

Q1.一个组织目前在其数据中心托管大量频繁访问的数据，包括键值对和半结构化文档。他们计划将这些数据转移到 AWS。以下哪项服务最有效地满足了他们的需求？

- A、 亚马逊红移
- B、 亚马逊 RDS
- C、 亚马逊发电机 B
- D、 亚马逊极光

答案 C

分析： <https://aws.amazon.com/blogs/aws/amazon-dynamodb-internet-scale-data-storage-the-nosql-way/>

Q2 Lambda 函数必须对私有子网中的 Amazon RDS 数据库执行查询。允许 Lambda 函数访问 Amazon RDS 数据库需要哪些步骤？（选择两个。）

- A、 为 Amazon RDS 创建 VPC 端点。
- B、 在 Amazon RDS VPC 中创建 Lambda 函数。
- C、 更改 Lambda 安全组的入口规则，允许 Amazon RDS 安全组。
- D、 更改 Amazon RDS 安全组的入口规则，允许使用 Lambda 安全组。
- E、 将互联网网关（IGW）添加到 VPC，将专用子网路由到 IGW。

回答广告

分析：

Q3.解决方案架构师需要使用 Amazon Redshift 构建弹性数据仓库。架构师需要在另一个区域重建红移集群。架构师可以采取哪种方法来满足这一需求？

- A、 修改红移群集并将跨区域快照配置到其他区域。
- B、 修改 Redshift 集群以每天拍摄 Amazon EBS 卷的快照，并与其他区域共享这些快照。
- C、 修改红移集群并配置备份，并在其他区域指定 Amazon S3 bucket。
- D、 修改 Redshift 集群以在导出模式下使用 AWS 雪球，并将数据传递到其他区域。

答：

分析：

红移跨区域快照。

亚马逊红移快照-亚马逊红移：将快照复制到另一个区域；从快照还原群集

Q4.一个流行的电子商务应用程序在 AWS 上运行。应用程序遇到性能问题。数据库无法处理高峰期间的查询和加载量。数据库正在 RDS Aurora 引擎上以可用的最大实例大小运行。

管理员应该如何提高性能？

- A、 将数据库转换为 Amazon Redshift。
- B、 创建 CloudFront 发行版。
- C、 将数据库转换为使用 EBS 配置的 IOPS。
- D、 创建一个或多个读取副本。

答案 D 分析：

Q5.解决方案架构师正在设计一个新的三层网络电子商务网站的架构，该网站必须全天候可用。预计每分钟请求量在 100 到 10000 之间。根据一天中的时间、节假日和促销活动，使用情况可能会有所不同。设计应能够处理这些卷，并在必要时能够处理更高的卷。

架构师应该如何设计架构，以确保 web 层是成本优化的，并且能够处理预期的流量？（选择两个。）

- A、 在 ELB 后面的自动缩放组中启动 Amazon EC2 实例。
- B、 将所有静态文件存储在多 AZ Amazon Aurora 数据库中。
- C、 创建一个指向 Amazon S3 中静态内容的 CloudFront 分发。
- D、 使用亚马逊路线 53 将流量路由到正确的区域。
- E、 使用 Amazon S3 多部分上传来提高上传时间。

回答 AC 分析：

Q6.解决方案架构师正在设计一个三层 web 应用程序。架构师希望限制对数据库层的访问，以仅接受来自应用服务器的流量。然而，这些应用服务器属于自动缩放组，数量可能会有所不同。

架构师应该如何配置数据库服务器以满足需求？

- A、 配置数据库安全组以允许来自应用程序服务器 IP 地址的数据库流量。
- B、 配置数据库安全组以允许来自应用程序服务器安全组的数据库通信。
- C、 配置数据库子网网络 ACL 以拒绝来自应用层子网的所有入站非数据库流量。
- D、 配置数据库子网网络 ACL 以允许来自应用层子网的入站数据库流量。

答案 B 分析：

Q7 解决方案架构师正在为一家媒体公司设计一个解决方案，该解决方案将从 Amazon EC2 实例流式传输大量数据。数据流通常较大且连续，并且必须能够支持高达 500 MB/s。

哪种存储类型将满足此应用程序的性能要求？

- A、EBS 配置 IOPS SSD
- B、EBS 通用 SSD
- C、EBS 冷硬盘
- D、EBS 吞吐量优化 HDD

答案 D

分析：

Q8.在本地运行的传统应用程序需要解决方案架构师能够打开防火墙，以允许访问几个 Amazon S3 存储桶。架构师已与 AWS 建立了 VPN 连接。

架构师应该如何满足这一要求？

- A、创建允许从公司网络访问 Amazon S3 的 IAM 角色。
- B、在 Amazon EC2 上配置代理并使用 Amazon S3 VPC 端点。
- C、使用 Amazon API 网关进行 IP 白名单。
- D、在客户网关上配置 IP 白名单。

答：

分析：

Q9.解决方案架构师正在设计一个数据库解决方案，该解决方案必须支持高速率的随机磁盘读写。它必须提供一致的性能，并且需要长期的持久性。

哪种存储解决方案最能满足这些要求？

- A、Amazon EBS 配置的 IOPS 卷
- B、Amazon EBS 通用卷
- C、亚马逊 EBS 磁卷
- D、Amazon EC2 实例存储

答：

分析：

Q10.解决方案架构师正在使用 AWS Lambda 设计解决方案，其中不同的环境需要不同的数据库密码。

架构师应该如何以安全和可扩展的方式实现这一点？

- A、 为每个环境创建一个 Lambda 函数。
- B、 使用 Amazon DynamoDB 存储环境变量。
- C、 使用加密的 AWS Lambda 环境变量。
- D、 实现用于分配变量的专用 Lambda 函数。

答案 C

分析：

解决方案架构师正在设计一个高可用性的网站，该网站由 AWS 外部托管的多个 web 服务器提供服务。如果实例没有响应，架构师需要将其从旋转中移除。满足这一要求的最有效方法是什么？

- A、 使用 Amazon CloudWatch 监控利用率。
- B、 使用 Amazon API 网关监控可用性。
- C、 使用 Amazon 弹性负载均衡器。
- D、 使用亚马逊路线 53 进行健康检查。

答案 D

分析：aws 之外的

Web 服务器

Q11 公司托管了一个流行的 web 应用程序。web 应用程序连接到在专用 VPC 子网中运行的数据库。只有通过 SSL 连接的客户才能访问 web 服务器。RDS MySQL 数据库服务器必须只能从 web 服务器访问。

架构师应该如何设计解决方案以满足需求，而不影响正在运行的应用程序？

- A、 在 web 服务器的子网上创建网络 ACL，并允许 HTTPS 入站和 MySQL 出站。
将数据库和 web 服务器放在同一子网上。
- B、 在 web 服务器的安全组上打开 HTTPS 端口，并将源设置为 0.0.0/0。打开数据库安全组上的 MySQL 端口并将其连接到 MySQL 实例。将源设置为 Web 服务器安全组。
- C、 在 web 服务器的子网上创建网络 ACL，并允许 HTTPS 入站，并将源指定为 0.0.0/0。
在数据库子网上创建网络 ACL，允许 web 服务器的 MySQL 端口入站，并拒绝所有出站流量。
- D、 在 web 服务器的安全组上打开 MySQL 端口，并将源设置为 0.0.0/0。在数据库安全组中打开 HTTPS 端口并将其连接到 MySQL 实例。将源设置为 Web 服务器安全组。

答案 B

分析:

Q12.如果一个组织需要一个易于管理和可扩展的平台来托管在 Nginx 上运行的 web 应用程序，那么应该使用哪种服务？

- A、AWSλ
- B、自动缩放
- C、AWS 弹性豆茎
- D、弹性负载平衡

答案 C 分析:

Q13.开发人员正在为一个读写密集型的小型数据库创建一个新的在线事务处理（OLTP）应用程序。数据库中的单个表在一天中不断更新，开发人员希望确保数据库性能一致。哪个 Amazon EBS 存储选项将实现最一致的性能，以帮助维护应用程序性能？

- A、配置 IOPS SSD
- B、通用 SSD
- C、冷硬盘
- D、吞吐量优化 HDD

答:

分析:

Q14.解决方案架构师正在设计一个日志处理解决方案，该解决方案需要支持高达 500 MB/s 吞吐量的存储。数据由 Amazon EC2 实例顺序访问。

哪种 Amazon 存储类型满足这些要求？

- A、EBS 配置 IOPS SSD（io1）
- B、EBS 通用 SSD（gp2）
- C、EBS 吞吐量优化硬盘（st1）
- D、EBS 冷硬盘（sc1）

答案 C

分析: <https://aws.amazon.com/ebs/faqs/>

一家公司的开发团队计划创建一个包含数百万张图片的 Amazon S3 bucket。团队希望最大化 AmazonS3 的读取性能。

公司应使用哪种命名方案？ A、 添加日期作为前缀。

B、 添加序列 id 作为后缀。

C、 添加十六进制哈希作为后缀。

D、 添加十六进制哈希作为前缀。

答案 D

分析：<https://aws.amazon.com/premiumsupport/knowledge-center/s3-bucket-performance-improve/>

问题 16.解决方案架构师需要设计一个解决方案，使安全团队能够检测、审查和执行云环境中发生的安全事件的根本原因分析。架构师必须提供当前和未来 AWS 区域所有 API 事件的集中视图。

架构师应该如何完成这项任务？

A、 在每个区域启用 AWS CloudTrail 日志记录。对所有未来区域重复此操作。

B、 为所有地区的所有 AWS 服务启用 Amazon CloudWatch 日志，并将其聚合到单个 Amazon S3bucket 中。

C、 启用 AWS Trusted Advisor 安全检查并报告所有地区的所有安全事件。

D、 通过创建新的轨迹启用 AWS CloudTrail，并将轨迹应用于所有区域。

答案 D

分析：

Q17.一家公司有一个使用专有文件系统的遗留应用程序，并计划将该应用程序迁移到 AWS。

公司应该使用哪种存储服务？

A、 亚马逊发电机 B

B、 亚马逊 S3

C、 亚马逊 EBS

D、 亚马逊 EFS

答案 D

分析：

Q18.一家公司计划将 AWS 用于所有新的批处理工作负载。该公司的开发人员使用 Docker 容器进行新的批处理。系统设计必须全天候适应关键和非关键批处理工作负载。

解决方案架构师应该如何以经济高效的方式设计此体系结构？

- A、 购买保留实例以运行所有容器。使用自动缩放组来调度作业。
- B、 在现场实例上托管容器管理服务。使用保留实例运行 Docker 容器。
- C、 使用 Amazon ECS 编排和自动扩展组：一个具有保留实例，一个具有点实例。
- D、 使用 Amazon ECS 管理容器编排。购买保留实例以同时运行所有批处理工作负载。

答案 C 分析：

Q19.一家公司正在评估亚马逊 S3 作为其日常分析师报告的数据存储解决方案。该公司对静态数据的安全性实施了严格的要求。具体而言，CISO 要求使用信封加密，并对信封密钥的使用、加密密钥的自动轮换以及加密密钥的使用时间和使用人的可见性进行单独许可。

解决方案架构师应采取哪些步骤来满足 CISO 要求的安全要求？

- A、 创建一个 AmazonS3 存储桶来存储报告，并使用客户提供的密钥（SSE-C）进行服务器端加密。
- B、 创建一个 AmazonS3 存储桶来存储报告，并使用 AmazonS 托管密钥（SSE-S3）进行服务器端加密。
- C、 创建一个 AmazonS3 存储桶来存储报告，并使用 AWS KMS 托管密钥（SSE-KMS）进行服务器端加密。
- D、 创建一个 Amazon S3 存储桶来存储报告，并使用 Amazon S33 版本控制和服务端加密，并使用 Amazon S3 托管密钥（SSE-S3）。

答案 C

分析：

如果客户的生产应用程序经常覆盖和删除数据，则每次请求时，应用程序都需要最新版本的数据。解决方案架构师应该推荐哪种存储来适应此用例？

- A、 亚马逊 S3
- B、 亚马逊 RDS
- C、 亚马逊红移
- D、 AWS 存储网关

答：

分析：

Q20.解决方案架构师有五个 web 服务器为域请求提供服务。以下哪项 Amazon Route 53 路由策略可以在所有健康的 web 服务器之间随机分配流量？

- A、简单
- B、故障转移
- C、加权
- D、多值

答案 D

分析：<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html>

Q21.在线事件注册系统托管在 AWS 中，使用 ECS 托管其前端层，并使用配置了多 AZ 的 RDS 托管其数据库层。哪些事件将使 Amazon RDS 自动执行到备用副本的故障切换？（选择两个。）

- A、在读取副本失败的情况下
- B、辅助数据库实例上的计算单元故障
- C、主可用性区域中的可用性损失
- D、主服务器上的存储故障
- E、辅助数据库实例上的存储失败

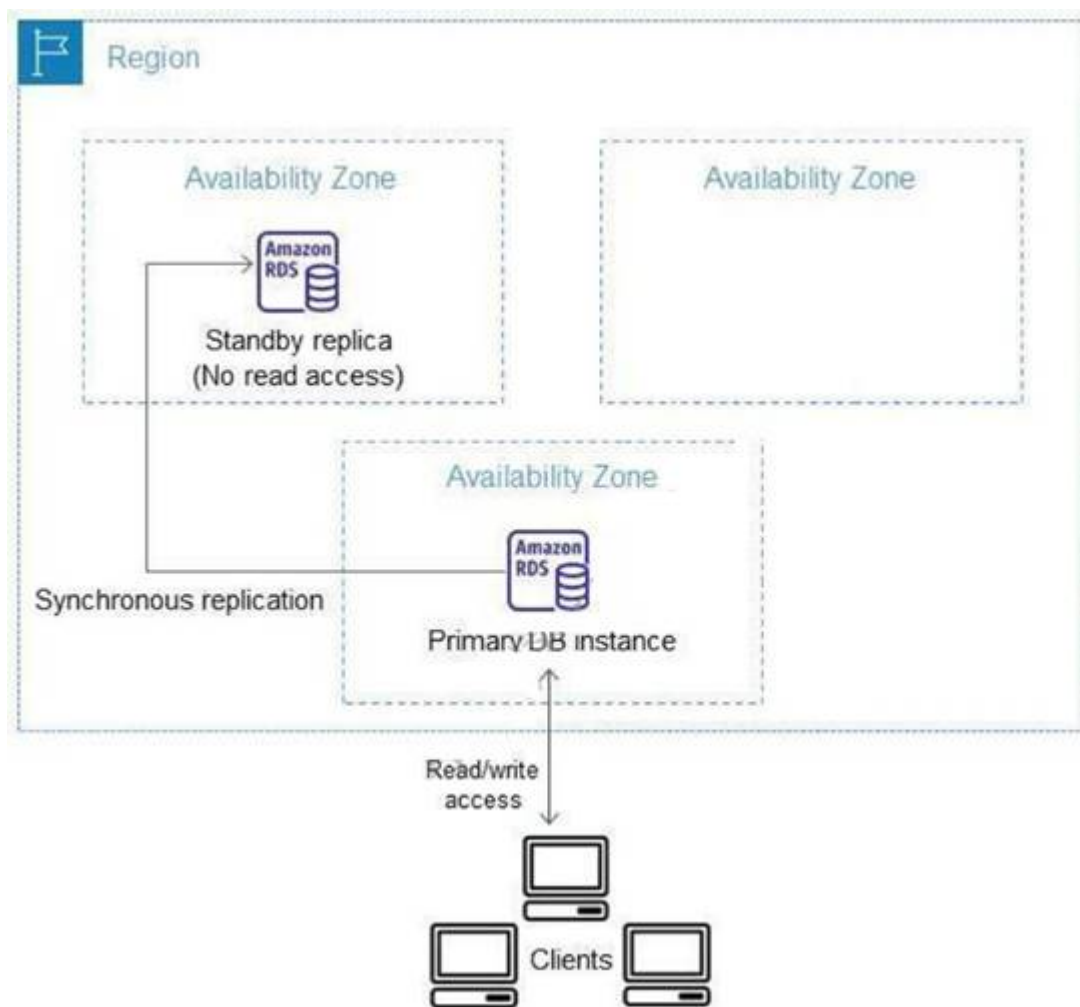
对裁谈会的答复

分析：

Amazon RDS 为使用多 AZ 部署的 DB 实例提供高可用性和故障转移支持。亚马逊 RDS 使用多种不同的技术提供故障切换支持。Oracle、PostgreSQL、MySQL 和 MariaDB 实例的多 AZ 部署使用亚马逊的故障转移技术。SQL Server DB 实例使用 SQL Server 数据库镜像（DBM）。

在多 AZ 部署中，Amazon RDS 自动在不同的可用性区域中提供和维护同步备用副本。主数据库实例跨可用性区域同步复制到备用副本，以提供数据冗余，消除 I/O 冻结，并将系统备份期间的延迟峰值降至最低。以高可用性运行数据库实例可以提高计划系统维护期间的可用性，并帮助保护数据库免受数据库实例故障和可用性区域中断的影响。

AmazonRDS 检测并自动从多 AZ 部署的最常见故障场景中恢复，因此您可以在没有管理干预的情况下尽快恢复数据库操作。



高可用性功能不是只读场景的扩展解决方案；您不能使用备用副本来服务读取流量。要为只读通信提供服务，应使用读取副本。出现以下任何情况时，Amazon RDS 会自动执行故障切换：主可用性区域中的可用性丢失。与主服务器的网络连接中断。主计算机上的计算单元故障。主服务器上的存储失败。

因此，正确答案是：

- 主可用性区域中的可用性损失
- 主服务器上的存储故障

以下选项不正确，因为所有这些方案都不会影响主数据库。

仅当主数据库是受影响的数据库时，才会发生自动故障转移。

- 辅助数据库实例上的存储失败
- 在读取副本失败的情况下
- 辅助数据库实例上的计算单元故障

参考文献：<https://aws.amazon.com/rds/details/multi-az/>

Q22.一家金融公司希望将其数据存储存储在 Amazon S3 中，但同时，他们希望将频繁访问的数据存储在本地服务器上。这是因为他们没有扩展本地存储的选项，这就是为什么他们正在寻找适合 AWS 使用的可扩展存储服务。

- A、使用亚马逊冰川
- B、对于频繁访问的数据，同时使用 Elasticache 和 S3
- C、使用带有 EBS 卷的 EC2 实例组来存储常用数据
- D、使用 Amazon 存储网关-缓存卷

答案 D

分析：

通过使用缓存卷，您可以将数据存储存储在 Amazon 简单存储服务（Amazon S3）中，并在本地网络中保留频繁访问的数据子集的副本。缓存卷在主存储上节省了大量成本，并最大限度地减少了在本地扩展存储的需要。您还可以保持对频繁访问数据的低延迟访问。这是该场景的最佳解决方案。

使用带有 EBS 卷的 EC2 实例组来存储常用数据是不正确的，因为 EC2 实例不是存储服务，它不提供所需的耐用性和可扩展性。

对频繁访问的数据同时使用 Elasticache 和 S3 是不正确的，因为这不是有效的。此外，问题明确指出，频繁访问的数据应该存储在本地服务器上，而不是 AWS 上。

使用亚马逊冰川是不正确的，因为它主要用于数据存档。

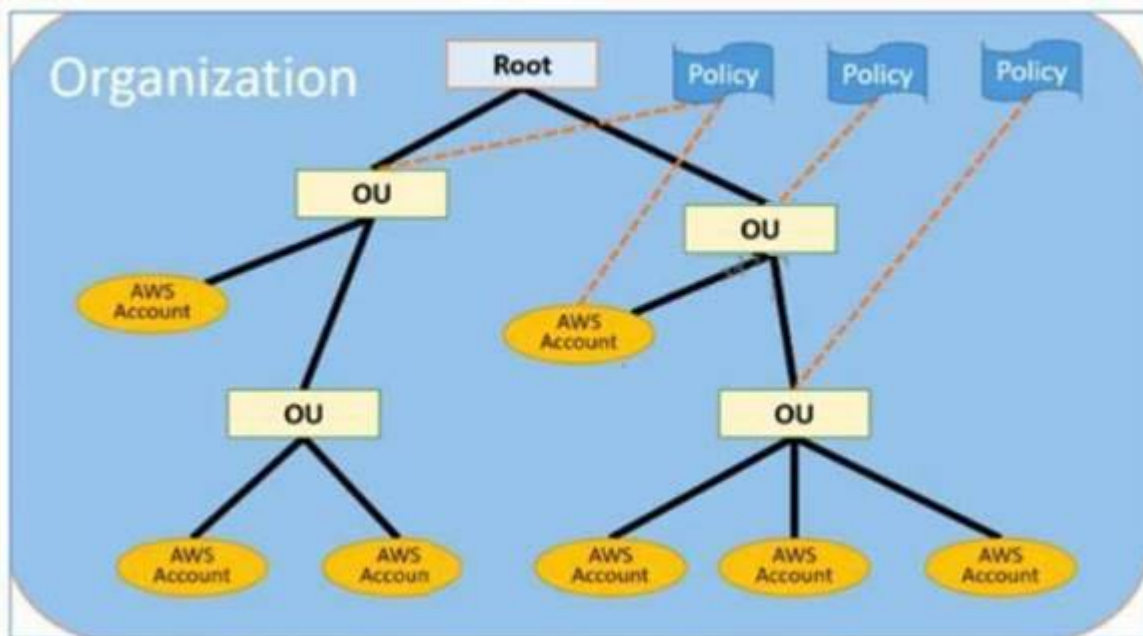
问题 23.一家跨国制造公司在 AWS 中拥有多个账户，以分离财务、人力资源、工程和许多其他部门。需要确保对服务和行动的某些访问受到适当控制，以符合公司的安全政策。作为解决方案架构师，哪种方式最适合设置公司的多账户 AWS 环境？

- A、通过身份联合向外部认证用户提供访问。设置 IAM 角色，为每个部门的用户指定权限，这些用户的身份与您的组织或第三方身份提供程序联合。
- B、通过设置对公司每个 AWS 账户的跨账户访问，连接所有部门。根据各自的部门创建 IAM 策略并将其附加到资源，以控制访问。
- C、设置可应用于所有 AWS 帐户的通用 IAM 策略。
- D、使用 AWS 组织和服务控制策略来控制每个帐户上的服务。

答案 D

分析：

使用 AWS 组织和服务控制策略来控制每个帐户上的服务是正确答案。参见下图：



AWS 组织为多个 AWS 帐户提供基于策略的管理。通过组织，您可以创建帐户组、自动创建帐户、应用和管理这些组的策略。组织使您能够跨多个帐户集中管理策略，而无需自定义脚本和手动流程。它允许您创建服务控制策略（SCP），集中控制多个 AWS 帐户的 AWS 服务使用。设置可应用于所有 AWS 帐户的通用 IAM 策略是不正确的，因为不可能为多个 AWS 帐户创建通用 IAM 政策。

该选项表示：通过设置对公司每个 AWS 帐户的跨帐户访问，连接所有部门。根据各自的部门创建 IAM 策略并将其附加到您的资源以控制访问是不正确的，因为尽管您可以设置对每个部门的跨帐户访问，但与使用 AWS 组织和服务控制策略（SCP）相比，这需要大量配置。如果您只有两个帐户要管理，而不是多个帐户，则跨帐户访问将是更合适的选择。

该选项表示：通过身份联合向外部认证用户提供访问。设置 IAM 角色以指定来自每个部门的用户的权限，这些用户的身份由您的组织或第三方身份提供商联合，这是不正确的，因为此选项侧重于为您的 AWS 帐户设置的身份联合身份验证，而不是多个 AWS 帐户的 IAM 策略管理。与此选项相比，AWS 组织和服务控制策略（SCP）的组合是更好的选择。

Q24 一家公司推出了一个全球新闻网站，部署到 AWS 并使用 MySQL RDS。该网站拥有来自世界各地的数百万观众，这意味着该网站阅读了大量数据库工作。所有数据库事务必须符合 ACID，以确保数据完整性。在这种情况下，以下哪项是提高 MySQL 数据库读取吞吐量的最佳选项？

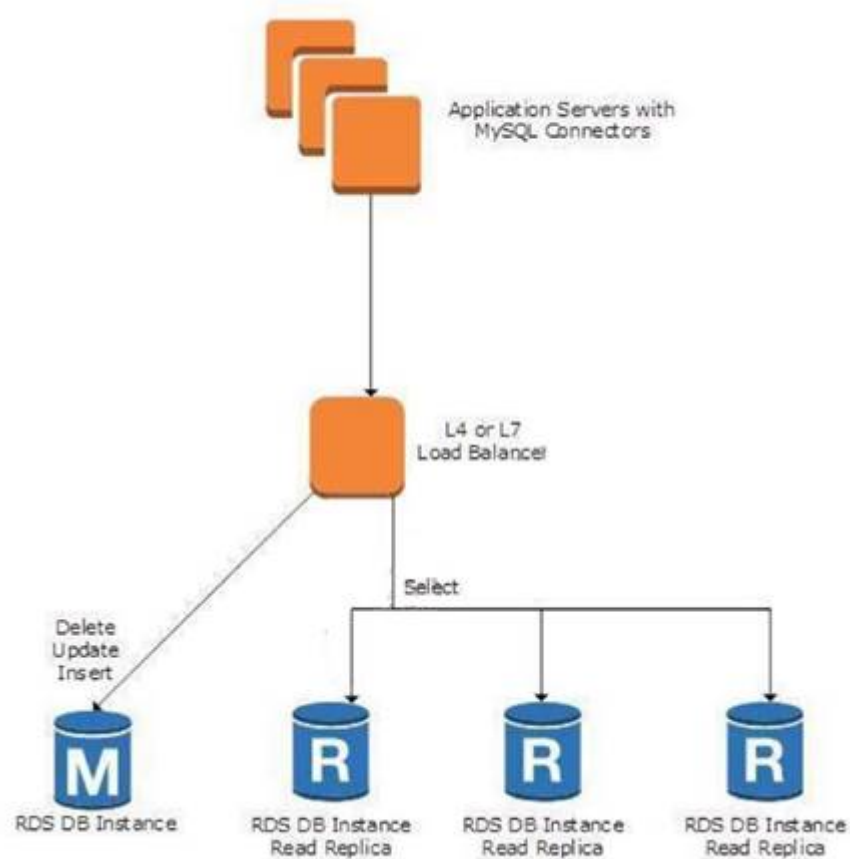
- A、启用 Amazon RDS 备用副本
- B、启用 Amazon RDS 读取副本
- C、使用 SQS 将请求排队
- D、启用多 AZ 部署

答案 B

分析：

Amazon RDS 读取副本为数据库（DB）实例提供了增强的性能和耐用性。此功能使您可以轻松地弹性扩展，超出单个数据库实例的容量限制，以应对读取繁重的数据库工作负载。您可以创建给定源数据库实例的一个或多个

个副本，并从数据的多个副本提供高容量应用程序读取流量，从而提高聚合读取吞吐量。当需要成为独立数据库实例时，还可以升级读取副本。Amazon RDS for MySQL、MariaDB、Oracle 和 PostgreSQL 以及 Amazon Aurora 中提供了读取副本。



启用多 AZ 部署是不正确的，因为多 AZ 配置功能主要用于实现数据库的高可用性和故障转移支持。启用 Amazon RDS 备用副本是不正确的，因为在多 AZ 部署中使用备用副本，因此它不是减少读取繁重数据库工作负载的解决方案。使用 SQS 将请求排队是不正确的。虽然 SQS 队列可以有效地管理请求，但它本身不能完全提高数据库的读取吞吐量。

一家初创公司计划开发一款多人游戏，使用 UDP 作为客户端和游戏服务器之间的通信协议。用户的数据将存储在键值存储中。作为解决方案架构师，您需要实现一个将流量分布到多个服务器的解决方案。

- A、使用网络负载均衡器分发流量，并将数据存储在 Amazon Aurora 中。
- B、使用应用程序负载均衡器分发流量，并将数据存储在 Amazon DynamoDB 中。
- C、使用网络负载均衡器分配流量，并将数据存储在 Amazon DynamoDB 中。
- D、使用应用程序负载均衡器分发流量，并将数据存储在 Amazon RDS 中。

答案 C

分析：

网络负载均衡器在开放系统互连（OSI）模型的第四层起作用。它每秒可以处理数百万个请求。负载均衡器收到连接请求后，将从目标组中为默认规则选择一个目标。对于 UDP 流量，负载均衡器使用基于协议、源 IP 地址、源端口、目标 IP 地址和目标端口的流哈希算法来选择目标。UDP 流具有相同的源和目标，因此在其整个生命周期内始终路由到单个目标。不同的 UDP 流具有不同的源 IP 地址和端口，因此可以将它们路由到不同的目标。

Feature



Protocols	HTTP, HTTPS
Platforms	VPC
Health checks	''''
CloudWatch metrics	ti'
Logging	V
Zonal fail-over	v'
Connection draining 1...Jv~*◆v◆, - - - - -t\、\	t,/



在这种情况下，一家初创公司计划创建一个多人游戏，使用 UDP 作为通信协议。由于 UDP 是第 4 层流量，我们可以限制使用网络负载均衡器的选项。用户的数据将存储在键值存储中。这意味着我们应该选择 Amazon DynamoDB，因为它支持文档和键值存储模型。

因此，正确的答案是：使用网络负载均衡器分配流量，并将数据存储在 Amazon 中发电机 B。“使用应用程序负载均衡器分发流量并将数据存储在 Amazon DynamoDB 中”的选项不正确，因为应用程序负载均衡器不支持 UDP。请记住，UDP 是第 4 层流量。因此，您应该使用网络负载均衡器。“使用网络负载均衡器分配流量并将数据存储在 Amazon Aurora 中”的选项是不正确的，因为 Amazon Aurora 是一种关系数据库服务。您应该使用 Amazon DynamoDB 而不是 Aurora。

“使用应用程序负载均衡器分发流量并将数据存储在 Amazon RDS 中”选项不正确，因为应用程序负载均衡器仅支持应用程序流量（第 7 层）。此外，Amazon RDS 不适合作为键值存储。您应该使用 DynamoDB，因为它支持文档和键值存储模型。

问题 26.一家技术公司目前拥有内部基础设施。他们目前存储空间不足，希望能够使用 AWS 云扩展存储空间。哪些 AWS 服务可以帮助他们实现这一要求？

A、Amazon 弹性块存储

B、亚马逊存储网关

C、亚马逊 EC2

D、亚马逊 SQS

答案 B

分析：

AWS 存储网关将本地软件设备与基于云的存储连接起来，以在本地 IT 环境和 AWS 存储基础设施之间提供数据安全功能的无缝集成。您可以使用该服务将数据存储在 AWS 云中，以实现可扩展和经济高效的存储，帮助维护数据安全。

Amazon EC2 是不正确的，因为这是一个计算服务，而不是存储服务。

Amazon 弹性块存储不正确，因为 EBS 主要用作 EC2 实例的存储。

Amazon SQS 是不正确的，因为这是一种消息队列服务，不会扩展您的内部存储容量。

Q27.大型跨国投资银行有一个 web 应用程序，它至少需要 4 个 EC2 实例才能运行，以确保它能够满足全球用户的需求。指示您确保此系统的容错性。以下哪项是最佳选择？

A、在应用程序负载均衡器后面的一个可用性区域中部署具有 4 个实例的自动扩展组。

B、在应用程序负载均衡器后面的 4 个可用性区域中的每个区域中部署一个具有 1 个实例的自动扩展组。

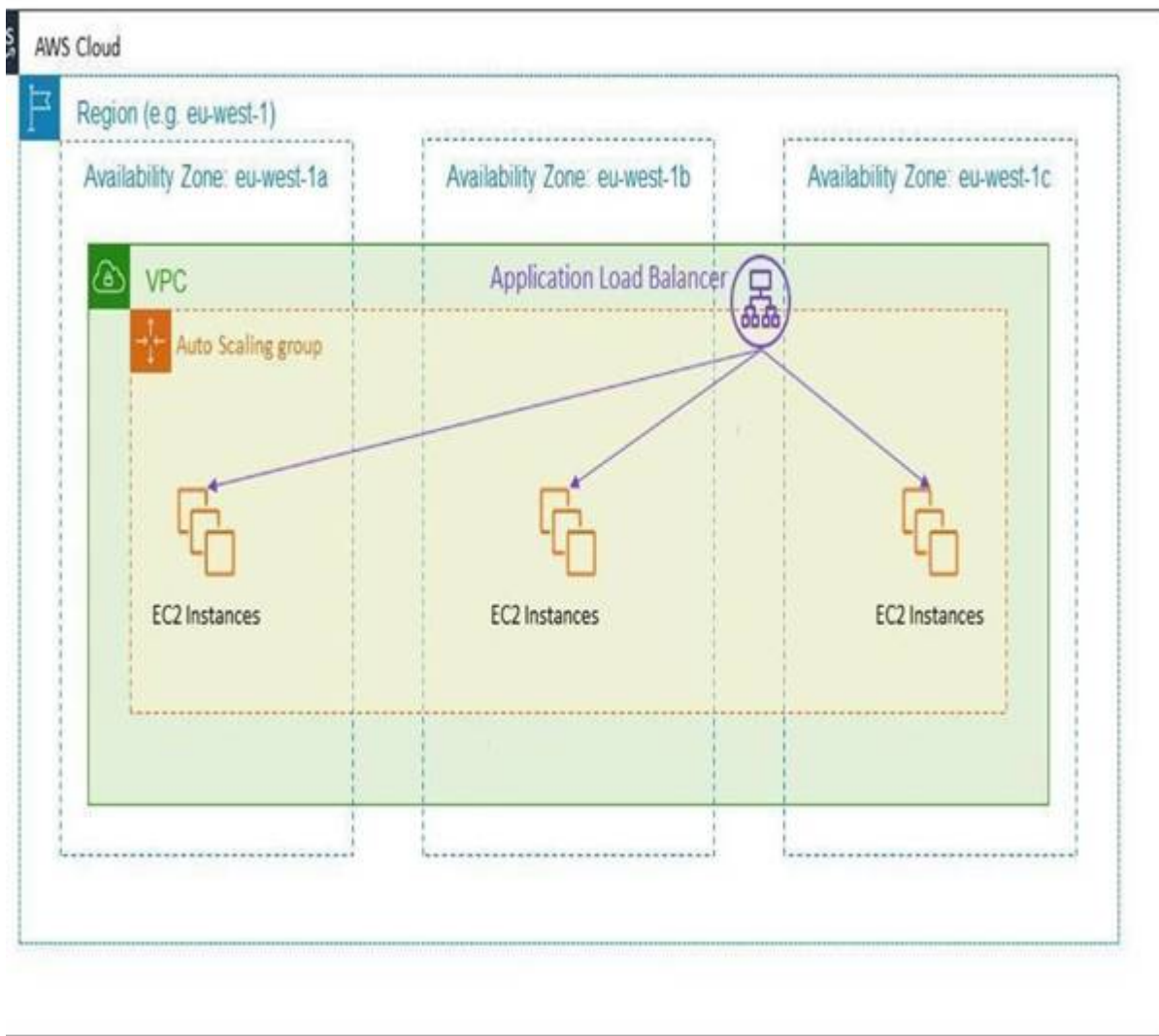
C、在应用程序负载均衡器后面的 3 个可用性区域中的每个区域中部署一个具有 2 个实例的自动扩展组。

D、在应用程序负载均衡器后面的 2 个可用性区域中的每个区域中部署一个具有 2 个实例的自动扩展组。

答案 C

分析：

容错是指即使用于构建系统的某些组件发生故障，系统仍能保持运行的能力。在 AWS 中，这意味着在服务器故障或系统故障的情况下，运行 EC2 实例的数量不应低于系统正常工作所需的最小实例数量。因此，如果应用程序至少需要 4 个实例，则在其中一个可用性区域发生中断或出现服务器问题时，应至少运行 4 个实例。



容错和高可用性之间的区别之一是前者指运行实例的最小数量。例如，您的系统至少需要 4 个运行实例，当前在两个可用性区域中部署了 6 个运行实例。其中一个可用性区域发生组件故障，导致 3 个实例失效。在这种情况下，系统仍然可以被视为高可用性，因为仍然有运行的实例可以容纳请求。但是，它不是容错的，因为未满足所需的最少四个实例。因此，正确的答案是：部署一个自动扩展组，在应用程序负载均衡器后面的 3 个可用性区域中的每个区域中部署 2 个实例。

该选项表示：部署一个自动扩展组，在一个应用程序负载均衡器是不正确的，因为如果一个可用性区域失效，则在所需的 4 个最小实例中，只有 2 个运行实例可用。尽管自动伸缩组可以再增加 2 个实例，但 web 应用程序的容错性已经受到了影响。

“在应用程序负载均衡器后面的一个可用性区域中部署一个具有 4 个实例的自动扩展组”选项是不正确的，因为如果可用性区域失效，将没有运行实例可用于容纳请求。

该选项表示：部署一个自动扩展组，在一个应用程序负载均衡器是不正确的，因为如果一个可用区域失效，则只有 3 个实例可用于容纳请求。

Q28 公司希望从中央数据湖查询驻留在多个 AWS 账户中的数据。每个帐户都有自己的 Amazon S3 存储桶，存储其业务功能特有的数据。不同帐户的用户必须根据其角色被授予访问数据湖的权限。哪种解决方案在满足所需访问模式的同时将开销和成本降至最低？

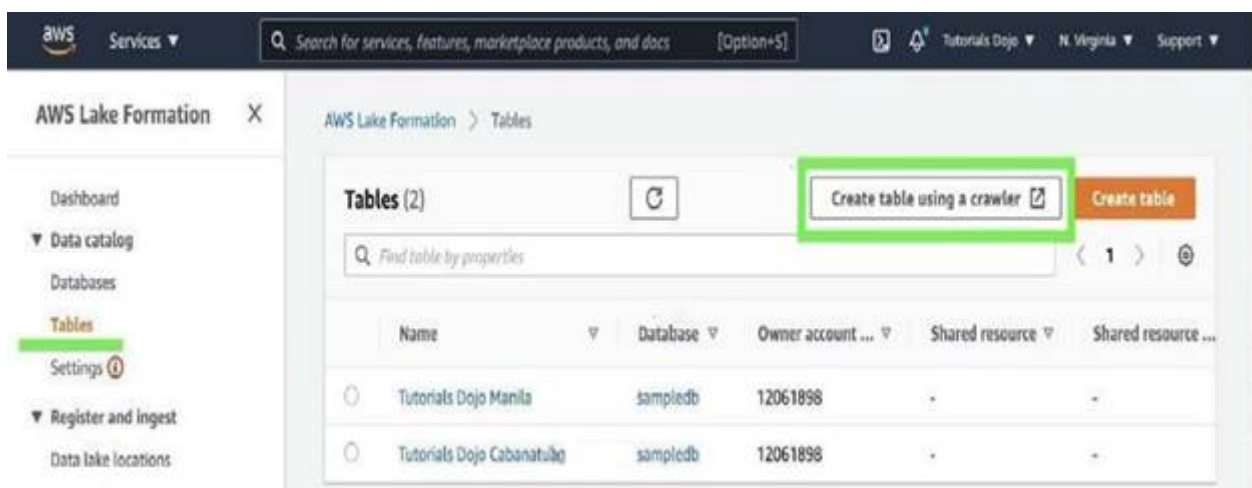
- A、 使用 AWS Central Tower 集中管理每个帐户的 S3 存储桶。
- B、 创建一个调度 Lambda 函数，用于将数据从多个帐户传输到 centralaccount 的 S3 存储桶
- C、 使用 AWS Kinesis Firehose 将多个帐户中的数据合并到单个帐户中。
- D、 使用 AWS Lake Formation 将多个帐户的数据合并到单个帐户中。

答案 D

分析：

AWS Lake Formation 是一项服务，可以在几天内轻松建立安全的数据湖。数据湖是一个集中、管理和安全的存储库，它以原始形式存储您的所有数据，并为分析做好准备。数据湖使您能够打破数据孤岛，并结合不同类型的分析，以获得见解并指导更好的业务决策。

亚马逊 S3 形成湖泊形成的储存层。如果已经使用了 S3，则通常首先注册包含数据的现有 S3 存储桶。湖形成数据湖创建新的桶，并将数据导入其中。AWS 总是将这些数据存储您的帐户中，只有您可以直接访问这些数据。



AWS Lake Formation 与 AWS Glue 集成，您可以使用它创建描述可用数据集及其适当业务应用程序的数据目录。Lake Formation 允许您定义策略，并在粒度级别通过简单的“授予和撤销数据权限”集控制数据访问。您可以使用联合为 IAM 用户、角色、组和 Active Directory 用户分配权限。您可以对目录对象（如表和列）而不是桶和对象指定权限。

因此，正确答案是：使用 AWS Lake Formation 将来自多个帐户的数据合并到单个帐户中。

“使用 AWS Kinesis Firehose 将多个帐户的数据合并到单个帐户”选项不正确。在每个帐户中设置 Kinesis Firehose 以将数据移动到单个位置既昂贵又不切实际。更好的方法是建立与 AWS Lake Formation 免费的交叉帐户共享。

“创建一个调度 Lambda 函数，用于将数据从多个帐户传输到中央帐户的 S3 存储桶”选项不正确。这可以通过利用 AWS SDK 来实现，但实现将是困难的，而且管理起来相当具有挑战性。请记住，场景明确提到解决方案必须最小化管理开销。

“使用 AWS 中央塔集中管理每个帐户的 S3 存储桶”选项不正确，因为 AWS 中央塔台服务主要用于管理和
管理多个 AWS 帐户，而不仅仅是 S3 存储池。使用 AWS 湖泊形成服务是更合适的选择。

**Q29A 媒体公司需要配置 Amazon S3 bucket，为面向公众的 web 应用程序提供静态资产。哪些方法可以确
保上传到 S3 bucket 的所有对象都可以通过互联网公开读取？（选择两个。）**

- A、 创建 IAM 角色，将 S3 存储桶中的对象设置为公共读取。
- B、 配置 S3 bucket 的跨源资源共享（CORS），以允许从所有域公开访问对象。
- C、 什么也不做。默认情况下，Amazon S3 对象已经是公共的。
- D、 配置 S3 存储桶策略，将所有对象设置为公共读取。
- E、 使用 S3 控制台上载对象时，授予对对象的公共读取访问权限。

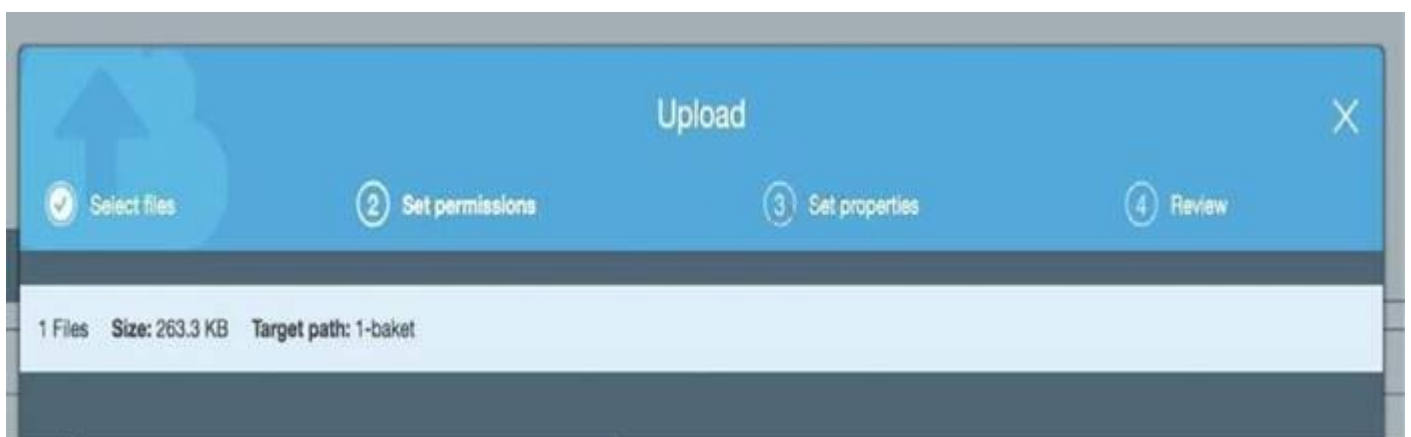
答：

分析：

默认情况下，所有 Amazon S3 资源（如桶、对象和相关子资源）都是私有的，这意味着只有创建它的
AWS 帐户持有人（资源所有者）才能访问资源。资源所有者可以通过编写访问策略向其他人授予访问权限。
在 S3 中，您还可以在上传期间设置对象的权限，使其公开。AmazonS3 提供的访问策略选项大致分为基于
资源的策略和用户策略。附加到资源（bucket 和对象）的访问策略称为基于资源的策略。

例如，存储桶策略和访问控制列表（ACL）是基于资源的策略。您还可以将访问策略附加到帐户中的用户。
这些称为用户策略。您可以选择使用基于资源的策略、用户策略或这些策略的组合来管理对 Amazon S3 资源
的权限。

您还可以在上载期间管理对象的公共权限。在“管理公共权限”下，您可以向普通公众（世界上的每个人）授予
对您上载的所有文件的对象的读取权限。授予公共读访问权限适用于一小部分用例，例如当 bucket 用于网站
时。



因此，正确答案是：

- 使用 S3 控制台上载对象时，授予对对象的公共读取访问权限。
- 配置 S3 存储桶策略，将所有对象设置为公共读取。

“配置 S3 bucket 的跨源资源共享（CORS）以允许从所有域公开访问对象”选项不正确。CORS 将只允许来自一个域（travel.cebu.com）的对象加载到另一个域中（palawan.com）。它不一定会在整个互联网上公开对象供公众访问。该选项表示：创建 IAM 角色以将 S3 存储桶中的对象设置为公共读取是不正确的。您可以创建 IAM 角色并将其附加到 EC2 实例，以便从 S3 bucket 中检索对象或添加新对象。IAM 角色本身不能直接将 S3 对象公开或更改每个对象的权限。

选项是：什么都不做。默认情况下 Amazon S3 对象已经是公共的是不正确的，因为默认情况下，所有 S3 资源都是私有的，因此只有创建资源的 AWS 帐户才能访问它们。

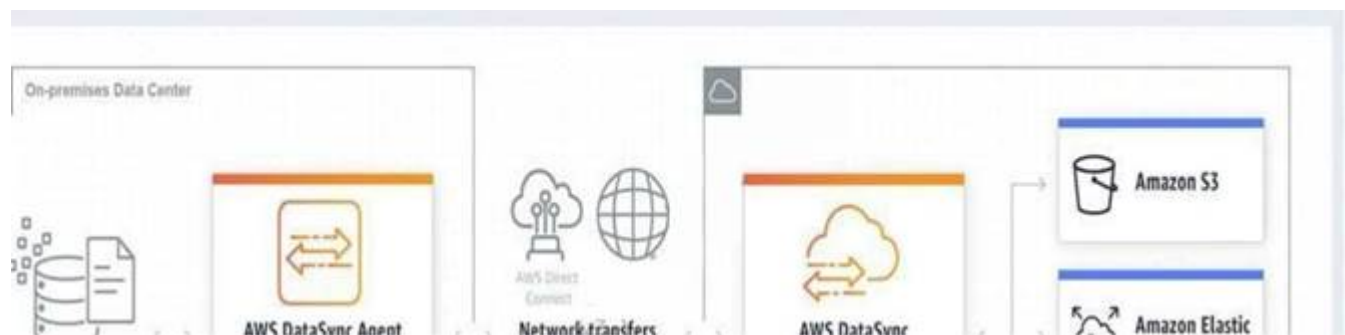
Q30.历史记录和频繁访问的数据都存储在内部存储系统中。当前数据量以指数速度增长。由于存储容量接近极限，该公司的解决方案架构师决定将历史记录转移到 AWS，以释放活动数据的空间。以下哪种体系结构在成本和运营管理方面提供了最佳解决方案？

- A、 使用 AWS 数据同步将历史记录从本地移动到 AWS。选择 Amazon S3 Glacier DeepArchive 作为数据的目的地。
- B、 使用 AWS 存储网关将历史记录从本地移动到 AWS。选择 Amazon S3 Glacier Deep Archive 作为数据的目的地。
- C、 使用 AWS 数据同步将历史记录从本地移动到 AWS。选择 Amazon S3 标准作为数据的目标。修改 S3 生命周期配置，在 30 天后将数据从标准层移动到 Amazon S3 Glacier Deep Archive。
- D、 使用 AWS 存储网关将历史记录从本地移动到 AWS。选择亚马逊 S3 冰川作为数据的目的地。修改 S3 生命周期配置，在 30 天后将数据从标准层移动到 Amazon S3 Glacier Deep Archive。

答：

分析：

AWS 数据同步使在本地存储和 Amazon S3、Amazon 弹性文件系统（Amazon EFS）或 Amazon FSx for Windows 文件服务器之间在线移动大量数据变得简单快捷。与数据传输相关的手动任务可能会降低迁移速度并加重 IT 操作负担。DataSync 消除或自动处理许多这些任务，包括脚本复制作业、调度和监控传输、验证数据以及优化网络利用率。DataSync 软件代理连接到您的网络文件系统（NFS）、服务器消息块（SMB）存储和自管理对象存储，因此您无需修改应用程序。DataSync 可以通过互联网或 AWS 直接连接链接以比开源工具快 10 倍的速度传输数百 TB 和数百万文件。您可以使用 DataSync 将活动数据集或存档迁移到 AWS，将数据传输到云中进行及时分析和处理，或将数据复制到 AWS 以实现业务连续性。开始使用数据同步很容易：部署数据同步代理，将其连接到文件系统，选择 AWS 存储资源，并开始在它们之间移动数据。您只为移动的数据付费。



由于问题主要是将历史记录从本地移动到 AWS，因此使用 AWS 数据同步是更合适的解决方案。您可以使用 DataSync 将冷数据从昂贵的内部存储系统直接移动到持久安全的长期存储，如 Amazon S3 Glacier 或 Amazon S3 Glacier Deep Archive。

因此，正确的答案是这样的选项：使用 AWS 数据同步将历史记录从本地移动到 AWS。选择 Amazon S3 Glacier Deep Archive 作为数据的目的地。

以下选项均不正确：

- 使用 AWS 存储网关将历史记录从本地移动到 AWS。选择 Amazon S3 Glacier Deep Archive 作为数据的目的地。
- 使用 AWS 存储网关将历史记录从本地移动到 AWS。选择 Amazon S3 Glacier 作为数据的目的地。修改 S3 生命周期配置，在 30 天后将数据从标准层移动到 Amazon S3 Glacier Deep Archive。

虽然您可以使用存储网关将数据从本地复制到 AWS，但它不适用于将大量数据传输到 AWS。存储网关主要用于提供对数据的低延迟访问，在本地缓存频繁访问的数据，同时在亚马逊云存储服务中安全持久地存储存档数据。Storage Gateway 通过只发送更改的数据并压缩数据来优化到 AWS 的数据传输。

该选项表示：使用 AWS 数据同步将历史记录从本地移动到 AWS。选择 AmazonS3 标准作为数据的目标。修改 S3 生命周期配置以在 30 天后将数据从标准层移动到 Amazon S3 Glacier Deep Archive 是不正确的，因为使用 AWS DataSync，您可以将数据从本地直接传输到 Amazon S3 GlacierDeep Architecture。您不必配置 S3 生命周期策略并等待 30 天将数据移动到 Glacier Deep Archive。

问题 31.一家跨国公司一直在构建其新的数据分析平台，该平台具有高性能计算工作负载（HPC），这需要一个可扩展的、符合 POSIX 的存储服务。数据需要跨多个 AZ 冗余存储，并允许来自托管在多个可用性区域上的数千个 EC2 实例的并发连接。以下哪种 AWS 存储服务最适合用于此场景？

- A、亚马逊松紧带
- B、Amazon 弹性文件系统
- C、亚马逊 EBS 卷
- D、亚马逊 S3

答案 B

分析：

在这个问题中，您应该注意这个短语，“允许来自多个 EC2 实例的并发连接”。

您可以选择各种 AWS 存储选项，但只要出现这些标准，请始终考虑使用

EFS 而不是使用 EBS 卷，它主要用作“块”存储，并且只能有一个到一个的连接

EC2 实例。Amazon EFS 是一个完全受管理的服务，可以轻松地在云中设置和扩展文件存储

亚马逊云。只需在 AWS 管理控制台中点击几下，即可创建文件系统，通过文件系统接口（使用标准操作系统文件 I/O API）访问 Amazon EC2 实例，并支持完整的文件系统访问语义（如强一致性和文件锁定）。

Amazon EFS 文件系统可以自动从千兆字节扩展到千兆字节，而无需提供存储。数十、数百甚至数千个 Amazon EC2 实例可以同时访问 Amazon EFS 文件系统，Amazon EFS 为每个 Amazon EC1 实例提供一致的性能。亚马逊 EFS 被设计为高度耐用和高度可用。

Q32. 公司需要实施一个解决方案，以处理全球用户的实时流数据。这将使他们能够跟踪和分析其网站和移动应用程序上全球分布的用户活动，包括点击流分析。解决方案应在地理位置接近用户的情况下处理数据，并以低延迟响应用户请求。以下哪种解决方案最适合此场景？

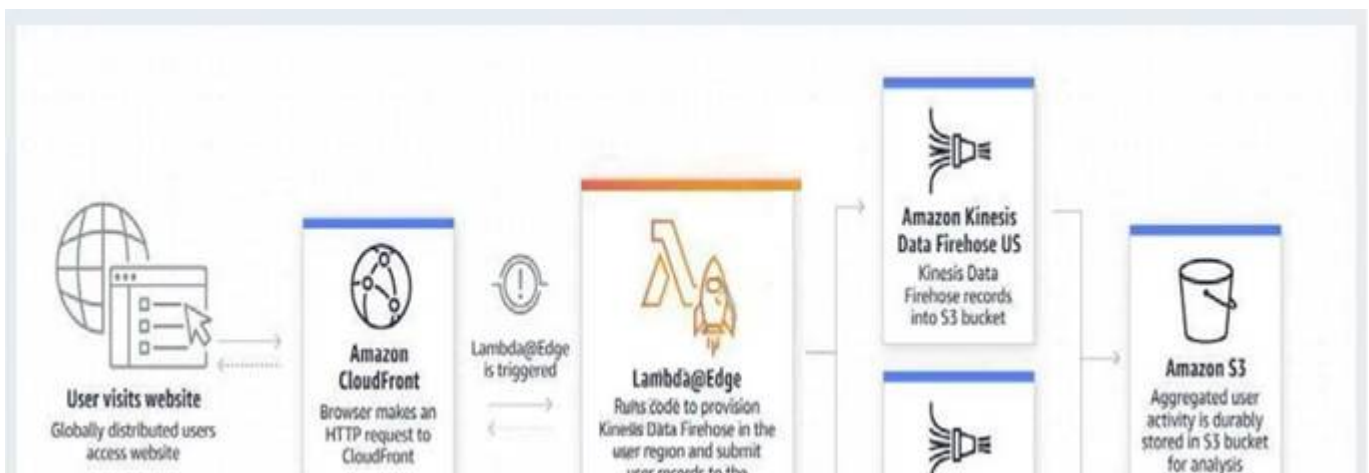
- A、 将 CloudFront 与 Lambda@Edge 以便在地理上接近用户并以低延迟响应用户请求的情况下处理数据。使用 Amazon Athena 处理实时流数据，并将结果持久存储到 Amazon S3 存储桶中。
- B、 使用具有地理邻近性路由策略的 CloudFront web 分发和路由 53，以处理与用户的地理邻近性数据，并以低延迟响应用户请求。使用 Kinesis 处理实时流数据，并将结果持久存储到 Amazon S3 存储桶中。
- C、 将 CloudFront 与 Lambda@Edge 以便在地理上接近用户并以低延迟响应用户请求的情况下处理数据。使用 Kinesis 处理实时流数据，并将结果持久存储到 Amazon S3 存储桶中。
- D、 使用具有基于延迟的路由策略的 CloudFront web 分发和路由 53，以便处理与用户地理接近的数据并以低延迟响应用户请求。使用 Kinesis 处理实时流数据，并将结果持久存储到 Amazon S3 存储桶中。

答案 C

分析：

Lambda@Edge 是 Amazon CloudFront 的一项功能，它可以让您更接近应用程序的用户运行代码，从而提高性能并减少延迟。具有 Lambda@Edge，您不必在世界各地的多个位置提供或管理基础设施。您只需支付所消耗的计算时间-当您的代码未运行时，不收取任何费用。具有 Lambda@Edge，您可以通过使 web 应用程序全球分布并提高其性能来丰富您的 web 应用程序—所有这些都无需服务器管理。Lambda@Edge 在中运行代码

对亚马逊云前端内容交付网络（CDN）生成的事件的响应。只需将代码上传到 AWS Lambda，它就可以在离最终用户最近的 AWS 位置以高可用性运行和扩展代码所需的一切。



使用 Lambda@Edge 与 Kinesis 一起，您可以处理实时流数据，以便跟踪和分析网站和移动应用程序上的全球分布用户活动，包括点击流分析。

因此，这个场景中的正确答案是这样的选项：将 CloudFront 与 Lambda@Edge 以便在接近用户的地理位置处理数据并以低延迟响应用户请求。使用 Kinesis 处理实时流数据，并将结果持久存储到 Amazon S3 存储桶中。

这些选项表示：使用 CloudFront web 分发和基于延迟的路由策略的路由 53，以便在地理位置接近用户的情况下处理数据，并以低延迟响应用户请求。使用 Kinesis 处理实时流数据，并将结果持久地存储到 Amazon S3 存储桶中，并使用 CloudFront web 分发和路由 53 以及地理邻近性路由策略，以便在地理位置接近用户的情况下处理数据并以低延迟响应用户请求。使用 Kinesis 处理实时流数据和将结果持久存储到 Amazon S3

存储桶都是不正确的，因为您只能使用路由 53 路由流量，因为它没有任何计算能力。该解决方案将无法处理和返回地理位置接近用户的数据，因为它不使用 Lambda@Edge。

选项表明：将 CloudFront 与 Lambda@Edge 以便在接近用户的地理位置处理数据并以低延迟响应用户请求。使用 Amazon Athena 处理实时流数据并将结果持久存储到 Amazon S3 存储桶是不正确的，因为尽管使用 Lambda@Edge 如果正确的话，Amazon Athena 只是一个交互式查询服务，使您能够使用标准 SQL 轻松分析 Amazon S3 中的数据。Kinesis 应用于实时处理流数据。

Q33.一家公司在使用默认网络 ACL 的公共子网中的 Linux Amazon EC2 实例上托管了一个 web 应用程序。该实例使用默认安全组，并具有附加的弹性 IP 地址。网络 ACL 已配置为阻止实例的所有流量。解决方案架构师必须允许端口 443 上的传入流量从任何源访问应用程序。哪些步骤组合将完成此要求？（选择两个。）

- A、在安全组中，添加一个新规则，以允许在端口 443 上从源 0.0.0/0 进行 TCP 连接
- B、在安全组中，创建新规则以允许端口 443 上的 TCP 连接到目标 0.0.0/0
- C、在网络 ACL 中，更新规则以允许端口 32768-65535 上的出站 TCP 连接到 destination0.0.0/0
- D、在网络 ACL 中，更新规则以允许端口 443 上的入站和出站 TCP 连接从源 0.0.0/0 到目标 0.0-0/0
- E、在网络 ACL 中，更新规则以允许端口 443 上的入站 TCP 连接从源 0.0.0/0 和端口 32768-65535 上的出站 TCP 连接到目标 0.0-0/0

答案：AE

分析：

要启用到实例上运行的服务的连接，关联的网络 ACL 必须允许服务正在侦听的端口上的入站流量，以及允许来自临时端口的出站流量。当客户端连接到服务器时，临时端口范围（1024-65535）中的随机端口将成为客户端的源端口。

然后，指定的临时端口将成为服务返回流量的目标端口，因此网络 ACL 中必须允许临时端口的出站流量。默认情况下，网络 ACL 允许所有入站和出站流量。如果网络 ACL 更具限制性，则需要显式允许来自临时端口范围的流量。

ACLs > acl-0f7a54f36f5c3a03f / Tutorials Dojo Network ACL - MINDORO

4f36f5c3a03f / Tutorials Dojo Network ACL - DAVAO

Actions ▾

6f5c3a03f

Default: No

VPC ID: vpc-23ad464a

Network ACL Outbound Rules

Outbound rules | Subnet associations | Tags

Rules (3)

Edit outbound rules

< 1 >

Type	Protocol	Port range	Destination	Allow/Deny
HTTPS (443)	TCP [6]	443	0.0.0.0/0	Allow
Custom TCP	TCP [6]	32768 - 65535	0.0.0.0/0	Allow
All traffic	All	All	0.0.0.0/0	Deny

Ephemeral Ports

Tutorials Dojo

发起请求的客户端选择临时端口范围。范围取决于客户端的操作系统。

- 许多 Linux 内核（包括 Amazon Linux 内核）使用端口 32768-61000。
- 来自弹性负载平衡的请求使用端口 1024-65535。
- 通过 Windows Server 2003 的 Windows 操作系统使用端口 1025-5000。
- Windows Server 2008 及更高版本使用端口 49152-65535。
- NAT 网关使用端口 1024-65535。
- AWS Lambda 函数使用端口 1024-65535。

例如，如果请求从 Internet 上的 Windows 10 客户端进入 VPC 中的 web 服务器，则网络 ACL 必须具有出站规则，以启用以端口 49152-65535 为目的地的流量。如果 VPC 中有一个实例是发起请求的客户端，则您的网络 ACL 必须具有入站规则，以便启用以特定于实例类型的临时端口为目的地的流量。

（亚马逊 Linux、Windows Server 2008 等）。在这种情况下，您只需要允许端口 443 上的传入流量。由于安全组是有状态的，您可以将任何更改应用于传入规则，并将自动应用于传出规则。

要启用到实例上运行的服务的连接，关联的网络 ACL 必须允许服务正在侦听的端口上的入站流量，以及允许来自临时端口的出站流量。当客户端连接到服务器时，临时端口范围（32768-65535）中的随机端口将成为客户端的源端口。因此，正确答案如下：

- 在安全组中，添加一个新规则，以允许在端口 443 上从源 0.0.0/0 进行 TCP 连接。
- 在网络 ACL 中，更新规则以允许端口 443 上的入站 TCP 连接从源 0.0.0/0 和端口 32768-65535 上的出站 TCP 连接到目标 0.0.0/0。

该选项表示：在安全组中，创建新规则以允许端口 443 上的 TCP 连接到目标 0.0.0.0/0 不正确，因为此步骤只允许从 EC2 实例到公共 Internet 的出站连接，这是不必要的。请记住，默认安全组已经包含允许所有出站流量的出站规则。

在网络 ACL 中，更新规则以允许端口 443 上的入站和出站 TCP 连接从源 0.0.0/0 到目标 0.0.0/0 的选项不正确，因为您的网络 ACL 必须具有出站规则以允许临时端口（32768-65535）。这些是将用作流量响应的客户端源端口的特定端口。

在网络 ACL 中，更新规则以允许端口 32768-65535 上的出站 TCP 连接到目标 0.0.0/0 的选项是不正确的，因为该步骤只是部分正确。您仍然需要添加来自端口 443 的入站规则，而不仅仅是临时端口（32768-65535）的出站规则。

Q34. 一家公司开发了一个 web 应用程序，并将其部署在使用 Amazon SQS 的 EC2 实例组上。请求保存为 SQS 队列中的消息，该队列配置了最大消息保留期。然而，在运行 13 天后，web 应用程序突然崩溃，队列中仍有 10000 条未处理的消息等待。由于他们开发了应用程序，他们可以很容易地解决问题，但他们需要向用户发送有关问题的通信。他们应该提供什么信息，未处理的消息会发生什么？

- A、告诉用户，不幸的是，他们必须重新提交所有请求，因为队列将无法一起处理 10000 条消息。
- B、告诉用户应用程序将很快投入运行，但是，三天前发送的请求需要重新提交。
- C、告诉用户，不幸的是，他们必须再次提交所有请求。
- D、告诉用户，应用程序将很快运行，所有收到的请求将在重新启动 Web 应用程序后处理。

答案 D

分析：

在 Amazon SQS 中，您可以将消息保留期配置为 1 分钟到 14 天的值。

默认值为 4 天。一旦达到邮件保留限制，您的邮件将自动删除。

单个 Amazon SQS 消息队列可以包含无限数量的消息。然而，对于标准队列，机上消息的数量限制为 120000 条，对于 FIFO 队列，限制为 20000 条。

消息是在消费组件从队列中接收到但尚未从队列中删除的消息后才飞行的。

在这种情况下，说明 SQS 队列配置了最大消息保留期。SQS 中的最大消息保留期为 14 天，这就是为什么这样的选项：告诉用户应用程序将很快运行，并且在 web 应用程序重新启动后处理所有收到的请求是正确答案，即不会丢失消息。

以下选项表示：告诉用户，不幸的是，他们必须再次提交所有请求，并告诉用户应用程序将很快运行。但是，三天前发送的请求需要重新提交，因为队列中没有丢失的消息，因此不需要重新提交任何以前的请求。

该选项表示：告诉用户，不幸的是，他们必须重新提交所有请求，因为队列将无法一起处理 10000 条消息，这是不正确的，因为队列可以包含无限数量的消息，而不仅仅是 10000 条消息。

Q35.公司有一个按需应变的 EC2 实例，该实例带有附加的 EBS 卷。有一个计划作业，在不使用实例的情况下，每午夜 12 点创建此 EBS 卷的快照。一天晚上，发生了一个生产事件，您需要在当前快照发生的同时对实例和 EBS 卷执行更改。在快照过程中使用 EBS 卷时，以下哪种情况是正确的？

- A、在快照完成之前，无法将 EBS 卷分离或连接到 EC2 实例
- B、快照正在进行时，EBS 卷可以在只读模式下使用。
- C、在快照完成之前，无法使用 EBS 卷。
- D、可以在快照进行时使用 EBS 卷。

答案 D


分析：

快照异步发生；立即创建时间点快照，但快照的状态是挂起的，直到快照完成（当所有修改的块都已转移到 Amazon S3 时），对于大型初始快照或许多块已更改的后续快照，这可能需要几个小时。

Create Snapshot

Select resource type ☐ Volume
☒ Instance

Instance ID*  

Description 

Exclude root volume ☐

  1 to 4 of 4  

Volume ID	Volume Type	Encryption
vol-11111111	Root	Encrypted
vol-22222222	EBS	Not Encrypted
vol-33333333	EBS	Not Encrypted
vol-44444444	EBS	Not Encrypted

Copy tags from volume 

Key	(127 characters maximum)	Value	(255 characters maximum)
-----	--------------------------	-------	--------------------------

This resource currently has no tags

Choose the Add tag button or click to add a Name tag

Add Tag 50 remaining (Up to 50 tags maximum)

* Required

Cancel **Create Snapshot**

在完成时，正在进行的快照不受正在进行的卷读写操作的影响。因此，您仍然可以正常使用 EBS 卷。当您基于快照创建 EBS 卷时，新卷以用于创建快照的原始卷的精确副本开始。复制卷在后台缓慢加载数据，以便您可以立即开始使用。如果您访问尚未加载的数据，卷将立即从 Amazon S3 下载请求的数据，然后继续在后台加载卷的其余数据。

Q36.贵公司有一项新的合规规则，每月审核每个 Windows 和 Linux EC2 实例，以查看任何性能问题。它们有 100 多个 EC2 实例在生产环境中运行，每个实例都必须有一个日志功能来收集有关该实例的各种系统详细信息。SysOps 团队将定期审查这些日志，并使用 AWS 分析工具分析其内容，结果需要保存在 S3 存储桶中。在这种情况下，以最小的工作量从实例收集和分析日志的最有效方法是什么？

- A、在每个实例中安装 AWS Inspector 代理，该代理将定期收集数据并将数据推送到 CloudWatch 日志。设置 CloudWatch 仪表板以正确分析所有实例的日志数据。
- B、在每个实例中安装 AWS SDK，并创建一个自定义守护程序脚本，用于收集数据并将数据推送到 CloudWatch 定期进行日志记录。启用 CloudWatch 详细监控，并使用 CloudWatch Logs Insights 分析所有实例的日志数据。
- C、在每个实例中安装 AWS Systems Manager 代理（SSM 代理），它将自动收集数据并将数据推送到 CloudWatch 日志。使用 CloudWatch Logs Insights 分析日志数据。
- D、在每个实例中安装统一的 CloudWatch 日志代理，它将自动收集数据并将数据推送到 CloudWatch 的日志。使用 CloudWatch Logs Insights 分析日志数据。

答案 D

分析：

为了将 Amazon EC2 实例和本地服务器的日志收集到 CloudWatch 日志中，AWS 提供了新的统一 CloudWatch 代理和旧的 CloudWatch logs 代理。建议使用具有以下优点的统一 CloudWatch 代理：

- 只需安装和配置一个代理即可收集日志和高级指标。
- 统一代理允许从运行 Windows Server 的服务器收集日志。
- 如果您使用代理来收集 CloudWatch 指标，则统一代理还可以收集额外的系统指标，以提高客户的可视性。
- 统一代理提供了更好的性能。



CloudWatch Logs Insights 使您能够在 Amazon CloudWatch 日志中交互式搜索和分析日志数据。您可以执行查询以帮助您快速有效地响应操作问题。如果出现问题，您可以使用 CloudWatch 日志洞察来识别潜在原因并验证已部署的修复。

CloudWatch Logs Insights 包括一种专门构建的查询语言，其中包含一些简单但功能强大的命令。CloudWatch Logs Insights 提供示例查询、命令描述、查询自动完成和日志字段发现，帮助您快速入门。示例查询包括几种类型的 AWS 服务日志。

该选项表示：在每个实例中安装 AWS SDK，并创建一个自定义守护程序脚本，定期收集数据并将数据推送到 CloudWatch 日志。启用 CloudWatch 详细监控，并使用 CloudWatch Logs Insights 分析所有实例的日志数据不正确。虽然这是一个有效的解决方案，但这需要大量的工作来实现，因为您必须分配时间将 AWS SDK 安装到每个实例，并开发自定义监控解决方案。请记住，问题是专门寻找一种可以用最少的努力实现解决方案。此外，在 CloudWatch 中启用详细监控以满足此场景的要求是不必要的，也是不经济的，因为这可以使用 CloudWatch 日志完成。

选项显示：在每个实例中安装 AWS 系统管理器代理（SSM 代理），它将自动收集数据并将数据推送到 CloudWatch 日志。使用 CloudWatch Logs Insights 分析日志数据不正确。尽管这也是一个有效的解决方案，但使用 CloudWatch 代理比使用 SSM 代理更有效。手动连接到实例以查看日志文件并解决 SSM 代理的问题

非常耗时。因此，为了更有效地监控实例，您可以使用 CloudWatch 代理将日志数据发送到 Amazon CloudWatch 日志。

选项显示：在每个实例中安装 AWS Inspector 代理，该代理将收集数据并将数据推送到 CloudWatch 定期记录。设置 CloudWatch 仪表板以正确分析所有实例的日志数据是不正确的，因为 AWS Inspector 只是一个安全评估服务，它只帮助您检查 EC2 实例的意外网络可访问性以及这些 EC2 实例上的漏洞。此外，设置 Amazon CloudWatch 仪表板并不合适，因为它主要用于您必须在单个视图中监控资源的场景，甚至是分布在不同 AWS 区域的资源。最好使用 CloudWatch Logs Insights，因为它使您能够交互式地搜索和分析日志数据。

Q37.在线加密货币交换平台托管在 AWS 中，在 MultiAZ 部署配置中使用 ECS 集群和 RDS。应用程序大量使用 RDS 实例来处理复杂的读写数据库操作。为了保持系统的可靠性、可用性和性能，您必须密切监视数据库实例上的不同进程或线程如何使用 CPU，包括每个进程占用的 CPU 带宽和总内存的百分比。以下哪项是正确监控数据库的最合适解决方案？

- A、 创建一个脚本，用于收集自定义指标并将其发布到 CloudWatch，该脚本跟踪 RDS 实例的实时 CPU 利用率，然后设置自定义 CloudWatch 仪表板以查看指标。
- B、 检查 Amazon RDS 控制台中随时可用的 CPU%和 MEM%指标，显示 RDS 实例的每个数据库进程消耗的 CPU 带宽和总内存的百分比。C、 在 RDS 中启用增强的监控。
- D、 使用 Amazon CloudWatch 监控数据库的 CPU 利用率。

答案 C

分析：

Amazon RDS 为运行数据库实例的操作系统（OS）提供实时指标。

您可以使用控制台查看数据库实例的度量，或者在您选择的监控系统中使用 CloudWatch 日志中的增强监控 JSON 输出。默认情况下，增强的监控指标存储在 CloudWatch 日志中 30 天。要修改指标存储在 CloudWatch 日志中的时间量，请更改 CloudWatch 控制台中 RDSOSMetrics 日志组的保留时间。

请注意，CloudWatch 和增强的监控指标之间存在某些差异。CloudWatch 从数据库实例的虚拟机监控程序收集有关 CPU 利用率的指标，增强的监控从实例上的代理收集其指标。因此，您可能会发现测量结果之间的差异，因为管理程序层只执行少量工作。因此，在 RDS 中启用增强的监控是这个特定场景中的正确答案。

如果您的 DB 实例使用较小的实例类，差异可能会更大，因为在单个物理实例上可能有更多虚拟机（VM）由管理程序层管理。当您希望查看数据库实例上的不同进程或线程如何使用 CPU 时，增强的监视度量非常有用。

Process List					
<input type="text" value="Filter process list"/>					
<div> <div>< 1 2 ></div> <div>⚙</div> </div>					
NAME ▾	VIRT ▾	RES ▾	CPU%	MEM% ▾	VMLIMIT ▾
▼ postgres [3181]!	283.55 MB	17.11 MB	0.02	1.72	
postgres: rdsadmin rdsadmin localhost(40156) idle [2953]!	384.7 MB	9.51 MB	0.02	0.95	

使用 Amazon CloudWatch 监控数据库的 CPU 利用率是不正确的。虽然您可以使用它来监控数据库实例的 CPU 利用率，但它不提供 RDS 实例中每个数据库进程所消耗的 CPU 带宽和总内存的百分比。请注意，CloudWatch 从数据库实例的管理程序收集有关 CPU 利用率的指标，而 RDS 增强监控则从实例上的代理收集其指标。

“创建一个脚本，收集并发布自定义指标到 CloudWatch，跟踪 RDS 实例的实时 CPU 利用率，然后设置自定义 CloudWatch 仪表板以查看指标”选项不正确。尽管您可以使用 Amazon CloudWatch 日志和 CloudWatch 仪表板来监控数据库实例的 CPU 利用率，但仅使用 CloudWatch 仍然不足以获得每个数据库进程所消耗的 CPU 带宽和总内存的特定百分比。与 RDS 中的增强监控功能相比，CloudWatch 提供的数据不够详细。还请注意，您无法直接访问 RDS 数据库实例的实例/服务器，这与 EC2 实例不同，在 EC2 实例中，您可以安装 CloudWatch 代理或自定义脚本以获取实例的 CPU 和内存利用率。

“检查 Amazon RDS 控制台中可用的 CPU%和 MEM%指标（显示 RDS 实例的每个数据库进程消耗的 CPU 带宽和总内存的百分比）的选项是不正确的，因为亚马逊 RDS 控制台中不可用 CPU%和 MEM%指标，这与此选项中所述相反。

Q38.一家公司在 EC2 实例上托管一个应用程序，该应用程序定期推送和获取 Amazon S3 中的数据。由于法规遵从性的变化，这些实例需要移动到专用子网上。随着这一变化，该公司希望通过配置其 AWS 资源来降低数据传输成本。如何以最具成本效益的方式实现这一点？

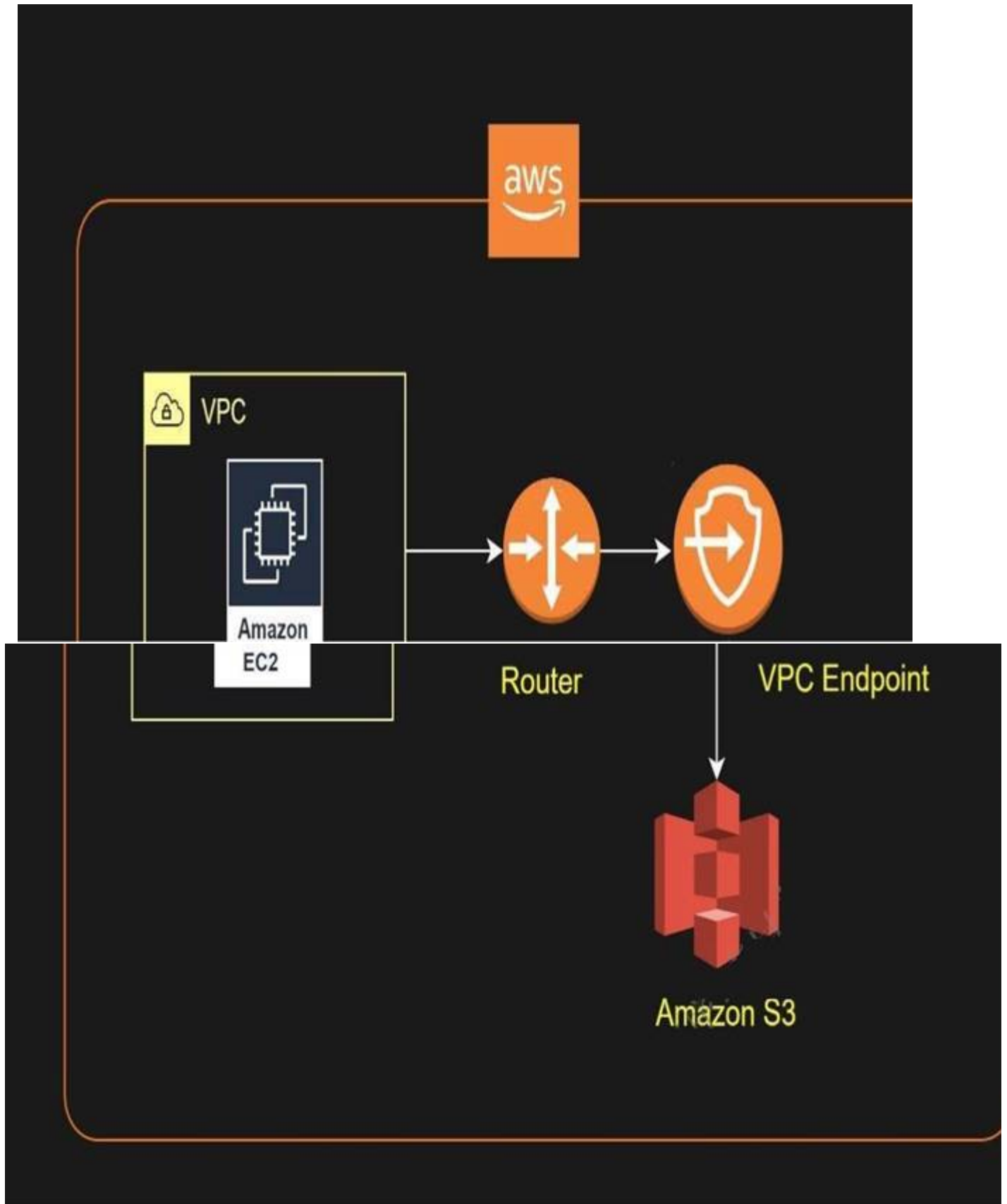
- A、 创建一个 AmazonS3 网关端点，以启用实例和 AmazonS 之间的连接。
- B、 设置 AWS 过境网关以访问 Amazon S3。
- C、 在公共子网中设置 NAT 网关以连接到 Amazon S3。
- D、 创建一个 AmazonS3 接口端点，以启用实例和 AmazonS 之间的连接。

答:

分析:

Amazon S3 的 VPC 端点通过提供到 S3 的可配置且高度可靠的安全连接，简化了从 VPC 内对 S3 的访问，无需互联网网关或网络地址转换（NAT）设备。当您创建 S3 VPC 端点时，您可以将端点策略附加到它，以控

制对 Amazon S3 的访问。您可以使用两种类型的 VPC 端点来访问 Amazon S3：网关端点和接口端点。网关端点是您在路由表中指定的网关，用于通过 AWS 网络从 VPC 访问 Amazon S3。接口端点扩展了网关端点的功能，使用私有 IP 地址将请求从 VPC 内部、本地或不同 AWS 区域路由到 Amazon S3。接口端点与网关端点兼容。如果 VPC 中有现有网关端点，则可以在同一 VPC 中使用这两种类型的端点。



使用网关端点不收取额外费用。然而，数据传输和资源使用的标准费用仍然适用。

因此，正确的答案是：创建一个 AmazonS3 网关端点，以实现实例和 AmazonS 之间的连接。

在公共子网中设置 NAT 网关以连接到 Amazon S3 的选项不正确。这将实现私有 EC2 实例和 Amazon S3 之间的连接，但这不是最具成本效益的解决方案。NAT 网关按小时计费，即使是空闲时间。

“创建 AmazonS3 接口端点以启用实例和 AmazonS 之间的连接”选项不正确。这也是一个可能的解决方案，但不是最具成本效益的解决方案。您为每个配置的接口端点支付小时费率。

设置 AWS 传输网关以访问 Amazon S3 的选项是不正确的，因为该服务主要用于通过中央集线器连接 VPC 和内部网络。

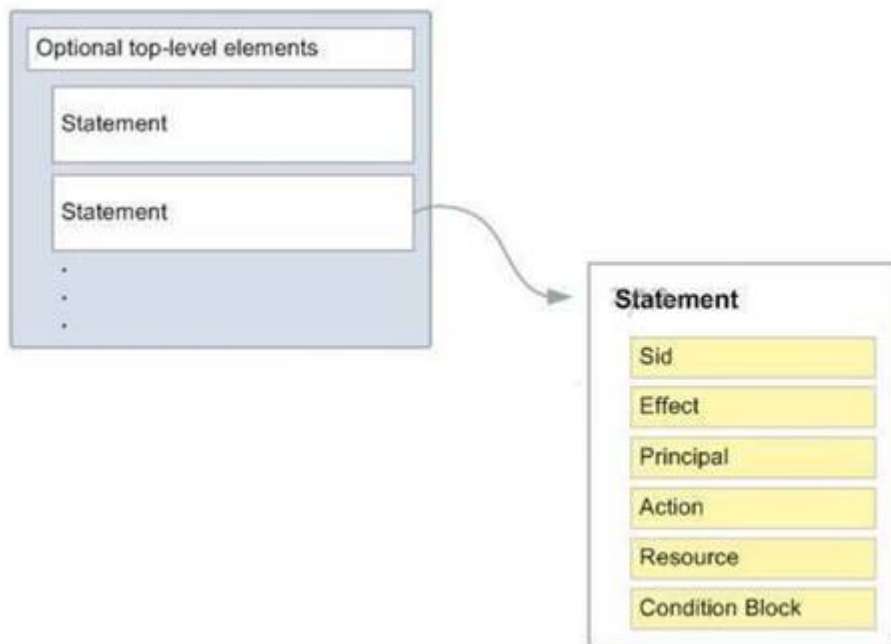
Q39.一家公司正在使用 AWS IAM 管理对 AWS 服务的访问。公司的解决方案架构师为 AWS Lambda 创建了以下 IAM 策略： {“版本”： “2012-10-17”， “声明”： [{“效果”： “允许”， “操作”： [“lambda:CreateFunction”， “lambda:DeleteFunction”], “资源”： “*”}, {“效果”： “拒绝”， “行动”： [“lambda:CreateFunction”， “lambda: DeleteFunction”， “lambda:InvokeFunction”“lambda:TagResource”], “Resource”： “*”， “条件”： {“IpAddress”： {aws:SourceIp:“187.5.104.11/32”} } }] } 此策略允许以下哪些选项？

- A、 使用 187.5.104.11/32 地址创建 AWS Lambda 函数。
- B、 使用 100.220.0.11/32 地址创建 AWS Lambda 函数。
- C、 使用 187.5.104.11/32 地址删除 AWS Lambda 函数。
- D、 从任何网络地址删除 AWS Lambda 函数。

答案 B

分析：

您可以通过创建策略并将其附加到 IAM 标识（用户、用户组或角色）或 AWS 资源来管理 AWS 中的访问。策略是 AWS 中的一个对象，当与标识或资源关联时，定义其权限。AWS 在 IAM 主体（用户或角色）发出请求时评估这些策略。策略中的权限决定是否允许或拒绝请求。大多数策略以 JSON 文档的形式存储在 AWS 中。



您可以使用 AWS 身份和访问管理（IAM）来管理对 Lambda API 和资源（如函数和层）的访问。根据给定的 IAM 策略，您可以从除 IP 地址 187.5.104.11/32 之外的任何网络地址创建和删除 Lambda 函数。由于策略中未拒绝 IP 地址 100.220.0.11/31，您可以使用此地址创建 Lambda 功能。

因此，正确答案是：使用 100.220.0.11/32 地址创建 AWS Lambda 函数。

“使用 187.5.104.11/32 地址删除 AWS Lambda 函数”选项不正确，因为该选项中使用的源 IP 被 IAM 策略拒绝。

表示：从任何网络地址删除 AWS Lambda 函数的选项不正确。无法从任何网络地址中删除 Lambda 函数，因为地址 187.5.104.11/32 被策略拒绝。

表示：使用 187.5.104.11/32 地址创建 AWS Lambda 函数的选项不正确。与上述选项一样，IAM 策略拒绝了 IP 地址 187.5.104.11/32。

Q40.一家科技公司拥有一个 CRM 应用程序，该应用程序托管在按需 EC2 实例的自动扩展组上。该应用程序在办公时间从早上 9 点到下午 5 点广泛使用。他们的用户抱怨说，应用程序在一天开始的时候性能很慢，但几个小时后就可以正常工作了。以下哪项可以确保应用程序在一天开始时正常工作？

- A、为自动缩放组配置计划缩放策略，以便在一天开始之前启动新实例。
- B、为您的体系结构设置应用程序负载平衡器（ALB），以确保流量在实例上正确分布。
- C、为自动缩放组配置动态缩放策略，以基于内存利用率启动新实例。
- D、为自动缩放组配置动态缩放策略，以基于 CPU 利用率启动新实例。

答：

分析：

基于计划的扩展允许您扩展应用程序以响应可预测的负载变化。例如，每周 web 应用程序的流量在星期三开始增加，星期四保持较高，星期五开始减少。您可以根据 web 应用程序的可预测流量模式规划扩展活动。



Auto Scaling group



Desired Capacity



Scale out as needed



Maximum size

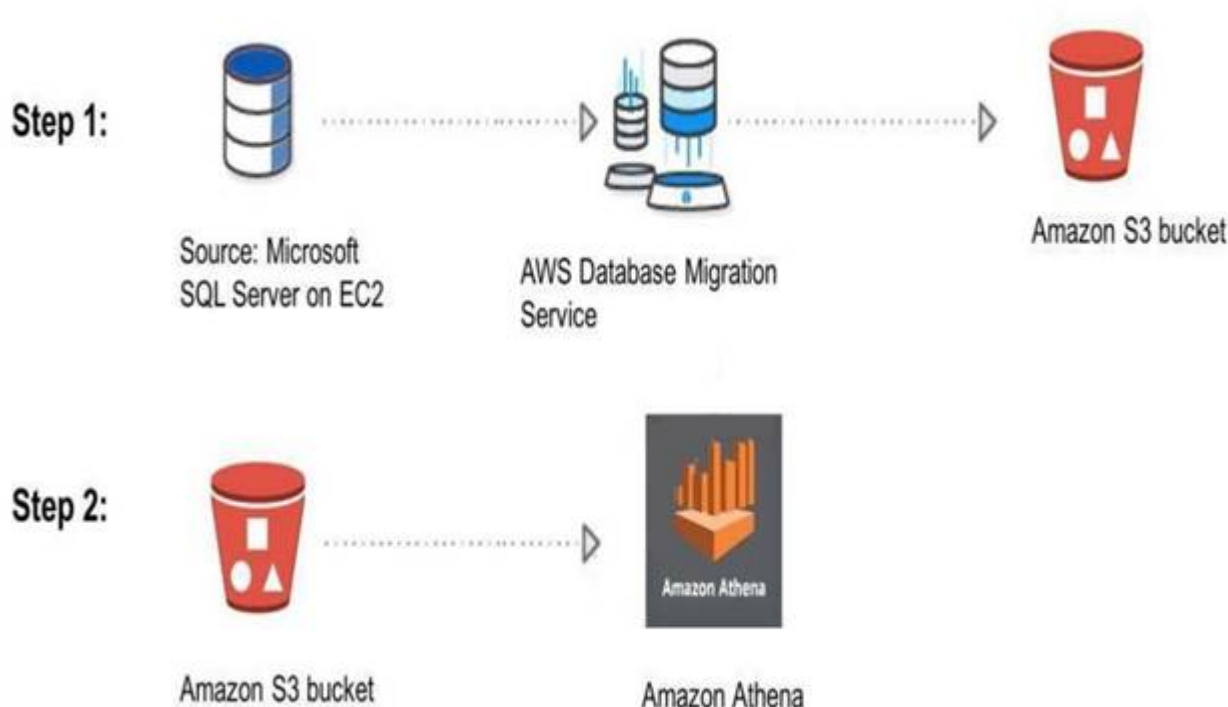
Q41. 一家公司决定将其第三方数据分析工具改为更便宜的解决方案。他们在 CSV 文件中发送了完整的数据导出，该文件包含所有分析信息。然后将 CSV 文件保存到 S3 存储桶中进行存储。您的经理要求您对提供的数据导出进行一些验证。在这种情况下，使用标准 SQL 分析导出数据最经济、最简单的方法是什么？

- A、 使用 `mysqldump` 客户端实用程序将 CSV 导出文件从 S3 加载到 MySQL RDS 实例。加载数据后，运行一些 SQL 查询以完成验证。
- B、 为了能够运行 SQL 查询，使用 AWS Athena 分析 S3 中的导出数据文件。
- C、 创建迁移工具，将 CSV 导出文件从 S3 加载到 DynamoDB 实例。加载数据后，使用 DynamoDB 运行查询。
- D、 使用迁移工具将 CSV 导出文件从 S3 加载到为在线分析处理（OLAP）设计的数据库，如 AWS RedShift。加载数据后运行一些查询以完成验证。

答案 B

分析：

Amazon Athena 是一个交互式查询服务，它可以使用标准 SQL 直接在 Amazon 简单存储服务（Amazon S3）中分析数据。通过 AWS 管理控制台中的一些操作，您可以将 Athena 指向存储在 Amazon S3 中的数据，并开始使用标准 SQL 运行特殊查询，并在几秒钟内获得结果。



Athena 是无服务器的，因此没有需要设置或管理的基础设施，您只需为运行的查询付费。Athena 自动扩展并行执行的查询，因此即使使用大型数据集和复杂查询，结果也很快。Athena 帮助您分析存储在 Amazon S3 中的非结构化、半结构化和结构化数据。

示例包括 CSV、JSON 或列数据格式，如 Apache Parquet 和 Apache ORC。您可以使用 Athena 使用 ANSI SQL 运行特殊查询，而无需将数据聚合或加载到 Athena 中。

因此，正确的答案是：为了能够运行 SQL 查询，使用 Amazon Athena 分析 S3 中的导出数据文件。

其余选项都不正确，因为不需要设置数据库来分析 CSV 导出文件。您可以使用经济高效的选项（AWS Athena），这是一种无服务器服务，使您只需为运行的查询付费。

Q42. 一家公司生成具有数百万行的大型金融数据集。解决方案架构师需要以列方式存储所有数据，以减少磁盘 I/O 请求的数量，并减少从磁盘加载所需的数据量。该银行现有一个第三方商业智能应用程序，该应用程序将连接到存储服务，然后为全球客户生成每日和每月财务报告。在这种情况下，哪种存储服务是满足需求的最佳存储服务？

- A、 亚马逊极光
- B、 亚马逊 RDS
- C、 亚马逊发电机 B
- D、 亚马逊红移

答案 D

分析：

Amazon Redshift 是一个快速、可扩展的数据仓库，它使分析数据仓库和数据湖中的所有数据变得简单且经济高效。Redshift 通过使用机器学习和大规模并行查询，提供了比其他数据仓库快十倍的性能

以及高性能磁盘上的列存储。在这种情况下，需要一个存储服务，该服务将由商业智能应用程序使用，并且数据必须以列方式存储。商业智能报告系统是一种在线分析处理（OLAP），已知 Redshift 支持该系统。此外，与其他选项不同，Redshift 还提供列存储。因此，这个场景中的正确答案是亚马逊红移。

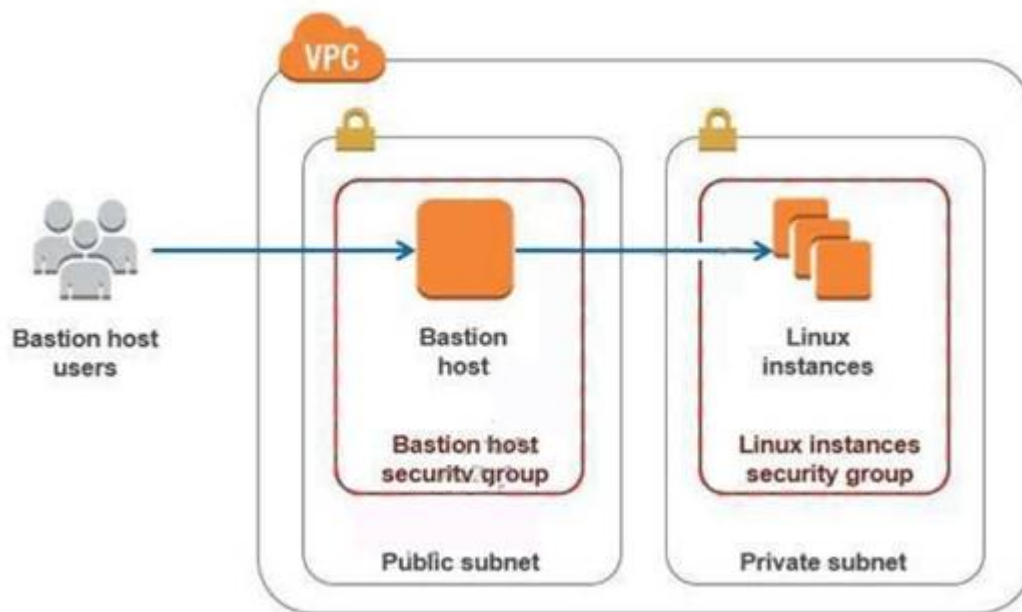
Q43. 一家公司正在虚拟私有云（VPC）中运行多层 web 应用程序场，该虚拟私有云未连接到其公司网络。他们通过互联网连接到专有网络，以管理在公共和私有子网中运行的 Amazon EC2 实例。解决方案架构师为应用程序实例安全组添加了一个具有 Microsoft 远程桌面协议（RDP）访问权限的堡垒主机，但公司希望进一步限制对专有网络中所有实例的管理访问。以下哪个 bastion 主机部署选项将满足此要求？

- A、 在公共子网中部署具有弹性 IP 地址的 Windows Bastion 主机，并允许 SSH 从任何位置访问 Bastion。
- B、 在企业网络上部署一台 Windows Bastion 主机，该主机具有对 VPC 中所有 EC2 实例的 RDP 访问权限。
- C、 在公共子网中部署具有弹性 IP 地址的 Windows Bastion 主机，并仅允许 RDP 从公司 IP 地址访问 Bastion。
- D、 在专用子网中部署具有弹性 IP 地址的 Windows 堡垒主机，并限制 RDP 仅从公司公共 IP 地址访问堡垒。

答案 C

分析：

正确的答案是在公共子网中部署具有弹性 IP 地址的 Windows Bastion 主机，并允许 RDP 仅从公司 IP 地址访问 Bastion。堡垒主机是网络上的专用计算机，专门设计并配置为抵御攻击。如果您在 AWS 中有一个堡垒主机，它基本上只是一个 EC2 实例。它应该位于公共子网中，具有公共或弹性 IP 地址，在安全组中定义了足够的 RDP 或 SSH 访问权限。用户通过 SSH 或 RDP 登录到 bastion 主机，然后使用该会话管理专用子网中的其他主机。



在企业网络上部署 Windows Bastion 主机，该主机具有对 VPC 中所有 EC2 实例的 RDP 访问权限，这是不正确的，因为您没有将 Bastion 主机部署到企业网络。它应该位于 VPC 的公共子网中。在专用子网中部署具有弹性 IP 地址的 Windows 堡垒主机，并限制 RDP 仅从公司公共 IP 地址访问堡垒是不正确的，因为它应该部署在公共子网中，而不是专用子网。在公共子网中部署具有弹性 IP 地址的 Windows Bastion 主机并允许 SSH 从任何地方访问 Bastion 是不正确的。由于它是 Windows 堡垒，您应该允许 RDP 访问，而不是 SSH，因为这主要用于基于 Linux 的系统。

Q44.公司有一个无服务器应用程序，由 AWS Amplify、Amazon API 网关和 Lambda 函数组成。应用程序连接到私有子网内的 Amazon RDS MySQL 数据库实例。Lambda 函数 URL 也被实现为函数的专用 HTTPS 端点，其值如下：<https://12june1898pil1pinas.lambda-url.us-west-2.on.aws/There> 在峰值负载期间，数据库抛出“太多连接”错误，阻止用户访问应用程序。公司可以采取哪种解决方案来解决这个问题？

- A、增加 Lambda 函数的内存分配
- B、在 Lambda 函数和 RDS 数据库实例之间提供 RDS 代理
- C、增加 API 网关的速率限制
- D、增加 Lambda 函数的并发限制

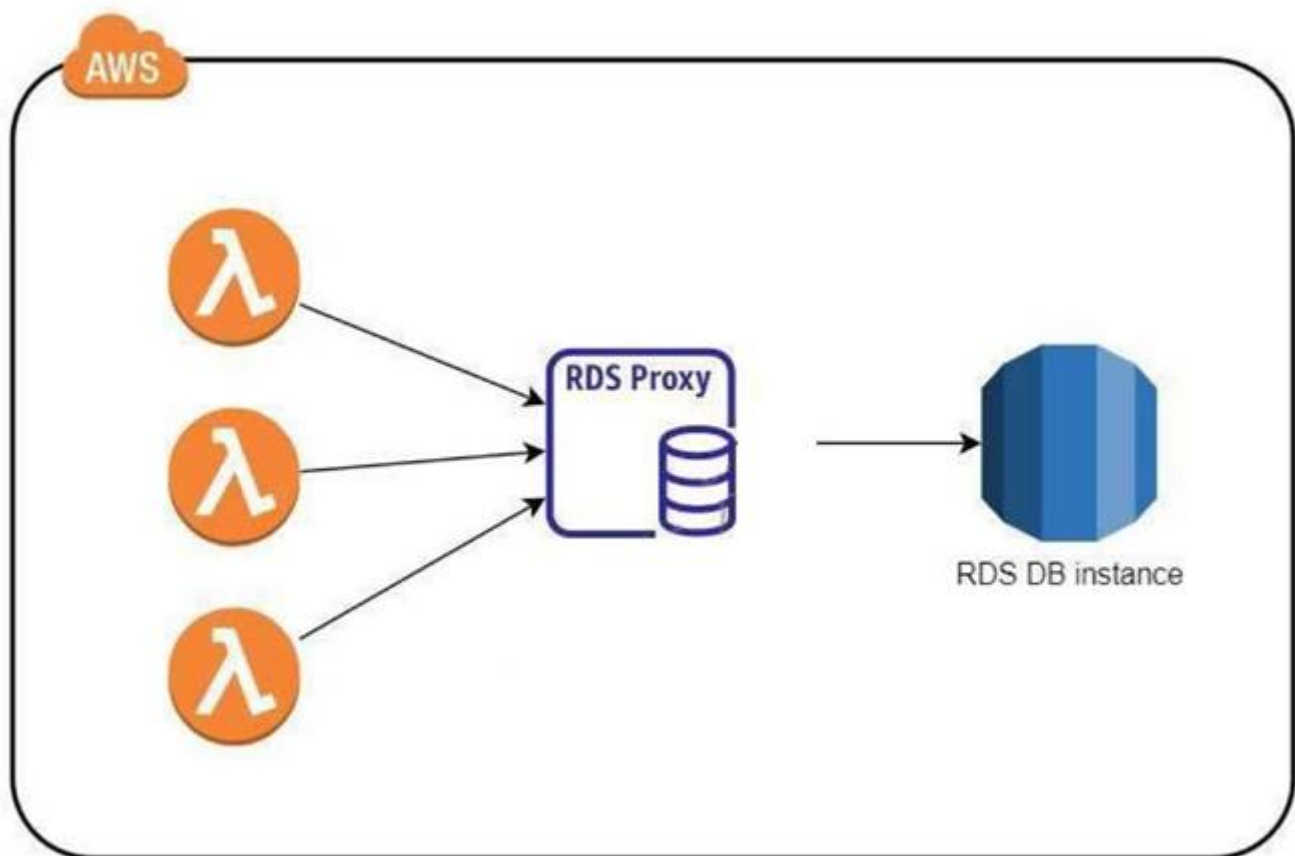
答案 B

分析：

如果连接到 MySQL 数据库的客户端发生“连接过多”错误，则表示所有可用连接都被其他客户端使用。打开连接会消耗数据库服务器上的资源。由于 Lambda 函数可以扩展到数万个并发连接，因此数据库需要更多的资源来打开和维护连接，而不是执行查询。

数据库可以支持的最大连接数在很大程度上取决于分配给它的内存量。升级到具有更高内存的数据库实例是解决此问题的一种简单方法。另一种方法是维护客户端可以重用的连接池。

这就是 RDS 代理的作用所在。



RDS 代理通过建立到数据库的热连接池，帮助您管理从 Lambda 到 RDS 数据库的大量连接。Lambda 函数与 RDS 代理交互，而不是与数据库实例交互。它处理扩展由并发 Lambda 函数创建的许多同时连接所需的连接池。这允许您的 Lambda 应用程序重用现有连接，而不是为每个函数调用创建新连接。

因此，正确答案是：在 Lambda 函数和 RDS 数据库实例格式之间提供 RDS 代理。表示：增加 Lambda 功能的并发限制的选项不正确。并发限制是指 AWS Lambda 可以同时处理的最大请求数。增加限制将允许更多请求打开数据库连接，这可能会使问题恶化。

“增加 API 网关的速率限制”选项不正确。这根本无法解决问题，因为它所做的只是增加客户端可以发出的 API 请求的数量。

表示：增加 Lambda 函数的内存分配的选项不正确。增加 Lambda 函数的内存只会使其运行进程更快。这可能会有帮助，但不太可能对消除错误产生任何重大影响。“连接太多”错误是与数据库相关的问题。

与数据库有关的解决方案，如升级到更大的数据库实例，或在本例中使用 RDS 代理创建数据库连接池，有更好的机会解决问题。

Q45.一家公司正在构建一个内部应用程序，为客户处理贷款、应计项目和利率。它们需要一种存储服务，该服务能够处理未来高达 16 TB 的存储容量的增加，并能够提供对其数据的最低延迟访问。web 应用程序将托管在单个 m5ad 中。24xlarge 保留 EC2 实例，它将处理数据并将数据存储到存储服务。您推荐以下哪种存储服务？

- A、EFS
- B、S3
- C、EBS
- D、存储网关

答案 C

分析:

Amazon Web 服务（AWS）提供云存储服务，以支持广泛的存储工作负载，如 Amazon S3、EFS 和 EBS。Amazon EFS 是一种与 Amazon EC2 一起使用的文件存储服务。Amazon EFS 提供了一个文件系统接口、文件系统访问语义（如强一致性和文件锁定）以及多达数千个 Amazon EC1 实例的并发访问存储。Amazon S3 是一个对象存储服务。Amazon S3 通过互联网 API 提供数据，可以在任何地方访问。Amazon EBS 是与 Amazon EC2 一起使用的块级存储服务。Amazon EBS 可以为需要从单个 EC2 实例访问数据的最低延迟的工作负载提供性能。您还可以将 EBS 存储容量增加到 16TB，或添加新卷以增加存储容量。

在这种情况下，该公司正在寻找一种存储服务，它可以提供对其数据的最低延迟访问，这些数据将由单个 m5ad 获取。24xlarge 保留 EC2 实例。使用 EFS 或 EBS 可以更好地支持这类工作负载，但在这种情况下，后者是最合适的存储服务。如上所述，EBS 为 EC2 实例提供了对数据的最低延迟访问，因为卷直接连接到实例。此外，该场景不需要可并发访问的存储，因为它们只有一个实例。因此，正确答案是 EBS。

Storage Need	Solution	AWS Services
Temporary storage	Consider using local instance store volumes for needs such as scratch disks, buffers, queues, and caches.	Amazon Local Instance Store
Multi-instance storage	Amazon EBS volumes can only be attached to one EC2 instance at a time. If you need multiple EC2 instances accessing volume data at the same time, consider using Amazon EFS as a file system.	Amazon EFS
Highly durable storage	If you need very highly durable storage, use S3 or Amazon EFS. Amazon S3 Standard storage is designed for 99.999999999 percent (11 nines) annual durability per object. You can even decide to take a snapshot of the EBS	Amazon S3 Amazon EFS

volumes. Such a snapshot then gets saved in Amazon S3, thus providing you the durability of Amazon S3. For information on EBS durability, see the [Durability Availability](#) section. EFS is designed for high durability and high availability, with data stored in multiple Availability Zones within an AWS Region.

Static data or web content

If your data doesn't change that often, Amazon S3 represents a more cost-effective and scalable solution for storing this fixed information. Also, web content stored on Amazon EBS requires a web server running on an EC2 instance; in contrast, you can deliver web content directly from Amazon S3 or from multiple EC2 instances using Amazon EFS.

