AWS Certified Advanced Networking - Specialty (ANS-C01) 考试指南

简介

AWS Certified Advanced Networking - Specialty (ANS-C01) 考试适用于担任 AWS 联网专家角色的个人。本考试旨在考核考生设计、实施、管理和保护 AWS 及大规模混合网络架构的能力。

同时，还考查考生能否完成以下任务：

- 使用 AWS 设计和开发混合联网解决方案和基于云的联网解决方案
- 根据 AWS 最佳实践实施核心 AWS 联网服务
- 面向所有 AWS 服务，运营和维护混合网络架构与基于云的网络架构
- 使用工具来部署和自动执行混合联网任务以及基于云的 AWS 联网任务
- 使用 AWS 原生联网结构和服务实施安全的 AWS 网络

目标考生描述

目标考生应具有 5 年或更长时间的联网经验，并具有 2 年或以上的云和混合联网经验。

AWS 知识推荐

目标考生应具备以下 AWS 知识：

- AWS 联网细微差别及其与 AWS 服务集成的关系
- AWS 安全最佳实践
- AWS 计算和存储选项及其基础一致性模型

有关考试中可能出现的技术和概念的列表、考试范围内的 AWS 服务和功能的列表，以及超出考试范围的 AWS 服务和功能的列表，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：

- **单选题：**具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；猜答案不会扣分。本考试包括 50 道试题，这些试题将影响您的分数。

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 Advanced Networking - Specialty (ANS-C01) 考试结果分为通过和未通过两种。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。

您的考试结果换算分数为 100-1000 分。最低及格分数为 750 分。您的分数表明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一个分类表，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。

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：网络设计（占计分内容的 30%）
- 领域 2：网络实施（占计分内容的 26%）
- 领域 3：网络管理和运营（占计分内容的 20%）
- 领域 4：网络安全、合规性和监管（占计分内容的 24%）

领域 1：网络设计

任务说明 1.1：设计一个纳入了边缘网络服务的解决方案，以便优化全球架构的用户性能和流量管理。

掌握以下知识：

- 内容分发网络使用的设计模式（例如 Amazon CloudFront）
- 全球流量管理的设计模式（例如 AWS Global Accelerator）
- 内容分发网络和全球流量管理与其他服务（例如 Elastic Load Balancing [ELB]、Amazon API Gateway）的集成模式

具备以下技能：

- 评估面向互联网的全球入站和出站流量需求，以便设计合适的内容分发解决方案

任务说明 1.2：设计满足公有、私有和混合使用要求的 DNS 解决方案。

掌握以下知识：

- DNS 协议（例如 DNS 记录、TTL、DNSSEC、DNS 委派、区域）
- DNS 日志记录和监控
- Amazon Route 53 功能（例如别名记录、流量策略、解析程序、运行状况检查）
- 将 Route 53 与其他 AWS 联网服务（例如 Amazon VPC）集成
- 将 Route 53 与混合、多账户和多区域选项集成
- 域名注册

具备以下技能：

- 使用 Route 53 公有托管区域
- 使用 Route 53 私有托管区域
- 在混合架构和 AWS 架构中使用 Route 53 Resolver 终端节点
- 使用 Route 53 进行全球流量管理
- 创建和管理域名注册

任务说明 1.3：设计集成负载均衡功能的解决方案，以便满足高可用性、可扩展性和安全性要求。

掌握以下知识：

- 负载均衡在 OSI 模型的第 3 层、第 4 层和第 7 层的工作原理
- 不同类型的负载均衡器，以及它们如何满足网络设计、高可用性和安全性的要求
- 根据使用案例应用到负载均衡的连接模式（例如，内部负载均衡器、外部负载均衡器）
- 负载均衡器的缩放系数
- 负载均衡器和其他 AWS 服务的集成（例如，Global Accelerator、CloudFront、AWS WAF、Route 53、Amazon Elastic Kubernetes Service [Amazon EKS]、AWS Certificate Manager [ACM]）
- 负载均衡器的配置选项（例如，代理协议、跨区域负载均衡、会话关联性 [粘性会话]、路由算法）
- 负载均衡器目标组的配置选项（例如，TCP、GENEVE、IP 与实例的对比）
- 适用于 Kubernetes 集群的 AWS 负载均衡器控制器
- 使用负载均衡器进行加密和身份验证的注意事项（例如 TLS 终止、TLS 直通）

