



Hello World  
Dev Conference 2025

Building the Future Together

AI 的可能性 ✦ 軟體開發的無限性



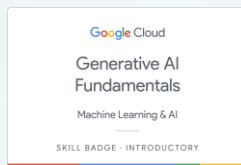
# 讓 SQL Server 聽你說話 - MCP 驅動的 AIOps

Room A (16:05 - 16:35) 2025.10.14

Jerry Hsu



Jerry HSU



## Expertise

- Problem solving
- SQL Server Performance tuning
- CDN / WAF optimization
- Hybrid cloud solution
- Design Thinking coach

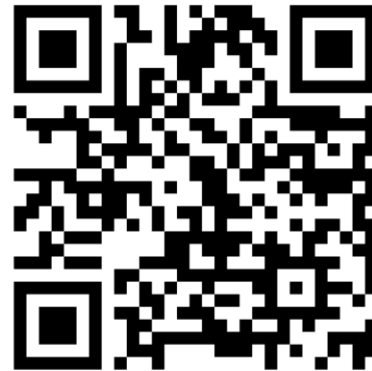
## Experience

- 華碩電腦 技術服務部 Lead
- 華碩電腦 系統開發課 Lead
- 東森購物 資深資料庫管理師
- 淡江大學資訊處 技士

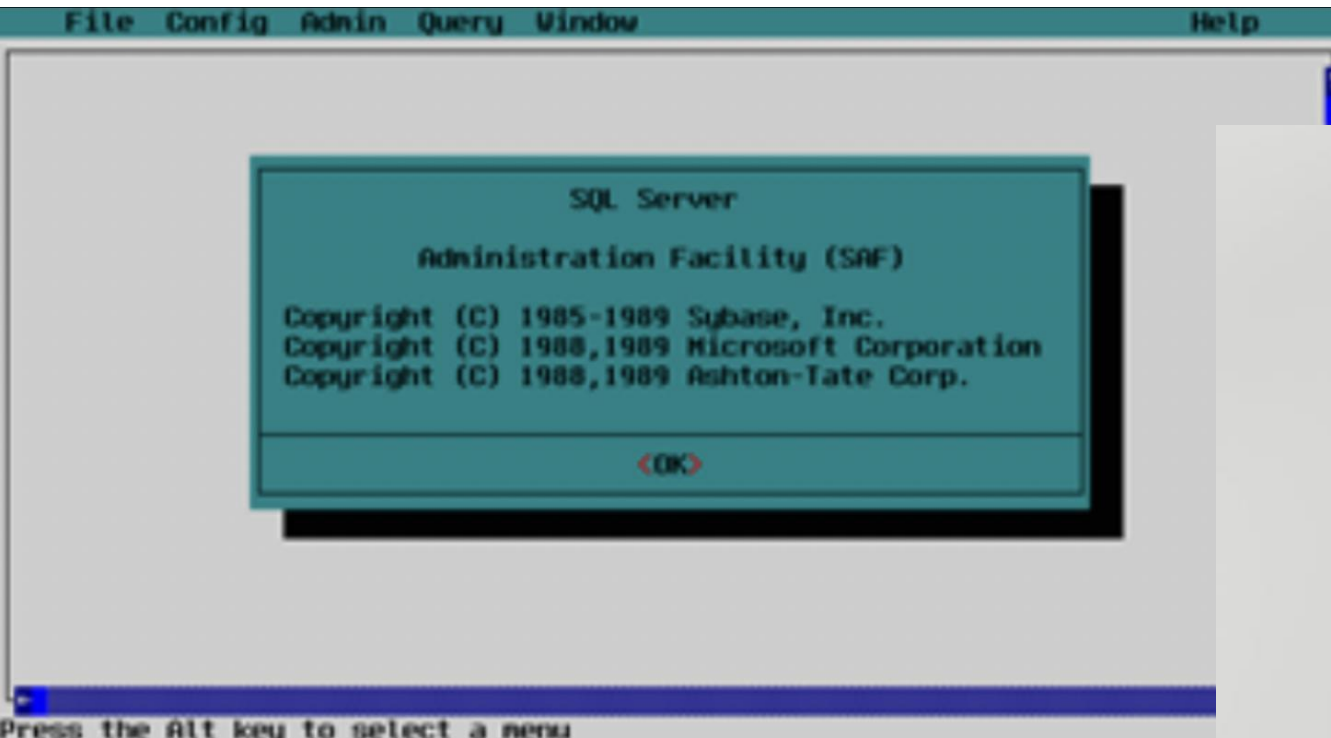
## Community

- 2025 Cloud Summit Taiwan
- 2024 東吳大學 設計思維與AI
- 2024 SQL Summit Speaker
- 2022 SQL Summit Speaker
- 2021 SQL Saturday Speaker
- TW SQL PASS 8<sup>th</sup> 幹部、籌辦台灣第一屆 SQL Saturday 年會

Join at  
**slido.com**  
**#1775 165**



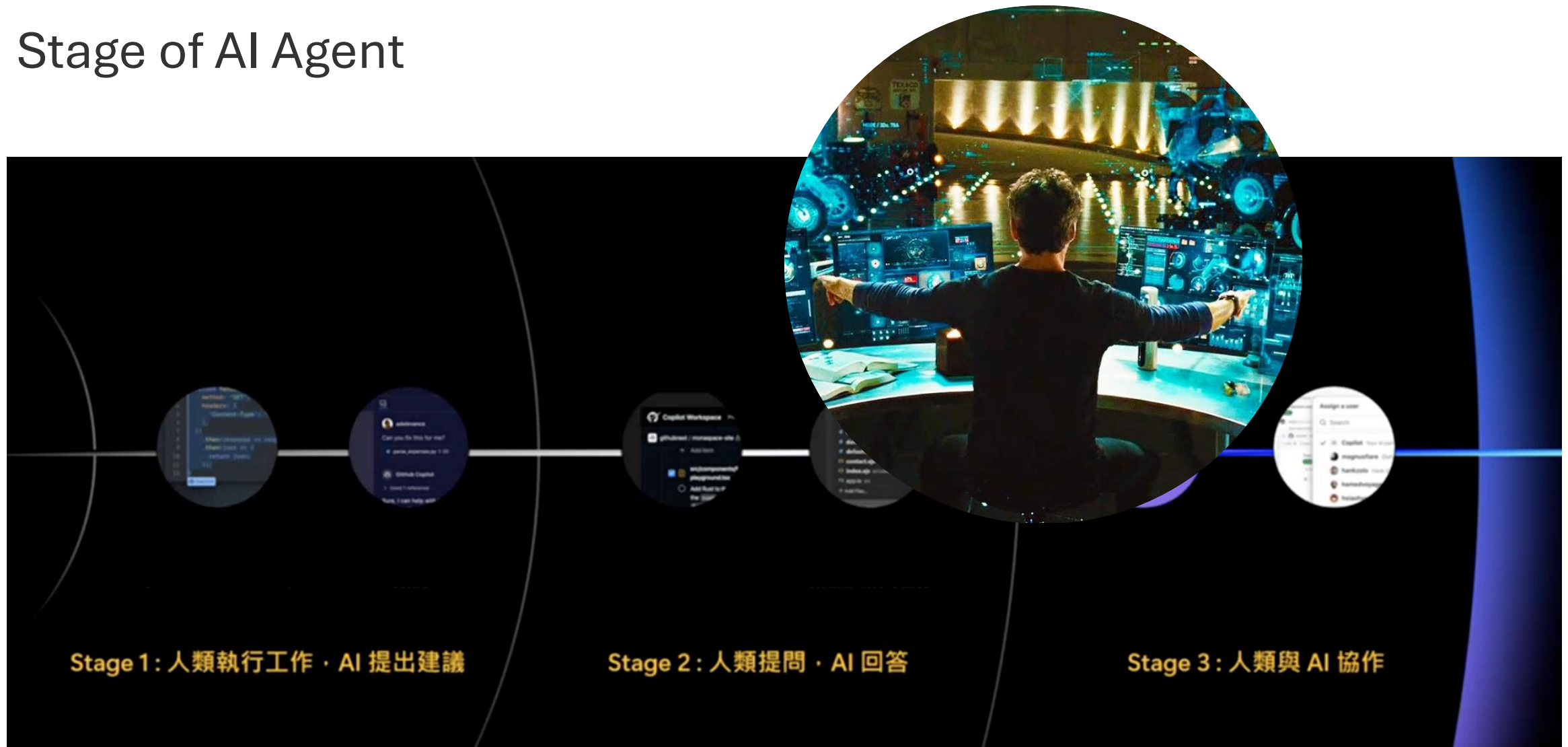
## MS SQL Server *from 1989 to 2025*



*from .com to AI*



## Stage of AI Agent



## Stage1 – 人類執行工作，AI 提出建議

LLM 為 DBA 的 AI 智慧助手，提高效率 and 減少人為錯誤。人類仍然是決策和執行的主體。

能協助 指令、知識理解和腳本生成

DBA 使用自然語言描述需求（如：「幫我寫一個備份資料庫的腳本」、「如何找出最耗時的十個查詢？」），AI 生成對應的 Shell Script 或 SQL 腳本。