存储网关不正确，因为它主要用于将本地存储扩展到 AWS 云。

S3 是不正确的，因为尽管它也具有高可用性和高可伸缩性，但与 EBS 不同，它仍然不提供对数据的最低级别访问。请记住，默认情况下，S3 不在 VPC 中，这意味着数据将通过公共互联网，这可能导致更高的延迟。您可以为 S3 设置 VPC 端点，但它的延迟仍然大于 EBS。EFS 是不正确的，因为该场景不需要可并发访问的存储，因为内部应用程序只托管在一个实例中。尽管与 S3 相比，EFS 可以提供对 EC2 实例的低延迟数据访问，但可以提供最低延迟访问的存储服务仍然是 EBS。

Q46. 解决方案架构师正在为应用程序设计高可用性环境。她计划在自动缩放组中的 EC2 实例上托管应用程序。其中一个条件要求在实例终止时保留存储在根 EBS 卷上的数据。应采取哪些措施来满足要求？

- A、 使用 AWS 数据同步将根卷数据复制到 Amazon S3。
- B、 配置 ASG 以挂起每个 EC2 实例的运行状况检查过程。
- C、 将 EBS 卷的 DeleteOnTermination 属性的值设置为 False。
- D、 为所有 EC2 实例启用终止保护选项。

答案 C

分析：

默认情况下，当实例终止时，将自动删除 Amazon EBS 根设备卷。但是，默认情况下，您在启动时附加的任何其他 EBS 卷，或您附加到现有实例的任何 EBS 卷即使在实例终止后也会持续存在。此行为由卷的

DeleteOnTermination 属性控制，您可以修改该属性。若要在实例终止时保留根卷，请将根卷的 DeleteOnTermination 属性更改为 False。

可以在启动实例时通过 AWS 控制台或通过 CLI/API 命令更改此 EBS 属性。

因此，正确答案是这样的选项：将 EBS 卷的 DeleteOnTermination 属性的值设置为 False。

表示：使用 AWS 数据同步将根卷数据复制到 Amazon S3 的选项不正确，因为 AWS 数据 sync 不适用于 Amazon EBS 卷。DataSync 可以在网络文件系统（NFS）共享、服务器消息块（SMB）共享、自管理对象存储、AWS Snowcone、Amazon 简单存储服务（Amazon S3）存储桶、Amazon 弹性文件系统（Amazon EFS）文件系统和 Amazon FSx for Windows 文件服务器文件系统之间复制数据。

“配置 ASG 以挂起每个 EC2 实例的健康检查进程”选项不正确，因为挂起健康检查进程将阻止 ASG 替换不健康的 EC2 实例。这可能会导致应用程序的可用性问题。

表示：为所有 EC2 实例启用终止保护选项的选项不正确。终止保护只会防止使用 Amazon EC2 控制台意外终止实例。

Q47 一家公司有一个静态公司网站，托管在标准 S3 bucket 中，并使用 Route 53 注册了一个新的 web 域名。您的经理指示您集成这两个服务，以便成功启动其公司网站。使用 Amazon Route 53 将流量路由到托管在 Amazon S3 Bucket 中的网站时，先决条件是什么？（选择两个。）

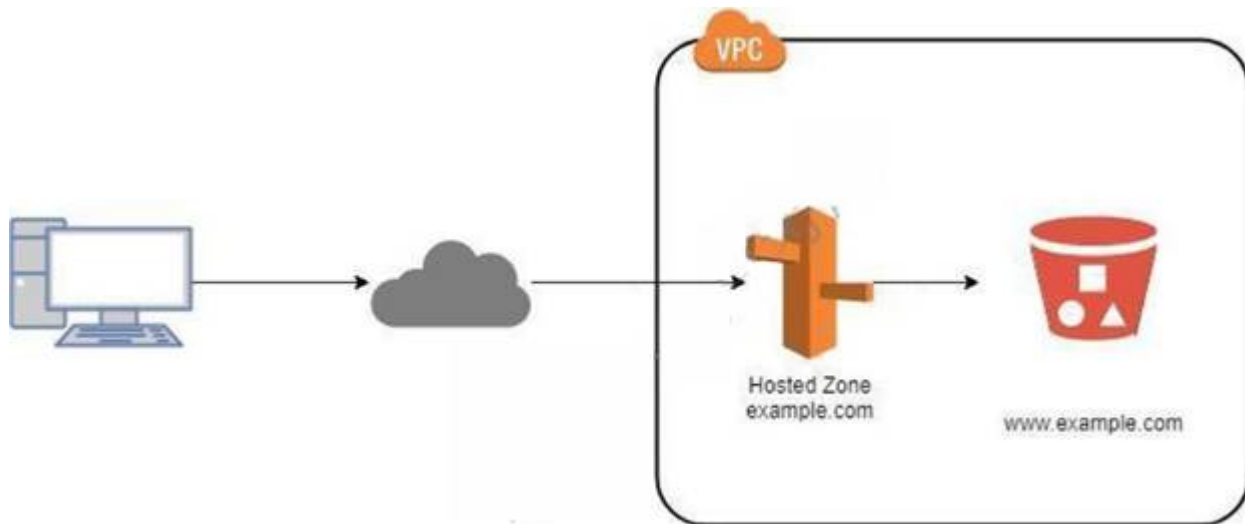
- A、记录集的类型必须为“MX”
- B、S3 存储桶名称必须与域名相同
- C、应在 S3 存储桶中启用跨源资源共享（CORS）选项
- D、注册域名
- E、S3 存储桶必须与托管区域位于同一区域中

答：屋宇署

分析：

以下是将流量路由到托管在 Amazon S3 Bucket 中的网站的先决条件：

- 被配置为托管静态网站的 S3 bucket。bucket 在域或子域中必须具有相同的名称。例如，如果要使用子域 portal.tutorialsdojo.com，bucket 的名称必须是 portal.tutorialsdojo.com。
- 注册域名。您可以使用路由 53 作为您的域注册商，也可以使用其他注册商。
- 路由 53 作为域的 DNS 服务。如果您使用路由 53 注册域名，我们会自动将路由 53 配置为该域的 DNS 服务。



表示：记录集必须为“MX”类型的选项不正确，因为 MX 记录指定了负责代表域名接受电子邮件的邮件服务器。这不是问题所要问的。表示：S3 存储桶必须与托管区域位于同一区域的选项不正确。S3 桶必须位于与托管区相同的区域中，以便路由 53 服务将业务路由到其中。

“应在 S3 存储桶中启用跨源资源共享（CORS）选项”的选项不正确，因为只有当一个域上的客户端 web 应用程序与另一个域中的资源交互时，才需要启用跨源资源共享。

Q48.解决方案架构师正在设计一个监控应用程序，该应用程序生成公司云基础设施所有运营活动的审计日志。他们的 IT 安全和合规团队要求应用程序保留日志 5 年，然后才能删除数据。建筑师如何满足上述要求？

- A、将审核日志存储在 Glacier vault 中，并使用 vault 锁定功能。
- B、将审核日志存储在 Amazon S3 bucket 中，并在 S3bucket 上启用多因素身份验证删除（MFA 删除）。
- C、将审核日志存储在 EBS 卷中，然后每月拍摄 EBS 快照。
- D、将审核日志存储在 EFS 卷中，并使用网络文件系统版本 4（NFSv4）文件锁定机制。

答：

分析：

亚马逊 S3 冰川（Glacier）保险库可以附加一个基于资源的保险库访问策略和一个保险库锁定策略。Vault 锁定策略是可以锁定的 Vault 访问策略。使用 Vault 锁定策略可以帮助您实施法规和法规遵从性要求。Amazon S3 Glacier 为您提供了一套 API 操作来管理保险库锁策略。

Vault Lock policy for BusinessCritical

The Vault Lock policy for the vault is shown below. [Click here to learn about writing a Vault Lock policy.](#)

Add a permission

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": {
        "AWS": "*"
      },
      "Action": "glacier:DeleteArchive",
      "Resource": "arn:aws:glacier:us-east-1::vaults/BusinessCritical",
      "Condition": {
        "NumericLessThanEquals": {
          "glacier:ArchiveAgeInDays": "365"
        }
      }
    }
  ]
}
```

Cancel

Initiate Vault

作为 Vault 锁定策略的示例，假设您需要保留存档一年，然后才能删除存档。要实现此要求，可以创建 Vault 锁定策略，该策略拒绝用户删除存档的权限，直到存档存在一年。您可以在锁定此策略之前测试它。锁定策略后，该策略将变得不可变。有关锁定过程的更多信息，请参阅 [Amazon S3 冰川库锁](#)。如果要管理可以更改的其他用户权限，可以使用 vault 访问策略 [Amazon S3 Glacier](#) 支持以下存档操作：上传、下载和删除。存档是不可变的，不能修改。因此，正确的答案是将审计日志存储在冰川保险库中，并使用保险库锁定功能。将审核日志存储在 EBS 卷中，然后每月拍摄 EBS 快照是不正确的，因为这不是一个合适且安全的解决方案。任何有权访问 EBS 卷的人都可以简单地删除和修改审核日志。快照也可以删除。将审计日志存储在 Amazon S3 bucket 中，并在 S3 bucket 上启用多因素身份验证删除（MFA 删除）是不正确的，因为这仍然不符合要求。如果有人可以访问 S3 存储桶，并且具有适当的 MFA 权限，则可以编辑审计日志。将审计日志存储在 EFS 卷中并使用网络文件系统版本 4（NFSv4）文件锁定机制是不正确的，因为如果将审计日志的数据完整性存储在具有网络文件系统第 4 版（NFSv4）文件锁机制的 EFS 卷，则审计日志的数据完整性仍然会受到损害，因此不适合作为文件的存储。尽管它将提供某种安全性，但文件锁仍然可以被覆盖，审核日志可能由其他人编辑。

Q49.一家公司对生产环境中使用的所有 AWS 资源进行了一次意外的 IT 审计。在审核活动期间，注意到您在应用程序中使用了标准和可转换保留 EC2 实例的组合。以下哪项是使用这两种类型的保留 EC2 实例的特点和好处？（选择两个。）

- A、可转换保留实例允许您交换另一个可转换保留的实例。
- B、它在专用于单个客户的硬件上的 VPC 中运行。
- C、未使用的标准保留实例可以稍后在保留实例市场出售。
- D、它可以让您在多个可用性区域和多个 AWS 区域中为 Amazon EC2 实例保留任何持续时间的容量。
- E、未使用的可转换保留实例可以稍后在保留实例市场出售。

答覆

分析：

与按需实例定价相比，保留实例（RIs）为您提供了显著的折扣（高达 75%）。

当您使用可转换 RIs 时，您可以灵活地更改族、操作系统类型和租约，同时受益于 RI 定价。这里需要记住的一点是，保留实例不是物理实例，而是应用于在您的帐户中使用按需实例的计费折扣。保留实例的提供类是标准的或可转换的。标准保留实例比可转换保留实例提供更大的折扣，但与可转换保留的实例不同，您不能交换标

准保留实例。您可以修改标准和可转换保留实例。请注意，在可转换保留实例中，您可以使用不同的实例类型和租约交换另一个可转换保留的实例。

保留实例的配置包括单个实例类型、平台、范围和期限租赁。如果您的计算需要更改，您可以修改或交换保留的实例。当您的计算需求发生变化时，您可以修改标准或可转换保留实例，并继续利用计费优势。您可以修改保留实例的可用性区域、范围、网络平台或实例大小（在相同实例类型内）。您还可以在保留实例市场上出售未使用的标准 RIs 实例，但不可转换 RIs 实例。

因此，正确的选项是：

- 未使用的标准保留实例可以稍后在保留实例市场出售。
- 可转换保留实例允许您交换其他实例族的另一个可转换保留的实例。

“未使用的可转换保留实例稍后可以在保留实例市场出售”选项不正确。这是不可能的。在保留实例市场上只能销售标准 RIs。

该选项表示：它可以让您在多个可用性中为 Amazon EC2 实例保留容量

任何持续时间的区域和多个 AWS 区域都是不正确的，因为您只能为特定 AWS 区域（区域保留实例）或特定可用性区域（区域预留实例）保留容量。您不能在一次 RI 购买中为多个 AWS 区域保留容量。

“它在专用于单个客户的硬件上的 VPC 中运行”选项是不正确的，因为这是专用实例的描述，而不是保留实例的描述。专用实例在专用于单个客户的硬件上的 VPC 中运行。

Q50. 一家公司拥有基于网络的票务服务，利用亚马逊 SQS 和 EC2 实例。使用来自 SQS 队列的消息的 EC2 实例被配置为尽可能频繁地轮询队列，以尽可能高地保持端到端吞吐量。解决方案架构师注意到，在紧密循环中轮询队列使用了不必要的 CPU 周期，由于响应为空，导致操作成本增加。在这种情况下，解决方案架构师应该如何使系统更具成本效益？

- A、 通过将 `ReceiveMessageWaitTimeSeconds` 设置为零，将 Amazon SQS 配置为使用短轮询。
- B、 通过将 `ReceiveMessageWaitTimeSeconds` 设置为大于零的数字，将 Amazon SQS 配置为使用长轮询。
- C、 通过将 `ReceiveMessageWaitTimeSeconds` 设置为零，将 Amazon SQS 配置为使用长轮询。
- D、 通过将 `ReceiveMessageWaitTimeSeconds` 设置为大于零的数字，将 Amazon SQS 配置为使用短轮询。

答案 B

分析：

在这种情况下，应用程序部署在一组 EC2 实例中，这些实例轮询来自单个 SQS 队列的消息。默认情况下，Amazon SQS 使用短轮询，仅查询服务器的子集（基于加权随机分布），以确定是否有任何消息可用于包含在响应中。短轮询适用于需要更高吞吐量的场景。但是，也可以将队列配置为使用长轮询，以降低成本。`ReceiveMessageWaitTimeSeconds` 是队列属性，它决定您使用的是短轮询还是长轮询。默认情况下，它的值为零，这意味着它正在使用短轮询。如果设置为大于零的值，则为长轮询。

因此，通过将 `ReceiveMessageWaitTimeSeconds` 设置为大于零的数字，将 Amazon SQS 配置为使用长轮询是正确答案。关于 SQS 长轮询的快速事实：

- 长轮询有助于减少使用 Amazon SQS 的成本，因为当没有消息可用于回复发送到 Amazon SQ 队列的 `ReceiveMessage` 请求时，可以减少空响应的数量，当消息在队列中可用但不包含在响应中时，可以消除假空响应。

- 长轮询通过允许 Amazon SQS 在发送响应之前等待队列中有消息可用，从而减少了空响应的数量。除非连接超时，否则对 ReceiveMessage 请求的响应至少包含一条可用消息，最多可达 ReceiveMessage 操作中指定的最大消息数。
- 长轮询通过查询所有（而不是有限数量的）服务器来消除假空响应。只要有消息可用，长轮询就会返回消息。

Q51.客户正在将其 ActiveMQ 消息传递代理服务转换到 AWS 云中，其中他们需要支持 NMS 和 MQTT 消息传递协议的替代异步服务。客户没有在云中重新创建消息服务所需的时间和资源。该服务必须具有高可用性，并且几乎不需要管理开销。以下哪项服务最适合用于满足上述要求？

- A、AWS 阶跃函数
- B、亚马逊 MQ
- C、亚马逊社交网站
- D、亚马逊主权财富基金

答案 B

分析：

Amazon MQ 是针对 Apache ActiveMQ 的托管消息代理服务，它使在云中设置和操作消息代理变得非常容易。将当前应用程序连接到 Amazon MQ 很容易，因为它使用行业标准的 API 和协议进行消息传递，包括 JMS、NMS、AMQP、STOMP、MQTT 和 WebSocket。使用标准意味着在大多数情况下，迁移到 AWS 时不需要重写任何消息传递代码。Amazon MQ、Amazon SQS 和 Amazon SNS 是适用于从初创企业到企业的任何人的消息服务。如果您正在将消息传递与现有应用程序一起使用，并且希望快速轻松地将消息传递服务移动到云中，建议您考虑使用 Amazon MQ。它支持行业标准 API 和协议，因此您可以从任何基于标准的 MessageBroker 切换到 Amazon MQ，而无需在应用程序中重写消息传递代码。

如果您正在云上构建全新的应用程序，那么强烈建议您考虑 Amazon SQS 和 Amazon SNS。Amazon SQS 和 SNS 是轻量级的、完全管理的消息队列和主题服务，几乎可以无限扩展，并提供简单易用的 API。您可以使用 Amazon SQS 和 SNS 来分离和扩展微服务、分布式系统和无服务器应用程序，并提高可靠性。

因此，Amazon MQ 是正确答案。

Amazon SNS 是不正确的，因为它更适合作为发布/订阅消息服务，而不是消息代理服务。

亚马逊 SQS 不正确。尽管这是一个完全受管理的消息队列服务，但与 Amazon MQ 不同，它不支持广泛的行业标准消息传递 API 和协议列表。此外，使用 AmazonSQS 需要对应用程序的消息传递代码进行额外更改，以使其兼容。

AWS Step 函数不正确，因为这是一个无服务器的函数编排器，而不是消息传递服务，与 Amazon MQ、AmazonSQS 和 Amazon SNS 不同。

Q52.公司有一个电子商务应用程序，将交易日志保存到 S3 存储桶中。CTO 指示您将应用程序配置为将事务日志保留一个月，以便进行故障排除，然后清除日志。您应该做什么来实现这一要求？

- A、在 Amazon S3 bucket 上添加一个新的 bucket 策略。

- B、在 Amazon S3 bucket 上启用 CORS，这将启用每月自动删除数据
- C、为 Amazon S3 bucket 创建一个新的 IAM 策略，该策略将在一个月后自动删除日志
- D、在 Amazon S3 bucket 上配置生命周期配置规则，以在一个月后清除事务日志

答案 D

分析：

在这种情况下，实现该需求的最佳方法是简单地在 AmazonS3 bucket 上配置生命周期配置规则，以便在一个月后清除事务日志。

生命周期配置允许您指定 bucket 中对象的生命周期管理。配置是一组一个或多个规则，其中每个规则定义了 AmazonS3 应用于一组对象的操作。

这些行动可分为以下几类：

转换操作—定义对象何时转换到另一个存储类。例如，您可以选择在创建后 30 天将对象转换为 STANDARD_IA（IA，用于不频繁访问）存储类，或者在创建后一年将对象归档到 GLACIER 存储类。过期操作-指定对象何时过期。然后 Amazon S3 代表您删除过期的对象。

因此，正确的答案是：在 AmazonS3 bucket 上配置生命周期配置规则，以便在一个月后清除事务日志。

在 Amazon S3 bucket 上添加新 bucket 策略的选项是不正确的，因为它没有提供解决方案来满足您在这种情况下任何需求。将 bucket 策略添加到 bucket，以授予其他 AWS 帐户或 IAM 用户对 bucket 及其对象的访问权限。

“为 Amazon S3 bucket 创建一个新的 IAM 策略，在一个月后自动删除日志”选项是不正确的，因为 IAM 策略主要用于指定 S3 bucket 上允许或拒绝的操作。无法将 IAM 策略配置为以任何方式自动清除日志。

在 Amazon S3 bucket 上启用 CORS，这将启用每月自动删除数据的选项不正确。CORS 允许加载在一个域中的客户端 web 应用程序与不同域中的资源交互。

Q53.一家公司计划减少 Amazon S3 传输到服务器的数据量，以降低运营成本并降低检索数据的延迟。要实现这一点，您需要使用简单结构化查询语言（SQL）语句来过滤 Maazon S3 对象的内容，并检索所需的数据子集。以下哪项服务将帮助您完成此要求？

- A、红移谱
- B、RDS
- C、S3 选择
- D、AWS 阶跃函数

答案 C

分析：

使用 AmazonS3Select，您可以使用简单结构化查询语言（SQL）语句来过滤 AmazonS3 对象的内容并检索所需的数据子集。通过使用 Amazon S3 Select 筛选这些数据，您可以减少 AmazonS3 传输的数据量，从而降低检索这些数据的成本和延迟。

Amazon S3 Select 适用于以 CSV、JSON 或 Apache Parquet 格式存储的对象。它还适用于使用 GZIP 或 BZIP2 压缩的对象（仅适用于 CSV 和 JSON 对象）以及服务器端加密对象。您可以将结果的格式指定为 CSV 或 JSON，还可以确定结果中记录的分隔方式。RDS 不正确。尽管 RDS 是一个 SQL 数据库，您可以在其中执行 SQL 操作，但它仍然无效，因为您希望将 SQL 事务应用于 S3 本身，而不是数据库，这是 RDS 无法做到的。红移光谱不正确。尽管 Amazon Redshift Spectrum 提供了类似于 S3 Select 的查询功能，但该服务更适用于从 S3 中托管的 Redshift 外部表查询数据。Redshift 查询是在集群资源上针对本地磁盘运行的。红移频谱查询使用针对 S3 中数据的每查询扩展资源运行，与 S3 选择相比，这可能需要额外的成本。AWS Step 函数是不正确的，因为它只允许您将多个 AWS 服务协调到无服务器工作流中，以便您可以快速构建和更新应用程序。

Q54.关于数据隐私，要求医疗保健公司遵守《医疗保险可携带性和责任法案》（HIPAA）。该公司将所有备份存储在 Amazon S3 存储桶中。要求存储在 S3 存储桶上的数据必须加密。这样做的最佳选择是什么？（选择两个。）

- A、在通过 HTTPS 将数据发送到 Amazon S3 之前，首先使用您自己的加密密钥在本地加密数据。
- B、将数据存储在启用加密的 EBS 卷上，而不是使用 Amazon S3。
- C、在 S3 存储桶上启用服务器端加密，以使用 AES-128 加密。
- D、将数据存储在加密的 EBS 快照中。

E、在 S3 存储桶上启用服务器端加密，以使用 AES-256 加密。

答案：AE

分析：

服务器端加密是关于静态数据加密，也就是说，Amazon S3 在将数据写入数据中心的磁盘时在对象级别加密数据，并在您访问数据时为您解密。只要您对您的请求进行身份验证，并且您拥有访问权限，您访问加密对象和未加密对象的方式就没有区别。例如，如果使用预先签名的 URL 共享对象，则该 URL 对加密和未加密对象的工作方式相同。

根据您选择如何管理加密密钥，您有三个互斥选项：

使用服务器端加密和 Amazon S3 托管密钥（SSE-S3）

使用 AWS KMS 托管密钥（SSE-KMS）进行服务器端加密

使用客户提供的密钥（SSE-C）进行服务器端加密

在通过 HTTPS 将数据发送到 Amazon S3 之前，先使用您自己的加密密钥在本地加密数据，并在 S3 存储桶上启用服务器端加密以使用 AES-256 加密，这些选项是正确的，因为这些选项分别使用客户端加密和 Amazon S3 托管密钥（SSE-S3）。客户端加密是在将数据发送到 Amazon S3 之前加密数据的行为，而 SSE-S3 使用 AES-256 加密。在启用加密的 EBS 卷上存储数据而不是使用 Amazon S3，并将数据存储在加密 EBS 快照中是不正确的，因为这两个选项都使用 EBS 加密而不是 S3。启用服务器-

在 S3 存储桶上使用 AES-128 加密的侧面加密是不正确的，因为 S3 不提供 AES-28 加密，仅提供 AES-256 加密。

Q55.解决方案架构师正在设计一个数据库的设置，该数据库将在 Amazon RDS for MySQL 上运行。他需要确保数据库能够自动故障转移到 RDS 实例，以便在发生故障时继续运行。架构也应尽可能高可用性。解决方案架构师应该采取以下哪些行动？

- A、跨不同的可用性区域创建五个读取副本。在可用性区域中断的情况下，将任何副本提升为主实例。
- B、在每个区域中创建五个跨区域读取副本。在可用性区域中断的情况下，将任何副本提升为主实例。
- C、通过启用多 AZ 部署，在另一可用性区域中创建备用副本。
- D、在数据库实例所在的同一区域中创建读取副本。此外，在另一个区域中创建一个读取副本，以在区域故障中生存。在可用性区域中断的情况下，将任何副本提升为主实例。

答案 C

分析：

您可以使用多 AZ 部署在多个 AZ 中运行 Amazon RDS DB 实例。Amazon 自动在不同的 AZ 中提供并维护一个备用 DB 实例。主数据库实例跨 AZs 同步复制到辅助实例，以提供数据冗余、故障切换支持、消除 I/O 冻结，并将系统备份期间的延迟峰值降至最低。

如场景中所述，架构必须满足两个要求：数据库应在发生故障时自动故障切换到 RDS 实例。

架构应尽可能高可用性。

因此，正确的答案是：通过启用多 AZ 部署，在另一个可用性区域中创建备用副本，因为它满足这两个要求。

该选项表示：在数据库实例所在的同一区域中创建读取副本。此外，在另一个区域中创建一个读取副本，以在区域发生故障时存活。在可用性区域中断的情况下，将任何副本提升为主实例是不正确的。尽管该体系结构提供了更高的可用性，因为它可以在区域故障中存活，但由于该过程不是自动化的，它仍然不能满足第一个要求。架构还应支持在出现故障时自动故障转移到 RDS 实例。

以下两个选项都不正确：

- 跨不同的可用性区域创建五个读取副本。在可用性区域中断的情况下，将任何副本提升为主实例
- 在每个区域中创建五个跨区域读取副本。在可用性区域中断的情况下，升级任何副本

要成为主实例，尽管在发生故障时，通过将读取副本提升到主实例中，这些架构可以实现高可用性，但它不支持自动故障切换到 RDS 实例，这也是问题中的一个要求。

Q56. 一家公司计划将其在本地运行的容器化应用程序套件迁移到 AWS 中的容器服务。该解决方案必须与云无关，并使用能够自动管理容器化工作负载和服务的开源平台。它还应该在不同的生产环境中使用相同的配置和工具。解决方案架构师应该如何正确迁移并满足给定的需求？

- A、使用 EKS 工作节点将应用程序迁移到 Amazon Elastic Kubernetes 服务。
- B、将应用程序迁移到使用 AWS Fargate 启动类型的 ECS 任务的 Amazon 弹性容器服务。
- C、将应用程序迁移到使用 Amazon EC2 启动类型的 ECS 任务的 Amazon 弹性容器服务。
- D、使用 Amazon EC2 实例工作节点将应用程序迁移到 Amazon 容器注册中心（ECR）。

答：

分析：

Amazon EKS 跨多个 AWS 可用性区域提供并扩展 Kubernetes 控制平面，包括 API 服务器和后端持久性层，以实现高可用性和容错性。

Amazon EKS 自动检测并替换不健康的控制平面节点，并为控制平面提供修补。Amazon EKS 与许多 AWS 服务集成，为您的应用程序提供可扩展性和安全性。这些服务包括用于负载分布的弹性负载平衡、用于身份验证的 IAM、用于隔离的 Amazon VPC 和用于日志记录的 AWS CloudTrail。

要将应用程序迁移到容器服务，您可以使用 Amazon ECS 或 Amazon EKS。但此场景中的关键点是云不可知和开源平台。请注意，Amazon ECS 是 AWS 专有的容器服务。这意味着它不是一个开源平台。Amazon EKS 是一个可移植、可扩展的开源平台，用于管理容器化工作负载和服务。

Kubernetes 被认为是云不可知的，因为它允许您将容器移动到其他云服务提供商。

Amazon EKS 运行最新版本的开源 Kubernetes 软件，因此您可以使用所有现有的

来自 Kubernetes 社区的插件和工具。在 Amazon EKS 上运行的应用程序与在任何标准 Kubernetes 环境上运行的程序完全兼容，无论是在本地数据中心还是公共云上运行。这意味着您可以轻松地将任何标准 Kubernetes 应用程序迁移到 Amazon EKS，而无需任何代码修改。

因此，正确的答案是：使用 EKS 工作节点将应用程序迁移到 Amazon 弹性 Kubernetes 服务。

“使用 Amazon EC2 实例工作节点将应用程序迁移到 Amazon 容器注册表（ECR）”选项不正确，因为 Amazon ECR 只是一个完全管理的 Docker 容器注册表。此外，此选项不是可以管理容器化工作负载和服务的开源平台。

“将应用程序迁移到使用 AWS Fargate 启动类型的 ECS 任务的 Amazon 弹性容器服务”选项是不正确的，因为在场景中说明您必须将应用程序套件迁移到开源平台。AWS Fargate 只是一个用于容器的无服务器计算引擎。它不是云不可知的，因为如果您将其移动到另一个云服务提供商，如 Microsoft Azure 或 Google cloud Platform（GCP），则无法使用相同的配置和工具。

选项是：将应用程序迁移到使用 Amazon EC2 启动类型的 ECS 任务的 Amazon 弹性容器服务。不正确，因为 Amazon ECS 是 AWS 专有的托管容器编排服务。

您应该使用 Amazon EKS，因为 Kubernetes 是一个开源平台，被认为是云不可知的。使用 Kubernetes，即使您将容器移动到另一个云服务提供商，您也可以使用当前在 AWS 中使用的相同配置和工具。

Q57. 一家公司计划在 AWS 中托管电影流应用程序。首席信息官（CIO）希望确保应用程序具有高可用性和可扩展性。应用程序部署到多个 AZ 上的 EC2 实例的自动扩展组。负载均衡器必须配置为将传入请求均匀分布到多个可用性区域中的所有 EC2 实例。解决方案架构师应该使用以下哪些功能来满足这些标准？

- A、 基于路径的路由
- B、 亚马逊专有网络 IP 地址管理器（IPAM）
- C、 跨区域负载均衡
- D、 AWS 直接连接站点链接

答案 C

分析：

负载均衡器的节点将请求从客户端分发到注册的目标。当启用跨区域负载均衡时，每个负载均衡器节点将流量分布到所有启用的可用性区域中的注册目标。当禁用跨区域负载均衡时，每个负载均衡器节点仅跨其可用性区域中的注册目标分配流量。

下图演示了跨区域负载均衡的效果。有两个已启用的可用性区域，可用性区域 A 中有两个目标，可用性区中有八个目标

B： 客户端发送请求，亚马逊路由 53 用负载均衡器节点之一的 IP 地址响应每个请求。这样分配流量，使得每个负载均衡器节点从客户端接收 50% 的流量。每个负载均衡器节点在其范围内的注册目标上分配其流量份额。如果启用跨区域负载均衡，则 10 个目标中的每个目标接收 10% 的流量。这是因为每个负载均衡器节点可以将 50% 的客户端流量路由到所有 10 个目标。

如果禁用跨区域负载平衡：

可用性区域 A 中的两个目标中的每一个都接收 25% 的流量。

可用性区域 B 中的八个目标中的每一个接收 6.25% 的流量。

这是因为每个负载平衡器节点只能将 50% 的客户端流量路由到其可用性区域中的目标。

对于应用程序负载均衡器，始终启用跨区域负载平衡。

对于网络负载平衡器和网关负载平衡器，默认情况下禁用跨区域负载平衡。创建负载平衡器后，可以随时启用或禁用跨区域负载平衡。创建经典负载平衡器时，跨区域负载平衡的默认值取决于如何创建负载平衡器。使用 API 或 CLI，默认情况下禁用跨区域负载平衡。

在 AWS 管理控制台中，默认选择启用跨区域负载平衡的选项。

创建经典负载均衡器后，您可以随时启用或禁用跨区域负载平衡。因此，正确的答案是启用跨区域负载均衡。亚马逊专有网络 IP 地址管理器（IPAM）不正确，因为这只是亚马逊专有网络中的一个功能，为网络管理员提供了自动化的 IP 管理工作流。它不允许负载平衡器将传入请求均匀分布到多个可用性区域中的所有 EC2 实例。

基于路径的路由不正确，因为此功能基于请求 URL 中的路径。它根据请求 URL 自动将流量路由到特定的目标组。此功能不会将每个负载平衡器节点设置为在所有启用的可用性区域中的注册目标之间分配流量。

AWS Direct Connect SiteLink 是不正确的，因为这是 AWS 直接连接的功能，而不是亚马逊弹性负载平衡的功能。AWS 直接连接站点链接功能仅允许您通过 AWS 全球网络主干在本地网络之间创建连接。

Q58.解决方案架构师需要确保亚马逊专有网络中的所有 AWS 资源不会超出各自的服务限制。架构师应准备一个系统，提供符合 AWS 最佳实践的资源调配实时指导。以下哪项服务最适合用于完成此任务？

- A、AWS 成本管理器
- B、亚马逊检查员
- C、AWS 预算
- D、AWS 可信顾问

答案 D

分析：

AWS Trusted Advisor 是一个在线工具，为您提供实时指导，帮助您按照 AWS 最佳实践提供资源。它会检查您的 AWS 环境，并提出节约资金、提高系统性能和可靠性或关闭的建议

安全漏洞。无论是建立新的工作流、开发应用程序，还是作为持续改进的一部分，请定期利用 Trusted Advisor 提供的建议，以帮助您以最佳方式提供解决方案。

Trusted Advisor 包括以下五类不断扩展的检查列表：

成本优化-通过强调未使用的资源和减少账单的机会，可能为您节省资金的建议。安全-识别可能使 AWS 解决方案不安全的安全设置。过错

容差-通过强调冗余不足、当前服务限制和资源过度利用，帮助提高 AWS 解决方案弹性的建议。性能-有助于提高应用程序速度和响应能力的建议。

服务限制-当服务使用率超过服务限制的 80%时，会告诉您的建议。

因此，本场景中的正确答案是 AWS Trusted Advisor。AWS 成本管理器是不正确的，因为它只是一个工具，可以让您查看和分析成本和使用情况。您可以使用主图、成本管理器成本和使用情况报告或成本管理器 RI 报告来探索使用情况和成本。它有一个易于使用的界面，可以让您可视化、理解和管理 AWS 的成本和使用情况。AWS 预算是不正确的，因为它只是让您能够设置自定义预算，当您的成本或使用量超过（或预计将超过）预算金额时，会提醒您。您还可以使用 AWS 预算设置预订利用率或覆盖率目标，并在利用率下降到您定义的阈值以下时接收警报。Amazon Inspector 是不正确的，因为它只是一个自动安全评估服务，有助于提高部署在 AWS 上的应用程序的安全性和合规性。Amazon Inspector 自动评估应用程序的暴露、漏洞和与最佳实践的偏差。

Q59.一家全球医学研究公司拥有一个分子成像系统，为每个客户提供分子和细胞水平上人体内发生的情况的频繁更新图像。系统托管在 AWS 中，图像托管在 CloudFront web 发行版后面的 S3 bucket 中。当一批新的图像上传到 S3 时，需要保留之前的图像，以防止它们被覆盖。以下哪种解决方案最适合解决此问题？

- A、 使 CloudFront web 发行版中的文件无效
- B、 为内容添加单独的缓存行为路径，并配置最小 TTL 为 0 的自定义对象缓存
- C、 在 S3 bucket 中添加缓存控制-无缓存、无存储或私有指令。使用版本化对象

答案 D

分析：

要控制分发版中提供的文件的版本，可以使文件无效，也可以为其指定版本文件名。如果您希望频繁更新文件，AWS 建议您主要使用文件版本控制，原因如下：

- 版本控制使您能够控制请求返回的文件，即使用户在本地或在公司缓存代理之后缓存了版本。如果您使文件无效，用户可能会继续看到旧版本，直到它从这些缓存中过期。
- CloudFront 访问日志包括文件的名称，因此版本控制使分析文件更改的结果更容易。
- 版本控制提供了一种向不同用户提供不同版本文件的方法。
- 版本控制简化了文件修订之间的前滚和后滚。

- 版本控制成本较低。您仍然需要为 CloudFront 付费，以便将文件的新版本传输到边缘位置，但您不必为文件无效付费。

使 CloudFront web 发行版中的文件无效是不正确的，因为即使使用无效将解决此问题，但与使用版本化对象相比，此解决方案的成本更高。

为内容添加单独的缓存行为路径，并配置最小 TTL 为 0 的自定义对象缓存是不正确的，因为这本身不足以解决问题。缓存行为主要用于为网站上文件的给定 URL 路径模式配置各种 CloudFront 功能。尽管此解决方案可能有效，但最好使用版本化对象，这样即使用户在本地或在公司缓存代理之后缓存了另一个版本，也可以控制系统将返回哪个映像。

在 S3 bucket 中添加 Cache Control no Cache、no store 或 private 指令是不正确的，因为虽然可以将源代码配置为添加 Cache 控件或 Expires 头字段，但您应该对对象而不是整个 S3 bucket 执行此操作。

Q60.一位解决方案架构师在一家金融公司工作。管理者希望能够自动将过时数据从 S3 存储桶传输到 AWS 中的低成本存储系统。架构师可以为他们提供的最佳解决方案是什么？

- A、使用 Cloud 持久迁移。
- B、使用 EC2 实例和调度作业将过时数据从其 S3 位置传输到 Amazon S3 Glacier。
- C、使用 S3 中的生命周期策略将过时数据移动到 Glacier。
- D、使用 Amazon SQS。

答案 C

分析：

在这种情况下，您可以使用 S3 中的生命周期策略自动将过时数据移动到 Glacier。AmazonS3 中的生命周期配置允许您指定 bucket 中对象的生命周期管理。配置是一组一个或多个规则，其中每个规则定义了 AmazonS3 应用于一组对象的操作。

这些行动可分为以下几类：

转换操作—定义对象何时转换到另一个存储类。例如，您可以选择在创建后 30 天将对象转换为 STANDARD_IA（IA，用于不频繁访问）存储类，或者在创建后一年将对象归档到 GLACIER 存储类。过期操作-指定对象何时过期。然后 Amazon S3 代表您删除过期的对象。

“使用 EC2 实例和调度作业将过时数据从其 S3 位置传输到 Amazon S3 Glacier”的选项是不正确的，因为您不需要在 EC2 中创建调度作业，因为您可以简单地使用 S3 中的生命周期策略。

“使用 Amazon SQS”选项不正确，因为 SQS 不是存储服务。AmazonSQS 主要用于通过将应用程序的传入请求排队来分离应用程序。

“使用云持久迁移”选项是不正确的，因为该服务只是一个高度自动化的提升和转移（重新托管）解决方案，可以简化、加快并降低将应用程序迁移到 AWS 的成本。您不能使用它自动将 S3 对象转换为更便宜的存储类。

Q61.一家软件开发公司正在使用 AWS Lambda 的无服务器计算来构建和运行应用程序，而无需设置或管理服务器。它们有一个连接到 MongoDB Atlas 的 Lambda 函数，这是一个流行的数据库即服务（DBaaS）平台，

还使用第三方 API 为其应用程序获取某些数据。其中一名开发人员被指示创建 MongoDB 数据库主机名、用户名和密码的环境变量，以及 Lambda 函数将用于开发、SIT、UAT 和 PROD 环境的 API 凭据。考虑到 Lambda 函数正在存储敏感的数据库和 API 凭据，如何保护这些信息，以防止团队中的其他开发人员或任何人以明文形式看到这些凭据？选择提供最大安全性的最佳选项。

- A、启用 SSL 加密，利用 AWS CloudHSM 存储和加密敏感信息。
- B、AWS Lambda 不为环境变量提供加密。将代码部署到 EC2 instance instead。
- C、不需要做任何事情，因为默认情况下，AWS Lambda 已经使用 AWS 密钥管理服务对环境变量进行了加密。
- D、创建一个新的 KMS 密钥，并使用它来启用加密帮助程序，利用 AWS 密钥管理服务来存储和加密敏感信息。

答案 D

分析：

创建或更新使用环境变量的 Lambda 函数时，AWS Lambda 将使用 AWS 密钥管理服务对其进行加密。调用 Lambda 函数时，这些值将被解密，并可用于 Lambda 代码。

第一次创建或更新使用区域中环境变量的 Lambda 函数时，将在 AWS KMS 中自动为您创建默认服务密钥。此密钥用于加密环境变量。但是，如果希望在创建 Lambda 函数后使用加密帮助程序和 KMS 加密环境变量，则必须创建自己的 AWS KMS 密钥，并选择它而不是默认密钥。选择默认键时会出现错误。创建自己的密钥使您具有更大的灵活性，包括创建、旋转、禁用和定义访问控制的能力，以及审核用于保护数据的加密密钥的能力。

“不需要做任何事情，因为默认情况下，AWS Lambda 已经使用 AWS 密钥管理服务对环境变量进行了加密”选项是不正确的。虽然默认情况下 Lambda 会加密函数中的环境变量，但敏感信息对其他访问 Lambda 控制台的用户仍然可见。这是因为 Lambda 使用默认 KMS 密钥加密变量，其他用户通常可以访问该密钥。此场景中的最佳选项是使用加密助手来保护环境变量。

选项“启用 SSL 加密”利用 AWS CloudHSM 存储和加密敏感信息也是不正确的，因为启用 SSL 只会在传输中加密数据。您的其他团队仍然可以在休息时查看明文。改用 AWS KMS。该选项表示：

AWS Lambda 不为环境变量提供加密。相反，将代码部署到 EC2 实例是不正确的，因为如前所述，Lambda 确实提供了环境变量的加密功能。

参考文献：

https://docs.aws.amazon.com/lambda/latest/dg/env_variables.html#env_encrypthttps://docs.aws.amazon.com/lambda/latest/dg/tutorial-env_console.html 查看此 AWS Lambda 备忘单：

<https://tutorialsdojo.com/aws-lambda/>

AWS Lambda 概述-AWS 中的无服务器计算：

<https://www.youtube.com/watch?v=bPVX1zHwAnY>

Q62.一家公司在应用程序负载均衡器后面的 EC2 实例自动扩展组上托管了一个电子商务网站。解决方案架构师注意到，该网站正在接收来自多个 IP 地址不断变化的系统的大量非法外部请求。为了解决性能问题，解决方案架构师必须实现一个解决方案，该解决方案将阻止非法请求，对合法流量的影响最小。

以下哪个选项符合此要求？

- A、在 AWS WAF 中创建常规规则，并将 web ACL 与应用程序负载均衡器关联。
- B、在 AWS WAF 中创建基于速率的规则，并将 web ACL 与应用程序负载均衡器关联。
- C、在应用程序负载均衡器的安全组中创建自定义规则，以阻止违规请求。
- D、创建自定义网络 ACL，并将其与应用程序负载均衡器的子网关联，以阻止违规请求。

答案 B

分析：

AWS WAF 与 Amazon CloudFront、应用程序负载均衡器（ALB）、Amazon API 网关和 AWS AppSync 紧密集成？AWS 客户通常用于为其网站和应用程序提供内容的服务。当您在 Amazon CloudFront 上使用 AWS WAF 时，您的规则将在世界各地靠近终端用户的所有 AWS 边缘位置运行。这意味着安全不会以牺牲性能为代价。阻止的请求在到达 web 服务器之前停止。当您在区域服务（如应用程序负载均衡器、亚马逊 API 网关和 AWS AppSync）上使用 AWS WAF 时，您的规则在区域内运行，可用于保护面向互联网的资源以及内部资源。

cm 基于速率的规则跟踪每个原始 IP 地址的请求速率，并在速率超过限制的 IP 上触发规则动作。您将限制设置为每 5 分钟时间跨度的请求数。您可以使用这种类型的规则对来自发送过多请求的 IP 地址的请求设置临时阻止。

基于给定场景，要求是限制来自非法请求的请求数量，而不影响真正请求。要实现此要求，可以使用 AWS WAF web ACL。创建自己的 web ACL 规则时有两种类型的规则：常规规则和基于速率的规则。您需要选择

后者为 web ACL 添加速率限制。创建 web ACL 后，可以将其与 ALB 关联。当规则动作触发时，AWS WAF 将动作应用于来自 IP 地址的其他请求，直到请求速率低于限制。

因此，正确的答案是：在 AWS WAF 中创建基于速率的规则，并将 web ACL 与应用程序负载均衡器关联。

“在 AWS WAF 中创建常规规则并将 web ACL 与应用程序负载均衡器关联”选项不正确，因为常规规则仅与规则中定义的语句匹配。如果需要为规则添加速率限制，则应创建基于速率的规则。“创建自定义网络 ACL 并将其与应用程序负载均衡器的子网关联以阻止违规请求”选项不正确。尽管 NACL 可以帮助您阻止传入流量，但此选项无法限制来自动态变化的单个 IP 地址的请求数。“在应用程序负载均衡器的安全组中创建自定义规则以阻止违规请求”选项不正确，因为安全组只能允许传入流量。请记住，您不能使用安全组来拒绝流量。此外，与 AWS WAF 不同，它不能限制应用程序的流量速率。

参考文献：

<https://docs.aws.amazon.com/waf/latest/developerguide/waf-rule-statement-type-rate-based.html><https://aws.amazon.com/waf/faqs/>

查看 AWS WAF 备忘单：

<https://tutorialsdojo.com/aws-waf/>

AWS 安全服务概述-WAF、Shield、CloudHSM、KMS：<https://www.youtube.com/watch?v=-1SRdeAmMo>

Q63.您的生产环境中发生了一个事件，存储在 S3 存储桶中的用户数据已经

被一位德沃普的初级工程师意外删除。该问题已上报给您的经理，几天后，您被指示改善 AWS 资源的安全和保护。以下哪些选项组合将保护 bucket 中的 S3 对象免受意外删除和覆盖？（选择两个。）

- A、启用版本控制
- B、启用 Amazon S3 智能分层
- C、仅通过预先签名的 URL 提供对 S3 数据的访问
- D、启用多因素身份验证删除
- E、禁止使用 IAM 存储桶策略删除 S3

答：屋宇署

分析：

通过使用版本控制和启用 MFA（多因素身份验证）删除，您可以保护和恢复 S3 对象，防止意外删除或覆盖。

版本控制是将对象的多个变体保持在同一个 bucket 中的一种方法。启用版本控制的存储桶使您能够从意外删除或覆盖中恢复对象。您可以使用版本控制来保存、检索和恢复存储在 AmazonS3 存储桶中的每个对象的每个版本。通过版本控制，您可以轻松地从意外的用户操作和应用程序故障中恢复。您还可以选择通过配置 bucket 来启用 MFA（多因素身份验证）删除来添加另一层安全性，这需要对以下操作进行额外身份验证：

- 更改 bucket 的版本控制状态
- 永久删除对象版本

MFA 删除需要两种形式的身份验证：

- 您的安全凭证
- 有效序列号、空格和六位代码的串联显示在经批准的身份验证设备上

仅通过预签名 URL 提供对 S3 数据的访问是不正确的，因为预签名 URL 允许访问 URL 中标识的对象。当客户将对象上传到您的 S3 bucket 时，预签名 URL 很有用，但无助于防止意外删除。不允许使用 IAM 存储桶策略进行 S3 删除是不正确的，因为您仍然希望用户能够删除存储桶中的对象，并且只希望防止意外删除。不允许使用 IAM 存储桶策略进行 S3 删除将限制您存储桶的所有删除操作。启用 AmazonS3 智能分层是不正确的，因为 S3 智能分层在这种情况下没有帮助。

参考：

<https://docs.aws.amazon.com/AmazonS3/latest/dev/Versioning.html> 查看此 Amazon S3 备忘单：

<https://tutorialsdodojo.com/amazon-s3/>

Q64.一家电信公司计划向开发者提供 AWS 控制台访问权限。公司政策要求使用身份联合和基于角色的访问控制。目前，已使用公司 Active Directory 中的组分配角色。在这种情况下，以下哪种服务组合可以为开发人员提供对 AWS 控制台的访问？（选择两个。）

- A、AWS 目录服务简单广告
- B、IAM 角色
- C、IAM 组
- D、AWS 目录服务 AD 连接器

答：屋宇署

分析：

考虑到公司使用的是企业活动目录，最好使用 AWS 目录服务 AD

连接器，便于集成。此外，由于角色已经使用公司 Active Directory 中的组分配，因此最好也使用 IAM 角色。请注意，一旦 Active Directory 通过 AWS 目录服务 AD 连接器与 VPC 集成，您可以将 IAM 角色分配给 Active Directory 中的用户或组。

AWS 目录服务提供了多种方式将亚马逊云目录和 Microsoft Active Directory (AD) 与其他 AWS 服务一起使用。目录存储有关用户、组和设备的消息，管理员使用它们来管理对信息和资源的访问。AWS 目录服务为希望在云中使用现有 Microsoft AD 或轻量级目录访问协议 (LDAP) 软件应用程序的客户提供了多种目录选择。它还为需要目录来管理用户、组、设备和访问的开发人员提供了相同的选择。AWS 目录服务简单广告是不正确的，因为它只提供了 AWS 提供的功能的一个子集

托管 Microsoft AD，包括管理用户帐户和组成员身份、创建和应用组策略、安全连接到 Amazon EC2 实例以及提供基于 Kerberos 的单点登录 (SSO) 的能力。在这种情况下，更适合使用的组件是 AD 连接器，因为它是一个目录网关，您可以使用它将目录请求重定向到本地 Microsoft Active directory。IAM 组不正确，因为这只是 IAM 用户的集合。组允许您为多个用户指定权限，这样可以更容易地管理这些用户的权限。在这种情况下，更适合使用 IAM 角色，以便获得创建 AWS 目录服务资源的权限。Lambda 不正确，因为它主要用于无服务器计算。参考：<https://aws.amazon.com/blogs/security/how-to-connect-your-on-premises-active-directory-to-aws-using-ad-connector/>查看这些 AWS IAM 和目录服务备忘单：

<https://tutorialsdojo.com/aws-identity-and-access-management-iam/> <https://tutorialsdojo.com/aws-目录服务/>这里是

AWS 目录服务的视频教程：

<https://youtu.be/4XeqotTYBtY>

Q65.人工智能驱动的外汇交易应用程序消耗数千个数据集来训练其机器学习模型。应用程序的工作负载需要一个高性能并行热存储来同时处理训练数据集。它还需要经济高效的冷库来归档那些利润低的数据集。

开发人员应该使用以下哪种亚马逊存储服务？

A、 分别将 Amazon FSx 用于 Windows 文件服务器和 Amazon S3 用于热存储和冷存储。

B、 分别使用 Amazon 弹性文件系统和 Amazon S3 进行热存储和冷存储。

C、 将 Amazon FSx 用于 Lustre，将 Amazon EBS 配置的 IOPS SSD (io1) 卷分别用于热存储和冷存储。

D、 将 Amazon FSx 用于 Lustre，将 Amazon S3 分别用于冷热存储。

答案 D

分析：

热存储是指保存频繁访问的数据（热数据）的存储。热存储是指保存访问频率较低的数据（热数据）的存储。冷存储是指保存很少访问的数据（冷数据）的存储。在定价方面，数据越冷，存储成本越低，需要时访问成本越高。

Amazon FSx For Lustre 是用于快速处理工作负载的高性能文件系统。Lustre 是一个流行的开源并行文件系统，它跨多个网络文件服务器存储数据，以最大限度地提高性能并减少瓶颈。

Amazon FSx for Windows 文件服务器是一个完全管理的 Microsoft Windows 文件系统，完全支持 SMB 协议、Windows NTFS 和 Microsoft Active Directory（AD）集成。Amazon Elastic 文件系统是一个完全管理的文件存储服务，可以轻松地在 Amazon 云中设置和扩展文件存储。

Amazon S3 是一种对象存储服务，提供业界领先的可扩展性、数据可用性、安全性和性能。S3 为不同的用例（频繁访问的数据、不经常访问的数据和很少访问的数据）提供了不同的存储层。

这个问题有两个要求：

高性能并行热存储，可同时处理训练数据集。经济高效的冷存储：为了保持在这种情况下很少访问的存档数据集，我们可以使用 Amazon FSx 来满足第一个需求，因为它为热数据提供了高性能的并行文件系统。关于第二个需求，我们可以使用 Amazon S3 来存储冷数据。亚马逊 S3 通过亚马逊 S3 冰川/冰川深度档案库支持冷藏系统。

因此，正确答案是：分别使用 Amazon FSx 进行 Lustre 和 Amazon S3 进行热存储和冷存储。

将 Amazon FSx 用于 Lustre 和 Amazon EBS 配置的 IOPS SSD（io1）卷分别用于热存储和冷存储是不正确的，因为配置的 IOP SSD（IO2）卷用于存储 I/O 密集型工作负载中使用的热数据（频繁访问的数据）。EBS 有一个名为“冷硬盘”的存储选项，但由于其价格，它不是数据存档的理想选择。EBS Cold HDD 比 Amazon S3 Glacier/GlacierDeep Archive 贵得多，通常用于读取顺序 Cold 数据频率较低的应用程序。

将 Amazon 弹性文件系统和 Amazon S3 分别用于热存储和冷存储是不正确的。尽管 EFS 支持并发访问数据，但它不具备机器学习工作负载所需的高性能能力。

分别使用 Amazon FSx For Windows File Server 和 Amazon S3 进行热存储和冷存储是不正确的，因为 Amazon FSx For Windows File Server 与 Lustre 不同，没有并行文件系统。

参考文献：

<https://aws.amazon.com/fsx/> <https://docs.aws.amazon.com/whitepapers/latest/cost-optimization-storage-optimization/aws-storage-services.html>

<https://aws.amazon.com/blogs/startups/picking-the-right-data-store-for-your-workload/> 查看此亚马逊 FSx 备忘单：
<https://tutorialsdodojo.com/amazon-fsx/>

Q66.新聘用的解决方案架构师负责管理一组云信息模板，这些模板用于 AWS 中公司的云架构。架构师访问了模板，并尝试分析 S3 存储桶的配置 IAM 策略。

上述 IAM 政策允许什么？（选择三个。）

```
{  
  "版本": "2012-10-17",  
  "声明": [  
    {  
      "Effect": "Allow",  
      "Action": "s3:ListBucket",  
      "Resource": "arn:aws:s3:::my-bucket"    }  
  ]  
}
```

```

    {"效果": "允许", "操作": ["s3:Get*",
                                "s3:List*"],
      "资源": "*"
    },
    {"效果": "允许",
      "操作": "s3:PutObject",
      "资源": "arn:aws:s3:::长滩岛/*"
    }
  ]
}

```

- A、具有此 IAM 策略的 IAM 用户可以读取 boracay S3 存储桶中的对象，但不允许列出存储桶中对象。
- B、具有此 IAM 策略的 IAM 用户可以更改长滩岛 S3 存储桶的访问权限。
- C、具有此 IAM 策略的 IAM 用户可以将对象写入长滩岛 S3 存储桶。
- D、具有此 IAM 策略的 IAM 用户可以从长滩岛 S3 存储桶读取对象。
- E、具有此 IAM 策略的 IAM 用户可以读取和删除长滩岛 S3 存储桶中的对象。
- F、具有此 IAM 策略的 IAM 用户可以从帐户拥有的所有 S3 存储桶中读取对象。

答：CDF

分析：

您可以通过创建策略并将其附加到 IAM 标识（用户、用户组或角色）或 AWS 资源来管理 AWS 中的访问。策略是 AWS 中的一个对象，当与标识或资源关联时，定义其权限。AWS 在 IAM 主体（用户或角色）发出请求时评估这些策略。策略中的权限决定是否允许或拒绝请求。大多数策略以 JSON 文档的形式存储在 AWS 中。AWS 支持六种类型的策略：基于身份的策略、基于资源的策略、权限边界、AWS 组织 SCP、ACL 和会话策略。

IAM 策略定义操作权限，而不管您使用何种方法执行操作。例如，如果策略允许 GetUser 操作，则具有该策略的用户可以从 AWS 管理控制台、AWS CLI 或 AWS API 获取用户信息。创建 IAM 用户时，可以选择允许控制台或编程访问。如果允许控制台访问，IAM 用户可以使用用户名和密码登录控制台。或者，如果允许编程访问，用户可以使用访问密钥来使用 CLI 或 API。

根据提供的 IAM 策略，用户只能获取、写入和列出长滩岛 s3 存储桶的所有对象。s3:PutObject 基本上意味着您可以向 s3 bucket 提交一个 PUT 对象请求来存储数据。

因此，正确答案是：

- 具有此 IAM 策略的 IAM 用户可以从帐户拥有的所有 S3 存储桶中读取对象。
- 具有此 IAM 策略的 IAM 用户可以将对象写入长滩岛 S3 存储桶。
- 具有此 IAM 策略的 IAM 用户可以从长滩岛 S3 存储桶读取对象。“允许具有此 IAM 策略的 IAM 用户更改 boracay S3 存储桶的访问权限”选项不正确，因为模板没有任何允许用户更改存储桶中访问权限的语句。

“允许具有此 IAM 策略的 IAM 用户读取长滩岛 S3 存储桶中的对象，但不允许列出存储桶中对象”选项不正确，因为在模板中可以清楚地看到，存在允许用户列出对象的 S3:list*。“允许具有此 IAM 策略的 IAM 用户读取和删除长滩岛 S3 存储桶中的对象”选项不正确。虽然可以从 bucket 中读取对象，但不能删除任何对象。

参考文献：

<https://docs.aws.amazon.com/AmazonS3/latest/API/RESTObjectOps.html>

https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html 查看此 Amazon S3 备忘单：

<https://tutorialsdojo.com/amazon-s3/>

问题 67.零售网站整天都有间歇性、零星和不可预测的事务性工作负载，难以预测。该网站目前在本地托管，计划迁移到 AWS。需要一个新的关系数据库，它可以自动扩展容量以满足应用程序的峰值负载需求，并在活动激增结束时缩减。

在这种情况下，以下哪个选项是最具成本效益和最合适的数据库设置？

- A、启动启用自动缩放的 DynamoDB 全局表。
- B、启动 Amazon Aurora 无服务器 DB 集群，然后设置集群的最小和最大容量。
- C、启动具有并发扩展的 Amazon Redshift 数据仓库集群。
- D、使用 burstable 性能数据库实例类类型启动 Amazon Aurora 配置的数据库集群。

答案 B

分析：

Amazon Aurora 无服务器是 Amazon Aurora 的按需自动扩展配置。Aurora 无服务器数据库集群是一个数据库集群，它可以根据应用程序的需要自动启动、关闭和扩展计算容量。Aurora Serverless 为不频繁、间歇、零星或不可预测的工作负载提供了相对简单、经济高效的选项。它可以提供这一功能，因为它可以自动启动，扩展计算能力以匹配应用程序的使用，并在不使用时关闭。

请注意，Aurora 的非无服务器数据库集群称为配置数据库集群。Aurora 无服务器集群和配置集群都具有相同类型的高容量、分布式和高可用存储卷。

使用 Amazon Aurora 而不使用 Aurora Serverless（配置的数据库集群）时，可以选择数据库实例类大小并创建 Aurora 副本以提高读取吞吐量。如果工作负载发生变化，您可以修改 DB 实例类大小并更改 Aurora 副本的数量。当数据库工作负载是可预测的时，此模型运行良好，因为您可以根据预期的工作负载手动调整容量。

然而，在某些环境中，工作负载可能是间歇性和不可预测的。可能会有可能只持续几分钟或几个小时的繁重工作，也可能有长时间的轻活动，甚至没有活动。一些示例包括具有间歇性销售事件的零售网站、在需要时生成报告的报告数据库、开发和测试环境以及具有不确定需求的新应用程序。在这些情况和许多其他情况下，可能很难在正确的时间配置正确的容量。当您为未使用的容量付费时，也会导致更高的成本。

使用 Aurora Serverless，您可以创建数据库端点，而无需指定 DB 实例类大小。您可以设置最小和最大容量。使用 Aurora Serverless，数据库端点连接到代理舰队，该代理舰队将工作负载路由到自动扩展的资源舰队。由于代理舰队，

连接是连续的，因为 Aurora Serverless 根据最小和最大容量规格自动扩展资源。数据库客户端应用程序无需更改即可使用代理舰队。Aurora 无服务器自动管理连接。扩展速度很快，因为它使用了一个“热”资源池，这些资源随时可以为请求提供服务。存储和处理是分开的，因此您可以缩小到零处理，只为存储付费。Aurora 无服务器为 Aurora DB 集群引入了新的无服务器 DB 引擎模式。非无服务器数据库集群使用配置的数据库引擎模式。

因此，正确的答案是：启动 Amazon Aurora 无服务器 DB 集群，然后设置集群的最小和最大容量。

“使用 burstable 性能数据库实例类类型启动 Amazon Aurora 配置的数据库集群”选项是不正确的，因为 Aurora 提供的数据库集群不适用于间歇性、零星和不可预测的事务性工作负载。当数据库工作负载是可预测的时，此模型运行良好，因为您可以根据预期的工作负载手动调整容量。这里更好的数据库设置是使用 Amazon Aurora 无服务器集群。

“启动启用自动缩放的 DynamoDB 全局表”选项是不正确的，因为尽管它使用自动缩放，但该场景明确指出您需要一个关系数据库来处理事务性工作负载。DynamoDB 是一个 NoSQL 数据库，不适合此用例。此外，不保证使用 DynamoDB 全局表，因为它主要用于需要一个完全管理、多区域和多主数据库的情况，该数据库为大规模全局应用程序提供快速、本地、读写性能。

“启动具有并发扩展的 Amazon Redshift 数据仓库集群”选项不正确，因为这种类型的数据库主要用于在线分析处理（OLAP），而不是在线事务处理（OLTP）。并发扩展只是 Amazon Redshift 的一个功能，它可以自动和弹性地扩展 Redshift 集群的查询处理能力，为数百个并发查询提供一致的快速性能。参考文献：

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-无服务器。它是如何工作的。htmlhttps://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-serverless.html>

Q68. 一个流行的社交媒体网站使用 CloudFront web 分发服务，向全球数百万用户提供静态内容。他们最近收到了许多投诉，称他们的用户花了很多时间登录他们的网站。有时，他们的用户也会遇到 HTTP 504 错误。您的经理指示您大幅缩短用户登录时间，以进一步优化系统。您应该一起使用以下哪些选项来建立一个经济高效的解决方案，以提高应用程序的性能？（选择两个。）

A、使用自定义 CloudFront web 分发版向用户提供的内容 Lambda@Edge，它允许 Lambda 函数在更靠近用户的 AWS 位置执行身份验证过程。

B、将应用程序部署到多个 AWS 区域，以适应世界各地的用户。设置具有延迟路由策略的路由 53record，以将传入流量路由到向用户提供最佳延迟的区域。

C、配置原点以向对象添加缓存控制最大年龄指令，并为最大年龄指定最长的实际值，以增加 CloudFront 分布的缓存命中率。

D、通过创建具有两个源的源组来设置源故障切换。指定一个作为主站，另一个作为第二站，当主站返回特定 HTTP 状态码失败响应时，CloudFront 会自动切换到第二站。

E、使用多个地理上分散的 VPC 连接到各个 AWS 区域，然后创建一个中转 VPC 连接所有资源。为了更快地处理请求，使用 AWS 无服务器应用程序模型（SAM）服务在每个区域设置 Lambda 函数。

回答广告

分析：

Lambda@Edge 允许您运行 Lambda 函数来定制 CloudFront 交付的内容，在 AWS 中靠近查看器的位置执行这些函数。这些函数响应 CloudFront 事件而运行，而无需配置或管理服务器。您可以使用 Lambda 函数在以下几点更改 CloudFront 请求和响应：

- CloudFront 收到来自查看器的请求后（查看器请求）
- 在 CloudFront 将请求转发到源站之前（源站请求）
- CloudFront 收到来自源站的响应后（源站响应）
- 在给定场景中，CloudFront 将响应转发给查看器（查看器响应）之前，可以使用 Lambda@Edge 允许您的 Lambda 函数自定义 CloudFront 交付的内容，并在更靠近用户的 AWS 位置执行身份验证过程。此外，您还可以通过创建一个具有两个源的源组来设置源故障转移，其中一个作为主源，另一个作为第二个源，当主源出现故障时，CloudFront 会自动切换到该源。这将缓解用户偶尔遇到的 HTTP 504 错误。

因此，正确答案是：

- 使用自定义 CloudFront web 分发版向用户提供的内容 Lambda@Edge，这允许您的 Lambda 函数在更靠近用户的 AWS 位置执行身份验证过程。
- 通过创建具有两个源的源组来设置源故障切换。指定一个作为主站，另一个作为第二站，当主站返回特定 HTTP 状态码失败响应时，CloudFront 会自动切换到第二站。该选项表示：使用多个地理上分散的 VPC 连接到各个 AWS 区域，然后创建一个中转 VPC 连接所有资源。为了更快地处理请求，使用 AWS 无服务器应用程序模型（SAM）服务在每个区域设置 Lambda 函数是不正确的，原因与上述相同。尽管在与过境 VPC 连接的各个区域建立多个 VPC 是有效的，但该解决方案仍然需要较高的设置和维护成本。更具成本效益的选择是：Lambda@Edge 相反“配置原点以向对象添加缓存控制最大年龄指令，并指定最大年龄的最长实际值以增加 CloudFront 分布的缓存命中率”选项是不正确的，因为在这种情况下，提高 CloudFront 分配的缓存命中比率是不相关的。您可以通过增加从 CloudFront edge 缓存服务的查看器请求的比例来提高缓存性能，而不是通过原始服务器获取内容。但是，请注意，场景中的问题是全局用户的身份验证过程缓慢，而不仅仅是静态对象的缓存。该选项表示：将应用程序部署到多个 AWS 区域，以适应世界各地的用户。使用延迟路由策略设置路由 53 记录以将传入流量路由到为用户提供最佳延迟的区域是不正确的，因为尽管这可能会解决性能问题，但由于您必须将应用程序部署到多个 AWS 区域，因此此解决方案会带来显著的实施成本。请记住，该场景要求提供一种以最小成本提高应用程序性能的解决方案。

参考文献：

[https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/high_availability_origin_failover.](https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/high_availability_origin_failover.html)

html

<https://docs.aws.amazon.com/lambda/latest/dg/lambda-edge.html> 查看这些 Amazon CloudFront 和 AWS Lambda 备忘单：

<https://tutorialsdojo.com/amazon-cloudfront/> <https://tutorialsdojo.com/aws-lambda/>

Q69.一款流行的手机游戏使用 CloudFront、Lambda 和 DynamoDB 作为其后端服务。播放器数据保存在 DynamoDB 表中，静态资产由 CloudFront 分发。然而，有很多人抱怨保存和检索玩家信息需要花费大量时间。为了提高游戏性能，您可以使用哪种 AWS 服务将 DynamoDB 响应时间从毫秒减少到微秒？

- A、DynamoDB 自动缩放
- B、亚马逊松紧带
- C、AWS 设备场
- D、亚马逊 DynamoDB 加速器（DAX）

答案 D

分析：

Amazon DynamoDB 加速器（DAX）是一个完全管理、高度可用的内存缓存，可以减少 Amazon DynamoDB 的响应时间从毫秒到微秒，甚至每秒数百万个请求。

Amazon ElastiCache 是不正确的，因为尽管您可以使用 Elasticach 作为数据库缓存，但与 DynamoDB DAX 相比，它不会将 DynamoDB 响应时间从毫秒减少到微秒。

AWS 设备场是不正确的，因为这是一个应用程序测试服务，允许您在多个设备上同时测试和交互 Android、iOS 和 web 应用程序，或在设备上实时再现问题。DynamoDB 自动缩放是不正确的，因为它主要用于自动化表和全局辅助索引的容量管理。

参考文献：

<https://aws.amazon.com/dynamodb/dax> <https://aws.amazon.com/device-farm>

查看此 Amazon DynamoDB 备忘单：<https://tutorialsdojo.com/amazon-dynamodb/>

Q70.一个流行的社交网络托管在 AWS 中，使用 DynamoDB 表作为其数据库。需要实现“关注”功能，用户可以订阅特定用户的某些更新，并通过电子邮件通知。以下哪一项是您应该实施以满足需求的最合适的解决方案？

- A、使用 Kinesis 客户端库（KCL），编写一个利用 DynamoDB Streams Kinesis 适配器的应用程序，该适配器将从 DynamoDB Streams 端点获取数据。当特定用户进行更新时，使用 SNS 通过电子邮件通知订户。
- B、启用 DynamoDB 流并创建 AWS Lambda 触发器，以及包含 Lambda 函数在运行时需要的所有权限的 IAM 角色。来自流记录的数据将由 Lambda 函数处理，然后该函数将向 SNS 主题发布消息，该消息将通过电子邮件通知订户。
- C、设置 DAX 群集以访问源 DynamoDB 表。创建一个新的 DynamoDB 触发器和一个 LambdaFunction。对于用户数据中的每一次更新，触发器将向 Lambda 函数发送数据，然后该函数将使用 SNS 通过电子邮件通知订户。
- D、创建一个使用 DynamoDB Streams Kinesis 适配器的 Lambda 函数，该适配器将从 DynamoDBStreams 端点获取数据。设置一个 SNS 主题，当特定用户进行更新时，该主题将通过电子邮件通知订户。

答案 B

分析：

DynamoDB 流是关于 Amazon DynamoDB 表中项目更改的有序信息流。当您在表上启用流时，DynamoDB 将捕获关于表中数据项的每次修改的信息。

每当应用程序创建、更新或删除表中的项时，DynamoDB Streams 都会使用修改项的主键属性写入流记录。流记录包含有关对 DynamoDB 表中单个项的数据修改的信息。您可以配置流，以便流记录捕获其他信息，例如修改项的“之前”和“之后”图像。

Amazon DynamoDB 与 AWS Lambda 集成，因此您可以创建触发器——自动响应 DynamoDB 流中事件的代码片段。使用触发器，您可以构建对 DynamoDB 表中的数据修改做出反应的应用程序。

如果在表上启用 DynamoDB 流，则可以将流 ARN 与您编写的 Lambda 函数相关联。修改表中的项后，新记录立即出现在表的流中。AWS Lambda 轮询流，并在检测到新的流记录时同步调用 Lambda 函数。Lambda 函数可以执行您指定的任何操作，例如发送通知或启动工作流。

因此，该场景中的正确答案是这样的选项：启用 DynamoDB 流并创建 AWS Lambda 触发器，以及包含 Lambda 函数在运行时需要的所有权限的 IAM 角色。来自流记录的数据将由 Lambda 函数处理，然后该函数将向 SNS 主题发布消息，该消息将通过电子邮件通知订户。该选项表示：使用 Kinesis 客户端库（KCL），编写一个利用 DynamoDB Streams Kinesis 适配器的应用程序，该适配器将从 DynamoDB Streams 端点获取数据。

什么时候

有由特定用户进行的更新，使用 SNS 通过电子邮件通知订户是不正确的，因为尽管这是一个有效的解决方案，但它缺少一个重要步骤，即启用 DynamoDB 流。有了 DynamoDB Streams Kinesis 适配器，您可以通过 KCL 接口开始开发应用程序，API 调用无缝指向 DynamoDB Streams 端点。请记住，默认情况下未启用 DynamoDB 流功能。

该选项表示：创建一个使用 DynamoDB Streams Kinesis 适配器的 Lambda 函数，该适配器将从 DynamoDB Streams 端点获取数据。设置一个 SNS 主题，当特定用户进行的更新不正确时，该主题将通过电子邮件通知订阅者，因为正如上面所述，您必须先手动启用 DynamoDB 流，然后才能使用其端点。该选项表示：

设置 DAX 群集以访问源 DynamoDB 表。创建一个新的 DynamoDB 触发器和一个 Lambda 函数。对于用户数据中的每一次更新，触发器都会将数据发送到 Lambda 函数，然后通过电子邮件通知订阅者。使用 SNS 是不正确的，因为 DynamoDB 加速器（DAX）功能主要用于显著提高数据库的内存读取性能，而不是捕获项级修改的时间顺序。在这种情况下，您应该使用 DynamoDB 流。

参考文献：

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Streams.html>

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Streams.Lambda.Tutorial.html> 查看此

Amazon DynamoDB 备忘单：<https://tutorialsdojo.com/amazon-dynamodb/>

Q71. 一组 web 应用程序托管在一个跨三个可用性区域的 EC2 实例自动扩展组中，并配置了默认设置。有一个应用程序负载均衡器将请求转发到 URL 路径上的相应目标组。由于应用程序的传入流量较少，因此触发了扩展策略。

哪个 EC2 实例将是自动缩放组终止的第一个实例？

- A、从最早的启动配置启动的 EC2 实例
- B、实例将由自动缩放组随机选择
- C、具有最少用户会话数的 EC2 实例
- D、运行时间最长的 EC2 实例

答:

分析:

默认终止策略旨在帮助确保网络体系结构均匀地跨越可用性区域。使用默认终止策略，自动缩放组的行为如下:

1. 如果多个可用性区域中存在实例，请选择实例最多且至少有一个实例不受扩展保护的可用性区域。如果有多个可用性区域具有此数量的实例，请选择具有使用最早启动配置的实例的可用性区域。
2. 确定所选可用性区域中哪些未受保护的实例使用最早的启动配置。如果有一个这样的实例，请终止它。
3. 如果根据上述标准有多个实例要终止，请确定哪些未受保护的实例最接近下一个计费小时。（这有助于您最大限度地利用 EC2 实例，并管理 Amazon EC2 使用成本。）如果有一个这样的实例，请终止它。
4. 如果有多个未受保护的实例最接近下一个计费时间，请随机选择其中一个实例。

以下流程图说明了默认终止策略的工作方式:

参考文献: <https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-instance-termination.html#default-终止->

政策

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-instance-termination.html> 查看此 AWS 自动缩放备忘单:

<https://tutorialsdojo.com/aws-auto-scaling/>

Q72.金融应用程序由 EC2 实例的自动扩展组、应用程序负载均衡器和多 AZ 部署配置中的 MySQL RDS 实例组成。为了保护客户的机密数据，您必须确保只能通过身份验证令牌使用特定于 EC2 实例的配置文件凭据访问 RDS 数据库。作为公司的解决方案架构师，您应该做以下哪项来满足上述要求?

- A、创建 IAM 角色并将其分配给 EC2 实例，这将授予对 RDS 实例的独占访问权。
- B、启用 IAM DB 身份验证。
- C、在应用程序中配置 SSL 以加密与 RDS 的数据库连接。
- D、使用 IAM 和 STS 的组合来限制通过临时令牌访问 RDS 实例。

答案 B

分析:

您可以使用 AWS 身份和访问管理 (IAM) 数据库身份验证对数据库实例进行身份验证。IAM 数据库身份验证与 MySQL 和 PostgreSQL 一起工作。使用这种身份验证方法，连接到 DB 实例时不需要使用密码。而是使用身份验证令牌。

身份验证令牌是 Amazon RDS 根据请求生成的唯一字符串。身份验证令牌使用 AWS 签名版本 4 生成。每个令牌的寿命为 15 分钟。您不需要在数据库中存储用户凭据，因为身份验证是使用 IAM 在外部管理的。您还可以使用标准数据库身份验证。IAM 数据库身份验证提供了以下好处:

进出数据库的网络流量使用安全套接字层 (SSL) 加密。您可以使用 IAM 集中管理对数据库资源的访问，而不是单独管理每个 DB 实例上的访问。

对于在 Amazon EC2 上运行的应用程序，您可以使用特定于您的 EC2 实例的配置文件凭据来访问您的数据库，而不是密码，以提高安全性。因此，基于上述参考，启用 IAM DB 身份验证是正确的答案。在应用程序中配置 SSL 以加密到 RDS 的数据库连接是不正确的，因为 SSL 连接未使用来自 IAM 的身份验证令牌。尽管为应用程序配置 SSL 可以提高飞行中数据的安全性，但在这种情况下，它仍然不是一个合适的选项。

创建 IAM 角色并将其分配给 EC2 实例（这将授予对 RDS 实例的独占访问权）是不正确的，因为尽管您可以创建 IAM 并将 IAM 角色分配给 EC3 实例，但仍需要将 RDS 配置为使用 IAM DB 身份验证。使用 IAM 和 STS 的组合通过临时令牌限制对 RDS 实例的访问是不正确的，因为在这种情况下，您必须使用 IAM DB 身份验证，而不是 IAM 和 ST 的组合。虽然 STS 用于发送临时令牌进行身份验证，但这不是 RDS 的兼容用例。

参考：

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/UsingWithRDS.IAMDBAuth.html> 查看此 Amazon RDS 备忘单：<https://tutorialsdojo.com/amazon-relational-database-service-amazon-rds/>

Q73 制药公司在其内部网络和 AWS 云中托管资源。他们希望所有的软件架构师都使用存储在 Active Directory 中的本地凭证访问这两个环境中的资源。在这种情况下，以下哪项可用于满足此要求？

- A、使用 Web 身份联合设置基于 SAML 2.0 的联合。
- B、使用 Microsoft Active Directory 联合身份验证服务（AD FS）设置基于 SAML 2.0 的联合身份验证。
- C、使用亚马逊专有网络
- D、使用 IAM 用户

答案 B

分析：

由于该公司使用的是实现安全断言标记语言（SAML）的 Microsoft Active Directory，因此您可以设置基于 SAML 的联盟，以便 API 访问 AWS 云。这样，您可以使用本地网络的登录凭据轻松连接到 AWS。AWS 支持 SAML 2.0 的身份联合，这是一个开放标准，许多身份提供者（IDP）都使用它。此功能支持联合单点登录（SSO），因此用户可以登录 AWS 管理控制台或调用 AWS API，而无需为组织中的每个人创建 IAM 用户。通过使用 SAML，您可以简化使用 AWS 配置联合的过程，因为您可以使用 IdP 的服务，而不是编写自定义身份代理代码。

在使用基于 SAML 2.0 的联合（如前面的场景和图中所述）之前，必须将组织的 IdP 和 AWS 帐户配置为相互信任。以下步骤描述了配置此信任的一般过程。在组织内部，您必须拥有支持 SAML 2.0 的 IdP，如 Microsoft Active Directory 联合身份验证服务（AD FS，Windows Server 的一部分）、Shibboleth 或其他兼容的 SAML 2.0 提供程序。

因此，正确答案是：使用 Microsoft Active Directory 联合身份验证服务（AD FS）设置基于 SAML 2.0 的联合身份验证。

使用 Web 身份联合设置基于 SAML 2.0 的联合是不正确的，因为这主要用于让用户通过知名的外部身份提供商（IdP）登录，例如登录亚马逊、Facebook 和谷歌。它不使用 Active Directory。使用 IAM 用户是不正确的，因为这种情况要求您使用存储在其 Active Directory 中的现有凭据，而不是 IAM 将生成的用户帐户。

使用 Amazon VPC 是不正确的，因为这只允许您提供 AWS 云的逻辑隔离部分，您可以在定义的虚拟网络中启动 AWS 资源。这与用户身份验证或 Active Directory 无关。

参考文献：

http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_saml.htmlhttps://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers.html 查看此 AWS IAM 备忘单: <https://tutorialsdojo.com/aws-identity-and-access-management-iam/>

Q74.一家公司有 3 名 DevOps 工程师, 负责软件开发和基础设施管理流程。其中一名工程师意外删除了一个托管在 Amazon S3 中的文件, 导致服务中断。

DevOps 工程师可以做些什么来防止这种情况再次发生?

- A、 为所有用户设置签名 URL。
- B、 使用 S3 不经常访问的存储来存储数据。
- C、 创建禁用删除操作的 IAM 存储桶策略。
- D、 在存储桶上启用 S3 版本控制和多因素身份验证删除。(正确)

答案 D

分析:

为了避免意外删除 Amazon S3 bucket, 您可以:

- 启用版本控制
- 启用 MFA (多因素身份验证) 删除

版本控制是将对象的多个变体保持在同一个 bucket 中的一种方法。您可以使用版本控制来保存、检索和恢复存储在 AmazonS3 存储桶中的每个对象的每个版本。通过版本控制, 您可以轻松地从事意的用户操作和应用程序故障中恢复。如果启用了 MFA (多因素身份验证) 删除, 则需要对以下任一操作进行额外身份验证:

- 更改 bucket 的版本控制状态
- 永久删除对象版本

使用 S3 不经常访问的存储来存储数据是不正确的。将存储类切换到 S3 不频繁访问不会有助于减少意外删除。为所有用户设置签名 URL 不正确。签名 URL 使您能够更好地控制对内容的访问, 因此此功能更多地处理访问而不是删除。创建禁用删除操作的 IAM 存储桶策略不正确。如果创建阻止删除的存储桶策略, 其他用户将无法删除应删除的对象。您只想防止意外删除, 而不是禁用操作本身。

参考:

<http://docs.aws.amazon.com/AmazonS3/latest/dev/Versioning.html> 查看此 Amazon S3 备忘单:

<https://tutorialsdojo.com/amazon-s3/>

Q75.每分钟记录天气数据的应用程序部署在 Spot EC2 实例组中, 并使用 MySQL RDS 数据库实例。目前, 只有一个 RDS 实例在一个可用性区域中运行。您计划通过同步数据复制到另一个 RDS 实例来改进数据库, 以确保高可用性。

以下哪项在 RDS 中执行同步数据复制?

- A、CloudFront 作为多 AZ 部署运行
- B、DynamoDB 读取副本
- C、RDS DB 实例作为多 AZ 部署运行
- D、RDS 读取副本

答案 C

分析：

当您创建或修改 DB 实例以作为多 AZ 部署运行时，Amazon RDS 会自动在不同的可用性区域中提供并维护同步备用副本。数据库实例的更新将跨可用性区域同步复制到备用数据库，以保持两者同步，并保护最新数据库更新免受数据库实例故障的影响。RDS 读取副本不正确，因为读取副本提供异步复制而不是同步复制。

作为多 AZ 部署运行的 DynamoDB 读取副本和 CloudFront 是不正确的，因为 DynamoDB 和 CloudFront 都没有读取副本功能。

参考：<https://aws.amazon.com/rds/details/multi-az/>

亚马逊 RDS 概述：

<https://youtu.be/aZmpLl8K1UU>

查看此 Amazon RDS 备忘单：<https://tutorialsdojo.com/amazon-relational-database-service-amazon-rds/>

Q76.解决方案架构师在监控 VPC 时发现了一系列 DDoS 攻击。架构师需要加强当前的云基础设施，以保护客户的数据。以下哪种解决方案最适合缓解此类攻击？

- A、使用 AWS Shield Advanced 检测和缓解 DDoS 攻击。
- B、安全组和网络访问控制列表的组合，仅允许授权流量访问专有网络。
- C、使用 AWS WAF 设置 web 应用程序防火墙，以过滤、监视和阻止 HTTP 流量。
- D、使用 AWS 防火墙管理器，设置安全层，以防止 SYN 洪水、UDP 反射攻击和其他 DDoS 攻击。

答：

分析：

针对针对在 Amazon 弹性计算云上运行的应用程序的攻击提供更高级别的保护

（EC2）、弹性负载平衡（ELB）、Amazon CloudFront 和 Amazon Route 53 资源，您可以订阅 AWS 盾牌前进了。除了标准提供的网络和传输层保护之外，AWS Shield Advanced 还提供了针对大型复杂 DDoS 攻击的额外检测和缓解功能，对攻击的近实时可视性，以及与 AWS WAF（web 应用程序防火墙）的集成。

AWS Shield Advanced 还可让您全天候访问 AWS DDoS 响应团队（DRT），并提供针对亚马逊弹性计算云（EC2）、弹性负载平衡（ELB）、亚马逊云前端和亚马逊路由 53 收费中的 DDoS 相关峰值。因此，正确的答案是：使用 AWS Shield Advanced 检测和缓解 DDoS 攻击。“使用 AWS 防火墙管理器，设置安全层以防止 SYN 洪水、UDP 反射攻击和其他 DDoS 攻击”的选项是不正确的，因为 AWS 防火墙管理员主要用于简化多个帐户和资源的 AWS WAF 管理和维护任务。

它无法保护您的专有网络免受 DDoS 攻击。

“使用 AWS WAF 设置 web 应用程序防火墙以过滤、监视和阻止 HTTP 流量”选项不正确。尽管 AWS WAF 可以帮助您阻止 VPC 的常见攻击模式，如 SQL 注入或跨站点脚本，但这仍然不足以抵御 DDoS 攻击。在这种情况下，最好使用 AWS Shield。

该选项表示：安全组和网络访问控制列表的组合仅允许授权流量访问您的 VPC 是不正确的。虽然使用安全组和 NACL 的组合可以有效地为 VPC 提供安全，但这不足以缓解 DDoS 攻击。

您应该使用 AWS Shield 以获得更好的安全保护。

参考文献：

https://d1.awsstatic.com/whitepapers/Security/DDoS_White_Paper.pdf <https://aws.amazon.com/shield/>

查看此 AWS Shield 备忘单：

<https://tutorialsdojo.com/aws-shield/>

AWS 安全服务概述-WAF、Shield、CloudHSM、KMS：<https://www.youtube.com/watch?v=-1SRdeAmMo>

Q77.一个旅游照片共享网站正在使用 Amazon S3 向您网站的访问者提供高质量照片。几天后，你发现还有其他旅游网站链接并使用你的照片。这给您的企业造成了经济损失。

缓解此问题的最有效方法是什么？

- A、为您的照片使用 CloudFront 发行版。
- B、使用 NACL 阻止违规网站的 IP 地址。
- C、配置 S3 bucket 以删除公共读取访问，并使用带有到期日期的预签名 URL。
- D、而是在 Amazon WorkDocs 上存储和私人提供高质量照片。

答案 C

分析：

在 Amazon S3 中，默认情况下，所有对象都是私有的。只有对象所有者有权访问这些对象。但是，对象所有者可以选择使用自己的安全凭据创建预签名的 URL 来与其他人共享对象，以授予下载对象的时间限制权限。为对象创建预签名 URL 时，必须提供安全凭据、指定存储桶名称、对象密钥、指定 HTTP 方法（下载对象）以及到期日期和时间。预签名的 URL 仅在指定的持续时间内有效。任何收到预签名 URL 的人都可以访问该对象。例如，如果您的 bucket 中有一个视频，并且 bucket 和对象都是私有的，则可以通过生成预签名的 URL。

对照片使用 CloudFront 发行版是不正确的。CloudFront 是一种内容交付网络服务，可加快向客户交付内容。

使用 NACL 阻止违规网站的 IP 地址也是不正确的。使用 NACL 阻止 IP 地址不是一种非常有效的方法，因为 IP 地址的快速更改很容易绕过此配置。

相反，在 Amazon WorkDocs 上存储和私下提供高质量照片是不正确的，因为 WorkDocs 只是一个完全管理、安全的内容创建、存储和协作服务。它不是存储静态内容的合适服务。Amazon WorkDocs 更常用于轻松创建、编辑和共享文档，以进行协作，而不是像 Amazon S3 那样提供对象数据。

参考文献：

<https://docs.aws.amazon.com/AmazonS3/latest/dev/ShareObjectPreSignedURL.html>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/ObjectOperations.html> 查看此 Amazon CloudFront 备忘单:

<https://tutorialsdojo.com/amazon-cloudfront/>

S3 预签名 URL 与云前端签名 URL 与源访问标识 (OAI) <https://tutorialsdojo.com/s3-presigned-urls-vs-cloudfront-signed-urls-vs-origin-access-identity-oai/AWS> 服务备忘单比较: <https://tutorialsdojo.com/comparison-of-aws-services/>

Q78.您所在的公司具有高可用性架构，由弹性负载均衡器和几个 EC2 实例组成，配置为在三个可用性区域自动扩展。您希望基于特定的度量来监控 EC2 实例，这在 CloudWatch 中是不可用的。以下哪项是 CloudWatch 中必须手动设置的自定义度量？

- A、来自 EC2 实例的网络数据包
- B、EC2 实例的 CPU 利用率
- C、EC2 实例的磁盘读取活动
- D、EC2 实例的内存利用率

答案 D

分析:

CloudWatch 有可用的 Amazon EC2 指标供您用于监控。CPU 利用率标识在选定实例上运行应用程序所需的处理能力。网络利用率标识单个实例的传入和传出网络流量量。磁盘读取度量用于确定应用程序从实例硬盘读取的数据量。这可用于确定应用程序的速度。但是，有些指标在 CloudWatch 中不易获得，如内存利用率、磁盘空间利用率等，可以通过设置自定义指标来收集。

您需要使用用 Perl 编写的 CloudWatch 监控脚本准备一个自定义度量。您还可以安装 CloudWatch 代理，以从 Amazon EC2 实例收集更多系统级指标。

以下是您可以设置的自定义指标列表:

-内存利用率-磁盘交换利用率-硬盘空间利用率-页面文件利用率-EC2 实例的日志收集 CPU 利用率、EC2 实例中的磁盘读取活动以及 EC2 实例外的网络数据包都不正确，因为默认情况下，这些指标在 CloudWatch 中随时可用。

参考文献:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/monitoring_ec2.html

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/mon-scripts.html#using_put_script 查看此 Amazon EC2 备忘单:

<https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/>查看此 Amazon CloudWatch 备忘单:

<https://tutorialsdojo.com/amazon-cloudwatch/>

Q79.解决方案架构师需要确保只能通过 SSH 连接从该 IP 地址 (110.238.98.71) 访问按需 EC2 实例。以下哪种配置将满足此要求？

- A、安全组入站规则：协议-UDP，端口范围-22，源 238.98.71/32
- B、安全组入站规则：协议——TCP。端口范围-22，源 238.98.71/0
- C、安全组入站规则：协议——TCP。端口范围-22，源 238.98.71/32
- D、安全组入站规则：协议-UDP，端口范围-22，源 238.98.71/0

答案 C

分析：

说明安全组充当实例的虚拟防火墙，以控制入站和出站流量。在 VPC 中启动实例时，最多可以为该实例分配五个安全组。安全组在实例级别而不是子网级别执行操作。因此，可以将 VPC 子网中的每个实例分配给一组不同的安全组。要求仅允许客户端的单个 IP，而不允许整个网络。因此，应使用适当的 CIDR 符号。/32 表示一个 IP 地址，/0 表示整个网络。请注意，SSH 协议使用 TCP 和端口 22。因此，正确答案是：协议？TCP，端口范围？22，源 110.238.98.71/32 协议？UDP，端口范围？22，Source238.98.71/32 和协议？UDP，端口范围？22，Source238.98.71/0 不正确，因为它们使用 UDP。协议 TCP，端口范围？22，源 110.238.98.71/0 不正确，因为它使用了 a/0 CIDR 表示法。协议 TCP，端口范围？22，源 110.238.98.71/0 不正确，因为它允许整个网络而不是单个 IP。

参考：

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html#security-组-Dojo> 的 AWS 认证解决方案架构师协会考试学习指南的规则教程：<https://tutorialsdojo.com/aws-certified-solutions-architect-associate/>

Q80.一个政府实体正在该市进行人口和住房普查。上传到其在线门户的每个家庭信息都存储在 Amazon S3 中的加密文件中。政府指定其解决方案架构师制定合规政策，以符合其合规标准的方式验证敏感数据。如果检测到包含个人身份信息（PII）、受保护健康信息（PHI）或知识产权（IP）的受损文件，也应提醒他们。架构师应实现以下哪项以满足此需求？

- A、设置和配置 Amazon Macie，以监控和检测 Amazon S3 数据的使用模式。
- B、设置并配置 Amazon Inspector，以便在其 Amazon S3 数据上检测到安全违规时发送警报通知。
- C、设置和配置 Amazon Rekognition，以监控和识别 Amazon S3 数据上的模式。
- D、设置并配置 Amazon GuardDuty，以监控 Amazon S3 数据上的恶意活动。

答：

分析：

Amazon Macie 是一种基于 ML 的安全服务，通过自动发现、分类和保护存储在 Amazon S3 中的敏感数据，帮助您防止数据丢失。Amazon Macie 使用机器学习来识别敏感数据，如个人身份信息（PII）或知识产权，分配商业价值，并提供了数据存储位置以及在组织中如何使用这些数据的可见性。

Amazon Macie 持续监控数据访问活动的异常情况，并在检测到未经授权访问或意外数据泄漏风险时发出警报。Amazon Macie 能够检测在敏感数据上意外设置的全局访问权限，检测源代码中 API 密钥的上传，并验证敏感客户数据的存储和访问方式符合其合规标准。

因此，正确的答案是：设置和配置 AmazonMacie，以监控和检测 AmazonS3 数据的使用模式。

“设置和配置 Amazon Rekognition 以监控和识别其 Amazon S3 数据上的模式”的选项是不正确的，因为 Rekognition 只是一种服务，可以识别对象、人物、文本、场景和活动，并检测图像或视频上的任何不当内容。“设置和配置 Amazon GuardDuty 以监控其 Amazon S3 数据上的恶意活动”的选项不正确，因为 GuardDuty 只是一个威胁检测服务，持续监控恶意活动和未授权行为，以保护您的 AWS 帐户和工作负载。“设置并配置 Amazon Inspector 以在其 Amazon S3 数据上检测到安全违规时发送警报通知”的选项是不正确的，因为 Inspector 基本上是一种自动安全评估服务，有助于提高部署在 AWS 上的应用程序的安全性和合规性。

参考文献: <https://docs.aws.amazon.com/macie/latest/userguide/what-is-macie.html>

<https://aws.amazon.com/macie/faq/> <https://docs.aws.amazon.com/macie/index.html>

查看此 Amazon Macie 备忘单: <https://tutorialsdojo.com/amazon-macie/>

AWS 安全服务概述-机密管理器、ACM、Macie: <https://www.youtube.com/watch?v=ogVamzF2Dzk>

一位 IT 顾问在一家大型金融公司工作。顾问的角色是帮助开发团队使用无状态 web 服务器构建高可用性 web 应用程序。在这种情况下

AWS 服务是否适合存储会话状态数据？（选择两个。）

- A、RDS
- B、红移谱
- C、发电机
- D、冰川
- E、弹力

行政长官的答覆

分析:

DynamoDB 和 ElastiCache 是正确答案。您可以在 DynamoDB 和 ElastiCache 上存储会话状态数据。这些 AWS 服务提供高性能的键值对存储，可用于构建高可用性 web 应用程序。

红移频谱是不正确的，因为这是一种数据仓库解决方案，您可以直接从数据仓库查询数据。Redshift 不适用于存储会话状态，但更适用于分析和 OLAP 过程。

RDS 也不正确，因为这是 AWS 的关系数据库解决方案。这种关系存储类型可能不是最适合会话状态的存储类型，与 DynamoDB 相比，它可能无法以相同的成本提供所需的性能。

S3 Glacier 是不正确的，因为这是一种用于数据存档和长期备份的低成本云存储服务。Glacier 的存档和检索速度太慢，无法处理会话状态。

参考文献:

<https://aws.amazon.com/caching/database-caching/>

<https://aws.amazon.com/caching/session-management/>查看

此 Amazon ElastiCache 备忘单:

<https://tutorialsdojo.com/amazon-elasticache/>

Q82. 一家公司有一个 web 应用程序，它使用 Windows Server 的 Internet 信息服务 (IIS)。文件共享用于将应用程序数据存储在公司内部数据中心的网络连接存储器上。为了实现高可用性系统，他们计划将应用程序和文件共享迁移到 AWS。

以下哪项可用于满足此要求？

- A、将现有文件共享配置迁移到 AWS 存储网关。
- B、将现有文件共享配置迁移到 Amazon FSx for Windows 文件服务器。
- C、将现有文件共享配置迁移到 Amazon EFS。
- D、将现有文件共享配置迁移到 Amazon EBS。

答案 B

分析:

Amazon FSx for Windows 文件服务器提供完全受管理的 Microsoft Windows 文件服务器，由完全本机 Windows 文件系统支持。Amazon FSx for Windows 文件服务器具有功能、性能和兼容性，可以轻松将企业应用程序提升并转移到 AWS 云。它可以从 Windows、Linux 和 macOS 计算实例和设备访问。数千个计算实例和设备可以同时访问文件系统。

在这种情况下，您需要将现有的文件共享配置迁移到云。在给出的选项中，最好的答案是 Amazon FSx。文件共享是文件系统上的特定文件夹，包括文件夹的子文件夹，您可以通过 SMB 协议访问这些文件夹。要从本地文件系统迁移文件共享配置，必须先将文件迁移到 Amazon FSx，然后再迁移文件共享的配置。因此，正确的答案是：将现有的文件共享配置迁移到 Amazon FSx for Windows 文件服务器。

“将现有文件共享配置迁移到 AWS Storage Gateway”选项不正确，因为 AWS Storage Gateway 主要用于将本地网络集成到 AWS，但不用于迁移应用程序。在存储网关中使用文件共享意味着您仍将保留本地系统，而不是完全迁移它。

“将现有文件共享配置迁移到 Amazon EFS”的选项是不正确的，因为在该场景中，公司使用的是在 Windows 服务器上运行的文件共享。请记住，Amazon EFS 仅支持 Linux 工作负载。

“将现有文件共享配置迁移到 Amazon EBS”选项不正确，因为 EBS 主要用作 EC2 实例的块存储，而不是共享文件系统。文件共享是文件系统中可以使用服务器消息块 (SMB) 协议访问的特定文件夹。Amazon EBS 不支持 SMB 协议。

参考文献:

<https://aws.amazon.com/fsx/windows/faqs/>

<https://docs.aws.amazon.com/fsx/latest/WindowsGuide/migrate-file-share-config-to-fsx.html> 查看此亚马逊 FSx 备忘单：<https://tutorialsdojo.com/amazon-fsx/>

Q83. 一家公司计划将其内部工作负载迁移到 AWS。当前体系结构由使用 Windows 共享文件存储的 Microsoft SharePoint 服务器组成。解决方案架构师需要使用高可用性的云存储解决方案，并可以与 Active Directory 集成以进行访问控制和身份验证。

以下哪个选项可以满足给定要求？

- A、使用 AWS 存储网关创建网络文件系统（NFS）文件共享。
- B、使用 Amazon FSx for Windows 文件服务器创建文件系统，并将其加入 AWS 中的 Active Directory 域。
- C、启动 Amazon EC2 Windows 服务器，将新的 S3 存储桶作为文件卷装入。
- D、使用 Amazon EFS 创建文件系统并将其加入 Active Directory 域。

答案 B

分析：

Amazon FSx for Windows 文件服务器提供完全管理、高度可靠和可扩展的文件存储，可通过行业标准服务消息块（SMB）协议访问。它构建在 Windows Server 上，提供了广泛的管理功能，如用户配额、最终用户文件还原和 Microsoft Active Directory（AD）集成。可以从 Windows、Linux 和 MacOS 计算实例和设备访问 Amazon FSx。数千个计算实例和设备可以同时访问文件系统。

Amazon FSx 与 Microsoft Active Directory 协作，以与现有的 Microsoft Windows 环境集成。您有两个选项为文件系统提供用户身份验证和访问控制：

AWS 管理 Microsoft Active Directory 和自我管理的 Microsoft Active Directory。请注意，为文件系统创建 Active Directory 配置后，无法更改该配置。但是，您可以从备份创建新的文件系统，并更改该文件系统的 Active Directory 集成配置。这些配置允许域中的用户使用其现有身份访问 Amazon FSx 文件系统，并控制对单个文件和文件夹的访问。

因此，正确的答案是：使用 Amazon FSx for Windows 文件服务器创建文件系统，并将其加入 AWS 中的 Active Directory 域。

“使用 Amazon EFS 创建文件系统并将其加入 Active Directory 域”选项不正确，因为 Amazon EFS 不支持 Windows 系统，仅支持 Linux 操作系统。您应该使用 Amazon FSx for Windows 文件服务器来满足场景中的要求。“启动 Amazon EC2 Windows 服务器以将新的 S3 存储桶作为文件卷装载”选项不正确，因为您无法将 Amazon S3 与现有的 Active Directory 集成以提供身份验证和访问控制。

“使用 AWS 存储网关创建网络文件系统（NFS）文件共享”选项不正确，因为 NFS 文件共享主要用于 Linux 系统。请记住，场景中的要求是使用 Windows 共享文件存储。因此，您必须使用 SMB 文件共享，它支持 Windows 操作系统和 Active Directory 配置。或者，您也可以使用 Amazon FSx for Windows 文件服务器文件系统。

参考文献：

<https://docs.aws.amazon.com/fsx/latest/WindowsGuide/aws-ad-integration-fsxW.html>
<https://aws.amazon.com/fsx/windows/faqs/>

Q84.一家媒体公司有一个亚马逊 ECS 集群，它使用 Fargate 启动类型来托管其新闻网站。应使用环境变量提供数据库凭证，以符合严格的安全合规性。作为解决方案架构师，您必须确保凭证是安全的，并且不能在集群本身上以明文形式查看凭证。

以下哪项是本场景中最合适的解决方案，您可以用最少的努力实现？

A、在 ECS 集群的 ECS 任务定义文件中，使用 Docker Secrets 存储数据库凭证，以集中管理这些敏感数据，并仅将其安全传输到需要访问的容器。机密在传输和静止期间被加密。只有通过 IAM 角色被授予显式访问权限的服务才能访问给定的机密，并且只能在这些服务任务运行时访问。

B、使用 AWS 系统管理器参数存储保存数据库凭证，然后使用 AWSKMS 对其进行加密。为您的 Amazon ECS 任务执行角色（taskRoleArn）创建 IAM 角色，并在任务定义中引用该角色，该任务定义允许访问 KMS 和参数存储。

在容器定义中，使用

C、要在容器中设置的环境变量和 Systems Manager 参数存储参数的完整 ARN，其中包含要呈现给容器的敏感数据。

D、C.将数据库凭证存储在 ECS 集群的 ECS 任务定义文件中，并使用 KMS 进行加密。将任务定义 JSON 文件存储在私有 S3 存储桶中，并确保在存储桶上启用 HTTPS 以加密传输中的数据。为 ECS 任务定义脚本创建一个 IAM 角色，允许访问特定的 S3 存储桶，然后在调用 ECS 注册任务定义时传递--cli input json 参数。参考 S3 bucket 中包含数据库凭证的任务定义 JSON 文件。

E、D.使用 AWS 机密管理器存储数据库凭证，然后使用 AWS KMS 对其进行加密。为您的 Amazon ECS 任务执行角色（taskRoleArn）创建基于源的策略，并将其与您的任务定义一起引用，该任务定义允许访问 KMS 和 AWS Secrets Manager。

在容器定义中，使用要在容器中设置的环境变量的名称和要呈现给容器的机密管理器机密（包含敏感数据）的完整 ARN 指定机密。

答案 B

分析：

通过将敏感数据存储在 AWS Secrets Manager Secrets 或 AWS Systems Manager 参数存储参数中，然后在容器定义中引用这些参数，Amazon ECS 使您能够将敏感数据注入容器。使用 EC2 和 Fargate 启动类型的任务都支持此功能。

秘密可以通过以下方式暴露给容器：

- 要将敏感数据作为环境变量注入容器，请使用 secrets 容器定义参数。
- 要在容器的日志配置中引用敏感信息，请使用 secretOptions 容器定义参数。

在容器定义中，使用要在容器中设置的环境变量的名称以及包含要呈现给容器的敏感数据的 secrets Manager secret 或 Systems Manager 参数 Store 参数的完整 ARN 指定 secrets。您引用的参数可以是

来自与使用它的容器不同的区域，但必须来自同一帐户。因此，正确的答案是这样的选项：使用 AWS Systems Manager 参数存储保存数据库凭证，然后使用 AWS KMS 对其进行加密。为您的 Amazon ECS 任务执行角色

(taskRoleArn) 创建 IAM 角色，并在任务定义中引用该角色，该任务定义允许访问 KMS 和参数存储。在容器定义中，使用要在容器中设置的环境变量的名称和包含要呈现给容器的敏感数据的 Systems Manager 参数存储参数的完整 ARN 指定机密。该选项表示：在 ECS 集群的 ECS 任务定义文件中，使用 Docker Secrets 存储数据库凭据，以集中管理这些敏感数据，并仅将其安全传输到需要访问的容器。机密在传输和静止期间被加密。只有通过 IAM 角色被授予显式访问权限的服务才能访问给定的机密，并且只有当这些服务任务正在运行时才是不正确的。虽然您可以使用 Docker Secrets 保护敏感数据库凭据，但此功能仅适用于 Docker Swarm。在 AWS 中，建议使用机密管理器或系统管理器参数存储来保护敏感数据。该选项表示：将数据库凭据存储在 ECS 集群的 ECS 任务定义文件中，并使用 KMS 进行加密。将任务定义 JSON 文件存储在私有 S3 存储桶中，并确保在存储桶上启用 HTTPS 以加密传输中的数据。为 ECS 任务定义脚本创建一个 IAM 角色，允许访问特定的 S3 存储桶，然后在调用 ECS 注册任务定义时传递--cli input json 参数。引用 S3 存储桶中包含数据库凭据的任务定义 JSON 文件不正确。虽然解决方案可能有效，但不建议在 S3 中存储敏感凭据。这需要大量开销和手动配置步骤，只需使用 Secrets Manager 或 Systems Manager 参数存储即可简化这些步骤。该选项表示：使用 AWS 机密管理器存储数据库凭据，然后使用 AWS KMS 对其进行加密。为您的 Amazon ECS 任务执行角色 (taskRoleArn) 创建基于资源的策略，并将其与您的任务定义一起引用，该任务定义允许访问 KMS 和 AWS Secrets Manager。在容器定义中，使用要在容器中设置的环境变量的名称和要呈现给容器的机密管理器机密 (包含敏感数据) 的完整 ARN 指定机密是不正确的。尽管使用 Secrets Manager 保护 ECS 中的敏感数据是有效的，但 Amazon ECS 不支持基于资源的策略。基于资源的策略的一个示例是 S3 桶策略。ECS 任务承担执行角色 (IAM 角色)，以便能够代表您调用其他 AWS 服务，如 AWS Secrets Manager。

参考文献：

<https://docs.aws.amazon.com/AmazonECS/latest/developerguide/specifying-sensitive-data.html>

<https://aws.amazon.com/blogs/mt/the-right-way-to-store-secrets-using-parameter-store/>查看这些亚马逊 ECS 和 AWS 系统管理器备忘单：<https://tutorialsdojo.com/amazon-elastic-container-service-amazon-ecs/>

<https://tutorialsdojo.com/aws-系统经理/>

Q85.公司需要部署至少 2 个 EC2 实例以支持其应用程序的正常工作负载，并自动扩展到 6 个 EC2 实例以处理峰值负载。体系结构在处理任务关键型工作负载时必须具有高可用性和容错性。作为公司的解决方案架构师，您应该如何满足上述要求？

- A、创建 EC2 实例的自动扩展组，并将最小容量设置为 2，最大容量设置为 6。使用 2 个可用性区域并为每个 AZ 部署 1 个实例。
- B、创建 EC2 实例的自动扩展组，并将最小容量设置为 2，最大容量设置为 4。在可用性区域 A 部署 2 个实例，在可用性区 B 部署 2 个
- C、创建 EC2 实例的自动扩展组，并将最小容量设置为 2，最大容量设置为 6。在可用性区域 A 中部署 4 个实例。
- D、创建 EC2 实例的自动伸缩组，并将最小容量设置为 4，最大容量设置为 6。在可用性区域 A 中部署 2 个实例，在可用性区 B 中部署另外 2 个实例

答案 D

分析：

AmazonEC2 自动伸缩有助于确保您拥有正确数量的 AmazonEc2 实例来处理应用程序的负载。创建 EC2 实例的集合，称为自动伸缩组。您可以指定每个自动伸缩组中的最小实例数，Amazon EC2 自动伸缩确保您的组不会低于此大小。您还可以指定每个自动伸缩组中的最大实例数，Amazon EC2 自动伸缩确保您的组不会超过此大小。

要为应用程序实现高可用性和容错体系结构，必须将所有实例部署到不同的可用性区域。这将帮助您在发生停机时隔离资源。请注意，要实现容错，您需要有冗余资源，以避免在服务器故障或可用性区域中断的情况下出现任何系统降级。拥有容错体系结构需要运行比通常需要的更多资源的额外成本。这是为了确保任务关键型工作负载得到处理。

由于该场景需要至少 2 个实例来处理常规流量，因此即使发生 AZ 中断，也应该有 2 个实例始终运行。您可以使用自动缩放组跨两个或多个可用性区域自动缩放计算资源。您必须将最小容量指定为 4 个实例，并且

最大容量为 6 个实例。如果每个 AZ 有 2 个实例在运行，即使 AZ 出现故障，您的系统仍将至少运行 2 个实例。

因此，此场景中的正确答案是：创建 EC2 实例的自动扩展组，并将最小容量设置为 4，最大容量设置为 6。在可用性区域 A 中部署 2 个实例，在可用性区 B 中部署另外 2 个实例。

该选项表示：创建 EC2 实例的自动扩展组，并将最小容量设置为 2，最大容量设置为 6。在可用性区域 A 中部署 4 个实例是不正确的，因为这些实例仅部署在单个可用性区域中。它无法保护您的应用程序和数据免受数据中心或 AZ 故障的影响。

该选项表示：创建 EC2 实例的自动扩展组，并将最小容量设置为 2，最大容量设置为 6。使用 2 个可用性区域并为每个 AZ 部署 1 个实例是不正确的。需要始终运行 2 个实例。如果发生 AZ 中断，ASG 将在未受影响的 AZ 上启动新实例。这种配置不会立即发生，这意味着在一段时间内，只剩下一个正在运行的实例。该选项表示：创建一个 EC2 实例的自动扩展组，并将最小容量设置为 2，最大容量设置为 4。在可用性区域 A 中部署 2 个实例，在可用性区 B 中部署两个实例是不正确的。尽管这满足了至少 2 个 EC2 实例和高可用性的要求，但最大容量设置是错误的。应将其设置为 6，以正确处理峰值负载。如果发生 AZ 中断并且系统处于峰值负载，则此设置中运行的实例数将仅为 4 而不是 6，这将影响应用程序的性能。

Q86.Docker 应用程序在负载均衡器后面的 Amazon ECS 集群上运行，大量使用 DynamoDB。我们指示您通过均匀地分配工作负载和有效地使用配置的吞吐量来提高数据库性能。

您会考虑为您的 DynamoDB 表实现以下哪项？

- A、使用具有低基数属性的分区键，每个项有几个不同的值。
- B、减少 DynamoDB 表中的分区键数。
- C、使用具有高基数属性的分区键，每个项具有大量不同的值。
- D、避免使用由分区键和排序键组成的复合主键。

答案 C

分析：

表主键的分区键部分确定存储表数据的逻辑分区。这又会影响底层物理分区。为表配置的 I/O 容量在这些物理分区之间平均分配。因此，不均匀分布 I/O 请求的分区键设计可能会创建“热”分区，从而导致节流并低效地使

用所配置的 I/O 容量。表的配置吞吐量的最佳使用不仅取决于单个项的工作负载模式，还取决于分区键设计。这并不意味着您必须访问所有分区键值以实现高效的吞吐量级别，甚至访问的分区键值的百分比必须很高。这确实意味着您的工作负载访问的分区键值越明显，这些请求在分区空间中的分布就越多。通常，随着访问的分区键值与分区键值总数之比的增加，您将更有效地使用配置的吞吐量。

这方面的一个例子是使用具有高基数属性的分区键，每个项都有大量不同的值。

减少 DynamoDB 表中分区键的数量是不正确的。与其这样做，您实际上应该添加更多内容来提高其性能，以便均匀分布 I/O 请求，而不是避免“热”分区。

使用具有低基数属性的分区键是不正确的，因为这与正确答案正好相反，每个项都有几个不同的值。请记住，您的工作负载访问的分区键值越明显，这些请求在分区空间中的分布就越多。相反，分区键值越不明显，它在分区空间中的分布就越不均匀，这实际上会降低性能。“避免使用由分区键和排序键组成的复合主键”选项是不正确的，因为如上所述，复合主键将为表提供更多分区，从而提高性能。因此，应该使用而不是避免。

参考文献：

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/bp-partition-key-uniform-load.html>

<https://aws.amazon.com/blogs/database/choosing-the-right-dynamodb-partition-key/>查看此 Amazon DynamoDB 备忘单：

<https://tutorialsdojo.com/amazon-dynamodb/>

亚马逊 DynamoDB 概述：<https://www.youtube.com/watch?v=3ZOyUNleorU>

Q87.组织需要为新的 Amazon EC2 实例提供持久块存储卷，以将数据从其内部网络迁移到 AWS。存储卷所需的最大性能为 64000 IOPS。

在这种情况下，以下哪项可用于满足此要求？

- A、启动 Amazon EFS 文件系统，并将其安装到基于 Nitro 的 Amazon EC2 实例，并将 `performancemode` 设置为最大 I/O。
- B、在 EC2 实例中直接连接多个实例存储卷，以提供最大 IOPS 性能。
- C、启动基于 Nitro 的 EC2 实例，并以 64000 IOPS 连接配置的 IOPS SSD EBS 卷（`io1`）。
- D、启动任何类型的 Amazon EC2 实例，并以 64000 IOPS 连接配置的 IOPS SSD EBS 卷（`io1`）。

答案 C

分析：

Amazon EBS 卷是一个持久的块级存储设备，可以连接到实例。将卷附加到实例后，可以像使用物理硬盘一样使用它。EBS 卷是灵活的。

AWS Nitro 系统是最新一代 EC2 实例的底层平台，使 AWS 能够更快地创新，进一步降低客户成本，并提供更多的好处，如增加安全性和新实例类型。

Amazon EBS 是一个持久块存储卷。它可以独立于实例的生命周期而持续。由于该场景要求您拥有一个高达 64000 IOPS 的 EBS 卷，因此必须启动一个基于 Nitro 的 EC2 实例。

因此，此场景中的正确答案是：启动一个基于 Nitro 的 EC2 实例，并连接一个具有 64000 IOPS 的配置 IOPS SSD EBS 卷（`io1`）。

表示：在 EC2 实例中直接连接多个实例存储卷以提供最大 IOPS 性能的选项不正确。尽管实例存储是块存储卷，但它不是持久性的，如果实例从停止状态重新启动，数据将消失（请注意，这与操作系统级重新启动不同。在操作系统级重启中，数据仍会在实例存储中保留）。实例存储仅为实例提供临时块级存储。这意味着，如果基础磁盘驱动器发生故障、实例停止以及实例终止，实例存储中的数据可能会丢失。该选项表示：启动 Amazon EFS 文件系统并将其安装到基于 Nitro 的 Amazon EC2 实例，并将性能模式设置为最大 I/O，这是不正确的。尽管 Amazon EFS 可以提供超过 64000 IOPS，但该解决方案使用的是文件系统，而不是块存储卷，这是场景中要求的。

表示：启动 EC2 实例并以 64000 IOPS 连接 io1 EBS 卷的选项不正确。为了实现配置 IOPS SSD 的 64000 IOPS，您必须配置基于 Nitro 的 EC2 实例。只有在 Nitro 系统上构建的实例的 IOPS 和吞吐量超过 32000 IOPS 时，才能保证最大 IOPS 和吞吐率。其他实例仅保证高达 32000 IOPS。

参考文献：

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volume-types.html#EBSVolumeTypes_piops

<https://aws.amazon.com/s3/storage-classes/> <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/instance-types.html> 查看此亚马逊 EBS 备忘单：

<https://tutorialsdojo.com/amazon-ebs/亚马逊 S3>

vs EFS vs EBS 备忘单：

<https://tutorialsdojo.com/amazon-s3-vs-ebs-vs-efs/>

Q88.解决方案架构师设计了一个无服务器架构，允许 AWS Lambda 访问美国东部（北弗吉尼亚州）地区名为 tutorialsdojo 的 Amazon DynamoDB 表。附加到 Lambda 函数的 IAM 策略允许它在表中放置和删除项目。必须更新策略以仅允许 tutorialsdojo 表中的两个操作，并防止修改其他 DynamoDB 表。以下哪项 IAM 政策符合此要求并遵循授予最低特权的原则？

A.

