examundo

AWS Cloud Practitioner 模拟考试（中文题库）

40 题，附答案。指南和译文由软件制作并核对，目前还没有人工审阅。

更新日期：2026 年 11 月 25 日 · examundo.tech/zh/aws-cloud-practitioner/

云技术与服务

1. 一家媒体公司每晚运行视频转码批处理任务，该任务可以容忍中断，并能从检查点恢复。哪种 EC2 购买选项能让这个工作负载的成本最低？

A media company runs a nightly video transcoding batch job that can tolerate interruptions and resumes from checkpoints. Which EC2 purchasing option MINIMIZES cost for this workload?

A. 按需实例（On-Demand Instances）
B. Spot 实例（Spot Instances）
C. 专属主机（Dedicated Hosts）
D. 预留实例（Reserved Instances）

2. 一家公司的容器应用基于开源 Kubernetes，现在要迁移到 AWS，并且要完全兼容现有的 Kubernetes 工具和 API。公司应该使用哪项 AWS 服务？

A company has an existing container-based application built using open-source Kubernetes and wants to migrate it to AWS while retaining full compatibility with existing Kubernetes tooling and APIs. Which AWS service should the company use?

A. Amazon ECS
B. AWS Fargate
C. Amazon EKS
D. AWS Batch

3. 一家零售公司有一个每晚生成报表的脚本，运行约 2 分钟，只在文件上传到 Amazon S3 时触发。公司不想管理服务器，也不想为闲置的服务器付费。哪项 AWS 计算服务最合适？

A retail company runs a nightly report-generation script that executes for about 2 minutes and is triggered only when a file is uploaded to Amazon S3. The company wants to avoid managing or paying for idle servers. Which AWS compute service is MOST appropriate?

A. 使用 EC2 启动类型的 Amazon Elastic Container Service (ECS)
B. Amazon EC2 预留实例（Reserved Instances）
C. AWS Lambda
D. 带 Auto Scaling 组的 Amazon EC2

4. 一个承载关键业务、对延迟敏感的事务型数据库，需要 EBS 卷类型中最高的持续 IOPS 性能和最低的延迟。应该选择哪种 EBS 卷类型？

A mission-critical, latency-sensitive transactional database requires the highest sustained IOPS performance and lowest latency available among EBS volume types. Which EBS volume type should be selected?

A. Throughput Optimized HDD (st1)
B. Provisioned IOPS SSD (io2 Block Express)
C. General Purpose SSD (gp3)
D. Cold HDD (sc1)

5. 一家公司有一批 EC2 实例，都需要同时共享访问同一组文件。公司应该使用哪项 AWS 存储服务？

A company runs a fleet of EC2 instances that all need simultaneous, shared access to the same set of files. Which AWS storage service should the company use?

A. Amazon S3 Glacier
B. Amazon EBS
C. Amazon EFS
D. Instance Store

---

6. 一位解决方案架构师需要一个全托管的关系型数据库服务，为兼容 MySQL 的工作负载自动完成打补丁、备份和故障转移。应该推荐哪项服务？

A solutions architect needs a fully managed relational database service that automates patching, backups, and failover for a MySQL-compatible workload. Which service should be recommended?

A. Amazon Redshift
B. Amazon DynamoDB
C. Amazon RDS
D. Amazon ElastiCache

---

7. 一家公司的应用运行在两个可用区的多个 Amazon EC2 实例上，需要一个所有实例都能同时挂载并读写的共享文件系统。哪项 AWS 存储服务最合适？

A company's application runs on multiple Amazon EC2 instances across two Availability Zones and requires a shared file system that all instances can mount and read/write to concurrently. Which AWS storage service is MOST appropriate?

A. Amazon S3
B. EC2 Instance Store
C. Amazon Elastic Block Store (EBS)
D. Amazon Elastic File System (EFS)

---

8. 一家全球 SaaS 公司在 us-east-1、eu-west-1 和 ap-southeast-1 三个区域（Region）部署了应用服务器。公司希望根据网络状况，自动把用户引导到响应最快的区域。哪种 Route 53 路由策略能满足这个要求？

A global SaaS company has application servers deployed in the us-east-1, eu-west-1, and ap-southeast-1 Regions. The company wants users automatically directed to whichever Region delivers the fastest response time based on network conditions. Which Route 53 routing policy meets this requirement?

A. 基于延迟的路由策略（Latency-based routing policy）
B. 简单路由策略（Simple routing policy）
C. 地理位置路由策略（Geolocation routing policy）
D. 加权路由策略（Weighted routing policy）

---

9. 一位数据分析师需要对存储在 Amazon S3 中的数 TB 日志数据直接运行即席（ad hoc）SQL 查询，不想配置任何服务器或集群，只按查询付费。应该使用哪项服务？

A data analyst needs to run ad hoc SQL queries directly against terabytes of log data stored in Amazon S3 without provisioning any servers or clusters, paying only per query. Which service should be used?

A. Amazon RDS
B. Amazon Redshift
C. Amazon EMR
D. Amazon Athena

---

10. 一家金融服务公司在审计期间必须能在约 5 分钟内，从 S3 Glacier Flexible Retrieval 取回归档的合规记录，但审计一年只有几次。哪种取回选项最能兼顾紧迫性和成本？

A financial services firm must be able to retrieve archived compliance records from S3 Glacier Flexible Retrieval within about 5 minutes during an audit, but audits occur only a few times per year. Which retrieval option BEST balances the urgency requirement with cost?

