

AWS Certified Solutions Architect - Professional (SAP-C02) 考试指南

简介

AWS Certified Solutions Architect - Professional (SAP-C02) 考试面向担任解决方案架构师角色的人员。该考试验证考生在基于 AWS Well-Architected Framework 设计 AWS 优化解决方案方面的高级技术技能和经验。

该考试还将验证考生仅使用 AWS Well-Architected Framework 就能完成以下任务的能力：

- 针对复杂的组织进行设计
- 针对新解决方案进行设计
- 持续改进现有解决方案
- 加快工作负载迁移和现代化

目标考生描述

目标考生应有至少 2 年的采用 AWS 服务设计和实施云科技解决方案的经验。此考生应能够评估云应用程序的要求，并针对在 AWS 上部署应用程序提供架构建议。目标考生还应该能够面对复杂组织，提供有关跨多个应用程序和项目的架构设计专家指导。

考试内容

答案类型

本考试具有两种类型的试题：

- **单选：** 具有一个正确答案和三个错误答案（干扰项）
- **多选：** 在 5 个或更多答案选项中具有两个或更多正确答案

选择一个或多个最准确表述或回答试题的答案。干扰项或错误答案是知识或技能不全面的考生可能会选择的答案选项。干扰项通常是与内容领域相符的看似合理的答案。

未回答的试题将计为回答错误；猜题不会扣分。考试包括 65 道计分试题。

不计分内容

考试包括 10 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考生答题情况以进行评估，以便将来将这些试题作为计分试题。在考试中不会标明这些不计分试题。

考试成绩

AWS Certified Solutions Architect - Professional (SAP-C02) 考试成绩分为及格和不及格。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。最低及格分数为 750 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平衡分数。

您的成绩单可能包含一个分类表，其中列出您在每个部分的考试成绩。此信息旨在提供有关您的考试成绩的一般反馈。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。您只需通过整个考试。

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。该表包含常规信息以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。通过考试的考生将不会收到此额外信息。

内容大纲

本考试指南包括考试的权重、测试领域和任务陈述，并未列出考试的全部内容。不过，本指南为每个任务陈述提供了额外的背景信息，以帮助指导您做好考试准备。下表列出了主要内容领域及其权重。该表位于完整考试内容大纲之前，其中包括额外的背景信息。每个领域中的百分比仅代表计分内容。

领域	在考试中所占的百分比
领域 1：针对复杂的组织设计解决方案	26%
领域 2：针对新解决方案进行设计	29%
领域 3：持续改进现有解决方案	25%
领域 4：加快工作负载迁移和现代化	20%
总计	100%

领域 1：针对复杂的组织设计解决方案

任务陈述 1：打造网络连接策略。

掌握以下知识：

- AWS 全球基础设施
- AWS 联网概念（例如，Amazon VPC、AWS Direct Connect、AWS VPN、传递路由、AWS 容器服务）
- 混合 DNS 概念（例如，Amazon Route 53 Resolver、本地部署 DNS 集成）
- 网络分段（例如，子网划分、IP 寻址、VPC 之间的连接）
- 网络流量监控

具备以下技能：

- 评估多个 VPC 的连接选项
- 评估本地部署、托管机房和云集成的连接选项
- 根据网络和延迟要求选择 AWS 地区和可用区
- 使用 AWS 工具对流量进行故障排除
- 利用服务终端节点进行服务集成

任务陈述 2：规定安全控制措施。

掌握以下知识：

- AWS Identity and Access Management (IAM) 和 AWS Single Sign-On
- 路由表、安全组和网络 ACL
- 加密密钥和证书管理（例如，AWS Key Management Service [AWS KMS]、AWS Certificate Manager [ACM]）
- AWS 安全、身份和合规性工具（例如 AWS CloudTrail、AWS Identity and Access Management、Access Analyzer、AWS Security Hub、Amazon Inspector）

具备以下技能：

- 评估跨账户访问管理
- 与第三方身份提供商集成
- 为静态数据和传输中数据部署加密策略
- 制定集中式安全事件通知和审计方面的策略

任务陈述 3：设计可靠且具有弹性的架构。

掌握以下知识：

- 恢复时间目标 (RTO) 和恢复点目标 (RPO)
- 灾难恢复策略（例如，使用 AWS Elastic Disaster Recovery [CloudEndure Disaster Recovery]、指示灯、热备用和多站点）
- 数据备份和恢复