```
{ "Version": "2012-18-17"声明* [ [ "sid":  
    "TutorialsdojoTablePolicy1",  
    "效果": "允许",  
    "行动": [  
        "dynamodb:PutItem",  
        "dynamodb:删除 ITEM"] 东-  
1:1286189812061898:tab1/tutorialsdojo"资源":  
    "arn:aws:dynamodb:us-  
    }  
    [  
    "sid": "TutorialsdojoTablePolicy2",  
    "效果": "允许",  
    "动作": "dynamodb:",
```

```
“资源”: “arn:aws:dynamodb:us-east-1:1206189812061898:table/tutorialsdojo”
]]}

B。

{“版本”: “2012-10-17”,

“声明”: [

*“Sid”: “TutorialsdojoTablePolicy”,

“效果”: “允许”,

“行动”: [

“DYNAMODBPUTITEM”“dynamodb:删除 LTEM”

]“资源”: “arn:aws:dynamodb:us-east-1:120618981206:table/tutorialsdojo”}}}C。

“版本”: “2012-10-17”,

“5 声明”: [

“sia”: “TutorialsdojoTablePolicy”,

“效果”: “允许”,

*行动: [

“dynamodb:PutItem”,

“dynamodb:删除项”

]

“资源”: “arn:aws:dynamodb:us-east-1:120618981206:table/”D。

版本: “2012-10-17。

“声明”: [“sid”: “Tutorialsdojotablepolicy1”,

“效果”: “允许”, “操作”:

[adom (dynamodb:PutItem”,

“dynamodb:Deleteltem”

]“资源”: “arn:aws:dynamodb:us-east-1:1206189812861898:t1e/tutorialsdoio”

}“Sid”: “TutorialsdojotablePolicy2”,

“效果”: “拒绝”,
```

“操作”: “dynamodb:*”, “资源”阿尼奥斯: 发电机 B:us-east-

1:1206189812061898: 表/**

答案 B

分析:

每个 AWS 资源都由 AWS 帐户拥有, 创建或访问资源的权限由权限策略控制。帐户管理员可以将权限策略附加到 IAM 标识 (即用户、组和角色), 某些服务 (如 AWS Lambda) 也支持将权限策略添加到资源。

在 DynamoDB 中, 主要资源是表。DynamoDB 还支持其他资源类型、索引和流。但是, 您只能在现有 DynamoDB 表的上下文中创建索引和流。这些被称为子资源。这些资源和子资源具有与之关联的唯一亚马逊资源名称 (ARN)。

例如, AWS 帐户 (123456789012) 在美国东部 (北弗吉尼亚州) (useast-1) 地区有一个名为 Books 的 DynamoDB 表。图书表的 ARN 为:

arn:aws:dynamodb:us-east-1:123456789012: 表格/书籍

策略是附加到标识或资源时定义其权限的实体。通过使用 IAM 策略和角色来控制访问, 它将授予 Lambda 函数访问 DynamoDB 表的权限。在该场景中, 声明将使用 Lambda 函数修改名为 tutorialsdojo 的 DynamoDB 表。由于只需要访问一个表, 因此需要在 IAM 策略的资源元素中指明该表。此外, 必须指定将在策略中生成的效果和操作元素。

因此, 这种情况下的正确答案是:

```
{
  "版本": "2012-10-17", "声明": [
    { "Sid":
      "TutorialsdojoTablePolicy",
      "效果": "允许",
      "行动": [
        "dynamodb:PutItem""dynamodb>DeleteI
tem"
      ], "资源": "arn:aws:dynamodb:us-east-1:120618981206:table/tutorialsdojo"}
  ]
}
```

下面的 IAM 策略不正确，因为该场景仅要求您允许 tutorialsdojo 表中的权限。在该策略中使用通配符：table/* 将允许 Lambda 函数修改您帐户中的所有 DynamoDB 表。

```
{
{
  "版本": "2012-10-17", "声明": [
    {
      "Sid": "TutorialsdojoTablePolicy",
      "效果": "允许",
      "行动": [
        "dynamodb:PutItem" "dynamodb>DeleteI
tem"
      ], "资源": "arn:aws:dynamodb:us-east-1:120618981206:table/*"
    }
  ]
}
```

下面的 IAM 策略不正确。第一条语句正确地允许对 tutorialsdojo DynamoDB 表执行 PUT 和 DELETE 操作。但是，第二个语句与第一个语句相反，因为它允许 tutorialsdojo 表中的所有 DynamoDB 操作。

```
{
  "版本": "2012-10-17", "声明": [
    { "Sid":
      "TutorialsdojoTablePolicy1",
      "效果": "允许",
      "Action": ["dynamodb:PutItem", "dynamodb>DeleteItem"], "Resource":
        "arn:aws:dynamoda:us-east-1:1206189812061898:table/tutorialsdojo"},
    { "Sid":
      "TutorialsdojoTablePolicy2",
      "效果": "允许",
      "行动": "dynamodb:*", "资源": "arn:aws:dynamodb:us-east-
1:1206189812061898:table/tutorialsdojo"
    }
  ]
}
```

下面的 IAM 策略不正确。与前面的选项一样，该策略的第一条语句正确地允许对 tutorialsdojo DynamoDB 表执行 PUT 和 DELETE 操作。然而，第二个声明与第一个声明相反，因为它否认了 DynamoDB 的所有动作。因此，此策略不允许对 AWS 帐户的所有 DynamoDB 表执行任何操作。

```
{ "Version": "2012-10-17", "Statement": [

  { "Sid":

    "TutorialsdojoTablePolicy1",

    "Effect": "Allow",

    "Action": [

      "dynamodb:PutItem", "dynamodb:DeleteI

tem"

    ], "Resource": "arn:aws:dynamodb:us-east-1:1206189812061898:table/tutorialsdojo" },

  { "Sid":