A. 批量取回（Bulk retrieval）
B. 加急取回（Expedited retrieval）
C. S3 Glacier Deep Archive 标准取回
D. 标准取回（Standard retrieval）

安全与合规

11. 一位审计员要求提供 AWS 的 SOC 2 Type II 报告和最新的 PCI DSS 合规证明（Attestation of Compliance），用于支持即将进行的客户审计。公司的合规团队应该从哪里获取这些文件?

An auditor requests a copy of AWS's SOC 2 Type II report and the current PCI DSS Attestation of Compliance to support an upcoming customer audit. Where should the company's compliance team obtain these documents?

A. AWS Trusted Advisor
B. AWS Security Hub
C. AWS Config conformance packs
D. AWS Artifact

---

12. 哪项 AWS 服务提供针对分布式拒绝服务（DDoS）攻击的托管防护?

Which AWS service provides managed protection against Distributed Denial of Service (DDoS) attacks?

A. Amazon GuardDuty
B. AWS Shield
C. AWS Firewall Manager
D. AWS WAF

---

13. 一家公司的安全团队想为 AWS 账户根用户的登录增加一层保护，不能只靠用户名和密码。团队应该启用哪项安全控制?

A company's security team wants to add an additional layer of login protection to the AWS account root user beyond just a username and password. Which security control should the team enable?

A. 多重身份验证（MFA）
B. AWS WAF web ACL 规则
C. AWS Certificate Manager
D. Amazon GuardDuty 威胁检测

---

14. 一家组织的财务团队想让 AWS Organizations 中生产组织单元（OU）下的任何成员账户都无法关闭 AWS CloudTrail 日志，即使该账户中的 IAM 管理员拥有完整管理权限也不行。组织应该使用哪项功能?

An organization's finance team wants to prevent any member account within a production organizational unit in AWS Organizations from disabling AWS CloudTrail logging, even if an IAM administrator in that account has full administrative permissions. Which feature should the organization use?

A. AWS Config conformance pack
B. CloudTrail 跟踪上的基于资源的策略
C. 应用在组织单元级别的服务控制策略（SCP）
D. 附加到每位管理员的 IAM 权限边界

---

15. 一家公司的 Web 应用运行在 Application Load Balancer 后面的 Amazon EC2 实例上，另有一个微服务运行在 AWS Lambda 上。按照 AWS 责任共担模型，哪项安全任务由公司负责?

A company runs a web application on Amazon EC2 instances behind an Application Load Balancer, and a separate microservice on AWS Lambda. Under the AWS shared responsibility model, which security task falls to the company?

A. 给 EC2 实例的客户机操作系统打补丁
B. 给 EC2 和 Lambda 底层的主机虚拟机监控程序（hypervisor）打补丁
C. 维护承载这两项服务的数据中心的物理安全
D. 给 Lambda 运行时环境打补丁

---

16. 一个 DevOps 团队用自动化流水线为开发人员创建 IAM 角色。安全要求规定：无论之后给角色附加什么策略，流水线创建的任何角色的权限都不能超过规定的最大范围。哪项 IAM 功能可以强制实现这一点?

A DevOps team uses an automated pipeline to create IAM roles for developers. Security requires that no role created by the pipeline, regardless of the policies later attached to it, can ever exceed a defined maximum set of permissions. Which IAM feature enforces this?

A. 基于资源的策略（Resource-based policy）
B. 权限边界（Permissions boundary）
C. 基于身份的策略（Identity-based policy）
D. 服务控制策略（Service control policy）

---

17. 一位合规官需要查明上周是哪位 IAM 用户删除了某个 Amazon S3 存储桶。哪项 AWS 服务提供这类 API 活动的记录?

A compliance officer needs to determine which IAM user deleted a specific Amazon S3 bucket last week. Which AWS service provides a record of this API activity?

A. AWS Trusted Advisor
B. Amazon CloudWatch
C. AWS CloudTrail
D. AWS Config

---

18. AWS Identity and Access Management (IAM) 中的 IAM 组有什么用途?

What is the purpose of an IAM group in AWS Identity and Access Management?

A. 为运行在 AWS 服务上的应用提供临时安全凭证
B. 加密存储在 Amazon S3 存储桶中的对象
C. 记录并监控 AWS 账户内的 API 调用
D. 把多个 IAM 用户归在一起，一次性为他们应用相同的权限策略

---

19. 一个安全团队希望在某个 EC2 实例开始与已知属于恶意软件命令与控制（command-and-control）基础设施的 IP 地址通信时，收到自动告警。哪项 AWS 服务是专为检测这类活动而设计的?

A security team wants to receive automated alerts when an EC2 instance begins communicating with an IP address known to be associated with malware command-and-control infrastructure. Which AWS service is purpose-built to detect this activity?

A. Amazon Inspector
B. Amazon GuardDuty
C. AWS Config
D. Amazon Macie

---

20. 一家公司的 Web 应用运行在 Amazon EC2 实例上，需要读写 Amazon S3 存储桶中的对象。哪种方式是授予应用这项访问权限的最安全方式?

A company hosts a web application on Amazon EC2 instances that must read and write objects in an Amazon S3 bucket. Which approach is the MOST secure way to grant the application this access?

A. 创建允许对象公开读写的存储桶策略
B. 把 IAM 用户的访问密钥（access key）和秘密访问密钥（secret key）存放在应用的配置文件中
C. 给 EC2 实例附加带有 S3 访问策略的 IAM 角色
D. 把 AWS 账户根用户凭证嵌入 EC2 实例的环境变量

云概念

21. AWS Cloud Adoption Framework (CAF) 的哪个视角侧重于让 IT 战略与业务目标保持一致，并为采用云建立业务论证（business case）?

Which AWS Cloud Adoption Framework (CAF) perspective focuses on aligning IT strategy with business goals and building a business case for cloud adoption?

