AWS Certified AI Practitioner (AIF-C01) 考试指南

简介

AWS Certified AI Practitioner (AIF-C01) 考试面向能够有效地展示对 AI/ML、生成式人工智能技术以及相关 AWS 服务和工具整体知识的掌握情况的个人（与具体的工作职务无关）。

本考试还考查考生能否完成以下任务：

- 了解 AI、ML 和生成式人工智能的一般性概念、方法和策略，以及 AWS 上的 AI、ML 和生成式人工智能概念、方法和策略。
- 了解如何正确使用 AI/ML 和生成式人工智能技术，从而能在考生所在企业/组织内提出相关问题。
- 针对特定使用案例，确定应该应用的正确 AI/ML 技术类型。
- 负责任地使用 AI、ML 和生成式人工智能技术。

目标考生描述

目标考生应具有长达 6 个月 AWS 上的 AI/ML 技术经验。目标考生会使用 AWS 上的 AI/ML 解决方案，但不一定需要会构建此类方案。

AWS 知识推荐

目标考生应掌握以下 AWS 知识：

- 熟悉 AWS 核心服务（例如 Amazon EC2、Amazon S3、AWS Lambda 和 Amazon SageMaker）及 AWS 核心服务使用案例
- 熟悉 AWS 云中安全性与合规性的 AWS 责任共担模式
- 熟悉用于保护和控制 AWS 资源访问权限的 AWS Identity and Access Management (AWS IAM)
- 熟悉 AWS 全球基础设施，包括 AWS 区域、可用区域和边缘站点的概念
- 熟悉 AWS 服务定价模型

超出目标考生考试范围的工作任务

下表列出了不要求目标考生能够完成的相关工作任务。列表并非详尽无遗。以下任务超出考试范围：

- 开发 AI/ML 模型或算法，或编写相关代码
- 实施数据工程或特征工程技术
- 执行超参数优化或模型优化
- 构建和部署 AI/ML 管道或基础设施
- 对 AI/ML 模型执行数学或统计分析
- 为 AI/ML 系统实施安全性或合规性协议
- 制定和实施 AI/ML 解决方案的监管框架和政策

有关范围内 AWS 服务和功能的列表以及范围外 AWS 服务和功能的列表，请参阅附录。

考试内容

题型

考试包含以下一种或多种题型：

- **单选题：** 有一个正确答案和三个错误答案（干扰项）。
- **多选题：** 在 5 个或更多答案选项中有两个或更多的正确答案。您必须选对所有正确答案才能得分。
- **排序题：** 列出完成指定任务可能需要的 3 至 5 个答案。您必须选择正确的答案并按正确的顺序排列答案，才能得分。
- **匹配题：** 显示 3 至 7 条提示和一列需要与之匹配的答案。您必须将所有答案与提示正确匹配才能得分。
- **案例研究题：** 针对一个场景提出两个或更多与该场景相关的问题。案例研究中的每个问题针对的都是同一个场景。案例研究中的每个问题都将单独评分。您在案例研究中正确回答的每个问题都将得到相应的分数。

未回答的试题将计为回答错误；猜答案不会扣分。本考试包括 50 道将影响您分数的试题。[1]

不计分内容

考试包括 15 道不计分试题，这些试题不影响您的分数。AWS 收集这些不计分试题的答题情况并进行评估，以备将来作为计分试题使用。在考试中不会标明这些不计分试题。

考试结果

AWS Certified AI Practitioner (AIF-C01) 考试结果分为及格和不及格。本考试按照 AWS 专业人员根据认证行业最佳实践和准则制订的最低标准进行评分。

您的考试成绩换算分数为 100 – 1000 分。最低及格分数是 700 分。您的分数表明您的总体考试答题情况以及是否通过考试。换算评分模型有助于在难度水平可能略有不同的多种考试形式中换算分数。

您的成绩单可能包含分类表，其中列出您在每个部分的考试结果。本考试采用补偿评分模型，这意味着您无需在每个部分都达到及格分数。您只需通过整体考试即可。

考试的每个部分具有特定的权重，因此，某些部分的试题比其他部分多。分类表包含一般信息，用于重点说明您的强项和弱项。在解读各个部分的反馈时，请务必小心谨慎。

---

[1]不适用于测试版考试。您可以在 AWS Certification 网站上详细了解有关测试版考试的一般说明。

内容大纲

本考试指南包括考试的权重、内容领域和任务表述，并未列出考试的全部内容。不过，每个任务表述都提供有额外的背景信息，有助于您备考。

考试中考查的内容领域和相应的权重如下：

- 领域 1： AI 和 ML 基础知识（计分内容的 20%）
- 领域 2： 生成式人工智能基础知识（计分内容的 24%）
- 领域 3： 基础模型的应用（计分内容的 28%）
- 领域 4： 负责任 AI 准则（计分内容的 14%）
- 领域 5： AI 解决方案的安全性、合规性和监管（计分内容的 14%）

