

AWS Certified AI Practitioner (AIF-C01) 考試指南

簡介

AWS Certified AI Practitioner (AIF-C01) 考試適用於能夠有效展示 AI/ML、生成式 AI 技術，以及相關聯 AWS 服務和工具的整體知識的個人，而且不受特定任務角色影響。

考試還會驗證考生是否有能力完成以下任務：

- 了解一般和 AWS 上的 AI、ML 和生成式 AI 概念、方法和策略。
- 了解如何適當使用 AI/ML 和生成式 AI 技術，以在考生的組織內提出相關問題。
- 確定適用於特定使用案例的正確 AI/ML 技術類型。
- 負責任地使用 AI、ML 和生成式 AI 技術。

目標考生描述

目標考生應該在 AWS 上摸索 AI/ML 技術達 6 個月。目標考生會使用，但不一定會在 AWS 上建置 AI/ML 解決方案。

AWS 知識推薦

目標考生應具備以下 AWS 知識：

- 熟悉核心 AWS 服務 (例如：Amazon EC2、Amazon S3、AWS Lambda 和 Amazon SageMaker) 和 AWS 核心服務使用案例
- 熟悉 AWS 雲端中安全性與合規的共同責任模型
- 熟悉 AWS Identity and Access Management (AWS IAM)，以保護和控制對 AWS 資源的存取
- 熟悉 AWS 全球基礎設施，包括 AWS 區域、可用區域和邊緣節點的概念
- 熟悉 AWS 服務定價模型

超出目標考生範圍的工作任務

以下清單包含預期目標考生無法執行的工作任務。此清單未列出所有詳情。以下任務超出考試範圍：

- 開發或編碼 **AI/ML** 模型或演算法
- 實作資料工程或特徵工程技術
- 執行超參數調校或模型最佳化
- 建置和部署 **AI/ML** 管道或基礎設施
- 對 **AI/ML** 模型進行數學或統計學分析
- 針對 **AI/ML** 系統實作安全性或合規通訊協定
- 為 **AI/ML** 解決方案開發和實作管控架構和政策

如需考試範圍內的 **AWS** 服務和特徵清單，以及超出範圍的 **AWS** 服務和功能清單的詳細資訊，請參閱附錄。

考試內容

試題類型

考試包含下列一種或多種問題類型：

- **單選題**：每題有一個正確的答案和三個不正確的答案 (錯誤選項)。
- **複選題**：每題有五個以上的答案選項，其中有兩個以上的正確答案。您必須選擇所有正確的答案才能得到分數。
- **排序題**：有 3–5 個答案清單，以完成指定的任務。您必須選取正確的答案，並依照正確順序排序答案，才能獲得分數。
- **配對題**：具有一份答案清單可與 3–7 個提示配對。您必須正確配對，才能獲得分數。
- **案例研究**：有一個情境，其中有二或多個題目都與此情境相關。案例研究中每個题目的情境都相同。案例研究中的每個題目都會單獨評估。在案例研究中只要答對每一道題目，就能獲得分數。

未回答的問題將以不正確計算；猜答不會扣分。此考試設有 **50** 個會影響您的分數的題目。¹

不計分內容

本考試設有 **15** 個不會影響您分數的不計分問題。**AWS** 會透過這些不計分問題來收集與考生表現相關的資訊，藉以評估這些問題能否在將來作為計分問題使用。考試中不能識別這些不計分的問題。

考試結果

The AWS Certified AI Practitioner (AIF-C01) 考試結果分為及格和不及格兩種。本考試的評分，將按照 **AWS** 專業人員根據認證產業最佳實務和指南所制定的最低標準來進行。

您的考試結果將以 **100** 至 **1,000** 分的比例分數呈現。最低及格分數為 **700** 分。您的分數表示您在考試中的整體表現，以及您是否通過。比例分數模型有助於將多種考試類型的得分放在一起比較，這些考試的難度級別可能略有不同。

