

AWS 解决方案架构师学习与备考

(第 3 版·SAA-C02)

[美] 本·派珀(Ben Piper) 著
大卫·克林顿(David Clinton)
殷海英 译

清华大学出版社

北 京

北京市版权局著作权合同登记号 图字：01-2022-0416

All Rights Reserved. This translation published under license. Authorized translation from the English language edition, entitled AWS Certified Solutions Architect Study Guide: Associate SAA-C02 Exam, 3rd Edition, ISBN 9781119713081, by Ben Piper, David Clinton, Published by John Wiley & Sons. Copyright © 2021 by John Wiley & Sons. No part of this book may be reproduced in any form without the written permission of the original copyrights holder. Copies of this book sold without a Wiley sticker on the cover are unauthorized and illegal.

本书中文简体字版由 Wiley Publishing, Inc. 授权清华大学出版社出版。未经出版者书面许可，不得以任何方式复制或传播本书内容。

本书封面贴有 Wiley 公司防伪标签，无标签者不得销售。

版权所有，侵权必究。举报：010-62782989, beiqinquan@tup.tsinghua.edu.cn。

图书在版编目(CIP)数据

AWS 解决方案架构师学习与备考：第 3 版. SAA-C02 / (美) 本·派珀 (Ben Piper), (美) 大卫·克林顿 (David Clinton) 著；殷海英译. —北京：清华大学出版社，2022.4

书名原文：AWS Certified Solutions Architect Study Guide: Associate SAA-C02 Exam, 3rd Edition

ISBN 978-7-302-60349-8

I. ①A… II. ①本… ②大… ③殷… III. ①软件设计 IV. ①TP311.5

中国版本图书馆 CIP 数据核字(2022)第 042217 号

责任编辑：王 军

封面设计：孔祥峰

版式设计：思创景点

责任校对：成凤进

责任印制：沈 露

出版发行：清华大学出版社

网 址：http://www.tup.com.cn, http://www.wqbook.com

地 址：北京清华大学学研大厦 A 座 邮 编：100084

社 总 机：010-83470000 邮 购：010-62786544

投稿与读者服务：010-62776969, c-service@tup.tsinghua.edu.cn

质 量 反 馈：010-62772015, zhiliang@tup.tsinghua.edu.cn

印 装 者：大厂回族自治县彩虹印刷有限公司

经 销：全国新华书店

开 本：170mm×240mm 印 张：22.75 字 数：485 千字

版 次：2022 年 4 月第 1 版 印 次：2022 年 4 月第 1 次印刷

定 价：98.00 元

产品编号：093829-01

在这个以云计算为主导的 IT 时代, AWS(Amazon Web Services)被公认为云计算的领航者, AWS 是全球最全面、应用最广泛的云平台, 遍布全球的数据中心, 为全球数百万用户提供 200 多项功能齐全的低成本、敏捷、创新的云端服务。AWS 提供从计算、存储和数据库等基础设施技术, 到人工智能、机器学习、数据湖以及物联网等新兴技术, AWS 所提供的云服务比任何其他云服务商都要丰富, 使用 AWS 可以让你以更高的效率、更低的成本以及更简捷的方法构建你的应用程序。同时, AWS 拥有最大且最具活力的云社区, 在全球拥有数百万活跃的客户和众多合作伙伴, 几乎在所有行业以及任何规模的企业中, 都能找到使用 AWS 获得成功的众多案例。AWS 始终非常重视信息安全, 并按照军事、金融及其他高度敏感性组织的要求构建其云端环境, 并带有 230 项安全、合规性及监管服务功能, 支持 90 个安全标准及合规性认证, 为存储客户数据的全部服务使用高强度的加密技术。利用 AWS, 可以使用最新的技术更快速地进行开发和创新, 因为 AWS 自己的创新技术是其他云服务提供商无法企及的。

IT 认证一直是 IT 从业人员掌握某项技能的证明。十多年前, 我担任某数据库公司的数据库大师级认证的考官, 那时候就发现越来越多的公司在招聘时需要应聘者提供相关的技术认证, 并在许多项目投标过程中也需要应标的企业配备具有相关技术认证的工程师。认证是对技能的一种证明, 但更重要的是, 通过学习与认证相关的知识, 可以真正掌握从事相关工作时所需的技能。本书包含两部分: 第 I 部分深入研究了 AWS 的每个核心服务。这些服务包括弹性计算云(Elastic Compute Cloud, EC2)、虚拟私有云(Virtual Private Cloud, VPC)、身份和访问管理(Identity and Access Management, IAM)、Route 53 和简单存储服务(Simple Storage Service, S3)等。第 II 部分由一组最佳实践及指导原则组成, 帮助你在云中设计、实现和运营所需的应用场景。本书在每章末尾提供相关测试题, 通过这些测试题可以让你更好地熟悉并通过 AWS 解决方案架构师考试。

说到我与 AWS 的相识, 说是偶然, 但也是必然。2013 年的夏天, 从事了 9 年关系数据库的教学之后, 我开始从事数据科学的教学工作。在准备秋季学期的数据科学课程时, 考虑学生们自己的计算机操作系统各异、各种设置也不尽相同, 如何能够让大家专注于课程本身, 而不是为设置复杂的数据科学运行环境而烦心。当时, 我的同事也是我的导师安东尼教授对我说, 未来的时代一定是以云为基础的信息技术高速发展的时代, 莫不如就在你的课程中使用云平台作为基础设施, 将所需的系统部署在云端, 从而实现稳定、统一、高效的计算环境。我听取了安东尼教授的建议, 并使用

AWS 作为课程的实验环境，这门课取得了很大的成功，所以在后续的数据分析、机器视觉以及高性能计算相关的课程中，我都将 AWS 作为演示环境，并向学生展示 AWS 所带来的各种卓越的功能。在不断使用 AWS 的过程中，我发现 AWS 在人工智能方面提供了诸多操作简单、但功能强大的服务，因此在清华大学出版社王军老师的帮助下，另一本与 AWS AI 服务相关的书籍也许很快就能和大家见面。在这里我要感谢他为我提供了新的与大家分享知识的方式，也感谢他帮助我出版了多本数据科学与人工智能相关的书籍。

最后，祝各位读者能够从本书中了解 AWS 所提供的精彩服务，也预祝那些打算参加 AWS 解决方案架构师考试的朋友能够顺利通过考试。

殷海英

作于加利福尼亚州埃尔赛贡多市

2022.1

作者简介

Ben Piper 是一名网络和云咨询顾问，他撰写了多本书，包括 *AWS Certified Cloud Practitioner Study Guide: Foundational CLF-C01 Exam*(Sybex, 2019)和 *Learn Cisco Network Administration in a Month of Lunches*(Manning, 2017)。

David Clinton 是一名 Linux 服务器管理员及 AWS 解决方案架构师，曾在学校和企业环境中从事 IT 基础设施工作。他写过很多书，包括与 Ben Piper 一起编写 *AWS Certified Cloud Practitioner Study Guide: Foundational CLF-C01 Exam*(Sybex, 2019)和 *Linux in Action*(Manning, 2018)，并为 Pluralsight 创建了 20 多个视频课程，讲授 AWS 和 Linux 管理、服务器虚拟化和 IT 安全等内容。

此前, David 当了 20 年的高中老师。目前他与妻子和家人居住在加拿大多伦多市。

致 谢

我们要感谢帮助我们完成《AWS 解决方案架构师学习与备考(第 3 版•SAA-C02)》的朋友们。

首先，特别感谢来自 Wiley 的朋友们。高级编辑 **Kenyon Brown**，他启动了该项目，并推动该书快速出版。他在整个项目中的经验和指导对该书的出版起着至关重要的作用。项目编辑 **Stephanie Barton** 推动了该书按时完成。通过她的编辑，使该书中的许多技术细节更易于阅读。

Todd Montgomery 审阅了各个章节以及习题，保证了该书技术上的准确性。他的评论和建议不仅使该书的内容更加精确，他还为章节复习问题提供了额外的想法，使它们更具有挑战性并更贴近考试。

最后，作者们要感谢彼此的付出！

准备任何认证考试都需要你计划有多少内容要从动手实践中获得，有多少内容只需要简单记忆一些事实和数字。我们参加了几十次 IT 认证考试，使我们了解明智地利用学习时间是多么重要。我们创作本书旨在帮助你发现自己在使用 AWS 平台时的优势和不足之处，以便你能够集中精力去学习。无论你是长期使用 AWS，还是对 AWS 比较陌生，我们都建议你从头到尾地仔细阅读本书。

想通过 AWS 认证解决方案架构师-助理级考试，需要理解 AWS 核心服务组件和操作，以及这些服务如何相互交互。请阅读各种 AWS 服务的官方文档。Amazon 提供了 HTML、PDF 以及 Kindle 形式的文档。用本书作为指导，可以帮助你找到自己的优势和不足，这样就可以集中精力完成学习内容。

在参加 AWS 认证解决方案架构师-助理级考试之前，你应该至少有 6 个月的 AWS 动手实践经验。如果你刚刚接触 AWS，我们强烈建议你将我们的 *AWS Certified Cloud Practitioner Study Guide: CLF-C01 Exam* 作为入门。

尽管《AWS 解决方案架构师学习与备考(第 3 版 • SAA-C02)》是专门为 AWS 认证解决方案架构师-助理级考试而设计的，但是我们的一些读者发现本书对于准备 SysOps 管理员及 DevOps 工程师考试也很有帮助。