领域 1： AI 和 ML 基础知识

任务表述 1.1： 解释基本 AI 概念和术语。

目标：

- 定义基本 AI 术语（例如，AI、ML、深度学习、神经网络、计算机视觉、自然语言处理 [NLP]、模型、算法、训练和推理、偏见、公平性、拟合、大型语言模型 [LLM]）。
- 描述 AI、ML 和深度学习之间的相似之处和不同之处。
- 描述各种类型的推理（例如，批量推理、实时推理）。
- 描述 AI 模型中不同类型的数据（例如，已标记数据和未标记数据、表格数据、时间序列数据、图像数据、文本数据、结构化数据和非结构化数据）。
- 描述有监督学习、无监督学习和强化学习。

任务表述 1.2： 确定 AI 的实际使用案例。

目标：

- 了解 AI/ML 可发挥价值的应用（例如，辅助人类决策、解决方案可扩展性、自动化）。
- 确定何时不适合应用 AI/ML 解决方案（例如，成本效益分析、需要特定结果而不是预测的情况）。
- 为特定使用案例选择适当的 ML 技术（例如，回归、分类、聚类）。
- 确定真实世界的 AI 应用示例（例如，计算机视觉、自然语言处理、语音识别、推荐系统、欺诈侦测、预测）。
- 解释 AWS 托管式 AI/ML 服务（例如 SageMaker、Amazon Transcribe、Amazon Translate、Amazon Comprehend、Amazon Lex、Amazon Polly）的功能。

任务表述 1.3： 描述 ML 开发生命周期。

目标：

- 描述 ML 管道的组件（例如，数据收集、探索性数据分析 [EDA]、数据预处理、特征工程、模型训练、超参数优化、评估、部署、监控）。
- 了解 ML 模型的来源（例如，开源预训练模型、训练自定义模型）。
- 描述在生产环境中使用模型的方法（例如，托管式 API 服务、自托管 API）。
- 确定 ML 管道每个阶段的相关 AWS 服务和功能（例如，SageMaker、Amazon SageMaker Data Wrangler、Amazon SageMaker 特征存放区、Amazon SageMaker 模型监控器）。
- 了解机器学习运维 (MLOps) 的基本概念（例如，实验、可重复流程、可扩展系统、管理技术债务、实现生产就绪、模型监控、模型再训练）。
- 了解模型性能指标（例如，准确率、ROC 曲线下面积 [AUC]、F1 分数）和业务指标（例如，每用户成本、开发成本、客户反馈、投资回报 [ROI]），以评估 ML 模型。

领域 2： 生成式人工智能基础知识

任务表述 2.1： 解释生成式人工智能的基本概念。

目标：

- 理解生成式人工智能基础概念（例如，词元、分块、嵌入、向量、提示工程、基于转换器的 LLM、基础模型、多模态模型、扩散模型）。
- 确定生成式人工智能模型的潜在使用案例（例如，图像、视频和音频生成；摘要；聊天机器人；翻译；代码生成；客户服务座席；搜索；推荐引擎）。
- 描述基础模型生命周期（例如，数据选择、模型选择、预训练、微调、评估、部署、反馈）。

任务表述 2.2： 了解生成式人工智能解决业务问题的能力和局限性。

目标：

- 描述生成式人工智能的优势（例如，适应性、响应性、简单性）。
- 确定生成式人工智能解决方案的缺点（例如，幻觉、可解释性、不准确、不确定性）。
- 了解选择合适的生成式人工智能模型时需考虑的各种因素（例如，模型类型、性能要求、能力、限制、合规性）。
- 确定生成式人工智能应用程序的商业价值和指标（例如，跨领域性能、效率、转化率、每用户平均收入、准确率、客户生命周期价值）。