具备以下技能：

- 根据 RTO 和 RPO 要求设计灾难恢复解决方案
- 实施自动从故障中恢复的架构
- 考虑纵向扩展和横向扩展选项以开发最佳的架构
- 设计有效的备份和恢复策略

任务陈述 4：设计一个多账户 AWS 环境。

掌握以下知识：

- AWS Organizations 和 AWS Control Tower
- 多账户事件通知
- 跨环境共享 AWS 资源

具备以下技能：

- 评估最适合组织需求的账户结构
- 推荐面向集中日志记录和事件通知的策略
- 开发多账户监管模型

任务陈述 5：确定成本优化和可见性策略。

掌握以下知识：

- AWS 成本和使用情况监控工具（例如，AWS Trusted Advisor、AWS 定价计算器、AWS Cost Explorer、AWS Budgets）
- AWS 购买选项（例如，预留实例、Savings Plans、Spot 实例）
- AWS 合理调整大小可见性工具（例如 AWS Compute Optimizer、Amazon S3 Storage Lens）

具备以下技能：

- 使用 AWS 工具监控成本和使用情况
- 制定有效的标记策略，将成本与业务部门对应起来
- 了解各购买选项对成本和性能的影响

领域 2：针对新解决方案进行设计

任务陈述 1：设计部署策略以满足业务需求。

掌握以下知识：

- 基础设施即代码 (IaC)（例如，AWS CloudFormation）
- 持续集成/持续交付 (CI/CD)
- 变更管理流程
- 配置管理工具（例如，AWS Systems Manager）

具备以下技能：

- 确定应用程序，或者确定新服务和功能的升级路径
- 选择服务以制定部署策略和实施适当的回滚机制
- 根据需要采用 Managed Services，以减少基础设施预置和修补开销
- 通过将复杂的开发和部署任务委派给 AWS 来利用高级技术

任务陈述 2：设计解决方案以确保业务连续性。

掌握以下知识：

- AWS 全球基础设施
- AWS 联网概念（例如，Route 53、路由方法）
- RTO 和 RPO
- 灾难恢复场景（例如，备份和还原、指示灯、热备用、多站点）
- AWS 上的灾难恢复解决方案

具备以下技能：

- 配置灾难恢复解决方案
- 配置数据和数据库复制
- 执行灾难恢复测试
- 构建经济高效的自动备份解决方案，支持跨多个可用区和/或 AWS 地区实现业务连续性
- 设计相应架构，使应用程序和基础设施在网络中断时仍然可用
- 利用流程和组件进行集中监控，以便主动从系统故障中恢复

任务陈述 3：根据要求确定安全控制。

掌握以下知识：

- IAM
- 路由表、安全组和网络 ACL
- 静态数据和传输中数据的加密选项
- AWS 服务终端节点
- 凭证管理服务
- AWS 托管的安全服务（例如 AWS Shield、AWS WAF、Amazon GuardDuty、AWS Security Hub）

具备以下技能：

- 指定遵守最低访问权限原则的 IAM 用户和 IAM 角色
- 使用安全组规则和网络 ACL 规则指定入站和出站网络流量
- 针对大规模 Web 应用程序制定攻击缓解策略
- 针对静态数据和传输中数据制定加密策略
- 为服务集成指定服务终端节点
- 制定补丁管理策略，以确保符合组织标准

任务陈述 4：设计满足可靠性要求的策略。

掌握以下知识：

- AWS 全球基础设施
- AWS 存储服务和复制策略（例如 Amazon S3、Amazon RDS、Amazon ElastiCache）
- 多可用区和多区域架构
- 弹性伸缩策略和事件
- 应用程序集成（例如，Amazon Simple Notification Service [Amazon SNS]、Amazon Simple Queue Service [Amazon SQS]、AWS Step Functions）
- 服务配额和限制

具备以下技能：

- 根据业务需求设计高可用性的应用程序环境
- 利用高级技术实现能承受故障发生的设计，确保系统无缝恢复
- 实施松散耦合的依赖关系
- 运行和维护高可用性架构（例如，应用程序故障转移、数据库故障转移）
- 利用 AWS Managed Services 实现高可用性
- 实施 DNS 路由策略（例如，Route 53 基于延迟的路由、地理位置路由、简单路由）

任务陈述 5：设计满足性能目标的解决方案。

掌握以下知识：

- 性能监控技术
- AWS 上的存储选项
- 实例系列和使用案例
- 专用数据库

具备以下技能：

- 设计可用于各种访问模式的大规模应用程序架构
- 根据业务目标设计弹性架构
- 应用设计模式，通过缓存、缓冲和副本实现性能目标
- 制定流程方法，为所需任务选择专用服务
- 设计合理调整大小策略