实践经验是考试成功的关键。《AWS 解决方案架构师学习与备考(第 3 版 • SAA-C02)》中的每一章都包含动手练习，你应该在阅读期间或者完成每章阅读之后立即完成这些练习。同时需要充分理解这些练习，虽然这些练习并没有涵盖所有 AWS 的服务使用场景，但这些练习为你打下了坚实的基础，将它们作为你的起点，并大胆地对这些实验进行修改，以适应你在工作中遇到的场景。但请了解，在练习中的一些操作使用了 AWS 的 Web 控制台，因为 AWS 在不断改进，所以一些屏幕截图、操作步骤和实际情况可能会存在一些差异。这也正是给你一个去深入研究 AWS 在线文档的好机会，推动你自己在 Web 控制台中探索。同时，尽管你可以使用 AWS 免费服务完成许多练习，但想顺利通过考试，需要做更多的练习，而这些练习会产生一些开销，但这笔钱值得花，因为获得认证是对你的未来职业发展的一项很好的投资。

每章中都包含一些练习题，用来全面测试你对该章节所涉及的服务和概念的理解情况，同时也可以测试你将之前章节中的概念和信息整合起来的能力。虽然这些问题的难度各不相同，但请放心，这些问题都是我们精心设计的，可以帮助你真实地了解自己对知识的理解并为考试做准备。要避免为了得到答案而匆忙回答问题的诱惑。一旦完成了每个章节的评估，参考答案不仅告诉你正确的答案，还会详细解释为什么这

个答案是正确的，而其他答案是错误的。

本书还包含一个由 39 个问题组成的自我评估考试，两个 50 个问题的练习考试，帮助你更好地准备考试。同时，抽认卡可帮助你学习和记忆准备考试所用到的关键信息。

《AWS 解决方案架构师学习与备考(第 3 版 • SAA-C02)》包含两部分内容：AWS 核心服务和良好架构的框架。

第 I 部分 AWS 核心服务

本书的第 I 部分“AWS 核心服务”深入研究了 AWS 的每个核心服务。这些服务包括你已经熟知的弹性计算云(Elastic Compute Cloud, EC2)、虚拟私有云(Virtual Private Cloud, VPC)、身份和访问管理(Identity and Access Management, IAM)、Route 53 和简单存储服务(Simple Storage Service, S3)等。

AWS 的一些服务看似相同，但通过学习你能够掌握这些服务之间的细微差别，更重要的是了解每种服务最适合应用的场景。

第 II 部分 良好架构的框架

本书的第 II 部分“良好架构的框架”由一组最佳实践及指导原则组成，帮助你在云中设计、实现和运营你所需的应用场景。这部分着重阐述了经过精心设计的五个方面：

- 可靠性
- 性能效率
- 安全性
- 成本优化
- 卓越运营

本书第 II 部分的每个章节都将和你一起重新审视 AWS 的核心服务。此外，因为并不是每个 AWS 服务都足以单独拿出来作为一个独立的章节，所以在这部分内容中，我们还引入了其他 AWS 服务，尽管这些服务可能不会被经常用到，但它们仍然会出现在考试中。

工作中，如何在上述五大部分取得最佳的平衡是作为解决方案架构师所必须掌握的关键技能。在开始学习第 II 部分内容之前，强烈推荐你仔细阅读《良好架构的框架白皮书》(*Well-Architected Framework white paper*)，该白皮书可以通过如下地址获取：
d0.awsstatic.com/whitepapers/architecture/AWS_Well-Architected_Framework.pdf。

本书将覆盖哪些内容

本书涵盖了准备 AWS 认证解决方案架构师助理级考试的相关内容：

第 1 章：云计算和 AWS 简介 该章提供 AWS 云计算平台与其核心服务及组件的概要性介绍。

第 2 章：Amazon 弹性计算云和 Amazon 弹性块存储 该章介绍在 AWS 上运行 Linux 和 Windows 工作负载的虚拟机技术——EC2 实例，以及 EC2 用于持久数据存储的弹性块存储服务。

第 3 章：AWS 存储 该章介绍 AWS 中的 S3(Simple Storage Service)和 Glacier 服务。这些服务为你的应用程序和互联网提供了无限制的数据存储服务。

第 4 章：Amazon 虚拟私有云 该章阐述 Amazon 虚拟私有云(Amazon VPC)。它是一个包含 AWS 服务所需网络资源的虚拟网络。

第 5 章：数据库服务 该章介绍 AWS 提供的一些托管数据库服务，包括关系数据库服务(RDS)、DynamoDB 和 Redshift。

第 6 章：认证和授权-AWS 身份和访问管理 该章介绍 AWS 身份和访问管理(IAM)，IAM 提供了保护账户中 AWS 资源的主要手段。

第 7 章：CloudTrail、CloudWatch 和 AWS Config 该章介绍如何监控和审计你的 AWS 资源。

第 8 章：域名系统和网络路由：Amazon Route 53 和 Amazon CloudFront 该章重点介绍域名系统(DNS)和 Route 53，该服务为内部 AWS 资源和互联网提供公共和私有 DNS 托管。该章还介绍 Amazon 的全球内容分发网络 CloudFront。

第 9 章：简单队列服务和 Kinesis 该章介绍如何使用简单队列服务(SQS)和 Kinesis 利用松耦合原理来创建可伸缩和高可用的应用程序。

第 10 章：可靠性支柱 该章展示如何构建和集成 AWS 服务，以实现应用程序的高可靠性。你将学习如何规划高可用性，并从不可避免的中断中进行恢复，以保持系统正常运行。

第 11 章：性能效率支柱 该章介绍如何构建高性能系统，以及如何使用 AWS 弹性基础设施来快速扩展以满足峰值需求。

第 12 章：安全性支柱 在该章，你将学习如何使用加密和安全控制来保护 AWS 上的数据和系统的机密性、完整性和可用性。你还将了解各种安全服务，如 GuardDuty、Inspector、Shield 和 Web 应用程序防火墙。

第 13 章：成本优化支柱 该章介绍如何预估和控制你在云中的成本。

第 14 章：卓越的运营支柱 在该章，你将学习如何让你的系统在 AWS 上平稳运行，以及如何使用 CloudFormation、Systems Manager 和 AWS 开发人员工具实现 DevOps 思维模式。

交互式在线学习环境和测试库

我们一直努力提供一些优秀的工具来帮助你完成认证考试。《AWS 解决方案架构师学习与备考(第 3 版·SAA-C02)》提供了交互式在线学习环境以及带有学习工具的

测试库，以帮助你准备认证考试，并增加你第一次通过的机会！该测试库的内容包括：

样题 本书提供的测试题将出现在前言部分的末尾以及每章末尾，此外，还有两个 50 题的练习考试。用这些问题测试你对学习与备考的了解程度。在线测试库可以运行在多个设备上。

抽认卡 在线文本库中有 100 张卡片，专门为强化你的记忆而设计，所以如果你一开始没有取得好成绩也不要气馁。这些卡片是为了确保你真正为考试做好了准备。不用担心，使用复习题、练习考试和抽认卡，当考试到来的时候，你会更有把握。问题以电子抽认卡格式提供(一个问题后面跟着一个正确答案)。可以使用抽认卡加强学习，并在考试前做最后的准备。

资源 你将从书中找到一些 AWS CLI 和其他代码的示例，可以复制并粘贴到自己的环境中使用。



注意：

访问 wiley.com/go/sybextestprep 进行注册并获得在线互动环境、测试库以及学习工具。

考试目标

AWS 认证解决方案架构师助理级(AWS Certified Solutions Architect – Associate)考试适用于具有在 AWS 平台上设计分布式系统及应用程序经验的人员。一般来说，在参加考试之前，你应该具备以下条件：

- 具有至少 1 年在 AWS 上进行系统设计的实践经验
 - 具有使用 AWS 提供的计算、网络、存储及数据库的实际操作经验
 - 基于客户的需求，利用架构设计原则为客户提供解决问题的能力
 - 提供实施指导的能力
 - 了解如何利用 AWS 的服务来满足特定技术需求
 - 了解良好的设计框架所涉及的五大主题
 - 了解 AWS 全球基础设施，包括用于连接它们的网络技术
 - 了解 AWS 安全服务以及它们如何与传统的本地安全基础设施集成
- 该考试涵盖 4 个不同的域，每个域都有不同的细分目标。

目标映射

下表列出了每个域及其在考试中的权重，以及书中涉及该域目标的章节。

域	考试占比/%	对应章节
域 1: 设计弹性架构	30	
1.1 设计多层体系结构解决方案		2, 3, 5, 8, 9, 10, 11
1.2 设计高可用性和容错架构		2, 3, 5, 7, 8, 9, 10, 11, 14
1.3 利用 AWS 服务设计解耦机制		4, 5, 9, 10, 11, 14
1.4 选择合适的弹性存储		2, 3, 5, 9, 10, 11
域 2: 设计高性能架构	28	
2.1 为工作负载确定弹性和可伸缩的计算解决方案		2, 3, 5, 7, 8, 9, 11
2.2 为工作负载选择高性能和可伸缩的存储解决方案		2, 3, 9, 11
2.3 为工作负载选择高性能的网络解决方案		5, 8, 9, 11
2.4 为工作负载选择高性能数据库解决方案		5, 11
域 3: 设计安全的应用程序和体系架构	24	
3.1 设计对 AWS 资源的安全访问		2, 3, 4, 6, 7, 12
3.2 设计安全的应用程序层		3, 6, 12
3.3 选择正确的数据安全选项		3, 4, 6, 7, 12
域 4: 设计成本优化的架构	18	
4.1 确定具有成本效益的存储解决方案		2, 3, 13
4.2 确定具有成本效益的计算和数据库服务		2, 13
4.3 设计成本优化的网络架构		8, 13

