aws training and certification

AWS Certified DevOps Engineer - Professional (DOP-C02) 考试指南

简介

AWS Certified DevOps Engineer - Professional (DOP-C02) 考试适用于担任 DevOps 工程师角色的个人。本考试考查考生在 AWS 上预置、运行和管理分布式系统和服务的技术专业知识。

本考试还考查考生能否完成以下任务：

- 在 AWS 上实施和管理持续交付系统和方法。
- 实施和自动完成安全控制、监管流程和合规性验证。
- 在 AWS 上定义和部署监控、指标和日志记录系统。
- 在 AWS 上实施高度可用、可扩缩且可自行修复的系统。
- 设计、管理和维护用于自动完成运行流程的工具。

目标考生描述

目标考生具有 2 年或更长时间的 AWS 环境预置、运行和管理经验。目标考生还具有软件开发生命周期以及编程和/或脚本编写经验。

建议掌握的 AWS 知识

目标考生满足以下条件：

- 具有构建高度自动化的基础设施的经验
- 具有管理操作系统的经验
- 具有现代开发和运营流程和方法的经验
- 具有保护 AWS 基础设施的经验

哪些内容被视为超出目标考生的范围？

以下列出的是不要求目标考生能够完成的相关工作任务（非详尽列表）。以下内容被视为超出考试范围：

- 高级网络知识（例如，高级路由算法、故障转移技术）
- 能够为开发人员提供深层次的安全建议
- 数据库设计、查询和性能优化
- 全栈应用程序代码开发

要查看可能在考试中涉及的特定工具和技术的详细列表以及列入考试范围的 AWS 服务列表，请参阅附录。

考试内容

答案类型

本考试具有两种类型的试题：

- **多选题：** 具有一个正确答案和三个错误答案（干扰项）
- **多选题答案:** 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描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。

考试结果

AWS Certified DevOps Engineer - Professional (DOP-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。

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。本指南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： SDLC 自动化	22%
领域 2： 配置管理和 IaC	17%
领域 3： 弹性云科技解决方案	15%
领域 4： 监控和日志记录	15%
领域 5： 事件响应	14%
领域 6： 安全性和合规性	17%
总计	**100%**

领域 1： SDLC 自动化

任务陈述 1： 实施 CI/CD 管道。

掌握以下知识：

- 软件开发生命周期 (SDLC) 概念、阶段和模型
- 单账户和多账户环境的管道部署模式

具备以下技能：

- 配置代码、映像和构件存储库
- 使用版本控制将管道与应用程序环境集成在一起
- 设置构建流程（例如 AWS CodeBuild）
- 管理构建和部署密钥（例如 AWS Secrets Manager、AWS Systems Manager Parameter Store）
- 确定相应的部署策略（例如 AWS CodeDeploy）

任务陈述 2： 将自动化测试集成到 CI/CD 管道中。

掌握以下知识：

- 不同类型的测试（例如，单元测试、集成测试、验收测试、用户界面测试、安全扫描）
- 在 CI/CD 管道的不同阶段合理地使用不同类型的测试

具备以下技能：

- 在生成提取请求或代码合并时运行构建或测试（例如 AWS CodeCommit、CodeBuild）
- 批量运行负载/压力测试、性能基准测试和应用程序测试
- 根据应用程序退出代码测量应用程序运行状况
- 自动执行单元测试和代码覆盖
- 在管道中调用 AWS 服务以进行测试

任务陈述 3： 构建和管理构件。

掌握以下知识：

- 构件使用案例和安全管理
- 创建和生成构件的方法
- 构件生命周期注意事项

具备以下技能：

- 创建和配置构件存储库（例如 AWS CodeArtifact、Amazon S3、Amazon Elastic Container Registry [Amazon ECR]）
- 配置构建工具以生成构件（例如 CodeBuild、AWS Lambda）
- 自动执行 Amazon EC2 实例和容器映像生成过程（例如 EC2 Image Builder）