具备以下技能：

- 根据使用案例选择合适的负载均衡器
- 将弹性伸缩与负载均衡解决方案集成
- 将负载均衡器与现有应用程序部署集成

任务说明 1.4：定义跨 AWS 和混合网络的日志记录和监控要求。

掌握以下知识：

- AWS 架构中的 Amazon CloudWatch 指标、代理、日志、警报、控制面板和见解，以便提供监控能力
- 架构中的 AWS Transit Gateway Network Manager，以便提供监控能力
- 架构中的 VPC Reachability Analyzer，以便提供监控能力
- 架构中的流日志和流量镜像，以便提供监控能力
- 访问日志记录（例如，负载均衡器、CloudFront）

具备以下技能：

- 确定日志记录和监控要求
- 推荐适当的指标以提供对网络状态的监控能力
- 捕获基准网络性能

任务说明 1.5：设计本地部署网络与 AWS 云之间的路由策略和连接架构。

掌握以下知识：

- 路由基础知识（例如，动态和静态对比，BGP）
- 物理互连的第 1 层和第 2 层概念（例如 VLAN、链路聚合组 [LAG]、光缆、巨型帧）
- 封装和加密技术（例如 Generic Routing Encapsulation [GRE]、IPsec）
- 跨 AWS 账户共享资源
- 重叠网络

具备以下技能：

- 确定混合连接的要求
- 使用 AWS 服务设计冗余混合连接模型（例如 AWS Direct Connect、AWS Site-to-Site VPN）
- 使用 BGP 属性设计 BGP 路由，以便根据所需的流量模式（负载共享、主动/被动）影响流量流动
- 在设计中，将软件定义的广域网 (SD-WAN) 与 AWS 集成（例如，Transit Gateway Connect、重叠网络）

任务说明 1.6：设计包括多个 AWS 账户、AWS 区域和 VPC 的路由策略和连接架构，以便支持不同的连接模式。

掌握以下知识：

- 不同的连接模式和使用案例（例如 VPC 对等连接、Transit Gateway、AWS PrivateLink）
- VPC 共享的功能和优势
- IP 子网和应对 IP 地址重叠的解决方案

具备以下技能：

- 根据需求使用最合适的服务来连接多个 VPC（例如，使用 VPC 对等连接、Transit Gateway、PrivateLink）
- 在多账户设置中使用 VPC 共享
- 通过使用可用的不同服务和选项（例如，NAT、PrivateLink、Transit Gateway 路由）来管理 IP 重叠

领域 2：网络实施

任务说明 2.1：在本地部署网络和 AWS 云之间实施路由和连接。

掌握以下知识：

- 路由协议（例如，静态、动态）
- VPN（例如，安全性、加速的 VPN）
- 第 1 层和要使用的硬件类型（例如，授权证书 [LOA] 文档、主机托管设施、Direct Connect）
- 第 2 层和第 3 层（例如 VLAN、IP 寻址、网关、路由、交换）
- 流量管理和 SD-WAN（例如 Transit Gateway Connect）
- DNS（例如，条件转发、托管区域、解析程序）
- 安全设备（例如，防火墙）
- 负载均衡（例如，第 4 层对比第 7 层、反向代理、第 3 层）
- 基础设施自动化
- AWS Organizations 和 AWS Resource Access Manager (AWS RAM)（例如，多账户 Transit Gateway、Direct Connect、Amazon VPC、Route 53）
- 测试连接（例如，Route Analyzer、Reachability Analyzer）
- VPC 的联网服务

具备以下技能：

- 为混合连接解决方案配置物理网络要求
- 配置静态或动态路由协议，与混合连接解决方案结合使用
- 配置现有本地部署网络以便连接到 AWS 云
- 使用 AWS 云配置现有的本地部署名称解析
- 配置和实施负载均衡解决方案
- 为 AWS 服务配置网络监控和日志记录
- 测试和验证环境之间的连接