评估测试

- 判断题：开发者支持计划提供对支持应用程序编程接口(API)的访问。
 - 正确
 - 错误
- 判断题：AWS 负责管理 EC2 实例的网络配置。
 - 正确
 - 错误
- 以下哪个服务对分离单个应用程序的组件最有帮助？
 - SNS
 - KMS
 - SQS
 - Glacier
- 想要在 EC2 上运行的应用程序需要根据运行该程序的物理硬件 CPU 插槽数及核心数量购买软件使用许可。你应该指定以下哪一种 **tenancy** 模型？
 - 专用主机
 - 独立实例
 - 共享 **tenancy**
 - 提供你自己的软件许可
- 判断题：改变 EC2 实例的实例类型会改变其弹性 IP 地址。
 - 正确
 - 错误

6. 判断题: 可以使用 Quick Start AMI(Amazon Machine Image)创建任何实例类型。
 - A. 正确
 - B. 错误
7. 哪个 S3 加密选项不需要 AWS 持久地存储用于解密数据的密钥?
 - A. 客户端加密
 - B. SSE-KMS
 - C. SSE-S3
 - D. SSE-C
8. 判断题: 持久性指标用来显示特定对象在一年中不会被 AWS 在无意中丢失的可能性的百分比。
 - A. 正确
 - B. 错误
9. 判断题: 将一个新对象上传到 S3 后, 在对象可用之前会有一个轻微的延迟(1 到 2 秒)。
 - A. 正确
 - B. 错误
10. 使用 CIDR 块 10.0.0.0/24 创建 VPC。你需要从自己的内部网络连接到这个 VPC, 但是内部网络使用的 IP 地址和 CIDR 有重叠。下面哪项是解决这个问题的有效方法?
 - A. 删除 CIDR 并使用 IPv6
 - B. 更改 VPC 的 CIDR
 - C. 重新创建带有不同 CIDR 的 VPC
 - D. 为 VPC 创建第二个 CIDR
11. 判断题: EC2 实例必须在公共子网中才能访问 Internet。
 - A. 正确
 - B. 错误
12. 判断题: 公共子网的路由表中必须有指向 Internet 网关的默认路由作为目标。
 - A. 正确
 - B. 错误
13. 下面哪个场景适合 DynamoDB?
 - A. 在 AWS 上运行 MongoDB 数据库
 - B. 存储大小超过 1GB 的二进制文件
 - C. 存储具有一致结构的 JSON 文档
 - D. 为网站存储图像资产
14. 判断题: 你可以在任何时候为现有表创建 DynamoDB 全局二级索引。
 - A. 正确
 - B. 错误
15. 判断题: 启用时间点 RDS 快照足以提供小于 10 分钟的 RPO(Recovery Point Objective)。
 - A. 正确
 - B. 错误
16. 以下哪个步骤对保护你的 AWS 账户最有效?
 - A. 删除不再使用的 IAM (Identity and Access Management)策略
 - B. 取消对 IAM 用户不必要的访问授权
 - C. 轮换 root 访问密钥
 - D. 限制对 S3 存储桶的访问
 - E. 轮换 SSH 密钥对

17. 下面哪个选项可以用于加密 EC2 实例的操作系统?
- A. AWS Secrets Manager
 - B. CloudHSM
 - C. AWS 密钥管理服务(KMS)
 - D. AWS 安全令牌服务(STS)
18. AWS 安全令牌服务(STS)生成的令牌与 IAM 访问密钥有什么区别?
- A. 由 STS 生成的令牌不能被 IAM 主体使用
 - B. IAM 访问密钥是唯一的
 - C. 由 STS 生成的令牌只能使用一次
 - D. 由 STS 生成的令牌到期
19. 判断题: EC2 每 5 分钟向 CloudWatch 发送一次实例内存利用率指标。
- A. 正确
 - B. 错误
20. 你配置了一个 CloudWatch 告警来监控 EC2 实例的 CPU 利用率。告警从 INSUFFICIENT_DATA 状态开始, 然后进入 ALARM 状态。你能从中得出什么结论?
- A. 实例最近被重新启动过
 - B. CPU 利用率过高
 - C. CPU 利用率超过告警阈值
 - D. 实例被停止
21. AWS Config 和 CloudTrail 在哪里存储日志?
- A. S3 存储桶
 - B. CloudWatch 日志
 - C. CloudTrail 事件
 - D. DynamoDB
 - E. Amazon Athena
22. 判断题: 私有子网中的 EC2 实例可以为位于 Route 53 中的公共托管区域解析“A”资源记录。
- A. 正确
 - B. 错误
23. 你希望使用 Route 53 将用户发送到离他们最近的应用程序负载均衡器。下面哪个路由策略可以让你以最小的代价完成这一工作?
- A. 延迟路由
 - B. 地址位置路由
 - C. 地理位置感知路由
 - D. 边缘路由
24. 判断题: 你可以在 Route 53 中使用现有域名, 而不需要将其注册到 AWS。
- A. 正确
 - B. 错误
25. 你正在设计一个应用程序, 它可以将多个图像文件合并成一个视频文件, 供互联网用户下载。下面哪个选项可以帮助你以最快、最高可用性和最经济的方式快速实现应用程序?
- A. EC2 spot fleet
 - B. lambda
 - C. 关系数据库服务(RDS)
 - D. Auto Scaling
26. 你正在使用 EC2 Auto Scaling, 并希望实现一个仅在每个实例的平均 CPU 利用率超过 90%时才添加一个额外实例的扩展策略。但是, 你不希望它每 5 分钟添加一个以上的实例。你应该使用以下哪种扩展策略?
- A. Simple
 - B. Step
 - C. Target tracking
 - D. PercentChangeInCapacity

27. 判断题: EC2 Auto Scaling 会自动替换由 root 用户直接终止的组实例。
- A. 正确 B. 错误
28. 哪个 ElastiCache 引擎可以持久存储数据?
- A. MySQL B. Memcached
C. MongoDB D. Redis
29. 以下哪项不是 AWS 服务?
- A. CloudFormation B. Puppet
C. OpsWorks D. Snowball
30. 判断题: S3 跨区域复制使用传输加速。
- A. 正确 B. 错误
31. 你可以在账户中停用以下哪些服务?
- A. 安全令牌服务(STS) B. CloudWatch
C. 虚拟私有云(VPC) D. lambda
32. 以下哪项服务可以提醒你注意 EC2 实例上的恶意软件?
- A. AWS GuardDuty B. AWS Inspector
C. AWS Shield D. AWS Web 应用防火墙
33. 判断题: 如果在 S3 存储桶上启用了版本控制, 则对该存储桶中未加密的对象应用加密策略, 将创建该对象的新加密版本。
- A. 正确 B. 错误
34. 如果继续运行, 哪种实例类型将继续产生成本?
- A. Spot B. Standard reserved
C. On-demand D. Convertible reserved
35. 判断题: EBS Lifecycle Manager(生命周期管理)可以对曾经附加到终止实例的卷进行快照。
- A. 正确 B. 错误
36. 以下哪项使你能够最快地启动新的 Web 服务器?
- A. lambda B. Auto Scaling
C. 弹性容器服务 D. CloudFront
37. 判断题: CloudFormation 堆栈名称区分大小写。
- A. 正确 B. 错误
38. CodeDeploy 可以在哪里寻找 appspec.yml 文件? (选择两个)
- A. GitHub B. CodeCommit
C. S3 D. CloudFormation
39. 判断题: 可以使用 CodeDeploy 或 AWS Systems Manager 命令文档来部署 lambda 应用程序。
- A. 正确 B. 错误

评估测试答案

1. B: 商业计划提供对支持 API 的访问, 而开发者支持计划则不提供。有关更多信息, 请参见第 1 章。
2. B: 客户负责管理 EC2 实例的网络配置。AWS 负责物理网络基础结构。有关更多信息, 请参见第 1 章。
3. C: 简单队列服务(SQS)允许在分布式系统中进行事件驱动的消息传递, 这些消息可以在协调较大过程的离散步骤时分离。有关更多信息, 请参见第 1 章。
4. A: “专用主机”选项可让你查看主机上的物理 CPU 插槽和核心数。有关更多信息, 请参见第 2 章。
5. B: 弹性 IP 地址不会更改。如果实例停止, 则附加到实例的公共 IP 地址也会更改, 就像更改实例类型时一样。有关更多信息, 请参见第 2 章。
6. A: Quick Start AMI 与实例类型无关。有关更多信息, 请参见第 2 章。
7. D: 使用 SSE-C, 你可以为 Amazon 提供自己的密钥, 以用于解密和加密数据。AWS 不会永久存储密钥。有关更多信息, 请参见第 3 章。
8. A: 持久性对应于存储在 S3 上的对象的平均每年预期损失, 不包括你删除的对象。可用性衡量 S3 用于检索这些对象的可用时间。更多信息见第 3 章。
9. B: S3 对新对象使用写入后读取一致性模型, 因此, 一旦将对象上传到 S3, 即可立即使用。有关更多信息, 请参见第 3 章。
10. C: 你无法更改 VPC 的主要 CIDR, 因此必须创建一个新的 CIDR 才能将其连接到内部网络。有关更多信息, 请参见第 4 章。
11. B: EC2 实例可以从私有子网访问 Internet, 只要它使用 NAT 网关或 NAT 实例。更多信息见第 4 章。
12. A: 公共子网的定义是具有默认路由的子网, 该默认路由指向 Internet 网关作为目标。否则, 它是一个私有子网。有关更多信息, 请参见第 4 章。
13. C: DynamoDB 是一个键值存储, 可用于存储最大 400 KB 的条目。有关更多信息, 请参见第 5 章。
14. A: 你可以随时为现有表创建全局二级索引。只有在创建表时才能创建本地二级索引。有关更多信息, 请参见第 5 章。
15. A: 启用时间点恢复可为你提供大约 5 分钟的 RPO。恢复时间目标(RTO)取决于要还原的数据量。有关更多信息, 请参见第 5 章。
16. B: 对于保护你的 AWS 账户, 列出的措施中最有效的方法是撤销 IAM 用户的不必要访问权限。有关更多信息, 请参见第 6 章。
17. C: KMS 可用于加密存储实例操作系统的弹性块存储(EBS)卷。有关更多信息, 请参见第 6 章。
18. D: STS 令牌到期, 而 IAM 访问密钥未到期。STS 令牌可以多次使用。IAM