## Stage2 – 人類提問，AI 回答

AI 的角色從一個被動的建議者，轉變為主動的分析師。

能協助整合、分析大量監控數據和日誌，回答複雜問題，提供深入的洞察。

DBA 提交一個緩慢查詢（ Slow Query ）， AI Agent 分析執行計畫（ Execution Plan ）、檢查索引使用情況、評估表格統計數據，並用易於理解的語言解釋瓶頸所在（如：「查詢未使用索引導致了全表掃描」），同時提出具體的優化建議（如：「在 [Posts].[OwnerId] 欄位上建立非叢集索引」）。

DBA 提問：「我的資料庫設定是否存在安全風險？」， AI Agent 掃描權限設定、網路配置、密碼策略等，並生成一份詳細報告與修補建議。

## Stage3 – 人類與 AI 協作

AI 成為自主行動的「資料庫代理」。人類 DBA 的角色轉變為監督者和策略制定者。

能交付高階的維運目標，由 AI 規劃複雜任務並執行。

DBA 只需設定目標（如：「將 top 10 緩慢查詢效能提升 20%」）。AI Agent 會持續分析查詢負載，自動改寫語法、測試、優化索引。所有操作都在人類監督下，並可設定自動執行或需要批准。

AI Agent 能預測未來的儲存和負載增長趨勢，並主動發出警示（如：「預計三週後磁碟空間將耗盡」）。當偵測到異常，能自動執行預先定義的修復流程，解決問題後再通知 DBA。人類只需介入處理更複雜或前所未見的故障。

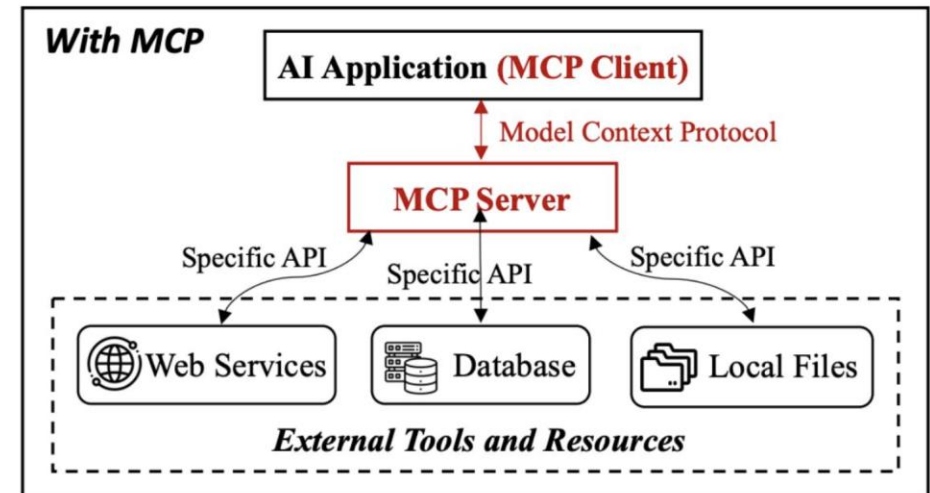
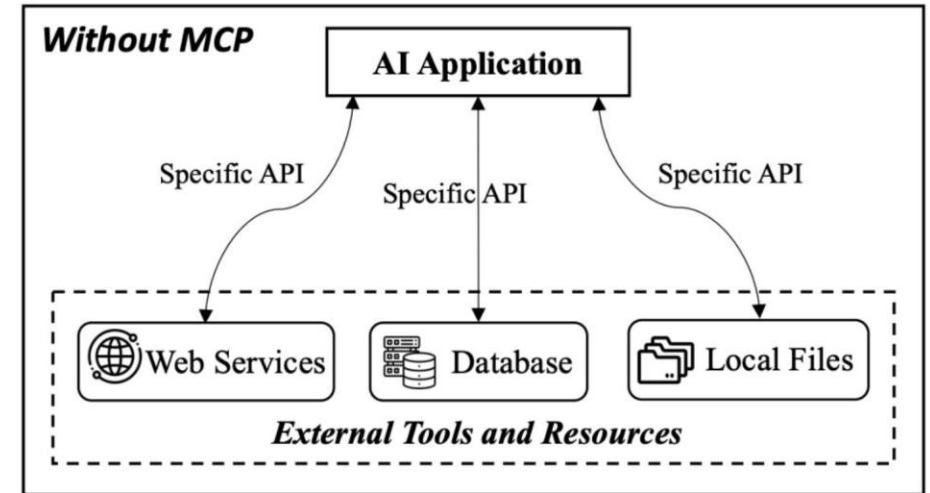
# Agenda

- MCP 與資料庫 Agent 的整合架構介紹
- SQL Server 常見維運任務與痛點分析
- 自然語言驅動的異常診斷與建議回應機制
- 如何讓 AI 協助你找出資料庫瓶頸
- 接下來的機會與挑戰
  - 安全合規
  - 工具擴充
  - .....