    "TutorialsdojoTablePolicy2",

    "Effect": "Deny",

    "Action": "dynamodb:*", "Resource": "arn:aws:dynamodb:us-east-

1:1206189812061898:table/*" }

]
```

Q89.公司要求存储在云中的所有数据在静止时进行加密。为了方便地与其他 AWS 服务集成，他们必须完全控制创建密钥的加密，并能够立即从 AWS KMS 中删除密钥材料。该解决方案还应能够独立于 AWS CloudTrail 审计密钥使用情况。

以下哪个选项将满足此要求？

- A、 使用 AWS 密钥管理服务在自定义密钥存储中创建 CMK，并将不可提取的密钥材料存储在 AmazonS3 中。
- B、 使用 AWS 密钥管理服务创建 AWS 拥有的 CMK，并在 AWS CloudHSM 中存储不可提取的密钥材料。
- C、 使用 AWS 密钥管理服务创建 AWS 管理的 CMK，并在 AWS CloudHSM 中存储不可提取的密钥材料。
- D、 使用 AWS 密钥管理服务在自定义密钥存储中创建 CMK，并将不可提取的密钥材料存储在 AWS CloudHSM 中。

答案 D

分析：

AWS 密钥管理服务（KMS）自定义密钥存储功能将 AWS CloudHSM 提供的控件与 AWS KMS 的集成和易用性结合起来。您可以配置自己的 CloudHSM 集群，并授权 AWS KMS 将其用作密钥的专用密钥存储，而不是默认

的 AWS KMS 密钥存储。在 AWS KMS 中创建密钥时，可以选择在 CloudHSM 集群中生成密钥材料。在自定义密钥存储中生成的 CMK 永远不会以明文形式离开 CloudHSM 集群中的 HSM，所有使用这些密钥的 AWS KMS 操作仅在 HSM 中执行。

AWS KMS 可以帮助您与其他 AWS 服务集成，以加密存储在这些服务中的数据，并控制对解密数据的密钥的访问。要立即从 AWS KMS 中删除密钥材料，可以使用自定义密钥存储。请注意，每个自定义密钥存储都与 AWS 帐户中的 AWS CloudHSM 集群关联。因此，当您在自定义密钥存储中创建 AWS KMS CMK 时，AWS KMS 会为您拥有和管理的 AWS CloudHSM 集群中的 CMK 生成并存储不可提取的密钥材料。如果您希望能够独立于 AWS KMS 或 AWS CloudTrail 审核所有密钥的使用情况，这也非常适合。由于您控制 AWS CloudHSM 集群，因此您可以选择独立于 AWS KMS 管理 CMK 的生命周期。您可能会发现自定义密钥存储有用的原因有四个：

您可能在单个租户 HSM 或您直接控制的 HSM 中保护的密钥。

您可能需要将密钥存储在已验证为 FIPS 140-2 第 3 级的 HSM 中（标准 AWS KMS 密钥存储中使用的 HSM 已验证或正在验证为第 2 级，并在多个类别中验证为第 3 级）。您可能需要能够立即从 AWS KMS 中删除关键材料，并通过独立的方式证明您已经这样做了。您可能需要能够独立于 AWS KMS 或 AWS CloudTrail 审核密钥的所有使用。

因此，该场景中的正确答案是：使用 AWS 密钥管理服务在自定义密钥存储中创建 CMK，并将不可提取的密钥材料存储在 AWS CloudHSM 中。“使用 AWS 密钥管理服务在自定义密钥存储中创建 CMK 并将不可提取的密钥材料存储在 Amazon S3 中”的选项是不正确的，因为 Amazon S3 不是用于存储加密密钥的合适存储服务。您必须改用 AWS CloudHSM。

使用 AWS 密钥管理服务创建 AWS 拥有的 CMK 并在 AWS CloudHSM 中存储不可提取的密钥材料，以及使用 AWS 密钥管理服务创建 AWS 管理的 CMK 和在 AWS 云 HSM 中保存不可提取密钥材料的选项都是不正确的，因为场景要求您对创建的密钥的加密拥有完全控制权。AWS 拥有的 CMK 和 AWS 管理的 CMK 由 AWS 管理。

此外，这些选项不允许您独立于 AWS CloudTrail 审核密钥使用情况。

参考文献：

<https://docs.aws.amazon.com/kms/latest/developerguide/custom-key-store-overview.html>

<https://aws.amazon.com/kms/faqs/>

<https://aws.amazon.com/blogs/security/are-kms-custom-key-stores-right-for-you/>查看 AWS KMS 备忘单：

<https://tutorialsdojo.com/aws-key-management-service-aws-kms/>

Q90. 托管在 EC2 中的应用程序使用来自 SQS 队列的消息，并与 SNS 集成，以在流程完成后向您发送电子邮件。运营团队收到了 5 份订单，但几个小时后，他们在收件箱中看到了 20 封电子邮件通知。

以下哪项可能是该问题的罪魁祸首？

- A、web 应用程序在处理完 SQS 队列中的消息后，不会删除这些消息。
- B、web 应用程序设置为长轮询，因此消息发送两次。
- C、web 应用程序无权使用 SQS 队列中的消息。
- D、web 应用程序设置为短轮询，因此某些消息不会被拾取

答：

分析：

始终记住，SQS 队列中的消息将继续存在，即使 EC2 实例处理了它，直到您删除该消息。您必须确保在处理后删除消息，以防止可见性超时过期后再次接收和处理消息。

分布式消息传递系统中有三个主要部分：

1. 分布式系统的组件（EC2 实例）
2. 您的队列（分布在 Amazon SQS 服务器上）
3. 队列中的消息。

您可以设置一个系统，该系统具有多个组件，这些组件向队列发送消息并从队列接收消息。队列冗余地跨多个 Amazon SQS 服务器存储消息。

请参阅 SQS 消息生命周期的第三步：

组件 1 将消息 A 发送到队列，消息冗余地分布在 Amazon SQS 服务器上。

当组件 2 准备好处理消息时，它使用队列中的消息，消息 a

返回。在处理消息 A 时，它将保留在队列中，并且在可见性超时期间不会返回到后续接收请求。组件 2 从队列中删除消息 A，以防止在可见性超时到期后再次接收和处理消息。

该选项表示：web 应用程序设置为长轮询，因此消息发送两次是不正确的，因为长轮询通过消除空响应（当没有消息可用于 ReceiveMessage 请求时）和假空响应（消息可用但不包含在响应中）的数量，有助于降低使用 SQS 的成本。在配置了长轮询的 SQS 队列中发送两次消息的可能性很小。

该选项表示：web 应用程序设置为短轮询，因此某些消息不会被拾取，这是不正确的，因为您正在接收来自 SNS 的电子邮件，其中消息肯定正在处理。在这种情况下，未收到的邮件不会导致 20 封邮件发送到您的收件箱。

表示：web 应用程序没有权限使用 SQS 队列中的消息的选项是不正确的，因为没有正确的权限会导致不同的响应。该场景表示消息被正确处理，但发送了 20 多条消息，所以访问队列并没有问题。参考文献：

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-message-生命周期>。

[htmlhttps://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-basic-建筑学](https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-basic-建筑学) html

查看此亚马逊 SQS 备忘单：<https://tutorialsdojo.com/amazon-sqs/>

Q91.解决方案架构师需要建立关系数据库，并制定灾难恢复计划，以缓解多区域故障。该解决方案需要 1 秒的恢复点目标（RPO）和小于 1 分钟的恢复时间目标（RTO）。

以下哪项 AWS 服务可以满足此要求？

- A、AWS 全球加速器
- B、亚马逊极光全球数据库
- C、具有跨区域读取副本的 Amazon RDS for PostgreSQL
- D、Amazon DynamoDB 全局表

答案 B

分析：

亚马逊极光全球数据库是为全球分布式应用程序设计的，允许单个亚马逊极光数据库跨越多个 AWS 区域。它可以复制您的数据，而不会影响数据库性能，在每个区域以低延迟实现快速本地读取，并提供区域范围内停机的灾难恢复。

Aurora 全局数据库支持延迟小于 1 秒的基于存储的复制。如果发生计划外停机，您分配的辅助区域之一可以升级为读写

在不到 1 分钟内实现功能。此功能称为跨区域灾难恢复。1 秒的 RPO 和不到 1 分钟的 RTO 为您的全球业务连续性计划提供了坚实的基础。

因此，正确答案是：亚马逊极光全球数据库。Amazon DynamoDB 全局表是不正确的，因为在场景中，解决方案架构师需要创建关系数据库，而不是 NoSQL 数据库。创建 DynamoDB 全局表时，它由多个副本表组成（每个 AWS 区域一个副本表），DynamoDB 将其视为单个单元。

具有跨区域读取副本的多 AZ Amazon RDS 数据库不正确，因为多 AZ 部署仅适用于单个区域，而不适用于多区域设置。此数据库设置无法提供 1 秒的 RPO 和小于 1 分钟的 RTO。此外，跨区域 RDS 读取副本的复制速度不如 Amazon Aurora 全局数据库。AWS 全球加速器是不正确的，因为这是一种简化流量管理并提高应用程序性能的网络服务。AWS 全局加速器不是关系数据库服务；因此，在这种情况下，这不是一个合适的服务。

参考文献：

<https://aws.amazon.com/rds/aurora/global-database/>

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-global-database.html> 亚马逊极光概

述：<https://youtu.be/iwS1h7rLNBQ>

查看此亚马逊极光备忘单：<https://tutorialsdojo.com/amazon-aurora/>

Q92.解决方案架构师正在 Amazon S3 bucket 中托管一个名为 tutorialsdojo 的网站。用户使用以下 URL 加载网站：<http://tutorialsdojo.s3-website-us-east-1.amazonaws.com> 还有一个新的要求是在网页上添加 JavaScript，以便通过使用 Amazon S3 API 端点（tutorialsdojo.s3.amazonaws.com）对同一个 bucket 发出经过身份验证的 HTTP GET 请求。测试时，您注意到 web 浏览器阻止 JavaScript 允许这些请求。以下哪一个选项是您应该为该场景实施的最合适的解决方案？

- A、启用跨区域复制（CRR）。
- B、在存储桶中启用跨源资源共享（CORS）配置。
- C、启用跨帐户访问。
- D、启用跨区域负载均衡。

答案 B

分析：

？

跨源资源共享（CORS）为加载在一个域中的客户端 web 应用程序定义了一种与不同域中的资源交互的方法。通过 CORS 支持，您可以使用 Amazon 构建丰富的客户端 web 应用程序

S3 并有选择地允许跨源访问您的 Amazon S3 资源。假设您在 Amazon S3 bucket 中托管一个名为“您的网站”的网站，用户加载该网站端点 <http://your-website.s3-website-useast-1.amazonaws.com>。现在，您希望在存储在此存储桶中的网页上使用 JavaScript，以便能够通过使用存储桶的 Amazon S3 API 端点（your-website.s3.amazonaws.com）对同一存储桶发出经过身份验证的 GET 和 PUT 请求。浏览器通常会阻止 JavaScript 允许这些请求，但使用 CORS，您可以配置您的 bucket 以显式启用来自网站的跨源请求。s3-website-us-east-1.amazonaws.com。

在这个场景中，您可以通过在 S3 bucket 中启用 COR 来解决这个问题。因此，在 bucket 中启用跨源资源共享（CORS）配置是正确答案。启用跨帐户访问不正确，因为跨帐户访问是 IAM 中的一项功能，而不是 Amazon S3 中的功能。启用跨区域负载均衡不正确，原因是跨区域负载均衡仅用于 ELB，而不适用于 S3。

启用跨区域复制（CRR）是不正确的，因为 CRR 是一种桶级配置，可以跨不同 AWS 区域中的桶自动异步复制对象。

参考文献：

<http://docs.aws.amazon.com/AmazonS3/latest/dev/cors.html>

<http://docs.aws.amazon.com/AmazonS3/latest/dev/ManageCorsUsing.html>

Q93. 托管在内部数据中心的多层应用程序计划迁移到 AWS。该应用程序有一个 MessageBroker 服务，它使用行业标准的消息传递 API 和协议，这些 API 和协议也必须迁移，而无需重写应用程序中的消息传递代码。以下哪项服务最适合您将消息服务移动到 AWS？

- A、 亚马逊社交网站
- B、 亚马逊 MQ
- C、 亚马逊主权财富基金
- D、 亚马逊 SQS

答案 B

分析：

Amazon MQ、Amazon SQS 和 Amazon SNS 是适用于从初创企业到企业的任何人的消息服务。如果您正在将消息传递与现有应用程序一起使用，并且希望快速轻松地将消息传递服务移动到云中，建议您考虑使用 Amazon MQ。它支持行业标准 API 和协议，因此您可以从任何基于标准的 MessageBroker 切换到 Amazon MQ，而无需在应用程序中重写消息传递代码。因此，Amazon MQ 是正确答案。

如果您正在云上构建全新的应用程序，那么强烈建议您考虑 Amazon SQS 和 Amazon SNS。Amazon SQS 和 SNS 是轻量级的、完全管理的消息队列和

主题服务几乎可以无限扩展，并提供简单易用的 API。您可以使用 Amazon SQS 和 SNS 来分离和扩展微服务、分布式系统和无服务器应用程序，并提高可靠性。

Amazon SQS 是不正确的，因为尽管这是一个完全受管理的消息队列服务，但与 Amazon MQ 不同，它不支持广泛的行业标准消息传递 API 和协议列表。此外，使用 Amazon SQS 需要对应用程序的消息传递代码进行额外更改，以使其兼容。

Amazon SNS 是不正确的，因为 SNS 更适合作为发布/订阅消息服务，而不是消息代理服务。

Amazon SWF 是不正确的，因为这是一个完全管理的状态跟踪和任务协调服务，而不是消息服务，与 Amazon MQ、AmazonSQS 和 Amazon SNS 不同。

参考文献：

<https://aws.amazon.com/amazon-mq/faqs/>

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/welcome.html#sqs-与-amazon-mq-sns-的区别>

查看此 Amazon MQ 备忘单：<https://tutorialsdojo.com/amazon-mq/Q94.一家>

公司在其 VPC 中托管多个应用程序。在监控系统时，他们注意到多个端

口扫描来自一个特定的 IP 地址块，该地址块试图连接到其 VPC 内的几

个 AWS 资源。内部安全团队要求在未来 24 小时内拒绝所有违规 IP 地址，

以确保安全。

以下哪种方法是快速临时拒绝指定 IP 地址访问的最佳方法？

A、在 EC2 实例的操作系统中配置防火墙，以拒绝来自 IP 地址块的访问。

B、在 EC2 实例的安全组中添加一条规则，以拒绝来自 IP 地址块的访问。

C、修改与 VPC 中所有公共子网关联的网络访问控制列表，以拒绝来自 IP 地址块的访问。

D、在 IAM 中创建策略以拒绝从 IP 地址块访问。

答案 C

分析：

要控制进出 VPC 网络的流量，可以使用网络访问控制列表（ACL）。它是 VPC 的可选安全层，用作控制进入一个或多个子网的流量的防火墙。这是其他选项中最好的解决方案，因为您可以在几分钟内轻松添加和删除限制。

在 IAM 中创建策略以拒绝来自 IP 地址块的访问是不正确的，因为 IAM 策略不控制 VPC 的入站和出站流量。

在 EC2 实例的安全组中添加规则以拒绝来自 IP 地址块的访问是不正确的。虽然安全组充当防火墙，但它仅在实例级别控制入站和出站流量，而不是在整个 VPC 上。

在 EC2 实例的操作系统中配置防火墙以拒绝来自 IP 地址块的访问是不正确的，因为在 EC2 示例的底层操作系统中添加防火墙是不够的；攻击者可以连接到其他 AWS 资源，因为网络访问控制列表仍然允许他们这样做。

参考：

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_ACLs.html 亚马逊专有网络概述：

<https://www.youtube.com/watch?v=oIDHKeNxvQQ>

查看此亚马逊 VPC 备忘单：<https://tutorialsdojo.com/amazon-vpc/>

Q95. 外汇交易平台，经常每分钟处理和存储全球金融数据，托管在您的内部数据中心，并使用 Oracle 数据库。由于其数据中心最近出现冷却问题，该公司迫切需要将其基础设施迁移到 AWS，以提高其应用程序的性能。作为解决方案架构师，您负责确保数据库正确迁移，并且在将来数据库服务器出现故障时保持可用。以下哪种解决方案最适合满足要求？

- A、使用多 AZ 部署在 RDS 中创建 Oracle 数据库。
- B、在 RDS 中启动 Oracle Real Application Clusters (RAC)。
- C、在启用了恢复管理器 (RMAN) 的 RDS 中启动 Oracle 数据库实例。
- D、使用 AWS 模式转换工具和 AWS 数据库迁移服务转换数据库模式。使用单个实例将 Oracle 数据库迁移到非集群 Amazon Aurora。

答:

分析:

Amazon RDS 多 AZ 部署为数据库 (DB) 实例提供了增强的可用性和耐用性，使它们自然适合生产数据库工作负载。提供多 AZ 数据库实例时，Amazon RDS 会自动创建主数据库实例，并将数据同步复制到不同可用性区域 (AZ) 中的备用实例。每个 AZ 都运行在其物理上不同的独立基础设施上，并设计为高度可靠。如果基础设施出现故障，Amazon RDS 将自动故障切换到备用 (或在 Amazon Aurora 的情况下切换到读取副本)，以便在故障切换完成后立即恢复数据库操作。由于 DB 实例的端点在故障转移后保持不变，因此应用程序可以恢复数据库操作，而无需手动管理干预。在这种情况下，要使用的最佳 RDS 配置是多 AZ 部署的 RDS 中的 Oracle 数据库，以确保高可用性，即使主数据库实例发生故障。因此，在多 AZ 部署的 RDS 中创建 Oracle 数据库是正确答案。

在启用了恢复管理器 (RMAN) 的 RDS 中启动 Oracle 数据库实例和在 RDS 中启动 Oracle Real Application Clusters (RAC) 是不正确的，因为 RDS 中不支持 Oracle RMAN 和 RAC。

选项表示：使用 AWS 模式转换工具和 AWS 数据库迁移服务转换数据库模式。使用单个实例将 Oracle 数据库迁移到非集群 Amazon Aurora 是不正确的，因为尽管此解决方案可行，但将 Oracle 数据库移植到 Aurora 需要时间，这是不可接受的。基于此选项，Aurora 数据库仅使用单个实例，没有读取副本，并且未配置为 Amazon Aurora DB 集群，这可能会提高数据库的可用性。

参考文献:

<https://aws.amazon.com/rds/details/multi-az/>

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZ.html> 查看此 Amazon RDS 备忘

单: <https://tutorialsdojo.com/amazon-relational-database-service-amazon-rds/>

Q96. 应用程序托管在 AWS Fargate 集群中，每当对象加载到 Amazon S3 bucket 上时，该集群就会运行批处理作业。ECS 任务的最小数量最初设置为 1，以节省成本，并且只会根据 S3 bucket 上传的新对象增加任务数量。处理完成后，bucket 变为空，ECS 任务计数应回到 1。哪一个选项最适合以最少的工作量实现？

- A、在 CloudWatch 中设置警报以监控 CloudTrail，因为 S3 对象级操作记录在云迹。创建两个用于增加/减少 ECS 任务计数的 Lambda 函数。根据 S3 事件，将这些设置为 CloudWatch 警报的相应目标。
- B、设置 CloudWatch 事件规则以检测 S3 对象放置操作，并将目标设置为 Lambda 函数，该函数将运行 Amazon ECS API 命令以增加 ECS 上的任务数量。创建另一个规则来检测 S3 删除操作，并运行 Lambda 函数以减少 ECS 任务的数量。

C、设置 CloudWatch 事件规则以检测 S3 对象放置操作，并将目标设置为任务数量增加的 ECS 集群。创建另一个规则来检测 S3 删除操作，并将目标设置为 ECS 集群，任务计数为 1。

D、在 CloudWatch 中设置警报以监控 CloudTrail，因为此 S3 对象级操作记录在 CloudTrail 上。根据 S3 事件，设置两个报警动作以更新 ECS 任务计数，以扩展/扩展。

答案 C

分析：

当某些 AWS 事件发生时，您可以使用 CloudWatch 事件来运行 Amazon ECS 任务。您可以设置一个 CloudWatch 事件规则，每当使用 Amazon S3 PUT 操作将文件上传到某个 Amazon S3Bucket 时，该规则将运行 Amazon ECS 任务。每当使用删除操作删除 S3 存储桶上的文件时，您还可以声明减少数量的 ECS 任务。首先，您必须为 S3 服务创建一个 CloudWatch 事件规则，以监视对象级操作？放置和删除对象。对于对象级操作，需要首先创建 CloudTrail 轨迹。在目标部分，选择“ECS 任务”，并输入所需的值，如集群名称、任务定义和任务计数。您需要两条规则吗？一个用于扩展，另一个用于缩减 ECS 任务计数。

因此，正确的答案是：设置 CloudWatch 事件规则以检测 S3 对象放置操作，并将目标设置为任务数量增加的 ECS 集群。创建另一个规则来检测 S3 删除操作，并将目标设置为 ECS 集群，任务计数为 1。该选项表示：设置 CloudWatch 事件规则以检测 S3 对象放置操作，并将目标设置为 Lambda 函数，该函数将运行 Amazon ECS API 命令以增加 ECS 上的任务数。创建另一个规则来检测 S3 删除操作，并运行 Lambda 函数以减少 ECS 任务的数量。这是不正确的。尽管此解决方案满足要求，但为此创建您自己的 Lambda 函数

这种情况其实并不必要。直接将 ECS 任务控制为 CloudWatch 事件规则的目标要简单得多。请注意，该场景要求最容易实现的解决方案。选项表示：在 CloudWatch 中设置警报以监控 CloudTrail，因为 S3 对象级操作记录在 CloudTrail 上。创建两个用于增加/减少 ECS 任务计数的 Lambda 函数。根据 S3 事件将这些设置为 CloudWatch 警报的相应目标是不正确的，因为使用 CloudTrail、CloudWatch Alarm 和两个 Lambda 函数会给您想要实现的目标带来不必要的复杂性。创建新规则时，CloudWatch 事件可以直接针对目标部分中的 ECS 任务。

选项表示：在 CloudWatch 中设置警报以监控 CloudTrail，因为此 S3 对象级操作记录在 CloudTrail 上。根据 S3 事件设置两个警报动作以将 ECS 任务计数更新为扩展/扩展不正确，因为您无法直接设置 CloudWatch 警报以更新 ECS 任务数。您必须改用 CloudWatch 事件。

参考文献：

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/events/CloudWatch-Events-tutorial-ECS.html>

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/events/Create-CloudWatch-Events-Rule.html> 查看此 Amazon CloudWatch 备忘单：

<https://tutorialsdojo.com/amazon-cloudwatch/>

Amazon CloudWatch 概览：

<https://www.youtube.com/watch?v=q0DmxfyGkeU>

Q97.在您工作的政府机构中，您被指派将机密税务文件放到 AWS 云上。然而，从安全的角度来看，有一个问题是什么可以穿上

AWS。AWS 中有哪些功能可以确保机密文档的数据安全？（选择二）

A、公共数据集卷加密

B、S3 本地数据加密

- C、S3 服务器端加密
- D、EBS 内部数据加密
- E、S3 客户端加密

行政长官的答覆

分析：

您可以通过加密保护 AWS 中数据的隐私，无论是在静止还是传输中。如果您的数据存储在 EBS 卷中，则可以启用 EBS 加密；如果数据存储在 Amazon S3 中，则可启用客户端和服务端加密。

公共数据集卷加密不正确，因为公共数据集设计为可公开访问。开始-本地数据加密和 S3 本地数据加密都是不正确的，因为 S3 和 EBS 不存在本地数据加密，因为这些服务位于 AWS 云中，而不是您的本地网络。

参考文献：

<https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingEncryption.html>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html><https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/使用公共数据集.html> 查看此 Amazon EC2 备忘单：<https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/> 查看此 Amazon S3 备忘单：<https://tutorialsdojo.com/amazon-s3/>

Q98.由亚马逊 EC2 托管的汽车经销商网站在亚马逊极光数据库中存储汽车列表

由亚马逊 RDS。一旦车辆售出，其数据必须从当前列表中删除，并转发至分布式处理系统。

以下哪个选项可以满足给定要求？

- A、创建 RDS 事件订阅并将通知发送到 AWS Lambda。配置 Lambda 函数，将事件通知扇出到多个 Amazon SQS 队列，以更新处理系统。
- B、创建 RDS 事件订阅并将通知发送到 Amazon SNS。配置 SNS 主题以将事件通知扇出到多个 Amazon SQS 队列。使用 Lambda 函数处理数据。
- C、创建调用 Lambda 函数的本机函数或存储过程。配置 Lambda 函数，将事件通知发送到 Amazon SQS 队列，供处理系统使用。
- D、创建 RDS 事件订阅并将通知发送到 Amazon SQS。配置 SQS 队列以将事件通知扇出到多个 Amazon SNS 主题。使用 Lambda 函数处理数据。

答案 C

分析：

您可以使用本机函数或存储过程从 Amazon Aurora MySQL 兼容版 DB 集群调用 AWS Lambda 函数。当您希望将运行在 Aurora MySQL 上的数据库与其他 AWS 服务集成时，这种方法非常有用。例如，您可能希望在数据库中修改表中的行时捕获数据更改。在这种情况下，只要从数据库中删除列表，就可以触发 Lambda 函数。然后，您可以编写函数的逻辑，将列表数据发送到 SQS 队列，并让不同的进程使用它。

因此，正确的答案是：创建调用 Lambda 函数的本机函数或存储过程。配置 Lambda 函数，将事件通知发送到 Amazon SQS 队列，供处理系统使用。

RDS 事件仅提供操作事件，如数据库实例事件、数据库参数组事件、数据库安全组事件和数据库快照事件。在该场景中，我们需要捕获数据修改事件（插入、删除、更新），这可以通过本机函数或存储过程实现。

因此，以下选项不正确：

- 创建 RDS 事件订阅并将通知发送到 Amazon SQS。配置 SQS 队列以将事件通知扇出到多个 Amazon SNS 主题。使用 Lambda 函数处理数据。
- 创建 RDS 事件订阅并将通知发送到 AWS Lambda。配置 Lambda 函数，将事件通知扇出到多个 Amazon SQS 队列，以更新处理系统。
- 创建 RDS 事件订阅并将通知发送到 Amazon SNS。配置 SNS 主题以将事件通知扇出到多个 Amazon SQS 队列。使用 Lambda 函数处理数据。

参考文献：

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL.Integrating.Lambda.html>

<https://aws.amazon.com/blogs/database/capturing-data-changes-in-amazon-aurora-using-aws-lambda/> 亚马逊极光概述：<https://youtu.be/iwS1h7rLNBQ>

查看此亚马逊极光备忘单：<https://tutorialsdojo.com/amazon-aurora/>

Q99.组织需要一个用于关键任务工作负载的持久块存储卷。备份数据将存储在对象存储服务中，30 天后，数据将存储到数据存档存储服务中。

您应该如何满足上述要求？

- A、在 EC2 实例中附加 EBS 卷。使用 Amazon S3 存储备份数据，并配置 lifecyclepolicy 将对象转换到 Amazon S3One Zone IA。
- B、在 EC2 实例中附加 EBS 卷。使用 Amazon S3 存储备份数据，并配置 lifecyclepolicy 将对象转换到 Amazon S3Glacier。
- C、在 EC2 实例中附加实例存储卷。使用 Amazon S3 存储备份数据，并配置 lifecycle 策略将对象转换到 Amazon S3One Zone IA。
- D、在现有 EC2 实例中附加实例存储卷。使用 Amazon S3 存储备份数据，并配置生命周期策略以将对象转换到 Amazon S3Glacier。

答案 B

分析：

Amazon 弹性块存储（EBS）是一种易于使用的高性能块存储服务，旨在与 Amazon 弹性计算云（EC2）一起使用，用于任何规模的吞吐量和事务密集型工作负载。广泛的工作负载，如关系和非关系数据库、企业应用程序、容器化应用程序、大数据分析引擎、文件系统和媒体工作流广泛部署在 Amazon EBS 上。

Amazon 简单存储服务（Amazon S3）是一种对象存储服务，提供业界领先的可扩展性、数据可用性、安全性和性能。这意味着所有规模和行业的客户都可以使用它来存储和保护一系列用例的任何数量的数据，如网站、移

动应用程序、备份和恢复、存档、企业应用程序、物联网设备和大数据分析。在 S3 生命周期配置中，您可以定义将对象从一个存储类转换到另一个存储类别的规则，以节省存储成本。Amazon S3 支持在存储类之间转换的瀑布模型，如下图所示：

在这个场景中，需要三个服务来实现这个解决方案。任务关键型工作负载意味着您需要一个持久块存储卷，为此设计的服务是 Amazon EBS 卷。第二个工作负载需要有一个对象存储服务，比如 Amazon S3，来存储备份数据。Amazon S3 使您能够将生命周期策略从 S3 标准配置到不同的存储类。对于最后一个，它需要存档存储，如 Amazon S3 Glacier。因此，此场景中的正确答案是：在 EC2 实例中附加一个 EBS 卷。使用 Amazon S3 存储备份数据，并配置生命周期策略以将对象转换到 Amazon S3 Glacier。该选项表示：在 EC2 实例中连接 EBS 卷。使用 Amazon S3 存储备份数据并配置生命周期策略以将对象转换到 Amazon S3 One Zone IA 是不正确的，因为此生命周期策略会将对象转换为不经常访问的存储类，而不是用于数据存档的存储类。

该选项表示：在现有 EC2 实例中附加实例存储卷。使用 Amazon S3 存储备份数据并配置生命周期策略以将对象转换到 Amazon S3 Glacier 是不正确的，因为实例存储卷只是 EC2 实例的临时块级存储。此外，在启动实例后，不能将实例存储卷附加到实例。只能在启动实例时为实例指定实例存储卷。该选项表示：在 EC2 实例中附加实例存储卷。使用 Amazon S3 存储备份数据并配置生命周期策略以将对象转换到 Amazon S3 One Zone-IA 不正确。与前面的选项一样，实例存储卷的使用不适用于任务关键型工作负载，因为如果底层磁盘驱动器发生故障、实例停止或实例终止，数据可能会丢失。此外，Amazon S3 Glacier 是一个更适合数据存档的选项，而不是 Amazon S3 One Zone IA。

参考文献：

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AmazonEBS.html> <https://aws.amazon.com/s3/storage-classes/>

查看此 Amazon S3 备忘单：<https://tutorialsdojo.com/amazon-s3/>

Dojo 的 AWS 存储服务备忘单教程：<https://tutorialsdojo.com/aws-cheat-sheets-storage-services/>

Q100.一位解决方案架构师正在为一家公司工作，该公司在不同的 AWS 区域拥有多个 VPC。架构师被指派建立一个日志记录系统，该系统将跟踪所有地区对 AWS 资源的所有更改，包括 IAM、CloudFront、AWS WAF 和 Route 53 中的配置。为了满足合规要求，解决方案必须确保日志数据的安全性、完整性和耐久性。它还应提供 AWS 管理控制台和 AWS CLI 中所有 API 调用的事件历史记录。

以下哪种解决方案最适合此场景？

A、使用 AWS CLI 在新的 S3 存储桶中设置新的 CloudTrail 跟踪，并传递--is 多区域跟踪和--include 全局服务事件参数，然后使用 KMS 加密对日志文件进行加密。

对 S3 存储桶应用多因素身份验证（MFA）删除，并通过配置存储桶策略确保只有授权用户才能访问日志。

B、使用 CloudTrail 控制台在新的 S3 bucket 中设置新的 CloudWatch trail，并传递--is-multi-region trail 参数，然后使用 KMS 加密来加密日志文件。对 S3 存储桶应用多因素身份验证（MFA）删除，并通过配置存储桶策略确保只有授权用户才能访问日志。

C、使用 AWS CLI 在新的 S3 存储桶中设置新的 CloudWatch trail，并传递--is multi-region trailand--include 全局服务事件参数，然后使用 KMS 加密对日志文件进行加密。

对 S3 存储桶应用多因素身份验证（MFA）删除，并通过配置存储桶策略确保只有授权用户才能访问日志。

D、使用 AWS CLI 在新的 S3 存储桶中设置新的 CloudTrail trail，并传递--is multi-region trailand--no include global service events 参数，然后使用 KMS 加密对日志文件进行加密。对 S3 存储桶应用多因素身份验证（MFA）删除，并通过配置存储桶策略确保只有授权用户才能访问日志。

答:

分析:

CloudTrail 中的事件是 AWS 帐户中活动的记录。此活动可以是可由 CloudTrail 监控的用户、角色或服务执行的操作。CloudTrail 事件提供了通过 AWS 管理控制台、AWS SDK、命令行工具和其他 AWS 服务进行的 API 和非 API 帐户活动的历史记录。有两种类型的事件可以记录在 CloudTrail 中:

管理事件和数据事件。默认情况下,跟踪日志管理事件,但不跟踪数据事件。轨迹可以应用于所有区域或单个区域。作为最佳实践,创建一条适用于 AWS 分区中您正在工作的所有区域的路径。这是在 CloudTrail 控制台中创建跟踪时的默认设置。

对于大多数服务,事件记录在操作发生的区域。对于全球服务,如 AWS 身份和访问管理(IAM)、AWS STS、Amazon CloudFront 和 Route 53,事件将发送到包括全球服务的任何跟踪,并记录为发生在美国东部(N.Virginia)地区。

在这种情况下,公司需要一个安全持久的日志记录解决方案,该解决方案将跟踪所有地区所有 AWS 资源的所有活动。在启用多区域跟踪的情况下,CloudTrail 可用于此情况,但是,它将仅涵盖区域服务(EC2、S3、RDS 等)的活动,而不适用于 IAM、CloudFront、AWS WAF 和 Route 53 等全球服务。为了满足要求,您必须在 AWS CLI 命令中添加--include global service events 参数。该选项表示:使用 AWS CLI 在新的 S3 存储桶中设置新的 CloudTrail trail,并同时传递--is multi-region trail 和--include global service events 参数,然后使用 KMS 加密对日志文件进行加密。在 S3 存储桶上应用多因素身份验证(MFA)删除,并确保只有授权用户可以通过配置存储桶策略来访问日志。这是正确的,因为它为您的日志数据提供了安全性、完整性和耐久性。此外,它还启用了--include-global service events 参数,该参数还将包括来自全局服务的活动,如 IAM、路由 53、, AWS WAF 和 CloudFront。

该选项表示:使用 AWS CLI 在新的 S3 存储桶中设置新的 CloudWatch 跟踪,并传递--is multi region 跟踪和--include 全局服务事件参数,然后使用 KMS 加密对日志文件进行加密。在 S3 存储桶上应用多因素身份验证(MFA)删除并确保只有授权用户可以通过配置存储桶策略访问日志是不正确的,因为您需要使用 CloudTrail 而不是 CloudWatch。

该选项表示:使用 CloudTrail 控制台在新的 S3 存储桶中设置新的 CloudWatch 跟踪,并传递--is 多区域跟踪参数,然后使用 KMS 加密对日志文件进行加密。在 S3 存储桶上应用多因素身份验证(MFA)删除并确保只有授权用户可以通过配置存储桶策略访问日志是不正确的,因为您需要使用 CloudTrail 而不是 CloudWatch。此外,此设置中还缺少--include 全局服务事件参数。该选项表示:使用 AWS CLI 在新的 S3 存储桶中设置新的 CloudTrail trail,并同时传递--is multi-region trail 和--no include global service events 参数,然后使用 KMS 加密对日志文件进行加密。在 S3 存储桶上应用多因素身份验证(MFA)删除并确保只有授权用户可以通过配置存储桶策略访问日志。这是不正确的,因为--is 多区域跟踪是不够的,因为您还需要添加--include global-service events 参数,而不是--no include 全局服务事件。参考文献:

<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-concepts.html#cloudtrail-概念-global-service 事件>

<http://docs.aws.amazon.com/IAM/latest/UserGuide/cloudtrail-integration.html>

<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-create-and-update-a-trail-by-using--awscli.html>

查看此 AWS CloudTrail 备忘单: <https://tutorialsdojo.com/aws-cloudtrail/>

Q101.一个在线购物平台托管在 Spot EC2 实例的自动缩放组上,并使用亚马逊极光 PostgreSQL 作为其数据库。需要优化集群中的数据库工作负载,您必须将生产流量的写入操作定向到高容量实例,并将内部员工发送的报告查询指向低容量实例。哪种配置最适合您的应用程序以及您的 Aurora 数据库集群来实现这一要求?

A、在应用程序中,使用 Aurora 数据库的实例端点来处理传入的生产流量,并使用集群端点来处理报告查询。

B、将应用程序配置为在生产流量和报告查询中使用阅读器端点，这将使您的 Aurora 数据库能够在所有 Aurora 副本之间自动执行负载平衡。

C、因为默认情况下，Aurora 将自动将生产流量引导到高容量实例，并将报告查询引导到低容量实例。

D、根据生产流量的指定标准在 Aurora 中创建自定义端点，并创建另一个自定义端点来处理报告查询。

答案 D

分析：

对的：

Amazon Aurora 通常涉及一个数据库实例集群，而不是单个实例。每个连接都由特定的 DB 实例处理。连接到 Aurora 集群时，指定的主机名和端口指向称为端点的中间处理程序。Aurora 使用端点机制来抽象这些连接。因此，当某些 DB 实例不可用时，您不必硬编码所有主机名，也不必编写自己的负载平衡和重新路由连接逻辑。对于某些 Aurora 任务，不同的实例或实例组执行不同的角色。例如，主实例处理所有数据定义语言（DDL）和数据操作语言（DML）语句。多达 15 个 Aurora 副本处理只读查询流量。使用端点，您可以根据您的用例将每个连接映射到适当的实例或实例组。例如，要执行 DDL 语句，可以连接到主实例。要执行查询，您可以连接到读卡器端点，Aurora 会自动在所有 Aurora 副本之间执行负载平衡。对于具有不同容量或配置的数据库实例的集群，可以连接到与数据库实例的不同子集关联的自定义端点。对于诊断或调优，您可以连接到特定实例端点，以检查特定 DB 实例的详细信息。

自定义端点基于 DB 实例的只读或读写能力以外的标准提供负载平衡的数据库连接。例如，您可以定义一个自定义端点，以连接到使用特定 AWS 实例类或特定 DB 参数组的实例。那你呢

可能会告诉特定用户组有关此自定义端点的信息。例如，您可以将内部用户引导到低容量实例以生成报告或进行临时（一次性）查询，并将生产流量引导到高容量实例。因此，根据生产流量的指定标准在 Aurora 中创建一个定制端点，并使用另一个自定义端点来处理报告查询是正确的答案。

将应用程序配置为在生产流量和报告查询中使用读取器端点，这将使您的 Aurora 数据库能够在所有 Aurora 副本之间自动执行负载平衡，这是不正确的，因为尽管读取器端点确实使您的 Aurora 数据库能在所有 Aurora 副本之间自动进行负载平衡，它仅限于执行读操作。您仍然需要使用自定义端点来根据指定的条件负载平衡数据库连接。

在您的应用程序中，使用 Aurora 数据库的实例端点来处理传入的生产流量，并使用集群端点来处理报告查询的选项是不正确的，因为 Aurora DB 集群的集群端点（也称为编写器端点）仅连接到该 DB 集群的当前主 DB 实例。此端点可以在数据库中执行写操作，如 DDL 语句，这非常适合处理生产流量，但不适合处理用于报告的查询，因为不会发送写数据库操作。此外，端点并不根据需求指向低容量或高容量实例。更好的解决方案是使用自定义端点。

默认情况下，Aurora 会自动将生产流量定向到高容量实例，而向低容量实例报告查询的选项是不正确的，因为默认情况下 Aurora 不会这样做。您必须创建自定义端点才能满足此要求。

参考：

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Overview.Endpoints.html> 亚马逊极光概述：

<https://youtu.be/iwS1h7rLNBQ>

查看此亚马逊极光备忘单：<https://tutorialsdodo.com/amazon-aurora/>

Q102. 一家公司正在使用 Amazon S3 存储频繁访问的数据。创建或删除对象时，S3 bucket 将向 Amazon SQS 队列发送事件通知。解决方案架构师需要创建一个解决方案，该解决方案将通知开发和操作团队已创建或删除的对象。

以下哪一项符合此要求？

- A、 为其他团队创建新的 Amazon SNS FIFO 主题。授予 Amazon S3 向第二个 SNS 主题发送通知的权限。
- B、 为其他团队设置另一个 Amazon SQS 队列。授予 Amazon S3 向第二个 SQS 队列发送通知的权限。
- C、 设置一个 Amazon SNS 主题并配置两个 Amazon SQS 队列以轮询 SNS 主题。

授予 Amazon S3 向 Amazon SNS 发送通知的权限，并更新 bucket 以使用新的 SNS 主题。

- D、 创建一个 Amazon SNS 主题，并配置两个 Amazon SQS 队列以订阅该主题。授予 Amazon S3 向 Amazon SNS 发送通知的权限，并更新 bucket 以使用新的 SNS 主题。

答案 D

分析：

AmazonS3 通知功能允许您在 bucket 中发生某些事件时接收通知。要启用通知，您必须首先添加一个通知配置，以标识您希望 Amazon S3 发布的事件以及您希望 Amazon S3 发送通知的目的地。将此配置存储在与 bucket 关联的通知子资源中。Amazon S3 支持以下可以发布事件的目的地：

- 亚马逊简单通知服务（Amazon SNS）主题
- Amazon 简单队列服务（Amazon SQS）队列
- AWSλ

在 Amazon SNS 中，扇出场景是将发布到 SNS 主题的消息复制并推送到多个端点，如 Amazon SQS 队列、HTTP（S）端点和 Lambda 函数。这允许并行异步处理。

例如，您可以开发一个应用程序，该应用程序在产品下订单时向 SNS 主题发布消息。然后，订阅 SNS 主题的 SQS 队列将收到新订单的相同通知。连接到其中一个 SQS 队列的 Amazon 弹性计算云（Amazon EC2）服务器实例可以处理订单的处理或履行。您可以将另一个 AmazonEC2 服务器实例连接到数据仓库，以分析收到的所有订单。根据给定场景，现有设置将事件通知发送到 SQS 队列。由于您需要向开发和运营团队发送通知，因此可以使用 Amazon SNS 和 SQS 的组合。通过使用消息扇出模式，您可以创建一个主题，并使用两个 Amazon SQS 队列订阅该主题。如果 Amazon SNS 收到事件通知，它将向两个订户发布消息。

请注意，Amazon S3 事件通知被设计为至少发送一次，并且只发送到一个目的地。不能为 S3 事件通知附加两个或多个 SNS 主题或 SQS 队列。因此，您必须向 Amazon SNS 发送事件通知。因此，正确的答案是：创建一个 Amazon SNS 主题并配置两个 Amazon SQS 队列以订阅该主题。授予 Amazon S3 向 Amazon SNS 发送通知的权限，并更新 bucket 以使用新的 SNS 主题。

该选项表示：为其他团队设置另一个 Amazon SQS 队列。授予 Amazon S3 向第二个 SQS 队列发送通知的权限是不正确的，因为您一次只能为 AmazonS3 事件通知添加 1 个 SQS 或 SNS。如果您需要将事件发送给多个订阅者，则应使用 Amazon SNS 和 Amazon SQS 实现消息扇出模式。选项是：为其他团队创建一个新的 Amazon SNS FIFO 主题。授予 Amazon S3 向第二个 SNS 主题发送通知的权限不正确。正如前面的选项中提到的，您一次只能为 Amazon S3 事件通知添加 1 个 SQ 或 SNS。此外，在这种情况下，Amazon SNS FIFO 主题和 Amazon SQS FIFO 队列都不适用。它们可以一起使用，以提供严格的消息排序和消息重复数据消除。每个服务的 FIFO 功能共同作用，作为一个完全受管理的服务，集成需要近实时数据一致性的分布式应用程序。

该选项表示：设置一个 Amazon SNS 主题并配置两个 Amazon SQS 队列以轮询 SNS 主题。授予 Amazon S3 向 Amazon SNS 发送通知并更新 bucket 以使用新 SNS 主题的权限是不正确的，因为您无法轮询 Amazon SNS。您应该将每个 Amazon SQS 队列配置为订阅 SNS 主题，而不是将队列配置为轮询 Amazon SNS。

参考文献：

<https://docs.aws.amazon.com/AmazonS3/latest/dev/ways-to-add-notification-config-to-bucket.html>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/NotificationHowTo.html#notification-如何概述>

<https://docs.aws.amazon.com/sns/latest/dg/welcome.html>

查看此 Amazon S3 备忘单：<https://tutorialsdojo.com/amazon-s3/>

亚马逊 SNS 概述：<https://www.youtube.com/watch?v=ft5R45IEUJ8>

Q103. 一家公司计划在其内部企业门户网站的专用子网中启动亚马逊 EC2 实例。出于安全目的，EC2 实例必须通过不通过公共互联网的私有端点向 Amazon DynamoDB 和 Amazon S3 发送数据。

以下哪项可以满足上述要求？

- A、 使用 AWS VPN CloudHub 通过私有端点路由所有对 S3 和 DynamoDB 的访问。
- B、 使用 AWS Transit Gateway 通过专用端点路由到 S3 和 DynamoDB 的所有访问。
- C、 使用 AWS Direct Connect 通过专用端点路由所有对 S3 和 DynamoDB 的访问。
- D、 使用专有网络端点通过私有端点路由所有对 S3 和 DynamoDB 的访问。

答案 D

分析：

VPC 端点允许您私自将 VPC 连接到由 AWS PrivateLink 支持的 AWS 和 VPC 端点服务，而无需互联网网关、NAT 计算机、VPN 连接或 AWS 直接连接。VPC 中的实例不需要公共 IP 地址与服务中的资源通信。专有网络和其他服务之间的流量不会离开亚马逊网络。

在该场景中，要求您配置私有端点，以便在不访问公共互联网的情况下向 Amazon DynamoDB 和 Amazon S3 发送数据。在给出的选项中，VPC 端点是最合适的服务，它允许您使用私有 IP 地址访问 DynamoDB 和 S3，而无需接触公共互联网。

因此，正确的答案是这样的选项：使用专有网络端点通过私有端点路由所有对 S3 和 DynamoDB 的访问。

表示：使用 AWS Transit Gateway 将 S3 和 DynamoDB 中的所有访问路由到公共端点的选项是不正确的，因为 Transit Gateway 只是通过一个中心集线器连接 VPC 和内部网络。它充当云路由器，允许您集成多个网络。“使用 AWS Direct Connect 通过专用端点路由所有对 S3 和 DynamoDB 的访问”选项不正确，因为 AWS DirectConnect 主要用于建立从您的房屋到 AWS 的专用网络连接。该场景并没有说该公司正在使用其内部服务器或具有混合云架构。

表示：使用 AWS VPN CloudHub 将 S3 和 DynamoDB 中的所有访问路由到专用端点的选项是不正确的，因为 AWS VPN 云中心主要用于提供远程站点之间的安全通信，而不是创建专用端点来访问亚马逊网络中的亚马逊 S3 和 DynamoDB。

参考文献：

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/vpc-endpoints-dynamodb.html>

<https://docs.aws.amazon.com/glue/latest/dg/vpc-endpoints-s3.html> 查看此亚马逊 VPC 备忘单：

<https://tutorialsdojo.com/amazon-vpc/>

Q104.一家公司在 EC2 实例的自动缩放组中托管了一个 web 应用程序。IT 经理担心资源的过度配置会导致更高的运营成本。已指示解决方案架构师在不影响应用程序性能的情况下创建经济高效的解决方案。

应使用哪种动态缩放策略来满足此要求？

- A、使用简单的缩放。
- B、使用暂停和恢复缩放。
- C、使用计划缩放。
- D、使用目标跟踪和缩放。

答案 D

分析：

自动缩放组包含一组 Amazon EC2 实例，出于自动缩放和管理的目的，这些实例被视为逻辑分组。自动缩放组还允许您使用 Amazon EC2 自动缩放功能，如健康检查替换和缩放策略。维护自动缩放组中的实例数和自动缩放组是 Amazon EC2 自动缩放服务的核心功能。自动缩放组的大小取决于设置为所需容量的实例数。您可以手动或使用自动缩放来调整其大小以满足需求。

步骤缩放策略和简单缩放策略是可供您使用的两个动态缩放选项。两者都要求您为扩展策略创建 CloudWatch 警报。两者都要求您指定报警的高阈值和低阈值。两者都要求您定义是否添加或删除实例，以及数量，或将组设置为精确的大小。策略类型之间的主要区别在于，您可以通过步骤缩放策略获得步骤调整。当应用阶跃调整时，它们会增加或减少自动缩放组的当前容量，这些调整会根据警报中断的大小而变化。

简单扩展的主要问题是，启动扩展活动后，策略必须等待扩展活动或运行状况检查替换完成，以及冷却期到期，然后才能响应其他警报。冷却期有助于防止在之前活动的影响可见之前启动额外的缩放活动。使用目标跟踪缩放策略，您可以根据特定指标的目标值增加或减少组的当前容量。此策略将有助于解决资源的过度配置问题。缩放策略根据需要添加或删除容量，以将度量保持在或接近指定的目标值。除了保持度量接近目标值之外，目标跟踪缩放策略还根据因负载模式变化而导致的度量变化进行调整。

因此，正确答案是：使用目标跟踪缩放。“使用简单缩放”选项不正确，因为在启动其他缩放活动之前，您需要等待冷却期结束。目标跟踪或步骤缩放策略可以立即触发缩放活动，而无需等待冷却期到期。“使用计划缩放”选项不正确，因为此策略主要用于可预测的流量模式。您需要使用目标跟踪扩展策略来优化基础架构的成本，而不影响性能。

“使用暂停和恢复缩放”选项不正确，因为该类型用于临时暂停由缩放策略和计划操作触发的缩放活动。

参考文献：

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scaling-target-tracking.html>

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/AutoScalingGroup.html> 查看此 AWS 自动缩放备忘单：

<https://tutorialsdojo.com/aws-auto-scaling/>

Q105. 公司需要设计一个在线分析应用程序，将红移集群用于其数据仓库。以下哪项服务允许他们监控 Redshift 实例中的所有 API 调用，并为审计和法规遵从性目的提供安全数据？

- A、 AWS CloudTrail
- B、 亚马逊云观察
- C、 AWS X 射线
- D、 亚马逊红移光谱

答:

分析:

AWS CloudTrail 是一项支持 AWS 帐户的治理、合规、运营审计和风险审计的服务。使用 CloudTrail，您可以在 AWS 基础设施中记录、持续监控和保留与操作相关的帐户活动。默认情况下，创建 AWS 帐户时，会在 AWS 帐户上启用 CloudTrail。什么时候

活动发生在您的 AWS 帐户中，该活动记录在 CloudTrail 事件中。通过转到事件历史记录，您可以在 CloudTrail 控制台中轻松查看最近的事件。CloudTrail 提供 AWS 帐户活动的事件历史记录，包括通过 AWS 管理控制台、AWS SDK、命令行工具、API 调用和其他 AWS 服务采取的操作。此事件历史简化了安全分析、资源更改跟踪和故障排除。

因此，正确答案是：AWS CloudTrail。

Amazon CloudWatch 不正确。尽管这这也是一个监控服务，但它无法跟踪对 AWS 资源的 API 调用。

AWS X 射线是不正确的，因为它不适合用于跟踪对 AWS 资源的每个 API 调用。它可以帮助您通过请求跟踪来调试和分析微服务应用程序，从而找到问题和性能的根本原因。

Amazon Redshift Spectrum 是不正确的，因为这不是一项监控服务，而是 Amazon Redshift 的一项功能，使您能够使用已使用的开放数据格式查询和分析 Amazon S3 中的所有数据，而无需数据加载或转换。

参考文献:

<https://aws.amazon.com/cloudtrail/>

<https://docs.aws.amazon.com/awsccloudtrail/latest/userguide/cloudtrail-user-guide.html> 查看此 AWS CloudTrail 备忘单: <https://tutorialsdojo.com/aws-cloudtrail/>

Q106. 一家初创公司正在使用 Amazon RDS 存储来自 web 应用程序的数据。大多数情况下，应用程序的用户活动性较低，但只要有新产品发布，它就会在几秒钟内收到流量突发。解决方案架构师需要创建一个解决方案，允许全球用户使用 API 访问数据。

解决方案架构师应如何满足上述要求？

- A、 使用 AmazonAPI 网关创建一个 API，并使用具有服务自动扩展功能的 AmazonECS 集群在几秒钟内处理突发流量。
- B、 使用 Amazon API 网关创建 API，并使用具有自动伸缩功能的 Amazon Elastic Beanstalk 在几秒钟内处理突发流量。

C、使用 Amazon API 网关创建一个 API，并使用一组自动伸缩的 Amazon EC2 实例来在几秒钟内处理突发流量。

D、使用 Amazon API 网关创建 API，并使用 AWS Lambda 在几秒钟内处理流量突发。

答案 D

分析：

AWS Lambda 允许您运行代码，而无需配置或管理服务器。您只需支付所消耗的计算时间。使用 Lambda，您可以为几乎任何类型的应用程序或后端服务运行代码

-均为零给药。只需上传代码，Lambda 就可以处理运行和扩展代码所需的一切，并具有高可用性。您可以将代码设置为从其他 AWS 服务自动触发，或直接从任何 web 或移动应用程序调用。第一次调用函数时，AWS Lambda 会创建函数的实例，并运行其处理程序方法来处理事件。当函数返回响应时，它保持活动状态并等待处理其他事件。如果在处理第一个事件时再次调用该函数，Lambda 将初始化另一个实例，该函数将同时处理两个事件。随着更多事件的到来，Lambda 将它们路由到可用实例，并根据需要创建新实例。当请求数量减少时，Lambda 会停止未使用的实例，以释放其他函数的扩展能力。

函数的并发性是在给定时间为请求提供服务的实例数。对于初始流量突发，函数在一个区域中的累积并发性可以达到 500 到 3000 之间的初始水平，每个区域都有所不同。

根据给定的场景，您需要创建满足这两个需求的解决方案。第一个要求是创建一个解决方案，允许用户使用 API 访问数据。要实现此解决方案，您可以使用 Amazon API 网关。第二个要求是在几秒钟内处理突发流量。在这种情况下，您应该使用 AWS Lambda，因为 Lambda 函数可以在大约 15-30 分钟内吸收合理的流量突发。Lambda 的扩展速度比 Amazon EC2、Amazon Elastic Beanstalk 或 Amazon ECS 的常规自动扩展功能更快。这是因为 AWS Lambda 比其他计算服务更轻量级。在幕后，Lambda 可以在几秒钟内将代码运行到数千个可用的 AWS 托管 EC2 实例（可能已经在运行），以适应流量。这比启动新 EC2 实例的自动缩放过程要快，这可能需要几分钟左右的时间。另一种方法是过度提供计算能力，但这将带来巨大的成本。实现给定需求的最佳选项是 AWS Lambda 和 Amazon API 网关的组合。

因此，正确的答案是：使用 Amazon API 网关创建 API，并使用 AWS Lambda 处理流量突发。

“使用 Amazon API 网关创建 API，并使用具有服务自动扩展功能的 Amazon ECS 集群在几秒钟内处理突发流量”的选项是不正确的。AWS Lambda 是比 Amazon ECS 更好的选择，因为它可以在几秒钟而不是几分钟内处理突发流量。“使用 Amazon API 网关创建 API 并使用具有自动伸缩功能的 Amazon Elastic Beanstalk 在几秒钟内处理流量突发”的选项是不正确的，因为与前面的选项一样，使用

自动缩放会延迟几分钟，因为它会启动 Amazon Elastic Beanstalk 将使用的新 EC2 实例。

该选项表示：使用 Amazon API 网关创建 API 并使用 Amazon EC2 实例的自动伸缩组在几秒钟内处理流量突发是不正确的，因为 Amazon EC2 自动伸缩以提供新资源的处理时间需要几分钟。请注意，在这种情况下，预计会在几秒钟内发生流量突发。参考文献：

<https://aws.amazon.com/blogs/startups/from-0-to-100-k-in-seconds-instant-scale-with-aws-lambda/>
<https://docs.aws.amazon.com/lambda/latest/dg/invoke-scaling.html> 查看 AWS Lambda 备忘单：

<https://tutorialsdojo.com/aws-lambda/>

Q107. 一家公司有一个云架构，由 Linux 和 Windows EC2 实例组成，每周 7 天，每天 24 小时处理大量金融数据。为了确保系统的高可用性，解决方案架构师需要创建一个解决方案，允许他们监控所有实例的内存和磁盘利用率指标。

以下哪项是最适合实施的监控解决方案？

- A、在 EC2 中启用增强的监控选项，并将 CloudWatch 代理安装到所有 EC2 实例，以便能够在 CloudWatch 仪表板中查看内存和磁盘利用率。
- B、使用 Amazon Inspector 并将 Inspector 代理安装到所有 EC2 实例。
- C、将 CloudWatch 代理安装到收集内存和磁盘利用率数据的所有 EC2 实例。

在 Amazon CloudWatch 控制台中查看自定义指标。

- D、对于内存和磁盘利用率指标已经可用的 EC2 实例，使用默认的 CloudWatch 配置。将 AWS 系统管理器（SSM）代理安装到所有 EC2 实例。

答案 C

分析：

Amazon CloudWatch 提供了可用的 Amazon EC2 指标，可用于监控 CPU 利用率、网络利用率、磁盘性能和磁盘读/写。如果您需要监控以下项目，您需要使用 Perl 或其他 shell 脚本准备一个自定义指标，因为没有现成的指标：内存利用率

磁盘交换利用率

磁盘空间利用率

页面文件利用率

日志收集

请注意，有一个多平台 CloudWatch 代理，可以安装在基于 Linux 和 Windows 的实例上。您可以使用单个代理从 Amazon EC2 实例和内部部署服务器收集系统指标和日志文件。此代理同时支持 Windows Server 和 Linux，并允许您选择要收集的指标，包括子资源指标，如每个 CPU 核心。建议您使用新代理而不是旧的监控脚本来收集度量和日志。因此，正确的答案是：将 CloudWatch 代理安装到收集内存和磁盘利用率数据的所有 EC2 实例。在 Amazon CloudWatch 控制台中查看自定义指标。该选项表示：在内存和磁盘利用率指标已经可用的 EC2 实例中使用默认的 CloudWatch 配置。将 AWS Systems Manager（SSM）代理安装到所有 EC2 实例是不正确的，因为默认情况下，CloudWatch 不会自动提供实例的内存和磁盘利用率指标。您必须设置自定义 CloudWatch 指标来监控实例的内存、磁盘交换、磁盘空间和页面文件利用率。“启用 EC2 中的增强监控选项并将 CloudWatch 代理安装到所有 EC2 实例，以便能够在 CloudWatch 仪表板中查看内存和磁盘利用率”的选项不正确，因为增强监控是 Amazon RDS 的一项功能。默认情况下，增强的监控指标在 CloudWatch 日志中存储 30 天。“使用 Amazon Inspector 并将 Inspector 代理安装到所有 EC2 实例”选项是不正确的，因为 Amazon Inspector 是一种自动安全评估服务，可帮助您测试 Amazon EC2 实例的网络可访问性以及在实例上运行的应用程序的安全状态。它不提供自定义指标来跟踪 VPC 中每个 EC2 实例的内存和磁盘利用率。

参考文献：

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/monitoring_ec2.html
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/mon-scripts.html#using_put_script 查看此 Amazon CloudWatch 备忘单：<https://tutorialsdojo.com/amazon-cloudwatch/>

CloudWatch 代理 vs SSM 代理 vs 自定义守护程序脚本：

<https://tutorialsdojo.com/cloudwatch-agent-vs-ssm-agent-vs-custom-daemon-scripts/AWS> 服务备忘单比较：
<https://tutorialsdojo.com/comparison-of-aws-services/>

Q108. 一家公司正在将其应用程序迁移到 AWS。他们的一个系统需要一个能够全局扩展并处理频繁模式更改的数据库。只要数据库中有模式更改，应用程序就不应该有任何停机时间或性能问题。它还应为高流量查询提供低延迟响应。

哪种数据库解决方案最适合用于实现此要求？

- A、 红移
- B、 亚马逊发电机 B
- C、 多 AZ 部署配置中的 Amazon RDS 实例
- D、 具有读取副本的 Amazon Aurora 数据库

答案 B

分析：

在继续回答这个问题之前，我们必须首先明确“模式”的实际定义。基本上，图式的英文定义是：以大纲或模型的形式表示计划或理论。

只要将模式视为数据库中数据的“结构”或“模型”。由于场景要求模式或数据结构频繁更改，因此您必须选择一个数据库，该数据库提供了添加或删除新类型数据的非刚性和灵活方式。这是在关系数据库和非关系

（NoSQL）数据库之间进行选择的经典示例。众所周知，关系数据库具有严格的模式，对于哪些数据（以及什么类型的数据）可以插入或不插入，有很多约束和限制。它主要用于必须支持跨多个表获取数据的复杂查询的场景。它最适合于具有复杂表关系的场景，但对于需要灵活模式的用例，它不适合使用。

对于 NoSQL，它不像关系数据库那样严格，因为您可以轻松地在表/集合条目中添加或删除行或元素。它还具有更灵活的模式，因为它可以在单个项中存储复杂的层次结构数据，与关系数据库不同，它不需要更改多个相关表。因此，这里使用的最佳答案是 NoSQL 数据库，如 DynamoDB。当您的业务需要低延迟响应高流量查询时，利用 NoSQL 系统通常具有技术和经济意义。

Amazon DynamoDB 通过避免这些问题来帮助解决限制关系系统可伸缩性的问题。在 DynamoDB 中，您专门设计了模式，以尽可能快速和廉价地进行最常见和最重要的查询。您的数据结构是根据业务用例的特定需求定制的。

请记住，由于以下原因，关系数据库系统不能很好地扩展：

- 它规范化数据并将其存储在需要多个查询才能写入磁盘的多个表中。
- 它通常会导致 ACID 兼容事务系统的性能成本。
- 它使用昂贵的连接来重新组合查询结果的所需视图。

对于 DynamoDB 而言，由于以下原因，其扩展良好：

- 其模式灵活性允许 DynamoDB 在单个项中存储复杂的分层数据。DynamoDB 不是一个完全无模式的数据库，因为模式的定义只是数据的模型或结构。
- 复合键设计允许它将相关项紧密存储在同一个表上。MultiAZ 部署配置中的 Amazon RDS 实例和具有读取副本的 Amazon Aurora 数据库都是不正确的，因为它们都是一种关系数据库。红移是不正确的，因为它主要用于 OLAP 系统。参考文献：

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/bp-general-nosql-design.html>
<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/bp-relational-modeling.html>

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/SQLtoNoSQL.html> 另外，请查看 AWS 认证解决方案架构师官方学习指南：第一版联合考试，并转到第 161 页，其中介绍了 NoSQL 数据库。

查看此 Amazon DynamoDB 备忘单：

<https://tutorialsdojo.com/amazon-dynamodb/>

Dojo 的 AWS 认证解决方案架构师助理考试学习指南教程：<https://tutorialsdojo.com/aws-certified-solutions-architect-associate/>

Q109. 一家公司正在使用 API 网关和 Lambda 的组合作为在线门户网站的 web 服务，每天有成千上万的客户访问该网站。他们将宣布一项新的革命性产品，预计该门户网站将在全球范围内吸引大量访问者。

如何保护后端系统和应用程序免受流量高峰的影响？

- A、在 API 网关中使用节流限制
- B、API 网关将自动扩展并处理大量流量峰值，因此您无需执行任何操作。
- C、手动升级 API 网关正在使用的 EC2 实例
- D、使用读取副本在 API 网关中部署多 AZ

答：

分析：

Amazon API 网关提供多个级别的节流，包括全局和服务调用。可以为标准速率和突发设置节流限制。例如，API 所有者可以在其 REST API 中为特定方法设置每秒 1000 个请求的速率限制，还可以将 Amazon API 网关配置为在几秒钟内处理每秒 2000 个请求。Amazon API 网关跟踪每秒的请求数。任何超过限制的请求都将收到 429 HTTP 响应。Amazon API 网关生成的客户端 SDK 在遇到此响应时自动重试调用。

因此，正确的答案是：在 API 网关中使用节流限制。说：API 网关将自动扩展并处理大量流量峰值，因此您不必做任何事情的选项是不正确的。尽管它可以使用 AWS 边缘位置进行扩展，但仍然需要配置节流以进一步管理 API 的突发。

手动升级 API 网关使用的 EC2 实例是不正确的，因为 API 网关是完全受管理的服务，因此您无法访问其底层资源。在具有读取副本的 API 网关中部署多 AZ 是不正确的，因为 RDS 具有多 AZ 和读取副本功能，而不是 API 网关。

参考：

https://aws.amazon.com/api-gateway/faqs/#Throttling_and_Caching 查看此 Amazon API 网关备忘单：

<https://tutorialsdojo.com/amazon-api-gateway/>

Q110. 一家公司正在设计一个银行门户，使用 Amazon ElastiCache for Redis 作为其分布式会话管理组件。由于您所在部门的其他云工程师可以访问您的 ElastiCache 集群，因此您必须在获得执行 Redis 命令的权限之前，通过要求他们输入密码来保护门户中的会话数据。作为解决方案架构师，您应该做以下哪项来满足上述要求？

- A、通过创建启用--transit-encryption 和--AUTH-token 参数的新 Redis 集群，使用 Redis AUTH 对用户进行身份验证。
- B、设置 Redis 复制组并启用 ATRestEncryptionEnabled 参数。
- C、设置 IAM 策略和 MFA，要求云工程师在访问 ElastiCache 集群之前输入 IAM 凭据和令牌。
- D、为 Redis 复制组启用传输中加密。

答:

分析:

使用 Redis AUTH 命令可以提高数据安全性，方法是要求用户在获得在受密码保护的 Redis 服务器上执行 Redis 命令的权限之前输入密码。因此，正确的答案是：通过创建一个启用了--transit encryption 和--AUTH token 参数的新 Redis 集群，使用 Redis AUTH 对用户进行身份验证。要要求用户在受密码保护的 Redis 服务器上输入密码，请在创建复制组或集群时以及在复制组或群集的所有后续命令中使用正确的密码包含参数--auth-token。

设置 IAM 策略和 MFA 要求云工程师在访问 ElastiCache 集群之前输入 IAM 凭据和令牌，这是不正确的，因为这在 IAM 中是不可能的。您必须使用 Redis AUTH 选项。

设置 Redis 复制组并启用 ATrestEncryptionEnabled 参数是不正确的，因为

Redis 静态加密功能仅保护内存数据存储中的数据。您必须改用 Redis AUTH 选项。

为 Redis 复制组启用传输中加密不正确。虽然传输中加密是解决方案的一部分，但它缺少了最重要的一点，即 Redis AUTH 选项。

参考文献:

<https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/auth.html>

<https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/encryption.html> 查看此 Amazon Elasticache 备忘

单: <https://tutorialsdojo.com/amazon-elasticache/>

Redis（集群模式启用 vs 禁用）vs Memcached: <https://tutorialsdojo.com/redis-cluster-mode-enabled-vs-disabled-vs-memcached/>

Q111. 一家公司计划在亚马逊 EC2 实例的自动扩展组中托管 web 应用程序。用户将在全球范围内使用该应用程序上传和存储多种类型的文件。根据用户趋势，超过 2 年的文件必须存储在不同的存储类中。该公司的解决方案架构师需要创建一个经济高效且可扩展的解决方案，以存储旧文件，同时仍提供耐用性和高可用性。

以下哪种方法可用于满足此要求？（选择两个。）

- A、使用 Amazon EBS 卷存储文件。配置 Amazon 数据生命周期管理器（DLM）以在 2 年后安排卷的快照。
- B、使用 Amazon S3 并创建一个生命周期策略，该策略将在 2 年后将对象移动到 Amazon S3 Glacier。
- C、使用 RAID 0 存储配置，将多个 Amazon EBS 卷分条存储在一起以存储文件。配置 Amazon 数据生命周期管理器（DLM）以在 2 年后安排卷的快照。
- D、使用 Amazon S3 并创建一个生命周期策略，该策略将在 2 年后将对象移动到 AmazonS3 标准 IA。
- E、使用 Amazon EFS 并创建一个生命周期策略，该策略将在 2 年后将对象移动到 Amazon EFS-IA。

答：屋宇署

分析：

Amazon S3 将数据存储为 bucket 中的对象。对象是一个文件和描述该文件的任何可选元数据。要在 Amazon S3 中存储文件，需要将其上传到 bucket。将文件作为对象上载时，可以设置对象和任何元数据的权限。桶是对象的容器。您可以有一个或多个桶。您可以控制每个 bucket 的访问，决定谁可以创建、删除和列出其中的对象。您还可以选择 Amazon S3 将存储 bucket 及其内容的地理区域，并查看 bucket 及其对象的访问日志。要将文件移动到其他存储类，可以使用 Amazon S3 或 Amazon EFS。这两个服务都有生命周期配置。请注意，Amazon EFS 只能在 90 天后将文件转换为 IA 存储类。由于您需要将超过 2 年的文件移动到更具成本效益和可扩展性的解决方案，因此您应该使用 Amazon S3 生命周期配置。使用 S3 生命周期规则，您可以将文件转换为 S3 标准 IA 或 S3 Glacier。使用 S3 Glacier 加速检索，您可以在 1-5 分钟内快速访问文件。

因此，正确答案是：

- 使用 Amazon S3 并创建一个生命周期策略，该策略将在 2 年后将对象移动到 Amazon S3 Glacier。
- 使用 Amazon S3 并创建一个生命周期策略，该策略将在 2 年后将对象移动到 Amazon S3 标准 IA。

“使用 Amazon EFS 并创建一个生命周期策略，该策略将在 2 年后将对象移动到 Amazon EFS-IA”的选项是不正确的，因为 EFS 生命周期策略的最大天数只有 90 天。要求是移动超过 2 年或 730 天的文件。选项显示：使用 Amazon EBS 卷存储文件。将 Amazon Data Lifecycle Manager (DLM) 配置为在 2 年后安排卷的快照是不正确的，因为 Amazon EBS 成本更高，而且没有 Amazon S3 那样可扩展。当多个 EC2 实例访问时，它有一些限制。在配置的 IOPS EBS 卷上使用多连接功能以允许多个 EC2 实例访问该卷，也会带来巨大的成本。选项说明：使用 RAID 0 存储配置，将多个 Amazon EBS 卷分条存储在一起以存储文件。配置 Amazon 数据生命周期管理器 (DLM) 在 2 年后安排卷的快照是不正确的，因为 RAID (独立磁盘冗余阵列) 只是一种数据存储虚拟化技术，它将多个存储设备结合起来，以实现更高的性能或数据耐用性。RAID 0 可以将多个卷条带化在一起，以获得比单个卷更高的 I/O 性能。另一方面，RAID 1 可以将两个卷镜像在一起，以实现实例冗余。

参考文献：

<https://docs.aws.amazon.com/AmazonS3/latest/dev/object-lifecycle-mgmt.html>
<https://docs.aws.amazon.com/efs/latest/ug/lifecycle-management-efs.html>
<https://aws.amazon.com/s3/faqs/> 查看此
Amazon S3 备忘单：<https://tutorialsdojo.com/amazon-s3/>

Q112.AWS 托管的在线医疗系统将用户的敏感个人信息 (PII) 存储在亚马逊 S3 存储桶中。主密钥和未加密数据均不得发送至 AWS，以符合公司的严格合规和监管要求。架构师应该使用哪种 S3 加密技术？

- A、使用带有客户端主密钥的 S3 客户端加密。
- B、使用带有 KMS 管理的客户主密钥的 S3 客户端加密。
- C、使用带有 KMS 托管密钥的 S3 服务器端加密。
- D、使用 S3 服务器端加密和客户提供的密钥。

答：

分析：

客户端加密是在将数据发送到 Amazon S3 之前加密数据的行为。要启用客户端加密，您有以下选项：

- 使用 AWS KMS 管理的客户主密钥。

- 使用客户端主密钥。

使用 AWS KMS 管理的客户主密钥启用客户端数据加密时，需要向 AWS 提供 AWS KMS 客户主密钥 ID（CMK ID）。另一方面，当您使用客户端主密钥进行客户端数据加密时，客户端主密钥和未加密数据永远不会发送到 AWS。安全地管理加密密钥非常重要，因为如果丢失它们，您将无法解密数据。

这是使用客户端主密钥的客户端加密的工作方式：

上传对象时，您向 Amazon S3 加密客户端提供客户端主密钥。客户端仅使用主密钥对随机生成的数据加密密钥进行加密。过程如下：

1. Amazon S3 加密客户端在本地生成一次性对称密钥（也称为数据加密密钥或数据密钥）。它使用数据密钥加密单个 AmazonS3 对象的数据。

客户端为每个对象生成单独的数据密钥。

2. 客户端使用您提供的主密钥加密数据加密密钥。客户端上传加密的数据密钥及其材料描述，作为对象元数据的一部分。客户端使用材料描述来确定用于解密的客户端主密钥。

3. 客户端将加密数据上传到 Amazon S3，并将加密数据密钥保存为对象元数据

（x-amz-meta-x-amz-key）在 Amazon S3 中。

下载对象时-客户端从 Amazon S3 下载加密对象。使用对象元数据中的材料描述，客户端确定使用哪个主密钥解密数据密钥。客户端使用主密钥解密数据密钥，然后使用数据密钥解密对象。

因此，正确的答案是使用 S3 客户端加密和客户端主密钥。使用带有 KMS 托管客户主密钥的 S3 客户端加密是不正确的，因为在使用 KMS 托管的客户主密钥进行客户端加密时，您向 AWS 提供了 AWS KMS 客户主密钥 ID（CMK ID）。该场景清楚地表明，主密钥和未加密数据都不应发送到 AWS。

使用带有 KMS 托管密钥的 S3 服务器端加密是不正确的，因为场景提到，未加密的数据永远不应发送到 AWS，这意味着您必须使用客户端加密，以便在发送到 AWS 之前先加密数据。这样，您可以确保没有未加密的数据上传到 AWS。此外，服务器端加密使用 AWS KMSManaged 密钥（SSEKMS）使用的主密钥由 AWS 上传和管理，这直接违反了不上传主密钥的要求。

使用 S3 服务器端加密和客户提供的密钥是不正确的，因为如上所述，在这种情况下，您必须使用客户端加密，而不是服务器端加密。对于使用客户提供密钥（SSE-C）的 S3 服务器端加密，您实际上提供了加密密钥，作为将对象上传到 S3 的请求的一部分。使用此密钥，Amazon S3 管理加密（写入磁盘时）和解密（访问对象时）。

参考文献：

<https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingEncryption.html>
<https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingClientSideEncryption.html>

Q113.一个应用程序由不同可用区域的专用子网中的多个 EC2 实例组成。应用程序使用单个 NAT 网关将软件补丁从 Internet 下载到实例。有一个

当 NAT 网关遇到故障或其可用区域出现故障时，保护应用程序免受单点故障的要求。

解决方案架构师应该如何重新设计体系结构，以使其更高可用性和成本效益

A、在每个可用性区域中创建三个 NAT 网关。在每个专用子网中配置路由表，以确保实例使用相同可用性区域中的 NAT 网关。

B、在每个可用性区域中创建 NAT 网关。在每个专用子网中配置路由表，以确保实例使用相同可用性区域中的 NAT 网关

C、在每个可用性区域中创建两个 NAT 网关。在每个公共子网中配置路由表，以确保实例使用相同可用性区域中的 NAT 网关。

D、在每个可用性区域中创建 NAT 网关。在每个公共子网中配置路由表，以确保实例使用相同可用性区域中的 NAT 网关。

答案 B

分析：

NAT 网关是一种高可用的、受管理的网络地址转换（NAT）服务，用于您在专用子网中访问 Internet 的资源。NAT 网关在特定的可用性区域中创建，并在该区域中实现冗余。

您必须在公共子网上创建 NAT 网关，以使私有子网中的实例能够连接到 Internet 或其他 AWS 服务，但防止 Internet 启动与这些实例的连接。

如果您在多个可用性区域中有资源，并且它们共享一个 NAT 网关，并且如果 NAT 网关可用区域已关闭，其他可用区域中的资源将无法访问 Internet。要创建独立于可用性区域的体系结构，请在每个可用性区域中创建 NAT 网关，并配置路由，以确保资源使用相同可用性区域内的 NAT 网关。因此，正确的答案是：在每个可用性区域中创建一个 NAT 网关。在每个专用子网中配置路由表，以确保实例使用相同可用性区域中的 NAT 网关。该选项表示：在每个可用性区域中创建 NAT 网关。在每个公用子网中配置路由表以确保实例在同一可用性区域中使用 NAT 网关是不正确的，因为您应该在专用子网而不是公用子网配置路由表，以关联专用子网中的正确实例。

选项说明：在每个可用性区域中创建两个 NAT 网关。在每个公共子网中配置路由表，以确保实例在同一可用性区域中使用 NAT 网关，并在每个可用性区域创建三个 NAT 网关。在每个专用子网中配置路由表，以确保在同一可用区域中使用 NAT 网关的实例都不正确，因为每个可用区域中的单个 NAT 网关就足够了。NAT 网关在本质上已经是冗余的，这意味着 AWS 已经在可用性区域中处理 NAT 网关中发生的任何故障。

参考文献：

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html>

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-comparison.html> 查看此亚马逊 VPC 备忘单：

<https://tutorialsdojo.com/amazon-vpc/>

Q114. 公司从不同国家收集大气数据，如温度、气压和湿度。每个站点都配备了各种气象仪器和高速互联网连接。每个位置的平均收集数据约为 **500GB**，将由位于弗吉尼亚州北部的天气预报应用程序进行分析。作为解决方案架构师，您需要以最快的方式聚合所有数据。

以下哪个选项可以满足给定要求？

A、设置站点到站点 VPN 连接。

B、在目标存储桶中启用传输加速，并使用多部分上传上传收集的数据。

C、将数据上传到最近的 S3 存储桶。设置跨区域复制并将对象复制到 destinationbucket。

D、使用 AWS Snowball Edge 传输大量数据。

答案 B

分析:

Amazon S3 是一种对象存储，用于存储和检索互联网上任何位置的任何数量的数据。它是一种简单的存储服务，以极低的成本提供业界领先的耐用性、可用性、性能、安全性和几乎无限的可扩展性。Amazon S3 的设计也非常灵活。存储所需的任何类型和数量的数据；读取同一条数据一百万次或仅用于紧急灾难恢复；构建简单的 FTP 应用程序或复杂的 web 应用程序。由于天气预报应用程序位于弗吉尼亚州北部，您需要在同一 AWS 区域传输所有数据。通过 Amazon S3 传输加速，您可以将与 Amazon S3s 之间的内容传输速度提高 50-500%，以实现更大对象的远程传输。多部分上传允许您将单个对象作为一组部分上传。上传对象的所有部分后，Amazon S3 将数据作为单个对象显示。这种方法是聚合所有数据的最快方法。因此，正确答案是：在目标存储桶中启用传输加速，并使用多部分上传上传收集的数据。

选项表示：将数据上传到最近的 S3 存储桶。设置跨区域复制并将对象复制到目标存储桶是不正确的，因为将对象复制至目标存储桶大约需要 15 分钟。请注意，场景中的要求是以最快的方式聚合数据。

“使用 AWS Snowball Edge 传输大量数据”选项不正确，因为将多达 80 TB 的数据传输到 AWS Snow ball Edge 的端到端时间大约为一周。“设置站点到站点 VPN 连接”选项不正确，因为在这种情况下不需要设置 VPN 连接。站点到站点 VPN 仅用于在内部网络和亚马逊 VPC 之间建立安全连接。此外，这种方法不是传输数据的最快方法。您必须使用 AmazonS3 传输加速。

参考文献:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/replication.html>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/transfer> 加速。html 查看此 Amazon S3 备忘单:

<https://tutorialsdojo.com/amazon-s3/>

Q115. 一家公司计划在 AWS 中构建数据分析应用程序，该应用程序将部署在按需 EC2 实例和 MongoDB 数据库的自动扩展组中。预计数据库将具有执行小型随机 I/O 操作的高吞吐量工作负载。作为解决方案架构师，您需要在 AWS 中正确设置和启动所需的资源。以下哪种类型最适合用于您的数据库？

- A、通用 SSD (gp2)
- B、冷硬盘 (sc1)
- C、吞吐量优化 HDD (st1)
- D、配置 IOPS SSD (io1)

答案 D

分析:

在给定卷配置中，某些 I/O 特性会驱动 EBS 卷的性能行为。SSD 支持的卷，如通用 SSD (gp2) 和配置的 IOPS SSD (io1)，无论 I/O 操作是随机的还是顺序的，都能提供一致的性能。HDD 支持的卷，如吞吐量

优化 HDD (st1) 和冷 HDD (sc1) 仅在 I/O 操作较大且连续时提供最佳性能。

在检查中，始终考虑 SSD 和 HDD 之间的差异，如下表所示。这将允许您轻松消除选项中非 SSD 或非 HDD 的特定 EBS 类型，具体取决于问题要求的存储类型是具有小的随机 I/O 操作还是大的顺序 I/O。

配置的 IOPS SSD (io1) 卷旨在满足 I/O 密集型工作负载的需要，特别是数据库工作负载，这些工作负载对存储性能和一致性非常敏感。与 gp2 不同，gp2 使用桶和信用模型来计算性能，io1 卷允许您在创建卷时指定一致

的 IOPS 速率，而 Amazon EBS 在给定一年中 99.9% 的时间内提供的 IOPS 性能在 10% 以内。通用 SSD (gp2) 是不正确的，因为尽管通用 SSD 是一种可以处理小型随机 I/O 操作的 SSD，但配置的 IOPS SSD 卷更适合满足 I/O 密集型数据库工作负载的需求，如 MongoDB、Oracle、MySQL 和其他许多。吞吐量优化的 HDD (st1) 和冷 HDD (sc1) 是不正确的，因为 HDD 卷（如吞吐量优化的硬盘和冷硬盘卷）更适合于具有大的顺序 I/O 操作的工作负载，而不是小的随机 I/O。

参考文献：

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html#EBSVolumeTypes_piops

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-io-characteristics.html> 亚马逊 EBS 概述-SSD vs 硬盘：

<https://www.youtube.com/watch?v=LW7x8wyLFvw>

查看此亚马逊 EBS 备忘单：<https://tutorialsdojo.com/amazon-ebs/>

Q116.一家在世界各地设有办事处的全球 IT 公司拥有多个 AWS 账户。为了提高效率并降低成本，首席信息官（CIO）希望建立一个集中管理 AWS 资源的解决方案。这将使他们能够集中采购 AWS 资源，并在其各个账户之间共享资源，如 AWS 传输网关、AWS 许可证管理器配置或 Amazon Route 53 解析器规则。

作为解决方案架构师，您应该在此场景中实现哪种选项组合？（选择两个。）

- A、使用 AWS 身份和访问管理服务设置跨账户访问，将轻松安全地与 AWS 账户共享资源。
- B、使用 AWS ParallelCluster 整合公司的所有账户。
- C、使用 AWS 资源访问管理器（RAM）服务轻松安全地与 AWS 账户共享资源。
- D、使用 AWS 控制塔轻松安全地与 AWS 账户共享资源。
- E、使用 AWS 组织合并公司的所有账户。

行政长官的答覆

分析：

AWS 资源访问管理器（RAM）是一项服务，使您能够轻松安全地与任何 AWS 账户或 AWS 组织内共享 AWS 资源。您可以与 RAM 共享 AWS 传输网关、子网、AWS 许可证管理器配置和 Amazon Route 53 解析器规则资源。许多组织使用多个账户来创建管理或计费隔离，并限制错误的影响。RAM 消除了多个账户中创建重复资源的需要，减少了在您拥有的每个账户中管理这些资源的操作开销。您可以在多账户环境中集中创建资源，并使用 RAM 通过三个简单步骤跨账户共享这些资源：创建资源共享、指定资源和指定账户。RAM 免费提供给您。

您可以集中采购 AWS 资源，并使用 RAM 与其他账户共享资源，如子网或许可证管理器配置。这消除了多账户环境中为每个账户提供重复资源的需要，减少了管理每个账户中的资源的操作开销。

AWS 组织是一种账户管理服务，允许您将多个 AWS 账户合并到您创建并集中管理的组织中。使用组织，您可以创建成员账户并邀请现有账户加入您的组织。您可以将这些账户组织为组并附加基于策略的控件。

因此，在这种情况下，正确的选项组合是：

- 使用 AWS 组织合并公司的所有账户。
- 使用 AWS 资源访问管理器（RAM）服务轻松安全地与 AWS 账户共享资源。

“使用 AWS 身份和访问管理服务设置跨帐户访问，以轻松安全地与您的 AWS 帐户共享您的资源”的选项是不正确的，因为尽管您可以使用 IAM 委托访问不同 AWS 帐户中的资源，这个过程非常繁琐，需要大量的操作开销，因为您必须手动设置对公司的每个 AWS 帐户的跨帐户访问。更好的解决方案是使用 AWS 资源访问管理器。

“使用 AWS 控制塔与您的 AWS 帐户轻松安全地共享您的资源”的选项是不正确的，因为 AWS 控制塔可提供最简单的方式来设置和管理新的、安全的多帐户 AWS 环境。这不是用于跨 AWS 帐户或组织内安全共享资源的最合适的服务。您必须使用 AWS 资源访问管理器（RAM）。

“使用 AWS ParallelCluster 合并公司的所有帐户”的选项是不正确的，因为 AWS ParallelCluster 只是一个 AWS 支持的开源集群管理工具，可以让您轻松地在 AWS 上部署和管理高性能计算（HPC）集群。在这个特定场景中，使用 AWS 组织来整合所有 AWS 帐户更为合适。

参考文献：<https://aws.amazon.com/ram/>

<https://docs.aws.amazon.com/ram/latest/userguide/shareable.html>

Q117.您所在的一家科技公司进行了总体拥有成本（TCO）分析，评估了亚马逊 S3 的使用情况与购买更多存储硬件的情况。结果是，所有 1200 名员工将被授予使用 Amazon S3 存储个人文档的权限。您需要考虑以下哪一项，以便设置一个解决方案，该解决方案包含公司 AD 或 LDAP 目录中的单点登录功能，并限制每个用户对 S3 存储桶中指定用户文件夹的访问？（选择两个。）

- A、 为公司目录中需要访问 3 存储桶中文件夹的 1200 个用户中的每一个设置匹配的 IAM 用户。
- B、 配置 IAM 角色和 IAM 策略以访问存储桶。
- C、 使用第三方单点登录解决方案，如 Atlassian Crowd、OKTA、OneLogin 等。
- D、 使用 Amazon WorkDocs 将每个用户映射到 S3 中指定的用户文件夹，以访问他们的个人文档。
- E、 设置联合代理或身份提供者，并使用 AWS 安全令牌服务生成临时令牌。

答案 B

分析：

该问题涉及 AWS 中临时凭证的常见场景之一。临时凭据在涉及身份联合、委派、跨帐户访问和 IAM 角色的场景中非常有用。在本例中，考虑到您还需要设置单点登录（SSO）功能，称为企业身份联合。

正确答案是：

- 设置联合代理或身份提供程序
- 设置 AWS 安全令牌服务以生成临时令牌
- 配置 IAM 角色和 IAM 策略以访问存储桶。在企业身份联盟中，您可以对组织网络中的用户进行身份验证，然后向这些用户提供 AWS 访问，而无需为他们创建新的 AWS 身份，并要求他们使用单独的用户名和密码登录。这被称为临时访问的单点登录（SSO）方法。AWS STS 支持开放标准，如安全断言标记语言（SAML）2.0，您可以使用 Microsoft AD FS 来利用 Microsoft Active Directory。您还可以使用 SAML 2.0 来管理您自己的用户身份联合解决方案。

使用第三方单点登录解决方案，如 Atlassian Crowd、OKTA、OneLogin 和许多其他解决方案是不正确的，因为您不必使用第三方向解决方案来提供访问。AWS 已经提供了在这种情况下可以使用的必要工具。使用 Amazon WorkDocs 将每个用户映射到 S3 中的指定用户文件夹以访问其个人文档是不正确的，因为没有直接的方法将

Amazon S3 与 Amazon WorkDocs 集成到这个特定场景中。Amazon WorkDocs 是一个完全管理、安全的内容创建、存储和

协作服务。使用 Amazon WorkDocs，您可以轻松创建、编辑和共享内容。因为它集中存储在 AWS 上，所以您可以在任何设备上的任何位置访问它。为公司目录中需要访问 S3 存储桶中文件夹的 1200 个用户中的每一个设置匹配的 IAM 用户是不正确的，因为不需要创建那么多 IAM 用户。此外，您希望帐户与 AD 或 LDAP 目录集成，因此 IAM 用户不符合这些标准。

参考文献：

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_saml.html

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_oidc.html

<https://aws.amazon.com/premiumsupport/knowledge-center/iam-s3-user-specific-folder/AWS> 身份服务概述：

<https://youtu.be/AIdUw0i8rr0> 查看此 AWS IAM 备忘单：

<https://tutorialsdojo.com/aws-identity-and-access-management-iam/>

Q118.您的 RDS 数据库实例的可用性区域中存在大量中断，导致您无法访问数据库。如果此事件再次发生，您可以采取什么措施防止丢失对数据库的访问？

- A、创建数据库的快照
- B、增加数据库实例大小
- C、创建读取副本
- D、启用多 AZ 故障切换

答案 D

分析：

Amazon RDS 多 AZ 部署为数据库（DB）实例提供了增强的可用性和耐用性，使它们自然适合生产数据库工作负载。对于这个场景，启用多 AZ 故障转移是正确答案。提供多 AZ 数据库实例时，Amazon RDS 会自动创建主数据库实例，并将数据同步复制到不同可用性区域（AZ）中的备用实例。每个 AZ 都运行在其物理上不同的独立基础设施上，并设计为高度可靠。

如果基础设施出现故障，Amazon RDS 将自动故障切换到备用（或在 Amazon Aurora 的情况下切换到读取副本），以便在故障切换完成后立即恢复数据库操作。

创建数据库快照允许您对数据库进行备份，但在 AZ 出现故障时不能立即提供可用性。所以这是不正确的。增加数据库实例大小不是解决此问题的方法。执行此操作可以解决升级计算容量的需要，但不能解决即使在其中一个可用性区域丢失的情况下也可以访问数据库的要求。创建读取副本是不正确的，因为这只是为读取繁重的数据库工作负载提供了增强的性能。虽然您可以升级读取副本，但其异步复制可能无法为您提供数据库的最新版本。

参考：

<https://aws.amazon.com/rds/details/multi-az/>

查看此 Amazon RDS 备忘单：

Q119.加密货币交易平台使用 AWS Lambda 和 API 网关内置的 API。由于最近关于比特币、以太坊和其他加密货币即将涨价的新闻和谣言，预计未来几天，交易平台的网站访客和新用户将大幅增加。

在这种情况下，如何保护平台的后端系统不受流量峰值的影响？

- A、在 VPC 中移动 Lambda 函数。
- B、在 API 网关中启用节流限制和结果缓存。
- C、在 API 网关前面使用 CloudFront 作为缓存。
- D、从使用 AWS Lambda 和 API 网关切换到使用 EC2 instances、ELB 和自动扩展的更具可扩展性和高可用性的体系结构。

答案 B

分析：

Amazon API 网关提供多个级别的节流，包括全局和服务调用。可以为标准速率和突发设置节流限制。例如，API 所有者可以在其 REST API 中为特定方法设置每秒 1000 个请求的速率限制，还可以将 Amazon API 网关配置为在几秒钟内处理每秒 2000 个请求。Amazon API 网关跟踪每秒的请求数。任何超过限制的请求都将收到 429 HTTP 响应。Amazon API 网关生成的客户端 SDK 在遇到此响应时自动重试调用。因此，在 API 网关中启用节流限制和结果缓存是正确答案。您可以通过配置 Amazon API 网关缓存并指定其大小（以 GB 为单位），将缓存添加到 API 调用中。缓存是为 API 的特定阶段提供的。这提高了性能并减少了发送到后端的流量。缓存设置允许您控制生成缓存键的方式以及为每个方法存储的数据的生存时间（TTL）。Amazon API 网关还公开了管理 API，帮助您使每个阶段的缓存无效。

表示：从使用 AWS Lambda 和 API 网关切换到使用 EC2 实例、ELB 和自动扩展的更具可扩展性和高可用性的架构是不正确的，因为不需要将应用程序转移到其他服务。

在 API 网关前面使用 CloudFront 作为缓存是不正确的，因为 CloudFront 只能加快内容交付，从而为用户提供更好的延迟体验。这对后端没有多大帮助。

在 VPC 中移动 Lambda 函数是不正确的，因为这个答案与被询问的内容无关。VPC 是您自己的虚拟私有云，您可以在其中启动 AWS 服务。

参考：

<https://aws.amazon.com/api-gateway/faqs/> 查看此

Amazon API 网关备忘单：

<https://tutorialsdojo.com/amazon-api-gateway/> 以下

是关于 Amazon API 网关的深入教程：

<https://youtu.be/XwfpPEFHKtQ>

Q120.内容管理系统（CMS）托管在一组自动扩展的按需 EC2 实例上，这些实例使用亚马逊极光作为其数据库。目前，系统将用户上传的文件文档存储在一个附加的 EBS 卷中。您的经理注意到系统性能相当慢，他已指示您改进系统架构。在这个场景中，您将如何实现一个可伸缩的、高可用的、符合 POSIX 的共享文件系统？

- A、 创建一个 S3 存储桶，并将其用作 CMS 的存储
- B、 将现有 EBS 卷升级到配置的 IOPS SSD 卷
- C、 使用松紧带
- D、 EFS 的使用

答案 D

分析：

Amazon 弹性文件系统（Amazon EFS）提供简单、可扩展、弹性文件存储，用于 AWS 云服务和内部资源。当安装在 Amazon EC2 实例上时，Amazon EFS 文件系统提供了标准文件系统接口和文件系统访问语义，允许您将 Amazon EFS 与现有应用程序和工具无缝集成。多个 Amazon EC2 实例可以同时访问 Amazon EFS 文件系统，从而允许 Amazon EFS 为在多个 Amazon EC2 实例上运行的工作负载和应用程序提供公共数据源。此特定场景测试您对 EBS、EFS 和 S3 的理解。在此场景中，有一组按需 EC2 实例，将用户的文件文档存储到一个附加的 EBS 卷。系统性能相当慢，因为体系结构不提供 EC2 实例对文件文档的并行共享访问。

尽管一个 EBS 卷可以连接到多个 EC2 实例，但只能在可用性区域内的实例上连接。我们需要的是能够跨越多个可用区域的高可用存储。还要注意，这里所需的存储类型是“文件存储”，这意味着 S3 不是最好的服务，因为它主要用于“对象存储”，S3 也不提供“文件夹”的概念。这就是为什么使用 EFS 是正确答案。

将现有 EBS 卷升级为配置的 IOPS SSD 卷是不正确的，因为 EBS 卷是存储区域网络（SAN）存储，而不是符合 POSIX 的共享文件系统。您必须改用 EFS。

使用 ElastiCache 是不正确的，因为这是一个内存数据存储，可以提高应用程序的性能，而这不是您所需要的，因为它不是文件存储。

参考：

<https://aws.amazon.com/efs/>

查看此亚马逊 EFS 备忘单：

<https://tutorialsdojo.com/amazon-efs/>

查看此 Amazon S3 vs EBS vs EFS 备忘单：<https://tutorialsdojo.com/amazon-s3-vs-ebs-vs-efs/>

Q121.一家公司采用混合云架构，将其内部数据中心与 AWS 中的云基础设施连接起来。他们需要为存储在本地的公司文档提供持久的存储备份，以及本地缓存，以提供对最近访问的数据的低延迟访问，从而减少数据出口费用。文档必须通过服务器消息块（SMB）协议存储到 AWS 并从 AWS 检索。这些文件必须在几分钟内立即可访问六个月，并存档十年，以满足数据法规遵从性要求。

在这种情况下，以下哪种方法是最佳和最具成本效益的实施方法？

- A、 启动一个新的文件网关，使用 AWS 存储网关连接到本地数据中心。将文档上传到文件网关，并设置生命周期策略，将数据移动到 Glacier 进行数据存档。

B、使用 AWS Snowmobile 从本地网络迁移所有文件。将文档上传到 S3bucket，并设置生命周期策略，将数据移动到 Glacier 进行存档。

C、建立直接连接，将本地网络集成到 VPC。

上传 Amazon EBS 卷上的文档，并使用生命周期策略自动将 EBS 快照移动到 S3 存储桶，然后再移动到 Glacier 进行存档。

D、启动一个新的磁带网关，使用 AWS 存储网关连接到本地数据中心。将文档上传到磁带网关，并设置生命周期策略以将数据移动到 Glacier 中存档。

答:

分析:

文件网关支持到 Amazon 简单存储服务（Amazon S3）的文件接口，并将服务和虚拟软件设备结合起来。通过使用这种组合，您可以使用行业标准文件协议（如网络文件系统（NFS）和服务器消息块（SMB））在 Amazon S3 中存储和检索对象。软件设备或网关作为运行在 VMware ESXi、Microsoft Hyper-V 或基于 Linux 内核的虚拟机（KVM）管理程序上的虚拟机部署到本地环境中。

网关提供对 S3 中作为文件或文件共享挂载点的对象的访问。使用文件网关，您可以执行以下操作：

- 您可以使用 NFS 版本 3 或 1 协议直接存储和检索文件。
- 您可以使用 SMB 文件系统版本 2 和 3 协议直接存储和检索文件。
- 您可以从任何 AWS 云应用程序或服务直接访问 Amazon S3 中的数据。
- 您可以使用生命周期策略、跨区域复制和版本控制来管理 Amazon S3 数据。您可以将文件网关视为 S3 上的文件系统挂载。AWS 存储网关支持亚马逊 S3 标准、亚马逊 S3 非频繁访问标准、亚马逊单一区域非频繁访问和亚马逊冰川存储类。创建或更新

在文件共享中，您可以选择对象的存储类。您可以选择 Amazon S3 标准或任何不经常访问的存储类，如 S3 标准 IA 或 S3 One Zone IA。存储在任何存储类中的对象都可以使用生命周期策略转换到 Amazon Glacier。

虽然您可以将对象直接从文件共享写入 S3 标准 IA 或 S3 One Zone IA 存储类，但建议您使用生命周期策略来转换对象，而不是直接从文件分享写入，尤其是如果您希望在存档对象后 30 天内更新或删除该对象。因此，正确答案是：启动一个新的文件网关，使用 AWS 存储网关连接到本地数据中心。将文档上传到文件网关，并设置生命周期策略，将数据移动到 Glacier 进行数据存档。

选项显示：启动一个新的磁带网关，使用 AWS 存储网关连接到本地数据中心。将文档上传到磁带网关并设置生命周期策略以将数据移动到 Glacier 进行存档是不正确的，因为尽管磁带网关在 Amazon Glaciers 中提供了经济高效且持久的存档备份数据，但它不符合在几分钟内立即检索的标准。它也不维护本地缓存，以提供对最近访问的数据的低延迟访问，并减少数据出口费用。因此，最好还是设置文件网关。

该选项表示：建立直接连接，将本地网络集成到 VPC。将文档上传到 Amazon EBS 卷上，并使用生命周期策略自动将 EBS 快照移动到 S3 存储桶，然后再移动到 Glacier 进行存档。这是不正确的，因为 EBS 卷与 S3 相比不耐用，如果您直接将文档存储到 S3 存储桶中，成本效率会更高。另一种解决方案是使用 AWS Direct Connect 和 AWS Storage Gateway 为高吞吐量工作负载需求创建连接，从而在本地文件网关和 AWS 之间提供专用网络连接。但是这个解决方案使用 EBS，因此，这个选项仍然是错误的。选项显示：使用 AWS Snowmobile 从内部网络迁移所有文件。将文档上传到 S3 存储桶并设置生命周期策略以将数据移动到 Glacier 进行存档是不正确的，因为 Snowmobile 主要用于将内部数据中心的整个数据迁移到 AWS。这不是一种合适的方法，因为该公司仍然采用混合云架构，这意味着他们将继续使用其内部数据中心以及 AWS 云基础设施。

参考文献:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/object-lifecycle-mgmt.html>

<https://docs.aws.amazon.com/storagegateway/latest/userguide/StorageGatewayConcepts.html> 查看此 Amazon S3 备

忘单: <https://tutorialsdojo.com/amazon-s3/>

Dojo 的 AWS 认证解决方案架构师助理考试学习指南教程: <https://tutorialsdojo.com/aws-certified-solutions-architect-associate-saa-c02/>

Q122. 一个 web 应用程序使用 CloudFront 将存储在 S3 存储桶中的图像、视频和其他静态内容分发给世界各地的用户。该公司最近推出了一种新的仅限会员访问其部分高质量媒体文件的方式。需要仅向其付费订户提供对多个私有媒体文件的访问,而无需更改其当前 URL。以下哪一项是您应该实现以满足此需求的最合适的解决方案?

- A、 将 CloudFront 分发版配置为使用匹配查看器作为其原始协议策略,该策略将自动匹配用户请求。如果请求是付费会员,则允许访问私人内容,如果不是会员,则拒绝访问。
- B、 使用自定义策略创建签名 URL,该策略仅允许成员查看私有文件。
- C、 配置 CloudFront 发行版以使用字段级加密来保护您的私有数据,并仅允许访问成员。
- D、 通过修改您的应用程序以确定用户是否应该访问您的内容,使用签名 Cookie 来控制谁可以访问 CloudFront 分发版中的私人文件。对于成员,将所需的 Cookie 头发送给查看器,查看器将仅对其解锁内容。

答案 D

分析:

CloudFront 签名 URL 和签名 Cookie 提供相同的基本功能:它们允许您控制谁可以访问您的内容。如果您希望通过 CloudFront 提供私人内容,并且您正在尝试决定是否使用签名 URL 或签名 Cookie,请考虑以下事项:

在以下情况下使用签名 URL:

- 您希望使用 RTMP 发行版。RTMP 发行版不支持签名 Cookie。
- 您希望限制对单个文件的访问,例如,应用程序的安装下载。
- 您的用户正在使用不支持 Cookie 的客户端(例如,自定义 HTTP 客户端)。在以下情况下使用签名 cookie:
- 您希望提供对多个受限文件的访问,例如,HLS 格式的视频的所有文件或网站订阅者区域中的所有文件。
- 您不想更改当前的 URL。

因此,该场景的正确答案是这样一个选项:使用签名 cookie,通过修改应用程序来确定用户是否应该访问您的内容,从而控制谁可以访问 CloudFront 分发版中的私有文件。对于成员,将所需的 Cookie 头发送给查看器,查看器将仅对其解锁内容。该选项表示:配置 CloudFront 发行版以使用匹配查看器作为其原始协议策略,该策略将自动匹配用户请求。如果请求是付费成员,则允许访问私有内容,如果不是成员,则拒绝访问。这是不正确的,因为匹配查看器是一种源协议策略,它将 CloudFront 配置为使用 HTTP 或 HTTPS 与源站通信,具体取决于查看器请求的协议。CloudFront 仅缓存对象一次,即使查看者使用 HTTP 和 HTTPS 协议发出请求。“使用自定义策略创建签名 URL,该策略只允许成员查看私有文件”选项不正确,因为签名 URL 主要用于提供对单个文件的访问,如以上说明所示。此外,该场景明确表示他们不想更改当前的 URL,这就是为什么实现签名 Cookie 比签名 URL 更合适的原因。选项显示:配置

CloudFront 发行版使用字段级加密来保护您的私人数据，只允许访问成员，这是不正确的，因为字段级加密只允许您安全地将用户提交的敏感信息上载到 web 服务器。它不提供下载多个私人文件的访问。

参考：

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-choosing-signed-cookies.html>

查看此 Amazon CloudFront 备忘单：

<https://tutorialsdojo.com/amazon-cloudfront/>

Q123. 一家公司在自动扩展的 EC2 实例组中托管其 web 应用程序

负载均衡器的应用。最近，解决方案架构师发现了一系列针对应用程序的 SQL 注入尝试和跨站点脚本攻击，这对他们的生产数据产生了不利影响。架构师应该实现以下哪项来减轻这种攻击？

- A、使用 AWS 防火墙管理器，设置阻止 SQL 注入和跨站点脚本攻击的安全规则。将规则与应用程序负载均衡器关联。
- B、使用 Amazon GuardDuty 防止应用程序中的任何进一步 SQL 注入和跨站点脚本攻击。
- C、设置安全规则，阻止 AWS Web 应用程序防火墙（WAF）中的 SQL 注入和跨站点脚本攻击。将规则与应用程序负载均衡器关联。
- D、使用 NetworkAccess 控制列表阻止 SQL 注入和跨站点脚本攻击起源的所有 IP 地址。

答案 C

分析：

AWS WAF 是一个 web 应用程序防火墙，允许您监控转发到 Amazon API 网关 API、Amazon CloudFront 或应用程序负载均衡器的 HTTP 和 HTTPS 请求。AWS WAF 还允许您控制对内容的访问。根据您的指定条件，例如请求源的 IP 地址或查询字符串的值，API 网关、CloudFront 或应用程序负载均衡器使用请求的内容或 HTTP 403 状态代码（禁止）响应请求。您还可以将 CloudFront 配置为在请求被阻止时返回自定义错误页面。

在最简单的层面上，AWS WAF 允许您选择以下行为之一：

是否允许除您指定的请求之外的所有请求？当您希望 CloudFront 或应用程序负载均衡器为公共网站提供内容时，这非常有用，但您也希望阻止来自攻击者的请求。

是否阻止除您指定的请求之外的所有请求？当您希望为受限网站提供内容时，这非常有用，该网站的用户可以通过 web 请求中的属性（例如他们用于浏览网站的 IP 地址）轻松识别。

对与指定属性匹配的请求进行计数？当您希望基于 web 请求中的新属性允许或阻止请求时，您首先可以配置 AWS WAF 来计算匹配这些属性的请求，而不允许或阻止这些请求。这可以让您确认您没有意外

配置 AWS WAF 以阻止您网站的所有流量。如果确信指定了正确的属性，则可以更改行为以允许或阻止请求。因此，该场景中的正确答案是：设置安全规则，阻止 AWS Web 应用程序防火墙（WAF）中的 SQL 注入和跨站点脚本攻击。将规则与应用程序负载均衡器关联。

使用 Amazon GuardDuty 来防止应用程序中的任何进一步 SQL 注入和跨站点脚本攻击是不正确的，因为 Amazon GuardDuty 只是一种威胁检测服务，它持续监控恶意活动和未授权行为，以保护您的 AWS 帐户和工作负载。使用 AWS 防火墙管理器设置阻止 SQL 注入和跨站点脚本攻击的安全规则，然后将规则关联到应用程序

负载均衡器是不正确的，因为 AWS 防火墙管理员只是简化了 AWS WAF 和 AWS Shield 跨多个帐户和资源的高级管理和维护任务。

使用网络访问控制列表阻止 SQL 注入和跨站点脚本攻击起源的所有 IP 地址是不正确的，因为这是 VPC 的可选安全层，用作控制进出一个或多个子网流量的防火墙。NACL 无法有效阻止 SQL 注入和跨站点脚本攻击

参考文献：

<https://aws.amazon.com/waf/> <https://docs.aws.amazon.com/waf/latest/developerguide/what-is-aws-waf.html> 查看

AWS WAF 备忘单：

<https://tutorialsdojo.com/aws-waf/>

AWS 安全服务概述-WAF、Shield、CloudHSM、KMS： <https://www.youtube.com/watch?v=-1SRdeAmMo>

Q124. 保险公司将 SAP HANA 用于其日常 ERP 运营。由于客户偏好，他们无法迁移该数据库，因此需要将其与 VPC 中的当前 AWS 工作负载集成，在 VPC 中，他们需要建立站点到站点的 VPN 连接。需要在 VPC 之外配置什么，才能成功实现站点到站点的 VPN 连接？

- A、 虚拟专用网关的 EIP
- B、 VPC 中用于通过 NAT 实例路由流量的主路由表
- C、 公共子网中的专用 NAT 实例
- D、 内部网络客户网关外部接口的互联网可路由 IP 地址（静态）

答案 D

分析：

默认情况下，您启动到虚拟私有云（VPC）中的实例无法与您自己的网络通信。通过将虚拟专用网关连接到 VPC、创建自定义路由表、更新安全组规则以及创建 AWS 管理的 VPN 连接，您可以从 VPC 访问网络。

尽管术语 VPN 连接是一个通用术语，但在亚马逊专有网络文档中，VPN 连接指的是专有网络和您自己的网络之间的连接。AWS 支持互联网协议安全（IPsec）VPN 连接。

客户网关是 VPN 连接一侧的物理设备或软件应用程序。要创建 VPN 连接，必须在 AWS 中创建客户网关资源，该资源向 AWS 提供有关客户网关设备的信息。接下来，您必须设置客户网关外部接口的 Internet 可路由 IP 地址（静态）。下图说明了单个 VPN 连接。VPC 有一个连接的虚拟专用网关，您的远程网络包括一个客户网关，您必须将其配置为启用 VPN 连接。您设置了路由，以便将来自 VPC 绑定到网络的任何流量路由到虚拟专用网关。

说：公共子网中的专用 NAT 实例和 VPC 中的主路由表通过 NAT 实例路由流量的选项是不正确的，因为您不需要 NAT 实例来创建 VPN 连接。

虚拟专用网关的 EIP 不正确，因为您没有将 EIP 连接到 VPG。

参考文献：

https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html

<https://docs.aws.amazon.com/vpc/latest/userguide/SetUpVPNConnections.html> 查看此亚马逊 VPC 备忘单：

<https://tutorialsdojo.com/amazon-vpc/>

Q125. 一家公司有一个数据分析应用程序，用于更新实时外汇仪表盘，另一个独立应用程序将数据存档到亚马逊红移。两个应用程序都配置为通过使用 Amazon Kinesis 数据流同时独立地使用来自同一流的数据。然而，他们注意到，在很多情况下，碎片迭代器会意外地过期。经过检查，他们发现 Kinesis 使用的 DynamoDB 表没有足够的容量来存储租赁数据。

以下哪种解决方案最适合纠正此问题？

- A、使用亚马逊 Kinesis 数据分析来正确支持数据分析应用程序，而不是 Kinesis DataStream。
- B、升级 DynamoDB 表的存储容量。
- C、增加分配给碎片表的写入容量。
- D、使用 DynamoDB 加速器（DAX）启用内存加速。

答案 C

分析：

每个 GetRecords 请求都会返回一个新的 shard 迭代器（作为 NextShardIterator），然后在下一个 GetRecords 要求中使用它（作为 ShardIterator）。通常，这个碎片迭代器在使用之前不会过期。但是，您可能会发现碎片迭代器过期，因为您调用 GetRecords 的时间超过 5 分钟，或者因为您重新启动了消费者应用程序。如果碎片迭代器在您使用之前立即到期，这可能表明 Kinesis 使用的 DynamoDB 表没有足够的容量来存储租约数据。如果有大量碎片，这种情况更可能发生。要解决此问题，请增加分配给碎片表的写入容量。

因此，增加分配给碎片表的写入容量是正确答案。升级 DynamoDB 表的存储容量是不正确的，因为 DynamoDB 是一个完全受管理的服务，可以自动扩展其存储，而无需手动设置。该场景指的是碎片表的写入容量，因为它表示 Kinesis 使用的 DynamoDB 表没有足够的容量来存储租赁数据。

使用 DynamoDB 加速器（DAX）启用内存加速是不正确的，因为 DAX 功能主要用于从毫秒响应时间到微秒提高 DynamoDB 表的读取性能。在这种情况下，它与 Amazon Kinesis 数据流没有任何关系。使用亚马逊 Kinesis 数据分析来正确支持数据分析应用程序而不是 Kinesis 的数据流是不正确的。尽管 Amazon Kinesis 数据分析可以支持数据分析应用程序，但它仍然不是解决此问题的合适解决方案。您只需增加分配给 shard 表的写入容量即可纠正问题，这就是为什么不需要切换到 Amazon Kinesis 数据分析。

参考：

[https://docs.aws.amazon.com/streams/latest/dev/kinesis-record-processor-](https://docs.aws.amazon.com/streams/latest/dev/kinesis-record-processor-ddb.html)

[ddb.htmlhttps://docs.aws.amazon.com/streams/latest/dev/troubleshooting-consumers.html](https://docs.aws.amazon.com/streams/latest/dev/troubleshooting-consumers.html) 查看此亚马逊 Kinesis 备忘单：<https://tutorialsdojo.com/amazon-kinesis/>

Q126. 世界各地的客户使用的 web 应用程序托管在经典负载均衡器后面的 EC2 实例自动扩展组中。您需要通过允许多个域在同一 IP 地址上提供 SSL 通信来保护应用程序。

为了满足上述要求，您应该执行以下哪项操作？

- A、使用弹性 IP 并使用 AWS CertificateManager 将多个第三方证书上传到您的经典负载均衡器中。
- B、通过将多个 SSL 证书添加到允许多个域以服务 SSL 流量，在您的经典负载均衡器上使用服务器名称指示（SNI）。

C、使用 AWS 证书管理器生成 SSL 证书并创建 CloudFront web 分发。将证书与 web 分发版关联，并启用对服务器名称指示（SNI）的支持。

D、在 AWS 中，不可能允许多个域通过同一 IP 地址提供 SSL 通信

答案 C

分析：

Amazon CloudFront 从每个边缘位置提供您的内容，并提供与专用 IP 相同的安全性

自定义 SSL 功能。SNI 自定义 SSL 适用于大多数现代浏览器，包括 Chrome 版本 6 及更高版本（在 Windows XP 及更高或 OS X 10.5.7 及更高的版本上运行）、Safari 版本 3 及更高（在 Windows Vista 及更高版或 Mac OS X 10.5.6 及更高级版本上运行），Firefox 2.0 及更高，以及 Internet Explorer 7 及更高级（运行在 Windows Vista 和更高版本上）。某些用户可能无法访问您的内容，因为一些较旧的浏览器不支持 SNI，并且无法与 CloudFront 建立连接以加载您内容的 HTTPS 版本。如果您需要支持 HTTPS 内容的非 SNI 兼容浏览器，建议使用专用 IP 自定义 SSL 功能。

通过添加多个 SSL 证书在经典负载均衡器上使用服务器名称指示（SNI）以允许多个域为 SSL 流量提供服务是不正确的，因为经典负载均衡器不支持服务器名称指示。您必须使用应用程序负载均衡器或 CloudFrontWeb 发行版来支持 SNI 功能。

使用弹性 IP 并使用 AWS 在应用程序负载均衡器中上传多个第三方证书

证书管理器是不正确的，因为与上面一样，经典负载均衡器不支持服务器名称指示（SNI），并且使用弹性 IP 不是允许多个域服务 SSL 流量的合适解决方案。您必须使用服务器名称指示（SNI）。“不可能允许多个域通过 AWS 中的同一 IP 地址提供 SSL 流量”选项不正确，因为 AWS 支持使用服务器名称指示（SNI）。参考文献：

<https://aws.amazon.com/about-aws/whats-new/2014/03/05/amazon-cloudfront-announces-sni-custom-ssl/>

[https://aws.amazon.com/blogs/security/how-to-help-achieve-mobile-app-transport-security-compliance-by-使用Amazon cloudfront 和 aws 证书管理器/](https://aws.amazon.com/blogs/security/how-to-help-achieve-mobile-app-transport-security-compliance-by-使用Amazon-cloudfront和aws证书管理器/)

查看此 Amazon CloudFront 备忘单：

<https://tutorialsdojo.com/amazon-cloudfront/>

SNI 自定义 SSL vs 专用 IP 自定义 SSL：

[https://tutorialsdojo.com/sni-custom-ssl-vs-dedicated-ip-custom-ssl/AWS 安全服务概述-机密管理器、](https://tutorialsdojo.com/sni-custom-ssl-vs-dedicated-ip-custom-ssl/AWS安全服务概述-机密管理器、)

ACM、Macie： <https://www.youtube.com/watch?v=ogVamzF2Dzk>

Q127.一家公司在同一可用性区域的虚拟私有云中两个按需 EC2 实例，但部署到不同的子网。一个 EC2 实例运行数据库，另一个 EC1 实例运行与数据库连接的 web 应用程序。您需要确保这两个实例可以

相互通信，使系统正常工作。为了使这些 EC2 实例能够在 VPC 内部通信，您必须检查哪些事项？（选择两个。）

A、确保 EC2 实例位于同一放置组中。

B、检查是否所有安全组都设置为允许应用程序主机通过正确的端口和协议与数据库通信。

C、检查两个实例是否为同一实例类。

D、检查是否将默认路由设置为 NAT 实例或 Internet 网关（IGW），以便它们进行通信。

E、检查网络 ACL 是否允许两个子网之间的通信。

答案是

分析：

首先，应正确设置网络 ACL，以允许两个子网之间的通信。还应正确配置安全组，以便 web 服务器可以与数据库服务器通信。

因此，以下是正确答案：

检查是否已将所有安全组设置为允许应用程序主机通过正确的端口和协议与数据库通信。

检查网络 ACL 是否允许两个子网之间的通信。如果两个实例都是同一个实例类，则表示“检查”的选项不正确，因为 EC2 实例不需要属于同一个类才能相互通信。

“检查默认路由是否设置为 NAT 实例或互联网网关（IGW）以供其通信”选项不正确，因为互联网网关主要用于与互联网通信。“确保 EC2 实例位于同一放置组中”选项是不正确的，因为放置组主要用于提供紧密耦合的节点到节点通信所需的低延迟网络性能。

参考：

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html 查看此亚马逊 VPC 备忘单：

<https://tutorialsdojo.com/amazon-vpc/>

Dojo 的 AWS 认证解决方案架构师助理考试学习指南教程：<https://tutorialsdojo.com/aws-certified-solutions-architect-associate/>

Q128.作为贵公司业务连续性计划的一部分，您的 IT 主管指示您尽快为 EC2 实例设置所有 EBS 卷的自动备份。自动备份所有 EBS 卷的最快、最经济高效的解决方案是什么？

A、使用 Amazon 数据生命周期管理器（Amazon DLM）自动创建 EBS 快照。

B、将您的 Amazon 存储网关设置为 EBS 卷作为数据源，并通过存储网关将备份存储在 PremiseServer 中。

C、使用 Amazon S3 中的 EBS 周期策略自动备份 EBS 卷。

D、对于自动化解决方案，创建一个调度作业，该作业通过 AWS CLI 调用“创建快照”命令，定期拍摄生产 EBS 卷的快照。

答：

分析：

您可以使用 Amazon Data Lifecycle Manager（Amazon DLM）自动创建、保留和删除用于备份 Amazon EBS 卷的快照。自动化快照管理可帮助您：

- 通过强制执行定期备份计划来保护有价值的数据。
- 根据审计员或内部合规部的要求保留备份。
- 通过删除过时的备份来降低存储成本。

结合 Amazon CloudWatch 事件和 AWS CloudTrail 的监控功能，Amazon DLM 为 EBS 卷提供了一个完整的备份解决方案，无需额外成本。因此，使用 Amazon Data Lifecycle Manager（Amazon DLM）自动创建 EBS 快照是正确答案，因为它是最快、最具成本效益的解决方案，提供了一种自动备份 EBS 卷的方法。

对于自动解决方案，创建一个通过 AWS CLI 调用“create-snapshot”命令以定期拍摄生产 EBS 卷快照的计划作业是不正确的，因为即使这是一个有效的解决方案，您仍然需要额外的时间来创建一个调用“createsnapshop”命令的计划作业。最好使用 Amazon Data Lifecycle Manager（Amazon DLM），因为它为您提供了最快的解决方案，使您能够自动创建、保留和删除 EBS 快照，而无需编写自定义 shell 脚本或创建计划作业。将您的 Amazon 存储网关设置为 EBS 卷作为数据源，并通过存储网关将备份存储在本地服务器中，这与 Amazon 存储不正确 Gateway 仅用于从本地服务器创建数据备份，而不是从 Amazon 虚拟私有云创建数据备份。

在 Amazon S3 中使用 EBS 周期策略自动备份 EBS 卷是不正确的，因为在 Amazon S3 中没有 EBS 周期政策。

参考文献：

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/snapshot-lifecycle.html>
<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-creating-snapshot.html> 查看此亚马逊 EBS 备忘单：

<https://tutorialsdojo.com/amazon-ebs/> 亚马逊 EBS 概述-

SSD 与

HDD： <https://www.youtube.com/watch?v=LW7x8wyLFv>

w&t=8s

Q129.由 HTML、CSS 和其他客户端 Javascript 组成的网站将托管在 AWS 环境中。网页上将显示多幅高分辨率图像。网站和照片应尽可能具有最佳的加载响应时间，并应能够扩展到高请求率。

以下哪种体系结构可以提供最具成本效益和最快的加载体验？

A、使用具有预先配置的 Apache web 服务器的 AMI 启动自动扩展组，然后相应地配置扩展策略。将图像存储在弹性块存储器中。然后，将实例的端点指向 AWS 全局加速器。

B、在 Amazon LightSail 实例中创建一个 Nginx web 服务器，以托管 HTML、CSS 和 Javascript 文件，然后启用缓存。上传 S3 存储桶中的图像。使用 CloudFront 作为 CDN，将图像更贴近终端用户。C、将

HTML、CSS、Javascript 和图像上传到单个 bucket 中。然后启用网站托管。

创建 CloudFront 分发并将域指向 S3 网站端点。

D、在 EC2 实例中创建一个 Nginx web 服务器，托管 HTML、CSS 和 Javascript 文件，然后启用缓存。上传 S3 存储桶中的图像。使用 CloudFront 作为 CDN，将图像更贴近终端用户。

答案 C

分析：

Amazon S3 是一种对象存储服务，提供业界领先的可扩展性、数据可用性、安全性和性能。此外，您可以使用 Amazon S3 来托管静态网站。在静态网站上，单个网页包括静态内容。Amazon S3 具有高度的可扩展性，您只需支付所使用的费用，您可以从小处开始，并根据自己的意愿扩展应用程序，而不会影响性能或可靠性。

Amazon CloudFront 是一种快速内容交付网络（CDN）服务，它以低延迟、高传输速度向全球客户安全地交付

数据、视频、应用程序和 API。CloudFront 可以与 Amazon S3 集成，以便将来自 S3 存储桶的数据快速交付给最终用户。从设计上讲，从 CloudFront 交付数据比从 S3 直接向用户交付数据更具成本效益。

给出的场景分别是关于存储和托管图像和静态网站。由于我们只是处理静态内容，我们可以利用 S3 的 web 托管功能。然后我们可以通过将其与 CloudFront 集成来进一步改进架构。这样，用户将能够更快地加载网页和图像，而不是从标准的 web 服务器上加载。因此，正确的答案是：在单个 bucket 中上传 HTML、CSS、Javascript 和图像。然后启用网站托管。创建 CloudFront 分发并将域指向 S3 网站端点。该选项表示：在 EC2 实例中创建一个 Nginx web 服务器，以托管 HTML、CSS 和 Javascript 文件，然后启用缓存。上传 S3 存储桶中的图像。使用 CloudFront 作为 CDN 来提供更接近最终用户的图像是不正确的。创建自己的 web 服务器只是为了在 AWS 中托管静态网站，这是一个成本高昂的解决方案。EC2 实例上的 Web 服务器通常用于托管动态 Web 应用程序。由于静态网站包含具有固定内容的网页，我们应该使用 S3 网站托管。

该选项表示：使用具有预先配置的 Apache web 服务器的 AMI 启动自动扩展组，然后相应地配置扩展策略。将图像存储在弹性块存储中。然后，将实例的端点指向 AWS 全局加速器是不正确的。这就是我们过去为静态网站提供服务的方式。现在，借助 S3 网站托管，我们可以在一个持久、高可用性和高度可扩展的环境中托管静态内容，而无需管理任何服务器。在 S3 中托管静态网站比在 EC2 实例中托管更便宜。此外，使用 ASG 扩展承载静态网站的实例是一个过度设计的解决方案，会带来不必要的成本。S3 自动扩展到高请求，您只需支付您使用的费用。

该选项表示：在 Amazon LightSail 实例中创建一个 Nginx web 服务器，以托管 HTML、CSS 和 Javascript 文件，然后启用缓存。上传 S3 存储桶中的图像。使用 CloudFront 作为 CDN 来提供更接近最终用户的图像是不正确的，因为尽管 LightSail 比 EC2 便宜，但与在 S3 上托管相比，创建自己的 LightSail web 服务器来托管静态网站仍然是一个相对昂贵的解决方案。此外，S3 自动扩展到高请求率。

Q130.您已经构建了一个 web 应用程序，每小时检查一次 S3 bucket 中的新项目。如果存在新项，则将消息添加到 SQS 队列中。您有一组 EC2 实例，它们从 SQS 队列中检索消息，处理文件，最后向您和用户发送一封电子邮件，确认项目已成功处理。您的同事将一个测试文件上传到 S3 bucket，几个小时后，您注意到您和您的同事收到了 50 封来自您应用程序的邮件，其中包含相同的消息。以下哪项最可能是应用程序向您和用户发送多封电子邮件的根本原因？

- A、应用程序中有一个错误。
- B、默认情况下，SQS 会自动删除消费者处理的消息。您的同事可能已经提交了 50 次请求，这就是您收到大量电子邮件的原因。
- C、SQS 队列的 `sqsSendMessage` 属性配置为 50
- D、您的应用程序在处理消息后不会向 SQS 队列发出删除命令，这就是为什么该消息返回队列并被多次处理的原因。

答案 D

分析：

在这种情况下，主要原因是您的应用程序在处理消息后没有向 SQS 队列发出删除命令，这就是为什么该消息返回队列并被多次处理的原因。

表示：SQS 队列的 `sqsSendMessage` 属性配置为 50 的选项不正确，因为 SQS 中没有 `sqsSendMessage` 属性。

表示：应用程序中存在错误的选项是一个有效答案，但由于场景中没有提到 EC2 实例删除了已处理的消息，因此问题最可能的原因是应用程序没有向 SQS 队列发出删除命令，如上所述。该选项表示：默认情况下，SQS 自动删除消费者处理的消息。您的同事可能已经提交了请求

50 次，这就是为什么你收到了很多电子邮件是不正确的，因为 SQS 不会自动删除邮件。

参考：<https://aws.amazon.com/sqs/faqs/>

查看此亚马逊 SQS 备忘单：

<https://tutorialsdojo.com/amazon-sqs/>

Q131.网络架构师开发了一个食品订购应用程序。架构师需要检索 EC2 服务器的实例 ID、公钥和公共 IP 地址，用于将属性标记和分组到本地运行的内部应用程序中。

以下哪个选项符合此要求？

- A、 亚马逊机器图像
- B、 实例用户数据
- C、 资源标签
- D、 实例元数据

答案 D

分析：

实例元数据是有关实例的数据，可用于配置或管理正在运行的实例。您可以从实例元数据中获取实例 ID、公钥、公共 IP 地址和许多其他信息，方法是在实例中向该 URL 发送 URL 命令：

<http://169.254.169.254/latest/meta-data/>

实例用户数据不正确，因为它主要用于执行常见的自动配置任务，并在实例启动后运行脚本。

资源标记不正确，因为这些是您分配给 AWS 资源的标签。每个标记由一个键和一个可选值组成，这两个值都由您定义。

Amazon 机器映像不正确，因为它主要提供启动实例所需的信息，该实例是云中的虚拟服务器。

参考：

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-metadata.htm> 亚马逊 EC2 概述：

https://www.youtube.com/watch?v=7VsGIHT_jQE

查看此 Amazon EC2 备忘单：

<https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/Dojo> 的 AWS 认证解决方案架构师助理考试学习指南教程：

<https://tutorialsdojo.com/aws-certified-solutions-architect-associate-saa-c02/>

Q132.在 AWS 中设计云架构需要 DevOps 工程师。工程师计划开发一个高可用性和容错架构，该架构由弹性负载均衡器和跨多个可用性区域部署的 EC2 实例的自动扩展组组成。这将由在线计费应用程序使用，该应用程序需要基于路径的路由、基于主机的路由和使用 WebSocket 的双向通信信道。

哪种类型的弹性负载均衡器最适合满足给定要求？

- A、网关负载均衡器
- B、网络负载均衡器
- C、负载均衡器的应用
- D、经典负载均衡器

答案 C

分析：

应用程序负载均衡器在请求级别（第 7 层）运行，根据请求内容将流量路由到目标（EC2 实例、容器、IP 地址和 Lambda 函数）。应用程序负载均衡器是 HTTP 和 HTTPS 流量高级负载均衡的理想选择，它提供了针对现代应用程序架构（包括微服务和基于容器的应用程序）交付的高级请求路由。应用程序负载均衡器通过确保始终使用最新的 SSL/TLS 密码和协议，简化并提高了应用程序的安全性。如果应用程序由多个单独的服务组成，则应用程序负载均衡器可以根据请求的内容（如主机字段、路径 URL、HTTP 头、HTTP 方法、查询字符串或源 IP 地址）将请求路由到服务。

基于主机的路由：您可以根据 HTTP 头的主机字段路由客户端请求，从而允许您从同一负载均衡器路由到多个域。基于路径的路由：您可以根据 HTTP 头的 URL 路径路由客户端请求。基于 HTTP 头的路由：您可以根据任何标准或自定义 HTTP 头的值路由客户端请求。

基于 HTTP 方法的路由：您可以基于任何标准或自定义 HTTP 方法路由客户端请求。

基于查询字符串参数的路由：您可以基于查询字符串或查询参数路由客户端请求。

基于源 IP 地址 CIDR 的路由：您可以根据源 IP 地址的 CIDR 来路由客户端请求，该源 IP 地址是请求发出的来源。

应用程序负载均衡器支持基于路径的路由、基于主机的路由以及对容器化应用程序的支持，因此，应用程序负载均衡器是正确答案。网络负载均衡器不正确。尽管它可以处理 WebSocket 连接，但它不支持基于路径的路由或基于主机的路由，这与应用程序负载均衡器不同。

经典负载均衡器是不正确的，因为这种类型的负载均衡器仅适用于在 EC2 经典网络中构建的应用程序。CLB 不支持基于路径的路由或基于主机的路由。网关负载均衡器不正确，因为它主要用于部署、扩展和运行第三方虚拟设备。它没有基于路径的路由或基于主机的路由功能。

参考文献：

<https://aws.amazon.com/elasticloadbalancing/features>

<https://aws.amazon.com/elasticloadbalancing/faqs/>

AWS 弹性负载均衡概述：

<https://youtu.be/UBl5dw59DO8>

查看 AWS 弹性负载均衡（ELB）备忘单：

<https://tutorialsdojo.com/aws-elastic-load-balancing-elb/>

应用程序负载均衡器 vs 网络负载均衡器 vs Classic 负载均衡器: <https://tutorialsdojo.com/application-load-balancer-vs-network-load-balancer-vs-classic-load-balancer/>

Q133.软件公司的资源托管在 AWS 和内部服务器上。我们要求您为使用这两种资源的应用程序创建一个解耦的体系结构。以下哪个选项有效？（选择两个。）

- A、使用 SWF 为解耦应用程序利用本地服务器和 EC2 实例
- B、使用 SQS 为您的去耦应用程序利用本地服务器和 EC2 实例
- C、使用 RDS 为您的解耦应用程序利用本地服务器和 EC2 实例
- D、使用 DynamoDB 为您的解耦应用程序利用本地服务器和 EC2 实例
- E、使用 VPC 对等连接本地服务器和去耦应用程序的 EC2 实例

回答 AB

分析:

Amazon 简单队列服务（SQS）和 Amazon 简单工作流服务（SWF）是可用于在 AWS 中创建解耦架构的服务。解耦体系结构是一种计算体系结构，它使计算组件或层能够独立执行，同时仍然相互连接。

Amazon SQS 提供可靠、高度可扩展的托管队列，用于在应用程序或微服务之间传输消息时存储消息。

Amazon SQS 允许您在分布式应用程序组件之间移动数据，并帮助您解耦这些组件。Amazon SWF 是一个 web 服务，它使

跨分布式应用程序组件协调工作。使用 RDS 为您的去耦应用程序同时使用本地服务器和 EC2 实例，使用 DynamoDB 为您的去耦应用程序同时利用本地服务器和 EC2 实例是不正确的，因为 RDS 和 DynamoDB 是数据库服务。

使用 VPC 对等连接本地服务器和分离应用程序的 EC2 实例是不正确的，因为您无法为本地网络和 AWS VPC 创建 VPC 对等。

参考文献:

<https://aws.amazon.com/sqs/>

<http://docs.aws.amazon.com/amazonswf/latest/developerguide/swf-welcome.html> 查看此亚马逊 SQS 备忘单:

<https://tutorialsdojo.com/amazon-sqs/>

亚马逊简单工作流（SWF）vs AWS 步骤功能 vs 亚马逊 SQS:

<https://tutorialsdojo.com/amazon-simple-workflow-swf-vs-aws-step-functions-vs-amazon-sqs/AWS> 服务备忘单比较: <https://tutorialsdojo.com/comparison-of-aws-services/>

Q134. 一家公司开发了一个膳食规划应用程序，提供一周的膳食建议以及用户的食物消费。应用程序驻留在 EC2 实例上，需要访问各种 AWS 服务以进行日常操作。以下哪项是允许 EC2 实例访问 S3 bucket 和其他 AWS 服务的最佳方式？

- A、在安全组中添加 API 凭据并将其分配给 EC2 实例。
- B、将 API 凭据存储在 bastion 主机中。
- C、在 IAM 中创建一个角色并将其分配给 EC2 实例。
- D、将 API 凭据存储在 EC2 实例中。

答案 C

分析：

处理 API 凭据的最佳实践是在身份访问管理（IAM）服务中创建新角色，然后将其分配给特定的 EC2 实例。这样，您就有了一种安全、集中的方式来存储和管理凭据。

在 EC2 实例中存储 API 凭据、在安全组中添加 API 凭据并将其分配给 EC2 实例以及在 bastion 主机中存储 API 凭证是不正确的，因为存储或使用来自 EC2 实例的 API 凭据不安全。您应该改用 IAM 服务。

参考：

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html> 查看此 AWS IAM 备忘单：<https://tutorialsdojo.com/aws-identity-and-access-management-iam/>

Q135. 一个组织在其内部数据中心存储和管理各公司的财务记录，该中心几乎没有空间。管理层决定将所有现有记录转移到云存储服务。所有未来的财务记录也将存储在云中。为了增加安全性，必须防止删除或覆盖所有记录。为了满足上述要求，您应该执行以下哪项操作？

- A、使用 AWS 数据同步来移动数据。将所有数据存储在 Amazon EFS 中并启用对象锁定。
- B、使用 AWS 存储网关建立混合云存储。将所有数据存储在 Amazon S3 中并启用 objectlock。
- C、使用 AWS 存储网关建立混合云存储。将所有数据存储在 Amazon EBS 和 enableobject lock 中。
- D、使用 AWS 数据同步来移动数据。将所有数据存储在 Amazon S3 中并启用对象锁定。

答案 D

分析：

AWS DataSync 允许您复制包含数百万文件的大型数据集，而无需使用开源工具构建自定义解决方案，或许可和管理昂贵的商业网络加速软件。您可以使用 DataSync 将活动数据迁移到 AWS，将数据传输到云以进行分析和处理，归档数据以释放本地存储容量，或将数据复制到 AWS 以实现业务连续性。

AWS 数据同步使您能够将本地数据迁移到 Amazon S3、Amazon EFS 和 Amazon FSx for Windows 文件服务器。您可以配置 DataSync 来创建整个数据集的初始副本，并计划

随后向 Amazon S3 增量传输不断变化的数据。启用 S3 对象锁定可防止现有和未来记录被删除或覆盖。AWS DataSync 主要用于将现有数据迁移到 Amazon S3。另一方面，如果您仍然希望保留对迁移数据的访问权，并从基于本地文件的应用程序进行持续更新，则 AWS 存储网关更适合。

因此，该场景中的正确答案是：使用 AWS 数据同步来移动数据。将所有数据存储在 Amazon S3 中并启用对象锁定。