访问密钥和 STS 令牌都是唯一的。IAM 主体可以使用 STS 令牌。有关更多信息, 请参见第 6 章。

19. B: EC2 不会跟踪实例的内存利用率。有关更多信息, 请参见第 7 章。

20. C: 转换为 ALARM 状态仅表示指标已超过阈值, 但没有告诉你阈值是什么。新创建的告警以 INSUFFICIENT_DATA 状态开始。有关更多信息, 请参见第 7 章。

21. A: 两者都将日志存储在 S3 存储桶中。有关更多信息, 请参见第 7 章。

22. A: 私有子网中的 EC2 实例仍然可以访问 Amazon 的私有 DNS 服务器, 该服务器可以解析存储在公共托管区域中的记录。有关更多信息, 请参见第 8 章。

23. C: 地理位置感知路由会将用户路由到最接近他们的位置。地理位置路由要求你创建特定位置的记录或创建默认记录。有关更多信息, 请参见第 8 章。

24. A: Route 53 是真正的 DNS 服务, 因为它可以托管任何区域的域名。你可以注册域名或者转移域名到 Route 53。有关更多信息, 请参见第 8 章。

25. B: lambda 是一个高度可用、可靠的“无服务器”计算平台, 可根据需要启动并进行弹性扩展以满足需求。EC2 竞价实例可能在短时间内被关闭。有关更多信息, 请参见第 10 章。

26. A: 一个简单的扩展策略会更改组的大小, 再次更改之前会进入一个冷却期。步进扩展策略没有冷却时间。目标跟踪策略尝试将指标保持在设定值。PercentChangeInCapacity 是简单的缩放调整类型, 而不是缩放策略。有关更多信息, 请参见第 10 章。

27. A: EC2 Auto Scaling 始终尝试保持最小的组大小, 或者保持所需容量(如果已设置)。有关更多信息, 请参见第 10 章。

28. D: ElastiCache 支持 Memcached 和 Redis, 但只有后者可以持久存储数据。有关更多信息, 请参见第 11 章。

29. B: Puppet 是 AWS 通过 OpsWorks 提供的配置管理平台, 但它本身并不是 AWS 服务。有关更多信息, 请参见第 11 章。

30. B: S3 跨区域复制在不同存储桶之间传输对象。传输加速使用 CloudFront 边缘位置来加速 S3 和 Internet 之间的传输。有关更多信息, 请参见第 11 章。

31. A: 你可以为除美国东部以外的所有地区停用 STS。有关更多信息, 请参见第 12 章。

32. A: GuardDuty 寻找潜在的恶意活动。Inspector 寻找可能导致妥协的漏洞。Shield 和 Web 应用防火墙可保护应用程序免受攻击。有关更多信息, 请参见第 12 章。

33. A: 对未加密的对象应用加密将创建该对象的新的加密版本。以前的版本保持未加密状态。有关更多信息, 请参见第 12 章。

34. C: 按需实例将继续运行并产生费用。预留实例的运行或停止费用相同。当前竞价实例价格超过你的出价时, 竞价实例将被终止。有关更多信息, 请参见第 13 章。

35. A: EBS Lifecycle Manager 可以创建任何 EBS 卷的计划快照, 而不管附加状态如何。有关更多信息, 请参见第 13 章。

36. C: 弹性容器服务使你可以运行能够在几秒钟内启动的容器。EC2实例花费的时间会更长。`lambda`是“无服务器的”，因此你不能使用它运行 Web 服务器。`CloudFront`提供缓存，但不是 Web 服务器。有关更多信息，请参见第 13 章。

37. A: `CloudFormation` 中的几乎所有内容都区分大小写。有关更多信息，请参见第 14 章。

38. A 和 C: `CodeDeploy` 查找包含要部署的应用程序的 `appspec.yml` 文件，该文件可以存储在 S3 或 GitHub 上。有关更多信息，请参见第 14 章。

39. B: 可以使用 `CodeDeploy` 将应用程序部署到 `lambda` 或 EC2 实例上。但是，`AWS Systems Manager` 命令文档仅适用于 EC2 实例。有关更多信息，请参见第 14 章。

第 I 部分 AWS 核心服务

第 1 章 云计算和 AWS 简介	3
1.1 云计算与虚拟化	3
1.1.1 云计算架构	4
1.1.2 云计算优化	4
1.2 AWS 云	5
1.3 AWS 平台架构	8
1.4 AWS 可靠性和合规性	10
1.4.1 AWS 责任共担模式	10
1.4.2 AWS 服务级别协议	11
1.5 使用 AWS	11
1.5.1 AWS CLI	11
1.5.2 AWS SDK	11
1.5.3 技术支持和在线资源	12
1.5.4 支持计划	12
1.5.5 其他支持资源	12
1.6 本章小结	13
1.7 考试要点	13
1.8 习题	14

第 2 章 Amazon 弹性计算云和 Amazon 弹性块存储	17
2.1 本章简介	17
2.2 EC2 实例	18
2.2.1 配置实例	18
2.2.2 配置实例行为	22
2.2.3 放置组	23
2.2.4 实例价格	23
2.2.5 实例的生命周期	24

2.2.6 资源标签	25
2.2.7 服务限制	25
2.3 EC2 存储卷	26
2.3.1 弹性块存储卷	26
2.3.2 实例存储卷	28
2.4 访问你的 EC2 实例	28
2.5 保护你的 EC2 实例	30
2.5.1 安全组	30
2.5.2 IAM 角色	30
2.5.3 NAT 设备	31
2.5.4 密钥对	31
2.6 EC2 Auto Scaling	32
2.6.1 启动配置	32
2.6.2 启动模板	32
2.6.3 Auto Scaling Group	33
2.6.4 Auto Scaling 选项	35
2.7 AWS Systems Manager	38
2.7.1 操作	39
2.7.2 洞察	41
2.8 AWS CLI 示例	42
2.9 本章小结	43
2.10 考试要点	44
2.11 习题	45

第 3 章 AWS 存储	49
3.1 本章简介	49
3.2 S3 服务架构	50
3.2.1 前缀和分隔符	50
3.2.2 处理大对象	51
3.2.3 加密	52
3.2.4 日志记录	52

3.3 S3 持久性和可用性	53	4.5 Internet 网关	77
3.3.1 持久性	53	4.6 路由表	78
3.3.2 可用性	54	4.6.1 路由	78
3.3.3 最终一致性数据	54	4.6.2 默认路由	79
3.4 S3 对象生命周期	54	4.7 安全组	81
3.4.1 版本控制	55	4.7.1 入站规则	81
3.4.2 生命周期管理	55	4.7.2 出站规则	82
3.5 访问 S3 对象	56	4.7.3 源端和目标端	82
3.5.1 访问控制	56	4.7.4 状态防火墙	83
3.5.2 预签名的 URL	57	4.7.5 默认安全组	83
3.5.3 静态网站	58	4.8 网络访问控制列表	84
3.6 Amazon S3 Glacier	59	4.8.1 入站规则	84
3.7 其他存储相关的服务	61	4.8.2 出站规则	87
3.7.1 Amazon 弹性文件 系统	61	4.8.3 同时使用网络访问 控制列表和安全组	88
3.7.2 Amazon FSx	61	4.9 公共 IP 地址	88
3.7.3 AWS 存储网关	61	4.10 弹性 IP 地址	89
3.7.4 AWS Snowball	61	4.11 AWS 全局加速器	91
3.7.5 AWS DataSync	62	4.12 网络地址转换	91
3.8 AWS CLI 示例	62	4.13 网络地址转换设备	92
3.9 本章小结	63	4.13.1 配置路由表来使用 NAT 设备	93
3.10 考试要点	64	4.13.2 NAT 网关	94
3.11 习题	64	4.13.3 NAT 实例	94
第 4 章 Amazon 虚拟私有云	69	4.14 VPC 对等(VPC Peering)	95
4.1 本章介绍	69	4.15 混合云网络	95
4.2 VPC CIDR 块	69	4.15.1 虚拟专用网(VPN)	96
4.2.1 次级 CIDR 块	70	4.15.2 AWS 中转网关	96
4.2.2 IPv6 CIDR 块	70	4.15.3 AWS Direct Connect	102
4.3 子网	72	4.16 高性能计算	103
4.3.1 子网 CIDR 块	72	4.16.1 Elastic Fabric Adapter	104
4.3.2 可用区域	73	4.16.2 AWS 并行集群(AWS ParallelCluster)	104
4.3.3 IPv6 CIDR 块	75	4.17 本章小结	105
4.4 弹性网络接口	75	4.18 考试要点	105
4.4.1 主/备私有 IP 地址	76	4.19 习题	106
4.4.2 绑定弹性网络接口	76		
4.4.3 增强的网络	77		