A. 安全视角（Security perspective）
B. 业务视角（Business perspective）
C. 平台视角（Platform perspective）
D. 治理视角（Governance perspective）

---

22. 一家公司用 AWS Lambda 部署了无服务器应用。按照 AWS 责任共担模型，即使 AWS 管理底层计算基础设施，哪项安全任务仍然由公司负责?

A company deploys a serverless application using AWS Lambda. Under the AWS shared responsibility model, which security task remains the company's responsibility even though AWS manages the underlying compute infrastructure?

A. 配置 IAM 执行角色和函数级权限
B. 给运行 Lambda 服务的服务器操作系统打补丁
C. 管理隔离 Lambda 执行环境的虚拟机监控程序（hypervisor）层
D. 维护承载 Lambda 函数的物理硬件

---

23. 在一次限时抢购中，零售商的应用在流量激增时，自动在负载均衡器后面增加 EC2 实例，流量回落后再把实例移除。这个场景最能体现哪种云特性?

During a flash sale, a retailer's application automatically adds EC2 instances behind a load balancer as traffic spikes and removes them once traffic subsides. Which cloud characteristic does this scenario BEST demonstrate?

A. 容错（Fault tolerance）
B. 高可用性（High availability）
C. 弹性（Elasticity）
D. 持久性（Durability）

---

24. 哪种做法最能体现卓越运营（Operational Excellence）支柱中“进行频繁、小规模、可回退的变更”这条设计原则?

Which practice BEST demonstrates the Operational Excellence pillar's design principle of making frequent, small, reversible changes?

A. 要求变更咨询委员会把所有更新合并成一次年度发布
B. 在每季度的维护窗口安排一次大型基础设施发布
C. 直接通过 AWS 管理控制台应用配置变更，不做任何跟踪
D. 通过带版本控制、有自动回滚的 CI/CD 流水线部署基础设施变更

---

25. 良好架构框架（Well-Architected Framework）的哪个支柱涵盖工作负载从基础设施或服务中断中恢复，并动态获取资源以满足需求的能力?

Which Well-Architected Framework pillar encompasses a workload's ability to recover from infrastructure or service disruptions and dynamically acquire resources to meet demand?

A. 成本优化（Cost optimization）
B. 可持续性（Sustainability）
C. 卓越运营（Operational excellence）
D. 可靠性（Reliability）

---

26. 一家公司的可持续发展团队要求云工程团队选择 AWS 区域并调整工作负载规模（rightsize），专门以减少运行计算和存储资源对环境的影响为目标。这个目标对应良好架构框架（Well-Architected Framework）的哪个支柱?

A company's sustainability team asks the cloud engineering group to select AWS Regions and rightsize workloads specifically to minimize the environmental impact of running compute and storage resources. This objective aligns with which Well-Architected Framework pillar?

A. 成本优化（Cost Optimization）
B. 卓越运营（Operational Excellence）
C. 性能效率（Performance Efficiency）
D. 可持续性（Sustainability）

---

27. 一位开发人员用 AWS Lambda 部署了一个函数，处理上传到 Amazon S3 的对象。与在自行管理的 EC2 实例上运行同样的工作负载相比，使用 Lambda 时，哪项安全责任从客户转移给了 AWS?

A developer deploys a function using AWS Lambda to process objects uploaded to Amazon S3. Compared to an equivalent workload running on self-managed EC2 instances, which security responsibility shifts from the customer to AWS when using Lambda?

A. 编写安全的应用代码
B. 加密存储在 S3 中的对象
C. 给底层操作系统打补丁
D. 配置 IAM 执行角色权限

---

28. 一家公司要求所有 IAM 用户使用多重身份验证（MFA），执行最小权限，并尽可能减少对长期访问密钥的依赖。这最能体现良好架构框架（Well-Architected）安全支柱的哪条设计原则?

A company requires multi-factor authentication for all IAM users, enforces least privilege permissions, and reduces reliance on long-term access keys wherever possible. Which Well-Architected Security pillar design principle does this BEST reflect?

A. 启用可追溯性（Enable traceability）
B. 建立强大的身份基础（Implement a strong identity foundation）
C. 将安全最佳实践自动化（Automate security best practices）
D. 在所有层应用安全（Apply security at all layers）

---

29. 一家零售公司的订单处理系统在限时抢购期间自动增加 EC2 实例数量，流量恢复正常后自动减少，全程无需人工干预。这种行为最能说明哪种云特性?

A retail company's order-processing system automatically increases the number of EC2 instances during a flash sale and decreases them once traffic returns to normal, without any manual intervention. Which cloud characteristic does this behavior BEST illustrate?

A. 弹性（Elasticity）
B. 高可用性（High availability）
C. 容错（Fault tolerance）
D. 可扩展性（Scalability）

---

30. 一家公司想通过选择使用可再生能源供电的 AWS 区域，以及调整资源规模（rightsizing）来减少不必要的配置和能耗，从而降低其云足迹对环境的影响。良好架构框架（Well-Architected Framework）的哪个支柱最直接地对应这个目标?

A company wants to reduce the environmental impact of its cloud footprint by selecting AWS Regions powered by renewable energy and by rightsizing resources to minimize unnecessary provisioning and energy consumption. Which Well-Architected Framework pillar MOST directly addresses this goal?