该选项表示：使用 AWS 数据同步来移动数据。将所有数据存储在 Amazon EFS 中并启用对象锁定是不正确的，因为 Amazon EFS 仅支持文件锁定。对象锁定是 Amazon S3 的一项功能，而不是 Amazon EFS。

选项说明：使用 AWS 存储网关建立混合云存储。将所有数据存储在 Amazon S3 中并启用对象锁定是不正确的，因为场景要求所有现有记录都必须迁移到 AWS。未来的记录也将存储在 AWS 中，而不是本地网络中。这意味着不需要设置混合云存储，因为内部存储将不再使用。

该选项表示：使用 AWS 存储网关建立混合云存储。在 Amazon EBS 中存储所有数据并启用对象锁定是不正确的，因为 Amazon EBS 不支持对象锁定。Amazon S3 是唯一能够锁定对象以防止对象被删除或覆盖的服务。

参考文献：

<https://aws.amazon.com/datasync/faqs/>

<https://docs.aws.amazon.com/datasync/latest/userguide/what-is-datasync.html>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/object-lock.html> 查看 AWS 数据同步备忘单：

<https://tutorialsdojo.com/aws-datasync/>

AWS 存储网关与数据同步：

<https://www.youtube.com/watch?v=tmfelrO-澳大利亚>

马逊 S3 vs EBS vs EFS 备忘单：

<https://tutorialsdojo.com/amazon-s3-vs-ebs-vs-efs/>

Q136.解决方案架构师创建了一个新的标准 S3 类存储桶，用于存储不经常访问的财务报告，但应在审计员请求时立即可用。为了节省成本，架构师将 S3 存储桶的存储类从标准更改为不频繁访问存储类。在里面 Amazon S3 标准-不频繁访问存储类，以下哪项陈述正确？（选择二）

- A、 非常适合用于数据存档。
- B、 它是为访问频率较低的数据设计的。
- C、 它提供了高延迟和低吞吐量性能
- D、 它专为需要快速访问的数据而设计。
- E、 它自动将数据移动到最经济高效的访问层，而无需任何操作开销。

答案：BC

分析：

Amazon S3 标准-不频繁访问 (Standard-IA) 是一个 AmazonS3 存储类，用于访问频率较低但需要快速访问的数据。标准-IA 提供了 Amazon S3 标准的高耐用性、吞吐量和低延迟，每 GB 存储价格和每 GB 检索费用较低。

这种低成本和高性能的结合使 Standard-IA 成为长期存储、备份和灾难恢复数据存储的理想选择。标准-IA 存储类是在对象级别设置的，可以与标准存储类存在于同一存储桶中，允许您使用生命周期策略在存储类之间自动转换对象，而无需任何应用程序更改。

主要特点：

- 与标准相同的低延迟和高吞吐量性能
- 设计用于 99.999999999% 的物体的耐用性
- 设计用于特定年份 99.9% 的可用性
- 支持 Amazon S3 服务级别协议以提供可用性
- 支持传输和静止数据的 SSL 加密-对象自动迁移的生命周期管理

因此，正确答案是：

- 它是为访问频率较低的数据设计的。
- 它专为需要快速访问的数据而设计。“自动将数据移动到最具成本效益的访问层而无需任何操作开销”的选项是不正确的，因为它实际上指的是 Amazon S3 智能分层，这是唯一一个云存储类，当访问模式发生变化时，通过在不同访问层之间移动对象来实现自动成本节约。

表示：它提供高延迟和低吞吐量性能的选项是不正确的，因为它应该是“低延迟”和“高吞吐量”。S3 自动扩展性以满足用户需求。表示“理想用于数据存档”的选项是不正确的，因为该语句指的是 Amazon S3 Glacier。Glacier 是一种安全、耐用、成本极低的云存储服务，用于数据存档和长期备份。

参考文献：

[https://aws.amazon.com/s3/storage-](https://aws.amazon.com/s3/storage-classes/)

[classes/ https://aws.amazon.com/s3/faqs](https://aws.amazon.com/s3/faqs) 查

看此 Amazon S3 备忘单：

<https://tutorialsdojo.com/amazon-s3/>

Q137.一家媒体公司正在为其图像处理应用程序设置 ECS 批处理架构。它将托管在一个 Amazon ECS 集群中，该集群具有两个 ECS 任务，将处理来自用户的图像上传和图像处理。第一个 ECS 任务将处理用户请求，将图像存储在 S3 输入桶中，并将消息推送到队列。第二个任务读取队列，解析包含对象名称的消息，然后下载对象。一旦图像被处理和转换，它将把对象上传到 S3 输出桶。要完成架构，解决方案架构师必须为 ECS 任务创建队列和必要的 IAM 权限。

架构师接下来应该做以下哪项？

A、 启动新的 Amazon Kinesis Data Firehose，并配置第二个 ECS 任务以从中读取数据。

创建 ECS 任务可以承担的 IAM 角色，以便访问 S3 存储桶和 Kinesis 数据消防软管。在任务定义的（任务定义 ARN）字段中指定 IAM 角色的 ARN。

B、启动新的 Amazon AppStream 2.0 队列，并配置第二个 ECS 任务从中读取。

创建 ECS 任务可以承担的 IAM 角色，以便访问 S3 bucket 和 AppStream 2.0 队列。在任务定义中声明 IAM 角色（taskRoleArn）。

C、新的 Amazon SQS 队列，并配置第二个 ECS 任务从中读取。创建一个由 ECS 任务扫描承担的 IAM 角色，以便访问 S3 存储桶和 SQS 队列。在任务定义中声明 IAM 角色（taskRoleArn）。

D、新的 Amazon MQ 队列，并配置第二个 ECS 任务从中读取。创建一个由 ECS 任务扫描承担的 IAM 角色，以便访问 S3 存储桶和 Amazon MQ 队列。在任务定义中将（EnableTaskIAMRole）选项设置为 true。

答案 C

分析：

Docker 容器特别适合批量作业工作负载。批处理作业通常是短命的，令人尴尬的并行作业。您可以将批处理应用程序打包到 Docker 映像中，以便可以将其部署到任何位置，例如 Amazon ECS 任务中。Amazon ECS 支持批量作业。您可以使用 Amazon ECS 运行任务操作一次运行一个或多个任务。运行任务操作在满足任务要求（包括 CPU、内存和端口）的实例上启动 ECS 任务。

例如，您可以为图像处理应用程序设置 ECS 批处理架构。您可以设置 AWS 创建 Amazon S3 bucket、Amazon SQS 队列、Amazon

CloudWatch 警报、ECS 群集和 ECS 任务定义。上传到输入 S3 存储桶的对象触发一个事件，将对象详细信息发送到 SQS 队列。ECS 任务部署一个 Docker 容器，从该队列读取数据，解析包含对象名称的消息，然后下载对象。一旦转换，它将把对象上传到 S3 输出桶。通过使用 SQS 队列作为所有对象详细信息的位置，您可以利用其可伸缩性和可靠性，因为队列将根据传入的消息自动伸缩，并且可以保留消息

配置。然后，ECS 集群将能够根据队列中的消息数量来增加或减少服务。

您必须创建 ECS 任务承担的 IAM 角色，以便访问 S3 bucket 和 SQS 队列。请注意，IAM 角色的权限没有为传入存储桶指定 S3 存储桶 ARN。这是为了避免 CloudFormation 模板中的循环依赖问题。您应该始终确保为 IAM 角色分配最少的权限。因此，正确答案是：

启动一个新的 Amazon SQS 队列，并配置第二个 ECS 任务从中读取。创建 ECS 任务可以承担的 IAM 角色，以便访问 S3 存储桶和 SQS 队列。在任务定义中声明 IAM 角色（taskRoleArn）。选项是：启动新的 Amazon AppStream 2.0 队列，并配置第二个 ECS 任务从中读取。创建 ECS 任务可以承担的 IAM 角色，以便访问 S3 bucket 和 AppStream 2.0 队列。在任务定义中声明 IAM 角色（taskRoleArn）是不正确的，因为 Amazon AppStream 2.0 是完全受管理的应用程序流服务，不能用作队列。您必须改用 Amazon SQS。选项显示：启动新的 Amazon Kinesis 数据消防软管，并配置第二个 ECS 任务从中读取。创建 ECS 任务可以承担的 IAM 角色，以便访问 S3 存储桶和 Kinesis 数据消防软管。

在任务定义的（taskDefinitionArn）字段中指定 IAM 角色的 ARN 是不正确的，因为 Amazon Kinesis Data Firehose 是一个完全管理的服务，用于提供实时流数据。尽管它可以将数据流传输到 S3 存储桶，但在这种情况下，它不适合用作批处理应用程序的队列。此外，IAM 角色的 ARN 应在 taskRoleArn 中声明，而不是在 taskDefinitionArn 字段中声明。该选项表示：启动一个新的 Amazon MQ 队列，并配置第二个 ECS 任务从中读取。创建 ECS 任务可以承担的 IAM 角色，以便访问 S3 存储桶和 Amazon MQ 队列。在任务定义中将（EnableTaskIAMRole）选项设置为 true 是不正确的，因为 Amazon MQ 主要用作托管消息代理服务，而不是队列。EnableTaskIAMRole 选项仅适用于需要额外配置的基于 Windows 的 ECS 任务。

参考文献：

<https://github.com/aws-samples/ecs-refarch-batch-processing>
https://docs.aws.amazon.com/AmazonECS/latest/developerguide/common_use_cases.html
<https://aws.amazon.com/ecs/faqs/>

Q138.公司有一个最优先的要求，即监控一些数据库指标，然后在出现问题时向运营团队发送电子邮件通知。哪些 AWS 服务可以满足这一要求？（选择两个。）

- A、 Amazon EC2 实例，运行 Berkeley Internet 域名域（绑定）服务器。
- B、 亚马逊云观察
- C、 简单通知服务（SNS）
- D、 亚马逊简单电子邮件服务
- E、 简单队列服务（SQS）

答案：BC

分析：

Amazon CloudWatch 和 Amazon 简单通知服务（SNS）是正确的。在此需求中，您可以使用 Amazon CloudWatch 监控数据库，然后使用 Amazon SNS 将电子邮件发送给运营团队。请注意，当您想要监控 EC2 实例时，应该使用 SNS 而不是 SES（简单电子邮件服务）。

CloudWatch 以日志、指标和事件的形式收集监控和操作数据，为您提供 AWS 资源、应用程序和运行在 AWS 和本地服务器上的服务的统一视图。SNS 是一种高度可用、持久、安全、完全管理的发布/订阅消息服务，使您能够将微服务、分布式系统和无服务器应用程序解耦。com

亚马逊简单电子邮件服务不正确。SES 是一种基于云的电子邮件发送服务，旨在发送通知和交易电子邮件。

Amazon 简单队列服务（SQS）不正确。SQS 是一种完全受管理的消息队列服务。与 SES 不同，它不监控应用程序，也不发送电子邮件通知。带有正在运行的 Berkeley Internet Name Domain（绑定）服务器的 Amazon EC2 实例不正确，因为绑定主要用作域名系统（DNS）web 服务。这仅适用于您有私人

参考文献：

<https://aws.amazon.com/cloudwatch/>

<https://aws.amazon.com/sns/>

查看此 Amazon CloudWatch 备忘单：<https://tutorialsdjo.com/amazon-cloudwatch/>

Q139.一家媒体公司有两个 VPC：VPC-1 和 VPC-2，它们之间有对等连接。VPC-1 只包含私有子网，而 VPC-2 只包含公共子网。该公司使用单个 AWS 直连连接和虚拟接口将其内部网络与 VPC-1 连接。以下哪种选项可提高连接到 VPC-2 的容错性？（选择两个。）

- A、 使用 AWS VPN CloudHub 在与 VPC-2 相同的区域创建新的 AWS 直连连接和专用虚拟接口。
- B、 在与 VPC-1 相同的 AWS 区域建立另一个 AWS 直连连接和专用虚拟接口。

- C、在 VPC-2 和内部网络之间通过互联网建立硬件 VPN。
- D、在 VPC-1 和内部网络之间通过互联网建立硬件 VPN。
- E、在与 VPC-2 相同的区域建立新的 AWS 直连连接和专用虚拟接口。

答：屋宇署

分析：

在这种情况下，您有两个 VPC，它们之间具有对等连接。请注意，VPC 对等连接不支持边缘到边缘路由。这意味着，如果对等关系中的任何一个 VPC 具有以下连接之一，则无法将对等关系扩展到该连接：

- VPN 连接或 AWS 直接连接到公司网络
- 通过互联网网关的互联网连接
- 通过 NAT 设备在专用子网中的 Internet 连接
- AWS 服务的网关 VPC 端点；例如 Amazon S3 的端点。
- （IPv6）ClassicLink 连接。您可以在链接的 EC2 Classic 实例和 VPC 对等连接另一侧的 VPC 中的实例之间启用 IPv4 通信。但是，EC2 Classic 不支持 IPv6，因此无法扩展此连接以进行 IPv6 通信。

例如，如果 VPC A 和 VPC B 是对等的，并且 VPC A 具有这些连接中的任何一个，则 VPC B 中的实例不能使用该连接访问连接另一侧的资源。类似地，连接另一端的资源不能使用连接访问 VPC B。因此，这意味着您不能使用 VPC-2 扩展 VPC-1 和本地网络之间存在的对等关系。例如，来自企业网络的流量不能通过 VPN 连接或 AWS 直接连接到 VPC-2 直接访问 VPC-1，这就是为什么以下选项不正确的原因：

- 使用 AWS VPN CloudHub 在与 VPC-2 相同的区域创建新的 AWS 直连连接和专用虚拟接口。
- 在 VPC-2 和内部网络之间通过互联网建立硬件 VPN。
- 在与 VPC-2 相同的区域建立新的 AWS 直连连接和专用虚拟接口。

您可以执行以下操作以提供高可用性、容错的网络连接：

com

- 在 VPC 和内部网络之间通过互联网建立硬件 VPN。
- 在同一 AWS 区域建立另一个 AWS 直连连接和专用虚拟接口。

参考文献：

<https://docs.aws.amazon.com/vpc/latest/peering/invalid-peering-configurations.html#edge-至边缘>
[vgwhhttps://aws.amazon.com/premiumsupport/knowledge-center/configure-vpn-backup-dx/](https://aws.amazon.com/premiumsupport/knowledge-center/configure-vpn-backup-dx/)
<https://aws.amazon.com/answers/networking/aws-multiple-data-center-ha-network-connectivity/>查看此亚马逊
VPC 备忘单：<https://tutorialsdojo.com/amazon-vpc/>

Q140.一家跨国游戏公司的解决方案架构师为 PS4、Xbox One 和任天堂 Switch 游戏机开发视频游戏，并为 Android 和 iOS 开发了许多移动游戏。由于他们的产品和服务范围广泛，架构师建议他们使用 API 网关。架构师可以告诉客户的 API 网关的关键特性是什么？（选择两个。）

- A、 使您能够通过其定制的操作系统（OS）旁路硬件接口在 AWS 上运行需要高级别节点间通信的应用程序。
- B、 它自动为 API 提供了一种类似于 GraphQL 的查询语言。
- C、 您只为接收的 API 调用和传输的数据量付费。
- D、 为您提供静态选播 IP 地址，作为一个或多个 AWS 区域中托管的应用程序的固定入口点。
- E、 您需要构建针对无服务器工作负载优化的 RESTful API 和 WebSocket API。

行政长官的答覆

分析：

Amazon API Gateway 是一个完全受管理的服务，使开发人员可以轻松创建、发布、维护、监控和保护任何规模的 API。只需在 AWS 管理控制台中点击几下，您就可以创建一个 API，作为应用程序从后端服务访问数据、业务逻辑或功能的“前门”，例如在 Amazon 弹性计算云（Amazon EC2）上运行的工作负载、在 AWS Lambda 上运行的代码或任何 web 应用程序。因为它可以使用 AWS Lambda，所以您可以在没有服务器的情况下运行 API。

com

Amazon API 网关处理接受和处理多达数十万个并发 API 调用所涉及的所有任务，包括流量管理、授权和访问控制、监控和 API 版本管理。亚马逊 API 网关没有最低费用或启动成本。您只为接收的 API 调用和传输的数据量付费。因此，正确答案是：

- 使您能够构建针对无服务器工作负载优化的 RESTful API 和 WebSocket API
- 您只为接收的 API 调用和传输的数据量付费。“它会自动为您的 API 提供类似于 GraphQL 的查询语言”的选项是不正确的，因为这不是由 API 网关提供的。“为您提供静态选播 IP 地址，作为一个或多个 AWS 区域中托管的应用程序的固定入口点”选项是不正确的，因为这是 AWS 全球加速器的功能，而不是 API 网关。

“允许您通过其自定义操作系统（OS）旁路硬件接口在 AWS 上大规模运行需要高级别节点间通信的应用程序”选项是不正确的，因为这是弹性结构适配器的功能，而不是 API 网关。参考文献：

<https://aws.amazon.com/api-gateway/> API 网关

[/https://aws.amazon.com/api-gateway/features/](https://aws.amazon.com/api-gateway/features/)查看

此 Amazon API 网关备忘单：

<https://tutorialsdojo.com/amazon-api-gateway/>

Dojo 的 AWS 认证解决方案架构师助理考试学习指南教程：<https://tutorialsdojo.com/aws-certified-solutions-architect-associate/>

Q141.一家公司有多 VPC，为其 web 应用程序套件启用了 IPv6。解决方案架构师试图部署一个新的 Amazon EC2 实例，但她收到一个错误，称子网上没有可用的 IP 地址。

解决方案架构师应该如何解决这个问题？

- A、 设置具有大 CIDR 范围的新的仅 IPv6 子网。将新子网与 VPC 关联，然后启动该实例。
- B、 设置具有更大 CIDR 范围的新 IPv4 子网。将新子网与 VPC 关联，然后启动该实例。
- C、 禁用 VPC 中的 IPv4 支持，并使用可用的 IPv6 地址。
- D、 确保专有网络仅具有 IPv6 CIDR。删除与 VPC 关联的任何 IPv4 CIDR。

答案 B

分析：

Amazon 虚拟私有云（VPC）是一项服务，允许您在定义的逻辑隔离虚拟网络中启动 AWS 资源。您可以完全控制虚拟网络环境，包括选择自己的 IP 地址范围、创建子网以及配置路由表和网络网关。您可以对虚拟私有云中的大多数资源同时使用 IPv4 和 IPv6，这有助于确保安全、方便地访问资源和应用程序。子网是 VPC 中的一系列 IP 地址。您可以将 AWS 资源启动到指定的子网中。创建 VPC 时，必须以 CIDR 块的形式为 VPC 指定一系列 IPv4 地址。每个子网必须完全位于一个可用性区域内，并且不能跨区域。您还可以选择将 IPv6 CIDR 块分配给 VPC，并将 IPv6 CIDR 块分配给子网。如果现有 VPC 仅支持 IPv4，并且子网中的资源配置为仅使用 IPv4，则可以为 VPC 和资源启用 IPv6 支持。您的 VPC 可以在双栈模式下运行——您的资源可以通过 IPv4 或 IPv6 或两者进行通信。IPv4 和 IPv6 通信相互独立。您无法禁用 VPC 和子网的 IPv4 支持，因为这是 Amazon VPC 和 Amazon EC2 的默认 IP 寻址系统。默认情况下，新 EC2 实例使用 IPv4 寻址协议。要解决该场景中的问题，您需要创建一个新的 IPv4 子网，并在新子网中部署 EC2 实例。因此，正确的答案是：设置一个具有更大 CIDR 范围的新 IPv4 子网。将新子网与 VPC 关联，然后启动实例。

通用域名格式

该选项表示：设置一个新的仅 IPv6 子网，该子网具有较大的 CIDR 范围。将新子网与 VPC 关联，然后启动实例是不正确的，因为您需要先添加 IPv4 子网，然后才能创建 IPv6 子网。

该选项表示：确保 VPC 仅具有 IPv6 CIDR。删除与专有网络相关联的任何 IPv4 CIDR 是不正确的，因为您不能拥有仅具有 IPv6 CIDR 的专有网络。VPC 中的默认 IP 寻址系统是 IPv4。您只能将 VPC 更改为双栈模式，其中您的资源可以通过 IPv4 或 IPv6 或两者进行通信，但不能仅通过 IPv6 进行通信。“禁用 VPC 中的 IPv4 支持并使用可用 IPv6 地址”选项不正确，因为您无法禁用 VPC 和子网的 IPv4 支持，因为这是默认 IP 寻址系统。

参考文献：

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-migrate-ipv6.html>

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-ip-addressing.html> <https://aws.amazon.com/vpc/faqs/>

查看此亚马逊 VPC 备忘单：<https://tutorialsdojo.com/amazon-vpc/>

Q142.一家保险公司计划在其 web 应用程序中实现消息过滤功能。为了实现这个解决方案，他们需要为每种类型的报价请求创建单独的 Amazon SQS 队列。

整个消息处理不应超过 24 小时。

作为公司的解决方案架构师，您应该做以下哪项来满足上述要求？

- A、创建多个 Amazon SNS 主题，并配置 Amazon SQS 队列以订阅 SNS 主题。根据报价请求类型将消息发布到指定的 SQS 队列。
- B、在 Amazon Kinesis 数据流中创建数据流。使用 Amazon Kinesis 客户端库根据报价请求类型将所有记录发送到指定的 SQS 队列。
- C、创建一个 Amazon SNS 主题，并配置 Amazon SQS 队列以订阅 SNS 主题。

将相同的消息发布到所有 SQS 队列。根据报价请求类型筛选每个队列中的消息。

com

- D、创建一个 Amazon SNS 主题，并配置 Amazon SQS 队列以订阅 SNS 主题。

在 SNS 订阅中设置过滤策略，以根据其报价请求类型将消息发布到指定的 SQS 队列。

答案 D

分析：

Amazon SNS 是一个完全管理的发布/订阅消息服务。使用 Amazon SNS，您可以使用主题将消息同时分发到多个订阅端点，如 Amazon SQS 队列、AWS Lambda 函数、HTTP 端点、电子邮件地址和移动设备（SMS、推送）。Amazon SQS 是分布式应用程序使用的消息队列服务，用于通过

轮询模型。它可以用于分离发送和接收组件，而不需要每个组件同时可用。

当发布到 SNS 主题的消息被复制并推送到多个端点（如 Amazon SQS 队列、HTTP（S）端点和 Lambda 函数）时，就会出现扇出场景。这允许并行异步处理。

例如，您可以开发一个应用程序，该应用程序在产品下订单时向 SNS 主题发布消息。然后，订阅 SNS 主题的两个或多个 SQS 队列将收到新订单的相同通知。连接到其中一个 SQS 队列的 Amazon 弹性计算云（Amazon EC2）服务器实例可以处理订单的处理或履行。您可以将另一个 Amazon EC2 服务器实例连接到数据仓库，以分析收到的所有订单。默认情况下，Amazon SNS 主题订户接收发布到该主题的所有消息。您可以使用 Amazon SNS 消息过滤为主题订阅分配过滤策略，订阅者将只接收他们感兴趣的消息。同时使用 Amazon SNS 和 Amazon SQS，可以将消息传递到需要立即通知事件的应用程序。这种方法称为 Amazon SQS 队列的扇出。因此，正确的答案是：创建一个 Amazon SNS 主题并配置 Amazon SQS 队列以订阅 SNS 主题。在 SNS 订阅中设置过滤策略，以根据其报价请求类型将消息发布到指定的 SQS 队列。

com

该选项表示：创建一个 Amazon SNS 主题，并配置 Amazon SQS 队列以订阅 SNS 主题。将相同的消息发布到所有 SQS 队列。基于报价请求类型筛选每个队列中的消息是不正确的，因为此选项将在所有 SQS 队列而不是其指定队列上分发相同的消息。您需要在 Amazon SNS 订阅中使用过滤器策略将消息扇出到多个 SQS 队列，以允许并行异步处理。这样，整个消息处理将不会超过 24 小时。

该选项表示：创建多个 Amazon SNS 主题，并配置 Amazon SQS 队列以订阅 SNS 主题。基于报价请求类型将消息发布到指定的 SQS 队列是不正确的，因为要实现场景中要求的解决方案，您只需要使用一个 Amazon SNS 主题。要将其发布到指定的 SQS 队列，必须设置允许扇出消息的筛选策略。如果您没有在 Amazon SNS 中设置过滤策略，订阅者将收到发布到 SNS 主题的所有消息。因此，使用多个 SNS 主题并不是这种场景的合适解决方案。

选项表示：在 Amazon Kinesis 数据流中创建数据流。使用 Amazon Kinesis 客户端库根据报价请求类型将所有记录发送到指定的 SQS 队列是不正确的，因为 Amazon KDS 不是消息过滤服务。您应该使用 Amazon SNS 和 SQS 将主题分发到指定队列。

参考文献:

<https://aws.amazon.com/getting-started/hands-on/filter-messages-published-to-topics/>
<https://docs.aws.amazon.com/sns/latest/dg/sns-message-filtering.html> <https://docs.aws.amazon.com/sns/latest/dg/snssqs-as-subscriber.html> 查看此亚马逊 SNS 和 SQS 备忘单:

<https://tutorialsdojo.com/amazon-sns/> <https://tutorialsdojo.com/amazon-sqs/>

亚马逊 SNS 概述: <https://www.youtube.com/watch?v=ft5R45IEUJ8>

Q143.一家音乐出版公司正在构建一个多层 web 应用程序, 该应用程序需要保存文档模型的键值存储。每个模型由乐队 ID、专辑 ID、歌曲 ID、作曲家 ID、歌词和其他数据组成。web 层将托管在具有 AWS Fargate 启动类型的 Amazon ECS 集群中。以下哪种设置最适合数据库层?

- A、启动亚马逊极光无服务器数据库。
- B、启动具有读取副本的 Amazon RDS 数据库。
- C、启动 DynamoDB 表。
- D、使用 Amazon WorkDocs 存储文档模型。

答案 C

分析:

Amazon DynamoDB 是一种快速、灵活的 NoSQL 数据库服务, 适用于需要任何规模的一致、单位毫秒延迟的所有应用程序。它是一个完全管理的云数据库, 支持文档和键值存储模型。其灵活的数据模型、可靠的性能和吞吐量的自动扩展使其非常适合移动、网络、游戏、广告技术、物联网和许多其他应用。

因此, 正确答案是: 启动 DynamoDB 表。

“启动具有读取副本的 Amazon RDS 数据库”选项不正确, 因为这是一个关系数据库。这不适合用作键值存储。更好的选择是使用 DynamoDB, 因为它支持文档和键值存储模型。使用 Amazon WorkDocs 存储文档模型的选项是不正确的, 因为 Amazon WorkDocs 只允许您共享内容、提供丰富的反馈和协作编辑文档。

它不是像 DynamoDB 那样的键值存储。

“启动 Amazon Aurora 无服务器数据库”选项不正确, 因为这种类型的数据库不适合用作键值存储。Amazon Aurora 无服务器是一种按需自动扩展的

Amazon Aurora 的配置, 其中数据库将根据应用程序的需要自动启动、关闭和扩展容量。它使您能够在云中运行数据库, 而无需管理任何数据库实例。对于不频繁、间歇或不可预测的工作负载, 它是一个简单、经济高效的选项, 而不是作为键值存储。参考文献: <https://aws.amazon.com/dynamodb/> <https://aws.amazon.com/nosql/key-value/> 查看此 Amazon DynamoDB 备忘单:

<https://tutorialsdojo.com/amazon-dynamodb/>

亚马逊 DynamoDB 概述: <https://www.youtube.com/watch?v=3ZOyUNIeorU>

Q144.应用程序托管在 AWS Fargate 中，并在多 AZ 部署配置中使用 RDS 数据库，具有多个读取副本。一位解决方案架构师被指示确保他们的所有数据库凭证、API 密钥和其他秘密都定期加密和轮换，以提高数据安全性。连接到 RDS 数据库时，应用程序还应使用最新版本的加密凭据。

以下哪项是保护凭据的最合适解决方案？

- A、 将数据库凭据、API 密钥和其他机密存储到 Systems Manager 参数存储中，每个参数都具有 aSecureString 数据类型。默认情况下，凭据会自动旋转。
- B、 将数据库凭据、API 密钥和其他机密存储在 AWS KMS 中。
- C、 将数据库凭据、API 密钥和其他机密存储到 AWS ACM。
- D、 使用 AWS 机密管理器存储和加密数据库凭据、API 密钥和其他机密。

启用所有凭据的自动轮换。

答案 D

分析：

AWS Secrets Manager 是一种 AWS 服务，可以让您更轻松的管理机密。秘密可以是数据库凭据、密码、第三方 API 密钥，甚至是任意文本。您可以使用 secrets Manager 控制台、secrets 管理器命令行界面（CLI）或 secrets 管理员 API 和 SDK 集中存储和控制对这些机密的访问。过去，当您创建从数据库检索信息的自定义应用程序时，通常必须在应用程序中嵌入用于直接访问数据库的凭据（秘密）。当轮换凭证时，您需要做的不仅仅是创建新凭证。您必须投入时间更新应用程序以使用新凭据。然后，您必须分发更新的应用程序。如果您有多个共享凭据的应用程序，并且您错过了其中一个应用程序的更新，则应用程序将中断。由于这种风险，许多客户选择不定期轮换他们的凭证，这有效地替代了一种风险。Secrets Manager 使您能够使用对 Secrets 管理器的 API 调用来替换代码中的硬编码凭据（包括密码），以编程方式检索机密。这有助于确保秘密不会被检查代码的人泄露，因为秘密根本不存在。此外，您还可以配置机密管理器，以便根据指定的计划自动为您旋转机密。这使您能够用短期机密替换长期机密，这有助于显著降低泄露风险。

因此，最适合此场景的解决方案是：使用 AWS 机密管理器存储和加密数据库凭据、API 密钥和其他机密。启用所有凭据的自动轮换。该选项表示：将数据库凭据、API 密钥和其他机密存储到 Systems Manager 参数存储中，每个都具有 SecureString 数据类型。默认情况下自动旋转凭据是不正确的，因为系统管理器参数存储默认情况下不旋转其参数。“将数据库凭据、API 密钥和其他机密存储到 AWS ACM”选项是不正确的，因为它只是一个受管理的私有 CA 服务，可帮助您轻松安全地管理私有证书的生命周期，以允许与应用程序进行 SSL 通信。这不是存储数据库或任何其他机密凭据的合适服务。

“在 AWS KMS 中存储数据库凭据、API 密钥和其他机密”选项是不正确的，因为这只会使您更容易创建和管理加密密钥，并控制各种 AWS 服务中加密的使用。这主要用于加密，而不是托管您的凭据。

参考文献：

<https://aws.amazon.com/secrets-manager/>

<https://aws.amazon.com/blogs/security/how-to-securely-provide-database-credentials-to-lambda-functions-通过使用 Windows 机密管理器/>

查看以下 AWS Secrets Manager 和 Systems Manager 备忘单：

<https://tutorialsdojo.com/aws-secrets-manager/> <https://tutorialsdojo.com/aws-systems-manager/>

AWS 安全服务概述-机密管理器、ACM、Macie: <https://www.youtube.com/watch?v=ogVamzF2Dzk>

Q145.一家广告公司目前正在开发一个概念验证项目，为其客户自动提供搜索引擎优化分析。贵公司在 AWS 中有一个 VPC，它以双栈模式运行，允许 IPv4 和 IPv6 通信。您将应用程序部署到一个 EC2 实例的自动扩展组中，前面有一个应用程序负载均衡器，用于均匀分布传入流量。您已经准备好上线，但需要将域名（tutorialsdojo.com）指向应用程序负载均衡器。

在路由 53 中，您将使用哪些记录类型来指向应用程序负载均衡器的 DNS 名称？（选择二）

- A、具有类型“A”记录集的别名
- B、具有类型“a”记录集的非别名
- C、具有类型“AAAA”记录集的别名
- D、具有“CNAME”记录集类型的别名
- E、具有“MX”记录集类型的别名

答覆

分析：

正确答案是：具有“AAAA”记录集类型的别名和具有“a”记录集中类型的别名。要将域流量路由到 ELB 负载均衡器，请使用 Amazon route 53 创建指向负载均衡器的别名记录。别名记录是 DNS 的路由 53 扩展。它类似于 CNAME 记录，但您可以为根域创建别名记录，如 tutorialsdojo.com 和子域，如 portal.tutorialsdojo.com。（您只能为子域创建 CNAME 记录。）要启用 IPv6 解析，您需要创建第二个资源记录 tutorialsdojo.com 别名 AAAA->myelb.us-west-2.elb.amazonaws.com，这是假设您的弹性负载均衡器支持 IPv6。具有“a”类型记录集的非别名是不正确的，因为您只能将非别名与 IP 地址的“a”类记录集一起使用。

“CNAME”记录集类型的别名不正确，因为无法在区域顶点创建 CNAME 记录。例如，如果注册 DNS 名称 tutorialsdojo.com，区域顶点是 tutorialsdojo.com。“MX”记录集类型的别名不正确，因为 MX 记录主要用于邮件服务器。它包括优先级编号和域名，例如：10 mailserver.tutorialsdojo.com。参考：

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-to-elb-load-balancer.html><https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resource-record-sets-select-names.html> 记录集选择别名和非别名。
html 查看此亚马逊路线 53 备忘单: <https://tutorialsdojo.com/amazon-route-53/>

Q146.一位解决方案架构师正在为一家在线酒店预订公司工作，该公司拥有来自网站和应用程序的 TB 级客户数据。有一个年度公司会议，架构师需要展示预订行为，并从客户的数据中获得新的见解。架构师正在寻找一种在近实时的海量数据集上执行超快速分析的服务。以下哪项服务使架构师能够存储大量数据并对其执行快速灵活的查询？

- A、 亚马逊发电机 B
- B、 亚马逊 RDS
- C、 亚马逊红移
- D、 亚马逊松紧带

答案 C

分析：

Amazon Redshift 是一个快速、可扩展的数据仓库，它使分析数据仓库和数据湖中的所有数据变得简单且经济高效。Redshift 通过使用机器学习、大规模并行查询执行和高性能磁盘上的列存储，提供了比其他数据仓库快十倍的性能。

您可以使用 Redshift 使用标准 SQL 和现有的商业智能（BI）工具分析所有数据。它还允许您对 TB 到 PB 的结构化和半结构化数据运行复杂的分析查询，使用复杂的查询优化、高性能存储上的列存储以及大规模并行查询执行。

因此，正确答案是：亚马逊红移。

亚马逊 DynamoDB 是不正确的。DynamoDB 是一个基于键值对的 NoSQL 数据库，用于快速处理动态增长和变化的小数据。但是，如果需要扫描大量数据（即一个查询中有许多键），性能将不是最佳的。Amazon ElastiCache 是不正确的，因为它用于通过提供内存数据库缓存系统来提高应用程序检索数据的性能、速度和冗余，而不是用于数据库分析过程。

Amazon RDS 不正确，因为它主要用于在线事务处理（OLTP）应用程序，而不是在线分析处理（OLAP）。

参考文献：

<https://docs.aws.amazon.com/redshift/latest/mgmt/welcome.html>

<https://docs.aws.amazon.com/redshift/latest/gsg/getting-started.html> 亚马逊红移概述：

<https://youtu.be/jlLERNzhHOg> 查看此亚马逊红移备忘单：<https://tutorialsdojo.com/amazon-redshift/>

Q147.您的一个 EC2 实例报告了不健康的系统状态检查。运营团队正在寻找一种更简单的方法来监控和修复这些实例，而不是手动修复它们。您将如何在 AWS 环境中自动监控和修复系统状态检查故障？

- A、 编写一个 python 脚本，查询每个实例状态检查的 EC2API
- B、 编写一个 shell 脚本，根据某些统计信息定期关闭和启动实例。
- C、 并实现第三方监控工具。
- D、 创建基于状态检查警报停止和启动实例的 CloudWatch 警报。

答案 D

分析：

使用 Amazon CloudWatch 警报操作，您可以创建自动停止、终止、重新启动或恢复 EC2 实例的警报。您可以使用“停止”或“终止”操作来帮助您节省资金

不再需要运行实例。您可以使用重新启动和恢复操作自动重新启动这些实例，或者在发生系统损坏时将它们恢复到新硬件上。编写一个 python 脚本，查询 EC2 API 的每个实例状态检查，编写一个 shell 脚本，根据某些统计数据定期关闭和启动实例，以及购买和实现第三方监控工具都是不正确的，因为当 CloudWatch Alarms 已经为您提供了这样一个低成本的功能时，没有必要经历这样的长度。参考：

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/UsingAlarmActions.html> 查看此 Amazon CloudWatch 备忘单：<https://tutorialsdojo.com/amazon-cloudwatch/>

Q148.解决方案架构师需要在亚马逊 VPC 中设置一个堡垒主机。只能通过 SSH 从公司数据中心访问。实现这一目标的最佳方式是什么？

- A、创建一个带有安全组的小型 EC2 实例，该安全组仅允许通过公司数据中心的 IP 地址访问端口 22。使用私钥（.pem）文件连接到 bastion 主机。
- B、使用安全组创建一个大型 EC2 实例，该安全组仅允许使用您自己的预配置密码访问端口 22。
- C、创建一个带有安全组的小型 EC2 实例，该安全组仅允许使用您自己预先配置的密码访问端口 22。
- D、创建具有安全组的大型 EC2 实例，该安全组仅允许通过公司数据中心的 IP 地址访问端口 22。使用私钥（.pem）文件连接到 bastion 主机。

答：

分析：

实现 bastion 主机的最佳方法是创建一个小型 EC2 实例，该实例应仅具有来自特定 IP 地址的安全组，以实现最大安全性。这将阻止对您的

这是主人的堡垒。还建议使用小型实例而不是大型实例，因为该主机将仅作为跳转服务器连接到 VPC 中的其他实例，而不是其他。因此，分配大型实例没有意义，因为它不需要太多计算能力来处理 SSH（端口 22）或 RDP（端口 3389）连接。可以使用具有普通用户 ID 和预配置密码的 SSH 作为凭据，但使用公钥对进行 SSH 身份验证更安全，以获得更好的安全性。

因此，该场景的正确答案是这样一个选项：创建一个小型 EC2 实例，其中包含一个安全组，该安全组仅允许通过公司数据中心的 IP 地址访问端口 22。使用私钥（.pem）文件连接到 bastion 主机。

创建具有安全组的大型 EC2 实例，该安全组仅允许使用您自己的预配置密码访问端口 22，以及创建具有仅允许使用自己的预设置密码访问端口 21 的安全组的小型 EC2 实例是不正确的。即使您有自己的预配置密码，任何人仍然可以通过 Internet 访问 SSH 连接，这构成了一个安全漏洞。

该选项表示：创建一个大型 EC2 实例，其安全组仅允许通过公司数据中心的 IP 地址访问端口 22。使用私钥（.pem）文件连接到 bastion 主机是不正确的，因为 bastion 主机不需要大型实例，因为它不需要太多 CPU 资源。

参考文献：

<https://docs.aws.amazon.com/quickstart/latest/linux-bastion/architecture.html>

<https://aws.amazon.com/blogs/security/how-to-record-ssh-sessions-established-through-a-bastion-host/> 查看此亚马逊 VPC 备忘单：

<https://tutorialsdojo.com/amazon-vpc/>

Q149. 一家公司拥有一个加密货币交换门户，该门户托管在应用程序负载均衡器后面的 EC2 实例自动扩展组中，并跨多个 AWS 区域部署。用户遍布全球，但大多数来自日本和瑞典。由于这两个地区的法规遵从性要求，您希望日本用户连接到亚太地区-东北-1 亚太地区（东京）的服务器，而瑞典用户应连接到 euwest-1 欧盟的服务器（爱尔兰）该地区。

以下哪项服务可以让您轻松满足此要求？ A、 使用路由 53 加权路由策略。

B、 使用路由 53 地理位置路由策略。

C、 设置启用地理限制功能的新 CloudFront web 分发。

D、 设置应用程序负载均衡器，将自动将流量路由到适当的 AWS 区域。

答案 B

分析：

地理位置路由允许您根据用户的地理位置选择服务于流量的资源，这意味着 DNS 查询源自的位置。例如，您可能希望将来自欧洲的所有查询路由到法兰克福地区的 ELB 负载均衡器。当您使用地理定位路由时，您可以本地化您的内容，并以用户的语言呈现部分或全部网站。您还可以使用地理位置路由将内容的分发限制到您拥有分发权限的位置。另一个可能的用途是以可预测的、易于管理的方式平衡端点之间的负载，以便将每个用户位置一致地路由到相同的端点。设置将自动将流量路由到适当 AWS 区域的应用程序负载均衡器是不正确的，因为弹性负载均衡器跨多个可用性区域而不是跨 AWS 区域在 EC2 实例之间分配流量。

在启用地理限制功能的情况下设置新的 CloudFront web 分发版是不正确的，因为 CloudFront 地理限制功能主要用于防止特定地理位置的用户访问您通过 CloudFront 网络分发版分发的内容。与路由 53 中的地理位置路由策略不同，它不允许您根据用户的地理位置选择服务于流量的资源。

使用路由 53 加权路由策略是不正确的，因为这不是满足此场景要求的合适解决方案。它只允许您将多个资源与单个域名（tutorialsdojo.com）或子域名（forums.tutorialdojo.com）关联，并选择路由到每个资源的流量。您必须改用地理位置路由策略。

参考文献：

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html> <https://aws.amazon.com/高级支持/知识中心/地理位置路由策略> 查看此 Amazon Route 53 备忘单：

<https://tutorialsdojo.com/amazon-route-53/>

延迟路由 vs 地理邻近路由 vs 地理定位路由：

<https://tutorialsdojo.com/latency-routing-vs-geoproximity-routing-vs-geolocation-routing/AWS> 服务备忘单比较：

<https://tutorialsdojo.com/comparison-of-aws-services/>

Q150. 一个情报机构开发了一个导弹跟踪应用程序，该应用程序托管在开发和生产 AWS 账户上。情报局的初级开发人员只能使用开发账户。她已获得安全许可，可以访问该机构的生产帐户，但访问只是临时的，只允许对 EC2 和 S3 进行写访问。以下哪项允许您发布短期访问令牌，作为临时安全凭证，以允许访问 AWS 资源？

A、 所有给定的选项都是正确的。

- B、使用 AWS 和 STS
- C、使用 AWS 和 SSO
- D、使用 AWS Cognito 发布 JSON Web 令牌（JWT）

答案 B

分析：

AWS 安全令牌服务（AWS STS）是一种服务，您可以使用该服务创建并向可信用户提供临时安全凭证，以控制对 AWS 资源的访问。临时安全凭据的工作方式与 IAM 用户可以使用的长期访问密钥凭据几乎相同。

在此图中，开发帐户（角色假设帐户）中的 IAM 用户 Alice 需要访问 Prod 帐户（角色拥有帐户）。下面是它的工作原理：

开发帐户中的 Alice 通过调用 AssumeRole 在 Prod 帐户中担任 IAM 角色（WriteAccess）。

STS 返回一组临时安全凭据。

Alice 使用临时安全凭据访问 Prod 帐户中的服务和资源。例如，Alice 可以调用 Amazon S3 和 Amazon EC2，这是由 WriteAccess 角色授予的。

使用 AWS Cognito 发布 JSON Web 令牌（JWT）是不正确的，因为 Amazon Cognito 服务主要用于用户身份验证，而不是提供对 AWS 资源的访问。JSON Web 令牌（JWT）用于用户身份验证和会话管理。使用 AWS SSO 是不正确的。虽然 AWS SSO 服务使用 STS，但它本身不会发出短期凭证。AWS 单点登录（SSO）是一种云 SSO 服务，可以方便地集中管理对多个 AWS 帐户和业务应用程序的 SSO 访问。表示上述所有内容的选项是不正确的，因为只有 STS 能够提供临时安全凭证。

参考：

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_temp.html AWS 身份服务概述：

<https://www.youtube.com/watch?v=AIUw0i8rr0>

查看此 AWS IAM 备忘单：

<https://tutorialsdojo.com/aws-identity-and-access-management-iam/Dojo> 的 AWS 认证解决方案架构师助理考试学习指南教程：<https://tutorialsdojo.com/aws-certified-solutions-architect-associate/>

Q151.一家数字媒体公司将静态内容分享给世界各地的高级用户，也分享给他们联合媒体文件的合作伙伴。该公司正在寻找降低服务器成本的方法，并以低延迟安全地向全球客户交付数据。应该使用哪种服务组合来提供最合适和最经济高效的体系结构？（选择两个。）

- A、亚马逊 S3
- B、AWS 全球加速器
- C、AWSλ
- D、亚马逊云端

E、AWS Fargate

回答广告

分析:

Amazon CloudFront 是一个快速内容交付网络（CDN）服务，它以低延迟、高传输速度安全地向全球客户交付数据、视频、应用程序和 API，所有这些都在一个开发人员友好的环境中。

CloudFront 与 AWS 集成？这两个物理位置都直接连接到 AWS 全球基础设施以及其他 AWS 服务。CloudFront 可与 AWS Shield for DDoS 缓解、Amazon S3、弹性负载平衡或 Amazon EC2 等服务无缝协作，作为应用程序的来源，以及

Lambda@Edge 运行更接近客户用户的自定义代码，并自定义用户体验。最后，如果您使用 AWS 来源，如 Amazon S3、Amazon EC2 或弹性负载平衡，则不需要为这些服务和 CloudFront 之间传输的任何数据付费。Amazon S3 是一种对象存储，用于存储和检索互联网上任何位置的任何数量的数据。这是一种简单的存储服务，它以非常低的成本提供了一个非常耐用、高度可用、可无限扩展的数据存储基础架构。

AWS 全球加速器和 Amazon CloudFront 是使用 AWS 全球网络及其全球边缘位置的独立服务。CloudFront 提高了可缓存内容（如图像和视频）和动态内容（如 API 加速和动态站点交付）的性能。全局加速器通过将边缘的数据包代理给在一个或多个 AWS 区域中运行的应用程序，提高了 TCP 或 UDP 上各种应用程序的性能。全局加速器非常适合非 HTTP 用例，如游戏（UDP）、物联网（MQTT）或 IP 语音，以及特别需要静态 IP 地址或确定性快速区域故障转移的 HTTP 用例。这两种服务都与 AWS Shield 集成，以提供 DDoS 保护。

因此，正确的选项是 Amazon CloudFront 和 Amazon S3。AWS Fargate 是不正确的，因为该服务只是一个用于容器的无服务器计算引擎，可与 Amazon 弹性容器服务（ECS）和 Amazon 弹性 Kubernetes 服务（EKS）一起使用。尽管这项服务比基于服务器的服务更具成本效益，但 Amazon S3 的成本仍然远低于 Fargate，尤其是在存储静态内容方面。

AWS Lambda 是不正确的，因为它只允许您在无服务器的情况下运行代码，而无需配置或管理服务器。虽然这也是一项经济高效的服务，因为您只需支付所消耗的计算时间，但您不能将其用于存储静态内容或作为内容交付网络（CDN）。更好的组合是 Amazon CloudFront 和 Amazon S3。

AWS 全球加速器不正确，因为此服务更适用于非 HTTP 用例，如游戏（UDP）、物联网（MQTT）或 IP 语音，以及特别需要静态 IP 地址或确定性快速区域故障转移的 HTTP 用例。此外，没有直接的方法可以将 AWS 全球加速器与 Amazon S3 集成。在这种情况下，更适合使用 Amazon CloudFront。

参考文献:

<https://aws.amazon.com/premiumsupport/knowledge-center/cloudfront-serve-static-website/>

<https://aws.amazon.com/blogs/networking-and-content-delivery/amazon-s3-amazon-cloudfront-a-match-云中制造>

[/https://aws.amazon.com/global-accelerator/faqs/](https://aws.amazon.com/global-accelerator/faqs/)

Q152.解决方案架构师正在构建云基础设施，其中 EC2 实例需要访问各种 AWS 服务，如 S3 和 Redshift。架构师还需要向系统管理员提供访问权限，以便他们可以部署和测试他们的更改。

应使用哪种配置来确保对资源的访问是安全的，并且不会受到影响？

（选择两个。）

A、将 AWS 访问密钥存储在 ACM 中。

- B、将 AWS 访问密钥存储在 EC2 实例中。
- C、启用多因素身份验证。
- D、为 Amazon EC2 实例分配 IAM 角色。
- E、为每个 Amazon EC2 实例分配一个 IAM 用户。

对裁谈会的答复

分析：

在这种情况下，正确答案是：

- 启用多因素身份验证
- 为 Amazon EC2 实例分配 IAM 角色

始终记住，为了访问其他 AWS 服务，您应该将 IAM 角色与 EC2 实例相关联，而不是 IAM 用户。IAM 角色的设计使应用程序可以安全地从实例发出 API 请求，而无需管理应用程序使用的安全凭据。您可以委托使用 IAM 角色进行 API 请求的权限，而不是创建和分发 AWS 凭据。

AWS 多因素身份验证（MFA）是一种简单的最佳实践，它在用户名和密码的基础上添加了额外的保护层。启用 MFA 后，当用户登录 AWS 网站时，将提示他们输入用户名和密码（第一个因素——他们知道什么），以及 AWS MFA 设备的身份验证码（第二个因素——拥有什么）。综上所述，这些因素为您的 AWS 帐户设置和资源提供了更高的安全性。您可以为您的 AWS 帐户和您在帐户下创建的个人 IAM 用户启用 MFA。MFA 还可用于控制对 AWS 服务 API 的访问。

在 EC2 实例中存储 AWS 访问密钥不正确。AWS 不建议这样做，因为它可能会受到损害。您可以使用 IAM 角色为这些应用程序提供临时访问密钥，而不是将访问密钥存储在 EC2 实例上，供在该实例上运行并发出 AWS API 请求的应用程序使用。

为每个 Amazon EC2 实例分配 IAM 用户是不正确的，因为不需要为此场景创建 IAM 用户，因为 IAM 角色已经提供了更大的灵活性和更容易的管理。将 AWS 访问密钥存储在 ACM 中是不正确的，因为 ACM 只是一种服务，可以让您轻松配置、管理和部署用于 AWS 服务和内部连接资源的公共和私有 SSL/TLS 证书。它不用作访问密钥的安全存储。

参考文献：

<https://aws.amazon.com/iam/details/mfa/>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html> 查看此 AWS IAM 备忘

单：<https://tutorialsdojo.com/aws-identity-and-access-management-iam/>

Q153. 一家公司计划将其所有应用程序迁移到 AWS。解决方案架构师建议将所有数据存储到 EBS 卷。首席技术官担心，由于法规遵从性要求、停机情况和 IOPS 性能，EBS 卷不适合现有工作负载。以下哪一点是证明 EBS 是用于迁移的最佳服务的有效点？（选择两个。）

- A、EBS 卷可以连接到任何可用性区域中的任何 EC2 实例。

- B、在可用性区域中创建 EBS 卷时，它将自动复制到单独的 AWS 区域，以防止由于任何单个硬件组件的故障而导致数据丢失。
- C、EBS 卷是脱离实例的存储，可以独立于实例的生命周期进行保存。
- D、EBS 卷在生产中支持实时配置更改，这意味着您可以在不中断服务的情况下修改卷类型、卷大小和 IOPS 容量。
- E、Amazon EBS 提供了创建任何 EBS 卷的快照（备份）并将卷中数据的副本写入 Amazon RDS 的能力，并将其冗余存储在多个可用性区域中

对裁谈会的答复

分析：

Amazon EBS 卷是一个持久的块级存储设备，可以连接到单个 EC2 实例。可以将 EBS 卷用作需要频繁更新的数据的主存储，例如实例的系统驱动器或数据库应用程序的存储。您还可以将它们用于执行连续磁盘扫描的吞吐量密集型应用程序。EBS 卷独立于 EC2 实例的运行寿命而存在。

以下是有关 EBS 卷的重要信息列表：

- 在可用性区域中创建 EBS 卷时，它将自动复制到该区域中，以防止由于任何单个硬件组件的故障而导致数据丢失。
- EBS 卷一次只能连接到一个 EC2 实例。
- 创建卷后，可以将其连接到同一可用性区域中的任何 EC2 实例
- EBS 卷是脱离实例的存储，可以独立于实例的生命周期进行保存。在创建实例期间终止 EC2 实例时，可以指定不终止 EBS 卷。
- EBS 卷在生产中支持实时配置更改，这意味着您可以在不中断服务的情况下修改卷类型、卷大小和 IOPS 容量。
- Amazon EBS 加密使用 256 位高级加密标准算法（AES-256）
- EBS 卷提供 99.999% 的 SLA。

该选项表示：当您在可用性区域中创建 EBS 卷时，它会自动复制到单独的 AWS 区域上，以防止由于任何单个硬件组件的故障而导致数据丢失，这是不正确的，因为当您在一个可用性区域创建 EBS 卷时，它只会在该区域内自动复制，而不会在单独的 AWS 区域上复制，以防止由于任何单个硬件组件的故障而导致的数据丢失。

“EBS 卷可以连接到任何可用性区域中的任何 EC2 实例”选项不正确，因为 EBS 卷只能连接到同一可用性区域的 EC2 实例。选项表示：Amazon EBS 提供创建任何 EBS 卷的快照（备份）的能力，并将卷中的数据副本写入 Amazon RDS，并在其中以多可用性冗余存储

区域几乎是正确的。但是，不是将卷存储到 Amazon RDS，而是将 EBS 卷快照发送到 Amazon S3。

参考文献：

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumes.html> <https://aws.amazon.com/ebs/特征/>

查看此亚马逊 EBS 备忘单：

<https://tutorialsdojo.com/amazon-ebs/>

以下是关于 EBS 的简短视频教程：

<https://youtu.be/ljYH5lHQdxo>

Q154. 公司需要评估和审计其 AWS 账户中的所有配置。它必须通过跟踪对任何 Amazon S3 存储桶所做的所有配置更改来强制执行严格的合规性。还应自动识别可公开访问的 S3 存储桶，以避免数据泄露。以下哪个选项将满足此要求？

- A、使用 AWS CloudTrail 并查看您的 AWS 帐户的事件历史记录。
- B、使用 AWS Trusted Advisor 分析您的 AWS 环境。
- C、使用 AWS IAM 生成凭证报告。
- D、使用 AWS 配置在 AWS 帐户中设置规则。

答案 D

分析：

AWS 配置是一项服务，它使您能够评估、审核和评估 AWS 资源的配置。Config 持续监控和记录 AWS 资源配置，并允许您根据所需配置自动评估记录的配置。通过配置，您可以查看 AWS 资源之间配置和关系的变化，深入了解详细的资源配置历史，并确定您对内部指南中指定的配置的总体合规性。这使您能够简化法规遵从性审核、安全性分析、更改管理和操作故障排除。

您可以使用 AWS 配置来评估 AWS 资源的配置设置。通过创建 AWS 配置规则，您可以在 AWS 帐户中实施理想配置。它还检查资源中应用的配置是否违反规则中的任何条件。AWS 配置仪表板显示规则和资源的合规状态。您可以验证资源是否符合所需配置，并了解哪些特定资源不符合配置。因此，正确答案是：使用 AWS 配置在 AWS 帐户中设置规则。“使用 AWS Trusted Advisor 分析 AWS 环境”选项不正确，因为 AWS Trust Advisor 仅提供最佳实践建议。它不能为您的 AWS 资源定义规则。“使用 AWS IAM 生成凭证报告”选项不正确，因为该报告将无法帮助您评估资源。IAM 凭证报告只是 AWS 帐户中所有 IAM 用户的列表。“使用 AWS CloudTrail 并查看 AWS 帐户的事件历史记录”选项不正确。尽管它可以跟踪更改并存储资源发生的历史记录，但该服务仍然无法强制执行规则以符合组织的策略。

参考文献：

<https://aws.amazon.com/config/>

<https://docs.aws.amazon.com/config/latest/developerguide/evaluate-config.html> 查看此 AWS 配置备忘单：

<https://tutorialsdojo.com/aws-config/>

Dojo 的 AWS 认证解决方案架构师助理考试学习指南教程：<https://tutorialsdojo.com/aws-certified-solutions-architect-associate-saa-c02/>

Q155. 一名数据工程师正在为一家诉讼公司的案件历史应用程序工作。工程师需要跟踪公司处理的所有案例。静态资产（如.jpg、.png 和.pdf 文件）存储在 S3 中，以提高成本效率和耐用性。由于这些文件对业务至关重要

要，工程师希望跟踪 S3 bucket 中发生的情况。工程师发现，每当 S3 bucket 中发生删除或写入操作时，S3 都会发出事件通知。S3 存储桶可能的事件通知目的地是什么？（选择两个。）

- A、SQS
- B、主权财富基金
- C、SES
- D、λ 函数
- E、运动

回答广告

分析：

AmazonS3 通知功能允许您在 bucket 中发生某些事件时接收通知。要启用通知，您必须首先添加一个通知配置，标识您希望 Amazon S3 发布的事件，以及您希望 Amazon S3 发送事件通知的目的地。

Amazon S3 支持以下发布事件的目的地：Amazon 简单通知服务（Amazon SNS）主题-一种协调和管理向订阅端点或客户端发送消息的 web 服务。

Amazon 简单队列服务（Amazon SQS）队列-提供可靠和可扩展的托管队列，用于存储在计算机之间传输的消息。

AWS Lambda-AWS Lambada 是一种计算服务，您可以上传代码，该服务可以使用 AWS 基础设施代表您运行代码。创建 Lambda 函数时，将自定义代码打包并上传到 AWS Lambda

Kinesis 是不正确的，因为它用于收集、处理和分析实时流数据，以便您能够及时了解并快速响应新信息，而不是用于事件通知。您必须使用 SNS、SQS 或 Lambda。

SES 是不正确的，因为它主要用于发送电子邮件，旨在帮助数字营销人员和应用程序开发人员发送营销、通知和交易电子邮件，而不是从 S3 发送事件通知。您必须使用 SNS、SQS 或 Lambda。SWF 是不正确的，因为它主要用于构建应用程序，这些应用程序使用亚马逊的云来跨分布式组件协调工作，而不是用于触发 S3 的事件通知。您必须使用 SNS、SQS 或 Lambda。

要在应用程序中开始使用此新功能，您需要执行以下操作：

如有必要，创建队列、主题或 Lambda 函数（为了简洁起见，我将其称为目标函数）。授予 S3 发布到目标或调用 Lambda 函数的权限。对于 SNS 或 SQS，您可以通过对主题或队列应用适当的策略来实现。对于 Lambda，必须创建并提供 IAM 角色，然后将其与 Lambda 函数关联。

安排调用应用程序以响应目标上的活动。稍后您将看到，这里有几个选项。

将 bucket 的通知配置设置为指向目标。

参考：

<https://docs.aws.amazon.com/AmazonS3/latest/dev/NotificationHowTo.html> 查看此 Amazon S3 备忘单：

<https://tutorialsdojo.com/amazon-s3/>

Dojo 的 AWS 认证解决方案架构师助理考试学习指南教程：<https://tutorialsdojo.com/aws-certified-solutions-architect-associate/>

Q156. 一家公司正在构建一个内部应用程序，作为两个用户上传图像的存储库。每当用户上传图像时，它将被发送到 **Kinesis** 数据流进行处理，然后存储在 S3 存储桶中。如果上传成功，应用程序将返回一个提示，通知用户操作成功。整个处理通常需要大约 5 分钟才能完成。以下哪个选项将允许您异步处理从上传请求到 **Kinesis**、S3 的应用程序请求，并以最具成本效益的方式返回回复？

- A、 将 Kinesis 数据流替换为 Amazon SQS 队列。创建一个 Lambda 函数来异步处理请求。
- B、 使用 SQ 组合对请求进行排队，然后使用按需 EC2 安装异步处理它们。
- C、 使用 Lambda 和 Step 函数的组合来编排服务组件并异步处理请求。
- D、 使用 SNS 组合缓冲请求，然后使用按需 EC2 实例异步处理请求。

答：

分析：

AWS Lambda 支持 Lambda 函数的同步和异步调用。只有在调用 Lambda 函数时，才能控制调用类型。当您使用 AWS 服务作为触发器时，每个服务的调用类型都是预先确定的。您无法控制这些事件源在调用 Lambda 函数时使用的调用类型。由于处理只需 5 分钟，因此 Lambda 也是一种经济高效的选择。您可以使用 AWS Lambda 函数处理 Amazon 简单队列服务（Amazon）中的消息

SQS）队列。Lambda 事件源映射支持标准队列和先进先出（FIFO）队列。使用 AmazonSQS，您可以通过将任务发送到队列并异步处理它们，从而从应用程序的一个组件中卸载任务。

Kinesis 数据流是一种实时数据流服务，需要提供碎片。

亚马逊

SQS 是一个更便宜的选择，因为您只需支付您使用的费用。由于在给定场景中不需要实时处理，因此使用 Amazon SQS 替换 Kinesis 数据流将节省更多成本。

因此，正确的答案是：将 Kinesis 流替换为 Amazon SQS 队列。创建将异步处理请求的 Lambda 函数。

使用 Lambda 和 Step 函数的组合来编排服务组件并异步处理请求是不正确的。AWS Step Functions 服务允许您将多个 AWS 服务协调到无服务器工作流中，以便快速构建和更新应用程序。虽然这可能是一个有效的解决方案，但由于应用程序没有太多的组件需要协调，因此成本效益不高。Lambda 函数可以有效地满足此场景中的需求，而无需使用阶跃函数。这项服务的成本效益不如 Lambda。

使用 SQ 组合对请求进行排队，然后使用按需 EC2 异步处理它们
实例和使用 SNS 组合来缓冲请求，然后使用 OnDemand EC2 实例异步处理它们都是不正确的，因为使用按需 EC2 实例不经济。最好使用 Lambda 函数。

参考文献：

<https://docs.aws.amazon.com/lambda/latest/dg/welcome.html>

<https://docs.aws.amazon.com/lambda/latest/dg/lambda-invocation.html> <https://aws.amazon.com/blogs/compute/newaws-lambda-controls-for-stream-processing-and-异步调用/>

AWS Lambda 概述-AWS 中的无服务器计算：

<https://www.youtube.com/watch?v=bPVX1zHwAnY>

Dojo 的 AWS 认证解决方案架构师助理考试学习指南教程：<https://tutorialsdojo.com/aws-certified-solutions-architect-associate/>

Q157.一家媒体公司在其内部服务器上托管了大约 250 TB 的大量存档数据。他们决定将这些数据转移到 S3，因为它的持久性和冗余性。该公司目前有一条 100 Mbps 的专用线路将其总部连接到互联网。以下哪一项是将所有这些数据导入 Amazon S3 的最快和最具成本效益的方法？

- A、直接上传到 S3
- B、使用 AWS 雪车将数据传输至 S3。
- C、建立 AWS 直接连接，然后将数据传输到 S3。
- D、订购多台 AWS 雪球设备，将文件上传到 Amazon S3。

答案 D

分析：

AWS Snowball 是一个 PB 级的数据传输解决方案，使用安全设备将大量数据传输到 AWS 云中或从 AWS 云端传输出去。使用 Snowball 解决了大规模数据传输的常见挑战，包括高网络成本、长传输时间和安全问题。使用 Snowball 传输数据简单、快速、安全，成本仅为高速互联网的五分之一。如果您需要更安全、更快速地将数 TB 到数 PB 的数据传输到 AWS，Snowball 是数据传输的有力选择。如果您不想对网络基础设施进行昂贵的升级，如果您经常遇到大量数据积压，如果您位于物理隔离的环境中，或者如果您所在的地区无法使用高速互联网连接或成本过高，则 Snowball 也是正确的选择。

根据经验，如果使用现有互联网连接的备用容量将数据上传到 AWS 需要一周以上的时间，那么您应该考虑使用 Snowball。例如，如果您有一个 100 Mb 的连接，可以单独用于传输数据，并且需要传输 100 TB 的数据，则需要 100 天以上的时间才能通过该连接完成数据传输。您可以在大约一周内使用多个雪球进行相同的转移。

因此，订购多个 AWS 雪球设备将文件上传到 Amazon S3 是正确的答案。将其直接上传到 S3 是不正确的，因为由于公司的互联网连接速度慢，这将花费太长时间才能完成。

建立 AWS 直接连接，然后将数据传输到 S3 是不正确的，因为为直接连接提供线路将花费太多时间，并且可能无法提供最快的数据传输解决方案。此外，该场景不保证建立从本地数据中心到 AWS 的专用连接。主要目标是将数据一次性迁移到 AWS，这可以通过使用 AWS 雪球设备实现。

使用 AWS Snowmobile 将数据传输到 S3 是不正确的，因为如果您需要将大量数据移动到 AWS 或需要传输高达 100PB 的数据，Snowmobile 更适合。这将用一个 45 英尺长的加固集装箱运输，由一辆半拖车牵引。请注意，您只需要迁移 250 TB 的数据，因此，这不是最合适和最经济高效的解决方案。

参考文献：

<https://aws.amazon.com/snowball/>

<https://aws.amazon.com/snowball/faqs/>

S3 传输加速 vs 直连 vs VPN vs 雪球 vs 雪地车：

<https://tutorialsdojo.com/s3-transfer-acceleration-vs-direct-connect-vs-vpn-vs-snowball-vs-snowmobile/AWS> 服务备忘单比较：<https://tutorialsdojo.com/comparison-of-aws-services/>

Q158. 一家公司正在与政府机构合作，改善交通规划和道路维护，以防止事故。建议的解决方案是实时管理交通基础设施，在检测到问题时向交通工程师和应急响应团队发出警报，并通过使用传感器和智能设备自动改变交通信号，使应急人员更快地到达事故现场。哪个 AWS 服务将允许该机构的开发人员将智能设备连接到基于云的应用程序？

- A、AWS 弹性豆茎
- B、AWS 云形成
- C、Amazon 弹性容器服务
- D、AWS 物联网核心

答案 D

分析：

AWS 物联网核心是一种托管云服务，可让连接的设备轻松安全地与云应用程序和其他设备交互。AWS 物联网核心提供跨各种连接设备和位置的安全通信和数据处理，因此您可以轻松构建物联网应用程序。AWS 物联网核心允许您将多个设备连接到云和其他设备，而无需部署或管理任何服务器。您还可以根据您定义的规则动态过滤、转换和处理设备数据。使用 AWS 物联网核心，您的应用程序可以随时跟踪并与您的所有设备通信，即使它们未连接。

因此，正确答案是：AWS 物联网核心。

AWS CloudFormation 是不正确的，因为它主要用于创建和管理架构，而不是处理连接的设备。您必须使用 AWS 物联网核心。AWS Elastic Beanstalk 是不正确的，因为它只是一个易于使用的服务，用于部署和扩展使用 Java、.NET、PHP 和 Node 开发的 web 应用程序和服务。js、Python 和其他编程语言。Elastic Beanstalk 不能用于将智能设备连接到基于云的应用程序。Amazon 弹性容器服务不正确，因为它主要用于创建和管理 docker 实例，而不是用于处理设备。

参考文献: [https://aws.amazon.com/iot-](https://aws.amazon.com/iot-core/)

[core/ https://aws.amazon.com/iot/](https://aws.amazon.com/iot/)

Q159. 商业银行有外汇交易应用程序。他们创建了一个 EC2 实例的自动扩展组，使银行能够处理当前流量并实现成本效益。他们希望自动缩放组在缩小 EC2 实例数量之前遵循预定义参数集，从而保护系统不受意外减速或不可用的影响。关于冷却期，以下哪项陈述是正确的？（选择两个。）

- A、 其默认值为 300 秒。
- B、 它确保自动缩放组不会在先前的缩放活动生效之前启动或终止其他 EC2 实例。
- C、 它确保自动缩放组在不停机的情况下启动或终止其他 EC2 实例。
- D、 其默认值为 600 秒。
- E、 它确保在自动缩放组扩展之前，EC2 实例有足够的时间冷却。

回答 AB

分析:

在自动缩放中，以下关于冷却期的陈述是正确的:

它确保自动缩放组不会在上一个缩放活动生效之前启动或终止其他 EC2 实例。

其默认值为 300 秒。

这是自动缩放组的可配置设置。

以下选项不正确:

- 它确保在自动缩放组扩展之前，EC2 实例有足够的时间冷却。
- 它确保自动缩放组在不停机的情况下启动或终止其他 EC2 实例。
- 其默认值为 600 秒。

这些陈述不准确，没有描述“冷却”一词对自动缩放的实际含义。冷却期是自动缩放组的可配置设置，有助于确保在上一个缩放活动生效之前不会启动或终止其他实例。在自动缩放组使用简单的缩放策略动态缩放后，它将等待冷却期结束，然后再恢复缩放活动。

下图演示了缩放冷却:

参考:

<http://docs.aws.amazon.com/autoscaling/latest/userguide/as-instance-termination.html> 查看此 AWS 自动缩放

备忘单: <https://tutorialsdojo.com/aws-auto-scaling/>

Dojo 的 AWS 认证解决方案架构师助理考试学习指南教程: <https://tutorialsdojo.com/aws-certified-solutions-architect-associate/>

Q160.组织需要控制多个 S3 桶的访问。他们计划使用网关端点来允许访问受信任的存储桶。

以下哪项可以帮助您实现此要求?

- A、为受信任的 S3 存储桶生成端点策略。
- B、为受信任的 VPC 生成 bucket 策略。
- C、为可信 VPC 生成端点策略。
- D、为受信任的 S3 存储桶生成存储桶策略。

答:

分析:

VPC 端点使您能够私自将 VPC 连接到由 AWS PrivateLink 提供支持的 AWS 服务和 VPC 端点服务,而无需互联网网关、NAT 设备、VPN 连接或 AWS 直接连接。VPC 中的实例不需要公共 IP 地址与服务中的资源通信。专有网络和其他服务之间的流量不会离开亚马逊网络。

创建 VPC 端点时,可以附加端点策略,该策略控制对所连接服务的访问。您可以修改附加到端点的端点策略,并添加或删除端点使用的路由表。端点策略不会覆盖或替换 IAM 用户策略或特定于服务的策略(如 S3 存储桶策略)。它是一个单独的策略,用于控制从端点到指定服务的访问。

我们可以使用 bucket 策略或端点策略来允许流量流向受信任的 S3 bucket。具有“可信 S3 存储桶”关键短语的选项将是本场景中的可能答案。要为每个 S3 bucket 配置 bucket 策略,而不是使用单个端点策略,需要花费大量时间。因此,您应该使用端点策略来控制到受信任 Amazon S3 存储桶的流量。因此,正确的答案是:为受信任的 S3 存储桶生成端点策略。“为受信任的 S3 存储桶生成存储桶策略”选项不正确。尽管这是一个有效的解决方案,但为每个 S3 bucket 设置 bucket 策略需要花费大量时间。这可以简单地通过创建 S3 端点策略来实现。

“为受信任的 VPC 生成 bucket 策略”选项不正确,因为您正在为受信任 VPC 生成策略。请记住,该场景只要求您允许受信任的 S3 bucket 的流量,而不是 VPC 的流量。

“为可信 VPC 生成端点策略”选项不正确,因为它只允许访问可信 VPC,而不允许访问可信 Amazon S3 存储桶引用:

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-endpoints-s3.html>

<https://aws.amazon.com/premiumsupport/knowledge-center/connect-s3-vpc-endpoint/> 亚马逊专有网络概述:

<https://www.youtube.com/watch?v=oIDHKeNxvQQ>

查看此亚马逊 VPC 备忘单: <https://tutorialsdojo.com/amazon-vpc/>

Q161. 一家公司有一个托管在 Amazon ECS Docker 容器上的企业 web 应用程序，其高性能计算工作负载使用 Amazon FSx for Lustre 文件系统。另一个 AWS 区域正在运行热备用环境，用于灾难恢复。分配了一名解决方案架构师来设计一个系统，该系统将仅在主应用程序堆栈发生中断时自动将实时流量路由到灾难恢复（DR）环境。架构师应该如何满足这一要求？

- A、 设置 CloudWatch 事件规则以监视主路由 53 DNS 端点，并创建自定义 Lambdafunction。使用函数执行 ChangeResourceRecordSets API 调用，以启动到辅助 DNS 记录的故障转移。
- B、 通过在主堆栈和 DR 环境上添加健康检查，在路由 53 中设置加权路由策略配置。配置网络访问控制列表和路由表，以允许路由 53 向健康检查中指定的端点发送请求。
- C、 通过在主服务端点上添加健康检查，在路由 53 中设置故障转移路由策略配置。配置路由 53 以在主资源不正常时将 DNS 查询定向到辅助记录。配置网络访问控制列表和路由表，以允许路由 53 向健康检查中指定的端点发送请求。通过将“评估目标运行状况”选项设置为“是”，启用该选项。
- D、 设置 CloudWatch 警报以监控主路由 53 DNS 端点，并创建自定义 Lambda 函数。使用函数执行 ChangeResourceRecordSets API 调用，以启动到辅助 DNS 记录的故障转移。

答案 C

分析：

当您希望主资源或资源组在大部分时间都可用，并且希望在所有主资源不可用的情况下，辅助资源或资源群处于备用状态时，请使用主动-被动故障切换配置。当响应查询时，路由 53 仅包括健康的主资源。如果所有主资源都不健康，则响应 DNS 查询，路由 53 开始仅包括健康的辅助资源。要创建具有一个主记录和一个辅助记录的主动-被动故障转移配置，只需创建记录并为路由策略指定故障转移。当主资源健康时，路由 53 使用主记录响应 DNS 查询。当主资源不健康时，路由 53 使用辅助记录响应 DNS 查询。您可以配置运行状况检查，以监视您通过 IP 地址或域名指定的端点。按照您指定的定期间隔，Route 53 通过 Internet 向您的应用程序、服务器或其他资源提交自动请求，以验证其是否可访问、可用和功能正常。或者，您可以配置运行状况检查以发出与用户发出的请求类似的请求，例如从特定 URL 请求网页。

当路由 53 检查端点的运行状况时，它会向创建运行状况检查时指定的 IP 地址和端口发送 HTTP、HTTPS 或 TCP 请求。要使健康检查成功，路由器和防火墙规则必须允许来自路由 53 健康检查程序使用的 IP 地址的入站流量。

因此，正确的答案是：通过在主服务端点上添加健康检查，在路由 53 中设置故障转移路由策略配置。配置路由 53 以在主资源不正常时将 DNS 查询定向到辅助记录。配置网络访问控制列表和路由表，以允许路由 53 向健康检查中指定的端点发送请求。通过将“评估目标运行状况”选项设置为“是”，启用该选项。

该选项表示：通过在主堆栈和 DR 环境上添加健康检查，在路由 53 中设置加权路由策略配置。配置网络访问控制列表和路由表，以允许路由 53 向健康检查中指定的端点发送请求。通过将“评估目标运行状况”选项设置为启用

“是”不正确，因为加权路由仅允许您将多个资源与单个域名（tutorialsdojo.com）或子域名（blog.tutorialddojo.com）关联，并选择路由到每个资源的流量。这可以用于多种用途，包括负载平衡和测试软件的新版本，但不用于故障切换配置。请记住，该场景表示，解决方案应仅在以下情况下自动将实时流量路由到灾难恢复（DR）环境：

主应用程序堆栈发生中断的事件。此配置在主环境和灾难恢复环境中的流量分配不正确。该选项表示：设置 CloudWatch 警报以监控主路由 53 DNS 端点，并创建自定义 Lambda 函数。使用函数执行 ChangeResourceRecordSets API 调用以启动到辅助 DNS 记录的故障转移是不正确的，因为设置 CloudWatch 警

报和使用路由 53 API 在这种情况下既不适用，也没有任何用处。请记住，CloudWatch ALM 主要用于监控 CloudWatch 指标。您必须改用故障转移路由策略。该选项表示：设置 CloudWatch 事件规则以监视主路由 53 DNS 端点并创建自定义 Lambda 函数。使用函数执行 ChangeResourceRecordsets API 调用以启动到辅助 DNS 记录的故障转移是不正确的，因为 Amazon CloudWatch 事件服务通常用于提供描述某些 Amazon Web 服务（AWS）资源变化的近实时系统事件流。CloudWatch 事件无法直接监控您的路由 53 端点的状态。您必须在路由 53 中配置健康检查和故障转移配置，以满足此场景中的要求。

参考文献：

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-types.html>

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/health-checks-types.html>

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-router-firewall-rules.html> 查看此亚马逊

逊路线 53 备忘单：<https://tutorialsdojo.com/amazon-route-53/>

问题 162：一位解决方案架构师正在为一家在其数据中心使用 Chef 配置管理的公司工作。她需要利用 AWS 中现有的厨师食谱。

她应该使用以下哪项服务？

- A、AWS 云形成
- B、AWS OpsWorks
- C、Amazon 简单工作流服务
- D、AWS 弹性豆茎

答案 B

分析：

AWS OpsWorks 是一种配置管理服务，提供 Chef 和 Puppet 的托管实例。Chef 和 Puppet 是自动化平台，允许您使用代码自动配置服务器。OpsWorks 允许您使用 Chef 和 Puppet 自动化服务器在 Amazon EC2 实例或本地计算环境中的配置、部署和管理。OpsWorks 有三种产品-用于厨师自动化的 AWS OpsWorks、用于木偶企业的 AWS OpsWorks 和 AWS Opworks 堆栈。

Amazon 简单工作流服务是不正确的，因为 AWS SWF 是云中完全受管理的状态跟踪器和任务协调器。它不允许您利用厨师食谱。AWS 弹性 Beanstalk 是不正确的，因为它处理应用程序的部署细节，包括容量配置、负载均衡、自动扩展和应用程序健康监控。它不允许您像亚马逊 SWF 那样利用厨师食谱。

AWS CloudFormation 是不正确的，因为它是一种服务，允许您创建相关 AWS 资源的集合，并以可预测的方式使用基础设施作为代码提供它们。它不允许您像 Amazon SWF 和 AWS Elastic Beanstalk 一样利用厨师食谱。

参考：<https://aws.amazon.com/opsworks/>

查看此 AWS OpsWorks 备忘单：

<https://tutorialsdojo.com/aws-opsworks/>

弹性 Beanstalk vs CloudFormation vs OpsWorks vs CodeDeploy:

<https://tutorialsdojo.com/elastic-beanstalk-vs-cloudformation-vs-opsworks-vs-codedeploy/AWS> 服务备忘单比

较: <https://tutorialsdojo.com/comparison-of-aws-services/>

Q163. 一个组织目前正在使用磁带备份解决方案在本地存储其应用程序数据。他们计划使用云存储服务将备份数据保存长达 10 年，每年可访问一次或两次。

以下哪一项是实施此解决方案最具成本效益的选项？

- A、使用 AWS 存储网关将数据直接备份到 Amazon S3 Glacier Deep Archive。
- B、订购 AWS Snowball Edge 设备，将备份直接导入 Amazon S3 Glacier。
- C、使用 AWS 存储网关将数据直接备份到 Amazon S3 Glacier。
- D、使用 Amazon S3 存储备份数据，并添加生命周期规则以将当前版本转换为 Amazon S3 Glacier。

答:

分析:

Tape Gateway 使您能够在 AWS 中用虚拟磁带替换本地使用的物理磁带，而无需更改现有备份工作流。磁带网关支持所有领先的备份应用程序，并在本地缓存虚拟磁带，以实现低延迟数据访问。Tape Gateway 加密网关和 AWS 之间的数据，以实现安全的数据传输，并压缩数据并在 Amazon S3 和 Amazon S3 Glacier 之间转换虚拟磁带，或 Amazon S3 Glacier Deep Archive，以最大限度地降低存储成本。该场景要求您将应用程序数据备份到云存储服务，以便长期保留将保留 10 年的数据。由于它使用磁带备份解决方案，因此使用 AWS 存储网关的选项必须是可能的答案。Tape Gateway 可以移动亚马逊 S3 冰川或亚马逊 S3 冰河深度存档存储类中存档的虚拟磁带，使您能够进一步降低在云中存储长期数据的每月成本，最高可达 75%。因此，正确的答案是：使用 AWS 存储网关将数据直接备份到 Amazon S3 Glacier Deep Archive。使用 AWS 存储网关将数据直接备份到 Amazon S3 Glacier 的选项不正确。尽管这是一个有效的解决方案，但移动到 S3 冰川比直接将其备份到冰川深度档案更昂贵。

该选项表示：订购 AWS Snowball Edge 设备将备份直接导入 Amazon S3 Glacier 是不正确的，因为 SnowballEdge 无法直接将备份集成到 S3 Glacier。此外，您必须使用 Amazon S3 Glacier Deep Archive 存储类，因为它比常规 Glaciers 类更具成本效益。

“使用 Amazon S3 存储备份数据并添加生命周期规则以将当前版本转换为 Amazon S3 Glacier”的选项不正确。尽管这是一种可能的解决方案，但在不使用存储网关的情况下，很难将磁带备份解决方案直接集成到 S3。参考文献:

<https://aws.amazon.com/storagegateway/faqs/> <https://aws.amazon.com/s3/storage-classes/>

AWS 存储网关概述:

<https://www.youtube.com/watch?v=pNb7xOBJjHE> 查看

此 AWS 存储网关备忘单:

<https://tutorialsdojo.com/aws-storage-gateway/>

Q164. 一家公司正在构建一个转录服务，其中一组 EC2 worker 实例处理上传的音频文件并生成文本文件作为输出。它们必须将这两个频繁访问的文件存储在相同的持久存储中，直到上传程序检索到文本文件。由于预期的需求激增，他们必须确保存储是可扩展的，并且可以在几分钟内检索。

在这种情况下，AWS 中的哪种存储选项既经济又可扩展？

- A、 单个 Amazon S3 桶
- B、 亚马逊 S3 冰川深度档案
- C、 具有快照的多个 Amazon EBS 卷
- D、 多实例存储

答:

分析:

Amazon 简单存储服务（Amazon S3）是一种对象存储服务，提供业界领先的可扩展性、数据可用性、安全性和性能。它提供了易于使用的管理功能，因此您可以组织数据并配置经过微调的访问控制，以满足特定的业务、组织和法规遵从性要求。Amazon S3 的设计具有 99.999999999%（11.9%）的耐用性，并为世界各地的公司存储数百万应用程序的数据。在这种情况下，需要具有经济高效和可扩展的存储。在给定选项中

最好的选择是使用 Amazon S3。这是一种简单的存储服务，以非常低的成本提供了高度可扩展、可靠和低延迟的数据存储基础设施。因此，正确答案是：一个 Amazon S3 bucket。

“多个带有快照的 Amazon EBS 卷”选项不正确，因为 Amazon S3 比 EBS 卷更具成本效益。

“多实例存储”选项不正确。与上面的选项一样，您必须使用 Amazon S3，因为它比实例存储卷更具可扩展性和成本效益。该选项表示：

Amazon S3 Glacier Deep Archive 不正确，因为它主要用于数据检索时间可能超过 12 小时的数据档案。因此，它不适合存储和频繁访问数据的转录服务。

参考文献:

<https://aws.amazon.com/s3/pricing/> <https://docs.aws.amazon.com/AmazonS3/latest/gsg/GetStartedWithS3.html> 查

看此 Amazon S3 备忘单: <https://tutorialsdojo.com/amazon-s3/>

Q165. 一家公司计划进行网络安全审计。web 应用程序托管在一组自动扩展的 EC2 实例上，前面有一个应用程序负载均衡器，以均匀分布传入流量。解决方案架构师的任务是增强公司云基础设施的安全态势，并将 DDoS 攻击对其资源的影响降至最低。

以下哪项是应实施的最有效的解决方案？

- A、 配置 Amazon CloudFront 分发并将网络负载均衡器设置为源。

使用专有网络流量日志监控异常流量模式。设置一个自定义 AWS Lambda 函数，处理流日志并调用 Amazon SNS 进行通知。

B、配置 Amazon CloudFront 分发并将网络负载均衡器设置为源。

使用 Amazon GuardDuty 根据其安全发现阻止可疑主机。设置一个自定义 AWS Lambda 函数，处理安全日志并调用 Amazon SNS 进行通知。

C、配置 Amazon CloudFront 分发，并将应用程序负载均衡器设置为源。创建安全组规则并拒绝所有可疑地址。使用亚马逊 SNS 进行通知。

D、配置 Amazon CloudFront 分发，并将应用程序负载均衡器设置为源。使用 AWS WAF 创建基于速率的 webACL 规则，并将其与 Amazon CloudFront 关联。

答案 D

分析：

AWS WAF 是一个 web 应用程序防火墙，可帮助保护您的 web 应用程序或 API 免受可能影响可用性、危害安全性或消耗过多资源的常见 web 攻击。AWS WAF 使您能够创建阻止常见攻击模式（如 SQL 注入或跨站点脚本）的安全规则，以及过滤您定义的特定流量模式的规则，从而控制流量如何到达应用程序。您可以将 AWS WAF 部署在 Amazon CloudFront 上，作为您的 CDN 解决方案的一部分，该应用程序负载均衡器将您的 web 服务器或运行在 EC2 上的源服务器，或您的 API 的 Amazon API 网关。

要检测和缓解 DDoS 攻击，除了 AWS Shield 之外，还可以使用 AWS WAF。AWS WAF 是一种 web 应用程序防火墙，通过在线检查流量来帮助检测和缓解 web 应用程序层 DDoS 攻击。应用层 DDoS 攻击使用格式良好但恶意的请求来规避缓解并消耗应用程序资源。您可以定义包含一组条件、规则和动作的自定义安全规则，以阻止攻击流量。定义 web ACL 后，可以将其应用于 CloudFront 分发，web ACL 将按照配置时指定的优先级顺序进行评估。

.....

通过使用 AWS WAF，您可以在 CloudFront 发行版或应用程序负载均衡器上配置 web 访问控制列表（web ACL），以根据请求签名过滤和阻止请求。每个 Web ACL 由规则组成，您可以将这些规则配置为字符串匹配或正则表达式匹配一个或多个请求属性，例如 URI、查询字符串、HTTP 方法或头键。此外，通过使用 AWS WAF 基于速率的规则，当匹配规则请求超过您定义的阈值时，您可以自动阻止不良参与者的 IP 地址。来自违规客户端 IP 地址的请求将接收 403 禁止错误响应，并将保持阻止，直到请求速率下降到阈值以下。这对于缓解伪装为常规 web 流量的 HTTP 洪水攻击非常有用。建议您添加带有基于速率的规则 web ACL，作为 AWS Shield 高级保护的一部分。这些规则可以提醒您注意可能指示潜在 DDoS 事件的流量突然增加。基于速率的规则统计在任何五分钟内从任何单个地址到达的请求。如果请求的数量超过您定义的限制，则该规则可以触发一个操作，例如向您发送通知。

因此，正确的答案是：配置 AmazonCloudFront 分发，并将应用程序负载均衡器设置为源。使用 AWS WAF 创建基于速率的 web ACL 规则，并将其与 Amazon CloudFront 关联。该选项表示：配置 Amazon CloudFront 分发并将网络负载均衡器设置为源。使用专有网络流量日志监控异常流量模式。设置一个自定义 AWS Lambda 函数来处理流日志并调用 Amazon SNS 进行通知是不正确的，因为该选项仅允许您监控到达实例的流量。您不能使用专有网络流量日志来缓解 DDoS 攻击。

该选项表示：配置 Amazon CloudFront 分发，并将应用程序负载均衡器设置为源。创建安全组规则并拒绝所有可疑地址。使用亚马逊 SNS 进行通知不正确。要拒绝可疑地址，必须手动插入这些主机的 IP 地址。这是一项人工任务，不是可持续的解决方案。请注意，攻击者生成大量数据包或请求，以压倒目标系统。在这种情况下使用安全组无助于缓解 DDoS 攻击。该选项表示：配置 Amazon CloudFront 分发并将网络负载均衡器设置为源。使用 Amazon GuardDuty 根据其安全发现阻止可疑主机。设置自定义 AWS Lambda 函数来处理安全日志并调用 Amazon SNS 进行通知是不正确的，因为 Amazon GuardDuty 只是一个威胁检测服务。您应该使用 AWS WAF 并创建自己的基于 AWS WAF 速率的规则，以缓解伪装为常规 web 流量的 HTTP 洪水攻击。

参考文献:

<https://docs.aws.amazon.com/waf/latest/developerguide/ddos-overview.html>

<https://docs.aws.amazon.com/waf/latest/developerguide/ddos-get-started-rate-based-rules.html>

https://d0.awsstatic.com/whitepapers/Security/DDoS_White_Paper.pdf 查看 AWS WAF 备忘单:

<https://tutorialsdojo.com/aws-waf/>

AWS 安全服务概述-WAF、Shield、CloudHSM、KMS:

<https://www.youtube.com/watch?v=-1S RdeAmMo>

Q166.一家公司在 **ap-northeast-1** 和 **ap-southeast-2** 地区运行消息应用程序。解决方案

架构师需要创建路由策略，其中来自菲律宾和北印度的大部分流量将路由到 **ap-northeast-1** 区域的资源。解决方案架构师应使用哪种路由 53 路由策略？

- A、 加权路由
- B、 地质邻近路由
- C、 延迟路由
- D、 地理定位路由

答案 B

分析:

亚马逊路由 53 是一个高度可用和可扩展的域名系统 (DNS) 网络服务。您可以使用路由 53 以任意组合执行三个主要功能: 域注册、DNS 路由和健康检查。为域创建托管区域后, 例如, **.com**, 您创建记录来告诉域名系统 (DNS) 您希望如何为该域路由流量。例如, 您可能创建导致 DNS 执行以下操作的记录:

例如, 路由互联网流量。com 到数据中心中主机的 IP 地址。为该域路由电子邮件(jose.rizal@tutorialsdojo.com) 发送到邮件服务器 (mail.tutorialsdojo.com)。为名为 operations.manila.tutorialsdojo 的子域路由流量。com 转换为不同主机的 IP 地址。每个记录包括域或子域的名称、记录类型 (例如, 具有 MX 路由电子邮件类型的记录) 以及适用于记录类型的其他信息 (对于 MX 记录, 一个或多个邮件服务器的主机名以及每个服务器的优先级)。路由 53 有不同的路由策略可供选择。以下是一些政策:

延迟路由允许 Amazon 路由 53 为来自 AWS 区域的用户请求提供最低延迟。然而, 它不能保证同一地理区域的用户将从同一位置得到服务。

Geoproximity 路由允许 Amazon 根据用户和资源的地理位置将流量路由到您的资源。您还可以通过指定一个称为偏差的值, 选择将更多或更少的流量路由到给定资源。偏差会扩大或缩小将流量路由到资源的地理区域的大小。

地理位置路由允许您根据用户的地理位置选择服务于流量的资源，这意味着 DNS 查询源自的位置。加权路由允许您将多个资源与单个域名（`tutorialsdojo.com`）或子域名（`subdomain.tutorialdojo.com`）关联，并选择路由到每个资源的流量。在这种情况下，问题需要一个路由策略，该策略将允许路由 53 将流量从菲律宾和印度北部的较大部分路由到东京地区的资源。您需要使用地理近似路由并指定一个偏差，以控制将流量路由到资源的地理区域的大小。上面的示例图像在东京地区使用了 -40 的偏差，在悉尼地区使用了 1 的偏差。以这种方式设置偏差配置将导致 53 号公路将来自菲律宾中部和北部以及印度北部的交通路由到东京地区的资源。

因此，正确答案是：地质接近性路由。

地理位置路由是不正确的，因为您无法控制在地理位置路由中将流量路由到实例的覆盖范围大小。它只允许您根据用户的位置选择服务于流量的实例。

延迟路由是不正确的，因为它主要用于通过让路由 53 服务于来自提供最低延迟的 AWS 区域的用户请求来提高性能。加权路由不正确，因为它用于按指定的比例将流量路由到多个资源。这对于负载平衡和测试软件的新版本非常有用。

参考文献：<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html#routing-policy-geoproximity>

质邻近性

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html#routing-policy-geoproximity> 延迟路由 vs 地理邻近路由 vs

地理定位路由：<https://tutorialsdojo.com/latency-routing-vs-geoproximity-routing-vs-geolocation-routing/>

Q167.上传到 Amazon S3 bucket 的所有对象必须加密，以符合安全要求。bucket 将使用服务器端加密和 Amazon S3 托管加密密钥（SSE-S3），使用 256 位高级加密标准（AES-256）分组密码对数据进行加密。

必须使用以下哪些请求头？

- A、 x-amz-服务器端加密-客户密钥
- B、 x-amz 服务器端加密
- C、 x-amz-服务器端加密-客户算法
- D、 x-amz-server-side-encryption-customer-key-MD5

答案 B

分析：

服务器端加密保护静止数据。如果您使用服务器端加密与 Amazon S3 托管加密密钥（SSE-S3），Amazon S3 将使用唯一密钥加密每个对象，并且作为额外的保护措施，它使用定期旋转的主密钥加密密钥本身。Amazon S3 服务器端加密使用可用的最强块密码之一，256 位高级加密标准（AES-256）来加密数据。

如果需要对存储在 bucket 中的所有对象进行服务器端加密，请使用 bucket 策略。例如，以下存储桶策略拒绝上传对象的权限，除非请求包含请求服务器端加密的 x-amz-server-side-encryption 头：

但是，如果选择使用客户提供的加密密钥（SSE-C）进行服务器端加密，则必须使用以下请求头提供加密密钥信息：

x-amz-server-side-encryption-customer-algorithm

因此，使用 x-amz-server-side-encryption 报头是正确的，因为这是用于 Amazon S3 托管加密密钥（SSE-S3）的报头。

所有其他选项都不正确，因为它们用于 SSE-C。参考文献：

<https://docs.aws.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html><https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingServerSideEncryption.html> 和 <https://docs.aws.amazon.com/AmazonS3/latest/dev/ServerSideEncryptionCustomerKeys.html> 查看此 Amazon S3 备忘单：<https://tutorialsdojo.com/amazon-s3/>

Q168.公司要求将 80 TB 的数据仓库移动到云端。考虑到当前的带宽分配，传输数据需要 2 个月。哪种服务最经济高效，可以让您快速将数据上传到 AWS？

- A、AWS 雪球边缘
- B、AWS 雪地摩托
- C、AWS 直接连接
- D、Amazon S3 多部分上传

答：

分析：

AWS Snowball Edge 是一种具有有机载存储和计算能力的雪球设备，用于选择 AWS 功能。除了在本地环境和 AWS 云之间传输数据外，Snowball Edge 还可以承担本地处理和边缘计算工作负载。每个雪球边缘设备可以比互联网更快的速度传输数据。这种传输是通过区域运输公司运输设备中的数据来完成的。设备是坚固的运输容器，配有电子墨水运输标签。AWS 雪球边缘设备与标准雪球不同，因为它可以将 AWS 云的力量带到您的本地位置，并具有本地存储和计算功能。

雪球边缘设备有三种设备配置选项？存储优化、计算优化以及 GPU。

因此，正确答案是：AWS 雪球边缘。

AWS Snowmobile 是不正确的，因为这是一种用于向 AWS 传输大量数据的 EB 级数据传输服务。它不适合传输少量数据，如本场景中的 80 TB。每辆雪地摩托，一个 45 英尺长的坚固运输集装箱，由一辆半拖车牵引，最多可运输 100PB。更具成本效益的解决方案是订购雪球边缘设备。

AWS Direct Connect 不正确，因为它主要用于建立从您的房屋网络到 AWS 的专用网络连接。这不适用于一次性数据传输任务，如场景中所示。

Amazon S3 多部分上传是不正确的，因为此功能只允许您上传多个部分中的大型对象。它仍然使用该公司的相同互联网连接，这意味着由于其当前的带宽分配，传输仍然需要时间。

参考文献：

<https://docs.aws.amazon.com/snowball/latest/ug/whatissnowball.html>

<https://docs.aws.amazon.com/snowball/latest/ug/device-differences.html> 查看 AWS 雪球边缘备忘单：

<https://tutorialsdojo.com/aws-snowball-edge/>

AWS Snow 系列概述：<https://youtu.be/9Ar-51Ip53Q>

问题 169. DevOps 团队的一名成员向您咨询了一个 Amazon EC2 实例中的连接问题。应用程序架构最初设置为四个 EC2 实例，每个实例都有一个 EIP 地址，所有这些地址都属于公共非默认子网。您启动了另一个实例来处理应用程序不断增加的工作负载。EC2 实例也属于同一安全组。除了其中一个 EC2 实例无法通过互联网发送或接收流量外，其他一切都正常工作。

以下哪一项最可能是导致此问题的原因？

- A、EC2 实例正在未连接到 Internet 网关的可用性区域中运行。
- B、EC2 实例没有与其关联的公共 IP 地址。
- C、EC2 实例没有与其关联的私有 IP 地址。
- D、路由表未正确配置为允许通过 Internet 网关进出 Internet 的流量。

答案 B

分析：

IP 地址使 VPC 中的资源能够相互通信，并通过 Internet 与资源通信。

亚马逊 EC2 和亚马逊 VPC 支持 IPv4 和 IPv6 寻址协议。默认情况下，Amazon EC2 和 Amazon VPC 使用 IPv4 寻址协议。创建 VPC 时，必须为其分配 IPv4 CIDR 块（一系列私有 IPv4 地址）。无法通过 Internet 访问专用 IPv4 地址。要通过 Internet 连接到实例，或启用实例与其他具有公共端点的 AWS 服务之间的通信，可以为实例分配全局唯一的公共 IPv4 地址。

您可以选择将 IPv6 CIDR 块与 VPC 和子网关联，并将该块中的 IPv6 地址分配给 VPC 中的资源。IPv6 地址是公共的，可以通过互联网访问。所有子网都有一个可修改属性，该属性确定在该子网中创建的网络接口是否分配了公共 IPv4 地址，如果适用，还分配了 IPv6 地址。这包括在子网中启动实例时为实例创建的主网络接口（eth0）。无论子网属性如何，您仍然可以在启动期间覆盖特定实例的此设置。默认情况下，非默认子网的 IPv4 公共寻址属性设置为 false，默认子网将此属性设置为 true。例外情况是由 Amazon EC2 启动实例向导创建的非默认子网——向导将该属性设置为 true。您可以使用 Amazon VPC 控制台修改此属性。

在此场景中，有 5 个 EC2 实例属于同一安全组，应该能够连接到 Internet。主路由表配置正确，但连接到一个实例时出现问题。由于其他四个实例工作正常，我们可以假设安全组和路由表配置正确。此问题的一个可能原因是该实例没有公共或 EIP 地址。

还要注意，四个 EC2 实例都属于公共非默认子网。这意味着新的 EC2 实例在默认情况下将不具有公共 IP 地址，因为自 IPv4 公共寻址属性最初设置为 false。

因此，正确的答案是这样的选项：EC2 实例没有与其关联的公共 IP 地址。

“路由表未正确配置以允许通过 Internet 网关进出 Internet 的流量”选项不正确，因为与同一路由表和安全组关联的其他三个实例没有任何问题。表示：EC2 实例正在未连接到 Internet 网关的可用性区域中运行的选项不正确，因为可用性区域与可能导致问题的 Internet 网关（IGW）之间没有关系。

参考文献：

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario1.html

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-ip-addressing.html#vpc-ip> 地址子网查看此 Amazon VPC

备忘单：<https://tutorialsdojo.com/amazon-vpc/>

Q170.一家提供直观金融数据分析服务的初创公司向您咨询了其 AWS 架构。他们有一组 Amazon EC2 worker 实例，处理财务数据，然后输出客户使用的报告。您必须将生成的报告文件存储在持久存储中。随着这家初创公司在海外迅速扩张，需要存储的文件数量可能会随着时间的推移而增长，因此，他们还需要一种将报告更快地分发给全球客户的方法。

以下哪项是您应该用于此场景的经济高效且可扩展的存储选项？

- A、使用 Amazon S3 作为数据存储，使用 CloudFront 作为 CDN。
- B、使用 Amazon Redshift 作为数据存储，使用 CloudFront 作为 CDN。
- C、使用 Amazon Glacier 作为数据存储，使用 ElastiCache 作为 CDN。
- D、使用多个 EC2 实例存储进行数据存储，并使用 ElastiCache 作为 CDN。

答：

分析：

内容交付网络（CDN）几乎是任何现代 web 应用程序的关键组件。过去，CDN 只是通过在全球分布的一组缓存服务器上复制通常请求的文件（静态内容）来改进内容的交付。然而，随着时间的推移，CDN 变得更加有用。

对于缓存，CDN 将通过从附近的缓存边缘或存在点（PoP）交付内容的本地副本来减少应用程序源上的负载并改善请求者的体验。当 CDN 处理繁重的工作时，应用程序源可以打开连接并直接交付内容。最终结果是，应用程序源不需要扩展以满足静态内容的需求。

Amazon CloudFront 是一个快速内容交付网络（CDN）服务，它以低延迟、高传输速度安全地向全球客户交付数据、视频、应用程序和 API，所有这些都在一个开发人员友好的环境中。CloudFront 与 AWS 集成？这两个物理位置都直接连接到 AWS 全球基础设施以及其他 AWS 服务。Amazon S3 为备份和归档关键数据提供了一个高度持久、可扩展和安全的目的地。这是一个正确的选择，因为这家初创公司正在寻找一个持久的存储设备来存储音频和文本文件。此外，ElastiCache 仅用于缓存，而不是专门用作全球内容交付网络（CDN）。

使用 Amazon Redshift 作为数据存储，使用 CloudFront 作为 CDN 是不正确的，因为 Amazon Redshift 通常用作数据仓库。

使用 Amazon S3 Glacier 作为数据存储，使用 ElastiCache 作为 CDN 是不正确的，因为 Amazon S3 Glacier 通常用于数据存档。

将多个 EC2 实例存储用于数据存储和 ElastiCache 作为 CDN 是不正确的，因为存储在实例存储中的数据不持久。

参考文献: <https://aws.amazon.com/s3/>

<https://aws.amazon.com/caching/cdn/> 查

看此 Amazon S3 备忘单:

<https://tutorialsdojo.com/amazon-s3/>

Dojo 的 AWS 认证解决方案架构师助理考试学习指南教程: <https://tutorialsdojo.com/aws-certified-solutions-architect-associate/>

Q171. 一家公司推出了一个网站，接受高质量照片，并将其转化为可下载的视频蒙太奇。该网站提供了一个免费的高级帐户，保证更快的处理。免费和高级会员的所有请求都通过一个 SQS 队列，然后由一组生成视频的 EC2 实例处理。公司需要确保付费用户的优先权高于免费会员。

公司应如何重新设计其架构以满足这一需求？

- A、 使用 Amazon S3 存储和处理照片，然后生成视频蒙太奇。
- B、 为免费会员和高级会员创建一个 SQS 队列。将 EC2 实例配置为首先从高级队列中获取消息，如果它为空，则从自由成员的 SQS 队列中轮询。
- C、 对于高级会员提出的请求，请在 SQS 队列中设置更高的优先级，以便与自由会员提出的申请相比，优先处理。
- D、 使用亚马逊 Kinesis 实时处理照片并生成视频蒙太奇。

答案 B

分析:

Amazon 简单队列服务 (SQS) 是一种完全管理的消息队列服务，它使您能够分离和扩展微服务、分布式系统 and 无服务器应用程序。SQS 消除了与管理面向消息的中间件相关的复杂性和开销，并使开发人员能够专注于区分工作。使用 SQS，您可以在任何卷上的软件组件之间发送、存储和接收消息，而不会丢失消息或要求其他服务可用。

在这种情况下，最好为每种类型的成员创建两个单独的 SQS 队列。EC2 实例可以首先轮询高级成员的 SQS 队列，一旦完成，接下来就可以处理来自自由成员的消息。

因此，正确的答案是：为免费会员创建一个 SQS 队列，为高级会员创建另一个队列。将 EC2 实例配置为首先使用高级队列中的消息，如果它为空，则从自由成员的 SQS 队列中轮询。

“对于高级会员提出的请求，请在 SQS 队列中设置更高的优先级，以便与自由会员提出的申请相比，优先处理”选项不正确，因为您无法为 SQS 队列的单个项目设置优先级。

该选项表示：使用亚马逊 Kinesis 实时处理照片并生成视频蒙太奇是不正确的，因为亚马逊 Kinesis 用于处理流数据，不适用于该场景。

该选项表示：使用 Amazon S3 存储和处理照片，然后生成视频蒙太奇，这是不正确的，因为亚马逊 S3 用于持久存储，而不是处理数据。

参考：<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-best-practices.html>

查看此亚马逊 SQS 备忘单：<https://tutorialsdojo.com/amazon-sqs/>

Q172.一家公司在弹性负载均衡器后面开发了托管在 Amazon EC2 实例中的公共 API。这些 API 将由来自各自内部数据中心的不同客户使用。解决方案架构师收到一份报告，称 web 服务客户端只能访问其防火墙上的白名单上的可信 IP 地址。

您应该如何实现上述要求？

- A、将弹性 IP 地址与应用程序负载均衡器相关联。
- B、将弹性 IP 地址与网络负载均衡器相关联。
- C、在路由 53 中创建别名记录，该别名记录映射到负载均衡器的 DNS 名称。
- D、创建一个云前端分发，其源指向 web 服务器的私有 IP 地址。

答案 B

分析：

网络负载均衡器在开放系统互连（OSI）模型的第四层起作用。它每秒可以处理数百万个请求。负载均衡器收到连接请求后，从默认规则的目标组中选择一个目标。它尝试在侦听器配置中指定的端口上打开到选定目标的 TCP 连接。

基于给定场景，web 服务客户端只能访问受信任的 IP 地址。要解决此需求，您可以使用自带 IP（BYOIP）功能将可信 IP 用作网络负载均衡器（NLB）的弹性 IP 地址（EIP）。这样，就不需要使用新的 IP 地址重新建立白名单。

因此，正确的答案是：将弹性 IP 地址与网络负载均衡器相关联。表示：将弹性 IP 地址与应用程序负载均衡器关联的选项是不正确的，因为您无法为应用程序负载均衡器分配弹性 IP 地址。您可以做的另一种方法是在应用程序负载均衡器前面为网络负载均衡器分配一个弹性 IP 地址。“创建一个源指向 web 服务器私有 IP 地址的 CloudFront 分发”选项不正确，因为 web 服务客户端只能访问受信任的 IP 地址。解决此需求的最快方法是将弹性 IP 地址附加到

网络负载均衡器。表示：在路由 53 中创建一个别名记录，该记录映射到负载均衡器的 DNS 名称的选项不正确。由于防火墙上的可信 IP 地址，这种方法仍然不允许他们访问应用程序。

参考文献：

<https://aws.amazon.com/premiumsupport/knowledge-center/elb-attach-elastic-ip-to-public-nlb/>

<https://aws.amazon.com/blogs/networking-and-content-delivery/using-static-ip-addresses-for-application-负载均衡器/>

<https://docs.aws.amazon.com/elasticloadbalancing/latest/network/introduction.html> 查看此 AWS 弹性负载均衡备忘单：<https://tutorialsdojo.com/aws-elastic-load-balancing-elb/>

Q173. 会计应用程序使用配置有多 AZ 部署的 RDS 数据库来提高可用性。如果主数据库实例失败，RDS 会发生什么？

- A、在备用可用性区域中创建新的数据库实例。
- B、规范名称记录（CNAME）从主实例切换到备用实例。
- C、主数据库实例的 IP 地址被切换到备用数据库实例。
- D、主数据库实例将重新启动。

答案 B

分析：

在 Amazon RDS 中，故障转移是自动处理的，以便在主数据库实例发生故障时，您可以在没有管理干预的情况下尽快恢复数据库操作。在故障切换时，Amazon RDS 只需将数据库实例的规范名称记录（CNAME）翻转到备用状态，然后将其提升为新的主状态。表示：主数据库实例的 IP 地址切换到备用数据库实例的选项不正确，因为 IP 地址是每个子网的，子网不能跨越多个 AZ。表示：主数据库实例将重新启动的选项不正确，因为在发生故障时，没有可用于重新启动的数据库。

“在备用可用性区域中创建新数据库实例”选项不正确，因为启用了 multiAZ 后，您已经在另一个 AZ 中创建了备用数据库。

参考文献：[https://aws.amazon.com/rds/details/multi-](https://aws.amazon.com/rds/details/multi-az/)

[az/ https://aws.amazon.com/rds/faqs/](https://aws.amazon.com/rds/faqs/)

亚马逊 RDS 概述：<https://www.youtube.com/watch?v=aZmpLl8K1UU>

查看此 Amazon RDS 备忘单：<https://tutorialsdojo.com/amazon-relational-database-service-amazon-rds/>

问题 174：解决方案架构师正在为公司数据设计一种经济高效、高可用的存储解决方案。其中一个要求是确保在上传文件的修改版本时，文件的先前状态被保留并可检索。此外，为了满足法规遵从性，3 年以上的数据必须保存在存档中，并且每年只能访问一次。

解决方案架构师应该如何构建解决方案？

- A、创建一个启用了对象级版本控制的 S3 标准存储桶，并配置一个生命周期规则，在 3 年后将文件传输到 Amazon S3 Glacier Deep Archive。
- B、创建一个 S3 标准 bucket，并在治理模式下启用 S3 对象锁定。
- C、创建一个 S3 标准桶，启用 S3 对象锁定合规模式，然后配置一个生命周期规则，在 3 年后将文件传输到 Amazon S3 Glacier Deep Archive。

D、创建一个启用了对象级版本控制的单区域 IA 存储桶，并配置一个生命周期规则，在 3 年后将文件传输到 Amazon S3 冰川深度档案。

答:

分析:

AmazonS3 中的版本控制是将对象的多个变体保持在同一个 bucket 中的一种方法。您可以使用 S3 版本控制功能，用于保存、检索和恢复存储在存储桶中的每个对象的每个版本。通过版本控制，您可以更轻松地从意外的用户操作和应用程序故障中恢复。在为 bucket 启用版本控制后，如果 Amazon S3 同时接收到同一对象的多个写入请求，它将存储所有这些对象。因此，正确的答案是：创建一个启用了对象级版本控制的 S3 标准存储桶，并配置一个生命周期规则，在 3 年后将文件传输到 Amazon S3 Glacier Deep Archive。S3 对象锁定功能允许您使用一次写入多读（WORM）模型存储对象。在这种情况下，允许对对象进行更改，但应保留其以前的版本并保持可检索性。如果启用 S3 对象锁定功能，则无法上载对象的新版本。仅当您希望防止对象在固定时间内或无限期内被删除或覆盖时，此功能才有帮助。

因此，以下选项不正确：

- 创建一个 S3 标准 bucket，并在治理模式下启用 S3 对象锁定。
- 创建一个 S3 标准桶，启用 S3 对象锁定合规模式，然后配置一个生命周期规则，在 3 年后将文件传输到 Amazon S3 Glacier Deep Archive。该选项表示：创建一个启用了对象级别版本控制的单区域 IA 存储桶，并配置一个生命周期规则，在 3 年后将文件传输到 Amazon S3 Glacier Deep Archive，这是不正确的。单区域 IA 不是高度可用的，因为它只依赖一个可用区域来存储数据。

参考文献:

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/Versioning.html>

<https://aws.amazon.com/blogs/aws/newamazon-s3-storage-class-glacier-deep-archive/>查看此 Amazon S3 备忘单:

<https://tutorialsdojo.com/amazon-s3/>

Q175.一家公司计划推出一个应用程序，该应用程序需要一个数据仓库，用于其不经常访问的数据。您需要使用一个 EBS 卷来处理大型、连续的 I/O 操作。

以下哪种存储类型最经济高效，您应该使用它来满足要求？

- A、冷硬盘（sc1）
- B、吞吐量优化 HDD（st1）
- C、配置 IOPS SSD（io1）
- D、EBS 通用 SSD（gp2）

答:

分析:

冷硬盘卷提供了低成本的磁存储，以吞吐量而不是 IOPS 来定义性能。与吞吐量优化 HDD 相比，吞吐量限制较低，这是大型连续 colddata 工作负载的理想选择。如果您需要不频繁地访问数据，并希望节省成本，冷硬盘可提供廉价的块存储。请注意，不支持可引导的冷硬盘卷。

com

Cold HDD 提供了成本最低的 HDD 卷，专为访问频率较低的工作负载而设计。

因此，冷硬盘（sc1）是正确答案。

在检查中，始终考虑 SSD 和 HDD 之间的差异，如下表所示。这将允许您轻松消除选项中非 SSD 或非 HDD 的特定 EBS 类型，具体取决于问题要求的存储类型是具有小的随机 I/O 操作还是大的顺序 I/O。

EBS 通用 SSD（gp2）是不正确的，因为通用 SSD 卷成本更高，并且主要用于各种工作负载。建议将其用作系统启动卷、虚拟桌面、低延迟交互式应用程序等。

配置的 IOPS SSD（io1）是不正确的，因为这比冷硬盘的成本更高，因此，在这种情况下不具有成本效益。它为任务关键型低延迟或高吞吐量工作负载提供了最高性能的 SSD 卷，这在场景中是不需要的。吞吐量优化 HDD（st1）不正确，因为它主要用于频繁访问、吞吐量密集型工作负载。在这种情况下，与吞吐量优化的 HDD 不同，冷硬盘完全符合这一要求，因为它用于不经常访问的数据，并提供最低成本。参考文献：

<https://aws.amazon.com/ebs/details/>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html>

查看此亚马逊 EBS 备忘单：<https://tutorialsdojo.com/amazon-ebs/>

Q176.公司每天都从不同来源接收半结构化和结构化数据。解决方案架构师计划使用大数据处理框架来分析大量数据，并使用各种商业智能工具和标准 SQL 查询访问数据。以下哪项提供了满足此要求的最高效的解决方案？

- A、使用 Amazon Kinesis 数据分析并将处理后的数据存储在 Amazon DynamoDB 中。
- B、使用 AWS 胶水并将处理后的数据存储在 Amazon S3 中。
- C、创建一个 Amazon EC2 实例，并将处理后的数据存储在 Amazon EBS 中。
- D、创建一个 Amazon EMR 集群，并将处理后的数据存储在 Amazon Redshift 中。

答案 D

分析：

Amazon EMR 是一个托管集群平台，它简化了在 AWS 上运行大数据框架，如 Apache Hadoop 和 Apache Spark，以处理和分析大量数据。通过使用这些框架和相关的开源项目，如 ApacheHive 和 ApachePig，您可以为分析目的和商业智能工作负载处理数据。此外，您还可以使用 Amazon EMR 将大量数据转换和移出其他 AWS 数据存储和数据库。亚马逊红移是应用最广泛的云数据仓库。它使用标准 SQL 和现有的商业智能（BI）工具快速、简单和经济高效地分析所有数据。它允许您对 TB 到 PB 的结构化和半结构化数据运行复杂的分析查询，使用复杂的查询优化、高性能存储上的列存储以及大规模并行查询执行。

场景中的关键短语是“大数据处理框架”和“各种商业智能工具和标准 SQL 查询”来分析数据。要利用大数据处理框架，您需要

使用亚马逊 EMR。集群将执行数据转换（ETL），并将处理后的数据加载到 Amazon Redshift 中，用于分析和商业智能应用程序。因此，正确的答案是：创建一个 Amazon EMR 集群，并将处理后的数据存储在 Amazon Redshift 中。“使用 AWS Glue 并将处理后的数据存储在 Amazon S3 中”的选项是不正确的，因为 AWS Glue 只是一个无服务器 ETL 服务，它可以爬行您的数据、构建数据目录、执行数据准备、数据转换和数据接收。与 Amazon EMR 不同，它不允许您有效地利用不同的大数据框架。此外，Amazon S3 中的 S3 选择功能只能对来自特定 S3 对象的数据子集运行简单的 SQL 查询。要在 S3 bucket 中执行查询，需要使用 Amazon Athena。

使用 Amazon Kinesis 数据分析并将处理后的数据存储在 Amazon DynamoDB 中的选项是不正确的，因为与 Amazon Redshift 不同，Amazon DynamoDB 不完全支持使用标准 SQL 和商业智能（BI）工具。它还不允许您对 TB 到 PB 的结构化和半结构化数据运行复杂的分析查询。“创建一个 Amazon EC2 实例并将处理后的数据存储在 Amazon EBS 中”的选项是不正确的，因为单个 EBS 支持的 EC2 实例的计算能力非常有限。此外，它还需要管理开销，因为您必须自己手动安装和维护 EC2 实例的大数据框架。利用大数据框架的最合适的解决方案是使用 EMR 集群。

参考文献：

<https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-what-is-emr.html> 和
<https://docs.aws.amazon.com/redshift/latest/dg/loading-from-emr-data.html>

查看此亚马逊电子病历备忘单：<https://tutorialsdjo.com/amazon-emr/>

Q177. 一家公司有一个用 MEAN stack 编写的动态 web 应用程序，将在下个月推出。在前几周，访问量可能会非常高。在加载失败的情况下，如何设置 DNS 故障转移到静态网站？

- A、添加更多服务器以防应用程序失败。
- B、在另一个区域复制精确的应用程序架构，并配置基于 DNS 权重的路由。
- C、启用故障转移到本地数据中心中托管的应用程序。
- D、将路由 53 与故障转移选项一起使用到静态 S3 网站 bucket 或 CloudFront 分发。

答案 D

分析：

对于这个场景，使用带有故障转移选项的路由 53 到静态 S3 网站 bucket 或 CloudFront 分发是正确的。您可以创建一个新的路由 53，并将故障转移选项作为静态 S3 网站 bucket 或 CloudFront 分发的替代方案。

在另一个区域复制精确的应用程序架构并配置基于 DNS 权重的路由是不正确的，因为运行复制系统不是一个经济高效的解决方案。请记住，您正在尝试为 web 应用程序构建故障转移机制，而不是分布式设置。对本地数据中心中托管的应用程序启用故障转移是不正确的。尽管您可以将故障切换设置为本地数据中心，但您并没有最大化 AWS 环境，例如使用路由 53 故障切换。

在应用程序失败时添加更多服务器是不正确的，因为这不是处理故障转移事件的最佳方式。如果仅在应用程序失败的情况下添加更多服务器，则会有一段停机时间，使应用程序不可用。由于在此期间没有正在运行的服务器，因此在新服务器启动并运行之前，应用程序将在一段时间内不可用。

参考：

<https://aws.amazon.com/premiumsupport/knowledge-center/fail-over-s3-r53/>

<http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover.html> 查看此亚马逊路线 53 备忘单:

<https://tutorialsdojo.com/amazon-route-53/>

Q178.一家公司正在亚马逊 EC2 实例的自动缩放组中运行自定义应用程序。由于交换空间不足，几个实例失败。已指示解决方案架构师解决该问题，并有效监控每个 EC2 实例的可用交换空间。

以下哪个选项符合此要求？

- A、 在每个实例上安装 CloudWatch 代理，并监视 SwapUtilization 度量。
- B、 在 AWS CloudTrail 中创建新的跟踪，并配置 Amazon CloudWatch 日志以监控跟踪日志。
- C、 创建 CloudWatch 仪表板并监视交换的度量。
- D、 启用对每个实例的详细监视，并监视 SwapUtilization 度量。

答:

分析:

Amazon CloudWatch 是 AWS 云资源和您在 AWS 上运行的应用程序的监控服务。您可以使用 Amazon CloudWatch 收集和跟踪指标，收集和监控日志文件，并设置警报。Amazon CloudWatch 可以监控 AWS 资源，如 Amazon EC2 实例、Amazon DynamoDB 表和 Amazon RDS DB 实例，以及应用程序和服务生成的自定义指标，以及应用生成的任何日志文件。您可以使用 AmazonCloudWatch 获得资源利用率、应用程序性能和运行状况的全系统可见性。该场景中的主要需求是监视 SwapUtilization 度量。请注意，您不能使用 CloudWatch 的默认度量来监视 SwapUtilization 度量。要监视自定义度量，必须在 EC2 实例上安装 CloudWatch 代理。安装 CloudWatch 代理后，现在可以收集 EC2 实例的系统度量和日志文件。因此，正确的答案是：在每个实例上安装 CloudWatch 代理，并监视 SwapUtilization 度量。“在每个实例上启用详细监视并监视 SwapUtilization 度量”选项是不正确的，因为您无法仅通过启用详细监视选项来监视 SwapUtilization 度量。您必须在实例上安装 CloudWatch 代理。“创建 CloudWatch 仪表板并监视交换指标”选项不正确，因为必须先安装 CloudWatch 代理才能在仪表板中添加自定义指标。“在 AWS CloudTrail 中创建新的跟踪并配置 Amazon CloudWatch 日志以监控跟踪日志”选项不正确，因为 CloudTrail 无法帮助您监控自定义指标。CloudTrail 专门用于监控 AWS 帐户中的 API 活动。参考文献:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/mon-scripts.html> <https://aws.amazon.com/cloudwatch/常见问题/查看此 Amazon cloudwatch 备忘单:>

<https://tutorialsdojo.com/amazon-cloudwatch/>

Amazon CloudWatch 概览: <https://www.youtube.com/watch?v=q0DmxfyGkeU>

Q179.一家初创公司有一个托管 web 应用程序的 EC2 实例。未来几个月，用户数量预计将增长，因此，您需要在 AWS 架构中增加更多的弹性和可伸缩性，以满足需求。

以下哪个选项可以满足给定场景的上述要求？（选择两个。）

- A、 在 EC2 实例后面设置 AWS WAF。

- B、在 EC2 实例前面设置 S3 缓存。
- C、设置两个使用启动模板部署并与 AWS Glue 集成的 EC2 实例。
- D、设置两个 EC2 实例，并使用路由 53 基于加权路由策略路由流量。
- E、设置两个 EC2 实例，然后将它们放在弹性负载均衡器（ELB）后面。

答：德

分析：

使用弹性负载均衡器是为应用程序增加弹性的理想解决方案。或者，您也可以路由 53 中创建策略，例如加权路由策略，以将流量均匀分布到 2 个或更多 EC2 实例。因此，建立两个 EC2 实例，然后将它们置于弹性负载均衡器（ELB）后面，并建立两个 EC2 实例，并使用路由 53 基于加权路由策略路由流量是正确答案。

在 EC2 实例前面设置 S3 缓存是不正确的，因为这样做不会为 EC2 实例提供弹性和可伸缩性。

在 EC2 实例后面设置 AWS WAF 是不正确的，因为 AWS WAF 是一个 web 应用程序防火墙，可帮助保护您的 web 应用程序免受常见 web 攻击。此服务更多地是为应用程序提供安全性。

设置使用启动模板部署并与 AWS Glue 集成的两个 EC2 实例是不正确的，因为 AWS Glue 是一种完全受管理的提取、转换和加载（ETL）服务，使客户可以轻松准备和加载数据进行分析。它不为实例提供可伸缩性或弹性。

参考文献：

<https://aws.amazon.com/elasticloadbalancing>

<http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/Welcome.html> 查看 AWS 弹性负载均衡（ELB）备忘单：

<https://tutorialsdojo.com/aws-elastic-load-balancing-elb/>

查看此亚马逊路线 53 备忘单：

<https://tutorialsdojo.com/amazon-route-53/>

Q180. 一家公司最近采用了一种混合架构，将其内部数据中心集成到 AWS 云。分配给您的任务是配置专有网络并实施所需的 IAM 用户、IAM 角色、IAM 组和 IAM 策略。

在这种情况下，创建 IAM 策略的最佳实践是什么？

- A、确定用户需要做什么，然后为他们制定策略，让用户执行这些任务，包括其他管理操作。
- B、将所有权限授予任何 EC2 用户。
- C、使用最小特权原则，这意味着只授予执行任务所需的权限。
- D、使用最小特权原则，这意味着只授予最少数量的人完全根访问权限。

答案 C

分析：

AWS IAM 中的最佳实践之一是授予最小特权。创建 IAM 策略时，请遵循授予最低权限的标准安全建议，即只授予执行任务所需的权限。确定用户需要做什么，然后为他们制定策略，让用户只执行这些任务。因此，使用最小特权原则（即仅授予执行任务所需的权限）是正确答案。

从最小权限集开始，并根据需要授予其他权限。定义正确的权限集需要了解用户的目标。确定特定任务需要什么，特定服务支持什么操作，以及执行这些操作需要什么权限。

将所有权限授予任何 EC2 用户是不正确的，因为您不希望用户访问所有内容并执行不必要的操作。这样做不是好的安全做法。使用最小特权原则意味着只授予最少数量的人完全根访问权限是不正确的，因为这不是最小特权原则的正确定义。确定用户需要做什么，然后为他们制定允许用户执行这些任务（包括其他管理操作）的策略是不正确的，因为有些用户不应授予管理访问权限。在提供对资源的权限和访问权限时，应遵循最低特权原则。

参考：

<https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#use-权限组> 查看此 AWS IAM 备忘单：

<https://tutorialsdojo.com/aws-identity-and-access-management-iam/> 服务控制策略（SCP）与 IAM 策略：

<https://tutorialsdojo.com/service-control-policies-scp-vs-iam-policies/> AWS 服务备忘单比较：

<https://tutorialsdojo.com/comparison-of-aws-services/>

Q181. 一家公司现有的 VPC 在过去几个月内相当闲置。业务经理指示解决方案架构师集成公司的内部数据中心及其 VPC。架构师解释了他将要执行的任务列表，并讨论了虚拟专用网络（VPN）连接。业务经理并不精通技术，但他有兴趣了解 VPN 是什么及其好处。

在 AWS 中使用 VPN 的主要优势是什么？

- A、 它使您能够在网络 and 专有网络之间建立专用网络连接
- B、 它提供了从 VPC 到内部数据中心的经济高效的混合连接，绕过公共互联网。
- C、 它允许您使用具有 IP 安全（IPSec）或传输层安全（TLS）隧道的安全和专用会话将 AWS 云资源连接到本地数据中心。
- D、 它提供了两个 VPC 之间的网络连接，使您能够使用专用 IPv4 地址或 IPv6 地址在它们之间路由流量。

答案 C

分析：

亚马逊专有网络为您提供了灵活性，通过在远程网络和亚马逊专有网络中运行的软件 VPN 设备之间创建 VPN 连接，全面管理亚马逊专有网络连接的双方。如果您必须管理 VPN 连接的两端，或者出于法规遵从性目的，或者为了利用目前不受 Amazon VPC VPN 解决方案支持的网关设备，建议使用此选项。

您可以使用以下 VPN 连接选项将 Amazon VPC 连接到远程网络 and 用户：

AWS 站点到站点 VPN-在 VPC 和远程网络之间创建 IPsec VPN 连接。在站点到站点 VPN 连接的 AWS 端，虚拟专用网关或传输网关提供了两个 VPN 端点（隧道），用于自动故障切换。

AWS 客户端 VPN-一种基于托管客户端的 VPN 服务，可在 AWS 资源和本地网络之间提供安全的 TLS VPN 连接。

AWS VPN CloudHub-能够在虚拟专用网关上连接多个 AWS 站点到站点 VPN 连接。如果您希望启用使用站点到站点 VPN 连接的不同远程网络之间的通信，这将非常有用。

第三方软件 VPN 设备-您可以通过在运行第三方 VPN 设备的 VPC 中使用 Amazon EC2 实例创建到远程网络的 VPN 连接。通过 VPN 连接，您可以连接到云中的 Amazon VPC，与连接到分支机构的方式相同，同时使用 IP 安全（IPSec）或传输层安全（TLS）隧道建立安全和专用会话。

因此，正确的答案是这样的选项：它允许您使用 IP 安全（IPSec）或传输层安全（TLS）隧道的安全和专用会话将 AWS 云资源连接到内部数据中心，因为 VPN 连接的主要优点之一是您将能够安全地将 Amazon VPC 连接到其他远程网络。这样的选择是不正确的：它提供了从 VPC 到内部数据中心的低成本、混合连接，绕过公共互联网。尽管 VPN 确实提供了从 VPC 到内部数据中心的经济高效的混合连接，但它肯定不会绕过公共互联网。VPN 连接实际上通过公共互联网，与 AWS Direct Connect 连接不同，后者直接和专用连接到您的内部网络。该选项表示：它提供两个 VPC 之间的网络连接，使您能够使用专用 IPv4 地址或 IPv6 地址在它们之间路由流量，这是不正确的，因为这实际上描述了 VPC 对等，而不是 VPN 连接。

“它使您能够在网络和 VPC 之间建立专用网络连接”选项是不正确的，因为这是 AWS 直接连接而不是 VPN 的优势。

参考文献：

<http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpn-connections.html>

<https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/software-vpn-network-to-amazon.html>

亚马逊专有网络概述：<https://www.youtube.com/watch?v=oIDHKeNxvQQ>

查看此亚马逊 VPC 备忘单：

<https://tutorialsdojo.com/amazon-vpc/>

Dojo 的 AWS 认证解决方案架构师助理考试学习指南教程：<https://tutorialsdojo.com/aws-certified-solutions-architect-associate/>

一位解决方案架构师正在一家大型保险公司工作。为了遵守 HIPAA 法律，Amazon S3 上备份或存储的所有数据都需要在静止时进行加密。在这种情况下，假设 S3 用于存储金融相关数据，数据的最佳加密方法是什么？

（选择
二）

- A、将数据存储在加密的 EBS 快照中
- B、使用您自己的加密密钥加密数据，然后通过 HTTPS 端点将数据复制到 Amazon S3。
- C、在 S3 存储桶上启用 SSE 以使用 AES-256 加密
- D、将数据存储在启用加密的 EBS 卷上，而不是使用 Amazon S3E。使用 AWS Shield 保护您的静态数据

答案：BC

分析：

数据保护指的是在传输过程中（当数据往返于 Amazon S3 时）和静止时（当数据存储在 Amazon S3 数据中心的磁盘上时）保护数据。您可以使用 SSL 或客户端加密来保护传输中的数据。您可以使用以下选项来保护 Amazon S3 中的静态数据。是否使用服务器端加密？您请求 Amazon S3 在将对象保存到其数据中心的磁盘上之前对其进行加密，并在下载对象时对其进行解密。使用客户端加密？您可以在客户端加密数据，并将加密数据上传到 Amazon S3。

在这种情况下，您可以管理加密过程、加密密钥和相关工具。

因此，以下选项是正确答案：

- 在 S3 存储桶上启用 SSE 以使用 AES-256 加密
- 使用您自己的加密密钥加密数据，然后通过 HTTPS 端点将数据复制到 Amazon S3。这是指使用客户提供的密钥（SSE-C）进行服务器端加密。在加密 EBS 快照中存储数据和在启用加密的 EBS 卷上存储数据而不是使用 Amazon S3 都是不正确的，因为所有这些选项都是为了保护 EBS 卷中的数据。请注意，S3 存储桶不使用 EBS 卷来存储数据。使用 AWS Shield 保护静止数据是不正确的，因为 AWS Shield 主要用于保护整个 VPC 免受 DDoS 攻击。

参考文献：

[https://docs.aws.amazon.com/AmazonS3/latest/dev/serv-side-](https://docs.aws.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html)

[encryption.htmlhttps://docs.aws.amazon.com/AmazonS3/latest/dev/UsingClientSideEncryption.html](https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingClientSideEncryption.html) 查看此 Amazon

S3 备忘单：<https://tutorialsdojo.com/amazon-s3/>

Q183.一位为初创公司工作的解决方案架构师正在设计一个高性能计算（HPC）应用程序，该应用程序可供客户公开访问。初创公司创始人希望减轻对其应用程序的分布式拒绝服务（DDoS）攻击。

以下哪些选项不适合在这种情况下实施？（选择两个。）

- A、使用专用的 EC2 实例，以确保每个实例具有尽可能高的性能。
- B、向每个 EC2 实例添加多个弹性结构适配器（EFA），以增加网络带宽。
- C、为您的 EC2 实例使用具有自动伸缩组的应用程序负载平衡器。

通过将 Amazon RDS 数据库部署到新的专用子网，防止将其直接连接到 Internet 流量。D、使用 AWS 屏蔽和 AWS WAF。

- E、使用 Amazon CloudFront 服务分发静态和动态内容。

回答 AB

分析：

请注意，该问题询问了不适用于防止分布式拒绝服务（DDoS）攻击的可行缓解技术。

拒绝服务（DoS）攻击是一种可使最终用户无法访问您的网站或应用程序的攻击。为此，攻击者使用各种技术消耗网络或其他资源，中断合法终端用户的访问。

要保护您的系统免受 DDoS 攻击，您可以执行以下操作：

- 使用 Amazon CloudFront 服务分发静态和动态内容。
- 为您的 EC2 实例使用具有自动扩展组的应用程序负载平衡器，然后通过部署到专用子网来限制到 Amazon RDS 数据库的直接互联网流量。
- 在 Amazon CloudWatch 中设置警报，以查找高网络输入和 CPU 利用率指标。AWS 区域内可用的服务，如弹性负载平衡和 Amazon 弹性计算云（EC2），允许您构建分布式拒绝服务弹性并扩展以处理给定区域内的意外流量。

AWS 边缘位置提供的服务，如 Amazon CloudFront、AWS WAF、Amazon Route53 和 Amazon API Gateway，允许您利用边缘位置的全球网络，为您的应用程序提供更大的容错能力和更大的流量管理规模。

此外，您还可以使用 AWS Shield 和 AWS WAF 来加强您的云网络。AWS Shield 是一种托管 DDoS 保护服务，分为两层：标准层和高级层。AWS Shield 标准应用始终在线检测和内联缓解技术，如确定性数据包过滤和基于优先级的流量整形，以最小化应用程序停机时间和延迟。AWS WAF 是一个 web 应用程序防火墙，可帮助保护 web 应用程序免受可能影响应用程序可用性、危害安全性或消耗过多资源的常见 web 攻击。您可以使用 AWS WAF 定义可定制的 web 安全规则，以控制访问 web 应用程序的流量。如果您使用 AWS Shield Advanced，您可以使用 AWS WAF，而无需为这些受保护的资源支付额外费用，并可以与 DRT 合作创建 WAF 规则。

使用专用 EC2 实例来确保每个实例具有尽可能高的性能不是可行的缓解技术，因为专用 EC2 实例只是实例计费选项。虽然它可以确保每个实例提供最大性能，但这本身不足以缓解 DDoS 攻击。

向每个 EC2 实例添加多个弹性结构适配器（EFA）以增加网络带宽也是不可行的选择，因为这样做主要是为了提高性能，而不是为了减少 DDoS 攻击。此外，每个 EC2 实例只能附加一个 EFA。弹性结构适配器（EFA）是一种网络设备，可以连接到 Amazon EC2 实例，以加速高性能计算（HPC）和机器学习应用程序。以下选项是可用于防止 DDoS 的有效缓解技术：

- 使用 Amazon CloudFront 服务分发静态和动态内容。
- 为您的 EC2 实例使用具有自动伸缩组的应用程序负载平衡器。通过将 Amazon RDS 数据库部署到新的专用子网，防止将其直接连接到 Internet 流量。
- 使用 AWS 屏蔽和 AWS WAF。

参考文献：

<https://aws.amazon.com/answers/networking/aws-ddos-attack-mitigation/>

https://d0.awsstatic.com/whitepapers/DDoS_White_Paper_June2015.pdf DDoS 攻击缓解的最佳实践：

<https://youtu.be/HnoZS5jj7pk/>

Q184.应用程序需要使用简单的 SQL 表达式从存储在 Amazon S3 存储桶中的大型 CSV 文件中检索数据子集。查询是在 Amazon S3 中进行的，必须只返回所需的数据。

应采取以下哪些行动？

A、 基于 bucket 的名称和对象的元数据执行 S3 选择操作。

- B、基于 bucket 的名称和对象标记执行 S3 选择操作。
- C、根据桶的名称执行 S3 选择操作。
- D、根据 bucket 的名称和对象的键执行 S3 选择操作。

答案 D

分析：

S3 Select 使应用程序能够使用简单的 SQL 表达式从对象中检索数据的子集。通过使用 S3 Select 仅检索应用程序所需的数据，可以实现性能的大幅提高。Amazon S3 由 bucket、对象键、对象元数据、对象标记和许多其他组件组成，如下所示：

Amazon S3 bucket 名称是全局唯一的，名称空间由所有 AWS 帐户共享。AmazonS3 对象密钥指的是密钥名称，它唯一标识 bucket 中的对象。AmazonS3 对象元数据是提供对象信息的名称-值对。Amazon S3 对象标记是用于对象标记以分类存储的密钥对值。您可以执行 S3 Select，根据 bucket 的名称和对象的键，只查询 CSV 文件中的必要数据。下面的代码片段显示了如何使用 boto3（AWS SDK for Python）完成此操作：