第 5 章 数据库服务111	
5.1 本章介绍111	
5.2 关系数据库 112	
5.2.1 字段和属性 112	
5.2.2 使用多个表 112	
5.2.3 结构化查询语言 113	
5.2.4 在线事务处理和在线 分析处理 114	
5.3 Amazon 关系数据库服务..... 114	
5.3.1 数据库引擎 115	
5.3.2 软件许可事项 116	
5.3.3 数据库选件组 116	
5.3.4 数据库实例类 116	
5.3.5 存储 117	
5.3.6 读取副本 120	
5.3.7 高可用性(多个 AZ)..... 121	
5.3.8 单主机集群(Single- Master) 122	
5.3.9 多主机集群(Multi- Master) 123	
5.3.10 备份和恢复 123	
5.3.11 自动快照 123	
5.3.12 维护项目 124	
5.4 Amazon Redshift 124	
5.4.1 计算节点 124	
5.4.2 数据分布类型 125	
5.4.3 Redshift Spectrum 125	
5.4.4 AWS 数据库迁移 服务 125	
5.5 非关系数据库(NoSQL) 126	
5.5.1 存储数据 126	
5.5.2 查询数据 126	
5.5.3 非关系数据库的 类型 127	
5.6 DynamoDB 127	
5.6.1 分区和哈希键 127	
5.6.2 属性和条目 128	
5.6.3 吞吐能力..... 129	
5.6.4 读取数据..... 131	
5.6.5 全局表..... 132	
5.6.6 备份..... 132	
5.7 本章小结 132	
5.8 考试要点 133	
5.9 习题 133	
第 6 章 认证和授权——AWS 身份和 访问管理137	
6.1 本章介绍 137	
6.2 IAM 身份 138	
6.2.1 IAM 策略 138	
6.2.2 用户和 root 账户 139	
6.2.3 访问密钥..... 141	
6.2.4 用户组..... 142	
6.2.5 角色..... 143	
6.3 身份验证工具 144	
6.3.1 Amazon Cognito 144	
6.3.2 AWS 托管的 Microsoft AD 144	
6.3.3 AWS 单点登录 145	
6.3.4 AWS 密钥管理服务 (KMS) 145	
6.3.5 AWS 凭据管理器 145	
6.3.6 AWS CloudHSM..... 145	
6.4 AWS CLI 的示例 146	
6.5 本章小结 147	
6.6 考试要点 147	
6.7 习题 148	
第 7 章 CloudTrail、CloudWatch 和 AWS Config153	
7.1 本章介绍 153	
7.2 CloudTrail 154	
7.2.1 管理事件..... 154	
7.2.2 数据事件..... 155	
7.2.3 事件历史..... 155	

7.2.4	跟踪	155
7.2.5	日志文件完整性 验证	157
7.3	CloudWatch	158
7.3.1	CloudWatch 指标	158
7.3.2	指标的图形化	160
7.3.3	指标数学	161
7.3.4	CloudWatch Logs	163
7.3.5	CloudWatch 告警	165
7.3.6	Amazon EventBridge	168
7.4	AWS Config	169
7.4.1	配置记录器	169
7.4.2	配置项	170
7.4.3	配置历史	170
7.4.4	配置快照	170
7.4.5	监视变更	171
7.5	本章小结	172
7.6	考试要点	173
7.7	习题	173
第 8 章	域名系统和网络路由: Amazon Route 53 和 Amazon CloudFront	177
8.1	本章介绍	177
8.2	域名系统	178
8.2.1	名称空间	178
8.2.2	名称服务器	178
8.2.3	域和域名	179
8.2.4	域名注册	179
8.2.5	域名层级	179
8.2.6	完全限定域名	180
8.2.7	区域和区域文件	180
8.2.8	记录类型	180
8.2.9	别名记录	181
8.3	Amazon Route 53	181
8.3.1	域名注册	181
8.3.2	DNS 管理	182

8.3.3	可用性监控	183
8.3.4	路由策略	184
8.3.5	Traffic Flow	186
8.3.6	Route 53 解析器	187
8.4	Amazon CloudFront	187
8.5	AWS CLI 示例	188
8.6	本章小结	189
8.7	考试要点	189
8.8	习题	190
第 9 章	简单队列服务和 Kinesis	193
9.1	本章简介	193
9.2	简单队列服务	193
9.2.1	队列	194
9.2.2	队列类型	195
9.2.3	轮询	195
9.2.4	死信队列	196
9.3	Kinesis	196
9.3.1	Kinesis 视频流	196
9.3.2	Kinesis 数据流	197
9.3.3	Kinesis 数据管道	198
9.3.4	Kinesis 数据管道和 Kinesis 数据流	198
9.4	本章小结	199
9.5	考试要点	199
9.6	习题	199

第 II 部分 良好架构的框架

第 10 章	可靠性支柱	205
10.1	本章介绍	205
10.2	计算可用性	206
10.2.1	传统应用程序和云原生应用程序的可用性 差异	206
10.2.2	了解你的限制	209
10.2.3	提高可用性	209
10.3	EC2 Auto Scaling	209

10.3.1	启动配置	210	11.4.2	可视化	240
10.3.2	启动模板	210	11.5	优化数据操作	241
10.3.3	Auto Scaling 组	211	11.5.1	缓存	241
10.3.4	Auto Scaling 选项	212	11.5.2	分区与分片	243
10.4	数据备份和恢复	216	11.5.3	压缩	243
10.4.1	S3	216	11.6	本章小结	244
10.4.2	弹性文件系统	217	11.7	考试要点	244
10.4.3	弹性块存储	217	11.8	习题	245
10.4.4	数据库弹性	217	第 12 章	安全性支柱	249
10.5	创建弹性网络	218	12.1	本章介绍	249
10.5.1	VPC 设计注意事项	218	12.2	身份和访问管理	249
10.5.2	外部连接	219	12.2.1	保护 AWS 凭证	250
10.6	可用性设计	219	12.2.2	细粒度授权	250
10.6.1	设计 99%可用性	220	12.2.3	权限边界	251
10.6.2	设计 99.9%可用性	221	12.2.4	角色	253
10.6.3	设计 99.99%可用性	222	12.2.5	实施服务水平的保护	258
10.7	本章小结	223	12.3	安全调查控制	258
10.8	考试要点	223	12.3.1	CloudTrail	258
10.9	习题	224	12.3.2	CloudWatch Logs	259
第 11 章	性能效率支柱	227	12.3.3	使用 Athena 检索日志	260
11.1	本章简介	227	12.3.4	使用 AWS Config 审核资源配置	261
11.2	优化 AWS 核心服务性能	228	12.3.5	Amazon GuardDuty	263
11.2.1	计算	228	12.3.6	Amazon Inspector	264
11.2.2	存储	231	12.3.7	Amazon Detective	265
11.2.3	数据库	234	12.3.8	Security Hub	265
11.2.4	网络优化和负载均衡	235	12.4	保护网络边界	266
11.3	基础设施自动化	237	12.4.1	网络访问控制列表和安全组	266
11.3.1	CloudFormation	237	12.4.2	AWS Web 应用防火墙	266
11.3.2	第三方自动化解决方案	238	12.4.3	AWS Shield	267
11.4	审查和优化基础设施配置	239	12.5	数据加密	267
11.4.1	负载测试	239	12.5.1	静态数据	267

12.5.2	传输中的数据	269	14.2.5	防止更新特定资源	294
12.5.3	Macie	269	14.2.6	覆盖堆栈策略	295
12.6	本章小结	269	14.3	CodeCommit	295
12.7	考试要点	270	14.3.1	创建存储库	296
12.8	习题	270	14.3.2	存储库安全	296
第 13 章	成本优化支柱	275	14.3.3	使用 Git 与存储库交互	297
13.1	本章介绍	275	14.4	CodeDeploy	299
13.2	计划、跟踪和控制成本	275	14.4.1	CodeDeploy 代理	299
13.2.1	AWS Budgets	276	14.4.2	部署	299
13.2.2	监控工具	277	14.4.3	部署组	300
13.2.3	AWS Organizations	278	14.4.4	部署类型	300
13.2.4	AWS Trusted Advisor	278	14.4.5	部署配置	301
13.2.5	在线计算工具	279	14.4.6	生命周期事件	301
13.3	成本优化的计算	281	14.4.7	应用程序规范文件	302
13.3.1	最大化服务器密度	281	14.4.8	触发器和告警	303
13.3.2	EC2 预留实例	281	14.4.9	回滚	303
13.3.3	EC2 竞价实例	283	14.5	CodePipeline	303
13.3.4	Auto Scaling	284	14.5.1	持续集成(CI)	304
13.3.5	弹性块存储生命周期管理	285	14.5.2	持续交付(CD)	304
13.4	本章小结	285	14.5.3	创建 pipeline	304
13.5	考试要点	285	14.5.4	artifact	306
13.6	习题	286	14.6	AWS Systems Manager	306
第 14 章	卓越的运营支柱	289	14.6.1	操作	307
14.1	本章介绍	289	14.6.2	洞察	309
14.2	CloudFormation	289	14.7	AWS Landing Zone	310
14.2.1	创建堆栈	290	14.8	本章小结	311
14.2.2	删除堆栈	291	14.9	考试要点	311
14.2.3	使用多个堆栈	291	14.10	习题	312
14.2.4	堆栈更新	293	附录	习题解答	315

第 I 部分

AWS 核心服务

云计算和 AWS 简介

如今，云计算是许多重要技术创新和成长的土壤，Amazon Web Services(AWS)与其他任何平台相比，无疑是企业和用户工作负载的首选平台。如果你想成为 AWS 解决方案架构师，首先需要真正了解云计算以及 Amazon 的云计算工作原理。

为确保你对云计算有宏观的了解，本章将介绍如下基本知识：

- 云计算与其他应用程序及客户机-服务器模式的区别
- AWS 平台如何为你的资源提供安全灵活的虚拟网络环境
- AWS 如何提供超高的服务可靠性
- 如何访问和管理基于 AWS 的资源
- 可以在何处获取文档并为你的 AWS 部署提供帮助

1.1 云计算与虚拟化

所有云操作的核心技术都是虚拟化。如图 1-1 所示，虚拟化是将单个物理服务器的硬件资源划分为较小的单元。因此，该物理服务器可以托管并运行具有各自完整操作系统的多个虚拟机(Virtual Machine, VM)，每个虚拟机都具有自己的内存、存储和网络访问权限。