任务陈述 6：确定成本优化策略以满足解决方案的目标和目的。

掌握以下知识：

- AWS 成本和使用情况监控工具（例如，Cost Explorer、Trusted Advisor、AWS 定价计算器）
- 定价模型（例如，预留实例、Savings Plans）
- 存储分层
- 数据传输成本
- AWS Managed Services 产品

具备以下技能：

- 确定选择基础设施并合理调整大小的时机，以经济高效地利用资源
- 确定合适的定价模型
- 执行数据传输建模并选择服务来降低数据传输成本
- 针对支出和使用情况意识制定策略并实施控制措施

领域 3：持续改进现有解决方案

任务陈述 1：确定改善整体卓越运营的策略。

掌握以下知识：

- 警报和自动补救策略
- 灾难恢复规划
- 监控和日志记录解决方案（例如 Amazon CloudWatch）

- CI/CD 管道和部署策略（例如，蓝/绿、一次性、滚动）
- 配置管理工具（例如，Systems Manager）

具备以下技能：

- 确定最合适的日志记录和监控策略
- 评估当前的部署流程以获得改进机会
- 确定解决方案堆栈中自动化时机的优先级
- 推荐合适的 AWS 解决方案以实现配置管理自动化
- 设计故障场景活动，以支持恢复措施并进行练习来加深对恢复措施的理解

任务陈述 2：确定提高安全性的策略。

掌握以下知识：

- 数据留存、数据敏感性和数据法规要求
- 自动监控和补救策略（例如 AWS Config 规则）
- 密钥管理（例如，Systems Manager、AWS Secrets Manager）
- 最低访问权限原则
- 特定于安全性的 AWS 解决方案
- 修补做法
- 备份做法和方法

具备以下技能：

- 评估密钥和凭证的安全管理策略
- 审计环境是否符合最低访问权限原则
- 审查已实施的解决方案，确保各层的安全性
- 审查用户和服务的全面可追溯性
- 确定对漏洞检测的自动响应优先级
- 设计和实施修补及更新流程
- 设计和实施备份流程
- 采用补救技术

任务陈述 3：确定提高性能的策略。

掌握以下知识：

- 高性能系统架构（例如，弹性伸缩、实例队列和置放群组）
- 全球服务产品（例如 AWS Global Accelerator、Amazon CloudFront 和边缘计算服务）
- 监控工具集和服务（例如 CloudWatch）

- 服务协议 (SLA) 和关键绩效指标 (KPI)

具备以下技能：

- 将业务需求转化为可衡量的指标
- 测试可能的补救解决方案并提出建议
- 提议采用新技术和 Managed Services 的时机
- 评估解决方案并根据需求应用合适的大小调整
- 识别并检查性能瓶颈

任务陈述 4：确定提高可靠性的策略。

掌握以下知识：

- AWS 全球基础设施
- 数据复制方法
- 扩展方法（例如，负载均衡、弹性伸缩）
- 高可用性和弹性
- 灾难恢复方法和工具
- 服务配额和限制

具备以下技能：

- 了解应用程序的增长和使用趋势
- 评估现有架构以确定不够可靠的区域
- 修复单点故障
- 启用数据复制、自我修复以及弹性功能和服务

任务陈述 5：确定成本优化的时机。

掌握以下知识：

- 注重成本的架构选择（例如，利用 Spot 实例、扩展策略和合理调整资源规模）
- 采用价格模型（例如，预留实例、Savings Plans）
- 联网和数据传输成本
- 成本管理、警报和报告

具备以下技能：

- 分析使用情况报告以确定未充分利用的资源 and 过度使用的资源
- 利用 AWS 解决方案识别未使用的资源
- 根据预期使用模式设计账单告警

- 精细地调查 AWS Cost and Usage Report
- 将标记用于成本分配和报告

领域 4：加快工作负载迁移和现代化

任务陈述 1：选择可能迁移的现有工作负载和流程。

掌握以下知识：

- 迁移评估和跟踪工具（例如 AWS Migration Hub）
- 产品组合评估
- 资产规划
- 工作负载的优先级划分和迁移（例如，批次规划）

具备以下技能：

- 完成应用程序迁移评估
- 根据七种常见的迁移策略 (7R) 评估应用程序
- 评估总体拥有成本 (TCO)