```
client=boto3.client ('s3')

resp=client.select_object_content(

Bucket='tdojo-Bucket', #Bucket 名称。

Key='s3-select/tutorialsdojofile.csv', #对象键。

ExpressionType='SQL',
```

Expression="从 s3object s 中选择“Sample”，其中 s.\“tutorialsdojofile\”在['A', 'B']中。因此，正确答案是这样的选项：根据桶的名称和对象的键执行 S3 选择操作。

“根据存储桶名称和对象元数据执行 S3 选择操作”选项不正确，因为使用 S3 选择查询对象中的数据子集时不需要元数据。表示：基于 bucket 的名称和对象标记执行 S3 选择操作的选项是不正确的，因为对象标记只是为对象提供附加信息。当使用 S3 Select 进行查询时，这是不需要的，尽管这对于 S3 批处理操作很有用。您可以根据标记值对对象进行分类，以向 S3 批处理操作提供要操作的对象列表。表示：基于存储桶名称执行 S3 选择操作的选项不正确，因为您需要存储桶名称和对象密钥才能成功执行 S3 选择操作。

参考文献：

<https://docs.aws.amazon.com/AmazonS3/latest/dev/s3-glacier-select-sql-reference-select.html><https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingObjects.html> 查看此 Amazon S3 备忘单：
<https://tutorialsdojo.com/amazon-s3/>

Q185.初创企业在 AWS 云上部署了资源。目前，该公司正在接受一家外部审计公司的一系列定期审计，以确保合规性。

AWS 中可用的以下哪些服务可用于帮助确保为审计目的提供正确的信息？

- A、 亚马逊云观察
- B、 亚马逊 EC2
- C、 亚马逊云迹
- D、 亚马逊专有网络

答案 C

分析：

AWS CloudTrail 是一项支持 AWS 帐户的治理、合规、运营审计和风险审计的服务。使用 CloudTrail，您可以在 AWS 基础设施中记录、持续监控和保留与操作相关的帐户活动。CloudTrail 提供 AWS 帐户活动的事件历史记录，包括通过 AWS 管理控制台、AWS SDK、命令行工具和其他 AWS 服务采取的操作。此事件历史简化了安全分析、资源更改跟踪和故障排除。

CloudTrail 通过记录对您的帐户采取的操作，提供对用户活动的可见性。CloudTrail 记录关于每个动作的重要信息，包括谁发出请求、使用的服务、执行的动作、动作参数以及 AWS 服务返回的响应元素。此信息可帮助您跟踪对 AWS 资源所做的更改，并解决操作问题。CloudTrail 使确保遵守内部政策和监管标准变得更加容易。

因此，正确答案是：AWS CloudTrail。

Amazon VPC 是不正确的，因为 VPC 是 AWS 云的逻辑隔离部分，您可以在定义的虚拟网络中启动 AWS 资源。它不提供本场景中要求的审核信息。

AmazonEC2 是不正确的，因为 EC2 是一种在云中提供安全、可调整大小的计算能力的服务，并且在这种情况下不提供所需的信息，就像上面的选项一样。Amazon CloudWatch 是不正确的，因为它是 AWS 资源的监控工具。与上述选项一样，它不提供满足场景中需求所需的信息。

Q186.作为监管要求的一部分，大型电信公司需要对来自应用程序负载均衡器的所有组合日志文件进行分析。哪些 AWS 服务可以一起用于收集日志，然后轻松执行日志分析？

- A、 Amazon S3 用于存储 ELB 日志文件，EC2 实例用于使用自定义内置应用程序分析日志文件。
- B、 Amazon S3 用于存储 ELB 日志文件，Amazon EMR 用于分析日志文件。
- C、 Amazon DynamoDB 用于存储日志，EC2 用于分析日志。
- D、 Amazon EC2 带有 EBS 卷，用于存储和分析日志文件。

答案 B

分析:

在这种情况下，最好结合使用 Amazon S3 和 Amazon EMR：Amazon S3s 用于存储 ELB 日志文件，Amazon EMR 用于分析日志文件。ELB 中的访问日志存储在 Amazon S3 中，这意味着以下是有效选项：

- AmazonS3 用于存储 ELB 日志文件，EC2 实例用于使用定制的应用程序分析日志文件。
- Amazon S3 用于存储 ELB 日志文件，Amazon EMR 用于分析日志文件。然而，Amazon EMR 可以自动提供日志分析，这比构建定制的日志分析应用程序并将其托管在 EC2 中更经济。因此，选择：Amazon S3 用于存储 ELB 日志文件，Amazon EMR 用于分析日志文件是两者之间的最佳答案。访问日志记录是默认禁用的弹性负载均衡的可选功能。为负载均衡器启用访问日志记录后，弹性负载均衡将捕获日志并将其存储在指定为压缩文件的 Amazon S3 存储桶中。您可以随时禁用访问日志记录。Amazon EMR 提供了一个受管理的 Hadoop 框架，使得跨动态可扩展的 Amazon EC2 实例处理大量数据变得简单、快速且经济高效。它安全可靠地处理广泛的大数据用例，包括日志分析、web 索引、数据转换（ETL）、机器学习、金融分析、科学模拟和生物信息学。您还可以在 Amazon EMR 中运行其他流行的分布式框架，如 Apache Spark、HBase、Presto 和 Flink，并与其他 AWS 数据存储（如 Amazon S3 和 Amazon DynamoDB）中的数据交互。“Amazon DynamoDB 用于存储日志，EC2 用于分析日志”选项不正确，因为 DynamoDB 是 AWS 的 noSQL 数据库解决方案。在使用 EC2 分析日志时，将日志存储在 DynamoDB 中是低效的。

该选项表示：Amazon EC2 使用 EBS 卷存储和分析日志文件是不正确的，因为将 EC2 与 EBS 一起使用成本很高，而且与 S3 不同，EBS 可能无法为日志提供最持久的存储。

该选项表示：Amazon S3 用于存储 ELB 日志文件，EC2 实例用于使用定制的应用程序分析日志文件，这是不正确的，因为使用 EC2 分析日志效率低且成本高，因为您必须自己对分析器进行编程。参考文献：

<https://aws.amazon.com/emr/>

<https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-access-logs.html> 查看此亚马逊电子病历备忘单：

<https://tutorialsdojo.com/amazon-emr/>

查看 AWS 弹性负载均衡（ELB）备忘单：<https://tutorialsdojo.com/aws-elastic-load-balancing-elb/>

Q187. 一家公司部署了一个高性能计算（HPC）集群，该集群跨越多个可用性区域的多个 EC2 实例，并处理各种风模拟模型。目前，解决方案架构师的应用程序正在减速，经过进一步调查，发现这是由于延迟问题。

解决方案架构师应该实施哪种解决方案，以提供 HPC 集群的紧密耦合节点到节点通信所需的低延迟网络性能？

- A、跨多个可用区域设置 AWS 直连接，以提高带宽吞吐量和更一致的网络体验。
- B、在多个 AWS 区域的多个可用性区域中设置一个分散放置组。
- C、在同一 AWS 区域的单个可用性区域内设置集群放置组。
- D、使用 EC2 专用实例。

答案 C

分析:

当您启动一个新的 EC2 实例时，EC2 服务会尝试以这样一种方式放置该实例，即所有实例都分布在底层硬件上，以最小化相关故障。您可以使用放置组来影响一组相互依赖实例的放置，以满足工作负载的需要。根据工作负载的类型，可以使用以下放置策略之一创建放置组：

簇在可用性区域内将实例打包在一起。该策略使工作负载能够实现 HPC 应用中典型的紧密耦合节点到节点通信所需的低延迟网络性能。

隔断将实例分布在逻辑分区上，以便一个分区中的实例组不会与不同分区中的多个实例组共享底层硬件。这种策略通常用于大型分布式和复制工作负载，如 Hadoop、Cassandra 和 Kafka。传播严格地跨不同的底层硬件放置一组实例，以减少相关故障。建议将群集放置组用于受益于低网络延迟、高网络吞吐量或两者的应用程序。当大多数网络流量在组中的实例之间时，也建议使用它们。要为放置组提供最低延迟和最高每秒数据包网络性能，请选择支持增强网络的实例类型。

分区放置组可用于部署大型分布式和复制工作负载，

HBase 和 Cassandra，跨越不同的机架。当您将实例启动到分区放置组中时，AmazonEC2 会尝试在指定的分区数量上均匀分布实例。您还可以将实例启动到特定分区中，以便对实例的放置位置进行更多控制。

对于具有少量关键实例的应用程序，建议将分散放置组彼此分开。在排列放置组中启动实例可减少

实例共享同一机架时可能发生同时故障的风险。分散放置组提供对不同机架的访问，因此适合混合实例类型或随时间启动实例。扩展放置组可以跨越同一区域中的多个可用性区域。每个可用性区域每个组最多可以有七个运行实例。

因此，正确的答案是：在同一 AWS 区域的单个可用性区域内设置集群放置组。

“在多个 AWS 区域的多个可用性区域中设置分散放置组”选项是不正确的，因为尽管使用放置组对于该特定场景有效，但只能在单个 AWS 区域中设置放置组。扩展放置组可以跨越同一区域中的多个可用性区域。

“跨多个可用性区域建立 AWS 直接连接以提高带宽吞吐量和更一致的网络体验”选项是不正确的，因为这主要用于混合架构。它绕过公共互联网，建立从本地数据中心到 AWS 的安全专用连接，不用于 AWS 网络中的低延迟。

“使用 EC2 专用实例”选项不正确，因为这些是在中运行的 EC2 实例

专用于单个客户的硬件上的专有网络，在主机硬件级别与属于其他 AWS 帐户的实例物理隔离。它不用于减少延迟。参考文献：

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html> <https://aws.amazon.com/hpc/>查看

此 Amazon EC2 备忘单：<https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/Q188>。一家投资

银行正在与 IT 团队合作，以处理新数字钱包系统的发布。

应用程序将在多个 EBS 支持的 EC2 实例上运行，这些实例将用户的日志、事务和账单存储在 S3 存储桶中。由于严格的安全和法规遵从性要求，IT 团队正在探索如何在 EBS 卷和 S3 上安全存储敏感数据的选项。在 AWS 上存储敏感数据时，应执行以下哪个选项？（选择两个。）

A、创建 EBS 快照

- B、启用 Amazon S3 服务器端或使用客户端加密
- C、启用 EBS 加密
- D、将 EC2 实例从公用子网迁移到专用子网。
- E、使用 AWS 屏蔽和 WAF

答案：BC

分析：

启用 EBS 加密和启用 Amazon S3 服务器端或使用客户端加密是正确的。Amazon EBS 加密为您的 EBS 卷提供了一个简单的加密解决方案，无需构建、维护和保护您自己的密钥管理基础设施。在 Amazon S3 中，数据保护是指在传输过程中（当数据往返于 Amazon S3s 时）和静止时（当数据存储在 Amazon S3 数据中心的磁盘上时）保护数据。您可以使用 SSL 或客户端加密来保护传输中的数据。您可以使用以下选项来保护 Amazon S3 中的静态数据。

使用服务器端加密？您请求 Amazon S3 在将对象保存到其数据中心的磁盘上之前对其进行加密，并在下载对象时对其进行解密。使用客户端加密？您可以在客户端加密数据并将加密数据上传到 Amazon S3。在这种情况下，您可以管理加密过程、加密密钥和相关工具。创建 EBS 快照不正确，因为这是 EBS 的备份解决方案。它在执行时不提供 EBS 卷内数据的安全性。

将 EC2 实例从公用子网迁移到专用子网是不正确的，因为您要保护的数据是 EBS 卷和 S3 存储桶中的数据。将您的 EC2 实例移动到专用子网涉及不同的安全实践，在这种情况下，这并不能达到您想要的效果。使用 AWS Shield 和 WAF 是不正确的，因为它们可以保护您免受 web 应用程序的常见安全威胁。然而，您试图实现的是在 EBS 和 S3 中保护和加密您的数据。

参考文献：

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html>

<http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingEncryption.html> 查看此亚马逊 EBS 备忘单：

<https://tutorialsdojo.com/amazon-ebs/>

一位解决方案架构师正在一家大型 IT 咨询公司工作。其中一个客户正在 AWS 中启动一个文件共享 web 应用程序，该应用程序需要一个持久的存储服务来托管其静态内容，如 PDF、Word 文档、高分辨率图像等。架构师应使用哪种类型的存储服务来满足此要求？

- A、Amazon RDS 实例
- B、亚马逊 EBS 卷
- C、Amazon EC2 实例存储
- D、亚马逊 S3

答案 D

分析：

Amazon S3 是用于互联网的存储。它是一种简单的存储服务，为软件开发人员提供了一种耐用、可扩展、可靠、低延迟的数据存储基础设施，成本非常低。Amazon S3 为客户提供了高度耐用的存储基础设施。版本控制通过在客户意外覆盖或删除对象时提供恢复手段，提供了额外的保护级别。请记住，该场景需要静态内容的持久存储。这两个关键字实际上指的是 S3，因为它非常耐用，适合存储静态内容。

因此，Amazon S3 是正确答案。

Amazon EBS 卷不正确，因为与 S3 相比，它的持久性较差。此外，最好将静态内容存储在 S3 中，而不是 EBS 中。

Amazon EC2 实例存储是不正确的，因为它绝对不适合-一旦 EC2 实例重新启动，它所保存的数据将立即被清除。

Amazon RDS 实例不正确，因为 RDS 实例只是一个数据库，不适合存储静态内容。默认情况下，RDS 是不持久的，除非您将其启动为多 AZ 部署配置。

参考：

<https://aws.amazon.com/s3/faqs/>

<https://d1.awsstatic.com/whitepapers/Storage/AWS%20Storage%20Services%20Whitepaper-v9.pdf#page=24>

查看此 Amazon S3 备忘单：<https://tutorialsdojo.com/amazon-s3/>

Q190.本地服务器正在使用 SMB 网络文件共享来存储应用程序数据。该应用程序每天产生大约 50MB 的数据，但它只需要访问其中的一部分用于日常处理。为了节省存储成本，该公司计划将所有应用程序数据复制到 AWS，但他们希望保留以与本地文件共享相同的低延迟访问检索数据的能力。该公司没有能力开发该操作所需的工具。公司应使用哪种 AWS 服务？

- A、AWS 存储网关
- B、用于 Windows 文件服务器的 Amazon FSx
- C、AWS 虚拟专用网（VPN）
- D、AWS 雪球边缘

答：

分析：

AWS 存储网关是一种混合云存储服务，可让您在现场访问几乎无限的云存储。客户使用存储网关简化存储管理并降低成本

用于关键的混合云存储用例。其中包括将备份移动到云，使用云存储支持的本地文件共享，以及为本地应用程序提供 AWS 中数据的低延迟访问。

特别是对于这个场景，您可以使用 Amazon FSx 文件网关来支持本地应用程序的 SMB 文件共享。它还满足了低延迟访问的要求。Amazon FSx 文件网关有助于加快基于文件的存储迁移到云，从而实现更快的性能、更好的数据保护和更低的成本。

因此，正确答案是：AWS 存储网关。

AWS 虚拟专用网络（VPN）不正确，因为该服务主要用于建立从本地网络到 AWS 的加密连接。Amazon FSx for Windows 文件服务器不正确。这不会提供低延迟访问，因为所有文件都存储在 AWS 上，这意味着它们将通过互联网访问。AWS 存储网关支持本地缓存，无需任何开发开销，因此适用于低延迟应用程序。

AWS 雪球边缘不正确。雪球边缘是一种具有板载存储和计算能力的雪球设备，除了在本机环境和 AWS 云之间传输数据外，还可以进行本地处理。

它只是一个数据迁移工具，而不是存储服务。

参考文献：

<https://aws.amazon.com/storagegateway/>

<https://docs.aws.amazon.com/storagegateway/latest/userguide/CreatingAnSMBFileShare.html> AWS 存储网关概述：

<https://www.youtube.com/watch?v=pNb7xOBJjHE> 查看

此 AWS 存储网关备忘单：

<https://tutorialsdojo.com/aws-storage-gateway/>

Q191. 一家公司正在为将在 AWS 中部署的国际汇款服务建立云架构，该服务将在全球拥有数千名用户。该服务应全天候可用，以避免任何业务中断，并应具有足够的弹性，以处理整个 AWS 区域的中断。为了满足这一需求，解决方案架构师已将其 AWS 资源部署到多个 AWS 区域。他需要使用路由 53 并将其配置为尽可能多地将所有资源设置为始终可用。当资源变得不可用时，路由 53 应检测到它不健康，并在响应查询时停止包括它。

以下哪项是解决方案架构师在此场景中应使用的最容错路由配置？

- A、 使用一个主资源和一个辅助资源配置主动-主动故障切换。
- B、 配置具有多个主资源和辅助资源的主动-被动故障切换。
- C、 使用加权记录配置主动-被动故障切换。
- D、 使用加权路由策略配置主动-主动故障切换。

答案 D

分析：

您可以使用路由 53 运行状况检查来配置主动-主动和主动-被动故障切换配置。您可以使用除故障转移之外的任何路由策略（或路由策略的组合）配置主动-主动故障转移，也可以使用故障转移路由策略配置主动-被动故障转移。

主动-主动故障切换

当您希望所有资源在大部分时间都可用时，请使用此故障转移配置。当资源变得不可用时，路由 53 可以检测到它不健康，并在响应查询时停止包括它。

在主动-主动故障切换中，具有相同名称、相同类型（如 A 或 AAAA）和相同路由策略（如加权或延迟）的所有记录都处于活动状态，除非路由 53 认为它们不健康。路由 53 可以使用任何健康记录来响应 DNS 查询。主动-被动故障转移当您希望主资源或资源组在大部分时间可用，并且希望辅助资源或资源群在所有主资源不可用的情况下处于备用状态时，使用主动-被动的故障转移配置。当响应查询时，路由 53 仅包括健康的主资源。如

果所有主资源都不健康，则响应 DNS 查询，路由 53 开始仅包括健康的辅助资源。使用加权记录配置主动-被动故障切换和使用多个主资源和辅助资源配置主动-被动式故障切换是不正确的，因为

故障转移主要用于以下情况：您希望主资源或一组资源在大部分时间都可用，并且您希望在所有主资源不可用的情况下，辅助资源或资源组处于备用状态。在这种情况下，您的所有资源应尽可能随时可用，这就是为什么您必须使用主动-主动故障转移。配置具有一个主资源和一个辅助资源的主动-主动故障转移是不正确的，因为您无法使用一个主和一个次资源设置主动-主动的故障转移。请记住，主动-主动故障切换始终使用所有可用资源，而无需主资源或辅助资源。

参考文献：

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-types.html>

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html>

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-configuring.html> 亚马逊路线 53 概述：

<https://www.youtube.com/watch?v=Su308t19ubY>

查看此亚马逊路线 53 备忘单：<https://tutorialsdojo.com/amazon-route-53/>

Q192 一家公司拥有一个全球在线交易平台，来自世界各地的用户定期将数 TB 的交易数据上传到一个集中的 S3 存储桶。您应该在当前系统中使用什么 AWS 功能来提高吞吐量，并确保持续快速地将数据传输到 Amazon S3 存储桶，而不管用户位于何处？

- A、使用 CloudFront 源访问标识
- B、Amazon S3 传输加速
- C、FTP
- D、AWS 直接连接

答案 B

分析：

Amazon S3 传输加速支持在客户机和 Amazon S3Bucket 之间进行长距离、快速、轻松和安全的文件传输。传输加速利用了 Amazon CloudFront 全球分布的 AWS 边缘位置。当数据到达 AWS 边缘位置时，数据将通过优化的网络路径路由到 Amazon S3 存储桶。

FTP 是不正确的，因为文件传输协议不能保证快速吞吐量和一致、快速的数据传输。

AWS 直接连接是不正确的，因为您的用户遍布世界各地，而不仅仅是您的内部数据中心。直接连接成本太高，肯定不适合此目的。使用 CloudFront 源访问标识是不正确的，因为这是一个确保只有 CloudFront 才能提供 S3 内容的功能。它不会增加吞吐量，也不会确保向客户快速交付内容。参考：

<http://docs.aws.amazon.com/AmazonS3/latest/dev/transfer-acceleration.html> 查看此 Amazon S3 备忘单：

<https://tutorialsdojo.com/amazon-s3/>

S3 传输加速 vs 直连 vs VPN vs 雪球 vs 雪地车：

<https://tutorialsdojo.com/s3-transfer-acceleration-vs-direct-connect-vs-vpn-vs-snowball-vs-雪地摩托/AWS 服务备忘单>
比较: <https://tutorialsdojo.com/comparison-of-aws-services/>

Q193.在 Amazon EC2 中,您可以从启动实例到终止实例。您可以通过更改 EC2 实例状态来灵活控制计算成本。关于 EC2 账单,以下哪项陈述是正确的?(选择两个。)

- A、 当您的保留实例处于终止状态时,您将收到账单。
- B、 当 Spot 实例准备以停止状态停止时,您将收到账单。
- C、 当实例不处于运行状态时,您将不会因任何实例使用而付费。
- D、 当按需实例处于挂起状态时,您将收到账单。
- E、 当按需实例准备以停止状态休眠时,您将收到账单。

答案: AE

分析:

通过使用 Amazon EC2 管理您的实例,从启动到终止,您可以确保您的客户对您实例上托管的应用程序或站点拥有最佳体验。下图表示实例状态之间的转换。

请注意,您无法停止和启动实例存储备份实例:

以下是有效的 EC2 生命周期实例状态:

挂起-实例正在准备进入运行状态。实例在第一次启动时,或在处于停止状态后重新启动时,将进入挂起状态。

正在运行-实例正在运行并准备使用。

正在停止-实例正在准备停止。请注意,如果它准备停止,您将不会收到账单。但是,如果它只是准备休眠,您仍然会收到账单。已停止-实例已关闭,无法使用。实例可以随时重新启动。正在关闭-实例正在准备终止。已终止-实例已被永久删除,无法重新启动。请注意,应用于已终止实例的保留实例在其期限结束之前仍将根据其付款选项进行计费。

该选项表示:当您的按需实例准备以停止状态休眠时,您将收到账单,这是正确的,因为当实例状态正在停止时,如果它准备停止,您将不会收到账单。但是,如果它只是准备休眠,您仍将收到账单。“当您的保留实例处于终止状态时,您将被计费”选项是正确的,因为应用于终止实例的保留实例在其期限结束之前仍将根据其付款选项计费。事实上,我向亚马逊团队提出了一个关于保留实例的计费条件的拉取请求,该请求已被批准并反映在您的 AWS 官方文档中: <https://github.com/awsdocs/amazon-ec2-user-guide/pull/45>“当 OnDemand 实例处于挂起状态时,您将被计费”选项不正确,因为如果实例处于挂接状态,您将不会被计费。如果您的 Spot 实例准备以停止状态停止,则会向您计费的选项是不正确的,因为如果您的实例准备以终止状态停止,将不会向您计费。该选项表示:当实例不处于运行状态时,您将不会为任何实例使用计费,这是不正确的,因为该语句不完全正确。如果您的实例准备在停止状态下休眠,您仍然可以收取费用。

参考文献: <https://github.com/awsdocs/amazon-ec2-user-guide/pull/45>

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-lifecycle.html> 查看此 Amazon EC2 备忘单:

<https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/>

问题 194.一家全球新闻公司的解决方案架构师正在一个子网中配置一组 EC2 实例，该子网当前位于连接有互联网网关的 VPC 中。所有这些 EC2 实例都可以从 Internet 访问。架构师启动另一个子网并在其中部署 EC2 实例，但是架构师

无法从 Internet 访问 EC2 实例。

这个问题的可能原因是什么？（选择两个。）

- A、路由表未正确配置，无法通过 Internetgateway 将流量从 EC2 实例发送到 Internet。
- B、Amazon EC2 实例没有关联的公共 IP 地址。
- C、Amazon EC2 实例不是同一自动缩放组的成员。
- D、Amazon EC2 实例没有附加的弹性结构适配器（EFA）。
- E、路由表未正确配置，无法通过 customergateway（CGW）将流量从 EC2 实例发送到 Internet。

回答 AB

分析：

VPC 有一个隐式路由器，您可以使用路由表来控制网络流量的方向。VPC 中的每个子网必须与路由表相关联，该路由表控制子网的路由（子网路由表）。您可以将子网与特定路由表显式关联。否则，子网与主路由表隐式关联。

一个子网一次只能与一个路由表关联，但可以将多个子网与同一子网路由表关联。您可以选择将路由表与 internet 网关或虚拟专用网关（网关路由表）关联。这使您能够为通过网关进入 VPC 的入站流量指定路由规则

确保子网路由表中也有到 internet 网关的路由条目。如果此条目不存在，则实例位于专用子网中，无法从 internet 访问。如果无法从 Internet 访问您的 EC2 实例（反之亦然），您通常必须检查两件事：

- 它是否有 EIP 或公共 IP 地址？
- 路由表配置是否正确？

以下是正确答案：

- Amazon EC2 实例没有与其关联的公共 IP 地址。
- 路由表未正确配置，无法通过 Internet 网关将流量从 EC2 实例发送到 Internet。

“Amazon EC2 实例不是同一自动缩放组的成员”选项不正确，因为自动缩放组不影响 EC2 实例的 Internet 连接。“Amazon EC2 实例没有连接的弹性结构适配器（EFA）”选项不正确，因为弹性结构适配器只是一个网络设备，您可以连接到 Amazon EC1 实例，以加速高性能计算（HPC）和机器学习应用程序。EFA 使您能够利用 AWS 提供的可伸缩性、灵活性和弹性，实现本地 HPC 集群的应用程序性能。但是，您的 EC2 实例访问公共 Internet 并不需要此组件。“路由表未正确配置，无法通过客户网关（CGW）将流量从 EC2 实例发送到 Internet”选项不正确，因为在设置 VPN 时使用了 CGW。正确的网关应该是 Internet 网关。参考文献：

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario2.html

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Route_Tables.html 查看此亚马逊 VPC 备忘单:

<https://tutorialsdojo.com/amazon-vpc/>

Q195.一家公司的客户遍布全球，他们访问存储在多个 S3 存储桶中的产品文件，这些存储桶位于各自的 CloudFront web 发行版后面。他们目前希望将内容交付给特定的客户机，并且需要确保只有该客户机可以访问数据。目前，他们所有客户端都可以直接使用 S3URL 或通过 CloudFront 分发版访问他们的 S3 存储桶。解决方案架构师必须仅通过 CloudFront 提供私有内容，以确保文件的分发。架构师应该实施哪些行动组合来满足上述要求？（选择两个。）

- A、使用 S3 预签名 URL 以确保只有其客户端可以访问文件。删除使用 Amazon S3URL 为其他人读取文件的权限。
- B、使用 AWS 应用程序网格以确保只有其客户端可以访问文件。
- C、通过创建源访问标识（OAI）限制对源中文件的访问，并授予其读取存储桶中文件的权限。
- D、使用 AWS Cloud Map 确保只有他们的客户端可以访问这些文件。
- E、要求用户使用特殊的 CloudFront 签名 URL 或签名 Cookie 访问私人内容。

行政长官的答覆

分析:

许多在互联网上分发内容的公司希望限制对文档、业务数据和数据的访问，

用于选定用户（例如已支付费用的用户）的媒体流或内容。要使用 CloudFront 安全地提供此私有内容，您可以执行以下操作：

- 要求您的用户通过使用特殊的 CloudFront 签名 URL 或签名 Cookie 访问您的私人内容。
- 要求您的用户使用 CloudFront URL（而不是 Amazon S3 URL）访问您的亚马逊 S3 内容。不需要要求 CloudFront URL，但建议防止用户绕过您在签名 URL 或签名 Cookie 中指定的限制。您可以通过为 AmazonS3 bucket 设置源访问标识（OAI）来实现这一点。您还可以为配置为网站端点的专用 HTTP 服务器或 Amazon S3 bucket 配置自定义标头。

默认情况下，所有对象和桶都是私有的。如果您希望您的用户/客户能够将特定对象上传到您的 bucket，但不要要求他们具有 AWS 安全凭据或权限，则预签名 URL 非常有用。

您可以使用 AWS SDK for Java 或 AWS SDK 用于 .NET 以编程方式生成预签名 URL。如果您使用的是 Microsoft Visual Studio，您还可以使用 AWS 资源管理器生成预签名的对象 URL，而无需编写任何代码。任何收到有效预签名 URL 的人都可以编程方式上传对象。

因此，正确答案是：

- 通过创建源访问标识（OAI）限制对源中文件的访问，并授予其读取存储桶中文件的权限。
- 要求用户使用特殊的 CloudFront 签名 URL 或签名 Cookie 访问私人内容。

“使用 AWS App Mesh 以确保只有其客户端可以访问文件”的选项是不正确的，因为 AWS App Mesh 只是一个服务网格，它提供应用程序级网络，使您的服务能够轻松跨多种类型的计算基础设施进行通信。“使用 AWS 云地图以确保只有其客户端可以访问文件”的选项是不正确的，因为 AWS 云图只是一种云资源发现服务，允许您使用自定义名称命名应用程序资源，并自动更新动态变化资源的位置。

该选项表示：使用 S3 预签名 URL，以确保只有其客户端可以访问文件。删除使用 Amazon S3 URL 为其他人读取文件的权限是不正确的。虽然这可能是一个有效的解决方案，但它不能满足通过 CloudFront 提供私有内容的要求，因为它仅用于保护文件的分发。一个更好的解决方案是设置源访问标识（OAI），然后在 CloudFront web 分发中使用签名 URL 或签名 Cookie。

参考文献：

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/PrivateContent.html>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/PresignedUrlUploadObject.html> 查看此 Amazon CloudFront 备忘单：

<https://tutorialsdojo.com/amazon-cloudfront/>

S3 预签名 URL 与云前端签名 URL 与源访问标识（OAI）<https://tutorialsdojo.com/s3-presigned-urls-vs-cloudfront-signed-urls-vs-origin-access-identity-oai/AWS> 服务备忘单比较：<https://tutorialsdojo.com/comparison-of-aws-services/>

Q196. 一家公司计划使用持久存储服务将本地数据库备份存储到 AWS 云。

要移动备份数据，他们需要使用一种服务，该服务可以通过标准文件存储协议存储和检索对象，以实现快速恢复。

以下哪个选项将满足此要求？

- A、 使用 Amazon EBS 卷存储所有备份数据，并将其连接到 Amazon EC2 实例。
- B、 使用 AWS Snowball Edge 直接备份亚马逊 S3 冰川中的数据。
- C、 使用 AWS 存储网关文件网关将所有备份数据存储在 Amazon S3 中。
- D、 使用 AWS 存储网关卷网关存储备份数据，并使用 Amazon S3 API 操作直接访问备份数据。

答案 C

分析：

文件网关向 Amazon S3 提供了一个基于文件的接口，它显示为网络文件共享。它使您能够通过标准文件存储协议存储和检索 AmazonS3 对象。文件网关允许您现有的基于文件的应用程序或设备使用安全持久的云存储，而无需修改。使用文件网关，您配置的 S3 存储桶将作为网络文件系统（NFS）装载点或服务器消息块（SMB）文件共享。要将本地备份数据存储到持久的云存储服务，可以使用文件网关。通过标准文件存储协议（SMB 或 NFS）存储和检索对象的网关。文件网关使您现有的基于文件的应用程序、设备和工作流能够使用 Amazon S3，而无需修改。文件网关安全持久地将文件内容和元数据存储为对象，同时为本地应用程序提供对缓存数据的低延迟访问。

因此，正确答案是：使用 AWS 存储网关文件网关将所有备份数据存储在 Amazon S3 中。

表示：使用 AWS 存储网关卷网关存储备份数据，并使用 Amazon S3 API 操作直接访问备份数据的选项不正确。尽管这是一种可能的解决方案，但您无法使用 Amazon S3 API 直接访问卷网关。您应该使用文件网关访问 AmazonS3 中的数据。

“使用 Amazon EBS 卷存储所有备份数据并将其附加到 Amazon EC2 实例”的选项不正确。请注意，在该场景中，您需要将备份数据存储在持久存储服务中。Amazon EBS 卷不像 Amazon S3 那样持久。此外，文件存储协议（如 NFS 或 SMB）不受 EBS 的直接支持。“使用 AWS Snowball Edge 直接备份 Amazon S3 Glacier 中的数据”选项不正确，因为 AWS Snowball Edge 无法通过标准文件存储协议存储和检索对象。此外，Snowball Edge 无法直接将备份集成到 S3 Glacier。参考文献：

<https://aws.amazon.com/storagegateway/faqs/>

<https://aws.amazon.com/s3/storage-classes/>查看此

AWS 存储网关备忘单：

<https://tutorialsdojo.com/aws-storage-gateway/>

Q197.一家大型保险公司的 AWS 账户包含同一地区的三个 VPC（DEV、UAT 和 PROD）。UAT 使用 VPC 对等连接与 PROD 和 DEV 对等。所有 VPC 都具有非重叠的 CIDR 块。该公司希望推动从开发到生产的小型代码发布，以加快上市时间。以下哪个选项有助于公司实现这一目标？

- A、将 DEV 和 PROD VPC 更改为具有重叠的 CIDR 块，以便能够连接它们。
- B、使用适当的路由在 PROD 和 DEV 之间创建新的 VPC 对等连接。
- C、使用 VPC 对等连接作为目标，在 DEV 路由表中创建一个新的 PROD 条目。
- D、什么也不做。由于这两个 VPC 已经通过 UAT 连接，因此它们已经相互连接。

答案 B

分析：

VPC 对等连接是两个 VPC 之间的网络连接，使您能够在它们之间路由流量。任何一个 VPC 中的实例都可以彼此通信，就像它们在同一网络中一样。您可以在您自己的 VPC 之间创建 VPC 对等连接，与另一个 AWS 帐户中的 VPC，或与不同 AWS 区域中的 VP。

AWS 使用 VPC 的现有基础设施创建 VPC 对等连接；它既不是网关也不是 VPN 连接，不依赖于单独的物理硬件。通信不存在单点故障或带宽瓶颈。

使用 VPC 对等连接作为目标在 DEV 路由表中创建一个新条目以 PROD 是不正确的，因为即使您配置了路由表，两个 VPC 仍将断开连接，直到您在它们之间建立了 VPC 对等链接。

将 DEV 和 PROD VPC 更改为具有重叠的 CIDR 块以便能够连接它们是不正确的，因为您无法对等具有重叠 CIDR 块的两个 VPC。选项是：什么都不做。由于这两个 VPC 已经通过 UAT 连接，因此它们已经彼此连接是不正确的，因为不允许传递 VPC 对等。因此，即使 DEV 和 PROD 都在 UAT 中连接，这两个 VPN 也没有直接连接。

参考：

<https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-peering.html> 查看这些亚马逊专有网络和专有网络对等备忘单：

<https://tutorialsdojo.com/amazon-vpc/>

<https://tutorialsdojo.com/vpc-peering/> 以下

是 VPC 对等的快速介绍：

<https://youtu.be/i1A1eH8vLtk>

Q198. 由于查询请求量大，在线报告应用程序的数据库性能显著降低。解决方案架构师正试图说服她的客户为其应用程序使用 **Amazon RDS 读取副本**，而不是设置多 **AZ** 部署配置。架构师应该指出，在多 **AZ** 上使用读取副本的两个好处是什么？（选择两个。）

- A、它通过提高主数据库的 IOPS 来增强其读取性能，并通过 AWS 全局加速器加速其查询处理。
- B、允许对读取副本执行读操作和写操作，以补充主数据库。
- C、在可用性区域服务失败的情况下提供同步复制和自动故障切换。
- D、提供异步复制，并通过从主数据库中获取读取重数据库工作负载来提高主数据库的性能。
- E、它弹性地扩展，超出了单个数据库实例的容量限制，以适应大量读取的数据库工作负载。

答：德

分析：

Amazon RDS 读取副本为数据库（DB）实例提供了增强的性能和耐用性。此功能使您可以轻松地弹性扩展，超出单个数据库实例的容量限制，以应对读取繁重的数据库工作负载。

您可以创建给定源数据库实例的一个或多个副本，并从数据的多个副本提供高容量应用程序读取流量，从而提高聚合读取吞吐量。当需要成为独立数据库实例时，还可以升级读取副本。对于 MySQL、MariaDB、PostgreSQL 和 Oracle 数据库引擎，Amazon RDS 使用源数据库实例的快照创建第二个数据库实例。然后，只要源数据库实例发生更改，它就使用引擎的本机异步复制来更新读取副本。读取副本作为只允许只读连接的 DB 实例运行；应用程序可以连接到读取副本，就像连接到任何数据库实例一样。Amazon RDS 复制源数据库实例中的所有数据库。

当您为 Amazon RDS for MySQL、MariaDB、PostgreSQL 和 Oracle 创建读取副本时，Amazon RDS 在源数据库实例和读取副本之间使用公钥加密建立安全通信通道，即使在跨区域复制时也是如此。Amazon RDS 建立任何 AWS 安全配置，例如添加启用安全通道所需的安全组条目。您还可以在区域内或区域之间为使用 AWS 密钥管理服务（KMS）加密的 Amazon RDS for MySQL、MariaDB、PostgreSQL 和 Oracle 数据库实例创建读取副本。

因此，正确答案是：

- 对于读取繁重的数据库工作负载，它弹性地扩展超出单个数据库实例的容量限制。
- 提供异步复制，并通过从主数据库中获取大量的数据库工作负载来提高主数据库的性能。

“允许对读副本执行读和写操作以补充主数据库”选项不正确，因为读副本主要用于卸载主数据库实例的只读操作。默认情况下，您不能对读取副本执行写入操作。该选项表示：

在可用性区域服务失败的情况下提供同步复制和自动故障切换是不正确的，因为这是多 AZ 的好处，而不是读取副本的好处。此外，读取副本提供异步复制类型，而不是同步复制。“它通过提高 IOPS 来增强主数据库的读取性能，并通过 AWS 全局加速器加速查询处理”这一选项是不正确的，因为读取副本本身不会升级或增加主数据库实例的读取吞吐量，但它为应用程序提供了从副本获取数据的方法。这样，它提高了整个数据库层（而不仅仅是主数据库实例）的整体性能。它既不会提高 IOPS，也不会使用 AWS 全局加速器来加速主数据库的计算容量。AWS Global Accelerator 是一种与 RDS 无关的网络服务，它将用户流量引导到离客户端最近的应用程序端点，从而减少互联网延迟和抖动。它只是通过选播将流量路由到最近的边缘位置。

参考文献：

<https://aws.amazon.com/rds/details/read-replicas/> <https://aws.amazon.com/rds/features/multi-az/>

查看此 Amazon RDS 备忘单：

<https://tutorialsdojo.com/amazon-relational-database-service-amazon-rds/>附加教程-如何使我的 RDS MySQL 读副本可写？<https://youtu.be/j5da6d2TIPc>

Q199.一个主要的电视网络有一个在八个 Amazon T3 EC2 实例上运行的 web 应用程序。应用程序进程一致且未出现峰值的请求数。为了确保八个实例是：

解决方案架构师应始终运行，创建自动缩放组，并在所有实例之间均匀分配负载。

以下哪个选项可以满足给定要求？

- A、在 Amazon 弹性负载均衡器后面的一个可用性区域中部署 8 个具有自动扩展功能的 EC2 实例。
- B、在 Amazon ElasticLoad 平衡器后面的一个区域部署四个具有自动伸缩功能的 EC2 实例，在另一个区域中部署四个。
- C、在 Amazon 弹性负载均衡器后面的四个区域部署两个具有自动伸缩功能的 EC2 实例。
- D、在 Amazon 弹性负载均衡器后面的同一区域中，在一个可用性区域中部署四个具有自动伸缩功能的 EC2 实例，在另一可用性区域部署四个。

答案 D

分析：

最好的选择是在一个可用性区域部署四个 EC2 实例，在同一区域的另一可用性区域在 Amazon 弹性负载均衡器后面部署四个。这样，如果一个可用区域出现故障，则还有另一个可用的区域可以容纳流量。

当第一个 AZ 下降时，第二个 AZ 将只有初始的 4 个 EC2 实例。由于解决方案使用自动缩放，因此最终将缩放到 8 个实例。4 台服务器的 110% 计算容量可能会导致服务的某些降级，但不会导致完全中断，因为仍有一些实例处理请求。根据自动扩展组中的扩展配置，可以在几分钟内启动另外 4 个 EC2 实例。

T3 实例还具有突发或超出实例当前计算能力的突发稳定性能力，以便根据工作负载的要求获得更高的性能。因此，您的 4 台服务器将能够在短时间内管理 110% 的计算容量。这是云计算相对于我们的本地网络架构的力量。它提供了弹性和无与伦比的可扩展性。请注意，如果该区域的可用性区域发生中断，自动扩展将向剩余可用性区域启动额外的 EC2 实例。因此，正确答案是这样的选项：

在 Amazon 弹性负载均衡器后面的同一区域中，在一个可用性区域部署四个具有自动扩展功能的 EC2 实例，在另一个可用区部署四个。

“在 Amazon 弹性负载均衡器后面的一个可用性区域中部署八个具有自动扩展功能的 EC2 实例”选项是不正确的，因为该架构不是高度可用的。如果可用性区域下降，则您的 web 应用程序将无法访问。以下选项是不正确的：在 Amazon 弹性负载均衡器后面的一个区域部署四个具有自动伸缩的 EC2 实例，在另一个区域中部署四个 EC2 实例；在 Amazon 弹性负载均衡器之后的四个区域部署两个具有自动缩放的 EC2 实例，因为 ELB 被设计为仅在一个区域运行，而不是跨多个区域运行。参考文献：

<https://aws.amazon.com/elasticloadbalancing/>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-increase-availability.html> AWS 弹性负载均衡概述：

<https://youtu.be/UBI5dw59DO8>

查看 AWS 弹性负载均衡（ELB）备忘单：<https://tutorialsdojo.com/aws-elastic-load-平衡/>

Q200.一家航空航天工程公司最近采用了 AWS 的混合云基础设施。解决方案架构师的任务之一是为其 EC2 实例及其数据库实例启动具有公共和私有子网的 VPC。

关于亚马逊专有网络子网，以下哪项陈述是正确的？（选择两个。）

- A、每个子网跨越 2 个可用性区域。
- B、专用子网中的 EC2 实例只有在具有弹性 IP 时才能与 Internet 通信。
- C、VPC 中允许的块大小介于 /16 网络掩码（65536 IP 地址）和 /27 网络掩码（32 IP 地址）之间。
- D、每个子网映射到单个可用性区域。
- E、您创建的每个子网都自动与 VPC 的主路由表关联。

答：德

分析：

专有网络覆盖区域内的所有可用区域。创建 VPC 后，您可以在每个 VPC 中添加一个或多个子网可用性区域。创建子网时，为子网指定 CIDR 块，它是 VPC CIDR 块的子集。每个子网必须完全位于一个可用性区域内，并且不能跨区域。可用性区域是设计为与其他可用性区域中的故障隔离的不同位置。通过在单独的可用性区域中启动实例，可以保护应用程序不受单个位置故障的影响。

以下是关于子网您必须记住的要点：

- 每个子网映射到单个可用性区域。
- 您创建的每个子网都自动与 VPC 的主路由表关联。
- 如果子网的流量路由到 Internet 网关，则该子网称为公共子网。

该选项表示：专用子网中的 EC2 实例只有在具有弹性 IP 时才能与 Internet 通信，这是不正确的。私有子网中的 EC2 实例不仅可以通过弹性 IP 与互联网通信，还可以通过 NAT 实例或 NAT 网关与公共 IP 地址通信。请注意，

私有 IP 地址和公共 IP 地址之间存在区别。为了实现与互联网的通信，通过网络地址转换（NAT）将公共 IPv4 地址映射到主私有 IPv4 地址。

该选项表示：VPC 中允许的块大小介于/16 网络掩码（65536 IP 地址）和/27 网络掩码之间（32 个 IP 地址）不正确，因为 VPC 中允许的块大小介于/16 网络掩码（65536 个 IP 地址）、/28 网络掩码（16 个 IP 地址），而不是/27 网络掩码之间。“每个子网跨越 2 个可用区域”选项不正确，因为每个子网必须完全位于一个可用区域内，并且不能跨越区域。参考文献：

https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-ip-addressing.html> 查看此亚马逊专有网络备忘单：

<https://tutorialsdojo.com/amazon-vpc/>

Dojo 的 AWS 认证解决方案架构师助理考试学习指南教程：<https://tutorialsdojo.com/aws-certified-solutions-architect-associate/>

Q201.一家公司计划在 AWS 中建立云基础设施。在规划中，讨论了您需要部署两个应连续运行三年的 EC2 实例。EC2 实例的 CPU 利用率预计也是稳定和可预测的。

哪种亚马逊 EC2 定价类型最符合成本效益，最适合此场景？

- A、现场实例
- B、保留实例
- C、专用主机
- D、按需实例

答案 B

分析：

与按需实例定价相比，保留实例为您提供了显著的折扣（高达 75%）。此外，当将保留实例分配给特定可用性区域时，它们会提供容量保留，从而使您对在需要时启动实例的能力更有信心。

对于具有稳定状态或可预测使用的应用程序，与使用按需实例相比，保留实例可以提供显著的节省。

建议保留实例用于：

- 具有稳定状态使用的应用程序
- 可能需要保留容量的应用程序
- 承诺在 1 年或 3 年期限内使用 EC2 以降低总计算成本的客户参考：

<https://aws.amazon.com/ec2/pricing/> <https://aws.amazon.com/ec2/pricing/reserved-instances/>

亚马逊 EC2 概述：https://www.youtube.com/watch?v=7VsGIHT_jQE

查看此 Amazon EC2 备忘单: <https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/>

Q202.解决方案架构师无法使用家庭计算机通过 SSH 连接到新部署的 EC2 实例。然而，架构师能够成功访问 VPC 中的其他现有实例，没有任何问题。

架构师应检查并纠正以下哪项以恢复连接？

- A、配置 EC2 实例的安全组，以允许 IP 通过端口 22 进入流量。
- B、配置 VPC 的网络访问控制列表，以允许 IP 通过端口 22 进入流量。
- C、使用 Amazon 数据生命周期管理器。
- D、配置 EC2 实例的安全组，以允许 IP 通过端口 3389 进入流量。

答:

分析:

当通过 SSH 连接到 EC2 实例时，需要确保在 EC2 实例的安全组上允许端口 22。

安全组充当虚拟防火墙，控制一个或多个实例的流量。启动实例时，将一个或多个安全组与实例关联。您可以向每个安全组添加规则，以允许进出其关联实例的流量。您可以随时修改安全组的规则；新规则将自动应用于与安全组关联的所有实例。

使用亚马逊数据生命周期管理器是不正确的，因为它主要用于管理 AWS 资源的生命周期，而不允许某些流量通过。将 VPC 的网络访问控制列表配置为允许 IP 通过端口 22 进入流量是不正确的，因为这在这种情况下是不必要的，因为指定您可以连接到其他 EC2 实例。此外，网络 ACL 非常适合控制进出整个 VPC 的流量，而不仅仅是一个 EC2 实例。

配置 EC2 实例的安全组以允许通过端口 3389 从 IP 进入流量是不正确的，因为这与 RDP 而不是 SSH 有关。

参考:

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html> 查看以下 AWS 服务

比较备忘单: <https://tutorialsdojo.com/comparison-of-aws-services/>

Q203.解决方案架构师需要部署一个移动应用程序，以收集流行歌曲比赛的投票。来自世界各地的数百万用户将使用手机提交投票。这些投票必须收集并存储在一个高度可扩展和高度可用的数据存储中，该数据存储将被查询以进行实时排名。

架构师应该使用以下哪种服务组合来满足此要求？

- A、亚马逊红移和 AWS 移动中心
- B、亚马逊关系数据库服务（RDS）和亚马逊 MQ
- C、亚马逊极光和亚马逊认知
- D、亚马逊 DynamoDB 和 AWS AppSync

答案 D

分析：

当“耐用性”这个词出现时，您首先想到的是 Amazon S3。由于该服务在回答选项中不可用，我们可以查看其他可用的数据存储，即 Amazon DynamoDB。

DynamoDB 是一种耐用、可扩展、高可用的数据存储，可用于实时制表。您还可以将 AppSync 与 DynamoDB 结合使用，使您轻松构建协作应用程序，使共享数据实时更新。您只需使用简单的代码语句为应用程序指定数据，AWS AppSync 即可管理所有内容

需要保持应用程序数据实时更新。这将允许您的应用程序访问 Amazon DynamoDB 中的数据，触发 AWS Lambda 函数，或运行 Amazon Elasticsearch 查询，并组合这些服务中的数据以提供应用程序所需的准确数据。亚马逊红移和 AWS 移动中心是不正确的，因为亚马逊红移主要用于数据仓库和在线分析处理（OLAP）。尽管此服务可用于此场景，但 DynamoDB 仍然是首选，因为它具有更好的耐用性和可伸缩性。Amazon 关系数据库服务（RDS）和 Amazon MQ 以及 Amazon Aurora 和 Amazon Cognito 是该场景中可能的答案，但是，DynamoDB 更适合于不支持的简单移动应用程序

与企业 web 应用程序相比，具有复杂的数据关系。场景中说明移动应用程序将在世界各地使用，这就是为什么您需要全球支持的数据存储服务。与使用 DynamoDB 的全局表功能相比，为 RDS 和 Aurora 数据库实例实现多区域部署将是一项管理开销。

参考文献：

<https://aws.amazon.com/dynamodb/faqs/>

<https://aws.amazon.com/appsync/>

亚马逊 DynamoDB 概述：

<https://www.youtube.com/watch?v=3ZOyUNleorU>

查看此 Amazon DynamoDB 备忘单：

<https://tutorialsdojo.com/amazon-dynamodb/>

Dojo 的 AWS 认证解决方案架构师助理考试学习指南教程：<https://tutorialsdojo.com/aws-certified-solutions-architect-associate/>

Q204.一家金融科技初创公司在亚马逊 EC2 实例上部署了一个应用程序，该实例具有附加的实例存储卷和弹性 IP 地址。服务器只能从上午 8 点到下午 6 点访问，并且可以从下午 6 点到上午 8 点停止，以提高成本效率，使用 Lambda 和基于标签自动执行此操作的脚本。当 EC2 实例停止和启动时，会发生以下哪种情况？（选择两个。）

- A、实例的基础主机可能已更改。
- B、ENI（弹性网络接口）被分离。
- C、连接的实例存储设备上的所有数据都将丢失。
- D、弹性 IP 地址与实例解除关联。

E、不会有任何变化。

答覆

分析：

这个问题没有提到 EC2 实例的具体类型，但是，它说它将停止并启动。由于只有 EBS 支持的实例可以停止和重新启动，这意味着该实例是 EBS 支持。请记住，实例存储备份实例只能重新启动或终止，如果 EC2 实例停止或终止，则其数据将被擦除。如果您停止了 EBS 支持的 EC2 实例，该卷将被保留，但任何连接的实例存储卷中的数据将被擦除。请记住，EC2 实例有一个底层物理主机。如果实例停止，AWS 通常会将实例移动到新的主机。你的情况可能会继续

如果主机没有问题，则在同一主机上。此外，如果它是 EC2 Classic 实例，则它的弹性 IP 地址与实例解除关联。否则，如果是 EC2-VPC 实例，则弹性 IP 地址保持关联。

请注意，EBS 支持的 EC2 实例可以具有附加的实例存储卷。这就是为什么有一个选项提到实例存储卷的原因，该选项用于测试您对该特定存储类型的理解。您可以启动一个 EBS 支持的 EC2 实例并连接多个实例存储卷，但请记住，有些 EC2 实例类型不支持这种设置。

因此，正确答案是：

- 实例的基础主机可能已更改。
- 连接的实例存储设备上的所有数据都将丢失。“ENI（弹性网络接口）已分离”选项不正确，因为即使您停止了 EC2 实例，ENI 也将保持连接状态。

表示：弹性 IP 地址与实例解除关联的选项是不正确的，因为即使在停止实例后，EIP 实际上仍将与实例保持关联。表示“不会有任何更改”的选项是不正确的，因为一旦停止并再次启动 EC2 实例，EC2 实例中可能会有很多更改。AWS 可以将虚拟化 EC2 实例移动到另一主机计算机；该实例可能会获得一个新的公共 IP 地址，并且将删除连接的实例存储卷中的数据。

参考文献：

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-lifecycle.html>
<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ComponentsAMIs.html#存储> 查看此 Amazon EC2 备忘单：

<https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/Dojo> 的 AWS 认证解决方案架构师助理考试学习指南教程：<https://tutorialsdojo.com/aws-certified-solutions-architect-associate-saa-c02/>

Q205.一家媒体公司最近发布了他们新创建的 web 应用程序。许多用户试图访问该网站，但他们收到 503 服务不可用错误。系统管理员跟踪了 EC2 实例状态，发现容量已达到最大限制，无法处理所有请求。为了从应用程序的数据中获得见解，他们需要启动实时分析服务。以下哪项允许您批量读取记录？

- A、创建 Kinesis 数据流并使用 AWS Lambda 从数据流中读取记录。
- B、创建一个 Amazon S3 bucket 来存储捕获的数据，并使用 Amazon Athena 分析数据。
- C、创建 Kinesis 数据消防软管，并使用 AWS Lambda 从数据流中读取记录。

D、创建一个 Amazon S3 bucket 来存储捕获的数据，并使用 Amazon 红移光谱来分析数据。

答:

分析:

亚马逊 Kinesis 数据流 (KDS) 是一种大规模可扩展和持久的实时数据流服务。KDS 可以每秒从成千上万的数据源连续捕获千兆字节的数据。您可以使用 AWS Lambda 函数处理 Amazon KDS 中的记录。默认情况下，只要流中有记录可用，Lambda 就会调用函数。Lambda 可以同时处理每个碎片中的多达 10 个批次。如果增加每个碎片的并发批处理数，Lambda 仍然确保分区键级别的有序处理。

第一次调用函数时，AWS Lambda 会创建函数的实例，并运行其处理程序方法来处理事件。当函数返回响应时，它保持活动状态并等待处理其他事件。如果在处理第一个事件时再次调用该函数，Lambda 将初始化另一个实例，该函数将同时处理两个事件。随着更多事件的到来，Lambda 将它们路由到可用实例，并根据需要创建新实例。当请求数量减少时，Lambda 会停止未使用的实例，以释放其他函数的升级容量。由于媒体公司需要实时分析服务，您可以使用 Kinesis 数据流从数据中获取见解。收集的数据以毫秒为单位。使用 AWS Lambda 批量读取记录，并

调用函数处理批处理中的记录。如果 Lambda 从流中读取的批处理中只有一条记录，则 Lambda 只向函数发送一条记录。因此，该场景中的正确答案是：创建 Kinesis 数据流，并使用 AWS Lambda 从数据流中读取记录。

选项说：创建一个 Kinesis

数据消防软管和使用 AWS Lambda 从数据流读取记录不正确。虽然 Amazon Kinesis Data Firehose 几乎实时地捕获和加载数据，但 AWS Lambda 不能设置为其目的地。您可以编写 Lambda 函数并将其与 Kinesis Data Firehose 集成，以便在数据发送到下游之前请求对数据进行额外的定制处理。然而，这种集成主要用于流处理，而不是数据流的实际消耗。在这种情况下，您必须使用 Kinesis 数据流。以下选项均不正确：创建 Amazon S3 bucket 存储捕获的数据，使用 Amazon Athena 分析数据，创建 Amazon S3 bucket 存储捕捉的数据，并使用 Amazon Redshift Spectrum 分析数据。根据该场景，该公司需要一个实时分析服务，可以接收和处理数据。您需要使用 Amazon Kinesis 实时处理数据。

参考文献:

<https://aws.amazon.com/kinesis/data-streams/>

<https://docs.aws.amazon.com/lambda/latest/dg/with-kinesis.html> <https://aws.amazon.com/premiumsupport/> 知识中心 /503 错误经典/

查看此亚马逊 Kinesis 备忘单: <https://tutorialsdojo.com/amazon-kinesis/>

Q206.您所在的媒体公司在 Amazon EC2 上运行了一个视频转码应用程序。每个 EC2 实例轮询一个队列，以找出应该转码的视频，然后运行转码过程。如果此过程中断，视频将由另一个实例根据队列进行转码

系统该应用程序有大量积压的视频需要转码。您的经理希望通过添加更多的 EC2 实例来减少积压，但是，只有在积压减少之前才需要这些实例。

在这种情况下，哪种类型的 Amazon EC2 实例是最经济有效的类型？

A、现场实例

B、保留实例

C、专用实例

D、按需实例

答:

分析:

您需要一个实例，该实例不是用作主服务器，而是用作备用计算资源，以增强应用程序的代码转换过程。一旦积压大量减少，这些情况也应终止。此外，该场景提到，如果当前进程被中断，视频可以由另一个基于排队系统的实例进行转码。这意味着

应用程序可以优雅地处理 EC2 实例的意外终止，如在点实例终止的情况下

当现货价格高于您设定的最高价格时。因此，Amazon EC2 Spot 实例是该场景的最佳且经济有效的选择。

Amazon EC2 Spot 实例是 AWS 云中的备用计算能力，与按需价格相比，您可以获得大幅折扣。EC2 Spot 使您能够优化 AWS 云上的成本，并在相同预算下将应用程序的吞吐量扩展到 10 倍。通过在启动 EC2 实例时简单地选择现货，您可以节省高达 90% 的按需价格。按需实例和点实例之间的唯一区别是，当 EC2 需要恢复容量时，点实例可以被 EC2 中断两分钟的通知。

您可以指定当 Spot 实例中断时，Amazon EC2 是否应休眠、停止或终止 Spot 实例。您可以选择满足您需求的中断行为。请注意，自 2018 年 3 月起，现货 EC2 实例不再有“出价”。您只需设置最高价格即可。

保留实例和专用实例不正确，因为它们都不作为备用计算容量。按需实例是一个有效的选项，但现货实例比按需实例便宜得多。参考文献：

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/spot-interruptions.html>
<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/how-spot-instances-work.html>
<https://aws.amazon.com/blogs/compute/new-amazon-ec2-spot-pricing> 查看此 amazon ec2 备忘单：
<https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/>

Q207. 一家公司有一个按需 EC2 实例，位于 AWS 的一个子网中，该子网承载 web 应用程序。附加到此 EC2 实例的安全组具有以下入站规则：

Type ⓘ	Protocol ⓘ	Port Range ⓘ	Source ⓘ	Description ⓘ
SSH	TCP	22	0.0.0.0/0	

VPC 附带的路由表如下所示。您可以从 Internet 建立到 EC2 实例的 SSH 连接。但是，您无法使用 Chrome 浏览器连接到 web 服务器。

Destination	Target	Status	Propagated
10.0.0.0/27	local	Active	No
0.0.0.0/0	igw-b51618cc	Active	No

以下哪个步骤可以解决问题？

- A、 在路线表中，添加新的路线条目：10.0.0.1/27->本地 B。在路线表，添加新路线条目：0.0-0.0->igw-b51618cc
- C、 在安全组中，添加入站 HTTP 规则。
- D、 在安全组中，删除 SSH 规则。

答案 C

分析：

在这个特定场景中，您已经可以通过 SSH 连接到 EC2 实例。这意味着 VPC 的路由表没有问题。要解决此问题，只需更新安全组并添加入站规则以允许 HTTP 流量。

在安全组中，删除 SSH 规则的选项不正确，因为这样做不会解决问题。它只会禁用已经可用的 SSH 流量。选项如下：在路由表中，添加此新路由条目：

0.0.0.0->igw-b51618cc，在路由表中添加新的路由条目：10.0.1.0/27->local 不正确，因为无需更改路由表。

参考：

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html 查看此亚马逊 VPC 备忘单：

<https://tutorialsdojo.com/amazon-vpc/>

Q208.一家公司正在托管非生产环境中的 EC2 实例，并处理非优先级批处理加载，这些加载可以随时中断。

在这种情况下，可以应用于 EC2 实例的最佳实例购买选项是什么？

- A、 现场实例
- B、 按需容量预订
- C、 保留实例
- D、 按需实例

答：

分析:

Amazon EC2 Spot 实例是 AWS 云中的备用计算能力，与按需价格相比，您可以获得大幅折扣。当 EC2 需要恢复容量时，AWS EC2 可以在两分钟内通知中断。

要使用 Spot 实例，您需要创建一个 Spot 实例请求，其中包括实例数量、实例类型、可用区域以及您愿意为每个实例小时支付的最高价格。如果您的最高价格超过当前现货价格，Amazon EC2 将在容量可用时立即满足您的请求。否则，Amazon EC2 将等待您的请求得到满足或取消请求。

参考文献:

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-spot-instances.html><https://aws.amazon.com/ec2/spot/>

亚马逊 EC2 概述:

https://youtu.be/7VsGIHT_jQE

查看此 Amazon EC2 备忘单: <https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/>

Q209.一家制造公司在 AWS 中运行 EC2 实例。EC2 实例配置为自动缩放。由于服务器上的负载过大，许多请求丢失。自动伸缩正在启动新的 EC2 实例以相应地承担负载，但仍有一些请求丢失。

为了避免丢失最近提交的请求，您应该实施以下哪种最合适的解决方案？

- A、 将 Amazon Aurora 无服务器设置为按需自动扩展 EC2 实例的配置，并启用 Amazon Aurora 并行查询功能，以便对当前数据进行更快的分析查询。
- B、 使用 AmazonSQS 队列来解耦应用程序组件，并根据 AmazonCloudWatch 中的消息数量度量来扩展 EC2 实例。
- C、 使用带有附加弹性结构适配器（EFA）的应用程序的较大实例。
- D、 将自动扩展组替换为群集放置组，以实现紧密耦合的节点到节点通信所需的低延迟网络性能。

答案 B

分析:

Amazon 简单队列服务（SQS）是一种完全受管理的消息队列服务，可以轻松分离和扩展微服务、分布式系统和无服务器应用程序。从每个执行离散功能的单个组件构建应用程序提高了可伸缩性和可靠性，是现代应用程序的最佳实践设计。SQS 使分离和协调云应用程序的组件变得简单且经济高效。使用 SQS，您可以在任何卷上的软件组件之间发送、存储和接收消息，而不会丢失消息或要求其他服务始终可用。

Amazon SQS 队列中的消息数量并不仅仅定义所需的实例数量。事实上，队列中实例的数量可以由多个因素驱动，包括处理消息所需的时间和可接受的延迟量（队列延迟）。解决方案是使用每个实例的积压量度量，目标值是要维护的每个实例的可接受积压量。您可以按如下方式计算这些数字：

每个实例的待办事项：要确定每个实例的待处理事项，请从 Amazon SQS 度量 `ApproximateNumberOfMessages` 开始，以确定 SQS 队列的长度（可用消息数

用于从队列中检索)。将该数字除以车队的运行容量，对于自动扩展组，该容量是处于服务状态的实例数，以获得每个实例的积压。每个实例可接受的积压：要确定目标值，首先计算应用程序可以接受的延迟。然后，取可接受的延迟值，除以 EC2 实例处理消息所需的平均时间。

为了举例说明，假设当前的 `NumberOfMessages` 近似值为 1500，车队的运行容量为 10，如果每条消息的平均处理时间为 0.1 秒，最长可接受延迟为 10 秒，则每个实例的可接受积压为 $10/0.1$ ，等于 100

表示 100 是目标跟踪策略的目标值。由于每个实例的积压量目前为 150 ($1500/10$)，因此您的车队将扩展五个实例以保持与目标值的比例。因此，正确的答案是：使用 Amazon SQS 队列来解耦应用程序组件，并根据 Amazon CloudWatch 中的近似 `NumberOfMessages` 度量扩展 EC2 实例。

将自动扩展组替换为集群放置组以实现紧密耦合的节点到节点通信所需的低延迟网络性能是不正确的，因为尽管集群放置组确实允许您实现低延迟的网络性能，但您仍然需要为您的体系结构使用自动扩展来添加更多 EC2 实例。在应用程序中使用更大的实例和附加的弹性结构适配器 (EFA) 是不正确的，因为使用较大的 EC2 实例不会防止数据在出现较大峰值时丢失。您可以利用 SQS 的持久性和弹性来保持消息可供实例使用。Elastic Fabric Adapter (EFA) 只是 Amazon EC2 实例的网络接口，使客户能够在 AWS 上运行需要高级别节点间通信的应用程序。设置 Amazon Aurora 无服务器，以按需自动扩展 EC2 实例的配置，并启用 Amazon Aurora 用于对当前数据进行更快分析查询的并行查询功能是不正确的，因为尽管 Amazon Aurora 并行查询功能提供了对当前数据的更快分析查询，但 Amazon Aurora Serverless 是一种按需自动扩展的数据库配置，而不是 EC2 实例。这实际上是 Amazon Aurora 数据库的自动缩放配置，而不是计算服务。

参考文献：

<https://aws.amazon.com/sqs/>

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/welcome.html>

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-using-sqs-queue.html>

查看此亚马逊 SQS 备忘单：<https://tutorialsdojo.com/amazon-sqs/>

Q210.一家旅游公司有一套 web 应用程序，托管在一个应用程序负载均衡器后面的按需 EC2 实例自动扩展组中，该应用程序负载均衡器处理来自各种 web 域（如 i-lovemanila）的流量。我爱长滩岛。我爱宿务。com 和许多其他。为了提高安全性并降低总体成本，我们指示您通过允许多个域服务 SSL 流量来保护系统，而无需在每次添加新域时重新验证和重新验证证书。这种从 HTTP 到 HTTPS 的迁移将有助于提高他们的搜索引擎优化和谷歌搜索排名。以下哪项是满足上述要求的最具成本效益的解决方案？

- A、使用通配符证书处理多个子域和不同域。
- B、为证书中的每个附加域添加一个主题替代名称 (SAN)。
- C、使用控制台上载 ALB 中域的所有 SSL 证书，并将多个证书绑定到负载均衡器上的同一安全侦听器。ALB 将使用服务器名称指示 (SNI) 为每个客户端自动选择最佳 TLS 证书。
- D、创建一个新的 CloudFront web 分发，并将其配置为使用专用 IP 地址服务 HTTPS 请求，以便将您的备用域名与每个 CloudFront 边缘位置中的专用 IP 地址相关联。

答案 C

分析：

SNI 自定义 SSL 依赖于传输层安全协议的 SNI 扩展，该协议允许多个域通过同一 IP 地址提供 SSL 通信，包括查看者试图连接的主机名。

您可以在单个负载均衡器后面托管多个 TLS 安全应用程序，每个应用程序都有自己的 TLS 证书。为了使用 SNI，您需要做的就是将多个证书绑定到负载均衡器上的同一个安全侦听器。ALB 将自动为每个客户端选择最佳 TLS 证书。这些功能是免费提供的。

为了满足场景中的要求，您可以使用控制台上传 ALB 中域的所有 SSL 证书，并将多个证书绑定到负载均衡器上的同一安全侦听器。ALB 将使用服务器名称指示（SNI）为每个客户端自动选择最佳 TLS 证书。因此，正确的答案是这样的选项：使用控制台上传 ALB 中域的所有 SSL 证书，并将多个证书绑定到负载均衡器上的同一安全侦听器。ALB 将使用服务器名称指示（SNI）为每个客户端自动选择最佳 TLS 证书。使用通配符证书处理多个子域和不同域是不正确的，因为通配符只能处理多个子域名，而不能处理不同的域。将每个附加域的主题替代名称（SAN）添加到证书中是不正确的，因为尽管使用 SAN 是正确的，但每次添加新域时，您仍必须重新验证并重新验证证书。该场景中的一个要求是您不需要重新验证和重新验证证书，因此，此解决方案是不正确的。

“创建一个新的 CloudFront web 分发，并将其配置为使用专用 IP 地址为 HTTPS 请求提供服务，以便将您的备用域名与每个 CloudFront 边缘位置的专用 IP 地址相关联”的选项是不正确的，因为尽管使用专用 IP 地址来满足此要求是有效的，但此解决方案不具有成本效益。请记住，如果您将 CloudFront 配置为使用专用 IP 地址服务 HTTPS 请求，则会产生额外的每月费用。当您为 SSL/TLS 证书与 CloudFront 发行版关联时，收费开始。您可以简单地将证书上传到 ALB，并使用 SNI 以经济高效的方式处理多个域。

参考文献：

<https://aws.amazon.com/blogs/aws/new-application-load-balancer-sni/>

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/cnames-https-dedicated-ip-or-sni.html#cnames https 专用 ip>

<https://docs.aws.amazon.com/elasticloadbalancing/latest/application/create-https-listener.html> 查看此 Amazon CloudFront 备忘单：

<https://tutorialsdojo.com/amazon-cloudfront/SNI>

自定义 SSL vs 专用 IP 自定义 SSL：

<https://tutorialsdojo.com/sni-custom-ssl-vs-dedicated-ip-custom-ssl/AWS> 服务备忘单比较：

<https://tutorialsdojo.com/comparison-of-aws-services/>

Q211.重新设计了一个新的在线银行平台，使其具有微服务架构，其中复杂的应用程序被分解为更小的独立服务。新平台正在使用 Docker，因为应用程序容器最适合运行小型的、解耦的服务。新的解决方案应消除配置和管理服务器的需要，允许您为每个应用程序指定和支付资源，并通过设计应用程序隔离来提高安全性。以下哪项服务最适合用于将此新平台迁移到 AWS？

- A、亚马逊 EBS
- B、亚马逊 EFS
- C、亚马逊 EKS
- D、AWS Fargate

答案 D

分析：

AWS Fargate 是一个用于容器的无服务器计算引擎，可与 Amazon 弹性容器服务（ECS）和 Amazon 弹性 Kubernetes 服务（EKS）一起使用。Fargate 使您轻松专注于构建应用程序。Fargate 消除了配置和管理服务器的需要，允许您为每个应用程序指定和支付资源，并通过设计应用程序隔离来提高安全性。Fargate 分配了正确的计算量，无需选择实例和扩展集群容量。您只需支付运行容器所需的资源，因此不会过度配置和支付额外的服务器。Fargate 在自己的内核中运行每个任务或 pod，为任务和 pod 提供自己的独立计算环境。这使您的应用程序能够通过设计实现工作负载隔离和提高安全性。这就是为什么 Vanguard、Accenture、Foursquare 和 Ancestry 等客户选择在 Fargate 上运行其关键任务应用程序的原因。

因此，正确答案是：AWS Fargate。

Amazon EKS 是不正确的，因为它更适合运行 Kubernetes 管理基础设施，而不是 Docker。与 AWS Fargate 不同，它不需要提供和管理服务器，也不允许您为每个应用程序指定和支付资源。

AmazonEFS 是不正确的，因为它是一个用于基于 Linux 的工作负载的文件系统，用于 AWS 云服务和内部资源。

Amazon EBS 是不正确的，因为它主要用于提供与 AWS 云中的 Amazon EC2 实例一起使用的持久块存储卷。

参考文献：

<https://aws.amazon.com/fargate/>

https://docs.aws.amazon.com/AmazonECS/latest/developerguide/ECS_GetStarted_Fargate.html 查看此亚马逊 ECS 备忘单：<https://tutorialsdojo.com/amazon-elastic-container-service-amazon-ecs/>

Q212.一家公司建立了从其内部数据中心到 AWS 云的专用网络连接

使用 AWS 直接连接（DX）。核心网络服务，如域名系统（DNS）服务和 Active Directory 服务，都在本地托管。该公司拥有新的 AWS 账户，这些账户也将需要对这些网络服务的一致和专用访问。以下哪项可以以最低的运营开销和成本效益的方式满足这一要求？

- A、 创建新的 AWS VPN CloudHub。为其他 AWS accounts 设置虚拟专用网络（VPN）连接。
- B、 设置新的直连网关并将其与现有直连连接集成。在 AWS 帐户之间配置 VPC peering 连接，并将其与直接连接网关关联。
- C、 为将添加的每个新 AWS 帐户设置另一个直接连接。
- D、 创建新的直连网关，并将其与现有的直连连接集成。在 AWS 帐户之间设置 Transit Gateway，并将其与直接连接网关关联。

答案 D

分析：

AWS Transit Gateway 提供了连接 VPC 和内部网络的中心辐射式设计。您可以将所有混合连接（VPN 和直接连接）连接到一个单一的传输网关，在一个地方整合和控制您组织的整个 AWS 路由配置。它还控制如何使用路

由表在所有连接的分支网络之间路由流量。这种中心辐射模型简化了管理并降低了运营成本，因为 VPC 仅连接到传输网关以访问连接的网络。

通过使用转接虚拟接口将转接网关连接到直接连接网关，您可以管理同一 AWS 区域中多个 VPC 或 VPN 的单个连接。您还可以将前缀从本地发布到 AWS，以及从 AWS 发布到本地。AWS Transit Gateway 和 AWS Direct Connect 解决方案简化了亚马逊专有网络和您的网络之间通过专用连接的管理。它还可以最小化网络成本，提高带宽吞吐量，并提供比基于互联网的连接更可靠的网络体验。

因此，正确的答案是：创建一个新的直接连接网关，并将其与现有的直接连接集成。在 AWS 帐户之间设置传输网关，并将其与直接连接网关关联。

“为将要添加的每个新 AWS 帐户设置另一个直接连接”选项是不正确的，因为该解决方案需要大量额外成本。建立单个 DX 连接需要大量预算，并且需要花费大量时间。它还具有较高的管理开销，因为您需要管理所有 AWS 帐户的所有直接连接。

选项显示：创建一个新的 AWS VPN CloudHub。为其他 AWS 帐户设置虚拟专用网络（VPN）连接是不正确的，因为 VPN 连接无法提供对本地网络服务的一致和专用访问。请注意，VPN 连接穿越公共互联网，不使用专用连接。选项显示：设置新的直接连接网关，并将其与现有的直接连接集成。在 AWS 帐户之间配置 VPC 对等连接并将其与直接连接网关关联是不正确的，因为直接连接中不支持 VPC 对等。VPC 对等不支持可传递对等关系。参考文献：

<https://docs.aws.amazon.com/directconnect/latest/UserGuide/direct-connect-transit-gateways.html>
<https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connect-options/aws-direct-connect-aws-transit-gateway.html>

<https://aws.amazon.com/blogs/networking-and-content-delivery/integrating-sub-1-gbps-hosted-aws-transit-gateways/>

查看 AWS 过境网关备忘单：<https://tutorialsdojo.com/aws-transit-gateway/>

213. 一家公司将其财务报告和监管文件存储在亚马逊 S3 存储桶中。为了遵守 IT 审计，他们委托解决方案架构师跟踪添加到 bucket 中的所有新对象以及删除的对象。它还应该跟踪版本化对象是否被永久删除。架构师必须将 Amazon S3 配置为将这些事件的通知发布到队列中进行后处理，并发布到 Amazon SNS 主题中，该主题将通知运营团队。

以下哪项是架构师应该实现的最合适的解决方案？

- A、创建新的 Amazon SNS 主题和 Amazon SQS 队列。在 Bucket 上添加 S3 事件通知配置，以将 S3:ObjectCreated:* 和 ObjectRemoved:DeleteMarkerCreated 事件类型发布到 SQS 和 SNS。
- B、创建新的 Amazon SNS 主题和 Amazon MQ。在存储桶上添加 S3 事件通知配置，以将 S3:ObjectCreated:* 和 ObjectRemoved:DeleteMarkerCreated 事件类型发布到 SQS 和 SNS。
- C、创建新的 Amazon SNS 主题和 Amazon MQ。在 bucket 上添加 S3 事件通知配置，将 S3:ObjectAdded:* 和 S3:Object Removed:* 事件类型发布到 SQS 和 SNS。
- D、创建新的 Amazon SNS 主题和 Amazon SQS 队列。在 bucket 上添加 S3 事件通知配置，发布 S3:ObjectCreated:* 和 S3:ObjectRemoved:Delete 事件类型到 SQS 和 SNS。

答案 D

分析：

Amazon S3 通知功能允许您在 bucket 中发生某些事件时接收通知。要启用通知，您必须首先添加一个通知配置，以标识您希望 Amazon S3 发布的事件以及您希望 Amazon S3 发送通知的目的地。将此配置存储在与 bucket 关联的通知子资源中。Amazon S3 为您提供了一个 API 来管理此子资源。Amazon S3 事件通知通常在几秒钟内发送事件，但有时可能需要一分钟或更长时间。如果同时对单个非版本对象进行两次写入，则可能只发送一个事件通知。如果您希望确保每次成功写入都会发送事件通知，则可以在 bucket 上启用版本控制。使用版本控制，每次成功写入都将创建对象的新版本，并发送事件通知。

Amazon S3 可以发布以下事件的通知：

1. 创建事件的新对象
2. 对象移除事件
3. 还原对象事件
4. 减少冗余存储（RRS）对象丢失事件
5. 复制事件

Amazon S3 支持以下可以发布事件的目的地：

1. 亚马逊简单通知服务（Amazon SNS）主题
2. Amazon 简单队列服务（Amazon SQS）队列
3. AWS Lambda

如果通知最终写入触发通知的 bucket，这可能会导致执行循环。例如，如果 bucket 在每次上载对象时触发 Lambda 函数，并且该函数将对象上载到 bucket，则该函数会间接触发自身。要避免这种情况，请使用两个 bucket，或者将触发器配置为仅应用于用于传入对象的前缀。因此，正确答案是：创建一个新的 Amazon SNS 主题和 Amazon SQS 队列。在 bucket 上添加 S3 事件通知配置，以将 S3:ObjectCreated:* 和 S3:ObjectRemoved:Delete 事件类型发布到 SQS 和 SNS。

该选项表示：创建新的 Amazon SNS 主题和 Amazon MQ。在 bucket 上添加 S3 事件通知配置，以发布 S3:ObjectAdded:* 和 S3:Object Removed:* 事件类型到 SQS 和 SNS 不正确。Amazon s3 中没有 s3:ObjectAdded:* 类型。您应该在 bucket 中添加 s3 事件通知配置，以发布 s3:Object 创建的：* 类型的事件。此外，Amazon S3 支持将 Amazon MQ 作为发布事件的目的地。该选项表示：创建一个新的 Amazon SNS 主题和 Amazon SQS 队列。在 bucket 上添加 S3 事件通知配置，以将 S3:ObjectCreated:* 和 ObjectRemoved:DeleteMarkerCreated 事件类型发布到 SQS 和 SNS 是不正确的，因为

s3:ObjectRemoved:DeleteMarkerCreated 类型仅在为版本化对象创建删除标记时触发，而不是在删除对象或永久删除版本化对象时触发。该选项表示：创建新的 Amazon SNS 主题和 Amazon MQ。在存储桶上添加 S3 事件通知配置，以将 S3:ObjectCreated:* 和 ObjectRemoved:DeleteMarkerCreated 事件类型发布到 SQS 和 SNS 是不正确的，因为 Amazon S3 向 Amazon MQ 提供公共事件消息。您应该使用 Amazon SQS。此外

s3:ObjectRemoved:DeleteMarkerCreated 类型仅在为版本化对象创建删除标记时触发。请记住，当对象被删除或版本化对象被永久删除时，场景要求发布事件。参考文献：

<https://docs.aws.amazon.com/AmazonS3/latest/dev/NotificationHowTo.html>
<https://docs.aws.amazon.com/AmazonS3/latest/dev/ways-to-add-notification-config-to-bucket.html>
<https://aws.amazon.com/blogs/aws/s3-event-notification/>

查看此 Amazon S3 备忘单：<https://tutorialsdojo.com/amazon-s3/>

亚马逊 SNS 概述：

<https://www.youtube.com/watch?v=ft5R45IEUJ8>

Q214.一家数据分析公司正在建立一家创新的免结账杂货店。他们的解决方案架构师开发了一个实时监控应用程序，使用智能传感器收集顾客从杂货店冰箱和货架上获得的物品，然后自动从他们的账户中扣除。该公司希望分析经常购买的物品，并将结果存储在 S3 中，以便持久存储，以确定其客户的购买行为。必须使用什么服务来轻松捕获、转换和加载流数据到 Amazon S3、Amazon Elasticsearch 服务和 Splunk？

- A、 亚马逊 Kinesis 数据消防软管
- B、 亚马逊红移
- C、 亚马逊运动
- D、 亚马逊 SQS

答：

分析：

Amazon Kinesis Data Firehose 是将流数据加载到数据存储和分析工具的最简单方法。

它可以捕获、转换流数据并将其加载到 Amazon S3、Amazon Redshift、Amazon Elasticsearch 服务和 Splunk 中，使用您目前已经使用的现有商业智能工具和仪表板实现近实时分析。

它是一个完全受管理的服务，可以自动扩展以匹配数据吞吐量，不需要进行持续管理。它还可以在加载数据之前对数据进行批处理、压缩和加密，从而最大限度地减少目标使用的存储量并提高安全性。在下图中，您从智能冰箱收集数据，并使用 Kinesis data firehouse 准备和加载数据。S3 将被用作一种持久存储用于分析的数据的方法，并最终使用分析工具获取用于输出的数据。如果您需要实现流式大数据的实时处理，您可以将 Amazon Kinesis 数据 Firehose 与 Amazon Kinesis 数据流结合使用。Kinesis 数据流提供了记录排序，以及以相同顺序读取和/或重放记录到多个 Amazon Kinesis 应用程序的能力。Amazon Kinesis 客户端库（KCL）将给定分区密钥的所有记录交付给同一记录处理器，从而更容易构建从同一 Amazon Kinesis 数据流读取的多个应用程序（例如，执行计数、聚合和过滤）。亚马逊简单队列服务（Amazon SQS）不同于亚马逊 Kinesis 数据消防软管。SQS 提供了一个可靠、高度可扩展的托管队列，用于存储在计算机之间传输的消息。Amazon SQS 让您可以轻松地在分布式应用程序组件之间移动数据，并帮助您构建独立处理消息的应用程序（具有消息级 ack/fail 语义），如自动化工作流。Amazon Kinesis Data Firehose 主要用于将流数据加载到数据存储和分析工具中。

因此，正确答案是：亚马逊 Kinesis 数据消防软管。亚马逊 Kinesis 是不正确的，因为这是 AWS 的流式数据平台，在其下有四种不同的服务：Kinesis 数据消防软管、Kinesis 流、Kinesis 视频流和亚马逊 Kinesis 数据分析。对于场景中要求的特定用例，请使用 Kinesis 数据消防软管。Amazon Redshift 是不正确的，因为它主要用于数据仓库，使得在数据仓库和数据湖中分析数据变得简单和经济高效。它不符合

能够将数据加载和流式传输到数据存储中进行分析。您必须改用 Kinesis 数据消防软管。

Amazon SQS 是不正确的，因为您无法使用此服务捕获、转换和加载流数据到 Amazon S3、Amazon Elasticsearch 服务和 Splunk。您必须改用 Kinesis 数据消防软管。

Q215.一家公司正在使用亚马逊专有网络，其 CIDR 块为 31.0.0/27<，连接到内部数据中心。需要创建一个 Lambda 函数，该函数将每分钟处理大量加密货币交易，然后将结果存储到 EFS。在设置无服务器架构并将 Lambda 函数连接到 VPC 之后，解决方案架构师注意到在一天中的某些时间，EC2 错误类型（如 EC2RottleDexception）的调用错误增加。

以下哪项是导致此问题的可能原因？（选择两个。）

- A、在 Lambda 函数配置中只指定了一个子网。该子网的可用 IP 地址不足，并且没有其他子网或可用区域可以处理峰值负载。
- B、您功能的附加 IAM 执行角色没有访问 VPC 资源的必要权限。
- C、函数的关联安全组不允许出站连接。
- D、您的 VPC 没有足够的子网 ENI 或子网 IP。
- E、E.您的 VPC 没有 NAT 网关。

回答广告

分析：

您可以配置一个功能以连接到您帐户中的虚拟私有云（VPC）。使用 Amazon 虚拟专用云（Amazon VPC）为数据库、缓存实例或内部服务等资源创建专用网络。将您的功能连接到专有网络，以便在执行期间访问私有资源。

默认情况下，AWS Lambda 在 VPC 中安全运行函数代码。但是，要使 Lambda 功能能够访问专用 VPC 内的资源，您必须提供额外的 VPC 特定配置信息，包括 VPC 子网 ID 和安全组 ID。AWS Lambda 使用此信息设置弹性网络接口（ENI），使您的功能能够安全连接到专用 VPC 内的其他资源。

Lambda 函数无法直接连接到具有专用实例租赁的 VPC。要连接到专用 VPC 中的资源，请将其对等到具有默认租约的第二个 VPC。您的 Lambda 函数会根据其处理的事件数量自动缩放。如果您的 Lambda 功能访问专有网络，您必须确保您的专有网络具有足够的 ENI 容量，以支持 Lambda 函数的规模要求。还建议您在 Lambda 功能配置中的每个可用性区域中至少指定一个子网。通过在每个可用性区域中指定子网，如果一个可用性区域出现故障或 IP 地址不足，则 Lambda 函数可以在另一个可用区域中运行。如果您的 VPC 没有足够的 ENI 或子网 IP，您的 Lambda 功能将不会随着请求的增加而扩展，您将看到

EC2 错误类型的调用错误，如 EC2RottleDexception。对于异步调用，如果在没有相应的 CloudWatch 日志的情况下看到错误增加，则在控制台中同步调用 Lambda 函数以获得错误响应。

因此，这种情况的正确答案是：

- 在 Lambda 函数配置中只指定了一个子网。单个子网的可用 IP 地址不足，并且没有其他子网或可用区域可以处理峰值负载。
- 您的 VPC 没有足够的子网 ENI 或子网 IP。“您的 VPC 没有 NAT 网关”选项不正确，因为 NAT 网关中的问题不太可能导致请求节流问题或在 Lambda 中产生 EC2ThrottledException 错误。根据场景，问题只在一天中的

某些时间发生，这意味着问题只是间歇性的，功能在其他时间工作。我们还可以得出结论，可用性不是问题，因为应用程序已经在使用高可用性 NAT 网关，而不仅仅是 NAT 实例。

“函数的关联安全组不允许出站连接”选项是不正确的，因为如果关联的安全组不支持出站连接，则 Lambda 函数将根本无法工作。请记住，根据场景，问题只会间歇性发生。此外，互联网流量限制通常不会产生 EC2 RottleDexception 错误。该选项表示：您的功能的附加 IAM 执行角色没有访问 VPC 资源的必要权限，这是不正确的，因为正如上文所解释的，该问题是间歇性的，因此，该功能的 IAM 执行任务确实具有访问 VPC 的资源所需的权限，因为它在这些特定时间工作。如果问题确实引起

如果出现权限问题，则很可能返回 EC2AccessDeniedException 错误，而不是 EC2RottleDexception 错误。

参考文献：

<https://docs.aws.amazon.com/lambda/latest/dg/vpc.html>

<https://aws.amazon.com/premiumsupport/knowledge-center/internet-access-lambda-function/>
亚马逊。com/premiumsupport/knowledge-center/lambda-trouble-invoke-error-502-500/查看此 AWS lambda 备忘单：
<https://tutorialsdojo.com/aws-lambda/>

Q216.一家科技初创公司正在推出一个基于亚马逊 ECS 集群的按需食品配送平台，该集群具有 AWS Fargate 无服务器计算引擎和亚马逊极光。预计未来几周，数据库读取查询将显著增加。一位解决方案架构师最近向数据库集群发布了两个读取副本，以提高平台的可伸缩性。以下哪一项是架构师应该实现的最合适的配置，以将所有传入的读取请求平均地负载平衡到两个读取副本？

- A、使用亚马逊极光数据库的内置阅读器端点。
- B、启用 Amazon Aurora 并行查询。
- C、创建一个新的网络负载均衡器，将读取查询均匀分布到 AmazonAurora 数据库的读取副本。
- D、使用 Amazon Aurora 数据库的内置集群端点。

答：

分析：

Amazon Aurora 通常涉及一个数据库实例集群，而不是单个实例。每个连接都由特定的 DB 实例处理。连接到 Aurora 集群时，指定的主机名和端口指向称为端点的中间处理程序。Aurora 使用端点机制来抽象这些连接。因此，当某些 DB 实例不可用时，您不必硬编码所有主机名，也不必编写自己的负载平衡和重新路由连接逻辑。对于某些 Aurora 任务，不同的实例或实例组执行不同的角色。例如，主实例处理所有数据定义语言（DDL）和数据操作语言（DML）语句。多达 15 个 Aurora 副本处理只读查询流量。使用端点，您可以根据您的用例将每个连接映射到适当的实例或实例组。例如，要执行 DDL 语句，可以连接到主实例。要执行查询，您可以连接到读卡器端点，Aurora 会自动在所有 Aurora 副本之间执行负载平衡。对于具有不同容量或配置的数据库实例的集群，可以连接到与数据库实例的不同子集关联的自定义端点。对于诊断或调优，您可以连接到特定实例端点，以检查特定 DB 实例的详细信息。Aurora DB 集群的读卡器端点为数据库集群的只读连接提供负载平衡支持。将读取器端点用于读取操作，如查询。通过在只读 Aurora 副本上处理这些语句，该端点减少了主实例的开销。它还可以帮助集群根据集群中的 Aurora 副本数量按比例扩展处理同时选择查询的容量。每个 Aurora DB 集群都有一个读卡器端点。如果集群包含一个或多个 Aurora 副本，则读取器端点将在 Aurora 复制副本之间平衡每个连接请求。在这种情况下，只能在该会话中执行诸如 SELECT 之类的只读语句。如果集群只包含一个主实例，而没有 Aurora 副本，则读取器端点连接到主实例。在这种情况下，您可以通过端点执行写操作。

因此，正确的答案是使用亚马逊极光数据库的内置阅读器端点。“使用 Amazon Aurora 数据库的内置集群端点”选项不正确，因为集群端点（也称为编写器端点）仅连接到该数据库集群的当前主数据库实例。此端点可以在数据库中执行写操作，如 DDL 语句，这非常适合处理生产流量，但不适合处理用于报告的查询，因为不会发送写数据库操作。“启用 Amazon Aurora 并行查询”选项是不正确的，因为该功能仅允许 Amazon Aurora 在 Aurora 存储层的数千个 CPU 上下推并分配单个查询的计算负载。请注意，它不会将所有传入读取请求的负载均衡到两个读取副本。使用并行查询，查询处理被下推到 Aurora 存储层。查询获得了大量计算能力，并且需要通过网络传输的数据要少得多。同时，Aurora 数据库实例可以继续为事务提供服务

中断更少。这样，您可以在同一个 Aurora 数据库中同时运行事务性和分析性工作负载，同时保持高性能。“创建一个新的网络负载均衡器，将读取查询均匀分布到 Amazon Aurora 数据库的读取副本”选项是不正确的，因为网络负载均衡器不适合用于此要求，因为 NLB 主要用于将流量分配到服务器，而不是读取副本。您必须使用 Amazon Aurora 数据库的内置阅读器端点。

参考文献：

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Overview.Endpoints.html>
<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Overview.html><https://aws.amazon.com/rds/aurora/parallel-query/>

亚马逊极光概述：

<https://youtu.be/iwS1h7rLNBQ>

查看此亚马逊极光备忘单：<https://tutorialsdojo.com/amazon-aurora/Q217>。一家公

司正在使用多个 AWS 账户，这些账户使用 AWS 组织合并。他们希望将多个

S3 对象复制到另一个 S3 bucket 中，该 S3 buck 属于他们自己拥有的另一个

AWS 帐户。已指示解决方案架构师为此任务设置必要的权限，并确保目标帐

户拥有复制的对象，而不是发送对象的帐户。架构师如何实现这一需求？

A、在 S3 中，通过创建一个 bucket 策略来设置跨源资源共享（CORS），该策略允许 IAM 用户或角色将对象从一个帐户中的源 bucket 复制到另一帐户中的目标 bucket。

B、在源 S3 bucket 中启用请求者付费功能。由于两个 AWS 账户都是 AWS 组织的一部分，因此可通过合并账单免除费用。

C、在 S3 中，通过创建 IAM 客户管理策略来配置跨帐户权限，该策略允许 IAM 用户或角色将对象从一个帐户中的源存储桶复制到另一帐户中的目标存储桶。然后将策略附加到要用于在帐户之间复制对象的 IAM 用户或角色。

D、将来自两个不同 AWS 帐户的两个 S3 存储桶连接到 Amazon WorkDocs。设置跨帐户访问以集成两个 S3 存储桶。使用 Amazon WorkDocs 控制台将对象从一个帐户复制到另一个帐户，并将修改后的对象所有权分配给目标帐户。

答案 C

分析：

默认情况下，S3 对象由上传该对象的帐户拥有。这就是为什么授予目标帐户执行跨帐户复制的权限可以确保目标拥有复制的对象。您还可以通过将对象的访问控制列表（ACL）更改为 bucket owner 完全控制来更改对象的所有权。

但是，对于多个对象，对象 ACL 可能很难管理，因此最好将编程跨帐户权限授予目标帐户。对象所有权对于使用 bucket 策略管理权限非常重要。要使 bucket 策略应用于 bucket 中的对象，该对象必须由拥有该 bucket 的帐户拥有。还可以使用对象的 ACL 管理对象权限。但是，对于多个对象，对象 ACL 可能很难管理，因此最好使用 bucket 策略作为设置权限的集中方法。要确保目标帐户拥有从其他帐户复制的 S3 对象，请授予目标帐户执行跨帐户复制的权限。按照以下步骤配置跨帐户权限，将对象从帐户 a 中的源存储桶复制到帐户 B 中的目标存储桶：

- 将存储桶策略附加到帐户 a 中的源存储桶。
- 将 AWS 身份和访问管理（IAM）策略附加到帐户 B 中的用户或角色。
- 使用帐户 B 中的 IAM 用户或角色执行跨帐户复制。因此，正确答案是：

在 S3 中，通过创建 IAM 客户管理策略来配置跨帐户权限，该策略允许 IAM 用户或角色将对象从一个帐户中的源存储桶复制到另一帐户中的目标存储桶。然后将策略附加到要用于在帐户之间复制对象的 IAM 用户或角色。

该选项表示：在源 S3 bucket 中启用请求者付费功能。由于两个 AWS 账户都是 AWS 组织的一部分，因此可以通过合并账单免除费用。这是不正确的，因为如果您希望请求者而不是存储桶所有者支付数据传输请求和从 S3 存储桶下载的费用，则主要使用请求者付费功能。此解决方案缺少满足要求所需的 IAM 权限。这里最合适的解决方案是在 S3 中配置跨帐户权限。

在 S3 中，通过创建允许 IAM 用户或角色将对象从一个帐户的源存储桶复制到另一个帐户中的目标存储桶的存储桶策略来设置跨源资源共享（CORS）的选项是不正确的，因为 CORS 只是定义了一种方式，用于加载在一个域中的客户端 web 应用程序与不同域中的资源交互，而不是在不同的 AWS 帐户上。该选项表示：将两个不同 AWS 帐户的两个 S3 存储桶连接到 Amazon WorkDocs。设置跨帐户访问以集成两个 S3 存储桶。使用 Amazon WorkDocs 控制台将对象从一个帐户复制到另一个帐户，将修改后的对象所有权分配给目标帐户是不正确的，因为 Amazon WorkDocs 通常用于轻松协作、共享内容、提供丰富的反馈，以及与其他用户协作编辑文档。您无法直接将 WorkDocs 与不同 AWS 帐户拥有的 Amazon S3 bucket 集成。更好的解决方案是在 S3 中使用跨帐户权限来满足要求。参考文献：

<https://docs.aws.amazon.com/AmazonS3/latest/dev/example-walkthroughs-managing-access-example2.html>

[https://aws.amazon.com/premiumsupport/knowledge-center/copy-s3-objects-](https://aws.amazon.com/premiumsupport/knowledge-center/copy-s3-objects-account/)

[account/https://aws.amazon.com/premiumsupport/knowledge-center/cross-account-access-s3/](https://aws.amazon.com/premiumsupport/knowledge-center/cross-account-access-s3/)查看此 Amazon s3 备忘单：<https://tutorialsdojo.com/amazon-s3/>

Q218.一个文档共享网站正在使用 AWS 作为其云基础设施。免费用户可以上传总共 5 GB 的数据，而高级用户可以上传多达 5 TB 的数据。他们的应用程序将用户文件上传到 S3 存储桶，最大文件大小为 1 TB。

在这种情况下，应用程序在 S3 中上传大文件的最佳方式是什么？

A、使用多部分上传

- B、使用单个 PUT 请求上载大文件
- C、使用 AWS 导入/导出
- D、使用 AWS 滚雪球

答:

分析:

您可以存储的数据总量和对象数量是无限的。单个 AmazonS3 对象的大小可以从最小 0 字节到最大 5 TB 不等。在一次放置中可以上载的最大对象是 5 千兆字节。对于大于 100 兆字节的对象，客户应考虑使用多部分上传功能。

多部分上传 API 使您能够部分上传大型对象。您可以使用此 API 上载新的大型对象或复制现有对象。多部分上传是一个三步过程：启动上传，上传对象部分，上传所有部分后，完成多部分上传。收到完整的多部分上传请求后，Amazon S3 从上传的部分构建对象，然后您可以像访问 bucket 中的任何其他对象一样访问该对象。

使用单个 PUT 请求上载大文件是不正确的，因为使用单个 PUT 请求可以上载的最大文件大小为 5 GB。大于此值的文件将无法上载。使用 AWS Snowball 是不正确的，因为这是一种迁移工具，可以将大量数据从本地数据中心传输到 AWS S3，反之亦然。此工具不适用于给定场景。当您提供雪球时，设备会被运送给您，而不是您的客户。因此，您有责任保护设备。使用 AWS 导入/导出是不正确的，因为导入/导出类似于 AWS 雪球，其目的是用作迁移工具，而不是用于多客户消费，如给定场景中。

参考文献:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/mpuoverview.html> <https://aws.amazon.com/s3/faqs/> 查看此

Amazon S3 备忘单: <https://tutorialsdojo.com/amazon-s3/>

Q219.一位解决方案架构师正在为一家需要向 Amazon S3 传输 50 TB 本地数据的初创公司制定战略。该初创公司的数据中心和 AWS 之间的网络传输速度较慢，这导致了数据迁移的瓶颈。

解决方案架构师应该实现以下哪项？

- A、将 AWS 存储网关文件网关与内部数据中心集成。
- B、使用 AWS 雪球控制台中的雪球设备向 Amazon S3 请求导入作业。
- C、在目标 S3 存储桶上启用 Amazon S3 传输加速。
- D、在本地数据中心部署 AWS 迁移中心发现代理。

答案 B

分析:

AWS Snowball 使用安全、坚固的设备，因此您可以将 AWS 计算和存储功能带到您的边缘环境中，并将数据传输到 AWS 或从 AWS 传输出去。该服务为您提供雪球般的边缘设备，包括存储和可选的 Amazon EC2 和 AWS 物联网 Greengrass 计算，可运输、加固，

安全案例。通过 AWS Snowball，您可以将机器学习、数据分析、处理和存储的云功能带到您的边缘，用于迁移、短期数据收集甚至长期部署。AWS Snowball 设备可以使用或不使用互联网，不需要专门的 IT 操作员，设计用于远程环境。因此，正确的答案是：使用 AWS 雪球控制台中的雪球设备向 Amazon S3 请求导入作业。“在本地数据中心部署 AWS 迁移中心发现代理”选项不正确。AWS 迁移中心服务只是一个中心服务，它提供了一个位置来跟踪跨多个 AWS 和合作伙伴解决方案的应用程序迁移进度。该选项表示：

在目标 S3 存储桶上启用 Amazon S3 传输加速不正确，因为此 S3 功能不适合大规模数据迁移。启用此功能并不总是能保证更快的数据传输，因为它只适用于与 Amazon S3 存储桶之间的远程传输。“将 AWS 存储网关文件网关与本地数据中心集成”的选项是不正确的，因为该服务主要用于构建混合云解决方案，您仍然需要本地访问无限的云存储。根据该场景，此服务不是最佳选项，因为您仍将依赖现有的低带宽 internet 连接。参考文献：

<https://aws.amazon.com/snowball> <https://aws.amazon.com/blogs/storage/making-it-even-simpler-to-create-and-manage-your-aws-snow-家庭工作/>

查看 AWS 雪球备忘单：

<https://tutorialsdojo.com/aws-snowball/>

AWS Snow 系列概述：

<https://www.youtube.com/watch?v=9Ar-51Ip53Q>

Q220.一家全球在线体育博彩公司在 AWS 中托管了其受欢迎的 web 应用程序。他们正计划为他们的企业开发一个新的在线门户，他们聘请您为一个新在线门户实施云架构，该门户将接受全球体育投注。您开始使用在单个 EC2 实例上运行的关系数据库来设计系统，该实例需要一个 EBS 卷，可以支持高达 30000 IOPS。

在此场景中，您可以使用哪种 Amazon EBS 卷类型来满足此新在线门户的性能要求？

- A、EBS 通用 SSD (gp2)
- B、EBS 冷硬盘 (sc1)
- C、EBS 配置 IOPS SSD (io1)
- D、EBS 吞吐量优化硬盘 (st1)

答案 C

分析：

该场景需要具有高 IOPS 性能的关系数据库的存储类型。对于这些场景，SSD 卷比 HDD 卷更适合使用。请记住，SSD 的主要性能属性是 IOPS，而 HDD 是吞吐量。在检查中，始终考虑 SSD 和 HDD 之间的差异，如下表所示。这将允许您轻松消除选项中非 SSD 或非 HDD 的特定 EBS 类型，具体取决于问题要求的存储类型是具有小的随机 I/O 操作还是大的顺序 I/O。

由于要求为 30000 IOPS，因此必须使用 EBS 类型的配置 IOPS SSD。这为任务关键型低延迟工作负载提供了持续的性能。因此，EBS 提供的 IOPS SSD (io1) 是正确答案。

EBS 吞吐量优化 HDD (st1) 和 EBS 冷 HDD (sc1) 是不正确的，因为它们是更适合大型流式工作负载而不是事务数据库工作负载的 HDD 卷。

EBS 通用 SSD (gp2) 是不正确的，因为尽管通用 SSD 卷可用于此场景，但与配置的 IOPS SSD 卷不同，它不提供应用程序所需的高 IOPS。

参考：

<https://aws.amazon.com/ebs/details/>

亚马逊 EBS 概述-SSD 与 HDD：

<https://www.youtube.com/watch?v=LW7x8wyLFvw>

查看此亚马逊 EBS 备忘单：<https://tutorialsdojo.com/amazon-ebs/>

Q221.公司需要使用 Amazon Aurora 作为其 web 应用程序的 Amazon RDS 数据库引擎。

已指示解决方案架构师实施 90 天备份保留策略。以下哪个选项可以满足给定要求？

- A、 配置自动备份并将备份保留期设置为 90 天。
- B、 使用 CloudWatch 事件和 AWS Lambda 创建每日计划事件，以将 RDS automated 快照直接下载到 S3 存储桶。将超过 90 天的快照存档到 Glacier。
- C、 将 RDS 配置为自动将自动快照导出到 Amazon S3，并创建生命周期策略以在 90 天后删除对象。
- D、 创建一个 AWS 备份计划，每天拍摄快照，保留期为 90 天。

答案 D

分析：

AWS 备份是一种集中式备份服务，它使您可以在 AWS 云中跨 AWS 服务轻松且经济高效地备份应用程序数据，帮助您满足业务和法规备份合规性要求。AWS 备份提供了一个中心位置，您可以在这里配置和审核要备份的 AWS 资源，自动化备份计划，设置保留策略，并监控所有最近的备份和恢复活动，从而简化了对 AWS 存储卷、数据库和文件系统的保护。

在这种情况下，您可以使用 AWS 备份创建保留期为 90 天的备份计划。备份计划是定义何时以及如何备份 AWS 资源的策略表达式。将资源分配给备份计划，然后 AWS 备份会根据备份计划自动备份并保留这些资源的备份。

因此，正确的答案是：创建一个 AWS 备份计划，每天拍摄快照，保留期为 90 天。

“配置自动备份并将备份保留期设置为 90 天”选项不正确，因为自动备份的最大备份保留期仅为 35 天。“将 RDS 配置为自动将自动快照导出到 Amazon S3 并创建生命周期策略以在 90 天后删除对象”选项不正确，因为您无法将自动快照自动导出到 Amazon S3。您必须手动导出快照。该选项表示：

使用 CloudWatch 事件和 AWS Lambda 创建每日计划事件，将 RDS 自动快照直接下载到 S3 存储桶。将超过 90 天的快照存档到 Glacier 是不正确的，因为您无法直接将 RDS 中的自动快照下载或导出到 Amazon S3。您必须先复制自动快照，使其成为手动快照，然后才能将其移动到 Amazon S3 存储桶。对于这种情况，更好的解决方案是简单地使用 AWS 备份。参考文献：

<https://docs.aws.amazon.com/aws-backup/latest/devguide/create-a-scheduled-backup.html>
<https://aws.amazon.com/backup/faqs/> 查看这些 AWS 备忘单：
<https://tutorialsdojo.com/links-to-all-aws-cheat-sheets/>

Q222. 一家公司正在 AWS 上使用 CloudFormation 部署 Microsoft SharePoint Server 环境。这个解决方案架构师需要安装和配置由 Microsoft Active Directory 组成的体系结构 (AD) 域控制器、Microsoft SQL Server 2012、多个 Amazon EC2 实例来承载 Microsoft SharePoint Server 和许多其他依赖项。架构师需要确保

在继续创建堆栈之前，组件已正确运行。为了满足这一要求，架构师应该做以下哪项？

- A、在 CloudFormation 模板中配置 UpdateReplacePolicy 属性。使用 cfn 信号助手脚本安装和配置应用程序后发送成功信号。
- B、在 CloudFormation 模板中配置 DependsOn 属性。使用 cfn init helper 脚本安装和配置应用程序后发送成功信号。
- C、在 CloudFormation 模板中为实例配置 CreationPolicy 属性。使用 cfn 信号助手脚本安装和配置应用程序后发送成功信号。
- D、在 CloudFormation 模板中为实例配置 UpdatePolicy 属性。使用 cfn 信号助手脚本安装和配置应用程序后发送成功信号。

答案 C

分析：

您可以将 CreationPolicy 属性与资源关联，以防止其状态达到创建完成，直到 AWS CloudFormation 收到指定数量的成功信号或超过超时时间。要发出资源信号，可以使用 cfn 信号助手脚本或信号资源 API。AWS CloudFormation 将有效信号发布到堆栈事件，以便跟踪发送的信号数量。创建策略仅在 AWS CloudFormation 创建关联资源时调用。目前，支持创建策略的 AWS 云信息资源只有 AWS:: AutoScaling:: AutoScalingGroup、AWS:: EC2:: Instance 和 AWS:: CloudFormation:: WaitCondition。

如果希望在堆栈创建继续之前等待资源配置操作，请使用 CreationPolicy 属性。例如，如果在 EC2 实例上安装和配置软件应用程序，则可能希望在继续之前运行这些应用程序。在这种情况下，可以向实例添加 CreationPolicy 属性，然后在安装和配置应用程序后向实例发送成功信号。

因此，该选项表示：在 CloudFormation 模板中为实例配置 CreationPolicy 属性。在安装和配置应用程序后发送成功信号。使用 cfn 信号助手脚本是正确的。

该选项表示：在 CloudFormation 模板中配置 DependsOn 属性。在安装和配置应用程序后，使用 cfn init helper 脚本发送成功信号是不正确的，因为 cfn-init helper 脚本不适合用于向其他资源发送信号。您必须改用 cfn 信号。尽管您可以使用

DependsOn 属性以确保特定资源的创建遵循另一个资源的创建，最好使用 CreationPolicy 属性，因为它可以确保应用程序在堆栈创建之前正确运行。该选项表示：在 CloudFormation 模板中为实例配置 UpdatePolicy 属性。在安装和配置应用程序后使用 cfn 信号助手脚本发送成功信号是不正确的，因为 UpdatePolicy 属性主要用于更新资源和堆栈更新回滚操作。该选项表示：在 CloudFormation 模板中配置 UpdateReplacePolicy 属性。在安装和配置应用程序后使用 cfn 信号助手脚本发送成功信号是不正确的，因为 UpdateReplacePolicy 属性主要用于在堆栈更新操作期间替换资源时保留或在某些情况下备份资源的现有物理实例。

参考文献:

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-attribute-creationpolicy.html>

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/deploying.applications.html#deploy-门特穿行-cfn>

信号 <https://aws.amazon.com/blogs/devops/use-a-creationpolicy-to-wait-for-on-instance-configurations/> 查看此 AWS CloudFormation 备忘单: <https://tutorialsdojo.com/aws-cloudformation/>

AWS CloudFormation-模板、堆栈和变更集: <https://www.youtube.com/watch?v=9Xpuprxg7aY>

Q223. 公司需要每秒从网站和社交媒体源收集千兆字节的数据, 以获得对其产品的洞察, 并不断改善用户体验。为了满足这一设计要求, 您开发了一个应用程序, 该应用程序托管在 Spot EC2 实例的自动缩放组上, 该组处理数据并将结果存储到 DynamoDB 和 Redshift。解决方案应具有内置的增强扇出功能。

您可以使用哪一种完全管理的 AWS 服务来实时收集和处理大量数据记录流, 而管理开销最小?

- A、 亚马逊红移与 AWS 云开发套件 (AWS CDK)
- B、 针对 Apache Kafka 的 Amazon 托管流媒体 (Amazon MSK)
- C、 亚马逊 Kinesis 数据流
- D、 Amazon S3 接入点

答案 C

分析:

Amazon Kinesis 数据流用于实时收集和处理大量数据记录流。您可以使用 Kinesis 数据流快速、连续地获取和聚合数据。使用的数据类型包括 IT 基础设施日志数据、应用程序日志、社交媒体、市场数据源和网络点击流数据。由于数据获取和处理的响应时间是实时的, 因此处理通常是轻量级的。

下图说明了 Kinesis 数据流的高级架构。生产者不断将数据推送到 Kinesis 数据流, 消费者实时处理数据。

消费者

(例如在 Amazon EC2 上运行的自定义应用程序或 Amazon Kinesis Data Firehose 交付流) 可以使用 AWS 服务 (如 Amazon DynamoDB、Amazon Redshift 或 Amazon S3) 存储结果。

因此, 正确答案是: 亚马逊 Kinesis 数据流。AmazonS3 访问点是不正确的, 因为它主要用于管理 S3 对象的访问。AmazonS3 访问点是连接到 bucket 的命名网络端点, 您可以使用这些 bucket 执行 S3 对象操作, 例如上传和检索对象。Amazon Redshift with AWS Cloud Development Kit (AWS CDK) 是不正确的, 因为它主要用于数据仓库, 使得在数据仓库和数据湖中分析数据变得简单且经济高效。同样, 它不能满足实时收集和处理大量数据流的要求。将 AWS 云开发工具包 (AWS CDK) 与 Amazon Redshift 一起使用仍然不能满足这一要求。针对 Apache Kafka (Amazon MSK) 的 Amazon 托管流媒体不正确。虽然您可以使用 Amazon MSK 实时处理流数据, 但与 Amazon Kinesis 不同, 这项服务仍然需要大量的管理开销。此外, 它没有场景中所需的内置增强扇出功能。

参考文献: <https://docs.aws.amazon.com/streams/latest/dev/introduction.html>

<https://aws.amazon.com/kinesis/>

查看此亚马逊 Kinesis 备忘单: <https://tutorialsdojo.com/amazon-kinesis/>

Dojo 的 AWS 认证解决方案架构师助理考试学习指南教程: <https://tutorialsdojo.com/aws-certified-solutions-architect-associate/>

Q224. 一家公司计划使用按需 EC2 实例和 AWS 中的数据库构建 web 架构。然而, 由于预算限制, 该公司指示解决方案架构师选择一种数据库服务, 在这种服务中, 他们不再需要担心数据库管理任务, 如硬件或软件供应、设置、配置、扩展和备份。解决方案架构师应该推荐以下哪项服务?

- A、 亚马逊松紧带
- B、 亚马逊发电机 B
- C、 亚马逊 RDS
- D、 亚马逊红移

答案 B

分析:

基本上, 您不再需要担心数据库管理任务 (如硬件或软件配置、设置和配置) 的数据库服务称为完全管理数据库。这意味着 AWS 完全管理所有数据库管理任务和底层主机服务器。这里的主要区别在于问题中的关键词“缩放”。在 RDS 中, 您仍然需要手动扩展资源并创建读取副本以提高可伸缩性, 而在 DynamoDB 中, 这是自动完成的。

Amazon DynamoDB 是在这种情况下使用的最佳选项。它是一个完全管理的非关系数据库服务? 您只需创建一个数据库表, 设置自动扩展的目标利用率, 并让服务处理其余部分。您不再需要担心数据库管理任务, 如硬件或软件配置、设置和配置、软件修补、操作可靠的分布式数据库群集, 或在扩展时在多个实例上划分数据。DynamoDB 还允许您备份和恢复所有表以进行数据存档, 帮助您满足公司和政府的法规要求。

Amazon RDS 不正确, 因为这只是一个“托管”服务, 而不是“完全托管”。这意味着您仍然必须处理备份和其他管理任务, 例如何时将进行自动操作系统修补。

亚马逊 ElastiCache 不正确。尽管 ElastiCache 是完全管理的, 但它不是数据库服务, 而是内存中的数据存储。

亚马逊红移是不正确的。虽然这是完全管理的, 但它不是数据库服务, 而是数据仓库。

参考文献:

<https://aws.amazon.com/dynamodb/>

<https://aws.amazon.com/products/databases/>查看

此 Amazon DynamoDB 备忘单:

<https://tutorialsdojo.com/amazon-dynamodb/>

Q225. 一家科技公司目前正在为其 web 应用程序使用自动缩放。现在需要使用新的 AMI 来启动 EC2 实例组。需要进行以下哪些更改?

- A、创建新的目标组。
- B、什么也不做。您可以使用相同的启动配置直接启动自动缩放组中的 EC2 实例。
- C、创建新的启动配置。
- D、创建新的目标组并启动配置。

答案 C

分析：

启动配置是自动缩放组用于启动 EC2 实例的模板。创建启动配置时，可以为实例指定信息，例如 Amazon 机器映像（AMI）的 ID、实例类型、密钥对、一个或多个安全组以及块设备映射。如果您以前启动过 EC2 实例，则指定相同的信息以启动该实例。

您可以使用多个自动缩放组指定启动配置。但是，一次只能为自动缩放组指定一个启动配置，并且不能在创建启动配置后修改启动配置。因此，如果要更改自动缩放组的启动配置，则必须创建启动配置，然后使用新的启动配置更新自动缩放组。

对于这个场景，您必须创建一个新的启动配置。请记住，您不能在创建启动配置后修改它。

因此，正确的答案是：创建新的启动配置。选项是：什么都不做。您可以在自动缩放组中直接启动 EC2 实例，但启动配置不正确，因为您试图实现的是更改 EC2 实例组使用的 AMI。因此，您需要更改启动配置以更新实例正在使用的内容。选项“创建新目标组”和“创建新的目标组”以及“启动配置”都不正确，因为您只想更改实例使用的 AMI，而不是实例本身。目标组主要用于 ELB，而不是自动缩放。该场景没有提到架构具有负载均衡器。因此，您应该更新启动配置，而不是目标组。

参考文献：

<https://docs.aws.amazon.com/autoscaling/latest/userguide/LaunchConfiguration.html>
<https://docs.aws.amazon.com/autoscaling/ec2/userguide/autoscalinggroup.html> 查看此 AWS 自动缩放备忘单：

<https://tutorialsdojo.com/aws-auto-scaling/>

Q226.大型金融公司需要设置 Linux bastion 主机，以允许访问其 VPC 中运行的 Amazon EC2 实例。出于安全目的，只有从公司外部公共 IP 地址 175.45.116.100 连接的客户机才可以使用 SSH 访问主机。满足客户要求最佳选择是什么？

- A、安全组入站规则：协议？UDP，端口范围？22，来源 45.116.100/32
- B、安全组入站规则：协议？TCP。港口范围？22，来源 45.116.100/32
- C、网络 ACL 入站规则：协议？TCP，端口范围-22，源 45.116.100/0
- D、网络 ACL 入站规则：协议？UDP，端口范围？22，来源 45.116.100/32

答案 B

分析：

堡垒主机是网络上的专用计算机，专门设计并配置为抵御攻击。计算机通常托管单个应用程序，例如代理服务器，并且删除或限制所有其他服务以减少对计算机的威胁。在 AWS 中设置堡垒主机时，应只允许客户端的单

个 IP，而不允许整个网络。因此，在源代码中，应使用适当的 CIDR 符号。/32 表示一个 IP 地址，/0 表示整个网络。

表示：安全组入站规则：协议的选项？UDP，端口范围？22，源 175.45.116.100/32 不正确，因为 SSH 协议使用 TCP 和端口 22，而不是 UDP。表示：网络 ACL 入站规则：协议的选项？UDP，端口范围？22，源 175.45.116.100/32 不正确，因为 SSH 协议使用 TCP 和端口 22，而不是 UDP。除此之外，网络 ACL 充当整个 VPC 子网的防火墙，而安全组在实例级别上运行。由于您正在保护 EC2 实例，因此应该使用安全组。该选项表示：

网络 ACL 入站规则：协议？TCP，端口范围-22，Source 45.116.100/0 不正确，因为它允许整个网络而不是单个 IP 访问主机。

参考：

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-metadata.html> 查看此 Amazon EC2 备忘单：

<https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/>

Q227.解决方案架构师正在管理一家公司的 AWS 账户，该账户拥有大约 300 名 IAM 用户。他们有一项新的公司政策，要求更改所有 100 个 IAM 用户的相关权限，这些用户控制对 Amazon S3 存储桶的访问。

解决方案架构师将如何避免将策略应用于每个用户的耗时任务？

- A、创建新策略，并使用 shell 脚本将其应用于多个 IAM 用户。
- B、创建一个新的 S3 存储桶访问策略，每个 IAM 用户都可以无限访问。
- C、创建新的 IAM 角色并将每个用户添加到 IAM 角色。
- D、创建一个新的 IAM 组，然后添加需要访问 S3 存储桶的用户。

然后，将策略应用于 IAM 组。

答案 D

分析：

在这种情况下，最好的选择是将 IAM 组中的一组用户分组，然后应用具有对 Amazon S3 bucket 所需访问权限的策略。这将使您能够轻松添加、删除和管理用户，而不是手动为每 100 个 IAM 用户添加一个策略。创建新策略并使用 shell 脚本将其应用于多个 IAM 用户是不正确的，因为您需要一个新的 IAM 组用于此场景，而不是通过 shell 脚本将策略分配给每个用户。此方法可以节省您的时间，但之后将很难管理 IAM 组中不包含的所有 100 个用户。为每个 IAM 用户创建具有无限访问权限的新 S3 存储桶访问策略是不正确的，因为您需要一个新的 IAM 组，并且该方法也很耗时。创建新的 IAM 角色并将每个用户添加到 IAM 角色是不正确的，因为您需要使用 IAM 组而不是 IAM 角色。

参考：

http://docs.aws.amazon.com/IAM/latest/UserGuide/id_groups.html AWS 身份服务概述：

<https://www.youtube.com/watch?v=AIdUw0i8rr0>

查看此 AWS IAM 备忘单：

<https://tutorialsdojo.com/aws-identity-and-access-management-iam/Dojo> 的 AWS 认证解决方案架构师助理考试学习指南教程：<https://tutorialsdojo.com/aws-certified-solutions-architect-associate/>

Q228. 公司需要启动一个具有持久块存储的 Amazon EC2 实例来托管其应用程序。

存储的数据必须在静止时加密。

在这种情况下，以下哪项是最合适的存储解决方案？

- A、启用服务器端加密（SSE）的 Amazon EBS 卷。
- B、使用 SSL 加密的 Amazon EC2 实例存储。
- C、使用 AWS KMS 加密 Amazon EBS 卷。
- D、使用 AWS KMS 加密 Amazon EC2 实例存储。

答案 C

分析：

Amazon 弹性块存储（Amazon EBS）提供用于 EC2 实例的块级存储卷。EBS 卷的行为类似于原始、未格式化的块设备。您可以将这些卷作为设备装载到实例上。连接到实例的 EBS 卷公开为独立于实例生命周期的存储卷。

Amazon EBS 是给定选项中的持久块存储卷。它主要用作存储 EC2 实例的操作系统的根卷。要加密静止的 EBS 卷，可以使用 AWS KMS 客户主密钥加密 EC2 实例的启动卷和数据卷。因此，正确答案是：使用 AWS KMS 加密 Amazon EBS 卷。说：使用 SSL 加密的 Amazon EC2 实例存储和使用 AWS KMS 的加密 Amazon EC1 实例存储的选项都是不正确的，因为该场景需要持久块存储，而不是临时存储。此外，启用 SSL 在该场景中不是必需的，因为它主要用于加密传输中的数据。

“启用服务器端加密（SSE）的 Amazon EBS 卷”选项不正确，因为 EBS 卷仅使用 AWS KMS 加密。服务器端加密（SSE）实际上是 Amazon S3 的一个选项，但不是 Amazon EC2 的选项。

参考文献：

<https://aws.amazon.com/ebs/faqs/> <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AmazonEBS.html> 查看此

亚马逊 EBS 备忘单：<https://tutorialsdojo.com/amazon-ebs/>

Q229. 一家公司正在生成保存在其内部数据中心的机密数据。作为备份解决方案，该公司希望将数据上传到 Amazon S3 存储桶。根据其内部安全授权，数据加密必须在发送到 Amazon S3 之前完成。公司必须花时间管理和轮换加密密钥，并控制谁可以访问这些密钥。

以下哪种方法可以达到此要求？（选择两个。）

- A、使用客户端主密钥设置客户端加密。
- B、使用存储在 AWS 密钥管理服务（AWS KMS）中的客户主密钥设置客户端加密。

- C、使用 Amazon S3 托管加密密钥设置客户端加密。
- D、使用 EC2 密钥对设置服务器端加密（SSE）。
- E、使用存储在单独 S3 存储桶中的密钥设置服务器端加密。

回答 AB

分析：

数据保护指的是在传输过程中（当数据往返于 Amazon S3 时）和静止时（当数据存储在 Amazon S3 数据中心的磁盘上时）保护数据。您可以使用 SSL 或客户端加密来保护传输中的数据。您可以使用以下选项来保护 Amazon S3 中的静态数据：

使用服务器端加密？您请求 Amazon S3 在将对象保存到其数据中心的磁盘上之前对其进行加密，并在下载对象时对其进行解密。使用亚马逊 S3 的服务器端加密-托管密钥（SSE-S3）使用 AWS KMS 托管密钥的服务器端密码（SSE-KMS）使用客户提供密钥的服务器侧加密（SSE-C）使用客户端加密？您可以在客户端加密数据，并将加密的数据上载到

在本例中，您管理加密过程、加密密钥和相关工具。使用 AWS KMS 管理的客户主密钥（CMK）进行客户端加密使用客户主密钥进行客户端加密。因此，正确答案如下：

- 使用存储在 AWS 密钥管理服务（AWS KMS）中的客户主密钥设置客户端加密。
- 使用客户主密钥设置客户端加密。“使用存储在单独 S3 存储桶中的密钥设置服务器端加密”选项是不正确的，因为您必须使用 AWS KMS 来存储加密密钥，或者选择 AWS 管理的 CMK，以在 Amazon S3 中正确实现服务器端加密。此外，在 Amazon S3 中存储任何类型的加密密钥实际上都存在安全风险，不建议使用。“使用 Amazon S3 托管加密密钥设置客户端加密”选项不正确，因为您无法使用 Amazon S3 托管加密密钥进行客户端加密。顾名思义，Amazon S3 托管密钥完全由 AWS 管理，并自动旋转密钥，无需任何手动干预。对于这种情况，您必须在 AWS KMS 中设置客户主密钥（CMK），您可以管理、轮换和审核，或者使用手动维护的客户主密钥。“使用 EC2 密钥对设置服务器端加密（SSE）”选项不正确，因为您不能使用 Amazon EC2 实例的密钥对加密 S3 存储桶。您必须使用存储在 AWS KMS 中的客户主密钥或客户主密钥。参考文献：

<http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingEncryption.html>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingClientSideEncryption.html> 查看此 Amazon S3 备忘单：

<https://tutorialsdojo.com/amazon-s3/>

Q230.一家公司在私有子网中部署了多个 EC2 实例。解决方案架构师需要确保

100	ALL Traffic	ALL	ALL	0.0.0.0/0	ALLOW
101	Custom TCP Rule	TCP (6)	4000	110.238.109.37/32	DENY
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

所有 EC2 实例的安全性。在检查网络 ACL 的现有入站规则时，她看到了以下配置：

如果 IP 地址为 110.238.109.37 的计算机向 VPC 发送请求，会发生什么？

- A、最初，它将被允许，然后一段时间后，连接将被拒绝。

- B、它将被拒绝。
- C、最初，它将被拒绝，然后一段时间后，连接将被允许。
- D、这是允许的。

答案 D

分析：

规则从编号最低的规则开始计算。一旦一条规则与流量匹配，它就会立即应用，而不管任何更高编号的规则是否与它相矛盾。

我们这里有 3 条规则：

1. 规则 100 允许来自任何来源的所有流量。
2. 规则 101 拒绝来自 110.238.109.37 的所有流量。默认规则 (*) 拒绝来自任何源的所有流量。将首先评估规则 100。如果存在匹配，则将允许请求。否则，它将转到规则 101，重复相同的过程，直到它转到默认规则。在这种情况下，当有来自 238.109.37 的请求时，它将首先通过规则 100。由于规则 100 表示它将允许来自任何来源的所有流量，它将允许该请求，并且不会进一步评估规则 101（拒绝 110.238.109.37）或默认规则。

参考：

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_ACLS.html 查看此亚马逊 VPC 备忘单：

<https://tutorialsdojo.com/amazon-vpc/> 对的：

Q231. 一家公司目前有一款增强现实（AR）手机游戏，该游戏具有无服务器后端。它使用了使用 AWS CLI 启动的 DynamoDB 表来存储从播放器收集的所有用户数据和信息，并使用 Lambda 函数从 DynamoDB 中提取数据。该游戏每天被数百万用户用来读取和存储数据。

您将如何设计应用程序以提高其整体性能并使其更具可扩展性，同时保持低成本？（选择两个。）

- A、启用 DynamoDB 加速器（DAX），并确保启用自动缩放，并增加最大的读写容量。
- B、以 DynamoDB 为原点配置 CloudFront；使用 InGelasticache 在客户端设备上缓存频繁访问的数据。
- C、将 API 网关与 Lambda 结合使用，并在频繁访问的数据上启用缓存，并启用 DynamodB 全局复制。
- D、使用 AWS SSO 和 Cognoto 对用户进行身份验证，并让他们使用单点登录直接访问 DynamoDB。手动将配置的读写容量设置为更高的 RCU 和 WCU。
- E、由于默认情况下启用了自动缩放，因此配置的读写容量将自动调整。还启用了 DynamoDB 加速器（DAX），将性能从毫秒提高到微秒。

答覆

分析：

正确答案是以下选项：

- 启用 DynamoDB Accelerator (DAX)，确保启用自动缩放，并增加最大配置读写容量。
- 将 API 网关与 Lambda 结合使用，打开频繁访问数据的缓存，并启用 DynamoDB 全局复制。

Amazon DynamoDB 加速器 (DAX) 是一个完全管理、高度可用的内存缓存，可为 DynamoDB 提供高达 10 倍的性能改进？从毫秒到微秒？甚至每秒数百万个请求。DAX 完成了为 DynamoDB 表添加内存加速所需的所有繁重工作，无需开发人员管理缓存失效、数据填充或集群管理。

Amazon API Gateway 允许您创建一个 API，作为应用程序从后端服务（如运行在 AWS Lambda 上的代码）访问数据、业务逻辑或功能的“前门”。Amazon API 网关处理接受和处理多达数十万个并发 API 调用所涉及的所有任务，包括流量管理、授权和访问控制、监控和 API 版本管理。亚马逊 API 网关没有最低费用或启动成本。AWS Lambda 代表您自动缩放函数。每次收到函数的事件通知时，AWS Lambda 都会快速定位其计算机群中的空闲容量并运行代码。由于您的代码是无状态的，AWS Lambda 可以根据需要启动任意多个函数副本，而无需长时间的部署和配置延迟。

该选项表示：以 DynamoDB 为起点配置 CloudFront；使用 ElastiCache 在客户端设备上缓存频繁访问的数据不正确。尽管 CloudFront 使用边缘位置更快地向用户交付内容，但您仍然无法将 DynamoDB 表与 CloudFront 集成，因为这两个表不兼容。

该选项表示：使用 AWS SSO 和 Cognito 对用户进行身份验证，并让他们使用单点登录直接访问 DynamoDB。手动将配置的读写容量设置为更高的 RCU 和 WCU 是不正确的，因为 AWS 单点登录 (SSO) 是一种云 SSO 服务，它可以方便地集中管理对多个 AWS 帐户和业务应用程序的 SSO 访问。这对应用程序的可伸缩性和性能没有多大帮助。手动将配置的读写容量设置为更高的 RCU 和 WCU 是昂贵的，因为该容量将 24 小时运行，即使传入流量稳定且不需要扩展，也将保持不变。该选项表示：

由于默认情况下启用了自动缩放，因此配置的读写容量将自动调整。此外，启用 DynamoDB 加速器 (DAX) 将性能从毫秒提高到微秒是不正确的，因为默认情况下，在使用 AWS CLI 创建的 DynamoDB 表中未启用自动缩放。

参考文献：

<https://aws.amazon.com/lambda/faqs/>

<https://aws.amazon.com/api-gateway/faqs/>

<https://aws.amazon.com/dynamodb/dax/>

Dojo 的 AWS 认证解决方案架构师助理考试学习指南教程：<https://tutorialsdojo.com/aws-certified-solutions-architect-associate/>

Q232. 该国的一家大型金融公司拥有一个 AWS 环境，其中包含几个保留的 EC2 实例，托管一个上周已停用的 web 应用程序。为了节省成本，您需要尽快停止对保留实例收取费用。在这种情况下，您将采取哪些具有成本效益的步骤？（选择两个。）

- A、请联系 AWS 以取消您的 AWS 订阅。
- B、去亚马逊.com 在线购物网站，并出售保留的实例。
- C、转到 AWS 保留实例市场并出售保留实例。

D、尽快终止保留的实例，以避免在其到期时按按按需计费。

E、尽快停止保留的实例。

对裁谈会的答复

分析：

保留实例市场是一个平台，支持销售第三方和 AWS 客户未使用的标准保留实例，在长度和定价选项方面有所不同。例如，您可能希望在将实例移动到新的 AWS 区域、更改为新的实例类型、在期限到期前结束项目、业务需要更改或您拥有不需要的容量后出售保留实例。

因此，正确答案是：

- 转到 AWS 保留实例市场并出售保留实例。

- 尽快终止保留的实例，以避免在其到期时按按按需计费。

尽快停止保留实例是不正确的，因为停止的实例仍然可以重新启动。请注意，当保留实例到期时，保留实例所涵盖的任何实例都将按按需计费，成本明显更高。由于应用程序已经退役，因此没有必要保留未使用的实例。也可能存在关联的弹性 IP 地址，如果这些地址与停止的实例关联，则会产生费用。联系 AWS 取消 AWS 订阅是不正确的，因为您不需要关闭 AWS 帐户。

去亚马逊.com 在线购物网站和销售保留实例是不正确的，因为您必须使用 AWS 保留实例市场来销售您的实例。参考文献：

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ri-market-general.html>

docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-lifecycle.html 查看此 Amazon EC2 备忘单：

<https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/>

Q233.解决方案架构师需要以最便宜、最安全的方式设置堡垒主机。架构师应该是唯一可以通过 SSH 访问它的人。

以下哪一个步骤可以满足此要求？

- A、 设置一个大型 EC2 实例和一个仅允许访问端口 22 的安全组
- B、 设置一个大型 EC2 实例和一个仅允许通过 IP 地址访问端口 22 的安全组
- C、 设置一个小型 EC2 实例和一个安全组，只允许通过 IP 地址访问端口 22
- D、 设置一个小型 EC2 实例和一个仅允许访问端口 22 的安全组

答案 C

分析：

堡垒主机是一台服务器，其目的是从外部网络（如互联网）提供对专用网络的访问。由于其暴露于潜在的攻击，堡垒主机必须尽量减少渗透的机会。

要创建 bastion 主机，您可以创建一个新的 EC2 实例，该实例应该只有来自特定

最大安全性的 IP 地址。由于问题中也考虑了成本，因此您应该为主机选择一个小实例。默认情况下，AWS 使用 t2.micro 实例，但您可以在部署期间更改这些设置。

设置一个大型 EC2 实例和一个仅允许通过 IP 地址访问端口 22 的安全组是不正确的，因为您不需要配置一个大型的 EC2 实例来运行单个 bastion 主机。同时，您正在寻找最便宜的解决方案。

通用域名格式

设置一个大型 EC2 实例和一个仅允许在端口 22 上访问的安全组，以及设置一个小型 EC2 实例或一个仅支持在端口 22 访问的安全性组的选项都是不正确的，因为您没有将您的特定 IP 地址设置为安全组规则，这可能意味着您公开允许来自安全组中所有源的流量。这是错误的，因为您应该是唯一有权访问堡垒主机的人。

参考文献：

[https://docs.aws.amazon.com/quickstart/latest/linux-](https://docs.aws.amazon.com/quickstart/latest/linux-bastion/architecture.html)

[bastion/architecture.html](https://aws.amazon.com/blogs/security/how-to-record-ssh-sessions-built-through-a-bastion-host/)[https://aws.amazon.com/blogs/security/how-to-record-ssh-sessions-built-through-a-](https://aws.amazon.com/blogs/security/how-to-record-ssh-sessions-built-through-a-bastion-host/)

[bastion-host/](https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/)查看此 Amazon EC2 备忘单：<https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/>

Q234.一个在线股票交易应用程序将金融数据存储存储在 S3 存储桶中，其生命周期策略是每月将较旧的数据移动到 Glacier。有一个严格的合规要求，在任何时候都可以进行意外审计，在任何情况下，您都应该能够在 15 分钟内检索到所需的数据。您的经理指示您确保在需要时提供检索容量，并应处理高达 150 MB/s 的检索吞吐量。

为了满足上述要求，您应该执行以下哪项操作？（选择两个。）

- A、指定要检索的财务数据存档的范围或部分。
- B、使用批量检索访问财务数据。
- C、购买配置的检索能力。
- D、使用亚马逊冰川选择检索数据。
- E、使用快速检索访问财务数据。

行政长官的答覆

分析：

快速检索允许您在偶尔需要紧急请求存档子集时快速访问数据。对于除最大的存档（250 MB 以上）之外的所有存档，使用快速检索访问的数据通常在 1 分钟配置的容量可确保在您需要时提供快速检索的检索容量。

要进行快速、标准或批量检索，请将初始化作业（后作业）REST API 请求中的 Tier 参数设置为所需选项，或 AWS CLI 或 AWS SDK 中的等效选项。如果您购买了配置的容量，则所有快速检索都将通过您的配置容量自动提供。

配置的容量可确保您在需要时可以使用快速检索的检索容量。每单位容量至少每五分钟可执行三次快速检索，最多可提供 150 次

MB/s 的检索吞吐量。如果您的工作负载需要在几分钟内对数据子集进行高度可靠和可预测的访问，则应购买预配置的检索容量。在没有提供容量的情况下，可以接受快速检索，但需求异常高的罕见情况除外。但是，如果您在任何情况下都需要访问快速检索，则必须购买配置的检索容量。

使用 Amazon Glacier Select 检索数据是不正确的，因为这不是一个存档检索选项，主要用于使用简单结构化查询语言（SQL）语句直接在您的冰川数据存档上执行过滤操作。

使用批量检索访问财务数据是不正确的，因为批量检索通常在 5 年内完成。因此，这不满足在 15 分钟内检索数据的要求。配置的容量选项也与批量检索不兼容。指定要检索的财务数据存档的范围或部分是不正确的，因为使用范围存档检索不足以满足在给定时间段内检索整个存档的要求。此外，它不提供额外的检索容量，而这正是配置容量选项所能提供的。

参考文献：

<https://docs.aws.amazon.com/amazonglacier/latest/dev/downloading-an-archive-two-steps.html>

<https://docs.aws.amazon.com/amazonglacier/latest/dev/glacier-select.html> 查看此亚马逊 S3 冰川备忘单：

<https://tutorialsdojo.com/amazon-glacier/>

Q235.一家公司的 web 应用程序完全依赖速度较慢的基于磁盘的数据库，导致其运行速度较慢。为了提高性能，解决方案架构师使用 ElastiCache 将内存数据存储集成到 web 应用程序中。

Amazon ElastiCache 如何提高数据库性能？

- A、通过缓存数据库查询结果。
- B、它通过将读取查询从应用程序路由到读取副本来减少数据库的负载。
- C、它以低延迟和高传输速度安全地向全球客户提供数据。
- D、它提供了一个内存缓存，可将性能提高 10 倍，从毫秒到微秒，甚至每秒数百万个请求。

答：

分析：

ElastiCache 通过缓存查询结果来提高数据库的性能。inmemory 键值存储的主要目的是提供对数据副本的超快（亚毫秒延迟）和廉价访问。大多数数据存储具有经常访问但很少更新的数据区域。此外，查询数据库总是比在键值对缓存中查找键更慢和更昂贵。某些数据库查询执行起来特别昂贵，例如，涉及跨多个表联接的查询或具有密集计算的查询。通过缓存这些查询结果，您只需支付一次查询的费用，就可以多次快速检索数据，而无需重新执行查询。

“它以低延迟和高传输速度安全地向全球客户交付数据”的选项是不正确的，因为该选项描述了 CloudFront 的功能，而不是 ElastiCache。该选项表示：它提供了一个内存缓存，从毫秒到微秒，甚至每秒数百万个请求，性能提高了 10 倍，这是不正确的，因为该选项描述了 Amazon DynamoDB 加速器（DAX）的功能，而不是 ElastiCache。Amazon DynamoDB 加速器（DAX）是一个完全管理的、高可用的内存缓存。Amazon ElastiCache 无法提供从毫秒到微秒的性能改进，更不用说像 DAX 那样每秒数百万个请求了。“通过将读取查询从应用程序路由到读取副本来减少数据库负载”的选项是不正确的，因为该选项描述了 RDS 读取副本的功能，而不是 ElastiCache。Amazon RDS 读取副本使您能够在同一 AWS 区域或不同 AWS 区域内创建数据库实例的一个或多个只读副本。参考文献：<https://aws.amazon.com/elasticache/>

<https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/elasticache-use-cases.html> 查看此 Amazon

Elasticache 备忘单：<https://tutorialsdojo.com/amazon-elasticache/>

Q236.您正在 VPC 中自动创建 EC2 实例。因此，您编写了一个 python 脚本来触发 AmazonEC2API 在单个可用性区域中请求 50 个 EC2 实例。但是，您注意到，在 20 个成功请求之后，后续请求失败。这个问题的原因是什么？您将如何解决？

- A、默认情况下，AWS 允许每个区域最多提供 20 个实例。选择其他区域并重试失败的请求。
- B、Amazon EC2 API 存在问题。只需重新发送请求，这些请求将被成功配置。
- C、默认情况下，AWS 允许您为每个可用性区域提供最多 20 个实例。选择其他可用性区域，然后重试失败的请求。
- D、每个区域有一个基于需求实例限制的 vCPU，这就是后续请求失败的原因。

只需向 AWS 提交限额增加表，并在批准后重试失败的请求。

答案 D

分析：

根据需求实例限制，您只能在每个 vCPU 上运行按需实例，购买 20 个保留实例，并根据每个区域的动态现货限制请求现货实例。新的 AWS 账户可能以低于此处所述限额的限额开始。如果您需要更多实例，请使用您的用例填写 Amazon EC2 限额增加请求表，我们将考虑您的限额增加。限额增加与要求的区域相关。因此，正确的答案是：存在基于每个区域需求实例限制的 vCPU，这就是后续请求失败的原因。只需向 AWS 提交限额增加表，并在批准后重试失败的请求。选项表明：Amazon EC2 API 存在问题。只需重新发送请求，这些请求将被成功配置是不正确的，因为根据 VCPubased On Demand 实例限制，您只能运行按需实例。此外，购买 20 个保留实例的限制，以及每个区域的动态 Spot 限制请求 Spot 实例。因此，EC2 API 没有问题。

该选项表示：默认情况下，AWS 允许您为每个区域提供最多 20 个实例。如果失败的请求不正确，请选择其他区域并重试。无需选择其他区域，因为在向 AWS 提交申请表后，可以增加该限制。

该选项表示：默认情况下，AWS 允许您为每个可用性区域提供最多 20 个实例。选择其他可用性区域并重试。失败的请求不正确，因为 vCPU 基于需求

实例限制是按区域设置的，而不是按可用性区域设置的。在将申请表提交至后，可以增加此值 AWS。

参考文献：

https://docs.aws.amazon.com/general/latest/gr/aws_service_limits.html#limits_ec2

亚马逊。com/ec2/faqs/#How_many_instances_can_I_run_in_Amazon_ec2 查看此 Amazon ec2 备忘单：

<https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/>

Q237.一家公司在 AWS 中使用 EC2、自动缩放组、S3 和 SQS 的去耦应用程序。解决方案架构师以这样的方式设计架构：EC2 实例将使用来自 SQS 队列的消息，并将根据队列中的消息数量自动放大或缩小。

在这种情况下，以下哪项关于 SQS 的陈述是错误的？

- A、AmazonSQS 可以帮助您构建具有解耦组件的分布式应用程序。
- B、FIFO 队列只提供一次处理。

C、标准队列保留消息的顺序。

D、标准队列至少提供一次传递，这意味着每个消息至少传递一次。

答案 D

分析：

所有答案都是正确的，除了一个选项：标准队列保留消息的顺序。只有 FIFO 队列可以保留消息的顺序，而不是标准队列。

参考：<https://aws.amazon.com/sqs/faqs/>

查看此亚马逊 SQS 备忘单：

<https://tutorialsdojo.com/amazon-sqs/>

Dojo 的 AWS 认证解决方案架构师助理考试学习指南教程：<https://tutorialsdojo.com/aws-certified-solutions-architect-associate-saa-c02/>

Q238.托管在 Amazon RDS 上的生产 MySQL 数据库的磁盘存储空间不足。管理层已咨询其解决方案架构师，以在不影响数据库性能的情况下增加磁盘空间。

解决方案架构师如何以最小的运营开销满足需求？

A、将 DB 实例参数组的 `default_storage_engine` 更改为 MyISAM。

B、将 DB 实例存储类型修改为已配置 IOPS。

C、修改数据库实例设置并启用存储自动缩放。

D、增加为 DB 实例分配的存储空间。

答案 C

分析：

RDS 存储自动扩展可自动扩展存储容量，以响应不断增长的数据库工作负载，无停机时间。

资源调配不足可能导致应用程序停机，而资源调配过度可能导致资源利用不足和成本增加。通过 RDS 存储自动扩展，您只需设置所需的最大存储限制，自动扩展即可解决其余问题。RDS 存储自动缩放可连续监控实际存储消耗，并在实际利用率接近配置的存储容量时自动扩展容量。自动缩放适用于新的和现有的数据库实例。只需在 AWS 管理控制台中单击几下即可启用自动缩放。RDS 存储自动扩展不需要额外的成本。您只需支付运行应用程序所需的 RDS 资源。因此，正确的答案是：修改 DB 实例设置并启用存储自动缩放。

“增加数据库实例的分配存储”选项不正确。虽然这将解决磁盘空间不足的问题，但增加分配的存储可能会导致更改期间的性能下降。

表示：将 DB 实例参数组的 `default_storage_engine` 更改为 MyISAM 的选项不正确。

这只是 MySQL 的存储引擎。它不会以任何方式增加磁盘空间。“将 DB 实例存储类型修改为已配置 IOPS”选项不正确。这可能会提高磁盘性能，但不会解决数据库存储不足的问题。

参考文献:

<https://aws.amazon.com/about-aws/whats-new/2019/06/rds-storage-auto-scaling/>

docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_PIOPS.StorageTypes.html#USER_PIOPS.StorageTypes。html#USER_PI OPS.自动缩放

查看此 Amazon RDS 备忘单: <https://tutorialsdojo.com/amazon-relational-database-service-amazon-rds/>

Q239.一家公司安装了传感器来跟踪参观公园的人数。数据每天发送到 Amazon Kinesis 流,默认设置用于处理,其中消费者被配置为每隔一天处理数据。您注意到 S3 存储桶没有接收发送到 Kinesis 流的所有数据。您检查了传感器是否正确地将数据发送到 Amazon Kinesis,并验证数据确实每天发送。这可能是什么原因?

- A、默认情况下,Amazon S3 存储数据 1 天,并将其移动到 Amazon Glacier。
- B、传感器有问题。它们可能有一些间歇性连接,因此数据不会发送到流。
- C、默认情况下,数据记录仅在添加到 Kinesis 流后 24 小时内可访问。
- D、您的 AWS 帐户被黑客入侵,有人删除了您 Kinesis 流中的一些数据。

答案 C

分析:

Kinesis 数据流支持更改流的数据记录保留期。Kinesis 数据流是一个有序的数据记录序列,用于实时写入和读取。因此,数据记录临时存储在流中的碎片中。从记录添加到不再可访问的时间段称为保留期。Kinesis 数据流默认存储 24 小时至最多 8760 小时(365 天)的记录。

这就是 S3 存储桶中缺少数据的原因。要解决此问题,您可以将传感器配置为每天发送数据,而不是每隔一天发送一次数据,或者可以延长 Kinesis 数据流的保留期。

选项显示:传感器有问题。他们可能有一些断断续续的连接,因此,数据没有发送到流是不正确的。您已经验证了传感器工作正常,因此,这不是问题的根本原因。默认情况下,Amazon S3 存储 1 天的数据并将其移动到 Amazon Glacier 的选项是不正确的,因为默认情况下 Amazon S3 不存储 1 天数据并将数据移动到亚马逊冰川。该选项表示:您的 AWS 帐户被黑客入侵,有人删除了 Kinesis 流中的一些数据,这是不正确的。尽管这可能是一种可能性,但您应该首先验证 S3 存储桶中丢失数据是否有其他更可能的原因。请确保遵循并应用安全最佳实践,以防止被人入侵。

默认情况下,数据记录只能在添加到 Kinesis 流后的 24 小时内访问,这说明了此问题的根本原因。

参考:

<http://docs.aws.amazon.com/streams/latest/dev/kinesis-extended-retention.html> 查看此亚马逊 Kinesis 备忘单:

<https://tutorialsdojo.com/amazon-kinesis/>

Q240.创建了一个 Linux EC2 实例的自动扩展组,并在 CloudWatch 中启用了基本监控。

您注意到您的应用程序速度很慢,因此请您的一名工程师检查所有 EC2 实例。在检查实例之后,您注意到自动缩放组并没有像应该的那样启动更多实例,即使服务器已经有很高的内存使用率。架构师应该实现以下哪个选项来解决这个问题?

- A、启用对实例的详细监视。
- B、在 EC2 实例中安装 AWS SDK。创建一个脚本，如果内存使用率较高，该脚本将触发自动缩放事件。
- C、修改扩展策略以增加阈值以扩展实例数。
- D、将 CloudWatch 代理安装到 EC2 实例，这将触发自动扩展组向外扩展。

答案 D

分析：

Amazon CloudWatch 代理允许您从 Amazon EC2 实例和本地服务器收集系统指标和日志文件。代理同时支持 Windows Server 和 Linux，并允许您选择要收集的指标，包括子资源指标，如每个 CPU 核心。该场景的前提是 EC2 服务器具有高内存使用率，但由于默认情况下自动扩展组不会跟踪此特定指标，因此不会触发扩展活动。请记住，默认情况下，CloudWatch 不监视内存使用情况，只监视 CPU 利用率、网络利用率、磁盘性能和磁盘读/写。这就是为什么您必须在 EC2 实例中安装 CloudWatch 代理，以收集和监控自定义度量（内存使用），自动缩放组将使用该度量作为缩放活动的触发器。

因此，正确的答案是：将 CloudWatch 代理安装到 EC2 实例，这将触发自动扩展组的扩展。

选项显示：在 EC2 实例中安装 AWS SDK。创建一个脚本，该脚本将在内存使用率较高时触发自动缩放事件。这是不正确的，因为 AWS SDK 是一组编程工具，允许您创建使用 Amazon 云服务运行的应用程序。您必须对警报进行编程，这不是本场景的最佳策略。“启用对实例的详细监视”选项不正确，因为详细监视不提供内存使用的度量。CloudWatch 在其默认 EC2 指标集中不监控内存使用情况，而详细监控只提供更高频率的指标（1 分钟频率）。“修改扩展策略以增加阈值以扩展实例数”选项不正确，因为您已经将使用量最大化，这实际上会导致自动扩展事件。

参考文献：

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/Install-CloudWatch-Agent.html>https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/viewing_metrics_with_cloudwatch.html 和 https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/monitoring_ec2.html 查看这些 amazon ec2 和 CloudWatch 备忘单：<https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/> <https://tutorialsdojo.com/amazon-云表/>

Q241.一位软件开发人员就他正在构建的 web 应用程序所需的 AWS 资源咨询了云基础设施团队的技术负责人。开发人员知道实例存储只提供临时存储，当实例终止时，数据会自动删除。为了确保 web 应用程序的数据持久，应用程序应在连接了持久块级存储卷的 EC2 实例中启动。开发人员知道他们需要使用

EBS 卷，但他们不确定需要使用什么类型。在这种情况下，以下哪项关于 Amazon EBS 卷类型及其各自的使用情况是正确的？（选择两个。）

- A、单根 I/O 虚拟化（SR-IOV）卷适用于各种工作负载，包括中小型数据库、开发和测试环境以及启动卷。
- B、配置的 IOPS 卷提供具有一致和低延迟性能的存储，并专为 I/O 密集型应用程序（如大型关系数据库或 NoSQL 数据库）而设计。
- C、在所有 EBS 卷类型中，磁性卷的每 GB 成本最低，非常适合于数据访问不频繁的工作负载和存储成本最低的应用程序。
- D、支持多连接的通用 SSD（gp3）卷提供一致且低延迟的性能，并专为需要多 az 弹性的应用程序而设计。

E、在所有 EBS 卷类型中，Spot 卷的每 GB 成本最低，非常适合于数据访问不频繁的工作负载和存储成本最低的应用程序。

答案：BC

分析：

Amazon EBS 提供了三种卷类型，以最好地满足您的工作负载需求：通用（SSD）、配置 IOPS（SSD）和磁性。

通用（SSD）是一种新的、支持 SSD 的通用 EBS 卷类型，建议使用

客户的默认选择。通用（SSD）卷适用于各种工作负载，包括中小型数据库、开发和测试环境以及启动卷。

配置的 IOPS（SSD）卷提供具有一致和低延迟性能的存储，专为 I/O 密集型应用程序（如大型关系数据库或 NoSQL 数据库）而设计。在所有 EBS 卷类型中，磁性卷的每 GB 成本最低。磁卷非常适合数据访问不频繁的工作负载，以及存储成本最低的应用程序。请注意，这是上一代卷。最新的低成本磁存储类型是冷硬盘（sc1）和吞吐量优化硬盘（st1）卷。因此，正确答案是：

- 配置的 IOPS 卷提供具有一致和低延迟性能的存储，并专为 I/O 密集型应用程序（如大型关系数据库或 NoSQL 数据库）而设计。
- 在所有 EBS 卷类型中，磁性卷的每 GB 成本最低，非常适合于数据访问不频繁的工作负载和存储成本最低的应用程序。该选项表示：在所有 EBS 卷类型中，现货卷的每 GB 成本最低，非常适合数据访问不频繁的工作负载，以及存储成本最低的应用程序，这是不正确的，因为没有称为“现货卷”的 EBS 类型。但是，现货实例有一个实例购买选项。

“启用多连接的通用 SSD（gp3）卷提供一致且低延迟的性能，并且专为需要多 az 弹性的应用程序设计”选项不正确，因为多连接功能只能在 EBS 配置的 IOPS io2 或 io1 卷上启用。此外，多连接不会提供多 az 弹性，因为此功能仅允许将 EBS 卷连接到可用性区域内的多个实例上。表示：单根 I/O 虚拟化（SR-IOV）卷适用于各种工作负载，包括中小型数据库、开发和测试环境以及启动卷的选项是不正确的，因为 SR-IOV 与 Linux 上的增强网络相关，而不是与 EBS 相关。参考文献：

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html><https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AmazonEBS.html> 查看此亚马逊 EBS 备忘单：<https://tutorialsdojo.com/amazon-ebs/>

Q242.一家财富 500 强公司在全球拥有众多办事处和客户，已聘请您为其首席建筑师。您的员工和客户定期从全球各大洲的区域数据中心将千兆字节到兆字节的数据上传到一个集中的 S3 存储桶中。在财政年度结束时，有数千个数据被上传到位于 `apsoutheast-2`（悉尼）地区的中央 S3 存储桶，许多员工开始抱怨上传时间太慢。CTO 指示您尽快解决此问题，以避免在处理其全球财政年度结束（EOFY）报告时出现任何延迟。Amazon S3 中的哪项功能可以在长时间内实现快速、轻松和安全的文件传输

您的客户和 Amazon S3 bucket 之间的距离？

- A、跨区域复制
- B、多部分上传
- C、AWS 全球加速器
- D、转移加速度

答案 D

分析：

Amazon S3 传输加速支持在客户机和 Amazon S3bucket 之间进行长距离、快速、轻松和安全的文件传输。传输加速利用了 Amazon CloudFront 全球分布的 AWS 边缘位置。当数据到达 AWS 边缘位置时，数据将通过优化的网络路径路由到 Amazon S3 存储桶。

Amazon S3 传输加速可以将到和来自 Amazon S3 的内容传输速度提高 50-500%，用于更大对象的远程传输。拥有广泛用户的 web 或移动应用程序的客户，或托管在远离其 S3 存储桶的应用程序的用户，可以在互联网上体验到长时间和可变的上传和下载速度。S3 传输加速（S3TA）减少了可能影响传输的互联网路由、拥塞和速度的可变性，并从逻辑上缩短了远程应用到 S3 的距离。S3TA 通过 Amazon CloudFront 全球分布的边缘位置和 AWS 骨干网络路由流量，并通过网络协议优化，提高传输性能。

因此，转移加速度是正确答案。

AWS 全局加速器不正确，因为此服务主要用于优化从用户到应用程序的路径，从而提高 TCP 和 UDP 流量的性能。使用 Amazon S3 传输加速更适合此场景。跨区域复制是不正确的，因为这只是使您能够自动将 S3 对象从一个存储桶复制到位于不同 AWS 区域或同一区域内的另一个存储容器。多部分上传是不正确的，因为此功能仅允许您将单个对象作为一组部分上传。您可以独立地以任何顺序上传这些对象部分。如果任何部分的传输失败，您可以重新传输该部分而不影响其他部分。上传对象的所有部分后，AmazonS3 将这些部分组装起来并创建对象。通常，当对象大小达到 100 MB 时，应考虑使用多部分上传，而不是在单个操作中上传对象。

参考文献：<https://aws.amazon.com/s3/faqs/>

<https://aws.amazon.com/s3/transfer-acceleration/>

查看此 Amazon S3 备忘单：<https://tutorialsdojo.com/amazon-s3/>

Q243. 一家公司有一个基于 web 的订单处理系统，目前使用亚马逊 SQS 中的标准队列。IT 经理注意到，在很多情况下，订单被处理了两次。这个问题在处理过程中造成了很多麻烦，让客户非常不满意。经理已要求您确保此问题不会再次发生。

你能做些什么来防止这种情况在未来再次发生？（选择两个。）

- A、更改 SQS 的可见性超时。
- B、更改 Amazon SQS 中的保留期。
- C、替换 Amazon SQS，使用 Amazon 简单工作流服务。
- D、改用 Amazon SQS FIFO 队列。
- E、更改 SQS 中的消息大小。

对裁谈会的答复

分析：

Amazon SQS FIFO（先进先出）队列具有标准队列的所有功能，并具有额外功能，用于在操作和事件顺序至关重要或无法容忍重复时增强应用程序之间的消息传递，例如：

- 确保以正确的顺序执行用户输入的命令。-通过以正确的顺序发送价格修改来显示正确的产品价格。-在注册帐户之前阻止学生注册课程。

AmazonSWF 围绕任务分配提供了有用的保证。它确保任务不会重复，并且只分配一次。因此，即使对于特定的活动类型（或决策器的多个实例），您可能有多个工人，Amazon SWF 也将只将特定任务分配给一个工人（或一个决策器实例）。

此外，Amazon SWF 在工作流执行中一次最多保留一个未完成的决策任务。因此，您可以运行多个决策器实例，而不必担心两个实例同时在同一执行上运行。这些工具使您能够协调工作流程，而无需担心重复、丢失或冲突的任务。此场景中的主要问题是订单管理系统有时会产生重复订单。由于该公司正在使用 SQS，因此在 EC2 实例未能删除已处理的消息的情况下，消息可能会有重复。为了防止这个问题发生，您必须使用 Amazon 简单工作流服务而不是 SQS。

因此，正确答案是：

- 替换 Amazon SQS，使用 Amazon 简单工作流服务。
- 改用 Amazon SQS FIFO 队列。

更改 Amazon SQS 中的保留期是不正确的，因为保留期只是指定 Amazon SQS 应删除队列中已存在一段时间的消息。更改 SQS 的可见性超时是不正确的，因为对于标准队列，可见性超时不能保证不会收到两次消息。为了避免重复的 SQS 消息，最好将应用程序设计为幂等（在多次处理同一消息时，它们不应受到不利影响）。

更改 SQS 中的消息大小是不正确的，因为这在场景中根本不相关。

参考文献：

<https://aws.amazon.com/swf/faqs/>

<https://aws.amazon.com/swf/>

[https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-](https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-visibility-visibility-timeout.html)

[visibility-超时。html](https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-visibility-visibility-timeout.html) 查看此 Amazon SWF

备忘单：

<https://tutorialsdojo.com/amazon-simple-workflow-amazon-swf/>亚马逊简单工作流（SWF）vs AWS 步骤功能 vs 亚马逊 SQS：<https://tutorialsdojo.com/amazon-simple-workflow-swf-vs-aws-step-functions-vs-amazon-sqs/>

Q244.AWS 是一个在线交易平台，拥有全球数千名客户。为了减少延迟，您必须将用户流量引导到离客户端最近的应用程序端点。流量应通过选播静态 IP 地址路由到最近的边缘位置。AWS Shield 还应集成到 DDoS 保护解决方案中。

以下哪项是解决方案架构师应使用的最适合满足上述要求的服务？

- A、AWS WAF
- B、亚马逊云盾
- C、AWS PrivateLink

D、AWS 全球加速器

答案 D

分析：

AWS Global Accelerator 是一项服务，可提高本地或全球用户应用程序的可用性和性能。它提供静态 IP 地址，作为单个或多个 AWS 区域中应用程序端点的固定入口点，例如应用程序负载均衡器、网络负载均衡器或 Amazon EC2 实例。

AWS 全球加速器使用 AWS 全球网络优化从用户到应用程序的路径，提高 TCP 和 UDP 流量的性能。AWS Global Accelerator 持续监控应用程序端点的运行状况，并将在不到 1 分钟的时间内检测不健康的端点并将流量重定向到健康的端点。

许多应用程序，如游戏、媒体、移动应用程序和金融应用程序，需要非常低的延迟才能获得良好的用户体验。为了改善用户体验，AWS Global Accelerator 将用户流量引导到离客户端最近的应用程序端点，从而减少互联网延迟和抖动。它通过选播将流量路由到最近的边缘位置，然后通过 AWS 全球网络将流量路由至最近的区域端点。AWS 全球加速器可快速响应网络性能的变化，以提高用户的应用程序性能。

AWS 全球加速器和 Amazon CloudFront 是使用 AWS 全球网络及其全球边缘位置的独立服务。CloudFront 提高了可缓存内容（如图像和视频）和动态内容（如 API 加速和动态站点交付）的性能。全局加速器通过将边缘的数据包代理给在一个或多个 AWS 区域中运行的应用程序，提高了 TCP 或 UDP 上各种应用程序的性能。全局加速器非常适合非 HTTP 用例，如游戏（UDP）、物联网（MQTT）或 IP 语音，以及特别需要静态 IP 地址或确定性快速区域故障转移的 HTTP 用例。这两种服务都与 AWS Shield 集成，以提供 DDoS 保护。

因此，正确答案是 AWS 全球加速器。

Amazon CloudFront 是不正确的，因为尽管该服务使用边缘位置，但它不具备通过选播静态 IP 地址将流量路由到最近的边缘位置的能力。AWS WAF 是不正确的，因为此服务只是一个 web 应用程序防火墙，可帮助保护您的 web 应用程序或 API 免受可能影响可用性、危害安全性或消耗过多资源的常见 web 攻击

AWS PrivateLink 不正确，因为该服务仅在亚马逊网络上安全地提供 VPC、AWS 服务和内部应用程序之间的专用连接。它不通过选播静态 IP 地址将流量路由到最近的边缘位置。参考文献：

<https://aws.amazon.com/global-accelerator/>

<https://aws.amazon.com/global-accelerator/faqs/>查看

AWS 全球加速器备忘单：

<https://tutorialsdojo.com/aws-global-accelerator/>

Q245. 一家公司推出了一个在线平台，允许人们轻松购买、销售、消费和管理他们的加密货币。为了满足严格的 IT 审计要求，所有 AWS 资源上的每个 API 调用都应该被正确捕获和记录。您在专有网络中使用 CloudTrail 帮助您对 AWS 帐户进行合规、运营审计和风险审计。在这个场景中，CloudTrail 在哪里存储它创建的所有日志？

A、发电机

B、亚马逊 S3

C、亚马逊红移

D、RDS 实例

答案 B

分析：

创建 AWS 帐户时，会在其上启用 CloudTrail。当 AWS 帐户中发生活动时，该活动将记录在 CloudTrail 事件中。您可以通过转到事件历史记录轻松查看 CloudTrail 控制台中的事件。

事件历史记录允许您查看、搜索和下载 AWS 帐户中过去 90 天支持的活动。此外，您可以创建 CloudTrail 跟踪，以进一步归档、分析和响应 AWS 资源中的更改。trail 是一种配置，可以将事件传递到您指定的 Amazon S3 bucket。您还可以使用 Amazon CloudWatch 日志和 Amazon CloudWatch 事件交付和分析跟踪事件。您可以使用 CloudTrail 控制台、AWS CLI 或 CloudTrail API 创建跟踪。

其余的答案都不正确。DynamoDB 和 RDS 实例用于数据库；Amazon Redshift 用于水平扩展的数据仓库，允许您存储 TB 和 PB 的数据。

参考文献：

<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/how-cloudtrail-works.html><https://aws.amazon.com/cloudtrail/>

查看此 AWS CloudTrail 备忘单：

<https://tutorialsdojo.com/aws-cloudtrail/>

Q246.应用程序正在使用 AWS 中托管的 RESTful API，该 API 使用亚马逊 API 网关和 AWS Lambda。当用户请求通过 Amazon API 网关 API 到达底层服务时，需要跟踪和分析用户请求。

以下哪项服务最适合用于满足此要求？

A、CloudWatch

B.CloudTrail

C、AWS X 射线

D、专有网络流量日志

答案 C

分析：

您可以使用 AWS X-Ray 跟踪和分析用户请求，因为用户请求通过 Amazon API 网关 API 到达底层服务。API 网关支持所有 API 网关端点类型的 AWS X 射线跟踪：区域、边缘优化和专用。您可以在 X 射线可用的所有地区使用 AWS X 射线和 Amazon API 网关。

X 射线为您提供了整个请求的端到端视图，因此您可以分析 API 及其后端服务中的延迟。您可以使用 X 射线服务映射来查看整个请求的延迟以及与 X 射线集成的下游服务的延迟。您可以配置采样规则，根据您的指定的标准，

告诉 X 射线哪些请求进行记录，采样率是多少。如果从已被跟踪的服务调用 API 网关 API，则 API 网关会传递跟踪，即使 API 上未启用 X 射线跟踪。

您可以使用 API 网关管理控制台或 API 网关 API 或 CLI 为 API 阶段启用 X 射线。

VPC 流量日志是不正确的，因为这是一项功能，可以让您捕获整个 VPC 中进出网络接口的 IP 流量信息。虽然它可以捕获有关传入用户请求的一些详细信息，但最好使用 AWS X 射线，因为它提供了一种更好的方法，可以通过请求跟踪来调试和分析微服务应用程序，从而找到问题和性能的根本原因。

CloudWatch 不正确，因为这是一个监控和管理服务。当用户请求通过 Amazon API 网关 API 时，它不具备跟踪和分析用户请求的能力。CloudTrail 是不正确的，因为它主要用于所有 AWS 资源的 IT 审计和 API 日志记录。与 AWS X-Ray 不同，它不具备跟踪和分析用户请求的能力，因为用户请求通过亚马逊 API 网关 API。

参考：

<https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-xray.html> 查看 AWS X 射线备忘单：

<https://tutorialsdojo.com/aws-x-ray/>

使用 AWS X 射线检测应用程序：

<https://tutorialsdojo.com/instrumenting-your-application-with-aws-x-ray/>

Q247.实时数据分析应用程序使用 AWS Lambda 处理数据，并将结果以 JSON 格式存储到 S3 存储桶中。为了加快现有的工作流程，您必须使用一种服务，在该服务中，您可以对您的数据运行复杂的大数据分析，而无需将其移动到单独的分析系统中。您可以使用以下哪组服务来满足此要求？

- A、 亚马逊 X 射线，亚马逊海王星，DynamoDB
- B、 S3 选择，亚马逊海王星，DynamoDB DAX
- C、 亚马逊胶水，冰川选择，亚马逊红移
- D、 S3 选择，亚马逊雅典娜，亚马逊红移光谱

答案 D

分析：

Amazon S3 允许您在数据上运行复杂的大数据分析，而无需将数据移动到单独的分析系统中。在 AWS 中，有一套工具可以更快地分析和处理云中的大量数据，包括优化现有工作流并将其与 Amazon S3 集成的方法：

1. S3 选择

Amazon S3 Select 旨在帮助分析和处理 AmazonS3 存储桶中对象内的数据，更快更便宜。它通过提供使用简单 SQL 表达式从 AmazonS3 中的对象检索数据子集的能力来工作。您的应用程序不再需要使用计算资源来扫描和过滤对象中的数据，这可能会将查询性能提高 400%，并将查询成本降低 80%。您只需将应用程序更改为使用 SELECT 而不是 GET 即可利用 S3 SELECT。

2. 亚马逊与雅典娜

Amazon Athena 是一个交互式查询服务，可以使用标准 SQL 表达式轻松分析 AmazonS3 中的数据。Athena 是无服务器的，因此没有需要管理的基础设施，您只需为运行的查询付费。雅典娜很容易使用。只需指向

AmazonS3 中的数据，定义模式，然后开始使用标准 SQL 表达式进行查询。大多数结果都在几秒钟内交付。与雅典娜，

不需要复杂的 ETL 作业来准备数据进行分析。这使得具有 SQL 技能的任何人都可以轻松地快速分析大规模数据集。

3. 亚马逊红移光谱

Amazon Redshift 还包括 Redshift Spectrum，允许您直接对 Amazon S3 中的非结构化数据执行 SQL 查询。无需加载或转换，您可以使用开放数据格式，包括 Avro、CSV、Grok、ORC、Parquet、RCFile、RegexSerDe、SequenceFile、TextFile 和 TSV。Redshift Spectrum 根据检索到的数据自动扩展查询计算能力，因此无论数据集大小如何，针对 Amazon S3 的查询都运行得很快。参考：

https://aws.amazon.com/s3/features/#Query_in_Place

亚马逊红移概述：

<https://youtu.be/jlLERNzhHOg> 查看

以下 AWS 备忘单：

<https://tutorialsdojo.com/amazon-s3/>

[https://tutorialsdojo.com/amazon-](https://tutorialsdojo.com/amazon-athena/)

[athena/](https://tutorialsdojo.com/amazon-athena/)

[https://tutorialsdojo.com/amazon-](https://tutorialsdojo.com/amazon-redshift/)

[redshift/](https://tutorialsdojo.com/amazon-redshift/)

Q248.一家公司拥有一个高性能计算（HPC）集群，该集群由 EC2 实例组成，配置 IOPS 卷以处理事务密集型、低延迟的工作负载。解决方案架构师必须保持高 IOPS，同时通过设置卷的最佳队列长度来降低延迟。每个卷的大小为 10 GiB。

以下哪项是架构师应该设置的最合适的配置？

- A、将 IOPS 设置为 400，然后保持较低的队列长度。
- B、将 IOPS 设置为 500，然后保持较低的队列长度。
- C、将 IOPS 设置为 800，然后保持较低的队列长度。
- D、将 IOPS 设置为 600，然后保持高队列长度。

答案 B

分析：

配置的 IOPS SSD（io1）卷旨在满足 I/O 密集型工作负载的需要，特别是数据库工作负载，这些工作负载对存储性能和一致性非常敏感。与 gp2 不同，gp2 使用桶和信用模型来计算性能，io1 卷允许您在创建卷时指定一致的 IOPS 速率，而 Amazon EBS 在给定一年中 99.9% 的时间内提供的 IOPS 性能在 10% 以内。io1 卷的大小范围

可以从 4 GiB 到 16 TiB。您可以在 Nitro 系统实例系列上提供每卷 100 IOPS 到 64000 IOPS，在其他实例系列上最多 32000 IOPS。配置的 IOPS 与请求的卷大小（以 GiB 为单位）的最大比率为 50:1。例如，100 GiB 卷可以配置高达 5000 IOPS。在受支持的实例类型上，任何大小为 1280 GiB 或更大的卷都允许配置高达 64000 IOPS 的最大值（ $50 \times 1280 \text{ GiB} = 64000$ ）。

一个 io1 卷最多可提供 32000 IOPS，支持最大 I/O 大小为 256KIB，并产生高达 500 MiB/s 的吞吐量。当 I/O 大小最大时，峰值吞吐量达到 2000 IOPS。提供超过 32000 IOPS（最高可达 64000 IOPS）的卷支持最大 I/O 大小为 16kiB，并产生高达 1000 MiB/s 的吞吐量。卷队列长度是设备的挂起 I/O 请求数。延迟是 I/O 操作的真正端到客户端时间，换句话说，从向 EBS 发送 I/O 到从 EBS 接收到 I/O 读写完成确认之间的时间。队列长度必须与 I/O 大小和延迟正确校准，以避免在来宾操作系统或 EBS 网络链路上产生瓶颈。

每个工作负载的最佳队列长度不同，这取决于特定应用程序对 IOPS 和延迟的敏感性。如果您的工作负载没有提供足够的 I/O 请求，无法充分利用 EBS 卷的可用性能，那么您的卷可能无法提供您提供的 IOPS 或吞吐量。

事务密集型应用程序对增加的 I/O 延迟非常敏感，非常适合 SSD 支持的 io1 和 gp2 卷。通过保持低队列长度和卷可用的高 IOPS 数，可以在保持高 IOPS 的同时降低延迟。持续驱动卷的 IOPS 超过可用 IOPS 会导致 I/O 延迟增加。吞吐量密集型应用程序对增加的 I/O 延迟不太敏感，非常适合 HDD 支持的 st1 和 sc1 卷。通过在执行大型顺序 I/O 时保持高队列长度，可以保持 HDD 备份卷的高吞吐量。

因此，例如，可以为 10 GiB 卷提供高达 500 IOPS 的数据。任何大小为 640 GiB 或更大的卷都允许最高 32000 IOPS（ $50 \times 640 \text{ GiB} = 32000$ ）的资源调配。因此，正确的答案是将 IOPS 设置为 500，然后保持较低的队列长度。将 IOPS 设置为 400 然后保持低队列长度是不正确的，因为尽管 400 的值是可接受的值，但它不是 IOPS 的最大值。如果仅将该卷设置为 400，则无法充分利用该卷提供的可用 IOPS。以下选项均不正确：将 IOPS 设置为 600，然后保持高队列长度；将 IOPS 设为 800，然后保持低队列长度，因为 10GiB 卷的最大 IOPS 仅为 500。因此，任何大于最大值（如 600 或 800）的值都是错误的。此外，您应该通过保持较低的队列长度而不是较高的队列长度来降低延迟。

参考文献：

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html>
<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-io-characteristics.html> 亚马逊 EBS 概述-SSD 与 HDD:

<https://www.youtube.com/watch?v=LW7x8wyLFvw&t=8s>

查看此亚马逊 EBS 备忘单: <https://tutorialsdojo.com/amazon-ebs/>

Q249.解决方案架构师正在为公司的企业应用程序套件设计云架构。web 层和应用层都需要访问 Internet 以从公共 API 获取数据。但是，这些服务器应该无法从 Internet 访问。

架构师应实施以下哪些步骤以满足上述要求？

- A、 将 web 和应用层实例部署到公共子网，然后为每个 EC2 实例分配弹性 IP 地址。
- B、 将 web 和应用层实例部署到专用子网，然后为每个 EC2 实例分配弹性 IP 地址。
- C、 在专用子网中部署 NAT 网关，并从承载 web 和应用层的公共子网向其添加路由。
- D、 在公共子网中部署 NAT 网关，并从承载 web 和应用层的私有子网向其添加路由。

答案 D

分析:

您可以使用网络地址转换（NAT）网关使专用子网中的实例能够连接到 **internet** 或其他 AWS 服务，但阻止 **internet** 启动与这些实例的连接。您需要在您的帐户中创建和使用 NAT 网关。NAT 网关小时使用率和数据处理率适用。亚马逊 EC2 数据传输费用也适用。IPv6 流量不支持 NAT 网关——请改用仅出口的 **internet** 网关。要创建 NAT 网关，必须指定 NAT 网关应驻留的公共子网。在创建 NAT 网关时，还必须指定与 NAT 网关关联的弹性 IP 地址。一旦将弹性 IP 地址与 NAT 网关关联，则无法更改该地址。创建 NAT 网关后，必须更新与一个或多个专用子网关联的路由表，以将 **Internet** 绑定流量指向 NAT 网关。这使专用子网中的实例能够：

与互联网通信。每个 NAT 网关都在特定的可用性区域中创建，并在该区域中实现冗余。您可以在可用性区域中创建的 NAT 网关数量有限制。

因此，正确的答案是在公共子网中部署 NAT 网关，并从承载 **web** 和应用层的私有子网向其添加路由。将 **web** 和应用层实例部署到私有子网，然后为每个 EC2 实例分配弹性 IP 地址是不正确的，因为弹性 IP 地址只是静态的公共 IPv4 地址。

在这种情况下，您必须使用 NAT 网关。

在专用子网中部署 NAT 网关并从承载 **web** 和应用层的公用子网向其添加路由是不正确的，因为您必须在公用子网中而不是在专用子网上部署 NAT gateway。

将 **web** 和应用层实例部署到公共子网，然后为每个 EC2 实例分配弹性 IP 地址是不正确的，因为具有 EIP 地址是不相关的，因为它只是静态的公共 IPv4 地址。此外，您应该将 **web** 和应用层部署在私有子网中，而不是公共子网中以使其无法从 **Internet** 访问，然后只添加 NAT 网关以允许出站 **Internet** 连接。参考：

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html> 查看此亚马逊 VPC 备忘单：

<https://tutorialsdojo.com/amazon-vpc/>

Dojo 的 AWS 认证解决方案架构师助理考试学习指南教程：<https://tutorialsdojo.com/aws-certified-solutions-architect-associate-saa-c02/>

Q250.一家公司在 AWS 云中托管了一个 **web** 应用程序，应用程序日志被发送到 **Amazon CloudWatch**。最近，**web** 应用程序遇到了一些错误，只需重新启动实例即可解决。

每当发生相同的应用程序错误时，您将如何自动重新启动 EC2 实例？

A、首先，查看现有 **CloudWatch** 日志中与应用程序错误相关的关键字，以创建自定义度量。然后，为该自定义度量创建一个 **CloudWatch** 警报，该警报调用一个操作来重新启动 EC2 实例。

B、首先，查看现有 **CloudWatch** 日志中与应用程序错误相关的关键字，以创建自定义度量。然后，在 **Amazon SNS** 中为该自定义指标创建一个警报，该警报将调用一个操作来重新启动 EC2 实例。

C、首先，查看与应用程序错误相关的关键字的现有流日志，以创建自定义度量。然后，为该自定义度量创建一个 **CloudWatch** 警报，该警报调用一个操作来重新启动 EC2 实例。

D、首先，查看与应用程序错误相关的关键字的现有流日志，以创建自定义度量。然后，为该自定义度量创建一个 **CloudWatch** 警报，该警报调用一个 **Lambda** 函数，该函数调用一个动作来重新启动 EC2 实例。

答:

分析:

在这个场景中，您可以查看现有 CloudWatch 日志中与应用程序错误相关的关键字，以创建自定义度量。然后，为该自定义度量创建一个 CloudWatch 警报，该警报调用一个操作来重新启动 EC2 实例。

您可以使用 Amazon CloudWatch 警报操作创建自动停止、终止、重新启动或恢复 EC2 实例的警报。当不再需要实例运行时，可以使用停止或终止操作来帮助节省资金。您可以使用重新启动和恢复操作自动重新启动这些实例，或者在发生系统损坏时将它们恢复到新硬件上。因此，正确的答案是：首先，查看现有 CloudWatch 日志中与应用程序错误相关的关键字，以创建自定义度量。然后，为该自定义度量创建一个 CloudWatch 警报，该警报调用一个操作来重新启动 EC2 实例。

该选项表示：首先，查看现有 CloudWatch 日志中与应用程序错误相关的关键字，以创建自定义度量。然后，在 Amazon SNS 中为调用重新启动 EC2 实例的操作的自定义度量创建警报是不正确的，因为您无法在 Amazon SNS 中创建警报。以下选项不正确，因为流日志在 VPC 中使用，而不是在特定 EC2 实例上使用：

-首先，查看与应用程序错误相关的关键字的现有流日志，以创建自定义度量。然后，为该自定义度量创建一个 CloudWatch 警报，该警报调用一个操作来重新启动 EC2 实例。

首先，查看与应用程序错误相关的关键字的现有流日志，以创建自定义度量。然后，为该自定义度量创建一个 CloudWatch 警报，该警报调用一个 Lambda 函数，该函数调用一个动作来重新启动 EC2 实例。参考：

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/UsingAlarmActions.html> 查看此 Amazon CloudWatch 备忘单：<https://tutorialsdojo.com/amazon-cloudwatch/>

Q251. 一家公司拥有数百个 VPC，这些 VPC 与跨越 5 个 AWS 区域的数据中心有多个 VPN 连接。随着工作量的增加，公司必须能够跨多个帐户和 VPC 扩展网络，以跟上潮流。解决方案架构师的任务是将公司的所有内部网络、VPN 和 VPC 互连到单个网关中，包括支持跨多个 AWS 区域的区域间对等。

以下哪项是架构师应设置的支持所需互连性的最佳解决方案？

A、为区域间 VPC 访问设置 AWS VPN CloudHub，并为内部数据中心的 VPN 连接设置直接连接网关。在每个 VPC 中创建一个虚拟专用网关，然后为每个 AWS 直连连接到直连网关创建一个专用虚拟接口。

B、设置 AWS 直接连接网关，以实现区域间专有网络访问所有 AWS 资源和内部数据中心。设置链路聚合组（LAG）以聚合单个 AWS Direct Connect 端点上的多个连接，以便将其视为单个受管连接。在每个 VPC 中启动虚拟专用网关，然后为每个 AWS 直连连接到直连网关创建公共虚拟接口。

C、启用区域间 VPC 对等，允许跨不同 AWS 区域的多个 VPC 之间建立对等关系。设置一个网络配置，确保流量始终保持在全球 AWS 主干上，并且永远不会穿过公共互联网。

D、在每个区域设置一个 AWS 过境网关，以互连其内的所有网络。然后，通过对等连接在传输网关之间路由流量。

答案 D

分析:

AWS Transit Gateway 是一项服务，使客户能够将其亚马逊虚拟私有云（VPC）及其内部网络连接到单个网关。随着 AWS 上运行的工作负载数量的增长，您需要能够跨多个帐户和 Amazon VPC 扩展网络，以跟上增长。

今天，您可以使用成对连接的 Amazon VPC。然而，在没有集中管理连接策略的能力的情况下管理许多 Amazon VPC 之间的点对点连接在操作上可能成本高昂且繁琐。对于内部连接，您需要将 AWS VPN 连接到每个单独的亚马逊 VPC。当 VPC 的数量增长到数百个时，这种解决方案的构建非常耗时，而且难以管理。

使用 AWS Transit Gateway，您只需创建和管理从中央网关到网络中每个亚马逊专有网络、内部数据中心或远程办公室的单个连接。交通网关作为一个枢纽，控制交通如何在所有连接的网络之间进行路由，这些网络就像辐条。由于每个网络只需连接到中转网关，而不需要连接到每个其他网络，因此这种中心辐射模型大大简化了管理并降低了运营成本。任何新的 VPC 只需连接到中转网关，然后自动可用于连接到中转网关的所有其他网络。这种易连接性使您可以随着网络的增长轻松扩展网络。

它充当虚拟专用云（VPC）和 VPN 连接之间流量的区域虚拟路由器。过境网关根据网络流量弹性伸缩。通过传输网关的路由在第 3 层运行，在该层中，数据包根据其目的地 IP 地址发送到特定的下一跳附件。

传输网关附件既是数据包的源，也是数据包的目的地。您可以将以下资源连接到您的过境网关：

- 一个或多个 VPC
- 一个或多个 VPN 连接
- 一个或多个 AWS 直接连接网关
- 一个或多个传输网关对等连接

如果连接传输网关对等连接，则传输网关必须位于不同的区域。因此，正确的答案是：在每个区域设置一个 AWS 过境网关，将其内的所有网络互连。然后，通过对等连接在中转网关之间路由流量。该选项表示：设置 AWS 直接连接网关，以实现区域间 VPC 访问所有 AWS 资源和内部数据中心。设置链路聚合组（LAG）以聚合单个 AWS Direct Connect 端点上的多个连接，以便将其视为单个受管连接。在每个 VPC 中启动虚拟专用网关，然后为每个 AWS 直接连接创建公共虚拟接口。与直接连接网关的连接不正确。只能创建到直接连接网关的专用虚拟接口，而不能创建公共虚拟接口。在这种情况下，使用链路聚合组（LAG）也无关紧要，因为它只是一个逻辑接口，使用链路聚集控制协议（LACP）在单个 AWS 直接连接端点聚合多个连接，允许您将其视为单个受管连接。选项表示：启用区域间 VPC 对等，这允许跨不同 AWS 区域的 VPC 之间建立对等关系。这将确保流量始终保持在 AWS 主干上，并且永远不会穿越公共互联网。与仅使用中转网关相比，这将需要大量的手动设置和管理开销来成功构建一个功能性、无错误的跨区域 VPC 网络。尽管区域间 VPC 对等提供了一种在区域间共享资源或复制数据以实现地理冗余的经济高效的方式，但其连接不是专用的且高度可用。此外，它不支持公司在多个 AWS 地区的内部数据中心。该选项表示：设置 AWS VPN CloudHub，用于跨区域 VPC 访问，并设置直接连接网关，用于与内部数据中心的 VPN 连接。在每个 VPC 中创建虚拟专用网关，然后为每个 AWS 直接连接创建专用虚拟接口。与直接连接网关的连接不正确。该选项不满足将公司所有内部网络、VPN 和 VPC 互连到单个网关的要求，其中包括支持跨多个 AWS 区域的区域间对等。顾名思义，AWS VPN CloudHub 仅适用于 VPN，不适用于 VPC。它还无法管理数百个 VPC，这些 VPC 与跨越多个 AWS 区域的数据中心有多个 VPN 连接。参考文献：

<https://aws.amazon.com/transit-gateway/>

<https://docs.aws.amazon.com/vpc/latest/tgw/how-transit-gateways-work.html>

<https://aws.amazon.com/blogs/networking-and-content-delivery/building-a-global-network-using-aws-传输网关区域间对等/>

查看 AWS 过境网关备忘单：<https://tutorialsdojo.com/aws-transit-gateway/>

Q252.一款流行的增强现实（AR）手机游戏大量使用了在 AWS 中托管的 RESTful API。该 API 使用 Amazon API 网关和具有预配置读写能力的 DynamoDB 表。根据您的系统监控，DynamoDB 表在高峰负载期间开始限制请求，这会导致游戏性能下降。

以下哪项可以提高应用程序的性能？

- A、 将 DynamoDB 表添加到自动缩放组。
- B、 在 DynamoDB 表前面创建一个 SQS 队列。
- C、 将应用程序负载均衡器与 DynamoDB 表集成。
- D、 使用 DynamoDB 自动缩放

答案 D

分析：

DynamoDB 自动伸缩使用 AWS 应用程序自动伸缩服务，根据实际流量模式，代表您动态调整配置的吞吐量。这使表或全局辅助索引能够增加其配置的读写容量，以处理流量的突然增加，而无需节流。当工作负载减少时，应用程序自动扩展会降低吞吐量，因此您不必为未使用的调配容量付费。

使用 DynamoDB 自动缩放是最好的答案。DynamoDB 自动缩放使用 AWS 应用程序自动缩放服务来代表您动态调整配置的吞吐量。将应用程序负载均衡器与 DynamoDB 表集成是不正确的，因为应用程序负载均衡器不适合与 DynamoDB 一起使用，此外，这不会增加 DynamoDB 表的吞吐量。

将 DynamoDB 表添加到自动缩放组是不正确的，因为您通常将 EC2 实例放在自动缩放组中，而不是 DynamoDB 表中。在 DynamoDB 表前面创建 SQS 队列是不正确的，因为这不是高吞吐量 DynamoDB 表的设计原则。使用 SQS 是为了处理排队和轮询请求。这不会增加这种情况下所需的 DynamoDB 的吞吐量。参考：

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/AutoScaling.html> 查看此 Amazon DynamoDB 备忘单：

<https://tutorialsdojo.com/amazon-dynamodb/>

亚马逊 DynamoDB 概述：

<https://www.youtube.com/watch?v=3ZOyUNleorU>

Q253.一项新的公司政策要求 IAM 用户将密码的最小长度更改为 12 个字符。在随机检查后，您发现仍有员工不遵守政策。如何自动检查和评估帐户的当前密码策略是否符合公司密码策略？

- A、 创建一个计划的 Lambda 函数，该函数将运行一个自定义脚本，定期检查密码更改的符合性。
- B、 创建 CloudTrail 轨迹。通过将属性设置为“事件名称”并将查找值设置为“更改密码”来过滤结果。这很容易为您提供更改密码的用户列表。
- C、 在 Amazon CloudWatch 事件中创建规则。构建事件模式以匹配 IAM 上的事件。在事件模式中将事件名称设置为“更改密码”。将 SNS 配置为在用户更改密码时向您发送通知。
- D、 配置 AWS 配置以触发定期检查用户密码合规性的评估。

答案 D

分析：

AWS 配置是一项服务，它使您能够评估、审核和评估 AWS 资源的配置。Config 持续监控和记录 AWS 资源配置，并允许您根据所需配置自动评估记录的配置。在给定的场景中，我们可以通过配置配置规则来检查帐户上的 IAM_password_policy，从而利用 AWS 配置来检查密码策略的合规性。此外，由于 Config 与 AWS 组织集成，我们可以改进设置，将跨帐户的合规信息聚合到中央仪表板。

因此，正确的答案是：配置 AWS 配置以触发评估，定期检查用户密码的合规性。

创建 CloudTrail 轨迹。通过将属性设置为“事件名称”并将查找值设置为“更改密码”。这很容易为您提供更改其密码的用户列表。这是不正确的，因为此设置只会提供更改其各自密码的用户的名称。它不能让您检查他们的密码是否满足要求的最小长度。

创建一个调度的 Lambda 函数，该函数将运行一个自定义脚本，定期检查密码更改的符合性。这是一个有效的解决方案，但仍然不正确。AWS 配置已与 AWS Lambda 集成。您不必创建和管理自己的 Lambda 函数。您只需要定义一个配置规则，在其中检查合规性，Lambda 将处理评估。此外，您不能通过使用 Lambda 本身直接创建调度函数。您必须在 AWS CloudWatch 事件中创建一个规则，以便按照您定义的时间表运行 Lambda 函数。在 Amazon CloudWatch 事件中创建规则。构建事件模式以匹配 IAM 上的事件。在事件模式中将事件名称设置为“更改密码”。将 SNS 配置为在用户更改密码时向您发送通知。这是不正确的，因为此设置只会在用户更改其密码时提醒您。当然，您将有关于谁进行了更改的信息，但这不足以检查它是否符合所需的最小密码长度。这可以在 AWS 配置中轻松完成。

参考文献：

<https://docs.aws.amazon.com/config/latest/developerguide/evaluate-config-rules.html><https://aws.amazon.com/config/>

查看 AWS 配置备忘单：<https://tutorialsdojo.com/aws-config/>

Q254.一家公司在 Amazon S3 中存储了 200 TB 的备份文件。这些文件采用供应商专有格式。解决方案架构师需要使用供应商的专有文件转换软件从 Amazon S3 存储桶中检索文件，将文件转换为行业标准格式，并将文件重新上传回 Amazon S3s。解决方案必须将数据传输成本降至最低。以下哪个选项可以满足给定要求？

- A、 使用 AWS 雪球边缘设备导出数据。在设备上安装文件转换软件。转换数据并重新上传到 Amazon S3。
- B、 在不同区域部署 EC2 实例。在实例上安装转换软件。执行数据转换并将其重新上传到 Amazon S3。
- C、 在 Amazon S3 中安装文件转换软件。使用 S3 批处理操作执行数据转换。
- D、 在与 Amazon S3 相同的区域部署 EC2 实例。在实例上安装文件转换软件。执行数据转换并将其重新上传到 Amazon S3。

答案 D

分析：

Amazon S3 是一种对象存储，用于存储和检索互联网上任何位置的任何数量的数据。它是一种简单的存储服务，以极低的成本提供业界领先的耐用性、可用性、性能、安全性和几乎无限的可扩展性。Amazon S3 的设计也非常灵活。存储所需的任何类型和数量的数据；读取同一条数据一百万次或仅用于紧急灾难恢复；构建简单的 FTP 应用程序或复杂的 web 应用程序。您支付所有进出 Amazon S3 的带宽，但以下情况除外：

- 从互联网传输的数据。

- 当 Amazon EC2 实例与 S3 bucket 位于同一 AWS 区域（包括同一 AWS 区域中的不同帐户）时，将数据传输到该实例。
- 数据传输到 Amazon CloudFront。

为了最小化数据传输费用，您需要将 EC2 实例部署在与 Amazon 相同的区域

S3.注意，在同一 AWS 区域中，S3 和 EC2 之间没有数据传输成本。在实例上安装转换软件以执行数据转换，并将数据重新上传到 Amazon S3。因此，正确答案是：将 EC2 实例部署在与 Amazon S3 相同的区域。在实例上，安装文件转换软件。执行数据转换并将其重新上传到 Amazon S3。该选项表示：在 Amazon S3 中安装文件转换软件。使用 S3 批处理操作执行数据转换是不正确的，因为不可能在 Amazon S3 中安装软件。S3 批操作只是在单个请求中运行多个 S3 操作。它无法与转换软件集成。

选项显示：使用 AWS Snowball Edge 设备导出数据。在设备上安装文件转换软件。转换数据并重新上传到 Amazon S3 是不正确的。虽然这是可能的，但在该场景中没有提到公司拥有内部数据中心。因此，不需要滚雪球。

该选项表示：在不同区域部署 EC2 实例。在实例上安装文件转换软件。执行数据转换并将其重新上传到 Amazon S3 是不正确的，因为这种方法不会最小化数据传输成本。您应该将实例部署在与 Amazon S3 相同的区域。

参考文献：

<https://aws.amazon.com/s3/pricing/> <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AmazonS3.html> 查

看此 Amazon S3 备忘单：<https://tutorialsdojo.com/amazon-s3/>

Q255.一个 web 应用程序需要至少六个随时运行的 Amazon 弹性计算云（EC2）实例。您的任务是将应用程序部署到欧盟-爱尔兰地区的三个可用区域（EU-west-1a、EU-west-1b 和 EU-west-1c）。要求系统具有容错性，直到丢失一个可用性区域。

以下哪种设置是最具成本效益的解决方案，同时还能保持系统的容错性？

- A、 欧盟西部 1a 中 2 例，欧盟西部 1b 中 2 例和欧盟西部 1c 中 2 例
- B、 欧盟西部 1a 中有 6 例，欧盟西部 1b 中 6 例，而欧盟西部 1c 中没有
- C、 欧盟西部 1a 中 6 例，欧盟西部 1b 中 6 例和欧盟西部 1c 中 6 例
- D、 欧盟西部 1a 中 3 例，欧盟西部 1b 中 3 例和欧盟西部 1c 中 3 例

答案 D

分析：

基本上，容错是系统在某些组件发生故障的情况下保持运行的能力，而不会出现任何服务降级。在 AWS 中，它还可以指运行 EC2 实例或资源的最小数量，这些实例或资源应始终运行，以便系统正确运行并服务于其消费者。请注意，这与高可用性的概念非常不同，高可用性只涉及在发生故障时至少有一个正在运行的实例或资源。在这种情况下，eu-west-1a 中的 3 个实例、eu-west-1b 中的 3 例和 eu-west-1c 中的 3 实例是正确答案，因为即

使其中一个可用区域发生中断，系统仍然满足至少 6 个运行实例的要求。这也是其他选择中最具成本效益的解决方案。

该选项表示：eu-west-1a 中有 6 个实例，eu-west-1b 中 6 个实例和 eu-west-1c 中 6 个实例，这是不正确的，因为尽管该解决方案为系统提供了最大的容错能力，但在 3 个 AZ 中维护总共 18 个实例需要大量成本。该选项表示：eu-west-1a 中的 2 个实例、eu-west-1b 中的 2 个实例和 eu-west-1c 中的 2 个实例是不正确的，因为如果一个可用区域发生故障，则只有 4 个运行实例可用。尽管这是最具成本效益的解决方案，但它不提供容错。该选项表示：eu-west-1a 中有 6 个实例，eu-west-1b 中有 6 个实例，eu-west-1c 中没有实例，这是不正确的，因为尽管它提供了容错能力，但与上述选项相比，它不是最具成本效益的解决方案。此解决方案有 12 个运行实例，而正确答案只有 9 个实例。

参考文献：

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-increase-availability.html>https://media.amazonwebservices.com/AWS_Building_Fault_tolerance_Applications.pdf

Q256.您所在的公司位于 ap-northeast-1 地区拥有一套 AWS 资源。您的 IT 经理要求您创建一个 AWS CLI shell 脚本，该脚本将调用 AWS 服务，如果 ap-northeast-1 区域出现故障，该服务可能会在另一个区域中创建重复资源。复制的资源还应包含 VPC 对等配置和主堆栈中的其他网络组件。

以下哪项 AWS 服务可以帮助完成此任务？

- A、AWS 云形成
- B、亚马逊光帆
- C、亚马逊社交网站
- D、亚马逊 SQS

答：

分析：

AWS CloudFormation 是一种帮助您建模和设置 Amazon Web 服务资源的服务，这样您就可以花更少的时间管理这些资源，而更多的时间关注在 AWS 中运行的应用程序。

您可以创建一个模板来描述您所需的所有 AWS 资源（如 Amazon EC2 实例或 Amazon RDS DB 实例），AWS CloudFormation 负责为您提供和配置这些资源。这样，您就可以将 AWS 架构的精确副本，以及托管在一个区域中的所有 AWS 资源部署到另一个区域。因此，正确答案是 AWS CloudFormation。

Amazon LightSail 是不正确的，因为您不能使用它复制 VPC 中的资源。您必须改用 CloudFormation。

Amazon SQS 和 Amazon SNS 都是错误的，因为 SNS 和 SQS 只是消息服务。

参考文献：

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/Welcome.html><https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/using-cfn-cli-creating-stack.html> 查看此 AWS CloudFormation 备忘单：<https://tutorialsdojo.com/aws-cloudformation/>

AWS CloudFormation-模板、堆栈和变更集: <https://www.youtube.com/watch?v=9Xpuprxg7aY>

Q257.一家技术公司正在构建一个新的加密货币交易平台，允许买卖比特币、以太坊、Ripple、Tether 和其他许多产品。您被聘为云工程师，负责构建新交易平台所需的基础设施。在工作的第一周，您开始创建 CloudFormation YAML 脚本，这些脚本定义了应用程序所需的所有 AWS 资源。您的经理对您没有立即创建 EC2 实例、S3 bucket 和其他 AWS 资源感到震惊。他不理解您所做的基于文本的脚本，并要求您澄清。

在这种情况下，使用 Amazon CloudFormation 服务的好处是什么，您应该告诉您的经理澄清他的担忧？（选择两个。）

- A、支持整个 AWS 基础架构的建模、配置和版本控制
- B、允许您在文本文件中建模整个基础结构
- C、应用程序代码的存储位置
- D、提供高度耐用和可扩展的数据存储
- E、使用 CloudFormation 本身是免费的，包括已经创建的 AWS 资源。

回答 AB

分析:

AWS CloudFormation 为您提供了一种通用语言，用于描述和提供云环境中的所有基础设施资源。CloudFormation 允许您使用一个简单的文本文件，以自动化和安全的方式建模和提供应用程序跨所有区域和帐户所需的所有资源。该文件是云环境的唯一真实来源。AWS CloudFormation 免费提供，您只需支付运行应用程序所需的 AWS 资源。

因此，正确答案是：

- 支持整个 AWS 基础架构的建模、配置和版本控制
- 允许您在文本文件对整个基础设施进行建模。因为 CloudFormation 不是一种数据存储服务，所以“提供高度持久和可扩展的数据存储”选项是不正确的。表示：应用程序代码的存储位置不正确，因为 CloudFormation 不用于存储应用程序代码。您必须使用 CodeCommit 作为代码库，而不是 CloudFormation。

“使用云信息本身是免费的，包括已创建的 AWS 资源”选项是不正确的，因为尽管使用云信息服务是免费的但您必须支付您创建的 AWS 资源的费用。参考文献: <https://aws.amazon.com/cloudformation/>

<https://aws.amazon.com/cloudformation/faqs/>查看此 AWS CloudFormation 备忘单:

<https://tutorialsdojo.com/aws-cloudformation/>

Q258.一家使用机器学习收集和分析消费者数据的数据分析公司正在使用红移集群作为其数据仓库。指示您为其系统实施灾难恢复计划，以确保即使在 AWS 地区停机的情况下也能保持业务连续性。以下哪项是满足此要求的最佳方法？

- A、在 Amazon Redshift 集群中启用跨区域快照复制。

B、创建一个调度作业，该作业将自动获取红移集群的快照，并将其存储到 S3 存储桶中。
在 AWS 区域停机的情况下恢复快照。C、使用红移

群集的自动快照。

D、什么都不做，因为 Amazon Redshift 是一个高度可用、完全管理的数据仓库，可以承受整个 AWS 区域的中断。

答:

分析:

您可以将 Amazon Redshift 配置为将集群的快照复制到另一个区域。要配置跨区域快照复制，您需要为每个集群启用此复制功能，并配置在何处复制快照以及在目标区域中保留复制的自动快照的时间。为群集启用跨区域复制时，所有新的手动和自动快照都将复制到指定区域。该选项表示：创建一个调度作业，该作业将自动获取红移集群的快照，并将其存储到 S3 存储桶中。在 AWS 区域停机的情况下恢复快照是不正确的，因为尽管此选项是可能的，但这需要大量手动工作，因此不是最佳选项。

您应该改为配置跨区域快照副本。

“因为 Amazon Redshift 是一个高度可用的、完全管理的数据仓库，可以承受整个 AWS 区域的中断，所以什么都不做”的选项是不正确的，因为尽管 Amazon Redshift 是完全管理的数据库，但您仍然需要配置跨区域快照拷贝，以确保数据正确复制到另一个区域。使用红移集群的自动快照是不正确的，因为使用自动快照是不够的，并且在整个 AWS 区域关闭的情况下将不可用。参考：<https://docs.aws.amazon.com/redshift/latest/mgmt/managing-snapshots-console.html> 亚马逊红移概述：

<https://youtu.be/jlLERNzhHOg>

查看此亚马逊红移备忘单：<https://tutorialsdojo.com/amazon-redshift/>

Q259.一家公司在 AWS 中有一个分布式应用程序，它周期性地跨多个实例处理大量数据。解决方案架构师将应用程序设计为从任何实例故障中优雅地恢复。然后要求他以最具成本效益的方式启动应用程序。哪种类型的 EC2 实例将满足此要求？

- A、专用实例
- B、保留实例
- C、现场实例
- D、按需实例

答案 C

分析:

您需要一个 EC2 实例，它是其他类型中最具成本效益的。此外，它将承载的应用程序被设计为在实例失败的情况下进行正常恢复。

就成本效益而言，现货和保留实例是首选。由于应用程序可以从实例故障中优雅地恢复，因此 Spot 实例是这种情况下的最佳选择，因为它是最便宜的 EC2 实例类型。请记住，使用 Spot 实例时，会有中断。Amazon EC2 can

当现货价格超过最高价格、现货实例需求增加或现货实例供应减少时，中断现货实例。因此，正确答案是：点实例。

保留实例不正确。虽然您也可以使用保留实例来节省成本，但这需要承诺 1 年或 3 年的使用期限。由于您的流程仅定期运行，因此您将无法最大化使用保留实例的折扣价格。专用实例和按需实例也是不正确的，因为专用实例和按需实例不是用于应用程序的经济有效的解决方案。参考：

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/how-spot-instances-work.html> 查看此 Amazon EC2 备忘单：

<https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/> 以下是对 Spot 实例的深入了解：

<https://youtu.be/PKvss-RgSjI>

Q260. 一家公司计划将 NoSQL 数据库迁移到 EC2 实例。数据库被配置为自动复制数据，以保持数据的多个副本以备冗余。解决方案架构师需要启动具有高 IOPS 和顺序读/写访问的实例。如果 I/O 吞吐量是最高优先级，以下哪种选项满足要求？

- A、使用 EBS 卷的通用实例。
- B、使用 EBS 卷的内存优化实例。
- C、使用具有实例存储卷的存储优化实例。
- D、使用实例存储卷计算优化实例。

答案 C

分析：

AmazonEC2 提供了广泛的实例类型选择，并针对不同的用例进行了优化。实例类型包括 CPU、内存、存储和网络容量的不同组合，使您能够灵活地为应用程序选择适当的资源组合。每个实例类型都包括一个或多个实例大小，允许您根据目标工作负载的需求扩展资源。存储优化实例是为需要对本地存储上的非常大的数据集进行高顺序读写访问的工作负载而设计的。它们经过优化，可向应用程序提供每秒数万次低延迟随机 I/O 操作

（IOPS）。某些实例类型可以驱动比单个 EBS 卷更多的 I/O 吞吐量。您可以在 RAID 0 配置中将多个卷连接在一起，以使用这些实例的可用带宽。基于给定场景，NoSQL 数据库将迁移到 EC2 实例。NoSQL 数据库的合适实例类型是 I3 和 I3en 实例。此外，I3 和 I3en 实例的主要数据存储是非易失性内存快速（NVMe）SSD 实例存储卷。由于数据是自动复制的，因此使用实例存储卷不会有问题。因此，正确的答案是：使用具有实例存储卷的存储优化实例。“使用具有实例存储卷的计算优化实例”选项是不正确的，因为这种类型的实例非常适合于受益于高性能处理器的计算绑定应用程序。它不适用于 NoSQL 数据库。“使用 EBS 卷的通用实例”选项不正确，因为该实例仅提供计算、内存和网络资源的平衡。请注意，场景中的要求是高顺序读写访问。因此，必须使用存储优化实例。

“使用 EBS 卷的内存优化实例”选项不正确。尽管这种类型的实例适用于 NoSQL 数据库，但它不适用于需要对本地存储上的非常大的数据集进行高顺序读写访问的工作负载。参考文献：

[https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/storage-optimized-](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/storage-optimized-instances.html)

[instances.htmlhttps://docs.aws.amazon.com/AWSEC2/latest/UserGuide/instance-types.html](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/instance-types.html) Amazon EC2 概述：

https://www.youtube.com/watch?v=7VsGIHT_jQE

查看此 Amazon EC2 备忘单: <https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/>

Q261. 一家公司正在使用按需应变 EC2 实例来托管使用亚马逊实例商店支持的 AMI 的传统 web 应用程序。web 应用程序应该尽快退役, 因此需要终止 EC2 实例。

当实例终止时, 根卷上的数据会发生什么变化?

- A、数据自动保存为 EBS 快照。
- B、在实例重新启动之前, 数据不可用。
- C、数据将自动删除。
- D、数据自动保存为 EBS 卷。

答案 C

分析:

AMI 被分类为由 Amazon EBS 支持或由实例存储支持。前者意味着:

从 AMI 启动的实例的根设备是从 AmazonEBS 快照创建的 AmazonEBS 卷。后者意味着从 AMI 启动的实例的根设备是从 Amazon S3 中存储的模板创建的实例存储卷。

实例存储卷上的数据仅在实例的生命周期内保持, 这意味着如果实例终止, 数据将自动删除。因此, 正确答案是: 数据自动删除。参考:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ComponentsAMIs.html> Dojo 的 AWS 认证解决方案架构师助理考试学习指南教程:

<https://tutorialsdojo.com/aws-certified-solutions-architect-associate/>

Q262. 一家公司正在使用 AWS 目录服务, 通过 AD 连接器将其内部 Microsoft Active Directory (AD) 域与其 Amazon EC2 实例集成。以下基于身份的策略附加到使用 AWS 目录服务的 IAM 身份:

```
{  
  "版本": "2012-10-17", "声明": [  
    {  
      "Sid":  
      "DirectoryTutorialsDojo1234",  
      "效果": "允许",  
      "行动": [  
        "ds:"
```



```

], "资源": "arn:aws:ds:us-east-1:987654321012:目录/d-1234567890"11.} {

"效果": "允许",

"行动": [

"ec2:"

], "资源": "*"

}

]

}

```

以下哪项最能描述上述资源策略的功能？

A、 允许所有 AWS 目录服务（ds）调用，只要资源包含以下目录名：

目录教程 Dojo1234

B、 允许所有 AWS 目录服务（ds）调用，只要资源包含目录 ID：

987654321012

C、 允许所有 AWS 目录服务（ds）调用，只要资源包含目录 ID：

目录教程 Dojo1234

D、 允许所有 AWS 目录服务（ds）调用，只要资源包含目录 ID:D-1234567890

答案 D

分析：

AWS 目录服务提供了多种方式将亚马逊云目录和 Microsoft Active Directory（AD）与其他 AWS 服务一起使用。目录存储有关用户、组和设备的消息，管理员使用它们来管理对信息和资源的访问。AWS 目录服务为希望在云中使用现有 Microsoft AD 或轻量级目录访问协议（LDAP）软件应用程序的客户提供了多种目录选择。它还为需要目录来管理用户、组、设备和访问的开发人员提供了相同的选择。

每个 AWS 资源都由 AWS 帐户拥有，创建或访问资源的权限由权限策略控制。帐户管理员可以将权限策略附加到 IAM 标识（即用户、组和角色），某些服务（如 AWS Lambda）也支持将权限策略添加到资源。

以下资源策略示例允许所有 ds 调用，只要资源包含目录 ID“d1234567890”。

```

{

"版本": "2012-10-17", "声明": [

```

```

{
  "Sid": "VisualEditor0",
  "效果": "允许",
  "行动": [
    "ds:"

  ], "资源": "arn:aws:ds:us-east-1:123456789012:目录/d-1234567890", {
  "效果": "允许",
  "行动": [
    "ec2:"

