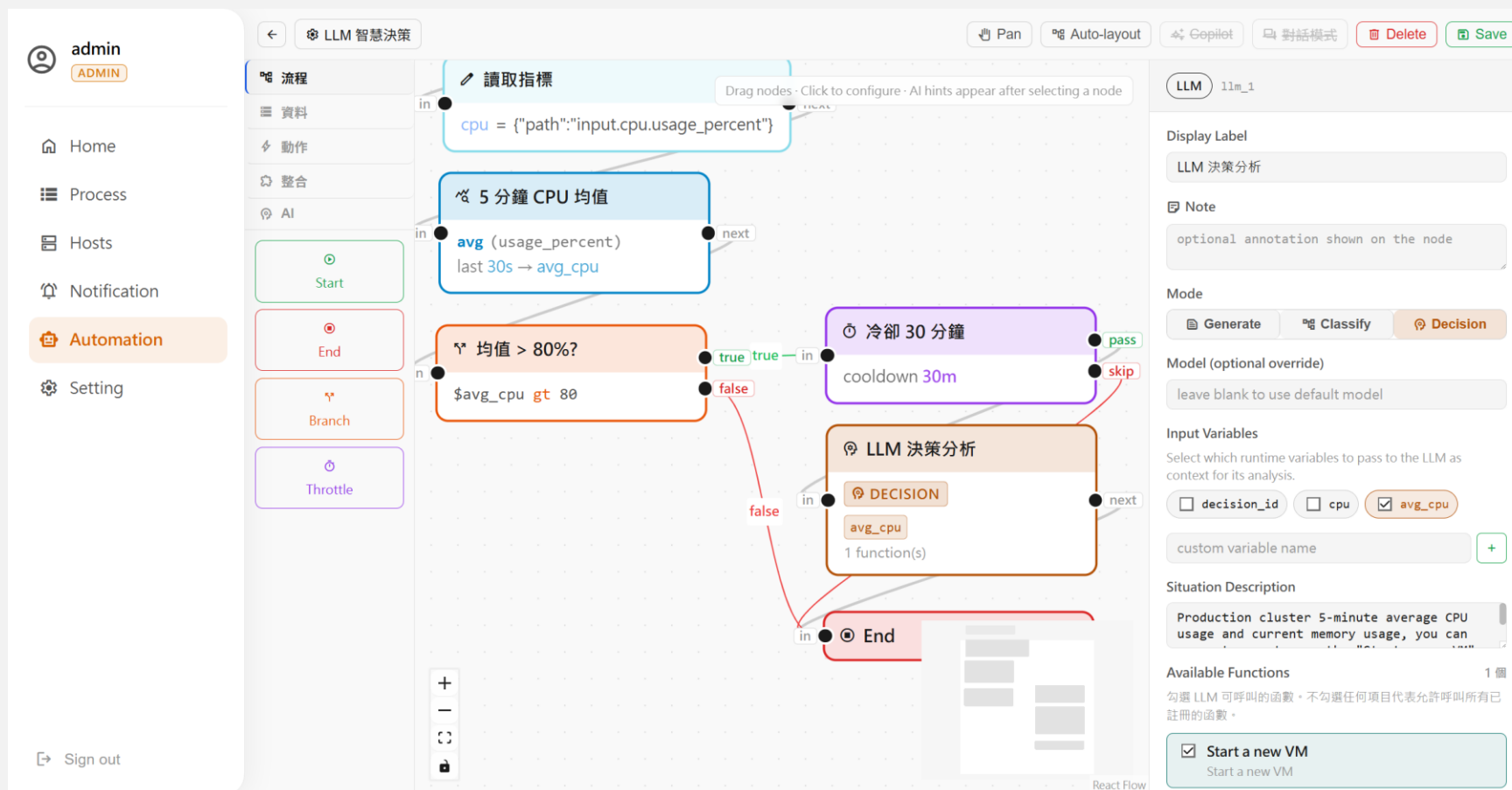
成果與展示

以圖表顯示節點狀態



成果與展示

Low Code 編輯介面



成果與展示

LLM 協同規劃

The screenshot displays the React Flow workflow editor interface. On the left is a sidebar with a user profile 'admin' and a list of navigation items: Home, Process, Hosts, Notification, Automation (highlighted), and Setting. Below these is a 'Sign out' button. The main workspace shows a workflow titled 'Webhook 告警推送'. A node palette on the left includes Start, End, Branch, and Throttle. The central canvas contains a 'Throttle' node (purple) with the label '冷卻 10 分鐘' and 'cooldown 10m'. It has two exit paths: 'pass' (green) and 'skip' (red). The 'pass' path leads to an 'http 發送 Webhook' node (blue) with a tooltip explaining that it sends a POST request with CPU and memory data to trigger external alerting. The right sidebar shows the configuration for the selected 'THROTTLE' node, including a 'Display Label' field, a 'Note' field, and a 'Cooldown period' section with preset options (30s, 1m, 5m, 15m, 30m, 1h) and a 'custom' button set to 600 seconds. A legend at the bottom right explains the exit paths: 'Pass → upper-right exit (triggers normally)' and 'Skip → lower-right exit (suppressed)'. The bottom right corner of the canvas has the text 'React Flow'.

成果與展示

應對措施推薦

admin
ADMIN

Home

Process

Hosts

Notification

Automation

Setting

Sign out

Automation

FlowsFunction LibraryPending Decisions 2

2 pending decisions awaiting approvalRefresh

HIGHHTTP Log 惡意掃描偵測2026/6/12 上午5:31:44Dismiss

IP 172.16.0.110 generated over 400 requests within a single second, all returning HTTP 404. The paths systematically enumerate admin panel variants (/admin-*, /admin-console, /admin-cp, etc.) with randomized User-Agents. This is a clear reconnaissance scan probing for exposed admin interfaces. Immediate blocking is recommended to prevent further probing or potential exploitation.

Block IP via iptables

Add an iptables DROP rule for source IP 172.16.0.110 to immediately terminate all traffic from the scanning host at the network level.
HTTP POST: http://localhost/iptables/block

Approve

Deny IP in Nginx config

Add 172.16.0.110 to the Nginx deny list and reload configuration to block the scanner at the application layer without affecting other services.
HTTP POST: http://localhost/nginx/deny

Approve

Continue monitoring only

No immediate action. Continue logging further requests from this IP for additional analysis before deciding on a block.
No action

Approve

HIGHLLM 智慧決策2026/6/12 上午5:32:41Dismiss

Average CPU usage in the production cluster is 85.11%, indicating high load. To balance the load, starting a new VM can distribute compute resources. The available function 'Start a new VM' provides a direct way to launch a new instance. Alternative actions include cloning an existing template VM or resizing current VMs to increase capacity. Monitoring is also an option if the load is expected to be transient.

感謝聆聽

Thanks for listening