第 15 章CHAPTER 15代理 AI 的使用者體驗UX for Agentic AI

如果我在結束書中涉及人工智慧設計模式的部分而不提及人工智慧代理，那我就失職了。OpenAI創始人Sam Altman最近在一篇部落格文章中表示：「我們相信，到2025年，我們可能會看到第一批AI代理『加入勞動力市場』，並實質性地改變公司的產出」（1）。許多人認為，人工智慧代理已經存在——只是分佈不均。然而，目前很少有例子表明與近乎未來主義的人工智慧化身互動的良好用戶體驗會是什麼樣子。幸運的是，在最近的 AWS re：Invent 大會上，我發現了一個很好的例子，說明與 AI
代理互動的使用者體驗可能是什麼樣子，我渴望在本章中與大家分享這一願景
（2）。但首先，人工智慧代理到底是什麼？

I would be remiss if I ended the part of the book that deals with AI design patterns without mentioning AI agents. Sam Altman, the founder of OpenAI, recently said in a blog post:“ We believe that, in 2025, we may see the first AI agents ‘ join the workforce ’ and materially change the output of companies ”(1). By many accounts, AI agents are already here—they are just not evenly distributed. However, few examples yet exist of what a good user experience of interacting with that near-futuristic incarnation of AI might look like. Fortunately, at the recent AWS re:Invent conference, I came upon an excellent example of what the UX of interacting with AI agents might look like, and I am eager to share that vision with you in this chapter (2). But first, what exactly are AI agents?

什麼是人工智慧代理？

What Are AI Agents?

想像一個蟻群。在典型的蟻群中，你有不同的螞蟻專長：工蟻、士兵、雄蜂、蟻后等。蟻群中的每隻螞蟻都有不同的工作;它們獨立運作，但作為一個有凝聚力的整體的一部分。你可以「僱用」一隻螞蟻（代理）來為你做一些簡單的半自主工作，這本身就很酷。然而，想像一下，您可以僱用整個蟻群來做一些更複雜或更有趣的事情：找出您的系統出了什麼問題，預訂您的旅行，或者.....幾乎可以做人類在電腦前能做的任何事情。每隻螞蟻本身都不是很聰明——相反，它們非常專業化來完成特定的工作。然而，綜合起來，螞蟻的不同專長呈現出一種我們與高階動物聯繫在一起的“ 集體智慧 ”。正如我們在書中使用的術語，“ 人工智能 ”與人工智能代理之間最顯著的區別是自主性。您無需向 AI
代理發出精確的指令或等待同步輸出——與一組 AI
代理的整個互動更加流暢和靈活，就像蟻群解決問題一樣。

Imagine an ant colony. In a typical ant colony, you have different specialties of ants: workers, soldiers, drones, queens, etc. Every ant in a colony has a different job; they operate independently yet as part of a cohesive whole. You can “ hire ” an individual ant (agent) to do some simple semi-autonomous job for you, which in itself is pretty cool. However, imagine that you can hire the entire ant colony to do something much more complex or interesting: Figure out what ’ s wrong with your system, book your trip, or … do pretty much anything a human can do in front of a computer. Each ant on their own is not very smart—they are instead highly specialized to do a particular job. However, put together, different specialties of ants present a kind of “ collective intelligence ” that we associate with higher-order animals. The most significant difference between “ AI, ” as we ’ ve been using the term in the book, and AI agents is autonomy. You don ’ t need to give an AI agent precise instructions or wait for synchronized output—the entire interaction with a set of AI agents is much more fluid and flexible, much like an ant colony would approach solving a problem.

人工智慧代理如何運作？

How Do AI Agents Work?

代理人工智慧可能以多種不同的方式運作——這是一個廣泛的主題，值得自己寫一本書（也許在一兩年內）。在本章中，我們將使用對系統問題進行故障排除的示例，作為涉及主管代理（也稱為“ 推理代理 ”）和一些工作代理的複雜流程的示例。當人工操作員收到有關問題的警報時，流程就會開始。他們展開調查，由主管代理領導的半自主人工智慧代理團隊幫助他們找到根本原因並就如何解決問題提出建議。讓我們在步驟圖中分解與 AI 代理互動的過程，如圖 15.1 所示。

There are many different ways that agentic AI might work—it ’ s an extensive topic worthy of its own book (perhaps in a year or two). In this chapter, we will use an example of troubleshooting a problem on a system as an example of a complex flow involving a supervisor agent (also called “ reasoning agent ”) and some worker agents. The flow starts when a human operator receives an alert about a problem. They launch an investigation, and a team of semi-autonomous AI agents led by a supervisor agent help them find the root cause and make recommendations about how to fix the problem. Let ’ s break down the process of interacting with AI agents in a step diagram, shown in Figure 15.1.