您的分數報告中可能會包含您在各部分的表現分級表。本考試採用補償性評分模式，這代表您並不需要在每個部分都獲得合格分數。您只需要通過整體的考試。

考試的每個部分都有特定的權重，因此有些部分需回答的問題比其他部分多。分級表包含一般資訊，其中重點標示了您的優勢和劣勢。在解釋部分級別意見時請格外慎重。

¹不適用於考試的測試版。您可以在 [AWS Certification 網站](#) 上找到更多有關測試版考試的資訊。

命題大綱

此考試指南包括權重、測試領域和考試的任務說明。本指南並不提供考試內容的詳盡列表。但是，每個任務說明的其他上下文均有助於您準備考試。

考試具有以下測試領域和權重：

- 領域 1：AI 和 ML 基礎知識 (佔計分內容的 20%)
- 領域 2：生成式 AI 的基礎知識 (佔計分內容的 24%)
- 領域 3：基礎模型的應用程式 (佔計分內容的 28%)
- 領域 4：負責任 AI 的指南 (佔計分內容的 14%)
- 領域 5：AI 解決方案的安全性、合規與管控 (佔計分內容的 14%)

領域 1：AI 和 ML 的基礎知識

任務說明 1.1：說明基本 AI 概念和術語。

目標：

- 定義基本 AI 術語 (例如：AI、ML、深度學習、神經網路、電腦視覺、自然語言處理 [NLP]、模型、演算法、訓練和推論、偏差、公平性、符合，大型語言模型 [LLM])。
- 描述 AI、ML 和深度學習之間的相似性和差異。
- 描述各種類型的推論 (例如：批次，即時)。
- 描述 AI 模型中不同類型的資料 (例如：標記和未標記、表格式、時間序列、影像、文字、結構化和非結構化)。
- 描述監督式學習、無監督學習和強化學習。

任務說明 1.2：識別 AI 的實務使用案例。

目標：

- 辨識可以讓 **AI/ML** 提供價值的應用程式 (例如：協助人類做決策、解決方案可擴展性，自動化)。
- 判斷 **AI /ML** 解決方案何時不適用 (例如：成本效益分析，以及需要特定結果而不是預測的情況)。
- 針對特定使用案例 (例如：迴歸、分類、叢集) 選取適當的 **ML** 技術。
- 識別現實世界 **AI** 應用程式的範例 (例如：電腦視覺、**NLP**、語音辨識、推薦系統，詐騙偵測、預測)。
- 說明 **AWS** 受管 **AI/ML** 服務的功能 (例如：**SageMaker**、**Amazon Transcribe**、**Amazon Translate**、**Amazon Comprehend**、**Amazon Lex**、**Amazon Polly**)。

任務說明 1.3：描述 ML 開發生命週期。

目標：

- 描述 **ML** 管道的元件 (例如：資料收集、探索資料分析 [**EDA**]、資料預處理、特徵工程、模型訓練、超參數調校、評估、部署、監控)。
- 了解 **ML** 模型的來源 (例如：開放原始碼預先訓練的模型、訓練自訂模型)。
- 描述在生產中使用模型的方法 (例如：受管 **API** 服務、自主託管 **API**)。
- 識別 **ML** 管道的每個階段的相關 **AWS** 服務和特徵 (例如：**SageMaker**、**Amazon SageMaker Data Wrangler**、**Amazon SageMaker Feature Store**、**Amazon SageMaker Model Monitor**)。
- 了解 **ML** 作業 (**MLOps**) 的基本概念 (例如：實驗、可重複的流程、可擴展的系統、管理技術債務、實現生產整備、模型監控、模型重新訓練)。
- 了解模型效能指標 (例如：準確度、**ROC** 曲線下方面積 [**AUC**]、**F1** 分數) 和商業指標 (例如：每位使用者成本、開發成本、客戶回饋、投資報酬率 [**ROI**]) 以評估 **ML** 模型。

領域 2：生成式 AI 的基礎

任務說明 2.1：說明生成式 AI 的基本概念。

目標：

- 了解基本的生成式 AI 概念 (例如：字符、分成區塊、嵌入、向量、提示詞工程、轉換器型的 LLM、基礎模型、多模態模型、擴散模型)。
- 識別生成式 AI 模型的潛在使用案例 (例如：影像、視訊和音訊生成、摘要、聊天機器人、翻譯、程式碼生成、客服、搜尋、推薦引擎)。
- 描述基礎模型生命週期 (例如：資料選擇、模型選擇、預先訓練、微調、評估、部署、回饋)。

任務說明 2.2：了解生成式 AI 解決商業問題的能力和限制。

目標：

- 描述生成式 AI 的優勢 (例如：適應性、回應性、簡易性)。
- 識別生成式 AI 解決方案的缺點 (例如：幻覺、可解譯性、不準確性、非確定性)。
- 了解各種因素以選取適當的生成式 AI 模型 (例如：模型類型、效能需求、功能、限制、合規)。
- 確定生成式 AI 應用程式的商業價值和指標 (例如：跨領域效能、效率、轉換率、每位使用者平均收入、準確度、客戶生命週期價值)。