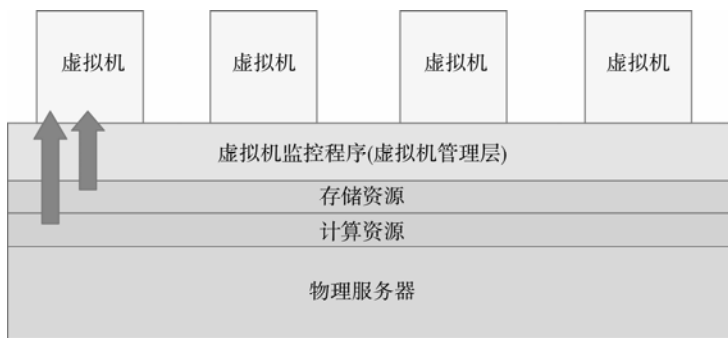


图 1-1 虚拟主机

利用虚拟化的灵活性，在几秒钟之内即可创建虚拟服务器，使你可以根据项目需求的时间点创建虚拟机，并在使用后将其删除。被释放的资源将立即进行回收，并可用于其他工作负载。通过采用灵活的管理方式，可以从硬件资源中获取最大的价值，并可以轻松地生成实验环境和沙箱环境。

1.1.1 云计算架构

像 AWS 这样的主流云服务商都拥有庞大的服务器资源，其维护着成千上万台服务器和存储设备以及连接它们所需的网络环境。精心构建的虚拟化环境可以将存储、内存、计算和网络带宽等资源以最有效的方式进行组合，从而可以快速为你提供虚拟主机。

云计算平台提供对计算资源池的按需自助服务访问，并根据使用量进行计量和收费。云计算系统使用精确的计费模型，有时一小时的花费只需要几分钱。

1.1.2 云计算优化

对于许多繁重的工作负载，使用云计算环境是一个不错的选择，因为它具有良好的可伸缩性，而且通常比传统方案提供更低的成本。想实现有效的部署配置，需要掌握以下三方面知识。

可伸缩性

在可伸缩的基础架构中，可以通过自动添加资源来有效满足应用程序意外增长的需求。如图 1-2 所示，这通常意味着动态地增加正在运行的虚拟机(或 AWS 称其为实例)的数量。

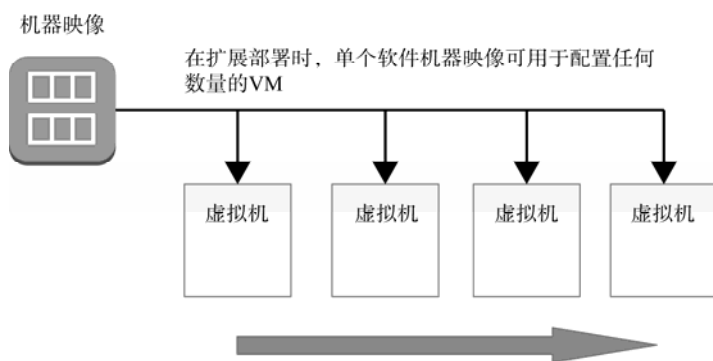


图 1-2 机器映像的副本会在启动时应用到新的 VM 中

AWS 提供了 Auto Scaling 服务。该服务可以使用预定义的机器映像，在必要时自动使用这些映像启动多个实例，从而满足用户增加的工作负载需求。

弹性

弹性原则涵盖了与可伸缩性相同的某些方面，两者都解决了系统如何面对不断变化的需求。在可伸缩环境中，当工作负载的需求增加时，可以通过预定义的机器映像创建更多的实例来满足需求。但是弹性的基础架构可以在需求下降时自动减少资源的使用。由于可以根据工作负载的需求增加或减少资源的数量，因此可以带来更好的成本效益。

成本管理

除了通过持续关注你所使用的资源来控制成本外，云计算还可以将 IT 支出从资本支出(CAPEX)架构转变为更接近运营支出(OPEX)的方式。

实际上，这意味着你不再需要为部署的每台新服务器预先花费 10 000 美元，也不用再关心电力、散热、安全防护以及机架空间等成本。取而代之的是，当需要运行应用程序时，只需要花费与之前自建环境相比微不足道的费用，就可以快速获得所需资源。

虽然当你长期使用云端作为基础设施环境的OPEX 不一定会一直低于你在数据中心自建的基础环境，但如果使用云端环境，从长期看，你不必担心基础设置资源不足的情况发生。同时，硬件环境不断进化，AWS可以在非常短的时间内，即可为用户提供最新的硬件环境，而这是传统自建环境无法做到的。

为了帮助你更好地理解云计算支出的全部内容，AWS 在 aws.amazon.com/tco-calculator 上提供了免费的总成本(TCO)计算器。该计算器可帮助你当前数据中心的成本与在 AWS 上使用相同资源所需的成本之间进行详细的逐条比较。

1.2 AWS 云

时刻关注 AWS 控制台中不断推出的新服务可能让人觉得力不从心，但是作为解决方案架构师，你应该将关注的重点放在核心服务类别上。本节将简要总结每个核心类别及其核心服务(如表 1-1 所示)。在本书的其他部分，你将学到更多关于所有这些服务的知识，请重点关注这些内容的定义，因为它们是你将要学习的所有其他内容的基础。

表 1-1 AWS 服务类别

类别	功能
计算	将传统的本地物理服务器上的角色复制到云上的服务，提供高级配置，包括 Auto Scaling、负载均衡，甚至是无服务器架构(一种以极小的占用空间提供服务器功能的函数)
网络	应用程序连接、访问控制和增强的远程连接
存储	各种存储平台，旨在满足用户即时访问以及长期备份的需求
数据库	适用于需要多种数据格式用例的托管数据解决方案，包括关系数据库、NoSQL 以及缓存
应用管理	监视、审计和配置 AWS 账户服务以及其中运行的资源
安全及身份管理	用于管理验证和授权，数据和连接加密，以及与第三方身份验证管理系统集成的服务

表 1-2 按类别列出了一些常用的 AWS 核心服务的功能。

表 1-2 AWS 核心服务(按类别)

类别	服务	功能
计算	弹性计算云(EC2)	EC2 服务器实例提供了在本地数据中心运行的服务器的虚拟版本。EC2 实例可以配置 CPU、内存、存储和网络接口配置文件，从而满足任何应用程序的需求，从简单的 Web 服务器到集成多层架构的实例集群。由于 EC2 实例是虚拟的，因此它们的资源效率更高，而且几乎可以进行实时部署
	lambda	Amazon 的 lambda 服务提供的无服务器应用程序体系结构，允许你使用面向公共的响应性服务，而不需要一个实际全天候运行的服务器。网络事件(如客户请求)可以触发执行基于代码的预定义操作。当操作(持续运行长达 15 分钟)完成时，lambda 事件结束，所有资源将自动关闭并释放
	Auto Scaling	运行的 EC2 实例可以生成自定义映像，并在现有实例不能满足客户需求时自动启动新的实例(或扩展)。随着需求下降，终止(或缩小)未被使用的实例，从而在满足用户需求的同时降低运行成本
	弹性负载均衡	可以将传入的网络流量定向到多个 Web 服务器中，以确保不会出现单个服务器负载过高，而其他服务器负载过低的情况。同时，可以保证流量不会被发送到发生故障的服务器
	弹性 Beanstalk	Beanstalk 是一项托管服务，用于抽象化 AWS 计算和网络基础架构的配置。你只需要推送应用程序代码即可，Beanstalk 会在后台自动启动和管理所有必要的服务
网络	虚拟私有云 (Virtual Private Cloud, VPC)	VPC 是高度可配置的网络环境，旨在承载你的 EC2(以及 RDS)实例。可以使用基于 VPC 的工具保护你的实例，也可以通过严格控制入站和出站网络访问对实例进行隔离，从而提高安全性
	Direct Connect	由第三方网络服务商提供的与 AWS 网络进行安全快速的网络连接。通过 Direct Connect，可以在本地数据中心或办公室与 AWS 的 VPC 之间建立增强型直连隧道
	Route 53	Route 53 是 AWS 的 DNS 服务，为你提供域名管理与注册、记录管理、路由协议以及健康状况检查，这些都与其他 AWS 资源完全集成

(续表)

类别	服务	功能
网络	CloudFront	CloudFront 是 Amazon 的分布式全球内容交付网络 (CDN)。当你正确配置 CloudFront 之后, CloudFront 可以将你网站内容的缓存版本存储在世界各地的边缘位置, 从而通过最高的访问效率和最低的延迟将它们交付给客户
存储	简单存储服务 (Simple Storage Service, S3)	S3 提供了高度通用、性能可靠且价格低廉的对象存储, 非常适合数据存储与备份。在大型的 AWS 生产过程中, 经常使用 S3 存储脚本、模板、日志文件等数据
	S3 Glacier	当需要以更低的成本长期存储大型归档数据, 并可以接受数小时的检索延迟时, 使用 S3 Glacier 是一个非常明智的选择, 并且 S3 Glacier 的生命周期管理与 S3 紧密集成
	弹性块存储 (Elastic Block Store, EBS)	EBS 提供了可持久使用的虚拟存储驱动器, 用于存储 EC2 实例的操作系统和工作数据。它们旨在模拟物理服务器上附加的存储驱动器和分区的功能
	存储网关(Storage Gateway)	Storage Gateway 是一个混合存储系统, 可以将 AWS 云存储作为本地存储设备使用。Storage Gateway 被认为是数据迁移、数据备份以及灾难恢复操作的绝佳工具
数据库	关系数据库服务 (Relational Database Service, RDS)	RDS 是一项 AWS 托管服务, 可为你构建稳定、安全、可靠的数据库实例。可以在 RDS 上运行各种 SQL 数据库引擎, 包括 MySQL、Microsoft SQL Server、Oracle 和 Amazon 自己的 Aurora
	DynamoDB	DynamoDB 是 AWS 的一项托管服务, 可用于快速、灵活、高度可伸缩的非关系数据库 (NoSQL) 工作负载
应用管理	CloudWatch	可以使用 CloudWatch 监视性能和资源利用率, 并在达到预设阈值时向你发送消息或触发自动响应操作
	CloudFormation	通过此服务, 可以使用模板文件定义完整的复杂 AWS 部署过程。可以通过编写脚本来使用任何 AWS 资源及功能, 通过 CloudFormation 可以更轻松地自动化、标准化和加速应用程序部署过程
	CloudTrail	CloudTrail 会收集你所有账户的 API 事件记录。这些记录将有助于账户审计和故障排查
	Config	Config 服务旨在帮助你进行 AWS 账户的变更管理及进行合规性检查。首先定义所需的配置状态基线, 然后 Config 将根据该基线, 在未来对资源状态进行评估。当配置与基线有较大差距时, 系统将向你发出通知或告警