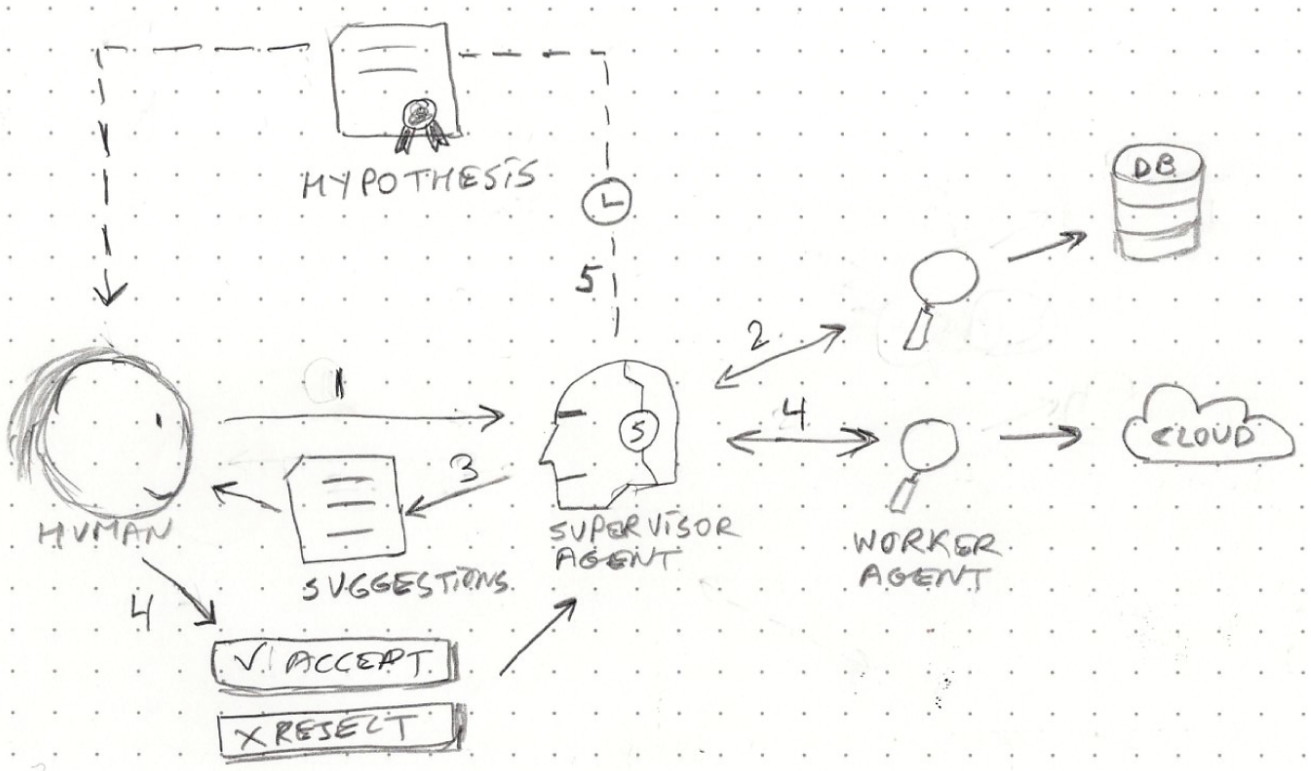

圖 15.1 多階段代理 AI 流程

Figure 15.1 Multistage agentic AI flow

多階段代理工作流程具有下列步驟：

A multistage agentic workflow has the following steps:

1. 人工操作員向主管 AI 代理發出一般請求。A human operator issues a general request to a supervisor AI agent.

2. 然後，主管 AI 代理啟動並向幾個專門的半自主工作 AI 代理發出一般請求，這些代理開始調查系統的各個部分（例如數據庫）以尋找根本原因。The supervisor AI agent then spins up and issues general requests to several specialized semi-autonomous worker AI agents that start investigating various parts of the system (e.g., a database) looking for the root cause.

3. Worker 代理程式會將發現項目帶回給主管代理程式，主管代理程式會將它們整理為人類操作員的建議。Worker agents bring back findings to the supervisor agent, which collates them as suggestions for the human operator.

4. 人工操作員接受或拒絕各種建議，這會導致主管代理啟動額外的工作人員進行調查（例如，雲端應用程式）。The human operator accepts or rejects various suggestions, which causes the supervisor agent to spin up additional workers to investigate (e.g., a cloud

application).

5. 經過幾個檢索週期後，主管代理會產生有關根本原因的假設，並將其交付給人工操作員。After several retrieval cycles, the supervisor agent produces a hypothesis about the root cause and delivers it to the human operator.

就像與典型的人類組織簽訂合約一樣，主管人工智慧代理擁有一支專門的人工智慧代理團隊可供使用。主管可以將訊息路由到其監督下的任何 AI Worker 代理程式，這些代理程式將執行任務並將結果傳達給主管。主管也可以選擇將任務指派給特定客服專員，並在稍後有更多資訊可用時傳送其他指示。最後，當任務完成時，輸出會傳回給使用者。然後，人類操作員可以選擇向監督的 AI
代理提供反饋或分配其他任務，在這種情況下，整個過程將重新開始 （3）。

Just like in the case of contracting a typical human organization, a supervisor AI agent has a team of specialized AI agents at their disposal. The supervisor can route a message to any of the AI worker agents under its supervision, which will do the task and communicate the results back to the supervisor. The supervisor may also choose to assign the task to a specific agent and send additional instructions later when more information becomes available. Finally, the output is communicated back to the user when the task is complete. A human operator then has the option to give feedback or assign additional tasks to the supervising AI agent, in which case the entire process begins again (3).