任務說明 2.3：描述用於建置生成式 AI 應用程式的 AWS 基礎設施和技術。

目標：

- 識別 AWS 服務和特徵以開發生成式 AI 應用程式 (例如：Amazon SageMaker JumpStart；Amazon Bedrock；PartyRock，一個 Amazon Bedrock Playground；Amazon Q)。
- 描述使用 AWS 生成式 AI 服務來建置應用程式的優勢 (例如：可存取性、進入門檻低、效率、成本效益、上市速度、達成商業目標的能力)。
- 了解 AWS 基礎設施對生成式 AI 應用程式的好處 (例如：安全性、合規性、責任、安防)。
- 了解 AWS 生成式 AI 服務的成本權衡 (例如：回應性、可用性、備援、效能、區域覆蓋範圍、基於字符的定價、佈建輸送量、自訂模型)。

領域 3：基礎模型的應用程式

任務說明 3.1：描述使用基礎模型的應用程式的設計考量。

目標：

- 識別選擇條件以選擇預先訓練的模型 (例如：成本、模態、延遲、多語系、模型大小、模型複雜度、自訂、輸入/輸出長度)。
- 了解推論參數對模型回應的效用 (例如：溫度、輸入/輸出長度)。
- 定義檢索增強生成 (RAG)，並描述其商業應用程式 (例如：Amazon Bedrock、知識庫)。
- 識別協助在向量資料庫中儲存嵌入項目的 AWS 服務 (例如：Amazon OpenSearch Service、Amazon Aurora、Amazon Neptune、Amazon DocumentDB [具有 MongoDB 相容性]、適用於 PostgreSQL 的 Amazon RDS)。
- 說明基礎模型自訂 (例如：預先訓練、微調、上下文學習、RAG) 的各種成本權衡方法。
- 了解客服在多步驟任務中的角色 (例如：Amazon Bedrock 代理人)。

任務說明 3.2：選擇有效的提示詞工程技術。

目標：

- 描述提示詞工程的概念和建構模組 (例如：情境式內容、指示、負面提示、模型潛空間)。
- 了解提示詞工程的技術 (例如：思路鏈、零樣本、單樣本、少樣本、提示詞範本)。
- 了解提示詞工程的好處和最佳實務 (例如：反應品質改進、實驗、防護機制、探索、獨特性和精準度、使用多個註解)。
- 定義提示詞工程的潛在風險和限制 (例如：暴露、中毒、劫持、越獄)。

任務說明 3.3：描述基礎模型的訓練和微調流程。

目標：

- 描述訓練基礎模型的關鍵要素 (例如：預先訓練、微調、持續預先訓練)。
- 定義微調基礎模型的方法 (例如：指令調校、適應特定領域的模型、轉移學習、持續預先訓練)。
- 描述如何準備資料以微調基礎模型 (例如：資料策管、管控、大小、標記、代表性、從人類回饋強化學習 [RLHF])。

任務說明 3.4：描述評估基礎模型效能的方法。

目標：

- 了解評估基礎模型效能的方法 (例如：人力評估、基準資料集)。
- 識別相關指標以評估基礎模型效能 (例如：召回率導向的摘要評估 [ROUGE]、雙語替換評測 [BLEU]、BertScore)。
- 確定基礎模型是否有效符合商業目標 (例如：生產力、使用者參與度、任務工程)。

領域 4：負責任 AI 的指南

任務說明 4.1：說明負責任 AI 系統開發。

目標：

- 識別負責任 AI 的特徵 (例如：偏差、公平性、包容性、穩健性、安全性、真實性)。
- 了解如何使用工具來識別負責任 AI 的特徵 (例如：Amazon Bedrock 安全護欄)。
- 了解選取模型的負責任實務 (例如：環境考量、永續性)。
- 識別使用生成式 AI 的法律風險 (例如：智慧財產權侵權索賠、偏差模型輸出、失去客戶信任、終端使用者風險、幻覺)。
- 識別資料集的特性 (例如：包容性、多樣性、經策管的資料來源、平衡資料集)。
- 了解偏差和變異的影響 (例如：對人口統計族群的影響、不準確性、過度擬合、低度擬合)。
- 描述偵測和監控偏差、可信度和真實性的工具 (例如：分析標籤品質、人力稽核、子群組分析、Amazon SageMaker Clarify、SageMaker Model Monitor、Amazon Augmented AI [Amazon A2I])。