任务陈述 4： 为实例、容器和无服务器环境实施部署策略。

掌握以下知识：

- 各种平台的部署方法（例如 Amazon EC2、Amazon Elastic Container Service [Amazon ECS]、Amazon Elastic Kubernetes Service [Amazon EKS]、Lambda）
- 应用程序存储模式（例如 Amazon Elastic File System [Amazon EFS]、Amazon S3、Amazon Elastic Block Store [Amazon EBS]）
- 可变部署模式与不可变部署模式的对比
- 可用于分发代码的工具和服务（例如 CodeDeploy、EC2 Image Builder）

具备以下技能：

- 配置安全权限以允许访问构件存储库（例如 AWS Identity and Access Management [IAM]、CodeArtifact）
- 配置部署代理（例如 CodeDeploy 代理）
- 排查部署问题
- 使用不同的部署方法（例如，蓝/绿、Canary）

领域 2： 配置管理和 IaC

任务陈述 1： 定义云基础设施和可重用组件以在整个生命周期内预置和管理系统。

掌握以下知识：

- 适用于 AWS 的基础设施即代码 (IaC) 选项和工具
- 基于 IaC 的平台的更改管理流程
- 配置管理服务和策略

具备以下技能：

- 编写和部署 IaC 模板（例如 AWS Serverless Application Model [AWS SAM]、AWS CloudFormation、AWS Cloud Development Kit [AWS CDK]）
- 跨多个账户和 AWS 地区应用 AWS CloudFormation 堆栈集
- 确定最佳的配置管理服务（例如 AWS OpsWorks、AWS Systems Manager、AWS Config、AWS AppConfig）
- 将基础设施模式、监管控制和安全标准实施到可重用 IaC 模板中（例如 AWS Service Catalog、CloudFormation 模块、AWS CDK）

任务陈述 2： 部署自动化功能以在多账户/多区域环境中创建、加入和保护 AWS 账户。

掌握以下知识：

- AWS 账户结构、最佳实践和相关的 AWS 服务

具备以下技能：

- 标准化和自动化账户预置和配置
- 创建、整合和集中管理账户（例如 AWS Organizations、AWS Control Tower）
- 为多账户和复杂组织结构应用 IAM 解决方案（例如 SCP、担任角色）
- 批量实施和开发监管和安全控制（AWS Config、AWS Control Tower、AWS Security Hub、Amazon Detective、Amazon GuardDuty、AWS Service Catalog、SCP）

任务陈述 3： 为复杂任务和大型环境设计和构建自动化解决方案。

掌握以下知识：

- 自动执行任务和流程的 AWS 服务和解决方案
- 与 AWS 软件定义的基础设施交互的方法和策略

具备以下技能：

- 自动执行系统清点、配置和补丁管理（例如 Systems Manager、AWS Config）

- 为复杂场景开发 Lambda 函数自动化功能（例如 AWS SDK、Lambda、AWS Step Functions）
- 自动将软件应用程序配置为所需的状态（例如 OpsWorks、Systems Manager State Manager）
- 保持软件合规性（例如 Systems Manager）

领域 3： 弹性云科技解决方案

任务陈述 1： 实施高度可用的解决方案以满足弹性和业务要求。

掌握以下知识：

- 多可用区和多区域部署（例如，计算层、数据层）
- SLA
- 有状态服务的复制和故障转移方法
- 实现高可用性的技术（例如，多可用区、多区域）

具备以下技能：

- 将业务要求转化为技术弹性需求
- 找出并修复现有工作负载中的单点故障
- 在可用的情况下启用跨区域解决方案（例如 Amazon DynamoDB、Amazon RDS、Amazon Route 53、Amazon S3、Amazon CloudFront）
- 配置负载均衡以支持跨可用区服务
- 配置应用程序和相关服务以支持多个可用区和区域，同时最大限度减少停机

任务陈述 2： 实施可扩缩以满足业务要求的解决方案。

掌握以下知识：

- 用于扩缩服务的相应指标
- 松散耦合的分布式架构
- 无服务器架构
- 容器平台

具备以下技能：

- 找出并修复扩缩问题
- 确定并实施相应的自动扩缩、负载均衡和缓存解决方案
- 部署基于容器的应用程序（例如 Amazon ECS、Amazon EKS）
- 在多个 AWS 地区中部署工作负载以实现全球可扩缩性
- 配置无服务器应用程序（例如 Amazon API Gateway、Lambda、AWS Fargate）