任务陈述 2：确定现有工作负载的最佳迁移方法。

掌握以下知识：

- 数据迁移选项和工具（例如 AWS DataSync、AWS Transfer Family、AWS Snow Family、S3 Transfer Acceleration）
- 应用程序迁移工具（例如 AWS Application Discovery Service、AWS Application Migration Service [CloudEndure Migration]、AWS Server Migration Service [AWS SMS]）
- AWS 联网服务和 DNS（例如，Direct Connect、AWS Site-to-Site VPN、Route 53）
- 身份服务（例如 AWS SSO、AWS Directory Service）
- 数据库迁移工具（例如 AWS Database Migration Service [AWS DMS]、AWS Schema Conversion Tool [AWS SCT]）
- 监管工具（例如，AWS Control Tower、Organizations）

具备以下技能：

- 选择合适的数据库传输机制
- 选择合适的应用程序传输机制
- 选择合适的数据传输服务和迁移策略
- 将合适的安全方法应用于迁移工具
- 选择合适的监管模式

任务陈述 3：为现有工作负载确定新架构。

掌握以下知识：

- 计算服务（例如 Amazon EC2、AWS Elastic Beanstalk）
- 容器（例如，Amazon Elastic Container Service [Amazon ECS]、Amazon Elastic Kubernetes Service [Amazon EKS]、AWS Fargate、Amazon Elastic Container Registry [Amazon ECR]）
- AWS 存储服务（例如，Amazon Elastic Block Store [Amazon EBS]、Amazon Elastic File System [Amazon EFS]、Amazon FSx、Amazon S3、Volume Gateway）
- 数据库（例如，Amazon DynamoDB、Amazon OpenSearch Service [Amazon Elasticsearch Service]、Amazon RDS、Amazon EC2 上的自管理数据库）

具备以下技能：

- 选择合适的计算平台
- 选择合适的容器托管平台
- 选择合适的存储服务
- 选择合适的数据库平台

任务陈述 4：确定现代化和增强的时机。

掌握以下知识：

- 无服务器计算产品（例如 AWS Lambda）
- 容器（例如，Amazon ECS、Amazon EKS、AWS Fargate）
- AWS 存储服务（例如，Amazon S3、Amazon EFS）
- 专用数据库（例如 DynamoDB、Amazon Aurora Serverless、ElastiCache）
- 集成服务（例如，Amazon SQS、Amazon SNS、Amazon EventBridge [Amazon CloudWatch Events]、Step Functions）

具备以下技能：

- 确定分离应用程序组件的时机
- 确定采用无服务器解决方案的时机
- 为容器选择合适的服务
- 确定使用专用数据库的时机
- 选择合适的应用程序集成服务

附录

本考试可能涵盖哪些关键的工具、技术和概念？

以下是考试中可能出现的工具和技术列表（非详尽列表）。该列表可能会有更改，其目的是帮助您了解考试涵盖的服务、功能或技术的一般范围。该列表中的一般工具和技术未按特定顺序显示。AWS 服务根据其主要功能进行分组。尽管在本考试中对其中一些技术的考查可能比其他技术多，但这些技术在该列表中的顺序和位置并不表明其相对的权重或重要性：

- 计算
- 成本管理
- 数据库
- 灾难恢复
- 高可用性
- 管理和监管
- 微服务和组件解耦
- 迁移和数据传输
- 联网、连接和内容分发
- 安全
- 无服务器设计原则
- 存储

考试范围内的 AWS 服务和功能

分析：

- Amazon Athena
- AWS Data Exchange
- AWS Data Pipeline
- Amazon EMR
- AWS Glue
- Amazon Kinesis Data Analytics
- Amazon Kinesis Data Firehose
- Amazon Kinesis Data Streams
- AWS Lake Formation
- Amazon Managed Streaming for Apache Kafka (Amazon MSK)
- Amazon OpenSearch Service
- Amazon QuickSight

应用程序集成:

- Amazon AppFlow
- AWS AppSync
- Amazon EventBridge (Amazon CloudWatch Events)
- Amazon MQ
- Amazon Simple Notification Service (Amazon SNS)
- Amazon Simple Queue Service (Amazon SQS)
- AWS Step Functions

业务应用程序:

- Alexa for Business
- Amazon Simple Email Service (Amazon SES)

区块链:

- Amazon Managed Blockchain

云财务管理:

- AWS Budgets
- AWS Cost and Usage Report
- AWS Cost Explorer
- Savings Plans

计算:

- AWS App Runner
- AWS Auto Scaling
- AWS Batch
- Amazon EC2
- Amazon EC2 Auto Scaling
- AWS Elastic Beanstalk
- Amazon Elastic Kubernetes Service (Amazon EKS)
- Elastic Load Balancing
- AWS Fargate
- AWS Lambda
- Amazon Lightsail
- AWS Outposts
- AWS Wavelength

容器:

- Amazon Elastic Container Registry (Amazon ECR)
- Amazon Elastic Container Service (Amazon ECS)
- Amazon ECS Anywhere
- Amazon Elastic Kubernetes Service (Amazon EKS)
- Amazon EKS Anywhere
- Amazon EKS Distro

数据库：

- Amazon Aurora
- Amazon Aurora Serverless
- Amazon DocumentDB (与 MongoDB 兼容)
- Amazon DynamoDB
- Amazon ElastiCache
- Amazon Keyspaces (针对 Apache Cassandra)
- Amazon Neptune
- Amazon RDS
- Amazon Redshift
- Amazon Timestream

开发工具：

- AWS Cloud9
- AWS CodeArtifact
- AWS CodeBuild
- AWS CodeCommit
- AWS CodeDeploy
- Amazon CodeGuru
- AWS CodePipeline
- AWS CodeStar
- AWS X-Ray

最终用户计算：

- Amazon AppStream 2.0
- Amazon WorkSpaces

前端 Web 和移动：

- AWS Amplify
- Amazon API Gateway
- AWS Device Farm
- Amazon Pinpoint

物联网：

- AWS IoT Analytics
- AWS IoT Core
- AWS IoT Device Defender
- AWS IoT Device Management
- AWS IoT Events
- AWS IoT Greengrass
- AWS IoT SiteWise
- AWS IoT Things Graph
- AWS IoT 1-Click

机器学习：

- Amazon Comprehend
- Amazon Forecast
- Amazon Fraud Detector
- Amazon Kendra
- Amazon Lex
- Amazon Personalize
- Amazon Polly
- Amazon Rekognition
- Amazon SageMaker
- Amazon Textract
- Amazon Transcribe
- Amazon Translate

管理和监管：

- AWS CloudFormation
- AWS CloudTrail
- Amazon CloudWatch
- Amazon CloudWatch Logs
- AWS Command Line Interface (AWS CLI)
- AWS Compute Optimizer
- AWS Config
- AWS Control Tower
- AWS License Manager
- Amazon Managed Grafana
- Amazon Managed Service for Prometheus
- AWS Management Console
- AWS Organizations
- AWS Personal Health Dashboard
- AWS Proton
- AWS Service Catalog
- Service Quotas
- AWS Systems Manager
- AWS Trusted Advisor
- AWS Well-Architected Tool

媒体服务：

- Amazon Elastic Transcoder
- Amazon Kinesis Video Streams

迁移和传输:

- AWS Application Discovery Service
- AWS Application Migration Service (CloudEndure Migration)
- AWS Database Migration Service (AWS DMS)
- AWS DataSync
- AWS Migration Hub
- AWS Schema Conversion Tool (AWS SCT)
- AWS Snow Family
- AWS Transfer Family

联网和内容分发:

- Amazon CloudFront
- AWS Direct Connect
- Elastic Load Balancing (ELB)
- AWS Global Accelerator
- AWS PrivateLink
- Amazon Route 53
- AWS Transit Gateway
- Amazon VPC
- AWS VPN

安全性、身份和合规性:

- AWS Artifact
- AWS Audit Manager
- AWS Certificate Manager (ACM)
- AWS CloudHSM
- Amazon Cognito
- Amazon Detective
- AWS Directory Service
- AWS Firewall Manager
- Amazon GuardDuty
- AWS Identity and Access Management (IAM)
- Amazon Inspector
- AWS Key Management Service (AWS KMS)
- Amazon Macie
- AWS Network Firewall
- AWS Resource Access Manager (AWS RAM)
- AWS Secrets Manager
- AWS Security Hub
- AWS Security Token Service (AWS STS)
- AWS Shield
- AWS Single Sign-On
- AWS WAF

存储:

- AWS Backup
- Amazon Elastic Block Store (Amazon EBS)
- AWS Elastic Disaster Recovery (CloudEndure Disaster Recovery)
- Amazon Elastic File System (Amazon EFS)
- Amazon FSx (适用于所有类型)
- Amazon S3
- Amazon S3 Glacier
- AWS Storage Gateway

超出考试范围的服务、功能和概念

以下非详尽清单列出了被视为超出考试范围的项目:

- Amazon GameLift
- 移动应用程序的前端开发
- 12 要素应用程序方法
- 操作系统的深入知识