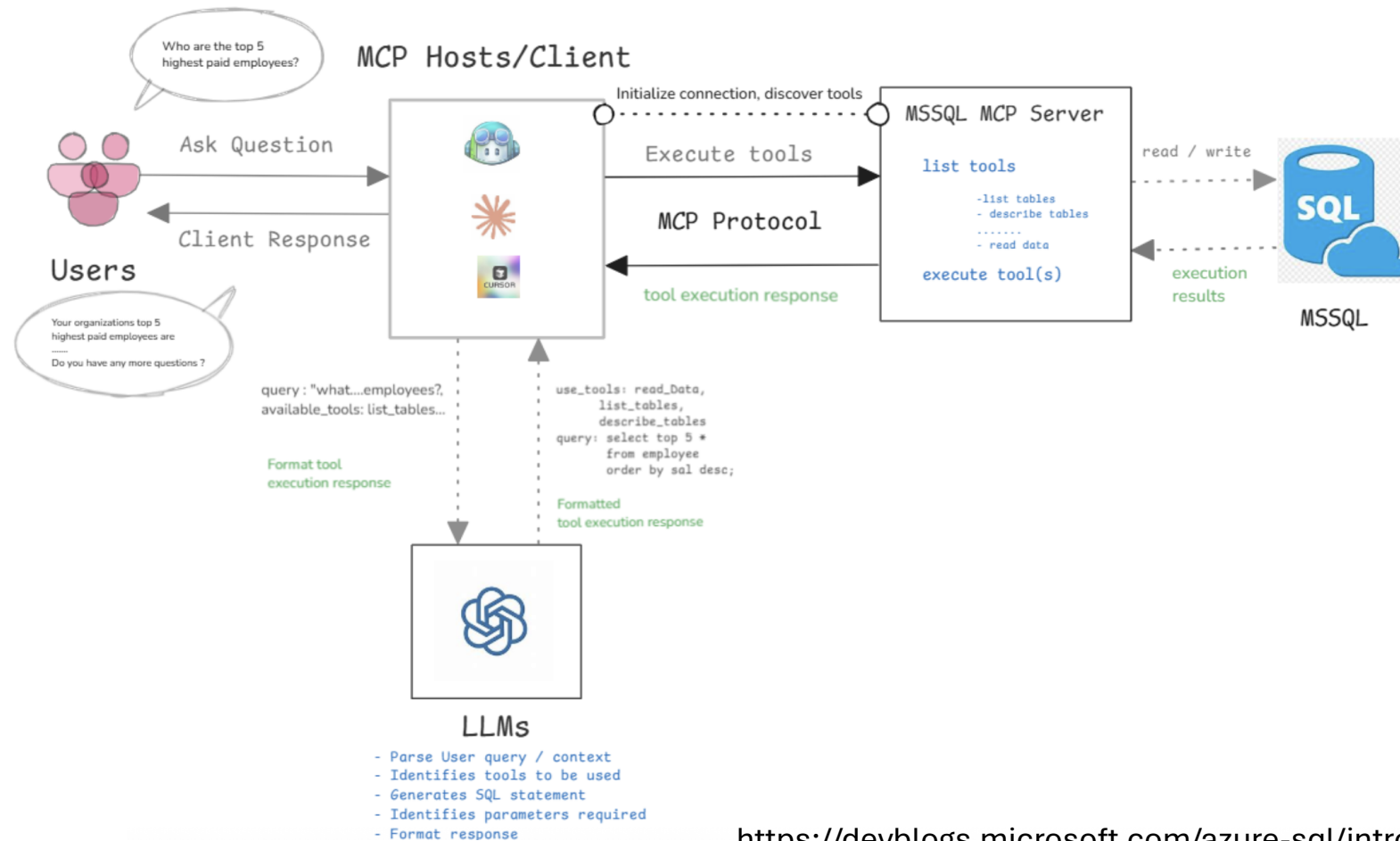
# MCP

MCP (Model Context Protocol) 是一個開放的標準，旨在讓大型語言模型 ( LLM ) 能透過標準化的方式與外部資料、工具和服務進行互動。

讓模型能存取資料、工具、API、資料庫等外部資源，但又不暴露機密或產生安全風險。



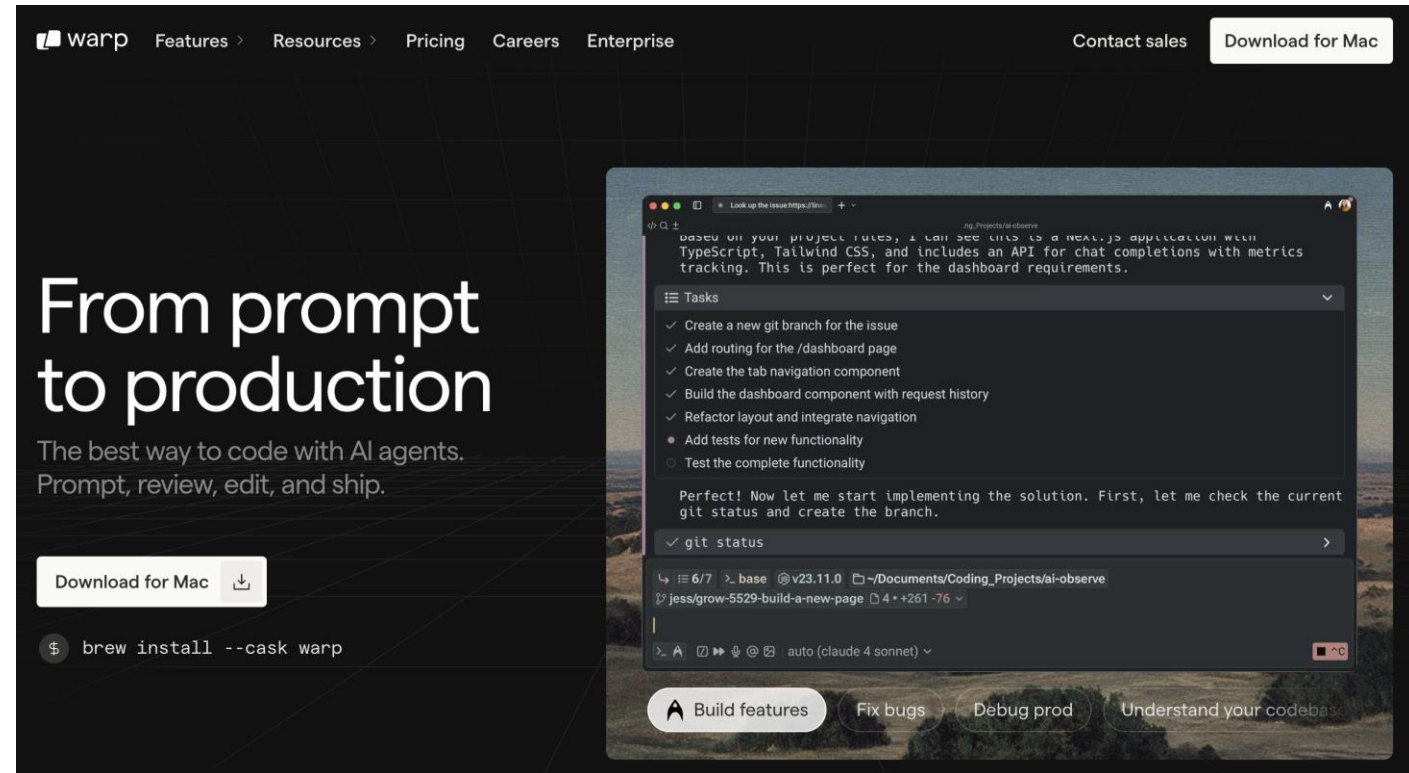
# MSSQL MCP Server AI-Agent Action Gateway



# MCP Client

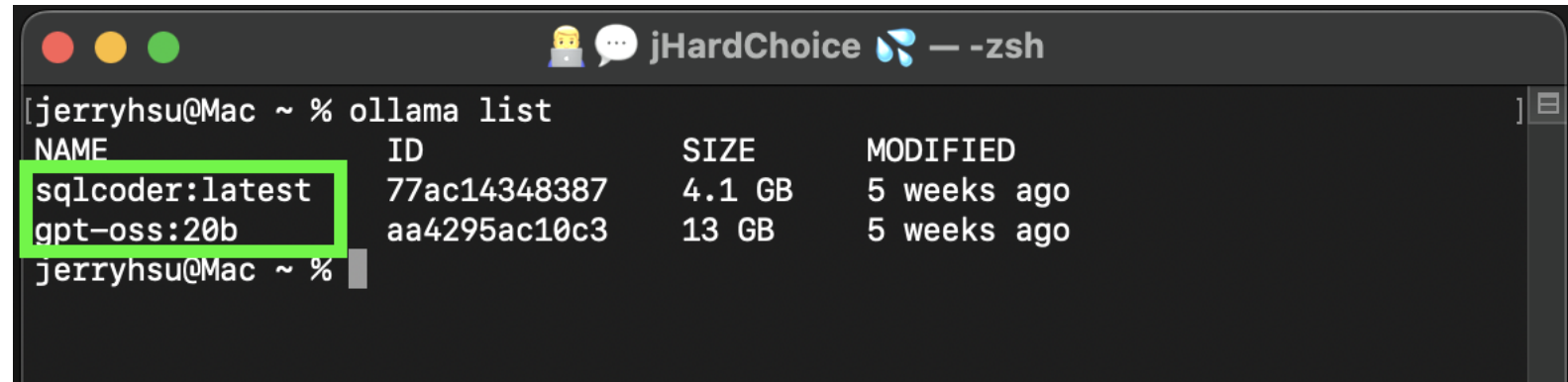
## Warp AI based terminal

- 能於 terminal 內詢問指令用法、錯誤原因或腳本建議。類似 Amazon Q
- 「自然語言 → 指令」並執行
- 支援 MCP
- ...