任务说明 2.2：跨多个 AWS 账户、区域和 VPC 实施路由及连接，以便支持不同的连接模式。

掌握以下知识：

- VPC 间和多账户连接（例如 VPC 对等连接、Transit Gateway、VPN、第三方供应商、SD-WAN、多协议标签交换 [MPLS]）
- 私有应用程序连接（例如 PrivateLink）
- 扩展 AWS 网络连接的方法（例如，Organizations、AWS RAM）
- 应用程序及客户端的主机和服务名称解析（例如 DNS）

- 基础设施自动化
- 身份验证和授权（例如 SAML、Active Directory）
- 安全性（例如，安全组、网络 ACL、AWS Network Firewall）
- 测试连接（例如，Route Analyzer、Reachability Analyzer、工具）

具备以下技能：

- 在单 VPC 或多 VPC 设计中使用 AWS 服务来配置网络连接架构（例如，DHCP、路由、安全组）
- 使用现有的第三方供应商解决方案配置混合连接
- 配置星型网络架构（例如，Transit Gateway、Transit VPC）
- 配置 DNS 解决方案以便实现混合连接
- 在网络边界之间实施安全性
- 使用 AWS 解决方案配置网络监控和日志记录

任务说明 2.3：实施复杂的混合和多账户 DNS 架构。

掌握以下知识：

- 何时使用私有托管区域和公有托管区域
- 变更流量管理模式的方法（例如，基于延迟、地理位置、权重）
- DNS 委派和转发（例如，条件转发）
- 不同的 DNS 记录类型（例如 A、AAAA、TXT、指针记录、别名记录）
- DNSSEC
- 如何在账户之间共享 DNS 服务（例如 AWS RAM）
- 出站和入站终端节点的要求和实施选项

具备以下技能：

- 配置 DNS 区域和条件转发
- 使用 DNS 解决方案配置流量管理
- 为混合网络配置 DNS
- 配置合适的 DNS 记录
- 在 Route 53 上配置 DNSSEC
- 在集中式或分布式网络架构中配置 DNS
- 在 Route 53 上配置 DNS 监控和日志记录

任务说明 2.4：自动化和配置网络基础设施。

掌握以下知识：

- 基础设施即代码 (IaC)（例如，AWS Cloud Development Kit [AWS CDK]、AWS CloudFormation、AWS CLI、AWS SDK、API）
- 事件驱动型网络自动化
- 预置云联网资源时，在 IaC 模板中使用硬编码指令的常见问题

具备以下技能：

- 创建和管理可重复的网络配置
- 集成事件驱动型联网功能
- 将混合网络自动化选项与 AWS 原生 IaC 集成
- 消除云联网环境中的风险并提高效率，同时保持尽可能低的成本
- 利用 IaC 实现云网络资源优化流程的自动化

领域 3：网络管理和运营

任务说明 3.1：维护 AWS 和混合网络上的路由和连接。

掌握以下知识：

- AWS 混合网络中使用的行业标准路由协议（例如，Direct Connect 上的 BGP）
- AWS 和混合网络的连接方法（例如，Direct Connect 网关、Transit Gateway、VIF）
- 限制和配额如何影响 AWS 联网服务（例如，带宽限制、路由限制）
- 可供自定义服务使用的私有和公有访问方法（例如 PrivateLink、VPC 对等连接）
- 可用的区域间和区域内通信模式

具备以下技能：

- 管理 AWS 的路由协议和混合连接选项（例如，通过 Direct Connect 连接、VPN）
- 维护对自定义服务的私有访问（例如 PrivateLink、VPC 对等连接）
- 使用路由表正确地引导流量（例如，自动传播、BGP）
- 设置对 AWS 服务的私有访问或公有访问（例如，Direct Connect、VPN）
- 通过动态和静态路由协议优化路由（例如，聚合路由、CIDR 重叠）

任务说明 3.2：监控和分析网络流量以便排除故障并优化连接模式。

掌握以下知识：

- 网络性能指标和可到达性约束（例如，路由、数据包大小）
- 用于评估网络性能和可到达性问题的相应日志和指标（例如数据包丢失）
- 用于收集和分析日志及指标的工具（例如 CloudWatch、VPC 流日志、VPC 流量镜像）
- 用于分析路由模式和问题的工具（例如，Reachability Analyzer、Transit Gateway Network Manager）