任务陈述 3： 实施自动化恢复流程以满足 RTO/RPO 要求。

掌握以下知识：

- 灾难恢复概念（例如 RTO、RPO）
- 备份和恢复策略（例如 Pilot light、温备用）
- 恢复过程

具备以下技能：

- 测试多可用区/多区域工作负载故障转移（例如 Amazon RDS、Amazon Aurora、Route 53、CloudFront）
- 确定并实施相应的跨区域备份和恢复策略（例如 AWS Backup、Amazon S3、Systems Manager）
- 配置负载均衡器以从后端故障中恢复

领域 4： 监控和日志记录

任务陈述 1： 配置日志和指标收集、聚合和存储。

掌握以下知识：

- 如何监控应用程序和基础设施
- Amazon CloudWatch 指标（例如，命名空间、指标、维度和精度）
- 实时摄取日志
- 静态和传输中的日志和指标的加密选项（例如，客户端和服务器端、AWS Key Management Service [AWS KMS]）
- 安全配置（例如，允许收集日志的 IAM 角色和权限）

具备以下技能：

- 安全地存储和管理日志
- 使用指标筛选条件从日志事件中创建 CloudWatch 指标
- 创建 CloudWatch 指标流（例如 Amazon S3 或 Amazon Kinesis Data Firehose 选项）
- 收集自定义指标（例如，使用 CloudWatch 代理）
- 管理日志存储生命周期（例如 S3 生命周期、CloudWatch 日志组保留）
- 使用 CloudWatch 日志订阅处理日志数据（例如 Kinesis、Lambda、Amazon OpenSearch Service）
- 使用筛选条件和模式语法或 CloudWatch Logs Insights 搜索日志数据
- 配置日志数据加密（例如 AWS KMS）

任务陈述 2： 审核、监控和分析日志及指标以检测问题。

掌握以下知识：

- 异常检测警报（例如 CloudWatch 异常检测）
- 常见的 CloudWatch 指标和日志（例如 Amazon EC2 的 CPU 使用率、Amazon RDS 的队列长度、Application Load Balancer 的 5xx 错误）
- Amazon Inspector 和常见的评估模板
- AWS Config 规则
- AWS CloudTrail 录入事件

具备以下技能：

- 构建 CloudWatch 控制面板和 Amazon QuickSight 可视化内容
- 将 CloudWatch 警报与 CloudWatch 指标（标准和自定义）相关联
- 为不同的服务配置 AWS X-Ray（例如，容器、API Gateway、Lambda）
- 分析实时日志流（例如，使用 Kinesis Data Streams）
- 使用 AWS 服务分析日志（例如 Amazon Athena、CloudWatch Logs Insights）

任务陈述 3： 为复杂环境自动执行监控和事件管理。

掌握以下知识：

- 事件驱动的异步设计模式（例如，发送到 Amazon Simple Notification Service [Amazon SNS] 或 Lambda 的 S3 事件通知或 Amazon EventBridge 事件）
- 自动扩缩各种 AWS 服务的功能（例如，EC2 Auto Scaling 组、RDS 存储自动扩缩、DynamoDB、ECS 容量提供程序、EKS 自动扩缩程序）
- 警报通知和操作功能（例如，发送到 Amazon SNS 或 Lambda 的 CloudWatch 警报、EC2 自动恢复）
- AWS 服务中的运行状况检查功能（例如 Application Load Balancer 目标组、Route 53）

具备以下技能：

- 配置自动扩缩解决方案（例如 DynamoDB、EC2 Auto Scaling 组、RDS 存储自动扩缩、ECS 容量提供程序）
- 创建 CloudWatch 自定义指标和指标筛选条件、警报和通知（例如 Amazon SNS、Lambda）
- 配置 S3 事件以处理日志文件（例如，使用 Lambda），并将日志文件传送到另一个目标（例如 OpenSearch Service、CloudWatch Logs）
- 配置 EventBridge 以根据特定事件模式发送通知