A. 可持续性（Sustainability）
B. 成本优化（Cost Optimization）
C. 可靠性（Reliability）
D. 性能效率（Performance Efficiency）

计费、定价与支持

31. 一家公司希望为稳定的计算用量基线获得折扣，同时在承诺期内可以自由更改实例系列、大小、操作系统和 AWS 区域，又不会失去折扣。哪种定价选项最能满足这个要求?

A company wants a discount for a consistent baseline of compute usage but also needs the freedom to change instance families, sizes, operating systems, and AWS Regions over the commitment period without losing the discount. Which pricing option BEST meets this requirement?

A. 标准预留实例（Standard Reserved Instances）
B. EC2 Instance Savings Plans
C. 按需容量预留（On-Demand Capacity Reservations）
D. Compute Savings Plans

---

32. 一位账单管理员需要最详细的 AWS 费用明细，细到每一行（line-item level），包括用量类型、资源 ID 和适用的费率，用于导入第三方财务报表工具。哪一项能提供这种详细程度？

A billing administrator needs the most detailed, line-item-level breakdown of AWS charges, including usage type, resource ID, and applied pricing rates, for import into a third-party financial reporting tool. Which resource provides this level of detail?

A. AWS Cost Explorer 图表
B. AWS Billing 控制台的摘要仪表板
C. AWS Trusted Advisor 成本优化检查
D. AWS Cost and Usage Report

---

33. 一家媒体公司有一批 EC2 实例，未来三年必须全天候（24/7）可用，但工程团队预计每年都会随着新实例系列的发布而迁移。哪种定价选项在适应这种灵活性的同时，节省的成本最多？

A media company runs a fleet of EC2 instances that must remain available 24/7 for the next three years, but the engineering team expects to migrate to newer instance families annually as they are released. Which pricing option provides the MOST cost savings while accommodating this flexibility?

A. 按需实例（On-Demand Instances）
B. Compute Savings Plans
C. 针对当前实例系列的标准预留实例（Standard Reserved Instances）
D. 使用持久请求（persistent request）的 Spot 实例

---

34. 一家使用 AWS Business Support 计划的医疗初创公司，想要一位指定的专人，主动提供架构指导、主持运营评审，并在故障期间与 AWS 服务团队协调。公司应该怎么做才能获得这项权益？

A healthcare startup on the AWS Business Support plan wants a named individual who proactively provides architectural guidance, hosts operational reviews, and coordinates with AWS service teams during outages. Which action should the company take to obtain this benefit?

A. 升级到 Enterprise Support 计划，获得专属的技术客户经理
B. 购买额外的 Business Support 席位
C. 启用 AWS Organizations 以获得共享的客户经理
D. 通过 Trusted Advisor 提交支持案例，申请专属联系人

---

35. 支撑一家电商公司业务的生产系统完全宕机。该公司使用 AWS Business Support。对于归类为“production system down”（生产系统宕机）的案例，AWS 的首次响应时间目标是多久？

A production system supporting an e-commerce company goes completely down. The company is subscribed to AWS Business Support. What is AWS's initial response time target for a case classified as 'production system down'?

A. 少于 1 小时
B. 少于 4 小时
C. 少于 12 小时
D. 少于 15 分钟

---

36. 一家公司每晚运行视频转码批处理任务，该任务可以容忍中断，重新启动也不影响最终输出。哪种 EC2 定价选项对这个工作负载的成本最低？

A company runs a nightly video-transcoding batch job that can tolerate interruption and be restarted without affecting the final output. Which EC2 pricing option provides the LOWEST cost for this workload?

A. 预留实例（Reserved Instances）
B. 按需实例（On-Demand Instances）
C. 专属主机（Dedicated Hosts）
D. Spot 实例（Spot Instances）

---

37. 一家快速成长的 SaaS 公司需要指定的技术客户经理（Technical Account Manager，TAM）、主动的架构指导、基础设施事件管理，以及针对业务关键系统宕机问题 15 分钟的响应时间。公司应该选择哪个 AWS Support 计划?

A rapidly growing SaaS company needs a designated Technical Account Manager (TAM), proactive architectural guidance, infrastructure event management, and a 15-minute response time for business-critical system down issues. Which AWS Support plan should the company select?

A. Enterprise On-Ramp Support
B. Business Support
C. Enterprise Support
D. Developer Support

---

38. 一家初创公司正在评估 Amazon EC2 定价选项，用于一次短期营销活动，开始和结束日期都无法预测。哪种定价模式允许公司只为实际使用的计算容量付费、按秒计费，并且无需预先承诺?

A startup is evaluating Amazon EC2 pricing options for a short-term marketing campaign with no predictable start or end date. Which pricing model allows the company to pay only for compute capacity consumed, billed by the second, with no upfront commitment?

A. 按需实例（On-Demand Instances）
B. Savings Plans
C. 专属主机（Dedicated Hosts）
D. 预留实例（Reserved Instances）

---

39. 一位解决方案架构师正在设计一个新的工作负载，想在部署任何资源之前，估算所设计的 AWS 架构的月度成本。应该使用哪个工具?

A solutions architect is designing a new workload and wants to estimate the monthly cost of a proposed AWS architecture before any resources are deployed. Which tool should be used?

A. AWS Budgets
B. AWS Cost and Usage Report
C. AWS Pricing Calculator
D. AWS Cost Explorer

---

40. 一家成长中的企业想要一位专属于自己账户的 AWS 技术客户经理（Technical Account Manager，TAM），提供主动指导和架构评审，而不是共享的 TAM 团队。公司应该选择哪个级别的 AWS Support 计划?