(续表)

类别	服务	功能
安全及身份管理	身份和访问管理 (Identity and Access Management, IAM)	IAM 可以用来管理用户及应用程序的访问, 以及对你的 AWS 账户进行身份验证。通过使用用户、组、角色和策略, 可以精准地控制访问及使用 AWS 资源的人员和对象
	密钥管理服务 (Key Management Service, KMS)	KMS 是一项托管服务, 可以管理加密密钥的创建及使用, 从而保护由你的 AWS 资源所使用的数据以及其他相关数据的安全
应用整合	目录服务	对于需要管理身份和关系的 AWS 环境, 目录服务可以将 AWS 资源与身份提供商 (例如 Amazon Cognito 和 Microsoft AD 域) 进行集成
	简单通知服务 (Simple Notification Service, SNS)	SNS 是一种通知工具, 可以自动将告警主题发布到其他服务 (如发布到 SQS 队列或触发 lambda 函数)、移动设备或电子邮件及短消息
	简单工作流 (Simple WorkFlow, SWF)	SWF 可以帮助你协调那些在 AWS 中需要按照特定顺序执行的 AWS 服务作业, 它是在云中完全托管的状态跟踪器和任务协调器
	简单队列服务 (Simple Queue Service, SQS)	SQS 允许在分布式系统中进行事件驱动的消息传递, 这些消息可以解耦, 同时可以用于协调较大过程的离散步骤。SQS 消息中包含的数据会被可靠地传输, 从而提高应用程序的容错能力
	API 网关	通过这个服务, 可以为基于 AWS 的应用程序创建和管理安全可靠的 API

1.3 AWS 平台架构

AWS 拥有全球范围内的数据中心。由于这些数据中心分布非常广泛, 因此可以通过在地理上靠近用户的位置托管你的工作负载, 从而减少网络传输延迟。它还可满足你对合规性的要求, 例如某些法规要求你将数据保留在特定的法律管辖范围内。

AWS 按照区域 (Region) 对数据中心进行管理和运营, 目前 AWS 在全球运营 21 个数据中心 (这不包括美国政府专用的 AWS GovCloud 区域), 并且这个数字在不断增长。在启动新的 AWS 资源时, 务必了解所选区域的重要性; 在不同区域中, 价格和服务可用性可能会有所不同。表 1-3 列出了所有 21 个 (非政府) 地区的数据中心, 以及每个地区的名称和核心端点地址。请注意, 访问和认证两个中国区域的数据中心需要单独的协议。

表 1-3 公开访问的 AWS 区域列表

区域名称	区域	端点地址
美国东都(俄亥俄)	us-east-2	us-east-2.amazonaws.com
美国西部(北加利福尼亚)	us-west-1	us-west-1.amazonaws.com
美国西部(俄勒冈)	us-west-2	us-west-2.amazonaws.com
亚太地区(中国香港)	ap-east-1	ap-east-1.amazonaws.com
亚太地区(孟买)	ap-south-1	ap-south-1.amazonaws.com
亚太地区(首尔)	ap-northeast-2	ap-northeast-2.amazonaws.com
亚太地区(大阪本地)	ap-northeast-3	ap-northeast-3.amazonaws.com
亚太地区(新加坡)	ap-southeast-1	ap-southeast-1.amazonaws.com
亚太地区(悉尼)	ap-southeast-2	ap-southeast-2.amazonaws.com
亚太地区(东京)	ap-northeast-1	ap-northeast-1.amazonaws.com
加拿大(中部)	ca-central-1	ca-central-1.amazonaws.com
中国(北京)	cn-north-1	cn-north-1.amazonaws.com.cn
中国(宁夏)	cn-northwest-1	cn-northwest-1.amazonaws.com.cn
欧洲(法兰克福)	eu-central-1	eu-central-1.amazonaws.com
欧洲(爱尔兰)	eu-west-1	eu-west-1.amazonaws.com
欧洲(伦敦)	eu-west-2	eu-west-2.amazonaws.com
欧洲(巴黎)	eu-west-3	eu-west-3.amazonaws.com
欧洲(斯德哥尔摩)	eu-north-1	eu-north-1.amazonaws.com
中东(巴林)	me-south-1	me-south-1.amazonaws.com

**注意：**

端点地址用于从应用程序代码或脚本内部远程访问你的 AWS 资源。诸如 ec2、apigateway 或 cloudformation 的前缀通常会添加到端点，用来指定特定的 AWS 服务，例如 cloudformation.us-east-2.amazonaws.com。可以在 docs.aws.amazon.com/general/latest/gr/rande.html 上查看端点地址及其前缀的完整列表。

由于低延迟访问非常重要，因此可以选择指定的边缘网络位置来提供某些 AWS 服务。这些服务包括 Amazon CloudFront、Amazon Route 53、AWS 防火墙管理器、AWS Shield 和 AWS WAF。有关可用位置的完整和最新列表，请参见 aws.amazon.com/about-aws/global-infrastructure/regional-product-services。

AWS 物理数据中心在你的 AWS 账户中显示为可用区域(Availability Zones, AZ)。一个区域(region)内可能有 6 个可用区域，例如 us-east-1a 和 us-east-1b，每个可用区域包含一个或多个数据中心。

可以从一个或多个虚拟私有云(VPC)中的特定区域组织资源。VPC 实际上是一个网络地址空间，可以在其中创建网络子网并将它与可用区域(AZ)相关联。如果配置正确，这个体系结构可以提供有效的资源隔离和持久复制。

1.4 AWS 可靠性和合规性

在你启动第一个服务之前，AWS 已经覆盖了许多基本的监管、法律和安全基础。AWS 在基础架构管理及相关资源中投入了大量的资金与精力。AWS 在对敏感数据的保护、数据的冗余性及精心优化的最佳实践策略等方面提供的服务是一般企业很难甚至无法实现的。

在适用情况下，AWS 平台上的资源符合许多国家和国际标准、框架和认证，包括 ISO 9001、FedRAMP、NIST 和 GDPR。更多有关信息，请参见 aws.amazon.com/compliance/programs。

1.4.1 AWS 责任共担模式

AWS 所提供的保障仅涵盖 AWS 的基础平台，因为你根据自己的业务需求来配置并使用 AWS 资源，所以你同样需要对这些资源的使用负责。对 AWS 责任共担模式的了解就显得尤为重要。

AWS 保证其物理服务器、存储设备、网络基础架构和托管服务等云端资源的安全并且不间断运行。如图 1-3 所示，AWS 客户应该对云中发生的一切负责。这涵盖了已安装操作系统的安全性及其操作、客户端数据、跨网络的数据移动、最终用户身份验证以及客户数据。

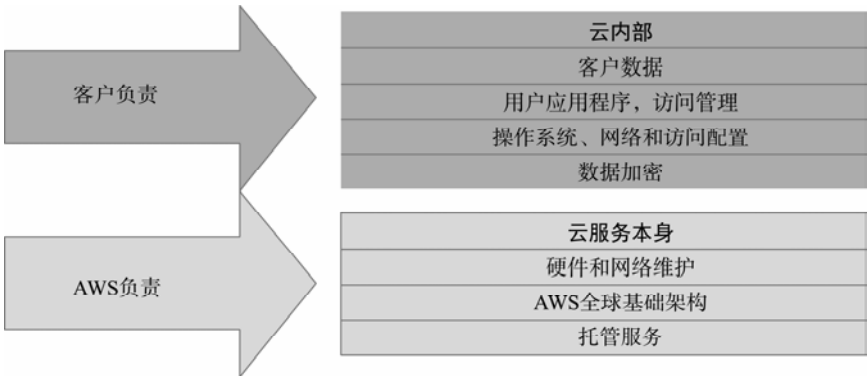


图 1-3 AWS 责任共担模式

1.4.2 AWS 服务级别协议

AWS 的“保证”并不意味着服务中断或安全漏洞永远不会发生。驱动器可能会停止运转，主要的电力系统也可能发生故障，并且自然灾害也可能发生。但是，如果出现问题，AWS 将提供服务积分，以在运行时间低于定义的阈值时补偿客户的损失。当然，这并不会帮助你恢复客户信心或失去业务。

保障级别的确切百分比将根据服务种类的不同而存在差异。例如，AWS EC2 的服务级别协议(SLA)被设定为 99.99%，这意味着可以期望每个月除了大约 4 分钟之外的所有时间都可以使用 EC2 实例、ECS 容器和 EBS 存储设备。

需要牢记的是，我们关心的不是故障是否会发生，而是故障何时发生。应该将你的应用程序构建在地理位置上分散，同时具有容错能力，以便在故障发生时，对你的客户几乎不产生任何影响。

1.5 使用 AWS

无论你选择运行哪种 AWS 服务，都需要使用一种方法来管理所有这些服务。基于浏览器的管理控制台是你了解服务功能及其在实际应用中的性能的绝佳方式。控制台几乎可以执行所有 AWS 的管理任务，同时提供了大量有用的可视化图形和帮助文档。但是，随着你对工作方式更加熟悉，尤其是当你的 AWS 部署变得越来越复杂时，你可能发现自己需要在控制台以外完成更多的工作。