# LLM

透過 Ollama 執行本地端模型



```
jerryhsu@Mac ~ % ollama list
NAME                ID                SIZE      MODIFIED
sqlcoder:latest     77ac14348387     4.1 GB    5 weeks ago
gpt-oss:20b         aa4295ac10c3     13 GB     5 weeks ago
jerryhsu@Mac ~ %
```

模型選用

- gpt-oss-20b 實現了在消費級硬體上運行企業級推理能力。僅需 16GB VRAM 即可運行。
- gpt-oss-120b 接近頂級閉源模型性能。需至少 80GB VRAM 如 H100。
- SQLCoder 適合自然語言生成 SQL 查詢，能處理 Text-to-SQL 任務。(7b / 15b / 34b / 70b)

# MCP Server

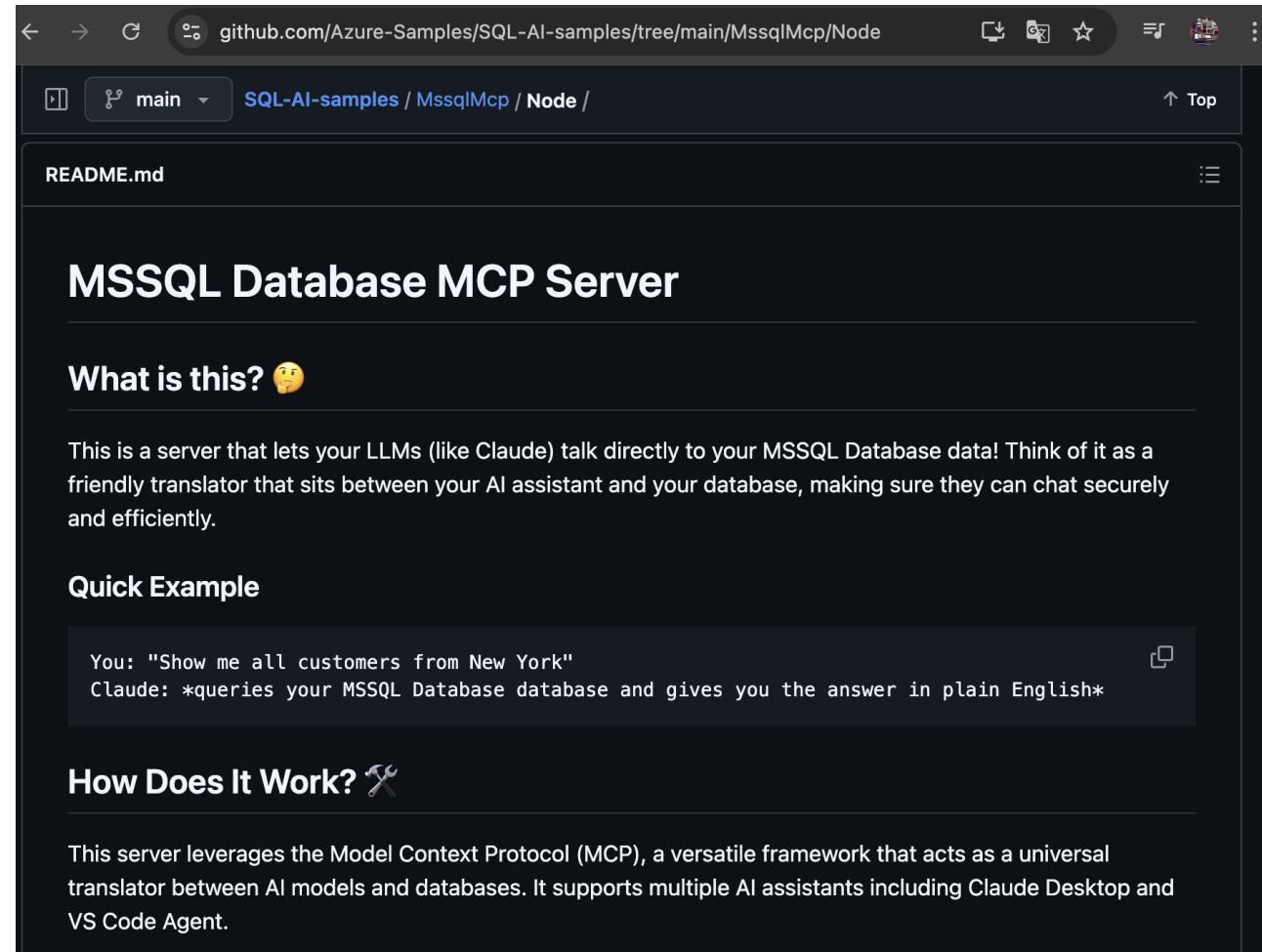
<https://github.com/Azure-Samples/SQL-AI-samples/tree/main/MssqlMcp/Node>

Authentication ( 身分驗證 )

確認「誰」在呼叫這個 MCP server

Authorization ( 授權 )

限制「可以做什麼」



<https://devblogs.microsoft.com/azure-sql/introducing-mssql-mcp-server/>

# MCP Server git repo 安全審查

## 使用 Visual Studio GitHub Copilot 分析

[Prompt] 我正在審查這個開源專案的程式碼庫。請作為一名資深安全分析師，幫我進行安全審查。審查重點：

- 惡意混淆 (Malicious Obfuscation)：特別關注任何看起來可疑、難以理解或有潛在惡意行為的程式碼段。
  - 資料竊取 (Data Exfiltration)：檢查是否有不當的外部連線、未經加密的資料傳輸，或對敏感資料 (如 API Key, PII, session token) 的處理不當。
  - 注入類漏洞 (如 SQLi, XSS, Command Injection)：是否有未經淨化的使用者輸入？
  - 身份驗證或授權缺陷：是否有不安全的認證/授權邏輯，可能導致權限提升或資料存取違規？
- 請將你的發現與 OWASP Top 10 對照。於每個潛在的安全問題，請：  
指出受影響的程式碼位置 (如果可能)。  
建議符合安全最佳實踐的修復方案。

CHAT

✓ Todos (4/5)

✓ Create scanning plan

✓ Search codebase for risky patterns

✓ Inspect flagged files

✓ Map findings to OWASP Top 10 2025

○ Produce final report

### 對應 OWASP Top 10 2025 (對照說明)

以下是本次發現與 OWASP Top 10 的對應 (以常見/通用 OWASP 分類來映射)：

- Injection (SQLi) — 主要問題：字符串拼接的 table/column/where/order；`InsertDataTool`，`DBA_InsertDataTool`，`ReadDataTool` (SQL 注入)
- Broken Access Control — 主要問題：`CallToolRequest` 未做完善授權、`ListToolsRequest` 在 read-only 下仍列出寫入工具
- Sensitive Data Exposure / Cryptographic Failures — 主要問題：`options.encrypt=false`、將 query/結果直接寫入日誌或回傳、使用 environment variables 保存密碼而無 secret store
- Security Misconfiguration — 主要問題：過度資訊回傳 (stack traces)、日誌未遮罩、缺乏 auth layer
- Insufficient Logging & Monitoring — 主要問題：缺結構化審計 (需記錄誰做了什麼)、容易漏報惡意行為
- (如果 OWASP 2025 有 "Excessive Data Exposure" 或 "Denial of Service" 類別) — 大型查詢與回傳可能造成資源耗盡與大量資料外洩

(備註：我使用的是 OWASP 分類的常見主題來對應本次發現；如果你希望我把每一項精確映射到 OWASP Top 10 2025 的確切編號與標題，我可以依你給的 OWASP 2025 官方列表做逐項對應。)