任務說明 4.2：辨識透明且可解釋模型的重要性。

目標：

- 了解透明可解釋的模型與不透明可解釋的模型之間的差異。
- 了解可識別透明且可解釋的模型的工具 (例如：Amazon SageMaker 模型卡、開放原始碼模型、資料、授權)。
- 識別模型安全與透明度之間的權衡 (例如：測量可解譯性和效能)。
- 了解可解釋之 AI 以人為本的設計原則。

領域 5：AI 解決方案的安全性、合規與管控

任務說明 5.1：說明安全 AI 系統的方法。

目標：

- 識別 AWS 服務和特徵以保護 AI 系統 (例如：IAM 角色、政策和許可；加密；Amazon Macie；AWS PrivateLink；AWS 共同責任模型)。
- 了解來源引用和記錄資料來源的概念 (例如：資料沿襲、資料編目、SageMaker 模型卡)。
- 描述安全資料工程的最佳實務 (例如：評估資料品質、實作增強隱私權技術、資料存取控制、資料完整性)。
- 了解 AI 系統的安全性和隱私權考量 (例如：應用程式安全性、威脅偵測、漏洞管理、基礎設施防護、提示注入、靜態和傳輸中加密)。

任務說明 5.2：辨識 AI 系統的管控與合規法規。

目標：

- 識別 AI 系統的法規合規標準 (例如：國際標準化組織 [ISO]、服務機構控管 [SOC]、演算法責任法)。
- 識別 AWS 服務和特徵，以協助管控和法規合規 (例如：AWS Config、Amazon Inspector、AWS Audit Manager、AWS Artifact、AWS CloudTrail、AWS Trusted Advisor)。
- 描述資料控管策略 (例如：資料生命週期、記錄、駐留、監控、觀察、保留)。
- 描述遵循管控協定的程序 (例如：政策、審查頻率、審查策略、管控架構如生成式 AI 安全範圍矩陣、透明度標準、團隊培訓需求)。

附錄

考試範圍內的 **AWS** 服務和功能

下列清單包含考試範圍內的 **AWS** 服務和功能。此清單未列出所有詳情，可能會有所變更。
AWS 產品項目會顯示在與產品主要功能一致的類別中：

分析：

- AWS Data Exchange
- Amazon EMR
- AWS Glue
- AWS Glue DataBrew
- AWS Lake Formation
- Amazon OpenSearch Service
- Amazon QuickSight
- Amazon Redshift

雲端財務管理：

- AWS Budgets
- AWS Cost Explorer

運算：

- Amazon EC2

容器：

- Amazon Elastic Container Service (Amazon ECS)
- Amazon Elastic Kubernetes Service (Amazon EKS)

資料庫：

- Amazon DocumentDB (with MongoDB compatibility)
- Amazon DynamoDB
- Amazon ElastiCache
- Amazon MemoryDB
- Amazon Neptune
- Amazon RDS

機器學習：

- Amazon 增強版 AI (Amazon A2I)
- Amazon Bedrock
- Amazon Comprehend
- Amazon Fraud Detector
- Amazon Kendra
- Amazon Lex
- Amazon Personalize
- Amazon Polly
- Amazon Q
- Amazon Rekognition
- Amazon SageMaker
- Amazon Textract
- Amazon Transcribe
- Amazon Translate

管理與控管：

- AWS CloudTrail
- Amazon CloudWatch
- AWS Config
- AWS Trusted Advisor
- AWS Well-Architected Tool

網路連結和內容交付：

- Amazon CloudFront
- Amazon VPC

安全、身分與合規性：

- AWS Artifact
- AWS Audit Manager
- AWS Identity and Access Management (AWS IAM)
- Amazon Inspector
- AWS Key Management Service (KMS)
- Amazon Macie
- AWS Secrets Manager

儲存：

- Amazon S3
- Amazon S3 Glacier

考試範圍外的 **AWS** 服務和功能

下列清單包含超出考試範圍的 **AWS** 服務和功能。此清單未列出所有詳情，可能會有所變更。與考試的目標任務角色完全無關的 **AWS** 產品會從此清單中排除：