人類不需要擔心任何內部事情——所有這些都由主管半自主地處理。人類需要做的就是陳述一個一般性要求，然後審查這個代理“組織”的輸出並做出反應。如果你能做這樣的事情，這正是你與蟻群溝通的方式：你會把工作分配給蟻后，讓她管理所有的工蟻、士兵、無人機等來完成任務。就像在蟻群中一樣，個體專業代理不需要特別聰明或直接與人類操作員溝通——他們只需要能夠半自主地解決他們被設計為執行的專門任務，並能夠將精確的輸出傳遞回主管代理，僅此而已。主管代理人的工作是進行所有的推理和溝通。這種人工智慧模型對於許多任務來說更有效率、更便宜且非常實用。讓我們看看詳細的互動流程，以便更好地理解現實世界中的這種體驗。

The human does not need to worry about any internal stuff—all that is handled semi-autonomously by the supervisor. All the human needs to do is state a general request, then review and react to the output of this agentic“organization.”This is exactly how you would communicate with an ant colony if you could do such a thing: You would assign the job to the queen and have her manage all the workers, soldiers, drones, and the like to accomplish the task. And much like in the ant colony, the individual specialized agent does not need to be particularly smart or to communicate with

the human operator directly—they need only to be able to semi-autonomously solve the specialized task they are designed to perform and be able to pass precise output back to the supervisor agent, and nothing more. The supervisor agent ’ s job is to do all of the reasoning and communication. This AI model is more efficient, cheaper, and highly practical for many tasks. Let ’ s look at the detailed interaction flow to better understand this experience in the real world.

使用案例：使用 AI 代理程式進行 CloudWatch 調查

Use Case: CloudWatch Investigation with AI Agents

為簡單起見，我們將遵循本章前面的工作流程圖，流程中的每個步驟都與圖表中的步驟相符。此範例來自 AWS re：Invent 2024—Don't get stuck： How connected telemetry keep you moving forward （COP322），由 AWS Events on YouTube 提供，從 53 分鐘開始 （2）。

For simplicity, we will follow the workflow diagram earlier in the chapter, with each step in the flow matching that in the diagram. This example comes from AWS re:Invent 2024—Don ’ t get stuck: How connected telemetry keeps you moving forward (COP322), by AWS Events on YouTube, starting at 53 minutes (2).

步驟 1

Step 1

如圖 15.2 所示，當使用者發現名為「機器人服務」的服務（螢幕截圖左上角）中的故障急劇增加並啟動新的調查時，該過程就會開始。然後，使用者將所有相關資訊以及可能的其他指令傳遞給主管代理。

As shown in Figure 15.2, the process starts when the user finds a sharp increase in faults in a service called “ bot service ” (top left in the screenshot) and launches a new investigation. The user then passes all pertinent information and perhaps additional instructions to the supervisor agent.

步驟 2

Step 2

在步驟 2（圖 15.3）中，主管代理收到請求並產生一堆工作 AI 代理，他們將半自主地檢查系統的不同部分。該過程是非同步的，這意味著右側建議的初始狀態是空的;調查結果不會在調查啟動後立即得出。

In Step 2 (Figure 15.3), the supervisor agent receives the request and spawns a bunch of worker AI agents who will semi-autonomously examine different parts of the system. The process is asynchronous, meaning the initial state of suggestions on the right is empty; findings do not come immediately after the investigation is launched.

步驟 3

Step 3

現在，工作代理返回一些“ 建議觀察 ”， 主管會處理這些觀察並添加到屏幕右側的建議中（見圖 15.4）。請注意，螢幕的右側現在更寬，以便更輕鬆地閱讀代理建議。在此畫面中，不同的代理程式會建議兩個非常不同的觀察值：第一個專門用於服務指標，第二個專門用於追蹤。

Now, the worker agents return with some “ suggested observations ” that the supervisor processes and adds to the suggestions on the right side of the screen (see Figure 15.4). Note that the right side of the screen is now wider to allow for easier reading of the agentic suggestions. In this screen, two very different observations are suggested by different agents: the first specializing in service metrics and the second specializing in tracing.

