Building Agentic AI with Amazon Bedrock AgentCore

AWS 課堂培訓

課程說明

在本課程中，您將學習如何將概念驗證代理提升為 AWS 上可投入生產的代理式 AI 解決方案。您將使用 Amazon Bedrock AgentCore 服務進行工具編排、身分管理和生產監控，以實作安全、可擴展且可部署的企業 AI 系統。

- 課程等級：中級
- 時長：1 天

活動

本課程包含簡報、實作實驗室和小組練習。

課程目標

在本課程中，您將學習：

- 定義代理式 AI 的特性，並將其與傳統 AI 系統區分。
- 識別核心代理元件及其互動方式。
- 說明 Bedrock AgentCore 服務如何支援代理式 AI。
- 使用支援的框架搭配 AgentCore Runtime 部署代理。
- 說明 AgentCore Runtime 的核心功能。
- 設定具有工作階段隔離的無伺服器執行環境。
- 設定 AgentCore Identity 以滿足企業安全需求。
- 使用 AgentCore Policy 建立原則以保護代理工具呼叫。
- 實作安全的權杖管理和權限委派。
- 確保符合資料治理和稽核要求。
- 實作不同的工具整合模式，包括內建工具和基於協定的工具。
- 設計和部署 Model Context Protocol (MCP) 伺服器和用戶端，以實現可擴展的代理功能。
- 說明代理工具使用的常見驗證模式。
- 設定 AgentCore Gateway 元件以實現安全且經授權的工具存取。
- 針對不同使用案例實作代理記憶體模式。
- 設定 AgentCore Memory 操作以進行情境感知開發。
- 最佳化生產工作負載的記憶體效能。
- 設定 AgentCore Observability 以進行生產監控。
- 實作 Amazon CloudWatch 整合和專門的追蹤功能。

- 說明 AgentCore Evaluations 的核心功能。
- 將代理系統與生產 API 和服務整合。
- 設計生產環境的部署策略。
- 評估生產就緒狀態並建立持續改善流程。

目標對象

本課程適用於：

- 尋求建構代理系統中級知識的軟體開發人員
- 探索 AI 功能並有興趣建構代理式 AI 系統的技術專業人員。
- 建構代理式 AI 解決方案的開發團隊。

先決條件

我們建議本課程的學員具備：

- Agentic AI Foundations

課程大綱

第 1 天：

模組 1：代理式 AI 模式基礎

- 代理建構區塊
- Amazon Bedrock AgentCore 簡介

模組 2：AgentCore Runtime 和框架整合

- 支援的框架和實作
- AgentCore Runtime 概觀
- 基礎設施和部署

模組 3：安全性和身分管理

- 安全性和身分管理
- 使用 AgentCore Identity 保護您的代理

模組 4：工具整合和 AgentCore Gateway

- Amazon Bedrock AgentCore Policy
- 內建工具和自訂整合
- Model Context Protocol (MCP)
- AgentCore Gateway

- 實作 AgentCore Gateway
- Amazon Bedrock AgentCore Policy

模組 5：代理記憶體實作

- 代理記憶體核心概念
- AgentCore Memory
- 保護 AgentCore Memory

實作實驗室：使用 Amazon Bedrock AgentCore 增強和擴展代理

模組 6：生產監控和可觀測性

- 使用 AgentCore Observability 監控代理
- 使用 AgentCore Evaluation 驗證代理效能

模組 7：課程總結

- 後續步驟和其他資源
- 課程摘要