- 在 EC2 实例上安装和配置代理（例如 AWS Systems Manager Agent [SSM Agent]、CloudWatch 代理）
- 配置 AWS Config 规则以修复问题
- 配置运行状况检查（例如 Route 53、Application Load Balancer）

领域 5： 事件响应

任务陈述 1： 管理事件源以处理事件，发出通知以及采取措施来响应事件。

掌握以下知识：

- 生成、捕获和处理事件的 AWS 服务（例如 AWS Health、EventBridge、CloudTrail、CloudWatch Events）
- 事件驱动的架构（例如，扇出、事件流、排队）

具备以下技能：

- 集成 AWS 事件源（例如 AWS Health、EventBridge、CloudTrail、CloudWatch Events）
- 构建事件处理工作流（例如 Amazon Simple Queue Service [Amazon SQS]、Kinesis、Amazon SNS、Lambda、Step Functions）

任务陈述 2： 实施配置更改以响应事件。

掌握以下知识：

- 实例集管理服务（例如 Systems Manager、AWS Auto Scaling）
- 配置管理服务（例如 AWS Config）

具备以下技能：

- 将配置更改应用于系统
- 修改基础设施配置以响应事件
- 修复非所需的系统状态

任务陈述 3： 排除系统和应用程序故障。

掌握以下知识：

- AWS 指标和日志记录服务（例如 CloudWatch、X-Ray）
- AWS 服务运行状况服务（例如 AWS Health、CloudWatch、Systems Manager OpsCenter）
- 根本原因分析

具备以下技能：

- 分析失败的部署（例如 AWS CodePipeline、CodeBuild、CodeDeploy、CloudFormation、CloudWatch 综合监控）
- 分析有关失败进程的事件（例如 Auto Scaling、Amazon ECS、Amazon EKS）

领域 6： 安全性和合规性

任务陈述 1： 批量实施身份和访问管理技术。

掌握以下知识：

- 相应地使用不同的 IAM 实体以进行人和机器访问（例如，用户、组、角色、身份提供程序、基于身份的策略、基于资源的策略、会话策略）
- 身份联合技术（例如，使用 IAM 身份提供程序和 AWS Single Sign-On）
- 使用 IAM 权限边界进行权限管理委派
- 组织 SCP

具备以下技能：

- 设计策略以实施最低权限访问
- 实施基于角色和基于属性的访问控制模式
- 自动为机器身份执行凭证轮换（例如 Secrets Manager）
- 管理权限以控制对人和机器身份的访问（例如，启用多重身份验证 [MFA]、AWS Security Token Service [AWS STS]、IAM 配置文件）

任务陈述 2： 应用自动化功能以进行安全控制和数据保护。

掌握以下知识：

- 网络安全组件（例如，安全组、网络 ACL、路由、AWS Network Firewall、AWS WAF、AWS Shield）
- 证书和公有密钥基础设施 (PKI)
- 数据管理（例如，数据分类、加密、密钥管理、访问控制）

具备以下技能：

- 在多账户和多区域环境中自动应用安全控制（例如 Security Hub、Organizations、AWS Control Tower、Systems Manager）
- 结合使用安全控制以应用纵深防御（例如 AWS Certificate Manager [ACM]、AWS WAF、AWS Config、AWS Config 规则、Security Hub、GuardDuty、安全组、网络 ACL、Amazon Detective、Network Firewall）
- 自动批量查找敏感数据（例如 Amazon Macie）
- 加密传输中的数据和静态数据（例如 AWS KMS、AWS CloudHSM、ACM）

任务陈述 3： 实施安全监控和审核解决方案。

掌握以下知识：

- 安全审核服务和功能（例如 CloudTrail、AWS Config、VPC 流日志、CloudFormation 偏差检测）
- 用于查找安全漏洞和事件的 AWS 服务（例如 GuardDuty、Amazon Inspector、IAM Access Analyzer、AWS Config）
- 常见的云安全威胁（例如，不安全的 Web 流量、泄露的 AWS 访问密钥、启用了公有访问或禁用了加密的 S3 存储桶）