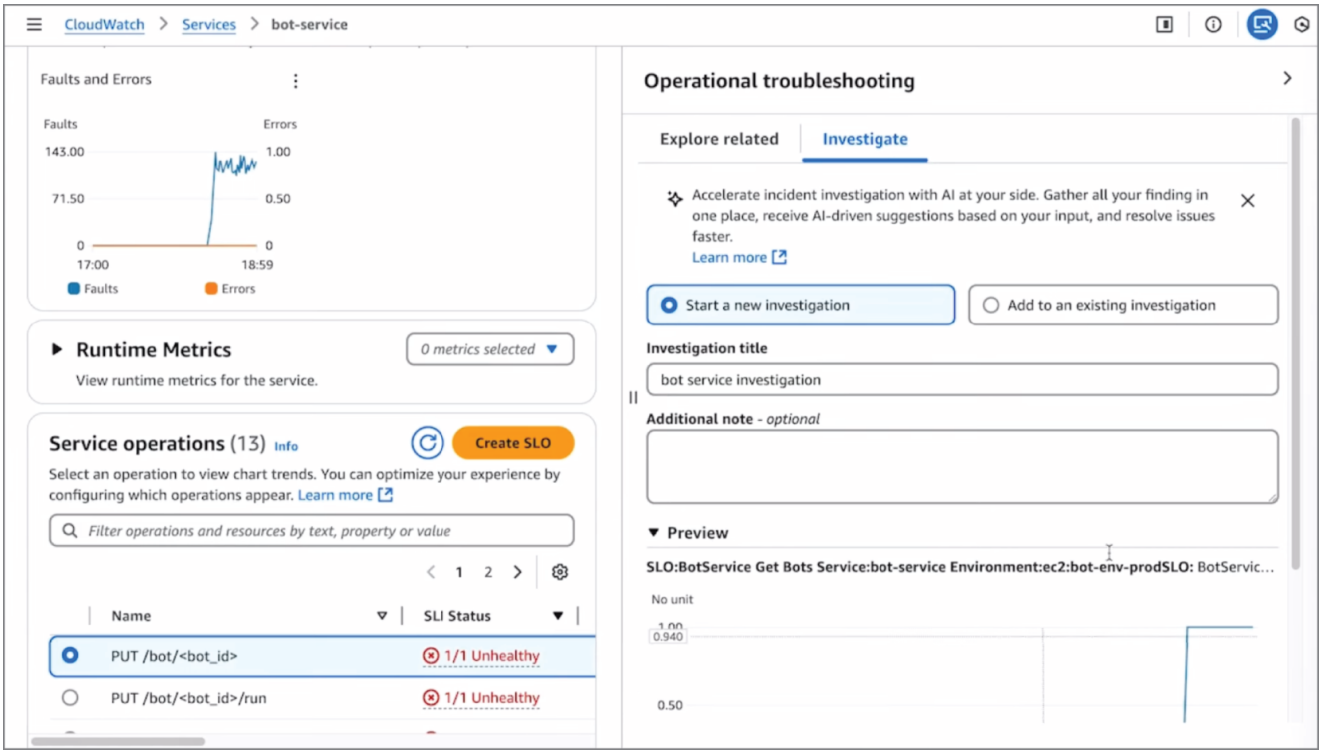

圖 15.2 第 1 步：人工操作員啟動新的調查

Figure 15.2 Step 1: The human operator launches a new investigation

來源：AWS 通過 YouTube （2）

Source: AWS via YouTube (2)

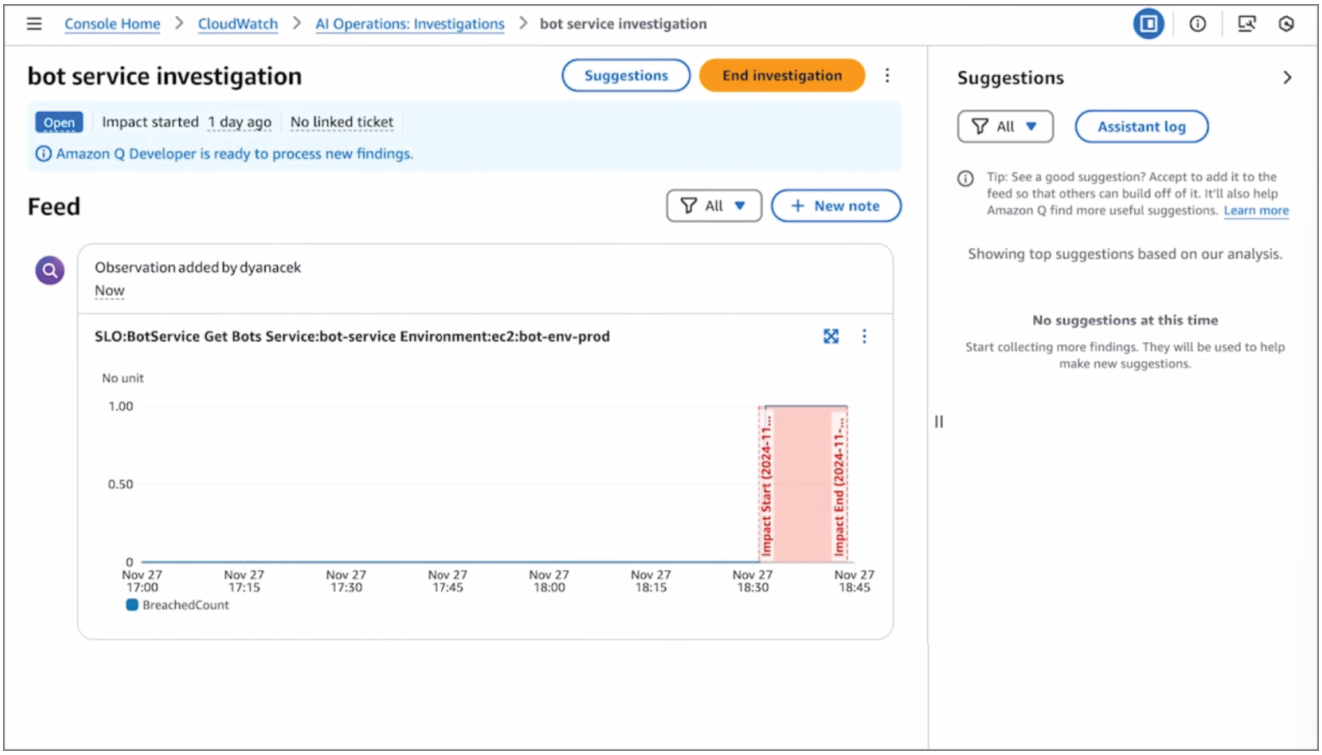

圖 15.3 步驟 2：主管代理啟動工作代理，需要時間才能報告

Figure 15.3 Step 2: The supervisor agent launches worker agents, which take time to report back

來源：AWS 通過 YouTube （2）

Source: AWS via YouTube (2)