### 其他建議 (工具與流程)

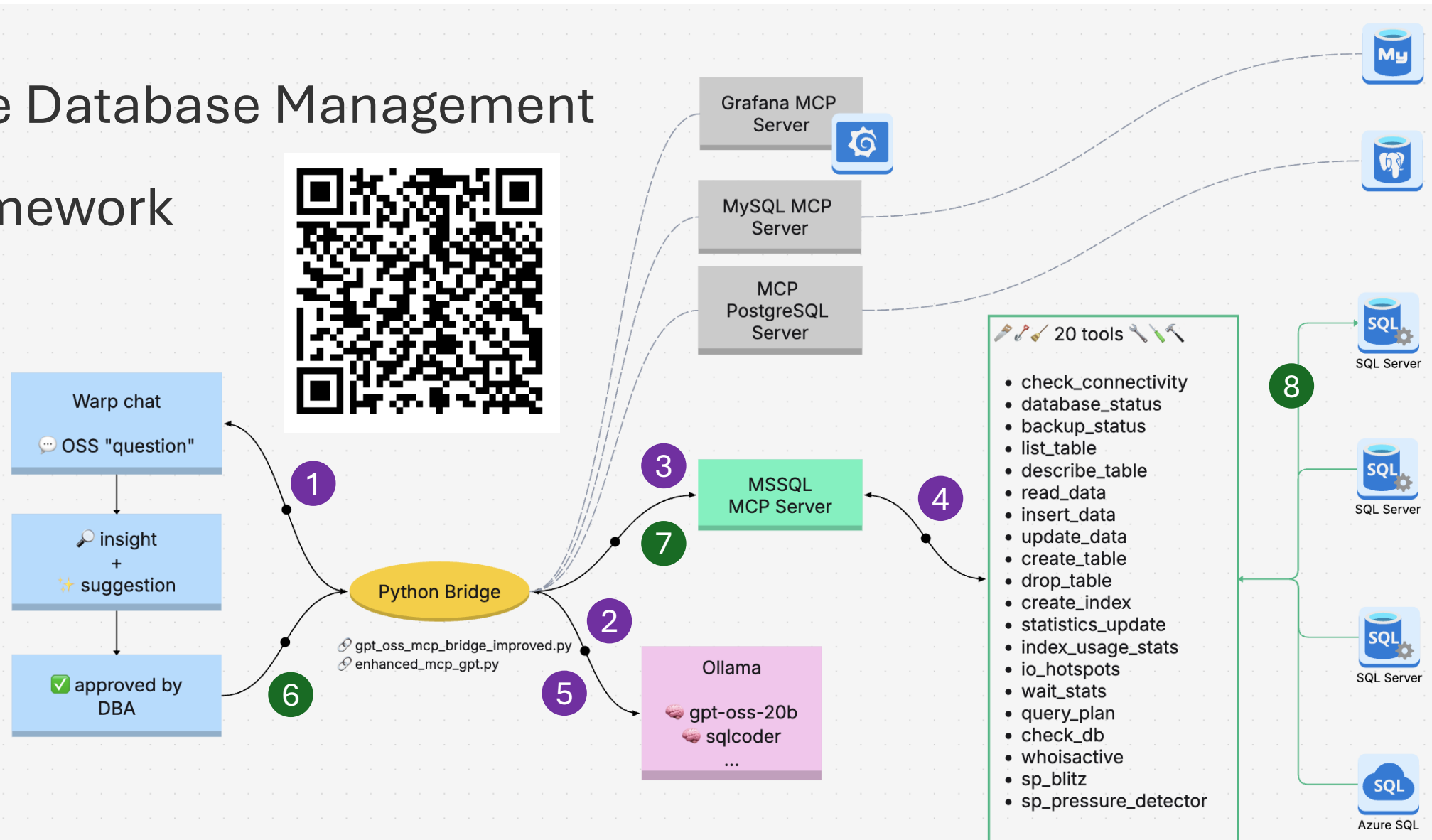
- 在 CI 中加入自動化安全掃描：
  - 靜態分析 (ESLint + security plugin)、npm audit、Snyk 或 Dependabot。
  - SAST (例如 semgrep 規則套用檢查 raw SQL 拼接與 process.env 洩露)。
- 在生產環境啟用集中化日誌與警示 (例如：失常查詢率、外部 IP 存取、嘗試執行寫工具)。

`package-lock.json`

Add context (#), extensions (@), commands (!)

Agent GPT-5 mini

# vibe Database Management framework



## Python bridge layer?

USER:

I would like to use Ollama GPT-OSS from Warp

AGENT:

I understand you'd like to use Ollama to run open-source LLMs locally. Let me help you set this up on your macOS system.

...

...

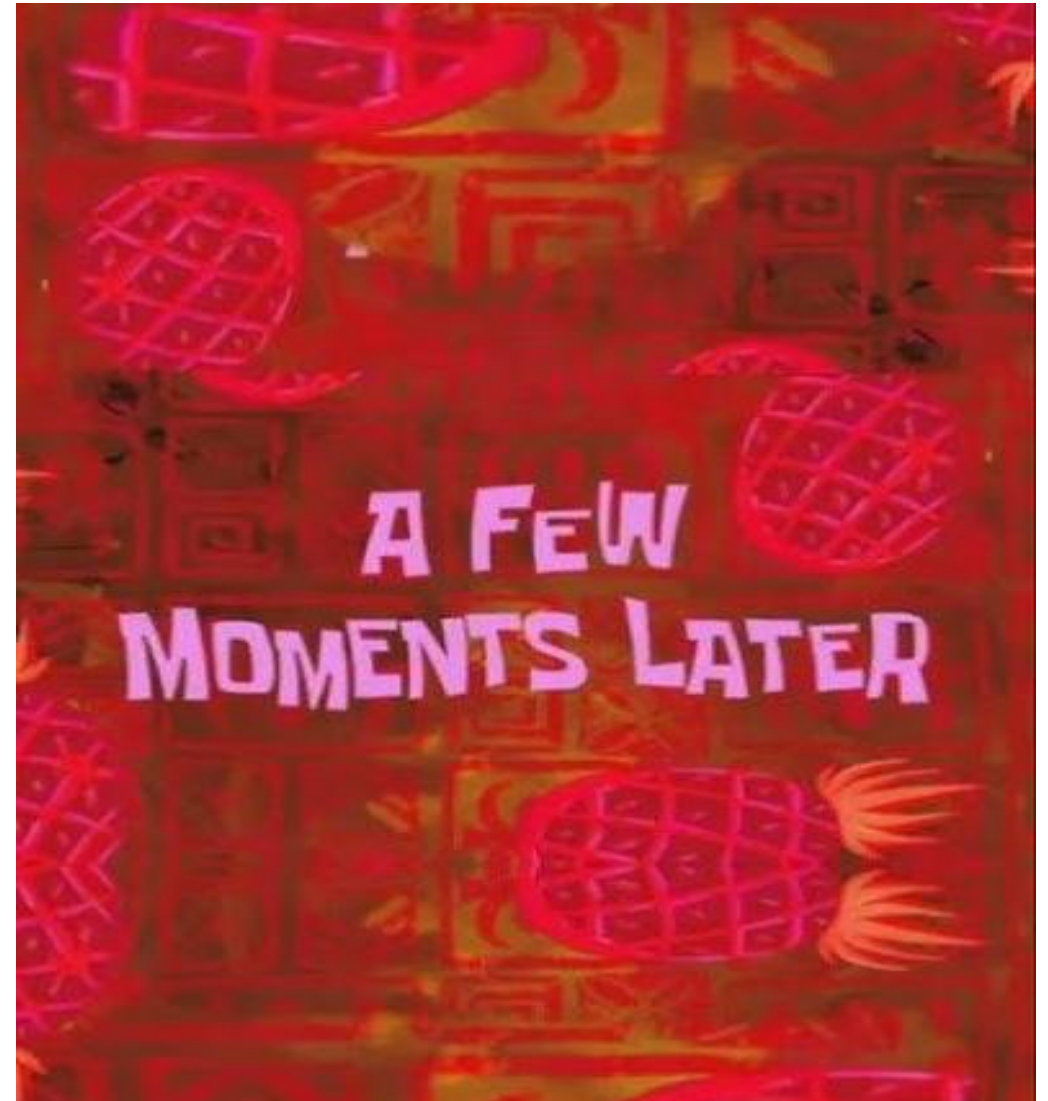
...

USER:

yes plz show me how to integrate into Warp

AGENT:

Great question! Let me show you several ways to integrate Ollama's GPT-OSS model with Warp terminal for a seamless AI-powered workflow.