具备以下技能：

- 分析工具输出，以便评估网络性能和排除连接故障（例如 VPC 流日志、Amazon CloudWatch Logs）
- 绘制或了解网络拓扑（例如，Transit Gateway Network Manager）
- 分析数据包以确定数据包整形中的问题（例如 VPC 流量镜像）
- 排除由网络配置错误导致的连接问题（例如 Reachability Analyzer）
- 验证网络配置是否符合网络设计要求（例如 Reachability Analyzer）
- 在网络配置更改时自动验证连接意图（例如 Reachability Analyzer）
- 对 VPC 中的数据包大小不匹配进行故障排除，以便恢复网络连接

任务说明 3.3：优化 AWS 网络从而提高性能、可靠性和成本效益。

掌握以下知识：

- 适合使用 VPC 对等连接或 Transit Gateway 的情况
- 减少带宽占用的不同方法（例如，单播与多播对比，CloudFront）
- 在 VPC 与本地部署环境之间进行数据传输的经济高效的连接选项
- AWS 上不同类型的网络接口
- Route 53 中的高可用性功能（例如，使用具有延迟和加权记录集的运行状况检查实现的 DNS 负载均衡）
- Route 53 中提供可靠性的选项的可用性
- 负载均衡和流量分配模式
- VPC 子网优化
- 针对各种连接类型上带宽的帧大小优化

具备以下技能：

- 针对网络吞吐量进行优化
- 选择合适的网络接口以便获得最佳性能（例如，弹性网络接口、Elastic Network Adapter [ENA]、Elastic Fabric Adapter [EFA]）
- 分析所提供的网络需求，在 VPC 对等连接、代理模式或 Transit Gateway 连接之间做出选择
- 在适当的网络连接服务上实施解决方案以便满足网络要求（例如 VPC 对等连接、Transit Gateway、VPN 连接）
- 在 VPC 和本地部署环境中实施多播功能
- 创建 Route 53 公有托管区域和私有托管区域及记录，以便优化应用程序的可用性（例如，通过私有区域 DNS 条目将流量路由到多个可用区）
- 针对弹性伸缩配置更新和优化子网，以便支持应用程序负载增长
- 更新和优化子网以防 VPC 中的可用 IP 地址耗尽（例如，辅助 CIDR）
- 配置跨连接类型的巨型帧支持
- 使用 Global Accelerator 优化网络连接，以便提高网络性能和应用程序可用性

领域 4：网络安全、合规性和监管

任务说明 4.1：实施和维护网络功能，以便满足安全和合规性需求及要求。

掌握以下知识：

- 基于应用程序架构的不同威胁模型
- 常见的安全威胁
- 保护不同应用程序流的机制
- 满足安全性和合规性要求的 AWS 网络架构

具备以下技能：

- 保护流入 AWS 的入站流量（例如 AWS WAF、AWS Shield、Network Firewall）
- 保护来自 AWS 的出站流量（例如，Network Firewall、代理、Gateway Load Balancer）
- 保护账户内或跨多个账户的 VPC 间流量安全（例如，安全组、网络 ACL、VPC 终端节点策略）
- 实施 AWS 网络架构以便满足安全性和合规性要求（例如，不受信任的网络、外围 VPC、三层架构）
- 为给定的网络架构开发威胁模型并确定适当的缓解策略

- 测试是否符合初始要求（例如，故障转移测试、弹性）
- 使用 AWS 自动报告安全事件和警报

任务说明 4.2：使用网络监控和日志记录服务验证和审计安全性。

掌握以下知识：

- AWS 中可用的网络监控和日志记录服务（例如 CloudWatch、AWS CloudTrail、VPC 流量镜像、VPC 流日志、Transit Gateway Network Manager）
- 警报机制（例如 CloudWatch 警报）
- 不同 AWS 服务中的日志创建（例如，VPC 流日志、负载均衡器访问日志、CloudFront 访问日志）
- 日志传输机制（例如 Amazon Kinesis、Route 53、CloudWatch）
- 审计网络安全配置的机制（例如，安全组、AWS Firewall Manager、AWS Trusted Advisor）