A growing enterprise wants a single, dedicated AWS Technical Account Manager (TAM) assigned specifically to its account to provide proactive guidance and architectural reviews, rather than access to a shared pool of TAMs. Which AWS Support tier should the company select?

A. Business Support
B. Developer Support
C. Enterprise Support
D. Enterprise On-Ramp Support

正确答案

1. B Spot 实例使用 EC2 的闲置容量，价格最多比按需价低 90%，适合能容忍中断、运行灵活的工作负载，比如带检查点的批量转码。按需实例按全价付费。预留实例要承诺 1 年或 3 年，适合稳定的长期用量。专属主机最贵，用于许可证或合规需要看到物理服务器的场景。

2. C Amazon EKS 是托管服务，运行的是经过认证的上游 Kubernetes 控制平面，所以现有的清单文件、kubectl 命令和 Kubernetes 生态工具无需修改就能用。ECS 是 AWS 自己的编排器，不兼容 Kubernetes API，需要重新设计。Fargate 是无服务器计算引擎，本身不提供 Kubernetes API。AWS Batch 用来调度批处理作业，不是托管的 Kubernetes 服务。

3. C AWS Lambda 是无服务器、事件驱动的服务，可以由 S3 上传事件直接触发，按请求数和执行时长计费，没有闲置服务器的费用。EC2 加 Auto Scaling 仍然要运行或启动实例，即使只跑 2 分钟也有成本和管理负担。预留实例要承诺 1 年或 3 年，不适合这种间歇的短任务。使用 EC2 启动类型的 ECS 仍然要自己配置底层 EC2 集群并打补丁。

4. B io2 Block Express 专为要求最高、对延迟敏感的事务型工作负载设计，在所有 EBS 类型中 IOPS 和吞吐量最高，延迟稳定在 1 毫秒以下。gp3 基线性能不错，但最大 IOPS 比 io2 Block Express 低得多，不适合要求极高的关键数据库。st1 和 sc1 是机械硬盘（HDD）卷，面向大块顺序读写（如大数据和日志处理），不适合低延迟、高 IOPS 的数据库事务。

5. C Amazon Elastic File System (EFS) 是全托管、可弹性伸缩的 NFS 文件系统，可以被数千个 EC2 实例同时挂载，非常适合共享文件访问。EBS 卷一次只能连接一个 EC2 实例（只有特定卷类型支持有限的 Multi-Attach），所以不适合广泛共享。S3 Glacier 是归档对象存储，不能当文件系统挂载。Instance Store 是与单台主机绑定的临时存储，实例停止后数据会丢失。

6. C Amazon RDS (Relational Database Service) 是托管服务，支持 MySQL、PostgreSQL、MariaDB 等引擎，能自动完成打补丁、备份和 Multi-AZ 故障转移这些费时的工作。Amazon DynamoDB 是托管的 NoSQL 键值和文档数据库，不是关系型，查询方式也不同。Amazon Redshift 是数据仓库，适合大规模分析查询，不适合事务型关系工作负载。Amazon ElastiCache 是内存缓存服务，用来加快应用速度，不是主要的关系数据存储。

7. D EFS 是托管、可弹性伸缩的 NFS 文件系统，设计上支持数千个 EC2 实例同时读写，包括跨多个可用区，所以最适合共享文件存储。EBS 卷一次只能连接一个 EC2 实例（少数卷类型的 Multi-Attach 是例外，且实例必须在同一可用区），不能当跨可用区的通用共享存储。S3 是通过 API 访问的对象存储，不是传统应用能挂载的 POSIX 文件系统。Instance Store 是临时存储，绑定单台主机，实例停止或终止后数据丢失。

8. A 基于延迟的路由策略使用 AWS 测得的用户网络到各区域的延迟，返回预计延迟最低的区域的记录；它并不测量每个应用端点的实际响应时间。加权路由按固定比例分配流量，不考虑性能，适合测试或逐步发布，不是为了提速。地理位置路由按用户所在位置分配，可能把用户导向地理上近、但实际不是最快的区域。简单路由只返回一条记录，没有健康检查，也没有性能判断。

9. D Amazon Athena 是无服务器的交互式查询服务，可以直接对 S3 中的数据运行标准 SQL，无需配置基础设施，按每次查询扫描的数据量收费，符合即席查询、按查询付费的要求。Amazon Redshift 是数据仓库，可用预置集群或无服务器计算，没有 Athena 这种直接扫描 S3、按查询付费的模式。Amazon EMR 支持托管集群和无服务器的 Spark、Hive 应用，但不是这种交互式 SQL 需求的最佳选择。Amazon RDS 是面向事务的关系数据库，不用来直接查询 S3 中的原始日志。

10. B 从 S3 Glacier Flexible Retrieval 加急取回，通常 1 到 5 分钟内返回数据，适合审计这种不常见但很紧急的访问，而且比把数据一直放在随时可快速访问的存储类别中便宜得多。标准取回需要 3 到 5 小时，批量取回需要 5 到 12 小时，都赶不上 5 分钟的要求。Glacier Deep Archive 标准取回最长 12 小时，存储类别和取回时间都不适合这种时间紧迫的审计。

11. D AWS Artifact 是自助门户，可以按需获取 AWS 的合规报告，包括 SOC 1/2/3、PCI DSS Attestation of Compliance 和 ISO 认证，也可以查看并接受 BAA 等协议。Trusted Advisor 提供成本、性能、安全和容错方面的账户优化检查，不提供合规文件。AWS Config conformance packs 用合规规则评估资源配置，但不提供 AWS 自己的第三方审计报告。Security Hub 汇总 GuardDuty、Inspector 等服务的安全发现，不提供合规认证。