## SQL Server 2025 日誌摘要

是的，我可以讀取多種類型的日誌：

### 最近的錯誤和異常

- 錯誤 241 (嚴重度 16): 轉換失敗錯誤 - 多次出現
- 錯誤 2601 (嚴重度 14): 重複鍵錯誤
- 錯誤 37536 (嚴重度 16): 系統錯誤
- 錯誤 18456 (嚴重度 14): 登入失敗 - `mcp_client` 用戶不存在

### ✓ 數據庫狀態

- **StackOverflow** 數據庫在 `16:33:40` 成功附加
- 所有數據庫都使用 **SIMPLE** 恢復模式 (除了 `model` 使用 **FULL**)
- 事務日誌重用等待狀態：**NOTHING** (表示正常)

### 📊 可用的日誌類型

1. 錯誤日誌 - `sys.dm_os_ring_buffers` (異常記錄)
2. Docker 容器日誌 - `docker logs sql2025`
3. 數據庫事務日誌狀態 - `sys.databases`
4. 系統活動日誌 - 各種 DMV

🔧 如果您需要更詳細的日誌，可以使用：

```
1 -- 查看 SQL Server 錯誤日誌
2 EXEC xp_readerrorlog 0, 1, NULL, NULL, '2025-10-11', '2025-10-12'
3
4 -- 查看代理日誌
5 EXEC xp_readerrorlog 0, 2
```

Vibe: 檢查資料庫日誌

OSS 調用 MCP tool `read_data` 查詢

`sys.dm_os_ring_buffers`

`sys.dm_exec_requests`

`sys.databases`

`sp_readerrorlog`

讓我也檢查登入用戶到數據庫用戶的映射：

✓ MCP Tool: read\_data

## StackOverflow 數據庫的用戶權限摘要

### 數據庫用戶

用戶名稱	類型	預設架構
dbo	WINDOWS_USER	dbo
guest	SQL_USER	guest
INFORMATION_SCHEMA	SQL_USER	-
sys	SQL_USER	-

### 角色成員

角色	成員
db_owner	dbo

### 實際讀取權限

基於以上資訊，可以讀取 StackOverflow 數據庫的用戶：

1. **sa** (系統管理員) - 完全權限
2. **dbo** - 數據庫擁有者，完全權限
3. 任何具有 **sysadmin** 角色的伺服器登入 - 完全權限

如果您想給其他用戶讀取權限，可以使用以下 T-SQL：

```
1 -- 創建新用戶並給予讀取權限
2 USE StackOverflow;
3
4 -- 如果需要創建登入 (在 master 數據庫中)
5 -- CREATE LOGIN [用戶名] WITH PASSWORD = '密碼';
6
7 -- 創建數據庫用戶並給予讀取權限
8 CREATE USER [用戶名] FOR LOGIN [用戶名];
9 ALTER ROLE db_datareader ADD MEMBER [用戶名];
```

讓 SQL Server 聽你說話 - MCP 驅動的 AIOps

Vibe: 檢查使用者權限

OSS 調用 MCP tool read\_data 查詢

sys.database\_permissions

sys.database\_principals

sys.database\_role\_members

gpt 我有哪些資料庫

讓我檢查您的 SQL Server 2025 容器中有哪些數據庫：

✓ MCP Tool: read\_data >

您目前的 SQL Server 2025 容器中有以下數據庫：

### 目前的數據庫列表

數據庫名稱	ID	創建日期	排序規則
master	1	2003-04-08	SQL_Latin1_General_CP1_CI_AS
tempdb	2	2025-10-11	SQL_Latin1_General_CP1_CI_AS
model	3	2003-04-08	SQL_Latin1_General_CP1_CI_AS
msdb	4	2025-08-20	SQL_Latin1_General_CP1_CI_AS
Stackoverflow	5	2025-10-11	SQL_Latin1_General_CP1_CI_AS

看起來您已經有一個 **Stackoverflow** 數據庫了（剛創建於今天 16:33），所以您的附加操作可能已經成功了！

如果您想檢查 Stackoverflow 數據庫中有哪些表，可以使用這個 T-SQL：

```
1 -- 檢查 Stackoverflow 數據庫中的表
2 USE Stackoverflow;
3 SELECT
4     TABLE_SCHEMA,
5     TABLE_NAME,
6     TABLE_TYPE
7 FROM INFORMATION_SCHEMA.TABLES
8 ORDER BY TABLE_SCHEMA, TABLE_NAME;
```

sql



Vibe: 我有哪些資料庫

OSS 調用 MCP tool read\_data 查詢  
sys.databases

✓ MCP Tool: read\_data

## SQL Server 2025 連線狀況摘要

### 連線統計

- 總 **Sessions**: 76 個
- 使用者 **Sessions**: 7 個 (排除系統 sessions)
- 活躍連線: 7 個

### 按登入名稱分類

登入名稱	連線數量
sa	72
NT AUTHORITY\NETWORK SERVICE	3
NT AUTHORITY\SYSTEM	1

### 按應用程式分類 (使用者 Sessions)

應用程式	Sessions
azdata	2
node-mssql	1
SQLAgent - Contained AG	1
SQLAgent - Email Logger	1
SQLAgent - Generic Refresher	1
SQLServerCEIP	1

### 分析

1. 主要連線來源: sa 帳戶有 72 個連線 (大部分是系統內部連線)
2. 外部工具: azdata 和 node-mssql 是外部客戶端連線
3. 系統服務: SQL Agent 相關服務正在運行
4. 實際使用者連線: 大約 3-4 個真實的使用者連線 (azdata + node-mssql)

大部分連線都是 SQL Server 內部的系統連線，實際的外部用戶連線相對較少，這是正常的狀況。

Vibe: 目前資料庫有幾個連線？

OSS 調用 MCP tool read\_data 查詢

sp\_whoisactive

sys.dm\_exec\_sessions

sys.dm\_exec\_connections

✓ 是的！在過去一小時內有新用戶被建立

👤 新建立的用戶：SO\_rd001

伺服器層級登入：

- 名稱：SO\_rd001
- 類型：SQL Login
- 建立時間：2025-10-11 16:48:18 (約 1 分鐘前)
- 修改時間：2025-10-11 16:48:19

數據庫層級用戶：

- 名稱：SO\_rd001
- 類型：SQL User
- 建立時間：2025-10-11 16:48:37 (約 1 分鐘前)
- 數據庫：StackOverflow

🔑 權限設定

- 數據庫角色：db\_owner (StackOverflow 數據庫的擁有者)
- 伺服器角色：無特殊伺服器角色

📄 摘要

- 這個用戶剛剛在約 1 分鐘前被建立
- 具有 StackOverflow 數據庫的完整權限 (db\_owner)
- 是一個 SQL 登入用戶，不是 Windows 驗證用戶
- 用戶名稱 "SO\_rd001" 可能代表 "StackOverflow read 001" 或類似的命名慣例

這個用戶看起來是專門為存取 StackOverflow 數據庫而建立的，具有該數據庫的完整權限。

Vibe: 這一個小時有使用者被建立嗎？

OSS 調用 MCP tool read\_data 查詢

sys.server\_principals

sys.database\_principals

sys.dm\_exec\_connections

讓我檢查近期的登入相關日誌：

```
✓ docker logs --since "2025-10-11T16:48:00" sql2025 >
```

## ✗ S0\_rd001 用戶還沒有登入過

### 📊 檢查結果摘要

1. 目前連線狀態：
  - S0\_rd001 目前沒有活躍的 session (0 個)
  - S0\_rd001 目前沒有活躍的連線 (0 個)
2. 用戶狀態：
  - 用戶已建立且啟用 (`is_disabled = false`)
  - 建立時間: `2025-10-11 16:48:18` (約 4 分鐘前)
3. 日誌檢查：
  - 在容器日誌中沒有找到 S0\_rd001 的登入嘗試記錄
  - 日誌顯示的都是 `mcp_client` 的登入失敗，沒有 S0\_rd001 相關記錄