具备以下技能：

- 创建和分析 VPC 流日志（包括流日志的基本字段和扩展字段）
- 创建和分析网络流量镜像（例如，使用 VPC 流量镜像）
- 使用 CloudWatch 实施自动警报
- 使用 CloudWatch 实施自定义指标
- 跨单个或多个 AWS 日志源关联和分析信息
- 实施日志传送解决方案
- 跨单个或多个 AWS 网络服务和账户实施网络审计策略（例如，Firewall Manager、安全组、网络 ACL）

任务说明 4.3：实施和维护数据及网络通信的机密性。

掌握以下知识：

- AWS 上可用的网络加密选项
- 通过 Direct Connect 建立 VPN 连接
- 传输中数据的加密方法（例如 IPsec）
- AWS 责任共担模式下的网络加密
- 适用于 DNS 通信的安全方法（例如 DNSSEC）

具备以下技能：

- 实施网络加密方法以便满足应用程序合规性要求（例如 IPsec、TLS）
- 实施加密解决方案来保护传输中的数据（例如，CloudFront、Application Load Balancer 和 Network Load Balancer、Direct Connect 上的 VPN、AWS 托管式数据库、Amazon S3、Amazon EC2 上的自定义解决方案、Transit Gateway）
- 使用证书颁发机构实施证书管理解决方案（例如，ACM、AWS Private Certificate Authority [ACM PCA]）
- 实施安全的 DNS 通信

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。列表并非详尽无遗，并且可能会有变更。AWS 产品/服务的类别与产品/服务的主要功能一致：

应用程序集成：

- Amazon EventBridge
- Amazon Simple Notification Service (Amazon SNS)
- Amazon Simple Queue Service (Amazon SQS)

计算：

- Amazon EC2
- Amazon EC2 Auto Scaling
- AWS Lambda

容器：

- Amazon Elastic Container Registry (Amazon ECR)
- Amazon Elastic Container Service (Amazon ECS)
- Amazon Elastic Kubernetes Service (Amazon EKS)
- AWS Fargate

成本管理：

- AWS Cost Explorer

前端 Web 和移动：

- Amazon API Gateway

管理和监管：

- AWS Auto Scaling
- AWS CLI
- AWS CloudFormation
- AWS CloudTrail
- Amazon CloudWatch

- AWS Config
- AWS Control Tower
- AWS Health Dashboard
- AWS 管理控制台
- AWS Organizations
- AWS Trusted Advisor
- AWS Well-Architected Tool

联网和内容分发：

- Amazon API Gateway
- AWS App Mesh
- AWS Client VPN
- AWS Cloud Map
- Amazon CloudFront
- AWS Direct Connect
- Elastic Load Balancing (ELB)
- AWS Global Accelerator
- 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 Firewall Manager
- AWS Identity and Access Management (IAM)
- AWS Network Firewall
- AWS Resource Access Manager (AWS RAM)
- AWS Shield
- AWS WAF

无服务器：

- Amazon API Gateway
- Amazon EventBridge
- AWS Fargate
- AWS Lambda
- Amazon Simple Notification Service (Amazon SNS)
- Amazon Simple Queue Service (Amazon SQS)
- Amazon Simple Storage Service (Amazon S3)

存储：

- Amazon S3

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。列表并非详尽无遗，并且可能会有变更。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：

- Amazon CloudSearch
- AWS Data Exchange
- AWS Data Pipeline
- Amazon EMR
- AWS Glue
- AWS Lake Formation
- Amazon Managed Streaming for Apache Kafka (Amazon MSK)
- Amazon OpenSearch Service
- Amazon QuickSight
- Amazon Redshift

AR 和 VR：

- Amazon Sumerian

区块链：

- Amazon Managed Blockchain
- Amazon Quantum Ledger Database (Amazon QLDB)

开发工具：

- AWS Device Farm
- AWS X-Ray

机器人：

- AWS RoboMaker

卫星：

- AWS Ground Station

调查问卷

本考试指南对您有帮助吗？ 请通过调查问卷，反馈您的意见。