12. B AWS Shield 是专门用来检测和缓解 DDoS 攻击的托管服务。Shield Standard 自动启用，不收额外费用；Shield Advanced 为关键工作负载提供更强的防护和 DDoS 费用保护。AWS WAF 按规则过滤 Web 请求，拦截 SQL 注入等攻击，属于另一类威胁。GuardDuty 检测更广泛的恶意活动，但不缓解 DDoS 流量。Firewall Manager 集中管理 WAF 和安全组规则，本身不是 DDoS 缓解引擎。

13. A MFA 在用户名和密码之外，再要求第二个验证因素，通常是虚拟设备或硬件设备生成的一次性动态密码，正好针对根用户的登录安全。AWS WAF 在应用层过滤恶意 Web 流量，与账户登录无关。GuardDuty 是威胁检测服务，在活动发生后分析日志，不是登录控制。AWS Certificate Manager 签发和管理 SSL/TLS 证书，与 AWS 账户用户的身份验证无关。

14. C AWS Organizations 中的服务控制策略（SCP）为成员账户中所有 IAM 用户和角色（包括管理员）设定权限上限，可以明确拒绝关闭 CloudTrail 这类操作，不受账户自身 IAM 策略影响。权限边界只作用于它所附加的那个 IAM 身份，而且可以在账户内被修改。CloudTrail 上的基于资源的策略不是限制 CloudTrail 访问的方式。Config conformance pack 只检测并报告不合规的配置，不会事先阻止操作。

15. A AWS 负责“云本身”的安全：主机基础设施、虚拟机监控程序（hypervisor）和物理设施；客户负责“云中”的安全。对 EC2 来说，客户要负责给客户机操作系统打补丁、更新应用和配置网络，因为 EC2 是非托管的计算服务。给虚拟机监控程序打补丁和维护数据中心物理安全是 AWS 的基础设施责任。Lambda 托管运行时的补丁也由 AWS 负责，客户只管理函数代码和配置，不需要像 EC2 那样给客户机操作系统打补丁。

16. B 权限边界是 IAM 的高级功能，设定基于身份的策略能授予用户或角色的最大权限，实际生效的权限始终是身份策略与边界的交集，所以即使之后附加了范围很宽的策略，也能防止权限提升（privilege escalation）。服务控制策略（SCP）作用于 AWS Organizations 的账户层面，不是针对单个角色。普通的基于身份的策略只负责授予权限，自己没有上限机制。基于资源的策略附加在 S3 存储桶或 KMS 密钥等资源上，不用来限制角色的权限上限。

17. C AWS CloudTrail 记录 API 活动，包括调用者身份、时间戳和执行的操作。S3 DeleteBucket 是管理事件，默认的 90 天事件历史中就有，合规官可以据此追查上周是哪位 IAM 用户发出了这个调用。CloudWatch 收集运维监控用的指标和日志，本身不记录谁调用了 API。AWS Config 跟踪资源配置状态随时间的变化，不是用来把某个 API 调用归到某个用户的。Trusted Advisor 提供最佳实践建议，不是用户活动的审计记录。

18. D IAM 组是 IAM 用户的集合，管理员可以把一个或多个策略附加到组上，组内每个成员都继承相同的权限，大规模管理权限更简单。为服务提供临时凭证是 IAM 角色的作用，不是组。加密 S3 对象由 S3 服务器端加密或 AWS KMS 完成。记录 API 调用是 AWS CloudTrail 的功能，不是 IAM 组的功能。

19. B GuardDuty 持续分析 VPC Flow Logs、DNS 日志和 CloudTrail 事件，并与精选的威胁情报源比对，标记命令与控制（C2）通信、加密货币挖矿或侦察等活动。Macie 发现并分类 S3 中的敏感数据（如 PII），不检测网络威胁。Inspector 对 EC2 和 ECR 做自动化漏洞和软件成分扫描，不做实时威胁检测。Config 跟踪资源配置状态和合规偏差，不识别恶意流量。

20. C EC2 的 IAM 角色通过实例元数据服务提供临时且自动轮换的凭证，不用在实例上存放长期访问密钥，实例被入侵时风险也更小。存放 IAM 用户密钥或根用户凭证会留下长期有效的密钥，容易泄露，也难以轮换。公开的存储桶策略把数据暴露给整个互联网，违反最小权限原则。Well-Architected 安全支柱建议使用基于角色的访问，而不是静态凭证。

21. B AWS CAF 的业务视角（Business perspective）帮助业务经理和财务负责人等相关人员，确保云投资与业务成果一致，并为迁移建立清晰的业务论证。平台视角涉及云环境的架构和配置。治理视角侧重于管理风险、优化业务价值所需的技能和流程。安全视角确保组织满足保密性、完整性和可用性要求。只有业务视角直接涉及战略一致性和财务论证。

22. A 即使是 Lambda 这样的无服务器服务，“云中的安全”仍然由客户负责：公司必须为每个函数定义最小权限的 IAM 执行角色、资源策略，并保护环境变量。与 Lambda 相关的“云本身的安全”都归 AWS，包括给主机操作系统打补丁、维护物理服务器和数据中心、管理虚拟机监控程序，以及客户函数之间的执行环境隔离，这些都不需要客户操作。这是常见的考试陷阱：考生以为无服务器去掉了所有安全责任，其实只去掉了基础设施层的责任。