### 🔍 結論

S0\_rd001 用戶雖然已經被建立並且擁有 StackOverflow 數據庫的完整權限 (`db_owner`)，但是：

- 已建立 - 4 分鐘前建立
- 已啟用 - 可以登入
- 有權限 - `db_owner` 角色
- 未登入 - 從未嘗試過登入

這個用戶可能是為了後續使用而預先建立的，目前還沒有被實際使用過。

Vibe: 那他有登入過嗎？

OSS 調用 MCP tool `read_data` 查詢

`sys.dm_exec_sessions`

`sys.dm_exec_connections`

`sys.sql_logins`

Run Cancel Disconnect Change Database: StackOverflow Estimated Plan

Enable Actual Plan Parse

```

1 use StackOverflow
2
3 select * from Posts

```

# 讓 SQL Server 聽你說話 - MCP 驅動的 AIOps

Results Messages

	Id	AcceptedA...	AnswerCou...	Body	ClosedDate	Commei
1	4	7	13	<p>I want to ...	NULL	1
2	6	31	5	<p>I have an ...	NULL	0
3	7	0	0	<p>An explici...	NULL	0
4	9	1404	64	<p>Given a <c...	NULL	7
5	11	1248	35	<p>Given a sp...	NULL	3
6	12	0	0	<p>Here's how...	NULL	11
7	13	0	25	<p>Is there a...	NULL	6
8	14	0	10	<p>What is th...	NULL	3
9	16	12446	6	<p>How do you...	NULL	0
1...	17	26	10	<p>How do I s...	NULL	3
1...	18	0	0	<p>For a tabl...	NULL	2
1...	19	531	23	<p>I'm lookin...	NULL	16
1...	21	0	0	<p>Many years...	NULL	1
1...	22	0	0	<p>The best w...	NULL	0
1...	24	49	6	<p>If I have ...	NULL	0
1...	25	1443907	9	<p>I'm having...	NULL	0
1...	26	0	0	<p>The answer...	NULL	0
1...	27	0	0	<p>@jeff</p>...	NULL	0
1...	29	0	0	<p>There are ...	NULL	4
2...	30	0	0	<p>I've had n...	NULL	0
2...	31	0	0	<p>The parent...	NULL	0
2...	33	0	0	<p><code>Math...	NULL	4
2...	34	0	8	<p>How do I f...	NULL	0

製造全表掃描慢查詢

select \* from Posts

返回 3,729,195 rows

耗時約 30 秒

基於我收集到的診斷信息，我來為你總結目前資料庫是否有緩慢查詢的狀況：

## 查詢性能分析結果

### 發現緩慢查詢

是的，你的資料庫確實有緩慢的查詢問題。 以下是主要發現：

#### 問題查詢排行榜

1. 最緩慢的查詢 - `SELECT * FROM Posts`
  - 平均 CPU 時間：24.3 秒 (24,298,164 微秒)
  - 平均執行時間：31.4 秒 (31,383,815 微秒)
  - 執行次數：5 次
  - 問題：這是一個全表掃描，讀取了 372 萬筆資料
2. 第二緩慢查詢 - 另一個 `SELECT * FROM Posts`
  - 平均 CPU 時間：21.6 秒
  - 平均執行時間：30.9 秒
  - 執行次數：1 次
3. 其他慢查詢
  - `COUNT(*)` 查詢：3.3 秒 CPU 時間
  - 複雜的系統查詢：0.4 秒 CPU 時間

#### 性能問題分析

主要問題：

- 全表掃描：Posts 表有 372 萬筆資料，執行 `SELECT *` 導致嚴重性能問題
- I/O 瓶頸：StackOverflow 資料庫檔案的讀取 I/O 延遲達 397,819 毫秒
- 缺少適當索引：查詢執行計畫顯示使用聚集索引掃描

Wait Stats 分析：

- 主要等待類型：`PWAIT_EXTENSIBILITY_CLEANUP_TASK` (99.74% 的等待時間)
- 這通常與擴展功能清理相關，不是性能瓶頸的主因

讓 SQL Server 聽你說話 - MCP 驅動的 AIOps

Vibe: 資料庫有緩慢的查詢嗎？

OSS 調用 MCP tool whoisactive

OSS 調用 MCP tool query\_plan

OSS 調用 MCP tool wait\_stats

OSS 調用 MCP tool sp\_pressure\_detector

# 🚀 SQL Server 查詢優化完整指南

基於診斷結果，我發現你的 Posts 表有 372 萬筆資料但只有主鍵索引，這正是性能問題的根源。以下是完整的優化策略：

## 📊 問題診斷總結

### 主要問題：

- Posts 表只有聚集索引（主鍵），缺乏其他索引
- `SELECT *` 查詢導致全表掃描
- 6.8GB 的表資料需要完整讀取
- I/O 延遲高達 397 秒

## 🎯 優化策略

### 1. 立即優化 - 查詢改寫

#### ❌ 避免這樣寫：

```
1 -- 最慢的查詢 (30+ 秒)
2 SELECT * FROM Posts;
```

sql



### 2. 建立關鍵索引

讓我為你建立最重要的索引來解決性能問題：

■ OK if I call this MCP tool?

Reject ^ C

Run ↻

```
MCP Tool: create_index ({"columns":
["PostTypeId", "CreationDate"], "includedColumns":
["Title", "Score", "ViewCount", "OwnerUserId"], "indexName": "IX_Posts_PostTypeId
_CreationDate", "isClustered": false, "isUnique": false, "schemaName": "dbo", "tbl
eName": "Posts"})
```

## 讓 SQL Server 聽你說話 - MCP 驅動的 AIOps

Vibe: 請說明怎麼優化？

OSS 調用 MCP tool describe\_table

OSS 調用 MCP tool index\_usage\_stats

OSS 調用 MCP tool statistics\_update

提供查詢改寫建議

更提議建立索引，詢問是否調用

MCP tool create\_index



MCP j.a.r.v.i.s demo

*Let's break some stuff. :P*

# Security concept - zero-trust policy

多因子驗證 ( MFA )

帳號最小原則 ( PoLP )

如：

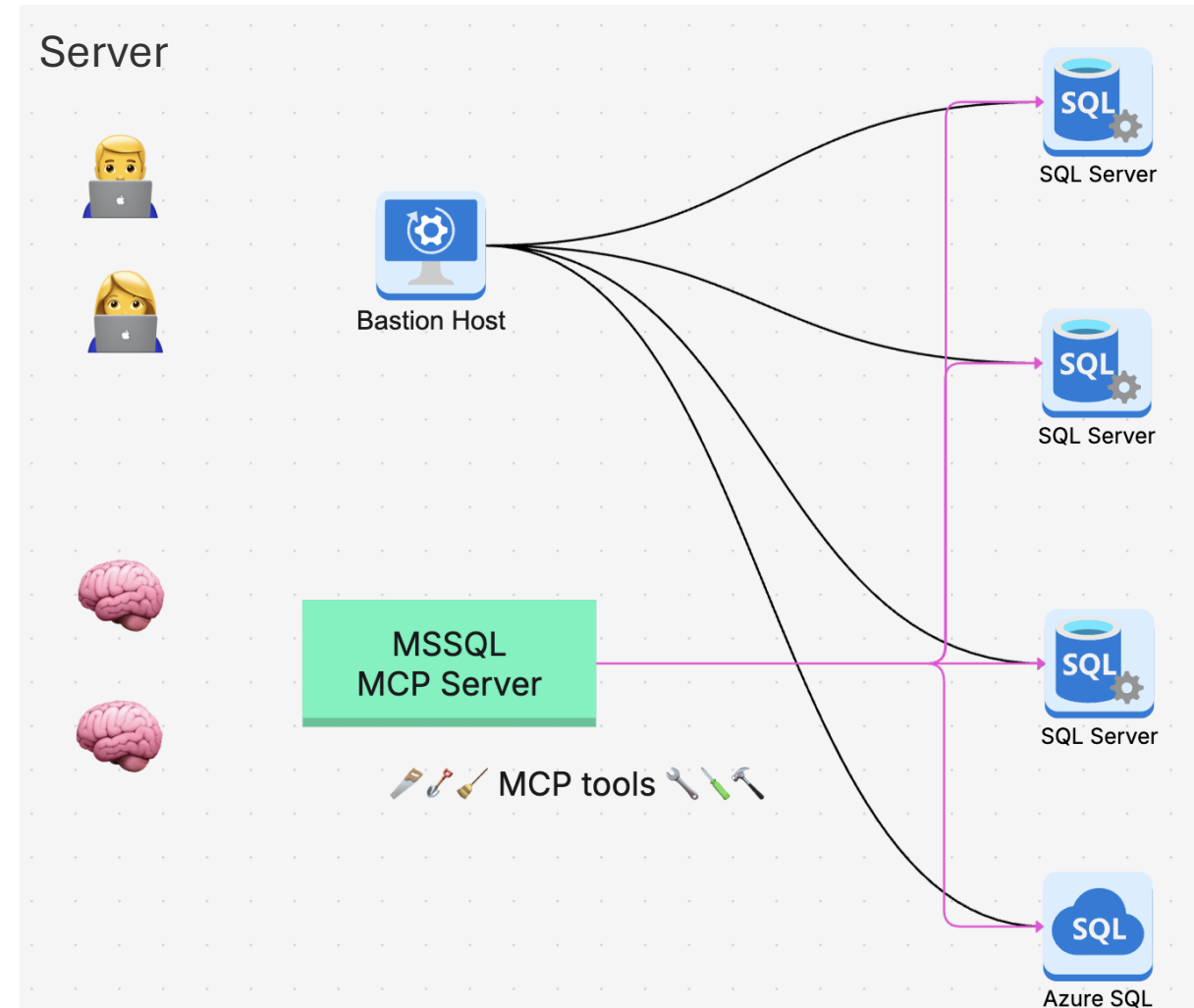
DBCC SHOW_STATISTICS	需要對目標資料表具有 <b>SELECT</b> 權限
DBCC SQLPERF(logspace)	需要 <b>VIEW SERVER STATE</b> 伺服器層級權限
DBCC INPUTBUFFER, OUTPUTBUFFER	需要 <b>VIEW SERVER STATE</b>