具备以下技能：

- 实施强大的安全审核
- 配置基于意外或异常安全事件的警报
- 配置服务和应用程序日志记录（例如 CloudTrail、CloudWatch Logs）
- 分析日志、指标和安全检查结果

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：

- 应用程序部署
- 应用程序集成
- 应用程序管道
- 自动化
- 代码存储库最佳实践
- 成本优化
- 部署要求
- 混合部署
- IAM 策略
- 指标、监控、告警和日志记录
- 网络 ACL 和安全组设计和实施
- 运行最佳实践
- 回滚过程

考试范围内的 AWS 服务和功能

分析：

- Amazon Athena
- Amazon EMR
- Amazon Kinesis Data Firehose
- Amazon Kinesis Data Streams
- Amazon OpenSearch Service
- Amazon QuickSight

应用程序集成：

- Amazon AppFlow
- Amazon EventBridge (Amazon CloudWatch Events)

计算：

- AWS App Runner

- Amazon EC2
- Amazon EC2 Auto Scaling
- EC2 Image Builder
- AWS Elastic Beanstalk
- AWS Serverless Application Repository

容器：

- AWS App2Container
- AWS Copilot
- Amazon Elastic Container Registry (Amazon ECR)
- Amazon Elastic Container Service (Amazon ECS)
- Amazon Elastic Kubernetes Service (Amazon EKS)
- Amazon EKS Distro
- AWS Fargate
- AWS 上的 Red Hat OpenShift Service (ROSA)

数据库：

- Amazon Aurora
- Amazon Aurora Serverless v2
- AWS Database Migration Service (AWS DMS)
- Amazon DocumentDB（与 MongoDB 兼容）
- Amazon DynamoDB
- Amazon ElastiCache
- 适用于 Redis 的 Amazon MemoryDB
- Amazon RDS
- Amazon Redshift

开发工具：

- AWS Cloud Development Kit (AWS CDK)
- AWS CloudShell
- AWS CodeArtifact
- AWS CodeBuild
- AWS CodeCommit
- AWS CodeDeploy
- Amazon CodeGuru
- AWS CodePipeline
- AWS CodeStar
- AWS Command Line Interface (AWS CLI)
- AWS Fault Injection Simulator
- AWS SDK 和工具
- AWS X-Ray

Management and Governance:

- AWS Auto Scaling
- AWS CloudFormation
- AWS CloudTrail
- Amazon CloudWatch
- Amazon CloudWatch Logs
- AWS Compute Optimizer
- AWS Config
- AWS Control Tower
- AWS Health
- AWS License Manager
- Amazon Managed Grafana
- Amazon Managed Service for Prometheus
- AWS OpsWorks
- AWS Organizations
- AWS Personal Health Dashboard
- AWS Proton
- AWS Resilience Hub
- AWS Service Catalog
- AWS Systems Manager
- AWS Trusted Advisor

联网和内容分发：

- Amazon API Gateway
- AWS Client VPN
- Amazon CloudFront
- Elastic Load Balancing (ELB)
- AWS PrivateLink
- Amazon Route 53
- AWS Site-to-Site VPN
- AWS Transit Gateway
- Amazon VPC

安全性、身份和合规性：

- AWS Certificate Manager (ACM)
- AWS CloudHSM
- Amazon Cognito

- Amazon Detective
- AWS Directory Service
- 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

无服务器：

- AWS Lambda
- AWS Serverless Application Model (AWS SAM)
- Amazon Simple Notification Service (Amazon SNS)
- Amazon Simple Queue Service（Amazon SQS）
- AWS Step Functions

存储：

- AWS Backup
- Amazon Elastic Block Store (Amazon EBS)
- AWS Elastic Disaster Recovery (CloudEndure Disaster Recovery)
- Amazon Elastic File System (Amazon EFS)
- 适用于 Lustre 的 Amazon FSx
- 适用于 NetApp ONTAP 的 Amazon FSx
- 适用于 OpenZFS 的 Amazon FSx
- 适用于 Windows File Server 的 Amazon FSx
- Amazon S3
- Amazon S3 Glacier
- AWS Storage Gateway