23. C 弹性（Elasticity）是自动扩大和缩小计算资源以匹配实时需求的能力，正是限时抢购场景中自动伸缩的表现。高可用性是通过跨位置的冗余基础设施减少停机时间，不是随需求伸缩。容错是组件出故障后仍能继续运行，不是按需求伸缩。持久性指数据的长期保存和完整性，与计算伸缩无关。

24. D 带版本控制的 CI/CD 流水线让团队频繁发布小的增量变更，自动回滚则保证变更出问题时能快速撤销，正好符合“频繁、小规模、可回退”的原则。每季度或每年一次的发布窗口恰恰相反：变更量大、不频繁、风险高，也很难干净地回退。不加跟踪地在控制台改配置，会失去这条原则要求的可回退性和可审计性，因为没有记录改了什么，也不知道怎么回滚。

25. D 可靠性支柱关注工作负载正确、一致地完成预期功能的能力，包括从故障中恢复、动态获取资源以满足需求，以及缓解配置错误或暂时的网络问题等中断。卓越运营侧重于流程改进和监控，不是专门针对故障恢复。成本优化是避免不必要的支出。可持续性是尽量减少运行工作负载对环境的影响。只有可靠性涵盖韧性（resilience）和自我修复的设计模式。

26. D 可持续性支柱于 2021 年加入，侧重于减少运行云工作负载对环境的影响，包括提高资源利用率、选择高效的区域，以及减少整体的能源和硬件消耗。成本优化针对的是财务支出，而不是环境影响，虽然做法有时会重叠。卓越运营关注为创造业务价值而运行和监控系统，不涉及环境目标。性能效率关注高效满足工作负载要求，不是这里明确提到的环境影响目标。

27. C 使用 EC2 时，给客户机操作系统打补丁属于客户负责的“云中”安全。使用 Lambda 时，AWS 全面管理底层计算环境，包括操作系统补丁，这是无服务器抽象的一部分，这项责任就转到了责任共担模型中 AWS 的一侧。无论计算是无服务器还是自行管理，IAM 执行角色配置、S3 加密设置和编写安全的应用代码仍由客户负责，因为这些控制位于 AWS 所管理的基础设施层之上。

28. B “建立强大的身份基础”这条原则的核心是执行最小权限、要求 MFA，并消除对长期静态凭证的依赖，与这个场景完全吻合。“启用可追溯性”侧重于实时记录、监控和审计操作，例如使用 AWS CloudTrail，这里没有提到。“在所有层应用安全”指在网络、计算和应用各层实施纵深防御。“将安全最佳实践自动化”指用基于软件的自动化机制来执行控制，也不是这个场景描述的具体做法。

29. A 弹性（Elasticity）特指近乎实时地自动、动态获取和释放资源，以匹配当前需求，符合场景中自动扩容和缩容的行为。可扩展性（Scalability）的含义更广，指系统能承受工作负载增长，不一定包含自动缩容。高可用性指系统以最少的停机时间保持可访问，容错指组件故障后仍能继续运行，这两者都不直接描述随需求波动自动调整容量。

30. A 可持续性支柱专门关注减少运行云工作负载对环境的影响，包括根据可再生能源的可用性选择区域，以及通过调整资源规模来减少浪费。调整规模虽然也能降低开支，但这里明确的目标是环境影响，而不是节省费用，这就是它与成本优化的区别。性能效率关注高效地使用资源来满足系统要求，不是专门针对环境成果。可靠性关注工作负载从中断中恢复的能力，与环境影响无关。

31. D Compute Savings Plans 自动适用于 EC2、Fargate 和 Lambda 的用量，不论实例系列、大小、操作系统、租赁方式或区域，灵活性最大，同时仍然是承诺 1 年或 3 年的每小时支出。EC2 Instance Savings Plans 把折扣锁定在某个区域内的特定实例系列，失去了跨系列的灵活性。标准预留实例绑定特定的实例系列和区域。按需容量预留只保证容量，没有折扣，也不能跨系列使用。

32. D AWS Cost and Usage Report (CUR) 是最全面、最精细的账单数据来源，提供细化到资源 ID、用量类型和费率的明细行，并且可以交付到 S3 存储桶，供数据仓库或 BI 平台等第三方财务工具导入。Cost Explorer 图表是给人查看的汇总可视化，不是可导出的原始明细。Billing 控制台的摘要仪表板只显示月度总额。Trusted Advisor 的成本检查会标出闲置资源等优化机会，但不提供精细的账单明细行。

33. B Compute Savings Plans 最多可省 66%，并且自动适用于任何 EC2 实例系列、大小、操作系统、租赁方式，甚至任何区域的 Fargate/Lambda 用量，所以每年换实例系列也不会损失折扣。标准预留实例绑定特定的实例系列和区域，更换系列会浪费未用完的预留价值。按需实例最灵活，但对确定会用满 3 年的用量没有折扣。Spot 实例可能被中断，不适合必须 24/7 可用的工作负载。

34. A 提供主动指导、运营评审，并在问题升级（escalation）时负责协调的技术客户经理（Technical Account Manager，TAM），是 Enterprise Support 独有的权益（Enterprise On-Ramp 下是共享的 TAM 团队）。Business Support 包含更快的响应和完整的 Trusted Advisor 检查，但没有专属 TAM。Trusted Advisor 是自动推荐工具，不是分配联系人的机制。Business Support 没有通过购买席位来获得 TAM 的模式。AWS Organizations 管理账单和账户结构，不负责分配客户经理。