分析：

- AWS Clean Rooms
- Amazon CloudSearch
- Amazon FinSpace
- Amazon Managed Streaming for Apache Kafka (Amazon MSK)

應用程式整合：

- Amazon AppFlow
- Amazon MQ
- Amazon Simple Workflow Service (Amazon SWF)

商業應用程式：

- Amazon Chime
- Amazon Honeycode
- Amazon Pinpoint
- Amazon Simple Email Service (Amazon SES)
- AWS Supply Chain
- AWS Wickr
- Amazon WorkDocs
- Amazon WorkMail

雲端財務管理：

- AWS Application Cost Profiler
- AWS Billing Conductor
- AWS Marketplace

運算：

- AWS App Runner
- AWS Elastic Beanstalk
- EC2 Image Builder
- Amazon Lightsail

容器：

- Red Hat OpenShift Service on AWS (ROSA)

客戶支援：

- AWS IQ
- AWS Managed Services (AMS)
- AWS re:Post Private
- AWS Support

資料庫：

- Amazon Keyspaces (適用於 Apache Cassandra)
- Amazon Quantum Ledger Database (Amazon QLDB)
- Amazon Timestream

開發人員工具：

- AWS AppConfig
- AWS 應用程式編寫器
- AWS CloudShell
- Amazon CodeCatalyst
- AWS CodeStar
- AWS 故障注入服務
- AWS X-Ray

終端使用者運算：

- Amazon AppStream 2.0
- Amazon WorkSpaces
- Amazon WorkSpaces 精簡用戶端
- Amazon WorkSpaces Web

前端 **Web** 和行動應用：

- AWS Amplify
- AWS AppSync
- AWS Device Farm
- Amazon Location Service

物聯網 (IoT)：

- AWS IoT Analytics
- AWS IoT Core
- AWS IoT Device Defender
- AWS IoT Device Management
- AWS IoT Events

- AWS IoT FleetWise
- FreeRTOS
- AWS IoT Greengrass
- AWS IoT 1-Click
- AWS IoT RoboRunner
- AWS IoT SiteWise
- AWS IoT TwinMaker

機器學習：

- AWS DeepComposer
- AWS HealthImaging
- AWS HealthOmics
- Amazon Monitron
- AWS Panorama

管理與控管：

- AWS Control Tower
- AWS Health 儀表板
- AWS 實驗室
- AWS License Manager
- Amazon Managed Grafana
- Amazon Managed Service for Prometheus
- AWS OpsWorks
- AWS Organizations
- AWS Proton
- AWS Resilience Hub
- AWS 資源總管
- AWS Resource Groups
- AWS Systems Manager Incident Manager
- AWS Service Catalog
- Service Quotas
- AWS Telco Network Builder
- AWS 使用者通知

媒體：

- Amazon Elastic Transcoder
- AWS Elemental MediaConnect
- AWS Elemental MediaConvert
- AWS Elemental MediaLive
- AWS Elemental MediaPackage
- AWS Elemental MediaStore
- AWS Elemental MediaTailor
- Amazon Interactive Video Service (Amazon IVS)
- Amazon Nimble Studio

遷移和傳輸：

- AWS Application Discovery Service
- AWS Application Migration Service
- AWS Database Migration Service (AWS DMS)
- AWS DataSync
- AWS Mainframe Modernization
- AWS Migration Hub
- AWS Snow Family
- AWS Transfer Family

網路連結和內容交付：

- AWS App Mesh
- AWS Cloud Map
- AWS Direct Connect
- AWS Global Accelerator
- AWS Private 5G
- Amazon Route 53
- Amazon Route 53 應用程式復原控制器
- Amazon VPC IP 位址管理器 (IPAM)

安全、身分與合規：

- AWS Certificate Manager (ACM)
- AWS CloudHSM
- Amazon Cognito
- Amazon Detective
- AWS Directory Service
- AWS Firewall Manager
- Amazon GuardDuty
- AWS IAM Identity Center
- AWS Payment Cryptography
- AWS Private Certificate Authority
- AWS Resource Access Manager (AWS RAM)
- AWS Security Hub
- Amazon Security Lake
- AWS Shield
- AWS Signer
- Amazon Verified Permissions
- AWS WAF

儲存：

- AWS Backup
- AWS 彈性災難復原

問卷調查

本考試指南對您有幫助嗎？請[參加問卷調查](#)，告訴我們您的想法。