1.5.1 AWS CLI

AWS 命令行接口(Command Line Interface, CLI)允许你从本地命令行执行复杂的 AWS 操作。一旦掌握了它的工作原理，就会发现它可以让事情变得更简单、高效。

例如，假设需要启动 6 个 EC2 实例来组成一个微服务环境。每个实例都将扮演单独的角色，因此需要略微不同的配置流程。通过单击一个又一个窗口从控制台启动实例会很快变得乏味和耗时，尤其是当你发现自己每隔几天就要重复一次操作时。但是整个过程可以通过一个简单的脚本来完成，你可以使用 AWS CLI 从本地终端 shell 或 PowerShell 界面运行这个脚本。

在 Linux、Windows 或 macOS 机器上安装和配置 AWS CLI 非常容易，但具体细节可能会根据你所使用的操作系统不同存在些许差异。有关最新的说明，请参见 docs.aws.amazon.com/cli/latest/userguide/installing.html。

1.5.2 AWS SDK

如果你想将对 AWS 资源的访问合并到你的应用程序代码中，你将需要根据不同

的编程语言使用 AWS 软件开发工具包(SDK)来实现。AWS 目前提供 9 种编程语言的 SDK, 包括 Java、.NET 和 Python, 以及许多包含 Android 和 iOS 的移动 SDK。同时提供 IntelliJ、Visual Studio 和 Visual Studio Team Services(VSTS)的工具包。可以在 aws.amazon.com/tools 上了解 AWS 开发人员工具的概述信息。

1.5.3 技术支持和在线资源

使用 AWS 就像生活中的诸多其他方面一样, 不会总是一帆风顺。你总会需要一些技术支持或者账户支持。AWS 提供多种类型的支持服务, 你应该了解具体可用的支持类型都有哪些。

当创建一个新的 AWS 账户时, 首先要选择支持计划的类型。你的业务需求和预算将决定你回答这个问题的答案。

1.5.4 支持计划

基础的支持计划对每个账户都是免费的, 并允许你访问客户服务以及相关文档、白皮书和支持论坛。客户服务帮助你解决有关账单和账户的支持问题。

开发者计划起步价为每月 29 美元, 并为一个账户持有人增加了云支持合作伙伴的访问权限, 同时提供有限的一般性指导和“系统受损”响应。

如果每月支付 100 美元(或以上)的支持服务费用, 那么可以选用商业计划。该计划将无限为你提供更快的保证响应时间, 以获取有关“功能受损”系统的帮助, 同时还提供个人指导和故障排除以及支持 API 的帮助。

最后, 企业支持计划涵盖了上面提到的所有功能, 并且包括直接与 AWS 解决方案架构师沟通, 从而进行运营和设计审查, 为你提供专属的技术支持客户经理及技术支持管家。对于复杂的、关键性任务的部署, 这些服务可以提供巨大的帮助。但你每个月至少需要支付 15 000 美元。

可以在 aws.amazon.com/premiumsupport/compare-plans 上了解有关 AWS 支持计划的更多信息。

1.5.5 其他支持资源

除了官方支持计划, 还有很多自助支持服务:

- AWS 社区帮助论坛对任何有效的 AWS 账户所有者开放(forums.aws.amazon.com)。
- 可以在 aws.amazon.com/documentation 查阅内容丰富及精心维护的 AWS 文档。
- AWS 良好架构页面(aws.amazon.com/architecture/well-architected)提供许多有价值的白皮书和文档, 这些白皮书和文档涉及云部署设计的最佳实践。

- 还有很多第三方公司为你的 AWS 部署提供商业支持。

1.6 本章小结

云计算以有效地将物理资源划分为更小、更灵活的虚拟单元为基础。企业可以用按需付费的方式“租用”这些单元，并通过有竞争力的成本、可伸缩且更加灵活的方式满足几乎任何网络应用程序及工作流的需求。

AWS 提供可靠且安全的资源，这些资源可以在越来越多的区域及可用区域中进行复制和全局分布。尽管责任共担模式要求你负责你在云中的部署，但 AWS 基础设施可以提供最佳实践及满足众多监管要求。

不断增长的 AWS 服务家族几乎涵盖了可以想象到的任何数字化需求，核心服务满足了计算、网络、数据库、存储、安全和应用程序管理以及集成需求。

可以通过管理控制台、AWS CLI 或使用 AWS SDK 生成的代码对 AWS 资源进行管理。通过支持计划、文档和帮助论坛可以获得多种技术和账户支持。AWS 还免费提供白皮书、用户指南和开发者指南，以及相关 Kindle 电子书。可以通过如下网址访问它们：

www.amazon.com/default/e/B007R6MVQ6/ref=dp_byline_cont_ebooks_1?redirectedFrom-KindleDb=true

1.7 考试要点

了解 AWS 平台体系结构 AWS 将其服务器和存储设备部署在全球多个区域，并在区域内划分为可用区域。这些可用区域允许通过复制技术来增强可用性，也允许进程和资源隔离以提高安全性和满足合规性要求。你应该利用这些特性设计自己的部署方式。

了解如何使用 AWS 管理工具 虽然可以通过浏览器访问 AWS 管理控制台，但你的大部分重要工作可能都是通过 AWS CLI 完成的，也可以通过在应用程序代码中调用 AWS SDK 来完成。

了解如何选择支持计划 理解哪个支持计划级别适合特定客户是构建成功部署的一个重要因素。作为架构师，你应该熟悉各种支持计划。

练习 1.1

使用 AWS CLI

在你的本地系统上安装(如果需要)和配置 AWS CLI，并通过列出账户中当前存在

的存储桶来确定它是否正常运行。作为额外的练习，创建一个 S3 存储桶，然后将一个简单的文件或文档从你的机器复制到你新创建的存储桶中。然后在浏览器控制台中确认该文件已经成功上传。

使用如下基本的 AWS CLI 命令完成你的练习：

```
aws s3 ls
aws s3 mb <bucketname>
aws s3 cp /path/to/file.txt s3://bucketname
```

1.8 习题

1. 开发人员希望运行完全预置的 EC2 实例，来支持其应用程序代码部署，并且不希望手动配置和启动必要的基础设施。他们应该使用下列哪个选项？

- A. AWS Lambda
- B. AWS Elastic Beanstalk
- C. Amazon EC2 Auto Scaling
- D. Amazon Route 53

2. 一些应用程序的最终用户抱怨从远程地理位置访问资源时出现了延迟。这些服务中哪一个最可能帮助减少延迟？

- A. Amazon CloudFront
- B. Amazon Route 53
- C. 弹性负载均衡
- D. Amazon Glacier

3. 以下哪项是弹性块存储的最佳应用场景？

- A. 需要价格低廉而且可靠的地方来存储你的应用程序可以访问的文件
- B. 需要安全的地方来存储本地服务器上的备份存档
- C. 需要按需计算周期的资源，以满足应用程序不断变化的需求
- D. 需要为 EC2 实例运行的文件系统提供持久性存储

4. 需要将公司本地用户访问控制与一些 AWS 资源集成在一起。以下哪些方法可以帮助你控制本地用户访问你的 AWS 资源及管理控制台？(选择两个)

- A. AWS 身份和访问管理(IAM)
- B. 密钥管理服务(KMS)
- C. AWS 目录服务
- D. 简单工作流(SWF)
- E. Amazon Cognito

5. 与从定义紧密的关系数据库结构中获得的数据相比，正在规划的应用程序所使用的数据需要更快的速度和更大的灵活性。你应该选择哪个 AWS 数据库服务？

- A. 关系数据库服务(RDS)
- B. Amazon Aurora
- C. Amazon DynamoDB
- D. 密钥管理服务(KMS)

6. 你已经在 AWS 爱尔兰地区启动了一个 EC2 应用服务器实例，需要从 Web 访问该实例。下面哪个是你应该使用的正确端点地址？

- A. compute.eu-central-1.amazonaws.com
 - B. ec2.eu-central-1.amazonaws.com
 - C. elasticcomputecloud.eu-west-2.amazonaws.com
 - D. ec2.eu-west-1.amazonaws.com
7. 在设置你的第一个 AWS 部署时，经常会遇到术语“可用区域”(AZ)。可用区域到底是什么？
- A. AWS 区域内的一个物理隔离的数据中心
 - B. 包含多个数据中心的区域
 - C. 单个区域内的资源所使用的单个网络子网
 - D. 数据中心内的一个独立的服务器机房
8. 在规划多层、多实例 AWS 应用程序时，需要一种方法有效地组织实例并配置它们的网络连接和访问控制。哪一个工具可以让你做到这一点？
- A. 负载均衡
 - B. Amazon 虚拟私有云(VPC)
 - C. Amazon CloudFront
 - D. AWS 终端节点(endpoint)
9. 你想确保使用 EC2 和 S3 资源构建的应用程序足够可靠，可以满足你行业内所需的法规要求。你应该检查什么？
- A. 历史运行时间日志记录
 - B. AWS 计划合规性工具
 - C. AWS 服务级别协议(SLA)
 - D. AWS 合规项目文档页面
 - E. AWS 责任共担模式
10. 你的组织运营团队成员需要一种通过本地命令行或 shell 脚本访问和管理 AWS 基础架构的方法。下列哪些工具可以帮助他们做到这一点？
- A. AWS Config
 - B. AWS CLI
 - C. AWS SDK
 - D. AWS 控制台
11. 在构建基于 AWS 的大型应用程序时，你的公司一直面临无法独自解决的配置问题，因此需要开发人员和 IT 团队负责人直接使用 AWS 技术支持服务。你应该购买哪种支持计划？
- A. 商业计划
 - B. 开发者计划
 - C. 基础计划
 - D. 企业计划