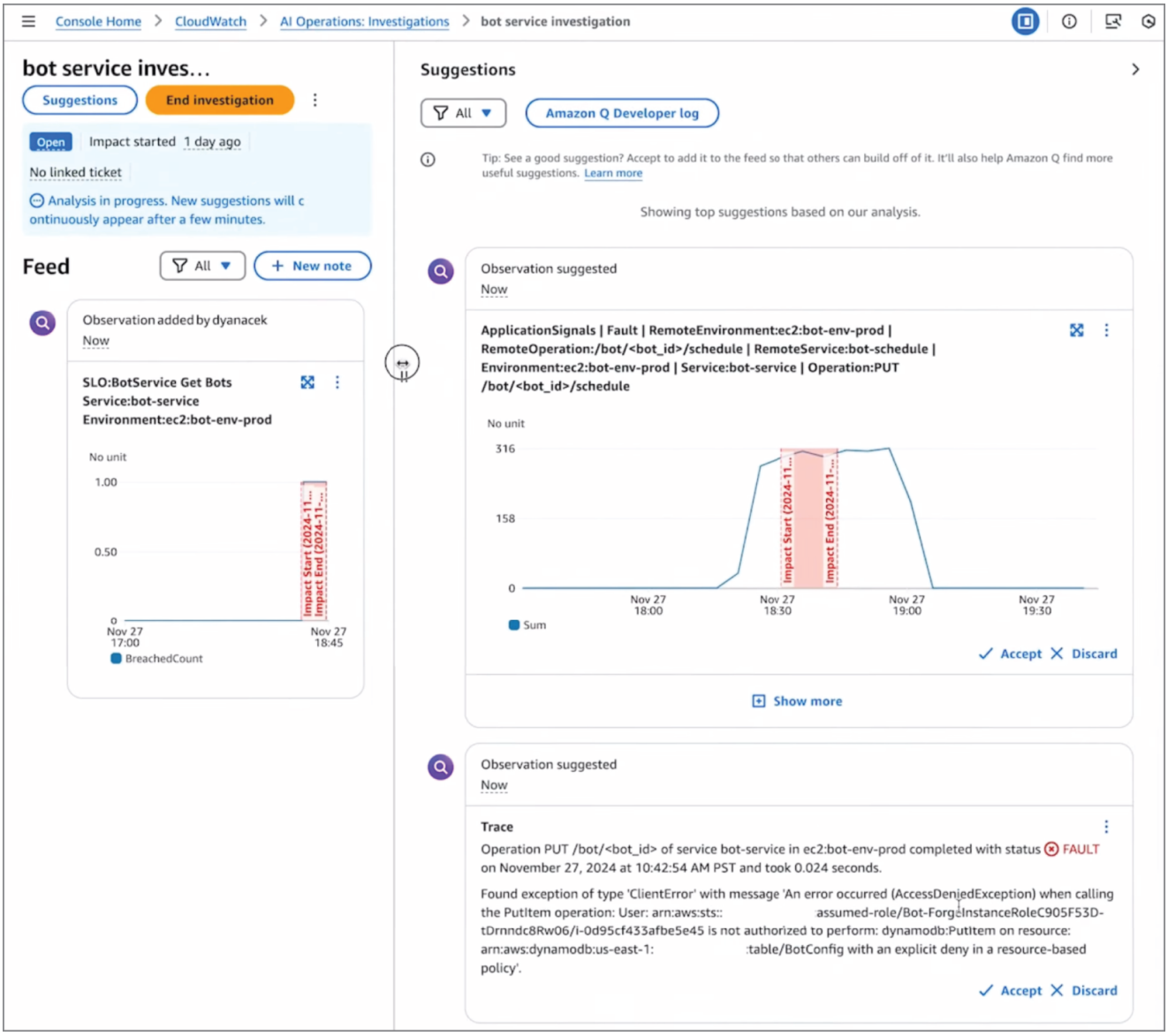

圖 15.4 步驟 3：工作代理返回有關系統問題的建議觀察結果

Figure 15.4 Step 3: Worker agents return with suggested observations concerning the system ’s problem

來源：AWS 通過 YouTube （2）

Source: AWS via YouTube (2)

這些「建議觀察」構成了調查的「證據」，旨在找到問題的根本原因。為了確定根本原因，此流程中的人工操作員透過指出哪些觀察最相關來幫助代理程式。因此，主管代理和人類並肩工作，共同確定問題的根本原因。

These “ suggested observations ” form the “ evidence ” in the investigation, which aims to find the root cause of the problem. To determine the root cause, the human operator in this flow helps the

agent by indicating which observations are most relevant. Thus, the supervisor agent and human work side by side to collaboratively determine the root cause of the problem.

步驟 4

Step 4

人工操作員通過單擊相關觀察結果上的“ 接受 ”來響應，這些觀察結果被添加到屏幕左側的調查“ 案例檔案 ”中，如圖 15.5 所示。現在，人工操作員已新增一些意見反應，以指出他們認為相關的資訊，代理程式程式將進入下一階段的調查。現在主管代理已收到用戶反饋，他們將停止發送“ 更多相同的內容 ”，而是在尋找根本原因時進行更深入的挖掘，並可能調查系統的不同方面。請注意，在圖 15.5
中，右側的新建議是不同的——這些建議現在正在查看日誌以尋找根本原因。

The human operator responds by clicking Accept on the relevant observations, which are added to the investigation “ case file ” on the left side of the screen, as shown in Figure 15.5. Now that the human operator has added some feedback to indicate the information they find relevant, the agentic process kicks in the next phase of the investigation. Now that the supervisor agent has received the user feedback, they will stop sending “ more of the same ” but instead will dig deeper and perhaps investigate a different aspect of the system as they search for the root cause. Note in Figure 15.5 that the new suggestions on the right are different—these are now looking at logs for a root cause.