DB Auditing

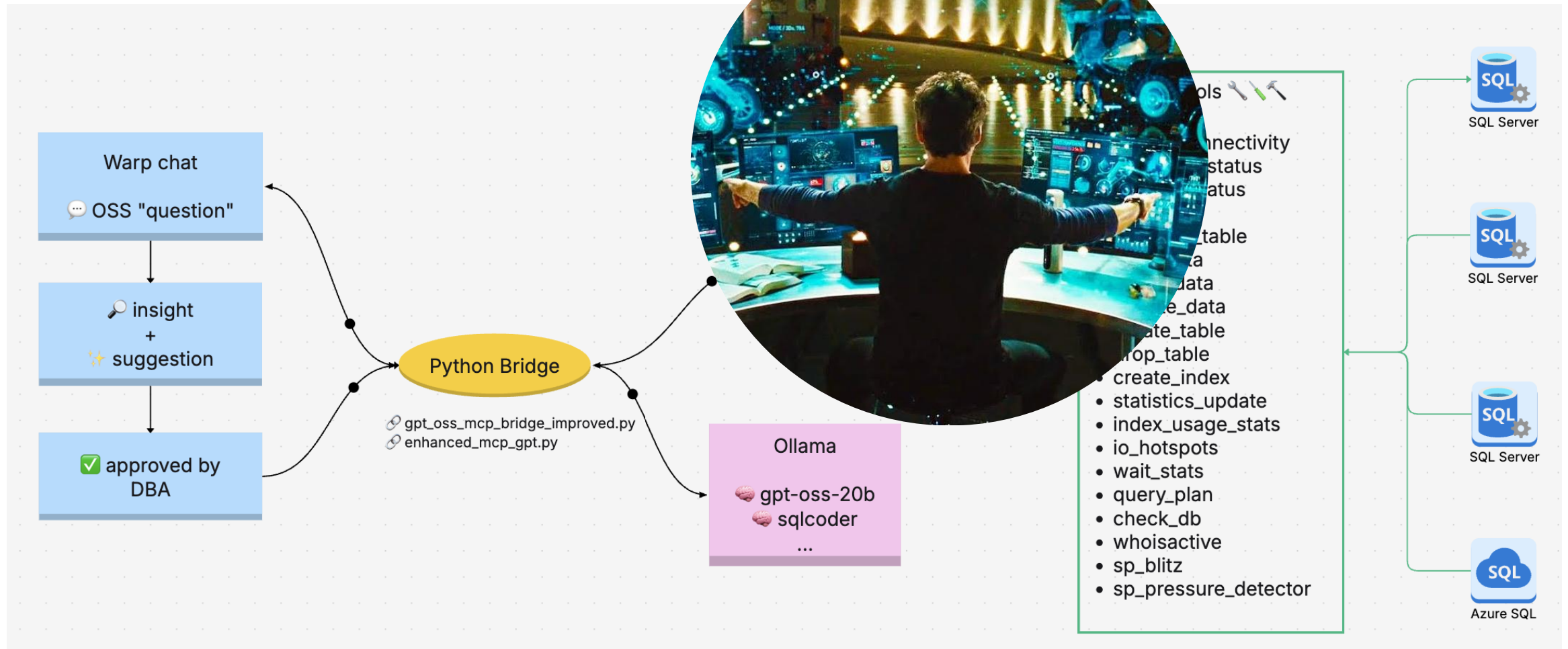
DB trace for MCP tools

IP Whitelist

## 💡 怎麼管 DBA 就怎麼管 MSSQL MCP



# Recap



## Weaknesses & Opportunities

相同的描述，LLM 可能會調用不同的 MCP tools

工具間的互補性

提示工程制定人設、tool SOP

MCP tool logging

## Next step for AI-Generation SQL DBA

### 擴大 MCP Server 群集

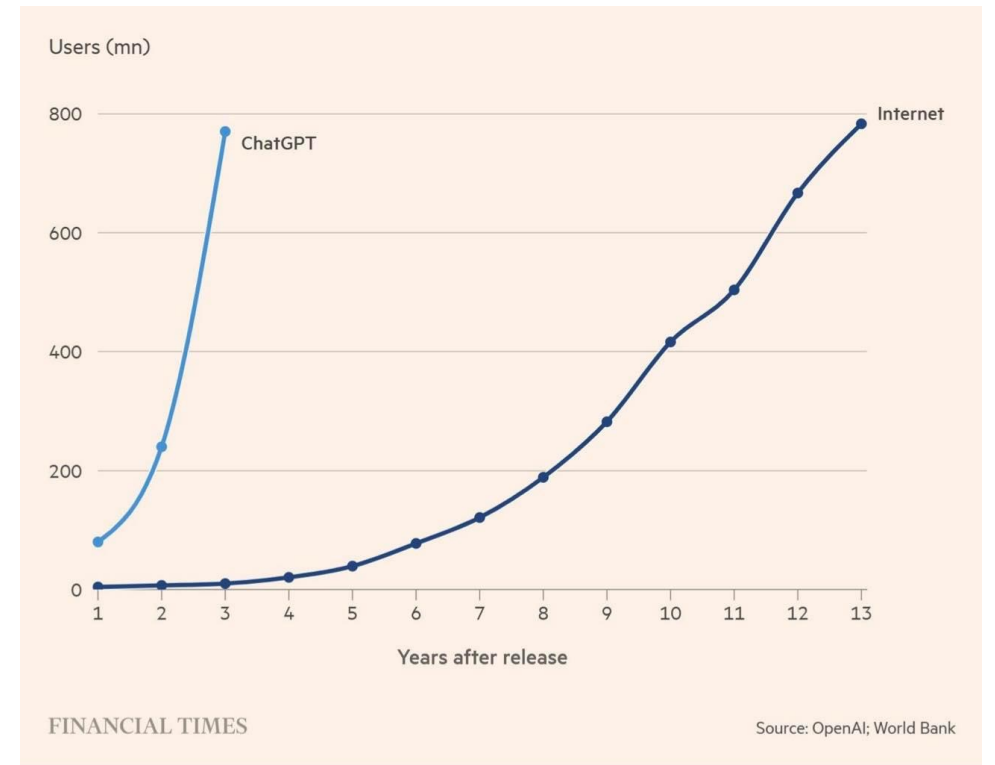
( 各類型資料庫、監控平台、Log平台 )

### 用工具建造更多工具

( index\_optimize, execution\_plan\_optimize, ha\_check,... )

### 用工具監管工具 ( Auditing MCP Server? )

### 用工具修復工具



1 年的 AI 時間，接近於 7 年的網路時間



**M**ay the SQL Server be with you

願 SQL Server 不僅聽你說話，也從此聽你的話

*Thank you for your time.*