任务表述 2.3： 描述用于构建生成式人工智能应用程序的 AWS 基础设施和技术。

目标：

- 确定用于开发生成式人工智能应用程序的 AWS 服务和功能（例如，Amazon SageMaker JumpStart；Amazon Bedrock；PartyRock [Amazon Bedrock 实验田]；Amazon Q）。
- 描述使用 AWS 生成式人工智能服务构建应用程序的优势（例如，可访问性、门槛较低、效率、成本效益、产品上市速度、实现业务目标的能力）。
- 了解 AWS 基础设施对生成式人工智能应用程序的益处（例如，安全性、合规性、负责任）。
- 了解 AWS 生成式人工智能服务的成本权衡（例如，响应能力、可用性、冗余、性能、区域覆盖范围、基于词元的定价、预置吞吐量、自定义模型）。

领域 3： 基础模型的应用

任务表述 3.1： 描述设计使用基础模型的应用程序时有哪些注意事项。

目标：

- 确定选择预训练模型的标准（例如，成本、模态、延迟、多语言、模型大小、模型复杂性、自定义、输入/输出长度）。
- 了解推理参数对模型响应的影响（例如，温度、输入/输出长度）。
- 定义检索增强生成 (RAG) 并描述其在业务中的应用（例如，Amazon Bedrock、知识库）。
- 确定有助于在向量数据库中存储嵌入的 AWS 服务（例如，Amazon OpenSearch Service、Amazon Aurora、Amazon Neptune、Amazon DocumentDB [兼容 MongoDB]、Amazon RDS for PostgreSQL）。
- 解释各种基础模型自定义方法（例如，预训练、微调、上下文学习、RAG）的成本权衡。
- 了解代理在多步骤任务中的作用（例如，Agents for Amazon Bedrock）。

任务表述 3.2： 选择有效的提示工程技术。

目标：

- 描述提示工程的概念和结构（例如，上下文、指令、否定提示、模型潜在空间）。
- 了解提示工程方法（例如，思维链、零样本、单样本、少量样本、提示模板）。
- 了解提示工程的益处和最佳实践（例如，响应质量改进、实验、防护机制、发现、特异性和简洁性，使用多条注释）。
- 定义提示工程的潜在风险和局限性（例如，暴露、投毒、劫持、越狱）。

任务表述 3.3： 描述基础模型的训练和微调过程。

目标：

- 描述训练基础模型的关键要素（例如，预训练、微调、持续预训练）。
- 定义微调基础模型的方法（例如，指令优化、针对特定领域调整模型、迁移学习、持续预训练）。
- 描述如何准备数据以微调基础模型（例如，数据策管、监管、调整大小、标记、代表性、人类反馈强化学习 [RLHF]）。

任务表述 3.4： 描述评估基础模型性能的方法。

目标：

- 了解评估基础模型性能的方法（例如，人工评估、基准数据集）。
- 确定评估基础模型性能的相关指标（例如，用于摘要和机器翻译评估的查全率导向研究 [ROUGE]、双语评估替换 [BLEU]、BERTScore）。
- 确定基础模型是否有效满足业务目标（例如，生产力、用户参与度、任务工程）。

领域 4： 负责任 AI 准则

任务表述 4.1： 解释负责任 AI 系统的开发。

目标：

- 确定负责任 AI 的特征（例如，偏见、公平性、包容性、稳健性、安全性、真实性）。
- 了解如何使用工具识别负责任 AI 的特征（例如，Amazon Bedrock 的防护机制）。
- 了解选择模型的负责任做法（例如，环境考量、可持续性、道德责任）。
- 确定使用生成式人工智能的法律风险（例如，知识产权侵权索赔、存在偏见的模型输出、失去客户信任、终端用户风险、幻觉）。
- 确定数据集的特征（例如，包容性、多样性、数据来源经策管、数据集平衡）。
- 了解偏差和方差的影响（例如，对人口统计群体的影响、不准确、过拟合、欠拟合）。
- 描述检测和监控偏见、可信度和真实性的工具（例如，分析标记质量、人工审核、亚组分析、Amazon SageMaker Clarify、SageMaker 模型监控器、Amazon Augmented AI [Amazon A2I]）。

任务表述 4.2： 了解模型透明且可解释的重要性。

目标：

- 了解透明且可解释的模型与不透明且不可解释的模型之间的区别。
- 了解用于识别透明且可解释的模型的工具（例如，Amazon SageMaker Model Cards、开源模型、数据、许可）。
- 确定模型安全性和透明度之间的权衡（例如，衡量可解释性和性能）。
- 了解为实现可解释 AI 而应遵循的以人为本的设计原则。