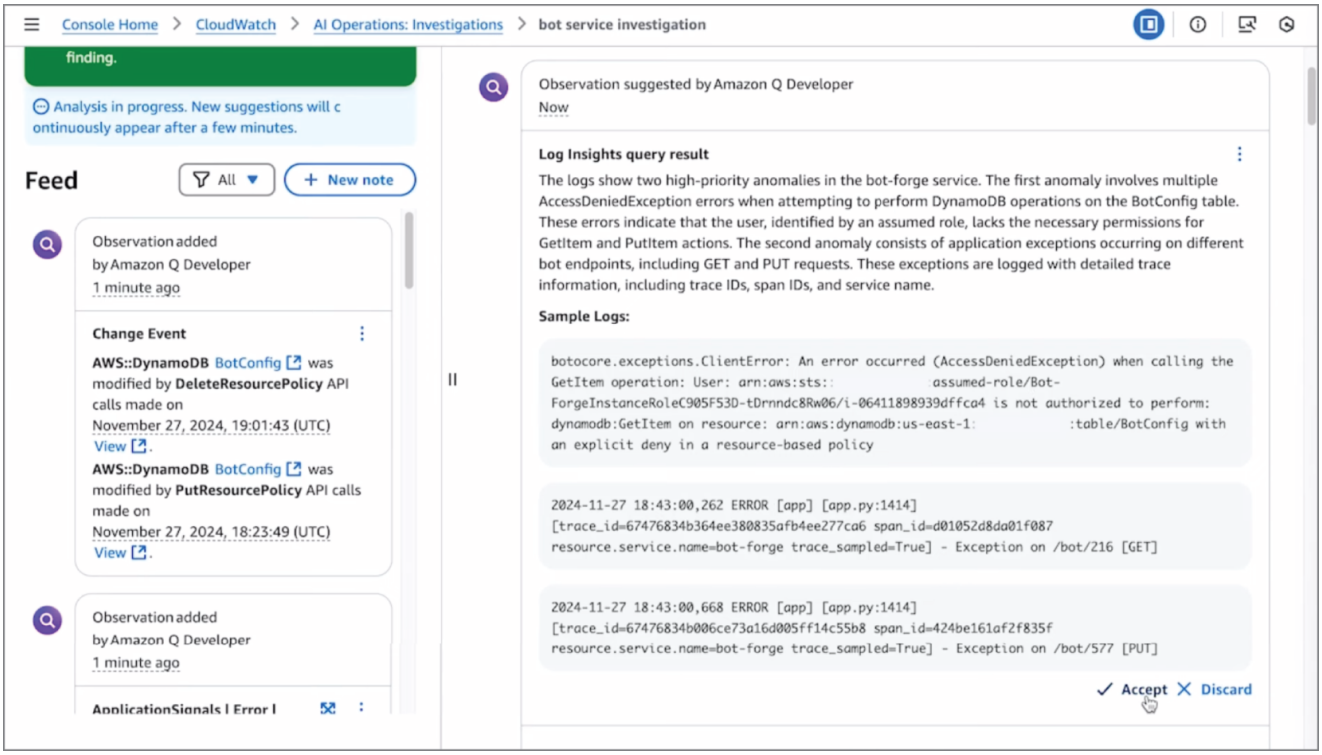

圖 15.5 第 4 步：收到使用者回饋後，客服人員進一步調查並提供不同的建議

Figure 15.5 Step 4: After receiving user feedback, the agents investigate further and offer different suggestions

來源：AWS 通過 YouTube （2）

Source: AWS via YouTube (2)

步驟 5

Step 5

最後，主管代理有足夠的資訊來確定問題的根本原因，因此它從證據收集切換到對根本原因的推理。在步驟 3 和 4 中，主管代理人提供了「建議的觀察」。現在，在第 5 步（圖 15.6）中，它已經準備好進行重大揭曉（如果你願意的話，“結局場景”），因此，就像文學偵探一樣，主管代理人會提供其“假設建議”。（這讓人想起“線索”遊戲，玩家輪流提出“建議”，然後，當他們準備撲上去時，他們會提出“指控”。主管代理在這裡也做同樣的事情！

Finally, the supervisor agent has enough information to take a stab at identifying the root cause of the problem, so it switches from evidence gathering to reasoning about the root cause. In steps 3 and 4, the supervisor agent provided“ suggested observations. ”Now, in step 5 (Figure 15.6), it is ready for a big reveal (the“ denouement scene, ”if you will) so, like a literary detective, the supervisor agent delivers its“ Hypothesis suggestion. ”(This is reminiscent of the game“ Clue ”where the players take turns making“ suggestions, ”and then, when they are ready to pounce, they make an“ accusation. ”The supervisor agent is doing the same thing here!)

建議的假設是正確的，當使用者按一下接受時，主管代理會提供解決問題的後續步驟和防止未來出現類似問題的建議（圖15.7）。代理人幾乎似乎在向人類搖手指，建議他們“實施適當的變革管理程序”——這是任何音響系統衛生的基礎！

The suggested hypothesis is correct, and when the user clicks Accept, the supervisor agent helpfully provides the next steps to fix the problem and recommendations to prevent similar issues in the future (Figure 15.7). The agent almost seems to wag a finger at the human by suggesting that they“ implement proper change management procedures ”—the foundation of any sound system hygiene!