35. A 在 Business Support 下，标记为“production system down”的案例，首次响应目标是少于 1 小时；这是响应目标，不是保证的 SLA。少于 15 分钟是 Enterprise Support 下“business-critical system down”（业务关键系统宕机）案例的响应目标。少于 4 小时对应“production system impaired”（生产系统受损，性能下降但仍在运行），严重程度低于完全宕机。少于 12 小时对应“system impaired”（系统受损），优先级比生产系统宕机低得多。

36. D Spot 实例使用 EC2 的闲置容量，价格最多比按需价低 90%，适合能容忍中断、运行灵活的工作负载，比如能承受两分钟中断通知的批量转码。按需实例没有折扣。预留实例要承诺 1 年或 3 年，适合稳定的工作负载，虽然比按需便宜，但对可中断的任务来说比不上 Spot 的价格。专属主机针对许可证或合规需求，是最贵的选项，与批处理任务省钱无关。

37. C Enterprise Support 包含指定的 TAM、主动指导、基础设施事件管理，以及业务关键系统宕机案例 15 分钟的首次响应目标；响应时间是目标，不是保证。Developer Support 没有 TAM，只在工作时间提供一般性指导。Business Support 对生产系统宕机的首次响应目标是 1 小时，没有 TAM。Enterprise On-Ramp Support 提供的是共享的 TAM 团队，而不是指定的 TAM，业务关键问题的首次响应目标是 30 分钟，达不到要求。

38. A 按需实例让客户按小时或按秒为计算容量付费，没有长期合同或预付费用，适合不可预测的短期工作负载。预留实例要承诺 1 年或 3 年才有折扣。Savings Plans 同样要在一段期限内承诺支出。专属主机提供物理服务器，用于许可证或合规需求，按需或预留计费，对用量不可预测的场景来说不是最灵活的通用选择。

39. C AWS Pricing Calculator 让架构师搭建设计中的架构（选择服务、实例类型、存储和数据传输估算），在实际部署任何资源之前就能得出估算的月度成本，非常适合部署前的规划。Cost Explorer、Cost and Usage Report 和 Budgets 都基于现有账户的实际历史或持续用量数据，所以都无法估算尚未构建的工作负载的成本。

40. C 只有完整的 Enterprise Support 计划包含专属的、指定的技术客户经理。Enterprise On-Ramp 是低于完整 Enterprise 的中间级别，提供共享的 TAM 团队，没有一位专属的 TAM。Business Support 提供完整的 Trusted Advisor 检查，也可以全天候（24/7）联系云支持工程师（Cloud Support Engineers），但完全没有 TAM。Developer Support 面向测试和开发，不支持生产系统，也没有 TAM。

英文关键词

shared responsibility model	责任共担模型	说明哪些安全工作归 AWS，哪些归客户
Region	区域	AWS 放置数据中心的一个地理地区
Availability Zone	可用区	区域内互相隔离的数据中心位置
elasticity	弹性	按实时需求自动增减资源
scalability	可扩展性	系统承受用量增长的能力
high availability	高可用性	靠冗余让停机时间很短
fault tolerance	容错	部件出故障时仍能继续运行

durability	持久性	数据长期保存而不丢失
workload	工作负载	在云上运行的应用及其资源
instance family	实例系列	用途相近的一组 EC2 实例类型
On-Demand Instances	按需实例	用多少付多少，没有长期承诺
Spot Instances	Spot 实例（竞价型实例）	低价使用闲置容量，可能被中断
Reserved Instances	预留实例	承诺 1 年或 3 年，换取折扣
Savings Plans	节省计划	承诺每小时消费额，换取折扣
Dedicated Hosts	专属主机	专供一个客户使用的物理服务器
upfront commitment	预先承诺	事先承诺付款或使用一段时间
spare capacity	闲置容量	暂时没有人使用的计算资源
batch job	批处理任务	集中处理大量数据、不需要人操作的任务
interruption	中断	任务运行到一半被收回或停止
serverless	无服务器	不用自己管理服务器就能运行代码
managed service	托管服务	由 AWS 负责运行和维护的服务
container	容器	把程序和它的依赖打包在一起
relational database	关系数据库	用表格存储数据，用 SQL 查询
data warehouse	数据仓库	用来分析大量数据的数据库
object storage	对象存储	用 API 存取整个文件，例如 S3
file system	文件系统	按文件和目录组织、可挂载的存储
latency	延迟	从发出请求到收到响应的时间
routing policy	路由策略	决定把用户引到哪里的规则
retrieval option	取回方式	从归档存储取数据的方式，快慢和价格不同
multi-factor authentication (MFA)	多重身份验证	登录时除密码外再验证一次
root user	根用户	账户里权限最大的登录身份
IAM role	IAM 角色	提供临时凭证的一种身份
least privilege	最小权限	只给完成工作所需的权限
permissions boundary	权限边界	限制一个用户或角色的最大权限
service control policy (SCP)	服务控制策略	限制组织里成员账户的最大权限
patching	打补丁	安装更新来修复漏洞
threat detection	威胁检测	发现恶意或可疑的活动

Well-Architected pillar	良好架构框架的支柱	评价架构的一个方面，例如成本优化
rightsizing	合理调整规模	让资源大小符合实际需要
Technical Account Manager (TAM)	技术客户经理	AWS 派给企业客户、主动提供指导的人

Examundo 是独立网站，与主办这些考试的机构没有隶属关系，也未获其认可。题目均为原创，不是考试真题。 examundo.tech/zh/aws-cloud-practitioner/