领域 5： AI 解决方案的安全性、合规性和监管

任务表述 5.1： 解释保护 AI 系统的方法。

目标：

- 确定用于保护 AI 系统的 AWS 服务和功能（例如，IAM 角色、策略和权限；加密；Amazon Macie；AWS PrivateLink；AWS 责任共担模式）。
- 了解来源引用和记录数据来源的概念（例如，数据沿袭、数据编目、SageMaker Model Cards）。
- 描述安全数据工程的最佳实践（例如，评估数据质量、实施隐私增强技术、数据访问控制、数据完整性）。
- 了解 AI 系统的安全和隐私注意事项（例如，应用程序安全、威胁检测、漏洞管理、基础设施保护、提示注入、静态加密和传输中加密）。

任务表述 5.2： 了解适用于 AI 系统的监管和合规性法规。

目标：

- 确定 AI 系统的监管合规标准（例如，国际标准化组织 [ISO]、System and Organization Controls [SOC]、算法问责法律）。
- 确定有助于监管和法规合规的 AWS 服务和功能（例如，AWS Config、Amazon Inspector、AWS Audit Manager、AWS Artifact、AWS CloudTrail、AWS Trusted Advisor）。
- 描述数据监管策略（例如，数据生命周期、日志记录、驻留、监控、观察、保留）。
- 描述遵循监管协议的流程（例如，政策、评审间隔、评审策略、生成式人工智能安全责任范围界定矩阵等监管框架、透明度标准、团队培训要求）。

附录

考试范围内的 AWS 服务和功能

下表列出了考试范围内的 AWS 服务和功能。此列表并非详尽无遗，并且可能会更改。AWS 产品/服务的类别与产品/服务的主要功能一致：

分析：

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

云财务管理：

- AWS Budgets
- AWS Cost Explorer

计算：

- Amazon EC2

容器：

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

数据库：

- Amazon DocumentDB（与 MongoDB 兼容）
- Amazon DynamoDB
- Amazon ElastiCache
- Amazon MemoryDB
- Amazon Neptune
- Amazon RDS

机器学习：

- Amazon Augmented 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

管理和监管：

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

联网和内容分发：

- Amazon CloudFront

- Amazon VPC

安全性、身份与合规性：

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

存储：

- Amazon S3
- Amazon S3 Glacier

超出考试范围的 AWS 服务和功能

下表列出了超出考试范围的 AWS 服务和功能。此列表并非详尽无遗，并且可能会更改。与考试的目标工作职责完全无关的 AWS 产品/服务被排除在此列表之外：

分析：

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

应用程序集成：

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

业务应用程序：

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

云财务管理：

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

计算：

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

容器：

- AWS 云端 Red Hat OpenShift 服务 (ROSA)

客户支持：

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

数据库：

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

开发工具：

- AWS AppConfig
- AWS 应用程序编辑器
- AWS CloudShell
- Amazon CodeCatalyst
- AWS CodeStar
- AWS Fault Injection Service
- AWS X-Ray

终端用户计算：

- Amazon AppStream 2.0
- Amazon WorkSpaces
- Amazon WorkSpaces 瘦客户端
- Amazon WorkSpaces Web

前端 Web 和移动：

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

物联网 (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

机器学习：

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

管理和监管：

- AWS Control Tower
- AWS Health Dashboard
- AWS Launch Wizard
- AWS License Manager
- Amazon Managed Grafana
- Amazon Managed Service for Prometheus
- AWS OpsWorks
- AWS Organizations
- AWS Proton
- AWS 韧性监测中心
- AWS 资源探索器
- AWS Resource Groups
- AWS Systems Manager Incident Manager
- AWS Service Catalog
- 服务配额
- AWS 电信网络构建器
- AWS 用户通知服务

媒体：

- 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

迁移与传输：

- 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

联网和内容分发：

- AWS App Mesh
- AWS Cloud Map
- AWS Direct Connect
- AWS Global Accelerator
- AWS 私有 5G 服务
- Amazon Route 53
- Amazon Route 53 应用程序恢复控制器
- Amazon VPC IP 地址管理器 (IPAM)

安全性、身份与合规性：

- 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

存储：

- AWS Backup
- AWS 弹性灾难恢复

调查问卷

本考试指南对您有多大帮助？ 请参与问卷调查，反馈您的意见。