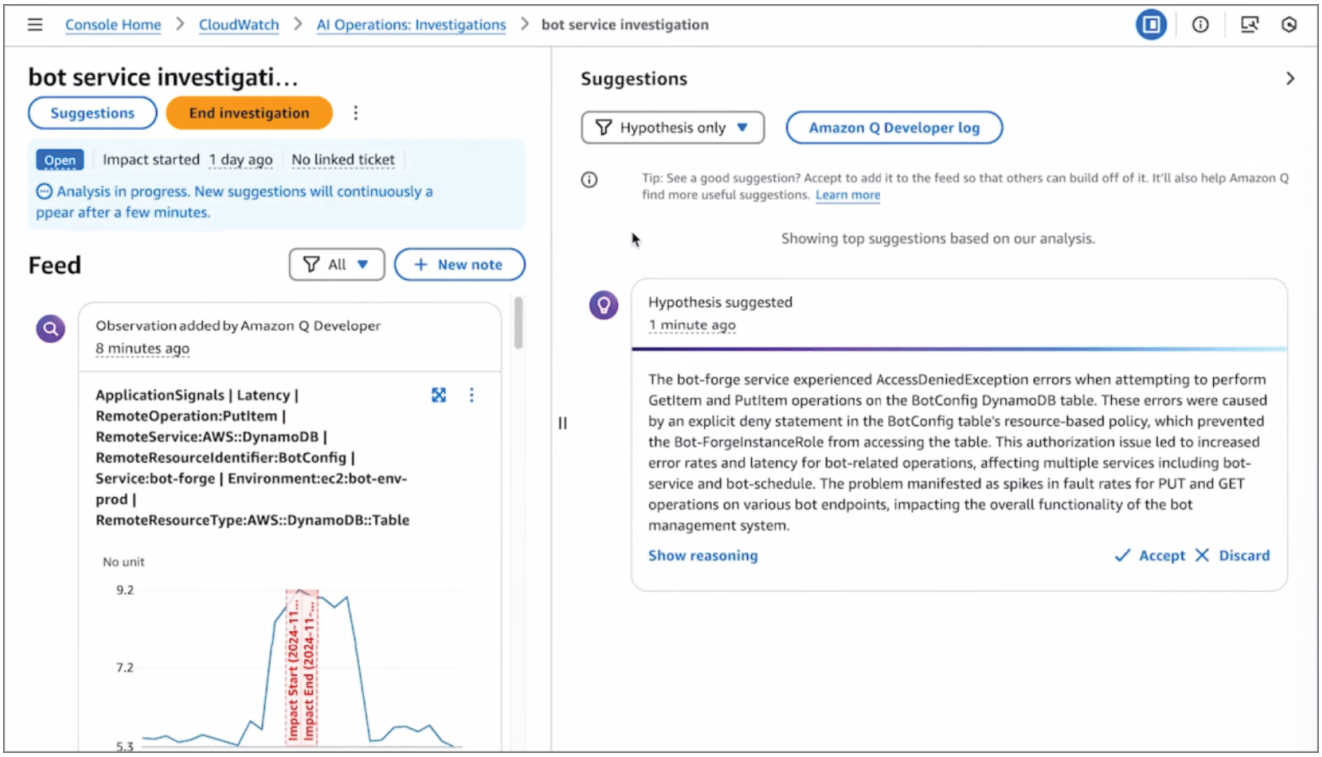

圖15.6 步驟5：主管代理人現在準備指出「犯罪」的罪魁禍首

Figure 15.6 Step 5: The supervisor agent is now ready to point out the culprit of the “ crime ”

來源：AWS 通過 YouTube （2）

Source: AWS via YouTube (2)

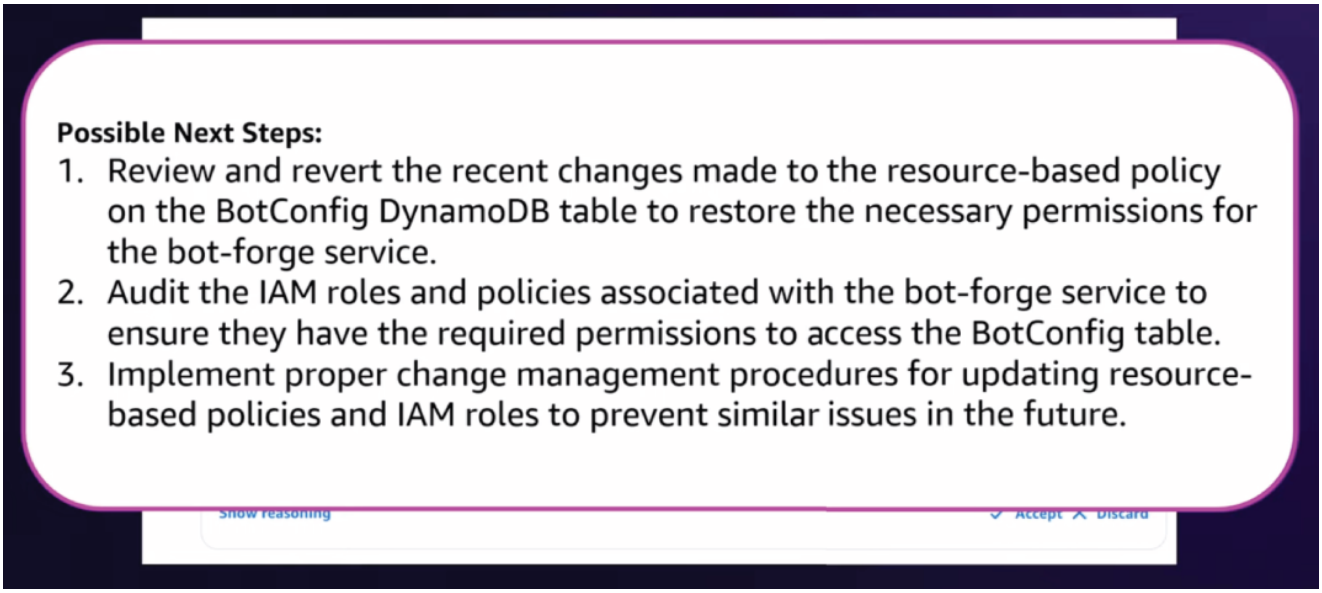

圖15.7 Supervisor Agent還提供了修復問題並防止將來出現的後續步驟

Figure 15.7 The supervisor agent also provides the next steps to fix the problem and prevent it in the future

來源：AWS 通過 YouTube （2）

Source: AWS via YouTube (2)

最後的思考

Final Thoughts

代理流程非常引人注目並成為當今許多人工智慧開發工作的重點的原因有很多。代理有效且經濟。它們允許更自然和靈活的人機界面，其中智能體填補了人類留下的空白，反之亦然，實際上成為人類和機器的思想融合，一個超級人類的“增強智能”，這遠遠超過其各個部分的總和。然而，要從與代理的互動中獲得最大價值，還需要徹底改變我們對人工智慧的看法。設計支援代理互動的使用者介面確實是創建「人工智慧優先」體驗的練習：

There are many reasons why agentic flows are highly compelling and are a focus of so much AI development work today. Agents are effective and economical. They allow for a much more natural and flexible human – machine interface, where the agents fill the gaps left by a human and vice versa, literally becoming a mind-meld of a human and a machine, a super human“ augmented intelligence, ”which is much more than the sum of its parts. However, getting the most value from interacting with agents also requires drastic changes in how we think about AI. Designing user interfaces that support agentic interactions is truly an exercise in creating“ AI-first ”experiences:

Flexible, Adjustable UI: Agents work alongside humans. To do that, AI agents require a flexible workflow that supports continuous interactions between humans and machines across multiple stages—starting an investigation, accepting evidence, forming a hypothesis, providing next steps, etc. It ’s a flexible looping flow consisting of multiple iterations.

Autonomy: While, for now, human-in-the-loop seems to be the norm for agentic workflows, agents show remarkable abilities to come up with hypotheses, gather evidence, and iterate the hypothesis as needed until they solve the problem. They do not get tired or run out of options and give up. AI agents can also effectively“ write code … a tool building its own tool ”(4) to explore novel ways to solve problems—this is new. This kind of interaction by nature requires an“ aggressive ”AI—for example, these agents are trained on maximum recall, open to trying every possibility to ensure the most

true positive outcomes (see our Value Matrix discussion in Chapter 5). This means that sometimes the agents will take an action "just to try it" without "thinking" about the cost of false positive or false negative outcomes. For example, an aggressive AI agent "doctor" might prescribe an invasive brain cancer biopsy procedure without considering lower-risk alternatives first or even stopping to get consent! All this requires a deeper level of human and machine analysis and multiple new approval flows for aggressive AI "exploration ideas" that might balloon operational costs and lead to human harm.

New Controls are Required: Although much of the interaction can be accomplished with existing screens, most agent actions are asynchronous, which means that most web pages with the traditional transactional, synchronous request/response models are a poor match for this new kind of interaction. We are going to need to introduce some new design paradigms. For example, start, stop, and pause buttons are a good starting point for controlling the agentic flow as otherwise you run a very real risk of ending up with the "The Sorcerer's Apprentice" situation from Fantasia (with self-replicating brooms fetching water without stopping, creating a huge expensive mess).

You "Hire" AI to Perform a Task: This is a radical departure from traditional tool use. Agents are no mere tools; they are intelligent reasoning entities with their own ways of doing things. AI service already consists of multiple specialized agents monitored by a supervisor. Very soon, we will introduce multiple levels of management with sub-supervisors and "team leads" reporting to the final "account executive agent" that deals with humans … just as human organizations do today. Historically, organizations needed to track the "3 Ps": products, people, and processes. Today, we are expanding the definition of the organization's "people" to include AI agents. That means developing workable UIs for safeguarding confidential information, role-based access control (RBAC), and agent versioning. Soon, safeguarding the agentic models and training data will be as important as signing NDAs with your human staff.

Continuously Learning Systems: To get full value out of agents, they need continuous learning. Agents learn, quickly becoming experts in whatever systems they work with. A new AI agent, like a new intern, will know very little, but they will quickly become the "adult in the room" with far more access and experience than most humans. This will have the effect of creating a massive power shift in the workplace. We need to be ready. (See Part 4 of this book for discussion on AI ethics.)

Regardless of how you feel about AI agents, it is clear that they are here to stay and evolve alongside their human counterparts. Therefore, we must understand how agentic AIs work and how to design systems that allow us to work with them safely and productively, emphasizing the best of what both

humans and machines can bring to the table.

參考

References

1. 1. 奧特曼，S.（2025）。反思。samaltman.com。https://blog.samaltman.com/reflections1. Altman, S. (2025). Reflections. samaltman.com. https://blog.samaltman.com/reflections

2. 2. AWS re：Invent 2024 - 不要陷入困境：互聯遙測如何讓您繼續前進（COP322）。（2024）. AWS 活動 on YouTube.com。www.youtube.com/watch?v=ad42UTjP7ds2. AWS re:Invent 2024 - Don’t get stuck: How connected telemetry keeps you moving forward (COP322). (2024). AWS Events on YouTube.com. www.youtube.com/watch?v=ad42UTjP7ds

3. 3. 卡薩，V.（2024）。分層 AI 代理： 使用 LangChain 創建主管 AI 代理。Medium.com https://vijaykumarkartha.medium.com/hierarchical-ai-agents-create-a-supervisor-ai-agent-using-langchain-315abbbd41333. Kartha, V. (2024). Hierarchical AI agents: Create a supervisor AI agent using LangChain. Medium.com https://vijaykumarkartha.medium.com/hierarchical-ai-agents-create-a-supervisor-ai-agent-using-langchain-315abbbd4133

4. 4. 莫利克，E.（2024）。當你給克勞德一隻滑鼠時。oneusefulthing.org。www.oneusefulthing.org/p/when-you-give-a-claude-a-mouse4. Mollick, E. (2024).When you give a Claude a mouse. oneusefulthing.org. www.oneusefulthing.org/p/when-you-give-a-claude-a-mouse