  ], "资源": "*"
}
]
}

```

因此，正确答案是这样的选项：允许所有 AWS 目录服务（ds）调用，只要资源包含目录 ID:d-1234567890。

表示：允许所有 AWS 目录服务（ds）调用，只要资源包含目录 ID:DirectoryTutorialsDojo1234 的选项不正确，因为 DirectoryTutorialsDojo1234 是语句 ID（SID），而不是目录 ID。

“允许所有 AWS 目录服务（ds）调用，只要资源包含目录 ID:987654321012”的选项不正确，因为号码：987654321012 是帐户 ID 而不是目录 ID。

如果资源包含目录名：DirectoryTutorialsDojo1234，则表示：允许所有 AWS 目录服务（ds）调用的选项不正确，因为 DirectoryTutorialsDojo1234 是语句 ID（SID），而不是目录名。

Q263. 一家公司最近推出了一个在欧盟东部地区运行的电子商务应用程序，该应用程序严格要求始终运行六个 EC2 实例。在该地区，有 3 个可用区域（AZ）可供您使用-eu-east-2a、eu-east-2b 和 eu-east-2c。

如果区域中的任何单个 AZ 不可用，以下哪种部署提供 100%的容错能力？（选择两个。）

A、 eu-east-2a 具有四个 EC2 实例，eu-east-2b 具有两个 EC2 示例，eu-east-2c 具有两个 EC2 实例

B、 eu-east-2a 具有两个 EC2 实例，eu-east-2b 具有四个 EC2 示例，eu-east-2c 具有两个 EC2 实例

- C、具有六个 EC2 实例的 eu-east-2a、具有六个 EC2 实例的欧盟-east-2b 和不具有 EC2 实例
- D、 eu-east-2a 具有三个 EC2 实例， eu-east-2b 具有三个 EC2 实例，而 eu-east-2c 具有三个 EC2 实例
- E、 eu-east-2a 具有两个 EC2 实例， eu-east-2b 具有两个 EC2 实例，而 eu-east-2c 具有两个 EC2 实例

对裁谈会的答复

分析：

容错是指即使用于构建系统的某些组件发生故障，系统仍能保持运行的能力。在 AWS 中，这意味着在服务器故障或系统故障的情况下，运行 EC2 实例的数量不应低于系统正常工作所需的最小实例数量。因此，如果应用程序至少需要 6 个实例，则在其中一个可用性区域发生中断或出现服务器问题时，应至少运行 6 个实例。在这种情况下，您必须模拟每个选项都有一个可用性区域不可用的情况，并检查它是否仍有 6 个正在运行的实例。因此，正确的答案是：eu-east-2a 有六个 EC2 实例， eu-east-2b 有六个 EC2 实例，以及 eu-east-2c 没有 EC2 实例和 eueast-2a 有三个 EC2 示例， eu-east-2b 三个 EC3 实例，以及欧盟-east-2c 三个 EC4 实例，因为即使其中一个可用区发生故障，仍会有 6 个活动实例。

参考：https://media.amazonwebservices.com/AWS_Building_Fault_Tolerant_Applications.pdf

Q264.新聘用的解决方案架构师正在检查公司 AWS 资源的所有安全组和网络访问控制列表规则。出于安全目的，应保护通过数据库层端口 1433 的 MS SQL 连接。以下是其 Microsoft SQL Server 数据库的安全组配置：托管在 EC2 实例的自动扩展组中的应用层是唯一需要连接到数据库的已标识资源。架构师应确保架构符合授予最低特权的最佳实践。

应对安全组配置进行以下哪些更改？

- A、对于 MS SQL 规则，将源更改为附加到应用层的网络 ACL ID。
- B、对于 MS SQL 规则，将源更改为附加到应用层的安全组 ID。
- C、对于 MS SQL 规则，将源更改为自动缩放组的基础实例的 EC2 实例 ID。
- D、对于 MS SQL 规则，将源更改为附加到应用层的静态选播 IP 地址。

答案 B

分析：

安全组充当实例的虚拟防火墙，以控制入站和出站流量。在 VPC 中启动实例时，最多可以为该实例分配五个安全组。安全组在实例级别而不是子网级别执行操作。因此，可以将 VPC 子网中的每个实例分配给一组不同的安全组。

如果您使用 Amazon EC2 API 或命令行工具启动实例，并且未指定安全组，则该实例将自动分配给 VPC 的默认安全组。如果使用 Amazon EC2 控制台启动实例，则可以选择为该实例创建新的安全组。

对于每个安全组，您将添加控制实例入站流量的规则，以及控制出站流量的单独规则集。本节介绍了您需要了解的有关 VPC 安全组及其规则的基本信息。

亚马逊安全组和网络 ACL 不会过滤到或来自链路本地地址（169.254.0.0/16）或 AWS 保留 IPv4 地址（这是子网的前四个 IPv4 地址，包括专有网络的亚马逊 DNS 服务器地址）的流量。类似地，流日志不捕获进出这些地址的 IP 流量。

在这种情况下，安全组配置允许来自任何地方的任何服务器（0.0.0/0）通过 1433 端口建立与数据库的 MS SQL 连接。这里最合适的解决方案是将源字段更改为附加到应用层的安全组 ID。因此，正确的答案是这样的选项：对于 MS SQL 规则，将源更改为附加到应用层的安全组 ID。表示：对于 MS SQL 规则，将源更改为自动缩放组的基础实例的 EC2 实例 ID 的选项不正确，因为使用自动缩放组基础实例的 EC2 实例 ID 作为源可能会导致间歇性问题。随着时间的推移，将添加新实例，并从自动缩放组中删除旧实例，这意味着您必须再次手动更新安全组设置。更好的解决方案是使用 EC2 实例的自动扩展组的安全组 ID。

表示：对于 MS SQL 规则，将源更改为附加到应用层的静态选播 IP 地址的选项不正确，因为静态选播地址主要用于 AWS 全局加速器，而不用于安全组配置。该选项表示：对于 MS SQL 规则，将源更改为网络 ACL 附加到应用层的 ID 不正确，因为您必须使用安全组 ID 而不是应用层的网络 ACL ID。请注意，网络 ACL 覆盖整个子网，这意味着使用相同子网的其他应用程序也将受到影响。

参考文献：

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.htmlhttps://docs.aws.amazon.com/vpc/latest/userguide/vpc_Security.html

Q265. 一家公司有一组 Linux 服务器运行在多个按需 EC2 实例上。审计团队希望收集和处理从这些服务器生成的应用程序日志文件，以用于其报告。在这种情况下，以下哪项服务最适合使用？

- A、 Amazon S3 Glacier Deep Archive 用于存储应用程序日志文件，AWS ParallelCluster 用于处理日志文件。
- B、 Amazon S3 用于存储应用程序日志文件，Amazon Elastic MapReduce 用于处理日志文件。
- C、 用于存储和处理日志文件的单个按需 Amazon EC2 实例
- D、 Amazon S3 Glacier 用于存储应用程序日志文件，Spot EC2 实例用于处理它们。

答案 B

分析：

Amazon EMR 是一个托管集群平台，它简化了在 AWS 上运行大数据框架，如 Apache Hadoop 和 Apache Spark，以处理和分析大量数据。通过使用这些框架和相关的开源项目，如 Apache Hive 和 Apache Pig，您可以为分析目的和商业智能工作负载处理数据。此外，您还可以使用 Amazon EMR 将大量数据转换和移出其他 AWS 数据存储和数据库，如 Amazon 简单存储服务（Amazon S3）和 Amazon DynamoDB。

因此，正确答案是：Amazon S3 用于存储应用程序日志文件，Amazon 弹性 MapReduce 用于处理日志文件。

该选项表示：Amazon S3 Glacier 用于存储应用程序日志文件，Spot EC2 实例用于处理它们，这是不正确的，因为 Amazon S3Glaciers 仅用于数据存档。该选项表示：单个按需 Amazon EC2 实例用于存储和处理日志文件是不正确的，因为 EC2 实例不是推荐的存储服务。此外，Amazon EC2 没有内置的数据处理引擎来处理大量数据。表示：Amazon S3 Glacier Deep Archive 用于存储应用程序日志文件，AWS ParallelCluster 用于处理日志文件的选项是不正确的，因为 Amazon S3 Glagier DeepArchive 的检索时间长，因此此选项不适用。此外，AWS ParallelCluster 只是一个 AWS 支持的开源集群管理工具，它使您可以轻松地在 AWS 上部署和管理高性能计算（HPC）集群。ParallelCluster 使用一个简单的文本文件，以自动化和安全的方式对 HPC 应用程序所需的所有资源进行建模和配置。

Q266.一家初创公司在新创建的具有默认设置的 VPC 中使用按需 EC2 实例启动了一个新的 FTP 服务器。服务器不应公开访问，只能通过 IP 地址 45.116.100 访问，而不能通过其他任何地方访问。

以下哪种方法最适合实施此要求？

A、在 EC2 实例的安全组中创建一个新的入站规则，详细信息如下：

协议：TCP 端口范围：20-21 来源：175.45.116.100/32

B、在 EC2 实例的子网中创建新的网络 ACL 入站规则，详细信息如下：

协议：TCP

端口范围：20-21

资料来源：175.45.116.100/0

允许/拒绝：允许

C、在 EC2 实例的子网中创建新的网络 ACL 入站规则，详细信息如下：

协议：UDP

端口范围：20-21

资料来源：175.45.116.100/0

允许/拒绝：允许

D、在 EC2 实例的安全组中创建一个新的入站规则，详细信息如下：

协议：UDP

端口范围：20-21

资料来源：175.45.116.100/32

答：

分析：

FTP 协议通过端口 20 和 21 使用 TCP。这应该在安全组或网络 ACL 入站规则中配置。根据场景的要求，您应该只允许客户端的单个 IP，而不是整个网络。因此，在源代码中，应使用适当的 CIDR 符号。/32 表示一个 IP 地址，/0 表示整个网络。在场景中，您使用默认设置在新创建的 VPC 中启动了 EC2 实例。您的 VPC 自动附带可修改的默认网络 ACL。默认情况下，它允许所有入站和出站 IPv4 流量以及 IPv6 流量（如果适用）。因此，如果 VPC 具有默认设置，则实际上不需要显式地将入站规则添加到网络 ACL 以允许入站流量。

以下选项不正确：

在 EC2 实例的安全组中创建一个新的入站规则，详细信息如下：

协议：UDP

端口范围：20-21

资料来源：175.45.116.100/32

虽然安全组的配置有效，但提供的协议不正确。请注意，FTP 使用 TCP 而不是 UDP。

以下选项也不正确：

在 EC2 实例的子网中创建新的网络 ACL 入站规则，详细信息如下：

协议：TCP

端口范围：20-21

资料来源：175.45.116.100/0

允许/拒绝：允许

虽然设置入站网络 ACL 有效，但源无效，因为它必须是 IPv4 或 IPv6 CIDR 块。在提供的 IP 地址中，/0 表示整个网络，而不是特定的 IP 地址。此外，在场景中，新创建的 VPC 具有默认设置，默认情况下，网络 ACL 允许所有流量。这意味着实际上不需要配置网络 ACL。

同样，以下选项也不正确：

在 EC2 实例的子网中创建新的网络 ACL 入站规则，详细信息如下：

协议：UDP

端口范围：20-21

资料来源：175.45.116.100/0

允许/拒绝：允许

正如上面所述，源代码也是无效的。请注意，FTP 使用 TCP 而不是 UDP，这是

这个选项错误的原因。此外，在场景中，新创建的 VPC 具有默认设置，默认情况下，网络 ACL 允许所有流量。这意味着实际上不需要配置网络 ACL。

参考文献：

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html> 查看此亚马逊专有网络备忘单：<https://tutorialsdojo.com/amazon-vpc/>

Q267.一家公司正在使用自动缩放组，该组被配置为在应用程序负载显著增加时启动新的 **t2.micro** EC2 实例。为了满足需求，您现在需要用更大的 **t2.2xlarge** 实例类型替换这些实例。您将如何实施此更改？

- A、手动更改每个 EC2 实例的实例类型。
- B、使用新实例类型创建新启动配置，并更新自动缩放组。
- C、只需在当前启动配置中将实例类型更改为 **t2.2xlarge**
- D、创建另一个自动缩放组并附加新实例类型。

答案 B

分析：

一次只能为自动缩放组指定一个启动配置，并且在创建启动配置后不能修改启动配置。因此，如果要更改自动缩放组的启动配置，则必须创建启动配置，然后使用新的启动配置更新自动缩放组。

因此，正确的答案是：使用新实例类型创建新的启动配置，并更新自动缩放组。

在当前启动配置中，只需将实例类型更改为 **t2.2xlarge** 的选项是不正确的，因为一旦创建启动配置，就无法更改启动配置。您必须创建一个新的。“创建另一个自动缩放组并附加新实例类型”选项不正确，因为无法直接将新实例类型附加或声明到自动缩放组。您必须首先使用新实例类型创建新的启动配置，然后将其附加到现有的自动缩放组。“手动更改每个 EC2 实例的实例类型”选项不正确，因为您不能直接更改 EC2 实例类型。这应该通过创建一个全新的启动配置，然后将其连接到现有的自动缩放组来完成。

参考文献：

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/LaunchConfiguration.html>

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/create-asg.html> 查看此 AWS 自动缩放备忘单：

<https://tutorialsdojo.com/aws-auto-scaling/>

Q268.一家公司在其内部数据中心拥有两层环境，由应用层和数据库层组成。我们指示您将其环境迁移到 AWS 云，并按照以下要求设计其 VPC 中的子网：

- 1.
- 2.有一个应用负载均衡器，它将在应用层中的服务器之间分配传入流量。2.应用层和数据库层不能从公共互联网访问。应用层应该只接受来自负载均衡器的流量。3.数据库层包含非常敏感的数据。它不能与其他 AWS 资源共享同一子网

具有环境中其他实例的自定义路由表。4.环境必须高度可用并且可扩展以处理因特网上的输入流量激增。

3.

您应该创建多少子网来满足上述要求？

A、 4

B、 6

C、 3

D、 2

答案 B

分析：

给定的场景表明，要成功地将两层环境从本地数据中心迁移到 AWS 云，需要满足 4 个要求。第一个要求意味着您必须使用应用程序负载平衡器（ALB）将传入流量分配到应用程序服务器。第二个要求指定应用程序层和数据库层都不能从访问

公共互联网。这意味着您可以为应用程序层和数据库层创建单个专用子网。然而，第三项要求提到，数据库层不应与其他 AWS 资源共享同一子网，以保护其敏感数据。这意味着您应该为应用层提供一个专用子网，为数据库层提供另一个专用子网。最后一个要求暗示需要使用至少两个

可用性区域以实现高可用性。这意味着您必须将应用程序服务器分配到两个 AZ 以及数据库，可以使用主从配置进行设置，以便在两个区域之间正确复制数据。如果同一可用性区域中有多个私有子网，其中包含需要向负载均衡器注册的实例，则只需要创建一个公共子网。每个可用性区域只需要一个公共子网；您可以将私有实例添加到驻留在该特定可用性区域中的所有私有子网中。

由于您有一个面向 internet 的公共负载平衡器，它有一组部署在私有子网中的后端 Amazon EC2 实例，因此必须在相同的可用性区域中创建相应的公共子网。这个新的公共子网位于专用 EC2 实例使用的专用子网之上。最后，您应该将这些公共子网与面向 Internet 的负载均衡器关联，以完成

设置。

总之，我们需要一个专用子网用于应用层，另一个用于数据库层。然后，我们需要在托管私有 EC2 实例的同一可用性区域中创建另一个公共子网，以便将面向 Internet 的公共负载平衡器正确连接到您的实例。这意味着我们必须使用总共 3 个子网，包括 2 个私有子网和 1 个公共子网。为了满足高可用性的要求，我们必须将堆栈部署到两个可用性区域。这意味着您必须将正在使用的子网数量增加一倍。还要注意，您必须在专用 EC2 服务器的同一可用性区域中创建相应的公共子网，以便它与负载均衡器正确通信。

因此，正确答案是 6 个子网。

参考文献：

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Scenario2.html

<https://aws.amazon.com/premiumsupport/knowledge-center/public-load-balancer-private-ec2/>查看此亚马逊 VPC 备忘单：

<https://tutorialsdojo.com/amazon-vpc/>

Q269.一家金融公司正在为其在线交易平台设计应用程序架构，该架构必须具有高可用性和容错性。他们的解决方案架构师将应用程序配置为使用位于美国东部地区的 Amazon S3 存储桶来存储大量日内财务数据。即使其中一个可用区域发生中断或区域服务故障，存储桶中存储的财务数据也不得受到影响。

架构师应该如何避免任何代价高昂的服务中断并确保数据的持久性？

- A、 创建生命周期策略，定期将 S3 存储桶备份到 Amazon Glacier。
- B、 将 S3 存储桶复制到支持 EBS 的 EC2 实例。
- C、 在另一个区域创建新的 S3 存储桶，并配置对位于 us-east-1 的存储桶的跨账户访问。
- D、 启用跨区域复制。

答案 D

分析：

在这种情况下，您需要启用跨区域复制，以确保您的 S3 存储桶不会受到影响，即使其中一个可用性区域发生中断或 us-east-1 中的区域服务故障。当您在 S3 中上传数据时，您的对象将冗余存储在您创建存储桶的区域内多个设施的多个设备上。因此，如果整个区域发生中断，如果不启用跨区域复制，则 S3 存储桶将不可用，这将使您的数据可用于其他区域。

请注意，可用性区域（AZ）与 Amazon EC2 实例而不是 Amazon S3 更相关，因此，如果 AZ 中出现任何中断，S3 存储桶通常不受影响，而仅受部署在该区域上的 EC2 实例的影响。

因此，正确答案是：启用跨区域复制。“将 S3 存储桶复制到 EBS 备份的 EC2 实例”选项是不正确的，因为 EBS 不像 Amazon S3 那样耐用。此外，如果承载卷的可用性区域下降，则数据也将无法访问。“创建生命周期策略以定期将 S3 存储桶备份到 Amazon Glacier”的选项是不正确的，因为 Glaciers 主要用于数据存档。您还需要将数据复制到另一个区域以获得更好的耐用性。

“在另一个区域创建一个新的 S3 存储桶，并配置对位于 us-east-1 的存储桶的跨帐户访问”选项是不正确的，因为如果您希望将对象的访问权限授予另一个 AWS 帐户，而不仅仅是授予另一 AWS 区域，则主要使用亚马逊 S3 中的跨帐户权限。例如，帐户马尼拉可以授予另一个 AWS 帐户（帐户宿务）访问其资源（如桶和对象）的权限。S3 跨帐户访问不会将数据从一个区域复制到另一个区域。更好的解决方案是启用跨区域复制（CRR）。参考文献：

<https://aws.amazon.com/s3/faqs/>

<https://aws.amazon.com/s3/features/replication/>

查看此 Amazon S3 备忘单：<https://tutorialsdojo.com/amazon-s3/>

Q270.web 应用程序托管在应用程序负载均衡器后面跨多个可用性区域部署的 EC2 实例的自动扩展组中。您需要为您的系统实现 SSL 解决方案以提高其安全性，这就是为什么您向第三方证书颁发机构（CA）请求 SSL/TLS 证书的原因。

在哪里可以安全地导入应用程序的 SSL/TLS 证书？（选择两个。）

- A、 一个 S3 存储桶，配置有服务器端加密和客户提供的加密密钥（SSE-C）。B.AWS 证书管理器
- C、 启用版本控制的私有 S3 存储桶
- D、 云锋
- E、 IAM 证书存储

答案 B

分析：

如果您从第三方 CA 获得证书，请将证书导入 ACM 或将其上载到 IAM 证书存储。因此，AWS 证书管理器和 IAM 证书存储是正确答案。ACM 允许您从 ACM 控制台以编程方式导入第三方证书。如果您所在地区没有 ACM，请使用 AWS CLI 将第三方证书上载到 IAM 证书存储区。启用版本控制的私有 S3 存储桶和配置有客户提供的加密密钥（SSE-C）的服务器端加密的 S3 存储池都不正确，因为 S3 不是存储 SSL 证书的合适服务。

CloudFront 不正确。虽然您可以将证书上传到 CloudFront，但这并不意味着您可以在其上导入 SSL 证书。您将无法导出在 CloudFront 中加载的证书，也无法将其分配给 EC2 或 ELB 实例，因为它将绑定到单个 CloudFront 发行版。

参考：

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/cnames-and-https-procedures.html#cname> 和 https 上传证书

查看此 Amazon CloudFront 备忘单：

<https://tutorialsdojo.com/amazon-cloudfront/>

AWS 安全服务概述-机密管理器、ACM、Macie: <https://www.youtube.com/watch?v=ogVamzF2Dzk>

Dojo 的 AWS 认证解决方案架构师助理考试学习指南教程: <https://tutorialsdojo.com/aws-certified-solutions-architect-associate-saa-c02/>

Q271. 一家公司有一个托管在按需应变 EC2 实例中的 web 应用程序。您正在创建一个需要实例的公共和私有 IP 地址的 shell 脚本。获取您的 shell 脚本可以使用的实例关联 IP 地址的最佳方法是什么？

- A、 通过使用 Curl 或 Get 命令从 <http://169.254.169.254/latest/meta-data/>
- B、 通过使用 CloudWatch 度量。
- C、 通过使用 Curl 或 Get 命令从 <http://169.254.169.254/latest/user-data/>
- D、 通过使用 IAM。

答：

分析：

实例元数据是有关 EC2 实例的数据，可用于配置或管理正在运行的实例。由于您的实例元数据可以从正在运行的实例中获得，因此不需要使用 Amazon EC2 控制台或 AWS CLI。在编写脚本以从实例运行时，这可能很有帮助。例如，您可以从实例元数据访问实例的本地 IP 地址，以管理与外部应用程序的连接。

要查看运行实例中的私有 IPv4 地址、公共 IPv4 地址和所有其他类别的实例元数据，请使用以下

URL: <http://169.254.169.254/latest/meta-data/>

参考:

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-metadata.html> 查看此 Amazon EC2 备忘单:

<https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/Dojo> 的 AWS 认证解决方案架构师助理

考试学习指南教程: <https://tutorialsdojo.com/aws-certified-solutions-architect-associate/>

Q272. 公司需要使用 IAM 将本地数据中心的轻量级目录访问协议 (LDAP) 目录服务集成到 AWS VPC。当前正在使用的标识存储与 SAML 不兼容。

以下哪项提供了实现集成的最有效方法?

- A、使用引用 LDAP 标识符和 AWS 凭据的 IAM 策略。
- B、使用 AWS 单点登录 (SSO) 服务在 AWS 和 LDAP 之间启用单点登录。
- C、开发本地自定义身份代理应用程序，并使用 STS 发布短期 AWS 凭据。
- D、每当更新 LDAP 凭据时，使用 IAM 角色旋转 IAM 凭据。

答案 C

分析:

如果您的身份存储与 SAML 2.0 不兼容，那么您可以构建一个自定义身份代理应用程序来执行类似的功能。代理应用程序对用户进行身份验证，向 AWS 请求用户的临时凭证，然后将其提供给用户以访问 AWS 资源。应用程序验证员工是否已登录到现有公司网络的身份和身份验证系统，该系统可能使用 LDAP、Active Directory 或其他系统。然后，身份代理应用程序为员工获取临时安全凭证。要获取临时安全凭据，identity broker 应用程序调用 AssumeRole 或 GetFederationToken 以获取临时安全凭证，具体取决于您希望如何管理用户的策略以及临时凭据何时到期。该调用返回由 AWS 访问密钥 ID、秘密访问密钥和会话令牌组成的临时安全凭证。identity broker 应用程序使这些临时安全凭据可用于内部公司应用程序。然后，应用程序可以使用临时凭证直接调用 AWS。应用程序缓存凭据，直到它们过期，然后请求一组新的临时凭据。

使用引用 LDAP 标识符和 AWS 凭据的 IAM 策略是不正确的，因为使用 IAM 策略不足以将 LDAP 服务集成到 IAM。您需要使用 SAML、STS 或自定义身份代理。

使用 AWS 单点登录 (SSO) 服务在 AWS 和 LDAP 之间启用单点登录是不正确的，因为该场景不需要 SSO，此外，您使用的标识存储不与 SAML 兼容。

无论何时更新 LDAP 凭据，使用 IAM 角色旋转 IAM 凭据都是不正确的，因为手动旋转 IAM 凭证并不是集成本地和 VPC 网络的最佳解决方案。您需要使用 SAML、STS 或自定义身份代理。参考文献:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_common-scenarios_federated-users.html

<https://aws.amazon.com/blogs/aws/aws-identity-and-access-management-now-with-identity-federation/Dojo> 的 AWS

认证解决方案架构师助理考试学习指南教程: <https://tutorialsdojo.com/aws-certified-solutions-architect-associate/>

Q273.一家公司计划在 Amazon EC2 实例中部署应用程序。应用程序将执行以下任务：

- 从 Amazon S3 存储桶读取大型数据集。
- 对数据集执行多阶段分析。
- 将结果保存到 Amazon RDS。

在多阶段分析期间，应用程序将在实例存储中存储大量临时文件。作为解决方案架构师，您需要为临时文件推荐具有高 I/O 性能的最快存储选项。

以下哪个选项符合此要求？

- A、在多个实例存储卷中配置 RAID 1。
- B、在实例中附加多个已配置的 IOPS SSD 卷。
- C、在多个实例存储卷中配置 RAID 0。
- D、在 Amazon S3 中启用传输加速。

答案 C

分析：

Amazon 弹性计算云（Amazon EC2）在 Amazon Web 服务（AWS）云中提供可扩展的计算能力。您可以使用 Amazon EC2 启动任意数量的虚拟服务器，配置安全和网络，并管理存储。Amazon EC2 使您能够放大或缩小规模，以处理需求的变化或人气的激增，从而减少预测流量的需要。RAID 0 配置使您能够通过分布在条带中的卷之间分布 I/O 来提高存储卷的性能。因此，如果添加存储卷，则吞吐量和 IOPS 将直接增加。此配置可以在 EBS 或实例存储卷上实现。由于场景中的主要需求是存储性能，因此需要使用实例存储卷。它使用 NVMe 或基于 SATA 的 SSD 提供高随机 I/O 性能。当您需要具有非常低延迟的存储时，这种类型的存储是一个很好的选择，并且您不需要在实例终止时保持数据。

因此，正确答案是：在多个实例存储卷中配置 RAID 0。该选项表示：

在 Amazon S3 中启用传输加速是不正确的，因为 S3 传输加速主要用于加快客户端和 S3 存储桶之间的千兆字节或兆字节数据传输。

“在多个实例卷中配置 RAID 1”选项不正确，因为 RAID 1 配置用于数据镜像。您需要配置 RAID 0 以提高存储卷的性能。

表示：在实例中附加多个已配置 IOPS SSD 卷的选项不正确，因为在该场景中不需要持久存储。此外，实例存储卷具有比 EBS 卷更高的 I/O 性能。

参考文献：

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/InstanceStorage.html><https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/raid-config.html> 查看此 Amazon EC2 备忘单：<https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/>

Q274.一位解决方案架构师正在为一家大型全球媒体公司工作，该公司在世界各地设有多个办公地点。建筑师被指示建立一个系统，向所有员工分发培训视频。使用 CloudFront，将使用什么方法提供存储在 S3 中但无法直接从 S3 公开访问的内容？

- A、为 CloudFront 创建一个源访问标识（OAI），并授予该 OAI 对 S3 存储桶中对象的访问权限。
- B、在 AWS WAF 中创建 web ACL 以阻止任何公共 S3 访问，并将其连接到 Amazon CloudFront 分发版。
- C、为 CloudFront 创建身份和访问管理（IAM）用户，并授予该 IAM 用户对 S3bucket 中对象的访问权限。
- D、创建一个 S3 存储桶策略，将 CloudFront 分发 ID 列为主体，将目标存储桶列为 MAZON 资源名称（ARN）。

答:

分析:

在 CloudFront 中创建或更新分发时，可以添加源访问标识（OAI）并自动更新 bucket 策略，以授予源访问标识访问您的 bucket 的权限。或者，您可以选择手动更改 bucket 策略或更改 ACL，它们控制 bucket 中单个对象的权限。

您可以使用 AWS 管理控制台或亚马逊 S3 API 更新 Amazon S3 存储桶策略:

- 授予 CloudFront origin 访问标识对 bucket 的适用权限。
- 拒绝访问您不想使用 Amazon S3 URL 访问的任何人。因此，正确答案是:
为 CloudFront 创建一个源访问标识（OAI），并授予该 OAI 对 S3 存储桶中对象的访问权限。

“为 CloudFront 创建一个身份和访问管理（IAM）用户，并将对 S3 存储桶中对象的访问权授予该 IAM 用户”选项不正确，因为您无法直接为特定的 Amazon CloudFront 发行版创建 IAM 用户。您必须使用源访问标识（OAI）。

“创建一个 S3 存储桶策略，将 CloudFront 分发 ID 列为主体，将目标存储桶列为 Amazon 资源名称（ARN）”的选项不正确，因为设置 Amazon S3 存储池策略

这是不够的。您必须首先在 CloudFront 中创建 OAI，并将该 OAI 用作 AmazonS3 bucket 中的授权用户。

“在 AWS WAF 中创建 web ACL 以阻止任何公共 S3 访问并将其连接到 Amazon CloudFront 发行版”的选项是不正确的，因为 AWS WAF 主要用于保护您的应用程序免受常见 web 漏洞的影响，而不是用于确保对 CloudFront 的独占访问。

参考:

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-tos3.html#向_oai_授予权限的私有属性查看此 Amazon CloudFront 备忘单:

<https://tutorialsdojo.com/amazon-cloudfront/>

S3 预签名 URL 与云前端签名 URL 与源访问标识（OAI）<https://tutorialsdojo.com/s3> 预签名 URL 与云前端签名 URL 与原始访问身份 oai/AWS 服务备忘单比较:

<https://tutorialsdojo.com/comparison-of-aws-services/>

Q275. 一家公司希望将其机密财务文件存储在每周访问的 AWS 中。建筑师被指示设置存储系统，该系统使用信封加密并自动进行密钥旋转。它还应该提供一个审计跟踪，显示谁使用了加密密钥，以及谁出于安全目的使用了该密钥。

架构师应该实现哪些操作组合，以最具成本效益的方式满足需求？（选择两个。）

- A、使用 Amazon S3 Glacier Deep Archive 存储数据。
- B、使用 Amazon S3 存储数据。
- C、Amazon 证书管理器
- D、使用 AWS KMS 托管密钥（SSE-KMS）配置服务器端加密。
- E、使用 Amazon S3 托管密钥（SSE-S3）配置服务器端加密。使用客户提供的密钥（SSE-C）配置服务器端加密。

答：屋宇署

分析：

服务器端加密是接收数据的应用程序或服务在其目的地对数据进行加密。AWS 密钥管理服务（AWS KMS）是一种结合安全、高可用硬件和软件的服务，以提供针对云的密钥管理系统。AmazonS3 使用 AWS KMS 客户主密钥（CMK）加密 AmazonS 对象。SSE-KMS 仅加密对象数据。未加密任何对象元数据。如果您使用客户管理的 CMK，您可以通过 AWS 管理控制台或 AWS KMS API 使用 AWS KMS 来集中创建加密密钥，定义控制密钥使用方式的策略，并审核密钥使用情况，以证明密钥使用正确。您可以使用这些密钥保护 Amazon S3 存储桶中的数据。

客户主密钥（CMK）是主密钥的逻辑表示。CMK 包括元数据，如密钥 ID、创建日期、描述和密钥状态。CMK 还包含用于加密和解密数据的密钥材料。您可以使用 CMK 加密和解密多达 4 KB（4096 字节）的数据。通常，您使用 CMK 生成、加密和解密在 AWS KMS 之外用于加密数据的数据密钥。这种策略称为信封加密。根据您的选择如何管理加密密钥，您有三个互斥选项：

使用服务器端加密与 Amazon S3 托管密钥（SSE-S3）？每个对象都使用唯一密钥加密。作为额外的保护措施，它使用一个主密钥对密钥本身进行加密，主密钥定期旋转。Amazon S3 服务器端加密使用最强大的块密码之一，256 位高级加密标准（AES-256）来加密您的数据。

使用存储在 AWS 密钥管理服务（SSEKMS）中的客户主密钥（CMK）进行服务器端加密？类似于 SSE-S3，但使用此服务有一些额外的好处和费用。CMK 的使用有单独的权限，可提供额外的保护，防止未经授权访问 Amazon S3 中的对象。SSE-KMS 还为您提供审计跟踪，显示何时使用 CMK 以及由谁使用 CMK。此外，您还可以创建和管理客户管理的 CMK，或者使用 AWS 管理的 CMKs，这些 CMK 对于您、您的服务和您的区域都是独一无二的。使用客户提供的密钥（SSE-C）进行服务器端加密？您管理加密密钥，Amazon S3 在写入磁盘时管理加密，在访问对象时管理解密。在这种情况下，公司需要将每周访问的财务文件存储在 AWS 中，解决方案应使用信封加密。这一要求可以通过使用配置了服务器端加密和 AWS KMS 托管密钥（SSE-KMS）的 Amazon S3 来实现。因此，使用 Amazon S3 存储数据并使用 AWS KMS 托管密钥（SSE-KMS）配置服务器端加密是正确答案。

使用 Amazon S3 Glacier Deep Archive 存储数据是不正确的。虽然这提供了最具成本效益的存储解决方案，但如果每周都频繁访问存储的文件，则它不是合适的服务。

使用客户提供的密钥（SSE-C）配置服务器端加密和使用 Amazon S3 托管密钥（SSE-S3）配置服务器侧加密都是不正确的。虽然您可以配置自动密钥轮换，但这两种方法不为您提供显示何时使用 CMK 以及由谁使用 CMK 的审计跟踪，这与使用 AWS KMS 托管密钥（SSE-KMS）的服务器端加密不同。

参考文献：

<https://docs.aws.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingKMSEncryption.html>

<https://docs.aws.amazon.com/kms/latest/developerguide/services-s3.html> 查看此 Amazon S3 备忘单：

<https://tutorialsdojo.com/amazon-s3/>

Q276.一家科技初创公司最近获得了一轮融资，以继续构建其移动外汇交易应用程序。您受聘在 AWS 中建立云架构，并实现高可用性、容错系统。对于他们的数据库，他们使用 **DynamoDB**，对于身份验证，他们选择使用 **Cognito**。由于移动应用程序包含机密金融交易，因此需要添加第二种身份验证方法，该方法不完全依赖于用户名和密码。

如何在 AWS 中实现这一点？

- A、将新的 IAM 策略添加到 Cognito 中的用户池。
- B、将多因素身份验证（MFA）添加到 Cognito 中的用户池，以保护用户的身份。
- C、开发一个与 Cognito 集成的定制应用程序，实现第二层身份验证。
- D、将 Cognito 与 Amazon SNS 移动推送集成，允许通过短信进行额外认证。

答案 B

分析：

您可以向用户池添加多因素身份验证（MFA），以保护用户的身份。MFA 添加了第二种身份验证方法，它不完全依赖于用户名和密码。您可以选择使用 SMS 文本消息或基于时间的一次性（TOTP）密码作为登录用户的第二因素。您还可以使用自适应身份验证及其基于风险的模型来预测何时可能需要另一个身份验证因素。它是用户池高级安全功能的一部分，该功能还包括针对受损凭证的保护。

参考：<https://docs.aws.amazon.com/cognito/latest/developerguide/managing-security.html>

Q277.一家公司有一个 OLTP（在线事务处理）应用程序，该应用程序使用 **Fargate** 启动类型托管在 **Amazon ECS** 集群中。它有一个亚马逊 **RDS** 数据库，存储其生产网站的数据。数据分析团队需要对数据库运行查询，以跟踪和审核所有用户事务。对生产数据库的这些查询操作不得以任何方式影响应用程序性能。

以下哪一项是您应该实施的最合适和最具成本效益的解决方案？ A、将 RDS 数据库的实例类型升级

为大型实例。

- B、设置新的 Amazon Redshift 数据库集群。将产品数据库迁移到红移，并允许 DataAnalytics 团队从中获取数据。
- C、设置生产数据库的新 Amazon RDS 读取副本。指导数据分析团队查询副本中的生产数据。
- D、在 RDS 中设置生产数据库的多 AZ 部署配置。指导数据分析团队从备用实例查询生产数据。

答案 C

分析：

Amazon RDS 读取副本为数据库（DB）实例提供了增强的性能和耐用性。此功能使您可以轻松地弹性扩展，超出单个数据库实例的容量限制，以应对读取繁重的数据库工作负载。

您可以创建给定源数据库实例的一个或多个副本，并从数据的多个副本提供高容量应用程序读取流量，从而提高聚合读取吞吐量。当需要成为独立数据库实例时，还可以升级读取副本。Amazon 中提供了读取副本

用于 MySQL、MariaDB、Oracle 和 PostgreSQL 以及 Amazon Aurora 的 RDS。

通过将读取查询从应用程序路由到读取副本，可以减少源数据库实例的负载。这些副本允许您弹性地扩展，超出单个数据库实例的容量限制，以应对读取繁重的数据库工作负载。

由于读取副本可以升级为主状态，因此它们作为分片实现的一部分非常有用。要对数据库进行分片，请添加一个读取副本并将其升级为主状态，然后从每个生成的数据库实例中删除属于另一个分片的数据。因此，正确的答案

is: 设置生产数据库的新 Amazon RDS 读取副本。指导数据分析团队查询副本中的生产数据。选项显示：设置新的 Amazon Redshift 数据库集群。将产品数据库迁移到 Redshift 并允许数据分析团队从中获取数据是不正确的，因为 Redshift 主要用于 OLAP（在线分析处理）应用程序，而不是 OLTP。该选项表示：在 RDS 中设置生产数据库的多 AZ 部署配置。指示数据分析团队从备用实例查询生产数据不正确，因为您无法直接连接到备用实例。这仅用于数据库故障转移时，当主实例遇到停机时。“将 RDS 数据库的实例类型升级为大型实例”的选项是不正确的，因为这需要大量成本。此外，生产数据库仍可能受到数据分析团队所做查询的影响。对于这种情况，更好的解决方案是使用读取副本。

参考文献：

<https://aws.amazon.com/caching/database-caching/>

<https://aws.amazon.com/rds/details/read-replicas/>

<https://aws.amazon.com/elasticache/> 查看此

Amazon RDS 备忘单：

<https://tutorialsdojo.com/amazon-relational-database-service-amazon-rds/>

Q278. 一家公司在一所著名大学部署了在线注册系统数据库，该数据库由 RDS 托管。解决方案架构师需要监控 Amazon CloudWatch 中的数据库指标，以确保注册系统的可用性。

Amazon CloudWatch 从提供更准确信息的 Amazon RDS DB 实例收集的增强监控指标是什么？（选择两个。）

- A、数据库连接
- B、CPU 利用率
- C、RDS 是子进程。
- D、可释放内存
- E、操作系统进程

行政长官的答覆

分析：

说明：Amazon RDS 为运行数据库实例的操作系统（OS）提供实时指标。您可以使用控制台查看数据库实例的指标，或在您选择的监控系统中使用 CloudWatch 日志中的增强监控 JSON 输出。CloudWatch 从数据库实例的虚拟机监控程序收集有关 CPU 利用率的指标，增强的监控从实例上的代理收集其指标。因此，您可能会发现测量结果之间的差异，因为管理程序层只执行少量工作。差异

如果您的 DB 实例使用较小的实例类，则可能会更大，因为在单个物理实例上可能有更多虚拟机（VM）由管理程序层管理。当您希望查看数据库实例上的不同进程或线程如何使用 CPU 时，增强的监视度量非常有用。

在 RDS 中，流程列表视图中显示的增强监控指标组织如下：

RDS 子进程？显示支持数据库实例的 RDS 进程摘要，例如，针对 Amazon aurora 数据库集群的 aurora 和针对 MySQL 数据库实例的 mysqld。进程线程嵌套在父进程之下。进程线程仅在其他指标相同时显示 CPU 利用率

对于进程的所有线程。控制台最多显示 100 个进程和线程。结果是消耗 CPU 和内存最多的进程和线程的组合。如果有超过 50 个进程和超过 50 个线程，控制台将显示每个类别中的前 50 个消费者。此显示可帮助您确定哪些流程对性能影响最大。RDS 进程？显示 RDS 管理代理、诊断监视进程和支持 RDS DB 实例所需的其他 AWS 进程使用的资源摘要。操作系统进程？显示了内核和系统进程的摘要，这些进程通常对性能影响最小。

CPU 利用率、数据库连接和可用内存不正确，因为这些只是 CloudWatch 中 Amazon RDS 指标提供的常规项目。请记住，场景要求增强监控指标。参考文献：

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/rds-metricscollected.html>

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_Monitoring.OS.html#USER_Monitoring.OS.CloudWatchLogs

查看此 Amazon CloudWatch 备忘单：

<https://tutorialsdojo.com/amazon-cloudwatch/>

查看此 Amazon RDS 备忘单：<https://tutorialsdojo.com/amazon-relational-database-service-amazon-rds/>

Q279.一个组织计划使用 AWS 直接连接在其内部网络和 AWS 之间建立专用连接。该组织需要推出一个完全受管理的解决方案，该解决方案将自动化和加速数据向各种 AWS 存储服务的复制。您会推荐以下哪种解决方案？

- A、使用 AWS 存储网关文件网关直接使用 SMB 文件系统协议存储和检索文件。
- B、使用 AWS 数据同步代理在互联网上快速移动数据。
- C、使用 AWS 数据同步代理在服务端点上快速移动数据。
- D、使用 AWS 存储网关磁带网关将数据存储存储在虚拟盒式磁带上，并将备份异步复制到 AWS。

答案 C

分析：

AWS DataSync 允许您复制包含数百万文件的大型数据集，而无需使用开源工具构建自定义解决方案，也无需许可和管理昂贵的商业网络加速软件。您可以使用 DataSync 将活动数据迁移到 AWS，将数据传输到云以进行分析和处理，归档数据以释放本地存储容量，或将数据复制到 AWS 以实现业务连续性。

AWS 数据同步通过互联网或 AWS Direct Connect 简化、自动化和加速向 AWS 存储服务复制大量数据。DataSync 可以在网络文件系统（NFS）、服务器消息块（SMB）文件服务器、自管理对象存储或 AWS Snowcone、亚马逊简单存储服务（Amazon S3）存储桶、亚马逊 EFS 文件系统和亚马逊 FSx for Windows 文件服务器文件系统之间复制数据。

将 AWS 数据同步代理部署到本地虚拟机监控程序或 Amazon EC2 中。要将数据复制到本地文件服务器或从本地文件服务器复制数据，请从 AWS 控制台下载代理虚拟机映像，并将其部署到本地 VMware ESXi、基于 Linux 内核的虚拟机（KVM）或 Microsoft Hyper-V 虚拟机监控。要将数据复制到云内文件服务器或从中复制数据，可以使用 DataSync 代理 AMI 创建 AmazonEC2 实例。在这两种情况下，必须部署代理，以便它可以使用 NFS、SMB 协议或

AmazonS3API。要设置 AWS Snowcone 设备和 AWS 存储之间的传输，请使用设备上预装的 DataSync 代理 AMI。由于该场景计划使用 AWS Direct Connect 实现本地和 AWS 之间的专用连接，因此您可以使用 DataSync 自动化和加速向 AWS 存储服务的在线数据传输。

这个

AWS 数据同步代理将部署在您的本地网络中，以加速向 AWS 的数据传输。要以编程方式连接到 AWS 服务，您需要使用 AWS 直接连接服务端点。

因此，正确的答案是：使用 AWS 数据同步代理在服务端点上快速移动数据。

“使用 AWS 数据同步代理在 Internet 上快速移动数据”选项是不正确的，因为该组织将使用 AWS 直接连接进行专用连接。这意味着连接不会通过公共互联网。使用 AWS Storage Gateway tape Gateway 将数据存储在虚拟盒式磁带上，并将备份异步复制到 AWS，以及使用 AWS Storage Gateway file Gateway 直接使用 SMB 文件系统协议存储和检索文件的选项都是不正确的，因为在这种情况下，您需要加速数据的复制，并且不建立混合云存储架构。AWS 存储网关根据您启动的网关类型，仅支持少数 AWS 存储服务作为目标。AWS 数据同步更适合于自动化和加速向各种 AWS 存储服务的在线数据传输。

参考文献：

<https://aws.amazon.com/datasync/faqs/>

<https://docs.aws.amazon.com/datasync/latest/userguide/what-is-datasync.html><https://docs.aws.amazon.com/general/latest/gr/dc.html>

AWS 数据同步概述：https://www.youtube.com/watch?v=uQDVZfj_VEA

查看 AWS 数据同步备忘单：<https://tutorialsdodo.com/aws-datasync/>

Q280.一家大型电子公司正在使用亚马逊简单存储服务来存储重要文档。出于报告目的，他们希望跟踪和记录对 S3 存储桶的每个请求访问，包括请求者、存储桶名称、请求时间、请求操作、引用人、周转时间和错误代码信息。该解决方案还应提供对 bucket 的对象级操作的更多可见性。以下选项中哪一个是满足要求的最佳解决方案？

- A、 启用 AWS CloudTrail 以审核所有 Amazon S3 bucket 访问。
- B、 为所有必需的 Amazon S3 存储桶启用服务器访问日志记录。
- C、 启用“请求者付费”选项，通过 AWS 计费跟踪访问。
- D、 为 PUT 和 POST 启用 Amazon S3 事件通知。

答案 B

分析：

Amazon S3 与 AWS CloudTrail 集成，该服务提供用户、角色或 AWS 服务在亚马逊 S3 中采取的行动记录。CloudTrail 将亚马逊 S3 的 API 调用子集捕获为事件，包括来自亚马逊 S3 控制台的调用和对亚马逊 S3 API 的代码调用。AWS CloudTrail 日志提供了用户、角色或 AWS 服务在 Amazon S3 中采取的操作记录，而 Amazon S3s 服务器访问日志提供了对 S3 bucket 的请求的详细记录。

对于这个场景，您可以使用 CloudTrail 和 Amazon S3 的服务器访问日志记录功能。但是，场景中提到，他们需要发送到 S3 bucket 的每个访问请求的详细信息，包括推荐人和周转时间信息。这两条记录在 CloudTrail 中不可用。

因此，正确的答案是：为所有必需的 AmazonS3 bucket 启用服务器访问日志记录。该选项表示：

启用 AWS CloudTrail 以审核所有 Amazon S3 存储桶访问是不正确的，因为单独启用 AWS 云跟踪不会提供对象级访问的详细日志信息。该选项表示：启用请求者付费选项以通过 AWS 计费跟踪访问是不正确的，因为该操

作指的是 AWS 计费，而不是日志记录。该选项表示：为 PUT 和 POST 启用 Amazon S3 事件通知是不正确的，因为我们正在寻找日志记录解决方案，而不是事件通知。参考文献：

<https://docs.aws.amazon.com/AmazonS3/latest/dev/cloudtrail-logging.html#cloudtrail-日志与服务器-日志>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/LogFormat.html>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/ServerLogs.html> 查看此 Amazon S3 备忘单：

<https://tutorialsdojo.com/amazon-s3/>

281.一家数据分析公司一直在其 AWS 云基础设施上构建新一代大数据和分析平台。他们需要一种存储服务，提供大数据应用程序所需的规模和性能，例如计算节点的高吞吐量，以及写后读取一致性和低延迟文件操作。此外，它们的数据需要跨多个 AZ 冗余存储，并允许来自多个 AZs 上托管的多个 EC2 实例的并发连接。您将使用以下哪种 AWS 存储服务来满足此要求？

A、冰川

B、S3

C、EBS

D、EFS

答案 D

分析：

在这个问题中，您应该注意两个关键字/短语：“文件操作”和“允许来自多个 EC2 实例的并发连接”。您可以选择各种 AWS 存储选项，但只要出现这些标准，请始终考虑使用 EFS，而不是使用 EBS 卷，EBS 卷主要用作“块”存储，一次只能连接一个 EC2 实例。Amazon EFS 提供了大数据应用程序所需的规模和性能，这些应用程序需要高吞吐量来计算节点，并具有写后读取一致性和低延迟文件操作。Amazon EFS 是一个完全管理的服务，可以轻松设置和扩展 Amazon 云中的文件存储。只需在 AWS 管理控制台中点击几下，即可创建文件系统，通过文件系统接口（使用标准操作系统文件 I/O API）访问 Amazon EC2 实例，并支持完整的文件系统访问语义（如强一致性和文件锁定）。Amazon EFS 文件系统可以自动从千兆字节扩展到千兆字节，而无需提供存储。数十、数百甚至数千个 Amazon EC2 实例可以同时访问 Amazon EFS 文件系统，Amazon EFS 为每个 Amazon EC2 实例提供一致的性能。亚马逊 EFS 被设计为高度耐用和高度可用。EBS 是不正确的，因为它不允许来自多个 AZ 上托管的多个 EC2 实例的并发连接，并且与 EFS 不同，它默认情况下不跨多个 AZs 冗余存储数据。S3 是不正确的，因为尽管它可以处理来自多个 EC2 实例的并发连接，但它不具备提供低延迟文件操作的能力，这在本场景中是必需的。Glacier 不正确，因为这是一种存档存储解决方案，不适用于此场景。参考文献：

<https://docs.aws.amazon.com/efs/latest/ug/performance.html> <https://aws.amazon.com/efs/faq/> 查看此亚马逊 EFS 备忘单：

<https://tutorialsdojo.com/amazon-efs/>

查看此 Amazon S3 vs EBS vs EFS 备忘单：

<https://tutorialsdojo.com/amazon-s3-vs-ebs-vs-efs/>

以下是亚马逊 EFS 的短视频教程：<https://youtu.be/AvGAozsfCrY>

Q282.一家公司在新创建的 VPC 中启动了一个 EC2 实例。他们注意到生成的实例没有关联的 DNS 主机名。

以下哪个选项可能是导致此问题的有效原因？

- A、新创建的 VPC 具有无效的 CIDR 块。
- B、应启用专有网络配置的 DNS 解析和 DNS 主机名。
- C、未启用 Amazon Route53。
- D、需要修改 EC2 实例的安全组。

答案 B

分析：

当您将 EC2 实例启动到默认 VPC 中时，AWS 为其提供与实例的公共 IPv4 和私有 IPv4 地址相对应的公共和私有 DNS 主机名。但是，当您将实例启动到非默认 VPC 中时，AWS 仅为实例提供一个私有 DNS 主机名。新实例将仅提供公共 DNS 主机名，具体取决于这两个 DNS

属性：您为 VPC 指定的 DNS 解析和 DNS 主机名，以及您的实例是否具有公共 IPv4 地址。

在这种情况下，新的 EC2 实例不会自动获得 DNS 主机名，因为 DNS 解析

并且在新创建的 VPC 中禁用 DNS 主机名属性。因此，正确答案是：应启用专有网络配置的 DNS 解析和 DNS 主机名。

“新创建的 VPC 具有无效的 CIDR 块”选项是不正确的，因为由于 AWS 验证方案，VPC 不太可能具有无效的 CIDR 块。“亚马逊路线 53 未启用”选项不正确，因为路线 53 不需要启用。路由 53 是 AWS 的 DNS 服务，但 VPC 支持分配实例主机名。“需要修改 EC2 实例的安全组”选项不正确，因为安全组只是实例的防火墙。它们根据一组安全组规则过滤流量。

参考文献：

<https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-dns.html> <https://aws.amazon.com/vpc/> 亚马逊专有网络概述：

<https://www.youtube.com/watch?v=oIDHKeNxvQQ>

查看此亚马逊 VPC 备忘单：<https://tutorialsdojo.com/amazon-vpc/>

Q283. 一家公司拥有一个全球新闻网站，由 EC2 实例组成。最近，网站上的负载增加，导致网站访问者的响应时间变慢。这个问题会影响公司的收入，因为如果网站在 10 秒后没有加载，一些读者往往会离开网站。AWS 中的以下哪些服务可用于解决此问题？（选择两个。）

- A、将 Amazon ElastiCache 用于网站的内存数据存储或缓存。
- B、将网站部署到不同 VPC 中的所有区域，以加快处理速度。
- C、使用 Amazon CloudFront 和网站作为自定义源。
- D、要获得更好的读取吞吐量，请使用 AWS 存储网关跨多个区域分发内容。

答覆

分析：

全球新闻网站存在延迟问题，因为该网站的读者来自全球各地。在这种情况下，您可以使用内容交付网络（CDN），这是一组地理分布的服务器，它们一起工作以提供 Internet 内容的快速交付。由于这是一个新闻网站，它的大部分数据都是只读的，可以缓存以提高读取吞吐量并避免来自服务器的重复请求。

在 AWS 中，Amazon CloudFront 是您可以使用的全球内容交付网络（CDN）服务，对于 web 缓存，Amazon ElastiCache 是合适的服务。因此，正确答案是：

- 使用 Amazon CloudFront 和网站作为自定义源。
- 将 Amazon ElastiCache 用于网站的内存数据存储或缓存。“为了更好地读取吞吐量，使用 AWS 存储网关跨多个区域分发内容”选项是不正确的，因为 AWS 存储 Gateway 用于存储。将网站部署到不同 VPC 中的所有区域以加快处理速度是不正确的，因为考虑到您可以使用 Amazon CloudFront 和 ElastiCache 来提高网站参考的性能，这将是成本高昂且完全不必要的：

<https://aws.amazon.com/elasticache/>

<http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Introduction.html> 查看此 Amazon CloudFront 备忘单：<https://tutorialsdojo.com/amazon-cloudfront/>

Q284.一家领先的 IT 咨询公司有一个应用程序，它通过亚马逊 ECS 集群处理大量金融数据流，然后将结果存储到 DynamoDB 表中。您必须设计一个解决方案来检测 DynamoDB 表中的新条目，然后自动触发 Lambda 函数来运行一些测试来验证处理过的数据。

什么解决方案可以容易地实现，以提醒 Lambda 函数新条目，同时需要对您的体系结构进行最小的配置更改？

- A、 启用 DynamoDB 流以捕获表活动并自动触发 Lambda 函数。
- B、 每当在 DynamoDB 表中创建新条目时，使用 CloudWatch 报警触发 Lambda 函数。
- C、 使用 Systems Manager 自动化检测 DynamoDB 表中的新条目，然后自动调用 LAMBDA 函数进行处理。
- D、 每次 ECS 集群成功处理财务数据时，使用 SNS 调用 Lambda 函数。

答：

分析：

Amazon DynamoDB 与 AWS Lambda 集成，因此您可以创建触发器——自动响应 DynamoDB 流中事件的代码片段。使用触发器，您可以构建对 DynamoDB 表中的数据修改做出反应的应用程序。

如果在表上启用 DynamoDB 流，则可以将流 ARN 与您编写的 Lambda 函数相关联。修改表中的项后，新记录立即出现在表的流中。AWS Lambda 轮询流，并在检测到新的流记录时同步调用 Lambda 函数。

您可以创建一个 Lambda 函数，该函数可以执行指定的特定操作，例如发送通知或启动工作流。例如，您可以设置一个 Lambda 函数，将每个流记录简单地复制到持久性存储（如 EFS 或 S3），以便在表中创建写入活动的永久审计跟踪。

假设您有一个移动游戏应用程序，它会写入教程 DojoCourses 表。无论何时更新 TutorialsDojoScores 表的 TopCourse 属性，都会将相应的流记录写入表的流中。然后，该事件可能触发 Lambda 函数，在社交媒体网络上发布祝贺消息。（该函数将简单地忽略任何未更新到 TutorialsDojoCourses 或未修改 TopCourse 属性的流记录。）因此，启用 DynamoDB 流来捕获表活动并自动触发 Lambda 函数是正确答案，因为只需最小的配置更改即可满足要求

使用 DynamoDB 流，只要有新条目，它就可以自动触发 Lambda 函数。每当在 DynamoDB 表中创建新条目时，使用 CloudWatch 报警触发 Lambda 函数是不正确的，因为 CloudWatch 警报仅监视服务度量，而不监视 DynamoDB 表数据中的更改。

每次 ECS 集群成功处理金融数据时使用 SNS 调用 Lambda 函数是不正确的，因为您不需要创建 SNS 主题来调用 Lambda 函数。您可以启用 DynamoDB streams，以较少的配置满足需求。使用 Systems Manager 自动化检测

DynamoDB 表中的新条目，然后自动调用 Lambda 函数进行处理是不正确的，因为 Systems Manager 自动服务主要用于简化 Amazon EC2 实例和其他 AWS 资源的常见维护和部署任务。它无法检测 DynamoDB 表中的新条目。

参考文献：

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Streams.Lambda.html>

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/溪流.html> 查看此 Amazon DynamoDB 备忘单：

<https://tutorialsdojo.com/amazon-dynamodb/>

Q285.您的客户希望在 AWS 中存储一些易于复制但保密的文件，而无需担心存储容量。在第一个月，所有这些文件都将被频繁访问，但之后，它们将很少被访问。旧文件将仅由开发人员访问，因此没有设置检索时间要求。但是，S3 bucket 中特定 tdojo 财务前缀下的文件将用于需要毫秒检索时间的后处理。考虑到这些条件，以下哪种选项将是满足客户存储需求的最经济高效的解决方案？

- A、将文件存储在 S3 中，然后在一个月后，将 tdojo 财务前缀的存储类更改为 S3-IA，同时使用生命周期策略保留 go to Glacier。
- B、将文件存储在 S3 中，一个月后，使用生命周期策略将存储桶的存储类更改为 S3-IA。
- C、将文件存储在 S3 中，然后在一个月后，将 tdojo 财务前缀的存储类更改为一个区域 IA，同时使用生命周期策略保留 go to Glacier。
- D、将文件存储在 S3 中，一个月后，使用 lifecyclepolicy 将存储桶的存储类更改为智能分层。

答案 C

分析：

最初，文件将被频繁访问，而 S3 是一个持久且高可用的存储解决方案。一个月后，文件将不再频繁访问，因此最好使用生命周期策略将其移动到存储成本较低的存储类。由于文件很容易复制，其中一些文件需要根据特定前缀过滤器（tdoj finance）快速检索，因此 S3 One Zone IA 将是存储这些文件的好选择。其他不包含此类前缀的文件将被转移到 Glacier 进行低成本存档。这种设置对客户来说也是最具成本效益的。

因此，正确的答案是：将文件存储在 S3 中，然后在一个月后，将 tdojo-finance 前缀的存储类更改为一个区域 IA，而剩余的将使用生命周期策略转到 Glacier。

该选项表示：将文件存储在 S3 中，然后在一个月后，使用生命周期策略将存储桶的存储类更改为 S3-IA，这是不正确的。尽管将文件移动到 S3-IA 是有效的，但与使用 S3-One Zone IA 和 Glacier 的组合相比，该解决方案的成本仍然更高。该选项表示：将文件存储在 S3 中，然后在一个月后，使用生命周期策略将存储桶的存储类更改为智能分层，这是不正确的。虽然 S3 智能分层可以在访问模式改变时自动在两个访问层（频繁访问和不频繁访问）之间移动数据，但它更适合于您不知道数据访问模式的场景。S3 智能分层可能需要一些时间来分析访问模式，然后才能将数据移动到更便宜的存储类，如 S3-IA，这意味着您可能在开始时支付更多的费用。此外，您已经知道文件的访问模式，这意味着您可以立即直接更改存储类并立即节省成本。

该选项表示：将文件存储在 S3 中，然后在一个月后，将 tdojo-finance 前缀的存储类更改为 S3-IA，而剩余的将使用生命周期策略的 go to Glacier 是不正确的。尽管 S3-IA 的成本低于 S3 标准存储类，但它仍然比 S3 One Zone IA 更昂贵。请记住，文件很容易复制，因此您可以安全地将数据移动到 S3 One Zone IA，如果发生中断，您可以简单地再次生成丢失的数据。参考文献：

<https://aws.amazon.com/blogs/compute/amazon-s3-adds-prefix-and-suffix-filters-for-lambda-function-触发>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/object-lifecycle-mgmt.html><https://docs.aws.amazon.com/AmazonS3/latest/dev/lifecycle-configuration-examples.html> 和 <https://aws.amazon.com/s3/pricing> 查看此 Amazon S3 备忘单: <https://tutorialsdojo.com/amazon-s3/>

Q286.为了节省成本，您的经理指示您分析和审查 AWS 云基础设施的设置。您还应该提供一个公司将其使用的所有 AWS 资源支付多少的估计。在这种情况下，以下哪项将产生成本？（选择两个。）

- A、 停止的按需 EC2 实例
- B、 公共数据集
- C、 连接到已停止 EC2 实例的 EBS 卷
- D、 正在运行的 EC2 实例
- E、 使用 Amazon VP

对裁谈会的答复

分析：

当 Amazon EC2 启动 AMI 实例的启动序列时，计费开始。当实例终止时，计费结束，这可能通过 web 服务命令、运行“shutdown-h”或实例失败而发生。当您停止一个实例时，AWS 会关闭它，但不会对停止的实例收取每小时使用费或数据传输费。但是，AWS 对任何 Amazon EBS 卷的存储收费。

因此，正在运行的 EC2 实例和连接到已停止 EC2 实例的 EBS 卷是正确答案，相反，已停止的按需 EC2 实例是不正确的，因为您已关闭的已停止 EC1 实例不收费。

使用亚马逊专有网络是不正确的，因为创建和使用专有网络本身没有额外的费用。其他 Amazon Web 服务的使用费，包括 Amazon EC2，仍然适用于这些资源的公开费率，包括数据传输费。

公共数据集是不正确的，因为亚马逊存储数据集不向社区收费，而且与所有 AWS 服务一样，您只需为自己应用程序使用的计算和存储付费。

参考文献：

<https://aws.amazon.com/cloudtrail/>

<https://aws.amazon.com/vpc/faqs>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-public-data-sets.html> 查看此 Amazon EC2 备忘

单: <https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/>

Q287.一家汽车公司正在使用 AWS 进行自动驾驶车辆开发和部署项目。该解决方案需要高性能计算（HPC）来收集、存储和管理大量数据，并支持深度学习框架。将使用的 Linux EC2 实例应具有比传统上在基于云的 HPC 系统中使用的 TCP 传输更低的延迟和更高的吞吐量。它还应增强实例间通信的性能，并且必须包括 OS 旁路功能，以允许 HPC 直接与网络接口硬件通信，以提供低延迟、可靠的传输功能。以下哪一项是实现上述要求的最合适的解决方案？

- A、 在每个 Amazon EC2 实例上附加一个弹性网络接口（ENI），以加速高性能计算（HPC）。
- B、 在每个 Amazon EC2 实例上连接一个弹性网络适配器（ENA），以加速高性能计算（HPC）。
- C、 在每个 Amazon EC2 实例上附加一个专用虚拟接口（VIF），以加速高性能计算（HPC）。
- D、 在每个 Amazon EC2 实例上连接一个弹性结构适配器（EFA），以加速高性能计算（HPC）。

答案 D

分析：

弹性结构适配器（EFA）是一种网络设备，可以连接到 Amazon EC2 实例，以加速高性能计算（HPC）和机器学习应用程序。EFA 使您能够利用 AWS 云提供的可伸缩性、灵活性和弹性，实现本地 HPC 集群的应用程序性能。

与基于云的 HPC 系统中传统使用的 TCP 传输相比，EFA 提供了更低、更一致的延迟和更高的吞吐量。它增强了实例间通信的性能，这对于扩展 HPC 和机器学习应用程序至关重要。它经过优化，可在现有 AWS 网络基础设施上工作，并可根据应用要求进行扩展。EFA 与 Libfabric 1.9.0 集成，支持用于 HPC 应用程序的开放式 MPI 4.0.2 和英特尔 MPI 2019 更新 6，以及用于机器学习应用程序的 Nvidia 集体通信库（NCCL）。Windows 实例不支持 EFA 的操作系统旁路功能。如果您附上

对于 Windows 实例的 EFA，该实例作为弹性网络适配器运行，不需要添加 EFA 功能。

弹性网络适配器（ENA）提供支持 VPC 网络所需的传统 IP 网络功能。EFA 提供与 ENA 相同的所有传统 IP 网络功能，还支持操作系统旁路功能。操作系统旁路使 HPC 和机器学习应用程序能够绕过操作系统内核并直接与 EFA 设备通信。因此，正确的答案是在每个 Amazon EC2 实例上附加一个弹性结构适配器（EFA），以加速高性能计算（HPC）。

在每个 Amazon EC2 实例上附加弹性网络适配器（ENA）以加速高性能计算（HPC）是不正确的，因为与 EFA 不同，弹性网络适配器没有操作系统旁路功能。

在每个 Amazon EC2 实例上附加弹性网络接口（ENI）以加速高性能计算（HPC）是不正确的，因为弹性网络接口（ENI）只是 VPC 中代表虚拟网卡的逻辑网络组件。它没有操作系统旁路功能，允许 HPC 直接与网络接口硬件通信，以提供低延迟、可靠的传输功能。

在每个 Amazon EC2 实例上附加专用虚拟接口（VIF）以加速高性能计算（HPC）是不正确的，因为专用虚拟接口仅允许您连接到专用 IP 地址或端点上的 VPC 资源。参考文献：

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/efa.html> <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/efa.html>

查看此弹性结构适配器（EFA）备忘单：<https://tutorialsdojo.com/elastic-fabric-adapter-efa/>

Q288.一家金融公司指示您自动化部门中的重复性任务，如修补程序管理、基础架构选择和数据同步，以改进其当前流程。您需要一个能够将多个 AWS 服务协调到无服务器 workflows 中的服务。在这种情况下，以下哪项是最具成本效益的服务？

- A、 AWS 阶跃函数

B、AWSλ

C、主权财富基金

D、AWS 批

答:

分析:

AWS Step 函数为现代应用程序提供无服务器编排。编排通过将工作流分解为多个步骤、添加流逻辑以及跟踪步骤之间的输入和输出，集中管理工作流。当应用程序执行时，步骤功能会维护应用程序状态，精确跟踪应用程序所处的工作流步骤，并存储在应用程序组件之间传递的数据的事件日志。这意味着，如果网络故障或组件挂起，您的应用程序可以从停止的地方恢复。

使用 Step 功能，应用程序开发更快、更直观，因为您可以独立于业务逻辑定义和管理应用程序的工作流。对其中一个进行更改不会影响另一个。您可以轻松地在一个位置更新和修改工作流，而无需管理、监控和维护多个点对点集成。Step Functions 将您的函数和容器从多余的代码中解放出来，因此您的应用程序编写速度更快，弹性更强，

并且易于维护。

SWF 不正确，因为这是一个完全受管理的状态跟踪器和任务协调器服务。它不为多个 AWS 资源提供无服务器编排。AWS Lambda 是不正确的，因为尽管 Lambda 用于无服务器计算，但它没有提供将多个 AWS 服务协调到无服务器工作流中的直接方法。AWS 批处理是不正确的，因为它主要用于在 AWS 中高效运行成千上万的批处理计算作业。参考：

<https://aws.amazon.com/step-functions/features/>查看

AWS Step 函数备忘单：

<https://tutorialsdojo.com/aws-step-functions/>

亚马逊简单工作流（SWF）vs AWS 步骤功能 vs 亚马逊 SQS：

<https://tutorialsdojo.com/amazon-simple-workflow-swf-vs-aws-step-functions-vs-amazon-sqs/> AWS 服务备忘单比

较：<https://tutorialsdojo.com/comparison-of-aws-services/>

Q289.一家媒体公司正在使用 Amazon EC2、ELB 和 S3 作为电影制作人的视频共享门户。他们使用标准的 S3 存储类来存储所有高质量视频，这些视频仅在发布的前三个月内频繁访问。

作为解决方案架构师，如果公司需要自动将媒体数据从 S3 存储桶传输或存档到 Glacier，您应该怎么做？

- A、使用 Amazon SQS
- B、使用 Amazon SWF
- C、使用自定义 shell 脚本将数据从 S3 桶传输到 Glacier
- D、使用生命周期策略

答案 D

分析：

您可以在 S3 中创建生命周期策略，自动将数据传输到 Glacier。生命周期配置允许您指定 bucket 中对象的生命周期管理。配置是一组一个或多个规则，其中每个规则定义了 AmazonS3 应用于一组对象的操作。

这些行动可分为以下几类：

过渡行动？其中定义对象何时转换到另一个存储类。例如，您可以选择在创建后 30 天将对象转换为 STANDARD_IA（IA，用于不频繁访问）存储类，或者在创建后一年将对象归档到 GLACIER 存储类。过期操作？在其中指定对象过期的时间。然后 Amazon S3 代表您删除过期的对象。

参考：

<https://docs.aws.amazon.com/AmazonS3/latest/dev/object-lifecycle-mgmt.html> 查看此 Amazon S3 备忘单：

<https://tutorialsdojo.com/amazon-s3/>

Q290.一家公司最近将其应用程序迁移到 AWS。解决方案架构师必须确保应用程序具有高可用性，并且不存在常见的 web 安全漏洞。哪种 AWS 服务最适合用来缓解分布式拒绝服务（DDoS）攻击，以避免攻击后端 EC2 实例？

- A、AWS WAF
- B、AWS 防火墙管理器
- C、AWS 屏蔽
- D、亚马逊卫士

答案 C

分析：

AWS Shield 是一种受管理的分布式拒绝服务（DDoS）保护服务，用于保护在 AWS 上运行的应用程序。AWS Shield 提供了始终在线检测和自动内联缓解，最大限度地减少了应用程序停机时间和延迟，因此无需让 AWS 支持从 DDoS 保护中获益。AWS 屏蔽有两层-标准和高级。所有 AWS 客户都可以免费享受 AWS Shield 标准的自动保护。AWS Shield 标准可抵御针对您的网站或应用程序的最常见、频繁发生的网络和传输层 DDoS 攻击。当您使用 AWS Shield 标准与 Amazon CloudFront 和 Amazon Route 53 一起使用时，您将获得针对所有已知基础设施（第 3 层和第 4 层）攻击的全面可用性保护。

AWS WAF 是不正确的，因为这是一种 web 应用程序防火墙服务，可帮助保护您的 web 应用程序免受可能影响应用程序可用性、危害安全性或消耗过多资源的常见攻击。虽然这可以帮助您抵御 DDoS 攻击，但仅 AWS

WAF 不足以完全保护您的 VPC。在这种情况下，您仍然需要使用 AWS Shield。AWS 防火墙管理器不正确，因为它只是简化了跨多个帐户和资源的 AWS WAF 管理和维护任务。

Amazon GuardDuty 是不正确的，因为它只是一种智能威胁检测服务，用于保护您的 AWS 帐户和工作负载。仅使用此功能无法完全保护您的 AWS 资源免受 DDoS 攻击。

参考文献：

<https://docs.aws.amazon.com/waf/latest/developerguide/waf-which-to-choose.html><https://aws.amazon.com/answers/networking/aws-ddos-attack-mitigation/> 攻击缓解/查看此 aws Shield 备忘单：

<https://tutorialsdojo.com/aws-shield/>

AWS 安全服务概述-WAF、Shield、CloudHSM、KMS：<https://www.youtube.com/watch?v=-1SRdeAmMo>

Q291. 一家公司计划开发一种定制的消息服务，该服务还将用于培训他们的人工智能，以实现他们计划在未来实现的自动响应功能。根据他们的研究和测试，该服务每天可以接收多达数千条消息，所有这些消息都将发送到亚马逊 EMR 进行进一步处理。至关重要的是，任何消息都不会丢失，不会产生重复，并且

它们在 EMR 中以与它们到达相同的顺序处理。以下哪个选项可以满足给定要求？

- A、 设置一个 Amazon SNS 主题来处理消息。
- B、 设置默认的 Amazon SQS 队列来处理消息。
- C、 创建 Amazon Kinesis 数据流以收集消息。
- D、 使用 AWS 数据管道创建管道以处理消息。

答案 C

分析：

所选 AWS 服务应满足的两个重要要求是数据不应丢失、持久性和按到达顺序流化数据。Kinesis 可以很好地完成这项工作，因为它的架构。Kinesis 数据流是一组具有一系列数据记录的碎片，每个数据记录都有一个由 Kinesis 的数据流分配的序列号。Kinesis 还可以轻松处理发送到服务的大量消息。

亚马逊 Kinesis 数据流支持流式大数据的实时处理。它提供记录排序，以及以相同顺序读取和/或重放记录到多个 Amazon Kinesis 应用程序的能力。Amazon Kinesis 客户端库（KCL）将给定分区密钥的所有记录交付给同一记录处理器，从而更容易构建从同一 Amazon Kinesis 数据流读取的多个应用程序（例如，执行计数、聚合和过滤）。设置默认的 Amazon SQS 队列来处理消息是不正确的，因为尽管 SQS 是一种有效的消息传递服务，但它不适用于需要根据接收顺序处理数据的场景。请注意，SQS 中的默认队列只是一个标准队列，而不是 FIFO（先进先出）队列。此外，SQS 不保证不会发送副本。设置 Amazon SNS 主题来处理消息是不正确的，因为 SNS 是 AWS 中的发布-订阅消息服务。SNS 可能无法处理一次接收和发送的如此大量的消息。它也不能保证数据的传输顺序与接收顺序相同。

使用 AWS 数据管道创建管道来处理消息是不正确的，因为它主要用作基于云的数据工作流服务，帮助您在不同 AWS 服务和内部数据源之间处理和移动数据。它不适用于从分布式源（如用户、物联网设备或点击流）收集数据。

参考文献：

<https://docs.aws.amazon.com/streams/latest/dev/introduction.html> 有关更多信息，请阅读“我什么时候应该使用亚马逊 Kinesis 数据流”和“我什么时候应该使用亚马逊 SQS？” Kinesis 数据流常见问题解答部分：

<https://aws.amazon.com/kinesis/data-streams/faqs/>

查看此亚马逊 Kinesis 备忘单: <https://tutorialsdojo.com/amazon-kinesis/>

Q292.解决方案架构师正在将几个基于 Windows 的应用程序迁移到 AWS，这些应用程序需要可扩展的文件系统存储以实现高性能计算（HPC）。存储服务必须完全支持 SMB 协议和 Windows NTFS、Active Directory（AD）集成和分布式文件系统（DFS）。以下哪项是架构师应使用的最适合实现此场景的存储服务？

- A、亚马逊 S3 冰川深度档案
- B、用于 Windows 文件服务器的 Amazon FSx
- C、AWS 数据同步
- D、亚马逊 FSx 的光泽

答案 B

分析：

Amazon FSx 提供完全管理的第三方文件系统。Amazon FSx 为您提供了与第三方文件系统的本机兼容性，并为工作负载提供了功能集，如基于 Windows 的存储、高性能计算（HPC）、机器学习和电子设计自动化（EDA）。您不必担心管理文件服务器和存储，因为 Amazon FSx 自动化了耗时的管理任务，如硬件配置、软件配置、修补和备份。Amazon FSx 将文件系统与云原生 AWS 服务集成在一起，使它们对更广泛的工作负载更有用。

Amazon FSx 为您提供了两种文件系统可供选择：用于 Windows 应用程序的 Amazon FSx 文件服务器和用于计算密集型工作负载的 Amazon FSx。对于基于 Windows 的应用程序，Amazon FSx 提供了完全管理的 Windows 文件服务器，其功能和性能针对“提升和转移”业务关键应用程序工作负载进行了优化，包括主目录（用户共享）、媒体工作流和 ERP 应用程序。它可以通过 SMB 协议从 Windows 和 Linux 实例访问。如果您有基于 Linux 的应用程序，Amazon EFS 是一个云本机完全管理的文件系统，提供简单、可扩展、弹性的文件存储，可通过 NFS 协议从 Linux 实例访问。

对于计算密集型和快速处理工作负载，如高性能计算（HPC）、机器学习、EDA 和媒体处理，Amazon FSx For Lustre 提供了一个针对性能优化的文件系统，输入和输出存储在 Amazon S3 上。

因此，正确答案是：Amazon FSx for Windows 文件服务器。Amazon S3 Glacier Deep Archive 是不正确的，因为该服务主要用于数据存档和长期备份的安全、耐用且成本极低的云存储。AWS 数据同步是不正确的，因为该服务只是提供了一种在本地存储和 Amazon S3 或 Amazon 弹性文件系统（Amazon EFS）之间在线移动大量数据的快速方法。Amazon FSx for Lustre 不正确，因为该服务不支持基于 Windows 的应用程序和 Windows 服务器。

参考文献: <https://aws.amazon.com/fsx/>

<https://aws.amazon.com/getting-started/use-cases/hpc/3/>

查看此亚马逊 FSx 备忘单: <https://tutorialsdojo.com/amazon-fsx/>

Q293.解决方案架构师正在现有云架构中设置配置管理。架构师需要使用 Chef 和 Puppet 部署和管理 EC2 实例，包括其他 AWS 资源。

以下哪项服务最适合在此场景中使用？

- A、 AWS OpsWorks
- B、 AWS 弹性豆茎
- C、 AWS 代码部署
- D、 AWS 云形成

答:

分析:

AWS OpsWorks 是一种配置管理服务，提供 Chef 和 Puppet 的托管实例。Chef 和 Puppet 是自动化平台，允许您使用代码自动配置服务器。OpsWorks 允许您使用 Chef 和 Puppet 自动化服务器在 Amazon EC2 实例或本地计算环境中的配置、部署和管理。

参考: <https://aws.amazon.com/opsworks/>

查看此 AWS OpsWorks 备忘单:

<https://tutorialsdojo.com/aws-opsworks/>

弹性 Beanstalk vs CloudFormation vs OpsWorks vs CodeDeploy:

<https://tutorialsdojo.com/elastic-beanstalk-vs-cloudformation-vs-opsworks-vs-codedeploy/AWS> 服务备忘单比较: <https://tutorialsdojo.com/comparison-of-aws-services/>

Q294.您正在工作的初创公司有一个批处理作业应用程序，当前托管在 EC2 实例上。它设置为使用默认设置处理 SQS 中创建的队列中的消息。您将应用程序配置为每周处理一次消息。两周后，您注意到应用程序没有处理所有消息。这个问题的根本原因是什么？

- A、 SQS 队列设置为短轮询。
- B、 SQS 中缺少权限。
- C、 Amazon SQS 已自动删除队列中超过最大消息保留期的消息。
- D、 批处理作业应用程序配置为长轮询。

答案 C

分析:

Amazon SQS 会自动删除队列中超过最大消息保留期的消息。默认消息保留期为 4 天。由于队列配置为默认设置，并且批处理作业应用程序每周只处理一次消息，因此队列中超过 4 天的消息将被删除。这是问题的根本原因。要解决此问题，可以使用 `SetQueueAttributes` 操作将消息保留期最多增加 14 天。

参考文献:

<https://aws.amazon.com/sqs/faqs/>

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-message-lifecycle.html>

Q295.一个组织计划在不使用虚拟化的专用物理服务器上运行应用程序。应用程序数据将存储在使用 NFS 协议的存储解决方案中。为了防止数据丢失,您需要使用持久的云存储服务来存储数据的副本。以下哪种解决方案最适合满足要求?

- A、为您的计算资源使用 AWS 存储网关硬件设备。配置卷网关以存储应用程序数据,并创建 Amazon S3 存储桶以存储数据备份。
- B、将 AWS 存储网关与网关 VM 设备一起用于计算资源。
配置文件网关以存储应用程序数据和备份数据。
- C、为您的计算资源使用 AWS 存储网关硬件设备。配置文件网关以存储应用程序数据,并创建 Amazon S3 存储桶以存储数据备份。
- D、为您的计算资源使用 AWS 存储网关硬件设备。配置卷网关以存储应用程序数据和备份数据。

答案 C

分析:

AWS 存储网关是一种混合云存储服务,通过将其链接到 S3,您可以在本地访问几乎无限的云存储。存储网关为您的本地应用程序提供 3 种类型的存储解决方案:文件、卷和磁带网关。AWS 存储网关硬件设备是一种物理、独立、经验证的服务器配置,用于内部部署。AWS 存储网关硬件设备是一种物理硬件设备,存储网关软件预装在经过验证的服务器配置上。硬件设备是一个高性能的 1U 服务器,您可以将其部署在数据中心或企业防火墙内部。当您购买并激活硬件设备时,激活过程会将您的硬件设备与 AWS 帐户关联。激活后,您的硬件设备将在控制台中显示为硬件页面上的网关。您可以将硬件设备配置为文件网关、磁带网关或卷网关类型。用于在硬件设备上部署和激活这些网关类型的过程与在虚拟平台上相同。由于公司需要运行专用的物理设备,您可以使用 AWS 存储网关硬件设备。它预装了存储网关软件,并提供了创建文件网关所需的所有资源。文件网关可以配置为使用 NFS 和 SMB 协议在 Amazon S3 中存储和检索对象。

因此,本场景中的正确答案是:使用 AWS 存储网关硬件设备来计算资源。配置文件网关以存储应用程序数据,并创建 Amazon S3 存储桶来存储数据备份。

该选项表示:将 AWS 存储网关与网关 VM 设备一起用于计算资源。配置文件网关以存储应用程序数据和备份数据是不正确的,因为根据场景,公司需要使用本地硬件设备,而不仅仅是虚拟机(VM)。

选项如下:为您的计算资源使用 AWS 存储网关硬件设备。配置卷网关以存储应用程序数据和备份数据,并为您的计算资源使用 AWS 存储网关硬件设备。配置卷网关来存储应用程序数据,并创建 Amazon S3 存储桶来存储数据备份,这两种方法都不正确。根据场景,要求是使用 NFS 协议而不是 iSCSI 设备的文件系统。在 AWS 存储网关存储解决方案中,只有文件网关可以使用 NFS 和 SMB 协议在 Amazon S3 中存储和检索对象。

参考文献:

<https://docs.aws.amazon.com/storagegateway/latest/userguide/hardware-appliance.html><https://docs.aws.amazon.com/storagegateway/latest/userguide/WhatIsStorageGateway.html> AWS 存储网关概述:

<https://www.youtube.com/watch?v=pNb7xOBJjHE> 查看

此 AWS 存储网关备忘单:

<https://tutorialsdojo.com/aws-storage-gateway/>

Q296.一家领先的媒体公司最近采用了混合云架构，要求他们将应用服务器和数据库迁移到 AWS 中。其中一个应用程序需要异构数据库

迁移，您需要将本地 Oracle 数据库转换为 AWS 中的 PostgreSQL。这需要在适当的数据迁移开始之前进行模式和代码转换。以下哪个选项是在 AWS 中迁移数据库的最合适方法？

- A、使用 Amazon Neptune 转换源模式和代码，以匹配 RDS 中目标数据库的模式和代码。在批处理过程中，使用 AWS 批处理有效地将数据从源数据库迁移到目标数据库。
- B、首先，使用 AWS 模式转换工具将源模式 and 应用程序代码转换为与目标数据库相匹配，然后使用 AWS 数据库迁移服务将数据从源数据库迁移到目标数据库。
- C、AWS 不支持异构数据库迁移。您必须首先将数据库转换为 PostgreSQL，然后将其迁移到 RDS。
- D、配置启动模板，自动转换源模式和代码以匹配目标数据库的模式和代码。然后，使用 AWS 数据库迁移服务将数据从源数据库迁移到目标数据库。

答案 B

分析：

AWS 数据库迁移服务帮助您快速、安全地将数据库迁移到 AWS。源数据库在迁移过程中保持完全运行，最大限度地减少依赖该数据库的应用程序的停机时间。AWS 数据库迁移服务可以将您的数据迁移到最广泛使用的商业和开源数据库。

AWS 数据库迁移服务可以将您的数据迁移到大多数广泛使用的商业和开源数据库。它支持同类迁移，如 Oracle 到 Oracle，以及不同数据库平台之间的异构迁移，如从 Oracle 到 Amazon Aurora。迁移可以从本地数据库迁移到 Amazon RDS 或 Amazon EC2，从 EC2 上运行的数据库迁移到 RDS，反之亦然，也可以从一个 RDS 数据库迁移到另一 RDS 数据库。它还可以在 SQL、NoSQL 和基于文本的目标之间移动数据。

在异构数据库迁移中，源和目标数据库引擎是不同的，如

Oracle 到 Amazon Aurora、Oracle 到 PostgreSQL 或 Microsoft SQL Server 到 MySQL 的迁移。在这种情况下，源数据库和目标数据库的模式结构、数据类型和数据库代码可能非常不同，需要在数据迁移开始之前进行模式和代码转换。这使异构迁移成为一个两步过程。首先使用 AWS 模式转换工具将源模式和代码转换为与目标数据库的模式和代码相匹配，然后使用 AWS 数据库迁移服务将数据从源数据库迁移到目标数据库。迁移期间，AWS 数据库迁移服务将自动完成所有必需的数据类型转换。源数据库可以位于 AWS 之外的您自己的场所中，在 Amazon EC2 实例上运行，

或者它可以是 Amazon RDS 数据库。目标可以是 Amazon EC2 或 Amazon RDS 中的数据库。该选项表示：配置一个启动模板，自动转换源模式和代码以匹配目标数据库的模式和代码。然后，使用 AWS 数据库迁移服务将数据从源数据库迁移到目标数据库是不正确的，因为启动模板主要用于 EC2 中，使您能够存储启动参数，这样您就可以不必在每次启动实例时都指定它们。

选项表示：使用 Amazon Neptune 转换源模式和代码，以匹配 RDS 中的目标数据库。在批处理过程中使用 AWS 批处理有效地将数据从源数据库迁移到目标数据库是不正确的，因为 Amazon Neptune 是一个完全受管理的图形数据库服务，不适合用于转换源模式。AWS 批处理不是数据库迁移服务

因此不适合在这种情况下使用。您应该使用 AWS 模式转换工具和 AWS 数据库迁移服务。

选项表示：AWS 不支持异构数据库迁移。您必须先将数据库转换为 PostgreSQL，然后将其迁移到 RDS。这是不正确的，因为 AWS 使用数据库迁移服务支持异构数据库迁移。参考文献：

<https://aws.amazon.com/dms/>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-launch-templates.html><https://aws.amazon.com/batch/>

查看此 AWS 数据库迁移服务备忘单：

<https://tutorialsdojo.com/aws-database-migration-service/>

AWS 迁移服务概述：<https://www.youtube.com/watch?v=yqNBkFMnsL8>

Q297.公司拥有内部数据中心和 AWS 云基础设施。它们存储它们的图形，

音频、视频和其他多媒体资产主要存储在其内部存储服务器中，并使用 S3 标准存储类存储桶作为备份。他们的数据仅在一周（7 天）内大量使用，但之后

期间，客户将很少使用它。解决方案架构师被指示在 AWS 中节省存储成本，同时保持在几分钟内获取其媒体资产子集的能力，以便对其云存储进行意外的年度数据审计。以下哪项是解决方案架构师可以实现以满足上述要求的有效选项？（选择两个。）

- A、在 bucket 中设置生命周期策略，以在一周（7 天）后将数据转换到 S3 Glacier Deep Archive 存储类。
- B、在 bucket 中设置生命周期策略，以在一周（7 天）后将数据转换为 S3 标准 IA 存储类。
- C、在 bucket 中设置生命周期策略，以在一周（7 天）后将数据转换到 Glacier。
- D、在 bucket 中设置生命周期策略，以便在 30 天后过渡到 S3 标准 IA
- E、在 bucket 中设置一个生命周期策略，以在一周（7 天）后将数据转换到 S3-一个区域不频繁访问存储类。

对裁谈会的答复

分析：

您可以在生命周期配置中添加规则，告诉 AmazonS3 将对象转换到另一个 AmazonS 存储类。例如：当您知道对象很少被访问时，您可以将它们转换为 STANDARD_IA 存储类。或者将您的数据转换到 GLACIER storage 类，以防您想要归档不需要实时访问的对象。在生命周期配置中，您可以定义将对象从一个存储类转换到另一个存储类别的规则，以节省存储成本。当您不知道对象的访问模式或访问模式随时间变化时，可以将对象转换为 INTELLIGENT_TIERING 存储类，以自动节省成本。当您希望从标准存储类转换为 STANDARD_IA 或 ONEZONE_IA 时，生命周期存储类转换有一个约束。以下限制适用：

- 对于较大的对象，转换到 STANDARD_IA 或 ONEZONE_IA 具有成本效益。Amazon S3 不会将小于 128 KB 的对象转换为 STANDARD_IA 或 ONEZONE_IA 存储类，因为这不符合成本效益。
- 对象必须在当前存储类中存储至少 30 天，然后才能将其转换为 STANDARD_IA 或 ONEZONE_IA。例如，您无法创建生命周期规则，以便在创建对象后一天将其转换为 STANDARD_IA 存储类。Amazon S3 不会在前 30 天内转换对象，因为较新对象的访问频率或删除速度通常比标准 IA 或 ONEZONE_IA 存储更高。
- 如果要转换非当前对象（在版本化存储桶中），则只能将至少 30 天非当前的对象转换为 STANDARD_IA 或 ONEZONE_IA 存储。

由于在 S3 中转换对象有时间限制，您只能在 30 天后将对象的存储类从 S3 标准存储类更改为 Standard IA 或 ONEZONE_IA 存储。此限制不适用于 INTELLIGENT_TIERING、GLACIER 和 DEEP_ARCHIVE 存储类。此外，要求要求媒体资产应在几分钟内提取，以便进行年度数据审计。这意味着检索每年只会发生一次。您可以在 Glacier 中使用快速检索，这将允许您在偶尔需要对档案子集的紧急请求时快速访问数据（在 1 分钟内）。在这种情况下，您可以在 bucket 中设置一个生命周期策略，以便在 30 天后过渡到 S3-标准 IA，或者，您也可以在一周（7 天）后直接将数据过渡到 Glacier。

因此，以下是正确答案：

- 在 bucket 中设置生命周期策略，以在一周（7 天）后将数据从标准存储类转换为 Glacier。

- 在 bucket 中设置生命周期策略，以便在 30 天后过渡到 S3 标准 IA。在存储桶中设置生命周期策略以在一周（7 天）后将数据转换为 S3-标准 IA 存储类，并在存储桶中将生命周期策略设置为在一周后（7 天），将数据转换到 S3-一个区域-不频繁访问存储类都是不正确的，因为 S3 中有一个约束，即对象必须在当前存储类中至少存储 30 天您可以将它们转换为 STANDARD_IA 或 ONEZONE_IA。无法在创建对象后 7 天内创建生命周期规则以将对象转换为 STANDARD_IA 或 ONEZONE_IA 存储类，因为只能在

30 天的时间已经过去。因此，这些选项是不正确的。在存储桶中设置生命周期策略以在一周（7 天）后将数据转换到 S3 Glacier Deep Archive 存储类是不正确的，因为尽管 Deep_Archive 存储类别提供了最具成本效益的存储选项，但它不具备进行快速检索的能力，这与 Glaciers 不同。如果发生意外的年度数据审计，您可能需要几个小时才能检索数据。参考文献：

<https://docs.aws.amazon.com/AmazonS3/latest/dev/lifecycle-transition-general-considerations.html><https://docs.aws.amazon.com/AmazonS3/latest/dev/restoring-objects.html><https://aws.amazon.com/s3/storage-classes/>

查看此 Amazon S3 备忘单：<https://tutorialsdojo.com/amazon-s3/>

Q298.一位解决方案架构师正在为一家快速发展的初创公司工作，该公司在过去 3 个月内刚刚开始运营。他们目前有一个内部活动目录和 10 台计算机。为了节省购买物理工作站的成本，他们决定在 AWS 的虚拟私有云中为新员工部署虚拟桌面。新的云基础设施应利用 AWS 中现有的安全控制，但仍可以与其内部网络通信。架构师将使用哪套 AWS 服务来满足这些要求？

- A、AWS 目录服务、VPN 连接和 Amazon S3
- B、AWS 目录服务、VPN 连接以及 AWS 身份和访问管理
- C、AWS 目录服务、VPN 连接和 ClassicLink
- D、AWS 目录服务、VPN 连接和 Amazon 工作区

答案 D

分析：

对于这个场景，最好的答案是：AWS 目录服务、VPN 连接和 Amazon 工作区。

首先，您需要一个 VPN 连接来连接 VPC 和您的内部网络。其次，您需要 AWS 目录服务与本地 Active Directory 集成，最后，您需要使用 Amazon 工作区在 VPC 中创建所需的虚拟桌面。参考文献：

<https://aws.amazon.com/directoryservice/>

<https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpn-connections.html>
<https://aws.amazon.com/workspaces/>

AWS 身份服务概述：<https://www.youtube.com/watch?v=AIdUw0i8rr0>

在 AWS 目录服务、亚马逊 VPC 和亚马逊工作区查看这些备忘单：

<https://tutorialsdojo.com/aws-directory-service/> <https://tutorialsdojo.com/amazon-vpc/>

Q299.一个健康组织正在使用一个具有多个 EBS 卷的大型专用 EC2 实例来托管其健康记录 web 应用程序。由于 EBS 卷所处理数据的保密性，且符合 HIPAA（健康保险便携性和责任法案）标准，因此必须对 EBS 卷进行加密。

在 EBS 加密中，AWS 使用什么服务来保护静态卷的数据？（选择两个。）

- A、在 AWS 密钥管理服务（KMS）中使用您自己的密钥。
- B、通过使用 S3 服务器端加密。
- C、通过使用 AWS 证书管理器（ACM）提供的 SSL 证书。
- D、通过使用存储在 CloudHSM 中的密码。
- E、通过使用 AWS 密钥管理服务（KMS）中的 Amazon 托管密钥。
- F、通过使用 S3 客户端加密。

答案：AE

分析：

Amazon EBS 加密提供 EBS 数据卷、启动卷和快照的无缝加密，无需构建和维护安全的密钥管理基础设施。EBS 加密通过使用 Amazon 托管密钥或您使用 AWS 密钥管理服务（KMS）创建和管理的密钥加密您的数据，从而实现静态数据安全。加密发生在托管 EC2 实例的服务器上，当数据在 EC2 实例和 EBS 存储之间移动时提供加密。因此，正确的答案是：在 AWS 密钥管理服务（KMS）中使用您自己的密钥，在 AWS 的密钥管理服务中使用亚马逊管理的密钥。

使用 S3 服务器端加密和使用 S3 客户端加密都是不正确的，因为它们仅与 S3 相关。

使用存储在 CloudHSM 中的密码是不正确的，因为您只在 CloudHSM 中存储密钥，而不是密码。使用 AWS 证书管理器（ACM）提供的 SSL 证书是不正确的，因为 ACM 仅提供 SSL 证书，而不提供 EBS 卷的数据加密。
参考：

<https://aws.amazon.com/ebs/faqs/>查看此

亚马逊 EBS 备忘单：

<https://tutorialsdojo.com/amazon-ebs/>

Q300.多媒体公司需要将 web 服务部署到以前从未使用过的 AWS 区域。该公司目前为其 Amazon EC2 实例设置了 IAM 角色，允许该实例访问 Amazon DynamoDB。他们希望新区域中的 EC2 实例具有完全相同的权限。

应该做些什么来实现这一点？

- A、将现有 IAM 角色分配给新区域中的实例。
- B、将 IAM 角色和关联策略复制到新区域，并将其附加到实例。
- C、在新区域中，创建新的 IAM 角色和关联策略，然后将其分配给新实例。
- D、创建实例的 Amazon 机器映像（AMI），并将其复制到新区域。

答：

分析：

在这种情况下，公司有一个现有的 IAM 角色，因此您不需要创建一个新角色。IAM 角色是可用于所有区域的全局服务，因此，您只需将现有 IAM 角色分配给新区域中的实例。

“在新区域中，创建一个新的 IAM 角色和关联策略，然后将其分配给新实例”选项不正确，因为您不需要创建另一个 IAM 角色-已经存在一个现有 IAM 角色。

将 IAM 角色和关联策略复制到新区域并将其附加到实例是不正确的，因为您不需要为每个区域复制 IAM 角色。对于两个区域上的实例，一个 IAM 角色就足够了。

创建实例的 Amazon 机器映像（AMI）并将其复制到新区域是不正确的，因为创建 AMI 映像不会影响实例的 IAM 角色。参考：<https://docs.aws.amazon.com/AmazonS3/latest/dev/NotificationHowTo.html> 查看此 Amazon S3 备忘单：<https://tutorialsdojo.com/amazon-s3/>

Q301.按需 EC2 实例启动到 VPC 子网中，网络 ACL 配置为允许所有入站流量并拒绝所有出站流量。实例的安全组具有允许从任何 IP 地址进行 SSH 的入站规则，并且没有任何出站规则。在这种情况下，需要进行哪些更改才能允许 SSH 连接到实例？

- A、 需要修改出站安全组和出站网络 ACL 以允许出站流量。
- B、 不需要采取任何行动。可以使用 SSH 从任何 IP 地址访问它。
- C、 需要修改网络 ACL 以允许出站流量。
- D、 需要修改出站安全组以允许出站流量。

答案 C

分析：

为了建立从家庭计算机到 EC2 实例的 SSH 连接，需要执行以下操作：

- 在安全组中，添加入站规则以允许 SSH 流量进入 EC2 实例。
- 在 NACL 上，添加入站和出站规则，以允许 SSH 流量进入 EC2 实例。之所以必须添加入站和出站 SSH 规则，是因为网络 ACL 是无状态的，这意味着允许入站流量的响应受出站流量规则的约束（反之亦然）。换句话说，如果您仅在 NACL 中启用了入站规则，则通信量只能进入，但 SSH 响应不会退出，因为没有出站规则。安全组是有状态的，这意味着如果传入请求被授予，那么传出流量也将被自动授予，而不管出站规则如何。参考文献：

https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_ACLS.html<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/authorizing-access-to-an-instance.html>

Q302.一家数据分析公司将大量数据存储在其内部数据中心。为了扩展存储系统，他们正在寻找云支持的存储卷，这些存储卷可以使用 Internet 小型计算机系统接口（iSCSI）设备从本地应用服务器装载。

他们有一个现场数据分析应用程序，经常在本地访问最新的数据子集，而很少访问较旧的数据。您需要尽可能减少扩展本地存储基础架构的需要，同时仍然为 web 应用程序提供对数据的低延迟访问。您将使用哪种类型的 AWS 存储网关服务来满足上述要求？

- A、 缓存模式下的卷网关
- B、 卷网关处于存储模式

C、磁带网关

D、文件网关

答:

分析:

在这种情况下，该技术公司正在寻找一种存储服务，使其分析应用程序能够频繁访问最新的数据子集，而不是整个数据集（正如前面提到的，旧数据很少被使用）。可以通过在 AWS 存储网关中设置缓存卷网关来满足此要求。

通过使用缓存卷，您可以将 Amazon S3 用作主要数据存储，同时在存储网关中本地保留频繁访问的数据。缓存卷最大限度地减少了扩展本地存储基础结构的需要，同时仍为应用程序提供了对频繁访问数据的低延迟访问。您可以创建大小高达 32 TiB 的存储卷，然后将这些卷作为 iSCSI 设备连接到本地应用程序服务器。当您写入这些卷时，网关将数据存储存储在 Amazon S3 中。它将最近读取的数据保留在本地存储网关的缓存中，并上传缓冲存储。

缓存卷的大小可以从 1 GiB 到 32 TiB 不等，必须四舍五入到最接近的 GiB。为缓存卷配置的每个网关最多可支持 32 个卷，总最大存储容量为 1024 TiB（1 PiB）。

在缓存卷解决方案中，AWS 存储网关将所有本地应用程序数据存储存储在 Amazon S3 的存储卷中。因此，正确答案是：卷网关处于缓存模式。存储模式下的卷网关不正确，因为要求提供对本地频繁访问的数据子集的低延迟访问。如果需要对整个数据集进行低延迟访问，则使用存储卷。

磁带网关是不正确的，因为它只是一种经济高效、耐用、长期的数据存档替代方案，在这种情况下不需要。

文件网关不正确，因为该场景要求您将卷装载为 iSCSI 设备。文件网关用于通过 NFS 和 SMB 协议存储和检索 AmazonS3 对象。参考文献：

<https://docs.aws.amazon.com/storagegateway/latest/userguide/存储网关概念.html#卷-网关概念>

<https://docs.aws.amazon.com/storagegateway/latest/userguide/WhatIsStorageGateway.html> AWS 存储网关概述：

<https://www.youtube.com/watch?v=pNb7xOBJjHE> 查看

此 AWS 存储网关备忘单：

<https://tutorialsdojo.com/aws-storage-gateway/>

Dojo 的 AWS 认证解决方案架构师助理考试学习指南教程：<https://tutorialsdojo.com/aws-certified-solutions-architect-associate-saa-c02/>

Q303.应用程序托管在 EC2 实例的自动缩放组中。为了改进监控过程，您必须根据一组缩放调整来配置当前容量的增加或减少。这应该通过为触发缩放过程的 CloudWatch 警报指定缩放度量和阈值来完成。

以下哪一项是您应该使用的最合适的缩放策略类型？

A、阶跃缩放

B、简单缩放

C、目标跟踪和缩放

D、计划缩放

答:

分析:

通过分步缩放,您可以为触发缩放过程的 CloudWatch 警报选择缩放度量和阈值,并定义当阈值在指定数量的评估期内违反时,应如何缩放可缩放目标。分步缩放策略基于一组称为分步调整的缩放调整来增加或减少可缩放目标的当前容量。调整根据警报破坏的大小而变化。启动缩放活动后,策略将继续响应其他警报,即使缩放活动正在进行。因此,当接收到报警消息时,应用程序自动缩放将评估所有违反的报警。配置动态缩放时,必须定义如何根据不断变化的需求进行缩放。例如,您有一个当前在两个实例上运行的 web 应用程序,当应用程序负载发生变化时,您希望自动缩放组的 CPU 利用率保持在 50%左右。这为您提供了额外的容量来处理流量高峰,而不需要维护过多的空闲资源。您可以将自动缩放组配置为自动缩放以满足此需要。策略类型决定如何执行缩放操作。

Amazon EC2 自动缩放支持以下类型的缩放策略:

目标跟踪缩放-根据特定指标的目标值增加或减少组的当前容量。这与恒温器保持家中温度的方式相似吗?您选择一个温度,恒温器完成其余的工作

- 根据一组缩放调整(称为阶跃调整)增加或减少组的当前容量,这些调整根据警报破坏的大小而变化。简单缩放-基于单个缩放调整增加或减少组的当前容量。

如果要根据利用率度量进行缩放,该利用率度量与自动缩放组中的实例数成比例增加或减少,则建议使用目标跟踪缩放策略。否则,最好使用步进缩放策略。因此,这种情况下的正确答案是逐步缩放。目标跟踪缩放不正确,因为目标跟踪缩放策略基于特定度量的目标值而不是一组缩放调整来增加或减少组的当前容量。简单缩放不正确,因为简单缩放策略基于单个缩放调整而不是一组缩放调整来增加或减少组的当前容量。计划缩放不正确,因为计划缩放策略基于允许您为可预测负载更改设置自己的缩放计划的计划。这不被视为动态缩放的类型之一。

参考文献:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scale-based-on-demand.html><https://docs.aws.amazon.com/autoscaling/application/userguide/applicationauto-scaling-step-scaling-policies.html>

Q304.一家公司通过记录所有 AWS 资源的 AWS API 调用历史记录来解决其云架构的操作问题。解决方案架构师必须实现一个解决方案,以快速识别对其环境中的资源所做的最新更改,包括 AWS 资源的创建、修改和删除。其中一个要求是生成的日志文件应加密,以避免任何安全问题。

以下哪种方法最适合实现加密?

- A、使用 CloudTrail 并将目标 S3 存储桶配置为使用 AES-128 加密算法的服务器端加密(SSE)。
- B、使用 CloudTrail 及其默认设置
- C、使用 CloudTrail 并将目标 Amazon Glacier 存档配置为使用服务器端加密(SSE)。
- D、使用 CloudTrail 并将目标 S3 存储桶配置为使用服务器端加密(SSE)。

答案 B

分析:

默认情况下,CloudTrail 事件日志文件使用 Amazon S3 服务器端加密(SSE)进行加密。您还可以选择使用 AWS 密钥管理服务(AWS KMS)密钥加密日志文件。您可以在 bucket 中存储日志文件,只要您愿意。您还可以定义 Amazon S3 生命周期规则来自动存档或删除日志文件。如果您需要有关日志文件传递和验证的通知,可以设置 Amazon SNS 通知。

使用 CloudTrail 并将目标 Amazon Glacier 存档配置为使用服务器端加密（SSE）是不正确的，因为 CloudTrail 将日志文件存储到 S3，而不是存储在冰川中。请注意，默认情况下，CloudTrail 事件日志文件已经使用 AmazonS3 服务器端加密（SSE）进行了加密。使用 CloudTrail 并将目标 S3 存储桶配置为使用服务器端加密（SSE）是不正确的，因为 CloudTrail 事件日志文件已经使用 Amazon S3 服务器端加密进行了加密，这就是您不必再这样做的原因。使用 CloudTrail 并将目标 S3 存储桶配置为使用 AES-128 加密算法的服务器端加密（SSE）是不正确的，因为默认情况下，CloudTrail 事件日志文件已使用 Amazon S3 服务器端加密进行加密。此外，SSE-S3 仅使用 AES-256 加密算法，而不是 AES-128。

参考文献：

<https://docs.aws.amazon.com/awsccloudtrail/latest/userguide/how-cloudtrail-works.html><https://aws.amazon.com/blogs/aws/category/cloud-trail/>

查看此 AWS CloudTrail 备忘单：<https://tutorialsdojo.com/aws-cloudtrail/>

Q305.一家公司的基础设施允许来自私有子网的 EC2 实例通过 NAT 实例从 Amazon S3 获取对象。公司的解决方案架构师被指示降低当前解决方案产生的成本。

解决方案架构师应该如何以最具成本效益的方式重新设计架构？

- A、删除 NAT 实例并创建 S3 网关端点以访问 S3 对象。
- B、删除 NAT 实例并创建 S3 接口端点以访问 S3 对象。
- C、将 NAT 实例替换为 NAT 网关以访问 S3 对象。
- D、为 NAT 实例使用较小的实例类型。

答：

分析：

VPC 端点使您能够私自将 VPC 连接到由 PrivateLink 提供支持的 AWS 服务和 VPC 端点服务，而无需互联网网关、NAT 设备、VPN 连接或 AWS 直接连接。VPC 中的实例不需要公共 IP 地址与服务中的资源通信。专有网络和其他服务之间的流量不会离开亚马逊网络。

端点是虚拟设备。它们是水平扩展、冗余和高可用的 VPC 组件，允许 VPC 中的实例和服务之间进行通信，而不会对网络流量施加可用性风险或带宽限制。有两种类型的专有网络端点：

接口端点和网关端点。您应该创建支持的服务所需的 VPC 端点类型。根据经验，大多数 AWS 服务使用 VPC 接口端点，S3 和 DynamoDB 除外，后者使用 VPC 网关端点。

使用网关端点不收取额外费用。然而，数据传输和资源使用的标准费用仍然适用。

假设您创建了一个 NAT 网关，并且有一个通过 NAT 网关路由到 Internet 的 EC2 实例。NAT 网关后面的 EC2 实例向其中一个 S3 存储桶发送 1GB 文件。EC2 实例、NAT 网关和 S3 存储桶位于同一地区美国东部（俄亥俄州），NAT 网关与 EC2 实例位于同一可用性区域。您的成本计算如下：

- NAT 网关小时收费：NAT 网关按小时收费。例如，该地区的费率为每小时 0.045 美元。
- NAT 网关数据处理费用：1 GB 数据通过 NAT 网关。应用 NAT 网关数据处理费用，将产生 0.045 美元的费用。
- 数据传输费用：这是标准的 EC2 数据传输费用。1GB 数据通过 NAT 网关从 EC2 实例传输到 S3。从 EC2 实例到 S3 的数据传输是免费的，因为它是从同一地区的 Amazon EC2 到 S3 进行数据传输。NAT 网关和 EC2

实例之间的数据传输也不收费，因为流量使用专用 IP 地址保持在同一可用区域。如果您的 NAT 网关和 EC2 实例位于不同的可用性区域，则会收取数据传输费用。总之，对于 NAT 网关处理的 1 GB 数据，您的费用为 0.045 美元，一旦 NAT 网关配置并可用，每小时 0.044 美元的费用将始终适用。在本例中，数据传输不收费。但是，如果您将文件发送到非 AWS 互联网位置，则会收取数据传输费用，因为它是从 Amazon EC2 到互联网的数据传输。为了避免本例中的 NAT 网关数据处理费用，您可以设置一个网关类型的 VPC 端点，并通过 VPC 端点路由来往 S3 的流量，而不是通过 NAT 网关。

使用网关型 VPC 端点不需要数据处理或每小时收费。因此，正确的答案是这样的选项：删除 NAT 实例并创建 S3 网关端点以访问 S3 对象。

表示：使用 NAT 网关替换 NAT 实例以访问 S3 对象的选项不正确。NAT 网关只是由 AWS 为您管理的 NAT 实例。它提供较少的操作管理，您可以为 NAT 网关运行的时间付费。这不是最有效的解决方案，因为您仍将为空闲时间付费。

表示：为 NAT 实例使用较小实例类型的选项不正确。虽然这可能会降低成本，但它仍然不是最具成本效益的解决方案。S3 网关端点仍然是最好的解决方案，因为它不需要额外的费用。

“删除 NAT 实例并创建 S3 接口端点以访问 S3 对象”选项不正确。接口端点是一个弹性网络接口，具有来自子网 IP 地址范围的专用 IP 地址。与网关端点不同，您仍然会收到接口端点运行时间及其处理的 GB 数据的账单。从成本角度来看，使用 S3 网关端点是最有利的解决方案。

参考文献：

<https://docs.aws.amazon.com/vpc/latest/privatelink/vpce-gateway.html> [https://aws.amazon.com/blogs/架构/使用amazon vpc 端点降低成本并提高安全性/](https://aws.amazon.com/blogs/架构/使用amazon-vpc-端点降低成本并提高安全性/)<https://aws.amazon.com/vpc/定价/>

查看此 Amazon S3 备忘单：

<https://tutorialsdojo.com/amazon-s3/>

Q306.应用程序托管在连接了多个 EBS 卷的 EC2 实例上，并使用 Amazon Neptune 作为其数据库。为了提高数据安全性，您加密了连接到实例的所有 EBS 卷，以保护存储在卷中的机密数据。关于加密的 Amazon 弹性块存储卷，以下哪项陈述正确？（选择两个。）

- A、快照会自动加密。
- B、在卷和实例之间移动的所有数据都被加密。
- C、快照不会自动加密。
- D、从加密快照创建的卷未加密。
- E、只有卷中的数据被加密，而不是卷和实例之间移动的所有数据。

回答 AB

分析：

Amazon 弹性块存储（Amazon EBS）提供用于 EC2 实例的块级存储卷。EBS 卷是高度可用和可靠的存储卷，可以连接到任何正在运行的实例

位于同一可用性区域。连接到 EC2 实例的 EBS 卷公开为独立于实例生命周期的存储卷。创建加密 EBS 卷并将其附加到支持的实例类型时，将加密以下类型的数据：

- 卷内静止的数据

- 在卷和实例之间移动的所有数据
- 从卷创建的所有快照
- 从这些快照创建的所有卷

加密操作发生在托管 EC2 实例的服务器上，确保实例与其连接的 EBS 存储之间的静态数据和传输数据的安全性。您可以加密 EC2 实例的启动卷和数据卷。参考文献：

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AmazonEBS.html>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html> 查看此亚马逊 EBS 备忘单：

<https://tutorialsdojo.com/amazon-ebs/>

Q307.一名解决方案架构师在一家跨国电信公司工作。IT 经理希望将其日志流（包括访问、应用程序和安全日志）整合到一个系统中。

一旦

合并后，公司将基于启发式实时分析这些日志。在未来的某个时候，公司将需要验证启发式，这需要返回过去 12 小时提取的数据样本。

满足这一要求的最佳方法是什么？

- A、首先，配置 Amazon Cloud Trail 以接收自定义日志，然后使用 EMR 对日志应用启发式。
- B、首先，将所有日志事件发送到 Amazon SQS，然后设置 EC2 服务器的自动伸缩组以使用日志，最后应用启发式。
- C、首先，设置 EC2 服务器的自动伸缩组，然后将日志存储在 Amazon S3 上，最后，使用 EMR 在日志上应用 Euristics。
- D、首先，将所有日志事件发送到 Amazon Kinesis，然后，开发一个客户端进程，在日志上应用启发式。

答案 D

分析：

在这种情况下，您需要一个能够实时收集、处理和分析数据的服务，因此，这里使用的正确服务是 Amazon Kinesis。

Amazon Kinesis 使您可以轻松收集、处理和分析实时流式数据，以便您能够及时了解并快速响应新信息。Amazon Kinesis 提供了以任何规模经济高效地处理流数据的关键功能，以及选择最适合您应用程序要求的工具的灵活性。

使用亚马逊 Kinesis，您可以获取实时数据，如视频、音频、应用程序日志、网站点击流以及用于机器学习、分析和其他应用程序的物联网遥测数据。Amazon Kinesis 使您能够在数据到达时对其进行处理和分析，并立即做出响应，而不必等到收集到所有数据后才开始处理。所有其他选项都不正确，因为与亚马逊 Kinesis 不同，这些服务不具备实时处理能力。

参考：<https://aws.amazon.com/kinesis/>

查看此亚马逊 Kinesis 备忘单：<https://tutorialsdojo.com/amazon-kinesis/>

Q308.一家公司计划在 AWS 中部署基于 Docker 的批处理应用程序。该应用程序将用于处理关键任务数据和非必要批处理作业。以下哪一项是实现此体系结构时最具成本效益的选项？

- A、使用 ECS 作为容器管理服务，然后设置保留和点 EC2 实例的组合，分别用于处理任务关键和非关键批处理作业。
- B、使用 ECS 作为容器管理服务，然后设置保留的 EC2 实例，用于处理任务关键型和非关键批处理作业。
- C、使用 ECS 作为容器管理服务，然后设置按需 EC2 实例，以处理关键任务和非关键批处理作业。
- D、使用 ECS 作为容器管理服务，然后设置 Spot EC2 实例，以处理任务关键型和非关键批处理作业。

答:

分析:

Amazon ECS 允许您在 Amazon EC2 按需实例、保留实例或点实例上使用托管或自定义调度程序运行批处理工作负载。您可以启动 EC2 实例的组合

根据您的工作负载设置经济高效的体系结构。您可以启动保留的 EC2 实例来处理任务关键型数据，并为处理非必要的批处理作业找到 EC2 实例。

亚马逊弹性容器服务（ECS）有两种不同的收费模式：Fargate 启动模式和 EC2 启动模式。使用 Fargate，您需要支付容器化应用程序请求的 vCPU 和内存资源的数量，而对于 EC2 启动类型模型，则不需要额外收费。您为存储和运行应用程序而创建的 AWS 资源（例如 EC2 实例或 EBS 卷）付费。你只为你使用的东西付费，因为您在使用它；没有最低费用，也没有前期承诺。

在这种情况下，最经济高效的解决方案是使用 ECS 作为容器管理服务，然后设置

设置保留和现场 EC2 实例的组合，分别用于处理任务关键型和非必要批处理作业。您可以使用计划保留实例（计划实例），这使您能够购买

在一年期限内，以指定的开始时间和持续时间每天、每周或每月重复进行的容量保留。这将确保您拥有不间断的计算能力来处理关键任务批处理作业。

因此，正确的答案是这样的选项：使用 ECS 作为容器管理服务，然后设置保留和点 EC2 实例的组合，分别处理任务关键和非关键批处理作业。

使用 ECS 作为容器管理服务，然后设置保留的 EC2 实例来处理任务关键和非关键批处理作业是不正确的，因为使用 Spot EC2 实例而不是保留实例可以更便宜地处理非关键批作业。使用 ECS 作为容器管理服务，然后设置按需 EC2 实例来处理关键任务和非关键批处理作业是不正确的，因为按需实例的成本高于保留和现场 EC2 实例。通过使用 Spot EC2 实例而不是按需实例，可以更便宜地处理非必要的批处理作业。使用 ECS 作为容器管理服务，然后设置 Spot EC2 实例来处理关键任务和非关键批处理作业是不正确的，因为尽管这种设置提供了其他选项中最便宜的解决方案，但它将无法提供所需的工作负载。使用 Spot 实例处理任务关键型工作负载并不合适，因为 AWS 可以随时终止这些类型的实例，这可能会影响关键处理。参考文献：

<https://docs.aws.amazon.com/AmazonECS/latest/developerguide/Welcome.html>

<https://aws.amazon.com/ec2/spot/containers-for-less/> 开始/查看此 Amazon ECS 备忘单：

[https://tutorialsdojo.com/amazon-elastic-container-service-amazon-ecs/AWS 容器服务概述](https://tutorialsdojo.com/amazon-elastic-container-service-amazon-ecs/AWS-容器服务概述)：

<https://www.youtube.com/watch?v=5QBgDX7O7pw>

Q309.实时收集、处理和分析股票数据的金融分析应用程序正在使用 Kinesis 数据流。生产者不断将数据推送到 Kinesis 数据流，而消费者实时处理数据。在亚马逊 Kinesis 中，消费者可以在哪里存储他们的结果？（选择两个。）

- A、冰川选择
- B、亚马逊与雅典娜
- C、亚马逊红移
- D、亚马逊 S3
- E、AWS 胶水

对裁谈会的答复

分析：

在亚马逊 Kinesis 中，生产商不断向 Kinesis 数据流推送数据，消费者实时处理数据。消费者（如在 Amazon EC2 上运行的自定义应用程序或 Amazon Kinesis Data Firehose 交付流）可以使用 AWS 服务（如 Amazon DynamoDB、Amazon Redshift 或 Amazon S3）存储结果。

因此，Amazon S3 和 Amazon Redshift 是正确答案。下图说明了 Kinesis 数据流的高级架构：

冰川选择不正确，因为这不是存储服务。它主要用于直接对存储在 Amazon Glacier 中的数据进行查询，仅从档案中检索用于分析的数据。AWS 胶水不正确，因为这不是存储服务。它是一种完全管理的提取、转换和加载（ETL）服务，使客户可以轻松准备和加载数据进行分析。Amazon Athena 是不正确的，因为这只是一个交互式查询服务，可以使用标准 SQL 轻松分析 Amazon S3 中的数据。它不是一种存储服务，您可以在其中存储消费者处理的结果。

参考：

<http://docs.aws.amazon.com/streams/latest/dev/key-concepts.html> 亚马逊红移概述：

<https://youtu.be/jlLERNzhHOg>

查看此亚马逊 Kinesis 备忘单：<https://tutorialsdojo.com/amazon-kinesis/Q310>. 客户

将其公司网站托管在面向公共负载均衡器后面的 web 服务器集群上。客户端还

使用亚马逊路由 53 来管理其公共 DNS。客户端应如何配置 DNS 区域 apex 记录

以指向负载均衡器？

- A、为负载均衡器 DNS 名称的 CNAME 记录创建别名。
- B、创建指向负载均衡器 DNS 名称的 CNAME 记录。
- C、创建别名为负载均衡器 DNS 名称的 A 记录。
- D、创建指向负载均衡器 IP 地址的 A 记录。

答案 C

分析：

Route 53 的 DNS 实现将用户请求连接到 Amazon Web 内部（和外部）运行的基础设施服务（AWS）。例如，如果您在弹性负载均衡器后面的 EC2 实例上运行多个 web 服务器，则路由 53 会将寻址到您的网站（例如 `www.tutorialsdojo.com`）的所有流量路由到负载均衡器 DNS 名称（例如 `elbtutorialsdojo123.elb.amazonaws.com`）。

此外，路由 53 支持别名资源记录集，它允许您将区域 apex（例如 `tutorialsdojo.com`）DNS 名称映射到负载均衡器 DNS 名称。由于扩展或软件更新，与弹性负载均衡器相关联的 IP 地址可以随时更改。路由 53 响应以下请求：

为负载均衡器设置一个 IP 地址的别名资源记录集。创建指向负载均衡器 IP 地址的 A 记录不正确。您应该使用指向负载均衡器 DNS 名称的别名记录，因为负载均衡器的 IP 地址可以随时更改。

创建指向负载均衡器 DNS 名称的 CNAME 记录是为负载均衡器 DNS 名称的 CNAME 记录创建别名是不正确的，因为无法为您的区域 apex 创建 CNAME 记录。您应该在 DNS 名称空间的顶部节点（也称为区域顶点）创建别名记录。例如，如果注册 DNS 名称 `tutorialsdojo.com`，区域顶点是 `tutorialsdojo.com`。不能直接为 `tutorialsdojo.com` 创建 CNAME 记录，但您可以为 `tutorialsdojo.com` 创建别名记录。将流量路由到 `www.tutorialsdojo.com`。

参考文献：

<http://docs.aws.amazon.com/govcloud-us/latest/UserGuide/setting-up-route53-zoneapex-elb.html>

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resource-record-sets-selecting-alias-and-non-alias.html>

查看此亚马逊路线 53 备忘单：<https://tutorialsdojo.com/amazon-route-53/>

Q311. 一家公司计划使用路由 53 而不是 ELB 来负载均衡对 web 应用程序的传入请求。系统部署到两个 EC2 实例，需要将流量分配到其中。您需要设置每个实例的特定流量百分比。您将使用哪种路由策略？

- A、故障转移
- B、加权
- C、地理定位
- D、潜伏期

答案 B

分析：

加权路由允许您将多个资源与单个域名（`tutorialsdojo.com`）或子域名（`portal.tutorialsdojo.com`）关联，并选择路由到每个资源的流量。这可以用于多种目的，包括负载均衡和测试软件的新版本。您可以通过指定权重来设置分配给资源的流量的特定百分比。

例如，如果您希望将流量的一小部分发送到一个资源，其余部分发送到另一个资源中，则可以指定权重为 1 和 255。权重为 1 的资源获得流量的 $1/256$ ($1/1+255$)，而另一资源获得 $255/256$ ($255/1+255$)。您可以通过改变权重逐渐改变平衡。如果要停止向资源发送流量，可以将该记录的权重更改为 0。

因此，正确答案是加权的。

延迟不正确，因为您无法使用此路由策略为 2 个 EC2 实例设置特定的流量百分比。延迟路由策略主要用于在多个 AWS 区域中拥有资源时，以及需要自动将流量路由到特定 AWS 区域，以提供最佳延迟和较少往返时间时。

故障转移不正确，因为如果要为 web 应用程序设置主动-被动故障转移配置，通常使用这种类型。

地理位置不正确，因为它更适合根据用户的位置路由流量，而不是将特定百分比的流量分配给两个 AWS 资源。

参考：<http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html> 亚马逊路线 53 概述：

<https://youtu.be/Su308t19ubY>

查看此亚马逊路线 53 备忘单：<https://tutorialsdojo.com/amazon-route-53/>

Q312.web 应用程序托管在 EC2 实例上，该实例处理在私有子网中启动的敏感金融信息。所有数据都存储在 Amazon S3 存储桶中。用户可以通过互联网访问财务信息。该公司的安全团队担心与亚马逊 S3 的互联网连接存在安全风险。

在这种情况下，您将如何以最具成本效益的方式解决此安全漏洞？

- A、更改 web 架构，通过由 AWS PrivateLink 支持的接口 VPC 端点访问 S3 中的财务数据。
- B、通过创建自定义 VPC 端点服务，更改 web 架构以访问 S3 bucket 中托管的金融数据。
- C、更改 web 架构以通过网关专有网络端点访问财务数据。
- D、更改 web 架构，通过 VPN 连接访问 S3 bucket 中的财务数据。

答案 C

分析：

请注意，您的专有网络位于一个更大的 AWS 网络中，服务（如 S3、DynamoDB、RDS 等）位于专有网络之外，但仍在 AWS 网络内。默认情况下，VPC 用于连接 S3 bucket 或任何其他服务的连接通过互联网网关穿越公共互联网。

VPC 端点使您能够私自将 VPC 连接到由 PrivateLink 提供支持的 AWS 服务和 VPC 端点服务，而无需互联网网关、NAT 设备、VPN 连接或 AWS 直接连接。VPC 中的实例不需要公共 IP 地址与服务中的资源通信。专有网络和其他服务之间的流量不会离开亚马逊网络。

VPC 端点有两种类型：接口端点和网关端点。您必须创建支持服务所需的 VPC 端点类型。

接口端点是具有专用 IP 地址的弹性网络接口，该专用 IP 地址用作目的地为支持服务的流量的入口点。网关端点是一个网关，它是路由表中指定路由的目标，用于指向受支持 AWS 服务的流量。因此，正确的答案是：改变 web 架构，通过网关 VPC 端点访问金融数据。

该选项表示：更改 web 架构以通过 VPN 连接访问 S3 存储桶中的金融数据是不正确的，因为 VPN 连接仍然通过公共互联网。在这种情况下，您必须使用 VPC 端点，而不是 VPN，才能将您的 VPC 私自连接到支持的 AWS 服务，如 S3。

“通过创建自定义 VPC 端点服务来更改 web 架构以访问 S3 bucket 中托管的金融数据”的选项是不正确的，因为“专有网络端点服务”与“专有网络终端服务”完全不同。使用 VPC 端点服务，您是服务提供商，您可以在 VPC 中创建自己的应用程序，并将其配置为 AWS PrivateLink 支持的服务（称为端点服务）。其他 AWS 主体可以使用接口 VPC 端点创建从其 VPC 到您的端点服务的连接。

该选项表示：更改 web 架构以通过由 AWS PrivateLink 提供支持的接口 VPC 端点访问 S3 中的金融数据是不正确的。尽管您可以使用接口 VPC 端点来满足需求，但与网关 VPC 端点不同，这种类型需要相关成本。请记住，如果您为 Amazon S3 bucket 使用网关专有网络端点，您将不会收到账单，这与按小时使用和数据处理收费的接口专有网络端点不同。请注意，场景明确要求最具成本效益的解决方案。参考文献：

[https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-](https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-endpoints.html)

[endpoints.htmlhttps://docs.aws.amazon.com/vpc/latest/userguide/vpce-gateway.html](https://docs.aws.amazon.com/vpc/latest/userguide/vpce-gateway.html) 查看此亚马逊专有网络备忘单：

<https://tutorialsdojo.com/amazon-vpc/>

Q313.一家新闻公司计划在 AWS 中使用硬件安全模块（CloudHSM）来安全存储其 web 应用程序的密钥。您已经启动了 CloudHSM 群集，但在几个小时后，一名支持人员三次错误地尝试使用硬件中的无效密码以管理员身份登录

安全模块。这导致 HSM 被归零，这意味着其上的加密密钥已被擦除。不幸的是，您没有存储在其他地方的密钥副本。如何获得硬件安全模块上存储的密钥的新副本？

- A、 请联系 AWS 支持，他们将为您提供密钥副本。
- B、 还原硬件安全模块的快照。
- C、 使用 Amazon CLI 获取密钥的副本。
- D、 如果您没有副本，密钥将永久丢失。

答案 D

分析：

尝试以管理员身份使用错误密码登录两次以上会将 HSM 设备归零。当 HSM 归零时，HSM 上的所有密钥、证书和其他数据都会被销毁。您可以使用群集的安全组来防止未经身份验证的用户将 HSM 归零。Amazon 无法访问您的密钥，也无法访问您硬件安全模块（HSM）的凭据，因此，如果您丢失了凭据，则无法恢复您的密钥。Amazon 强烈建议您在任何生产 CloudHSM 集群的单独可用性区域中使用两个或多个 HSM，以避免丢失加密密钥。

参考 CloudHSM 常见问题解答：

Q： 如果单个 HSM 实例失败，我会丢失密钥吗？

对如果您正在使用的 CloudHSM 群集出现故障，并且您没有使用两个或多个 HSM，则可能会丢失自最近的每日备份以来创建的密钥。Amazon 强烈建议您在任何生产 CloudHSM 集群中使用两个或多个 HSM，分别位于不同的可用性区域，以避免丢失加密密钥。

Q： 如果我丢失了 HSM 的凭据，Amazon 可以恢复我的密钥吗？不可以。Amazon 无法访问您的密钥或凭据，因此，如果您丢失了凭据，则无法恢复您的密钥。

参考文献：<https://aws.amazon.com/premiumsupport/knowledge-center/stop-cloudhsm/>

<https://aws.amazon.com/cloudhsm/常见问题/><https://d1.awsstatic.com/whitepapers/Security/security-of-aws-cloudhsm-backups.pdf>

Q314. 一家公司部署了一个 web 应用程序，将静态资产存储在 Amazon 简单存储服务（S3）存储桶中。解决方案架构师期望 S3 bucket 在高峰时间每秒立即接收 2000 多个 PUT 请求和 3500 个 GET 请求。

解决方案架构师应如何确保最佳性能？

- A、 什么也不做。Amazon S3 将自动管理这种规模的性能。
- B、 使用字节范围获取来检索每个 GET 请求的对象数据的多个范围。
- C、 为密钥名称添加随机前缀。
- D、 在键名称中使用可预测的命名方案，如序列号或日期-时间序列。

答：

分析：

Amazon S3 现在提供了更高的性能，支持每秒至少 3500 个添加数据的请求和每秒 5500 个检索数据的请求，这可以节省大量处理时间，无需额外收费。每个 S3 前缀都可以支持这些请求速率，从而可以简单地显著提高性能。

今天在 Amazon S3 上运行的应用程序将享受这种性能改进，而无需任何更改，在 S3 上构建新应用程序的客户无需进行任何应用程序定制即可实现这种性能。Amazon S3 对并行请求的支持意味着您可以根据计算集群的因素来扩展 S3 性能，而无需对应用程序进行任何定制。性能按前缀进行扩展，因此可以并行使用所需数量的前缀，以实现所需的吞吐量。前缀的数量没有限制。这种 S3 请求速率性能的提高消除了任何先前的随机对象前缀以实现更快性能的指导。这意味着您现在可以在 S3 对象中使用逻辑或顺序命名模式

命名没有任何性能影响。这一改进现在在所有 AWS 地区都可用。在每个 GET 请求中使用 ByteRange 获取来检索多个范围的对象数据是不正确的，因为尽管字节范围获取有助于实现更高的聚合吞吐量，但 Amazon S3 没有支持每个 GET 请求检索多个数据范围。使用 GET 对象请求中的范围 HTTP 头，可以从对象获取字节范围，只传输指定的部分。您可以使用到 Amazon S3 的并发连接从同一对象中获取不同的字节范围。获取较大对象的较小范围也允许应用程序在请求中断时缩短重试时间。

向密钥名称添加随机前缀是不正确的。在这种情况下不需要添加随机前缀，因为 S3 现在可以自动缩放以调整性能。您不再需要为此添加随机前缀，因为 S3 提高了性能，支持每秒至少 3500 个添加数据的请求和每秒 5500 个检索数据的请求，这涵盖了场景中的工作负载。

在密钥名称中使用可预测的命名方案（如序列号或日期时间序列）是不正确的，因为 Amazon S3 已经在每个 AWS 区域中维护了对象密钥名称索引。S3 按字母顺序存储键名。密钥名称指示密钥存储在哪个分区中。使用顺序前缀会增加 Amazon S3 针对大量密钥的特定分区的可能性，从而使分区的 I/O 容量无法承受。参考文献：

[https://docs.aws.amazon.com/AmazonS3/latest/dev/request-rate-perf-](https://docs.aws.amazon.com/AmazonS3/latest/dev/request-rate-perf-considerations.html)

[considerations.html](https://d1.awsstatic.com/whitepapers/amazon-s3/best-practices.pdf)<https://d1.awsstatic.com/whitepapers/amazon-s3/best-practices.pdf>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/GettingObjectsUsingAPIs.html> 查看此 Amazon S3 备忘单：

<https://tutorialsdojo.com/amazon-s3/>

Q315. 一家公司有 10 TB 不经常访问的财务数据文件需要存储在 AWS 中。

在为审计目的检索这些数据时，在特定的几周内很少访问这些数据。检索时间不严格，只要不超过 24 小时。以下哪一项是该场景的安全、持久和经济有效的解决方案？

- A、 将数据上传到 S3，然后使用生命周期策略将数据传输到 S3 一个区域 IA。
- B、 使用服务器消息块（SMB）协议将数据上传到 Amazon FSx for Windows 文件服务器。

C、将数据上传到 S3，然后使用生命周期策略将数据传输到 S3-IA。

D、将数据上传到 S3，并设置生命周期策略，以便在 0 天后将数据转换到 Glacier。

答案 D

分析：

Glacier 是一种经济高效的海量数据存档解决方案。批量检索是 S3 Glacier 成本最低的检索选项，使您能够在一天内以低廉的成本检索大量甚至 PB 的数据。批量检索通常在 5 年内完成？12 小时。您可以指定绝对或相对时间段（包括 0 天），在该时间段之后，指定的 Amazon S3 对象应转换到 Amazon Glacier。因此，正确的答案是这样的选项：将数据上传到 S3，并设置生命周期策略，在 0 天后将数据转换到 Glacier。

Glacier 有一个管理控制台，可用于创建和删除 Vault。但是，您不能使用管理控制台直接将档案上传到 Glacier。要上载照片、视频和其他文档等数据，您必须使用 AWS CLI 或编写代码，直接使用 REST API 或使用 AWS SDK。

请注意，将数据上传到 S3 控制台并将其存储类设置为“Glacier”是另一回事，因为将数据上传至 Glaciers 的正确方式仍然是通过其 API 或 CLI。这样，您可以设置 Vault 并配置检索选项。如果您使用 S3 控制台上传了数据，那么它将通过 S3 进行管理，即使它在内部使用 Glacier 存储类。将数据上传到 S3，然后使用生命周期策略将数据传输到 S3-IA 是不正确的，因为使用 Glacier 将比使用 S3-IA 更具成本效益。由于所需的恢复时间不应超过一天，冰川将是最佳选择。

使用服务器消息块（SMB）协议将数据上传到 Amazon FSx for Windows 文件服务器是不正确的，因为此选项的成本高于 Amazon Glacier，后者更适合存储不经常访问的数据。Amazon FSx for Windows 文件服务器提供完全管理、高度可靠和可扩展的文件存储，可通过行业标准服务器消息块（SMB）协议访问。

将数据上传到 S3，然后使用生命周期策略将数据传输到 S3 一个区域 IA 是不正确的，因为使用 S3 一区域 IA，数据将仅存储在单个可用性区域中，因此，此存储解决方案不耐用。与冰川相比，它的成本也更高。参考文献：

<https://aws.amazon.com/glacier/faqs/>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/object-lifecycle-mgmt.html><https://docs.aws.amazon.com/amazonglacier/latest/dev/upload-an-archive.html> 亚马逊 S3 和 S3 冰川概述：

<https://www.youtube.com/watch?v=lymyeN2tki4>

查看此亚马逊 S3 冰川备忘单：<https://tutorialsdojo.com/amazon-glacier/>

Q316.公司有一个按需应变的 EC2 实例，该实例带有附加的 EBS 卷。有一个计划作业，在不使用实例的情况下，每午夜 12 点创建此 EBS 卷的快照。有一天晚上

在生产事件中，您需要在快照当前发生的同时对实例和 EBS 卷执行更改。在快照过程中使用 EBS 卷时，以下哪种情况是正确的？

A、快照正在进行时，EBS 卷可以在只读模式下使用。

B、在快照完成之前，无法使用 EBS 卷。

C、在快照完成之前，无法将 EBS 卷分离或连接到 EC2 实例

D、可以在快照进行时使用 EBS 卷。

答案 D

分析：

快照异步发生；立即创建时间点快照，但快照的状态为挂起，直到快照完成（当所有修改的块都已转移到 Amazon S3），对于大型初始快照或后续快照（其中许多块已更改），这可能需要几个小时。

在完成时，正在进行的快照不受正在进行的卷读写操作的影响。因此，您仍然可以正常使用 EBS 卷。

当您基于快照创建 EBS 卷时，新卷以用于创建快照的原始卷的精确副本开始。复制卷在后台缓慢加载数据，以便您可以立即开始使用。如果您访问尚未加载的数据，卷将立即从 Amazon S3 下载请求的数据，然后继续在后台加载卷的其余数据。

参考文献：

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-creating-snapshot.html>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSSnapshots.html> 查看此亚马逊 EBS 备忘单：

<https://tutorialsdojo.com/amazon-ebs/>

Q317.在您工作的初创公司，要求您设计一个需要 NoSQL 数据库的 web 应用程序，该数据库对给定表的存储大小没有限制。这家初创公司在市场上还是一家新公司，能够管理数据库基础设施的人力资源非常有限。您可以实现的提供完全管理、可扩展和高可用 NoSQL 服务的最合适的服务是什么？

- A、SimpleDB
- B、亚马逊海王星
- C、发电机
- D、亚马逊极光

答案 C

分析：

术语“完全管理”意味着 Amazon 将管理服务的底层基础设施，因此，您不需要额外的人力资源来支持或维护服务。因此，亚马逊 DynamoDB 是正确答案。请记住，Amazon RDS 是一个托管服务，但不是“完全托管”，因为您仍然可以选择维护和配置数据库的底层服务器。AmazonDynamoDB 是一种快速、灵活的 NoSQL 数据库服务，适用于需要任何规模的一致、单位数毫秒延迟的所有应用程序。它是一个完全管理的云数据库，支持文档和键值存储模型。其灵活的数据模型、可靠的性能和自动扩展的吞吐量容量使其非常适合移动、网络、游戏、广告技术、物联网和许多其他应用。Amazon Neptune 不正确，因为它主要用作图形数据库。Amazon Aurora 是不正确的，因为这是一个关系数据库，而不是 NoSQL 数据库。SimpleDB 不正确。尽管 SimpleDB 也是一个高度可用和可扩展的 NoSQL 数据库，但与 DynamoDB 不同，它对给定表的请求容量或存储大小有限制。参考：

<https://aws.amazon.com/dynamodb/>

查看此 Amazon DynamoDB 备忘单：

DynamoDB 概述:

<https://www.youtube.com/watch?v=3ZOyUNleorU>

Q318.一家领先的电子商务公司需要一种存储解决方案，可由多个可用区域中的 1000 台 Linux 服务器同时访问。服务器托管在通过 NFSv4 协议使用分层目录结构的 EC2 实例中。该服务应该能够处理大规模快速变化的数据，同时仍然保持高性能。无论何时服务器从中提取数据，它都应该是高度耐用和高度可用的，几乎不需要管理。作为解决方案架构师，您应该使用以下哪种服务来满足上述要求，这是最具成本效益的选择？

- A、EFS
- B、S3
- C、EBS
- D、存储网关

答:

分析:

亚马逊网络服务（AWS）提供云存储服务，以支持广泛的存储工作负载，如 EFS、S3 和 EBS。您必须了解何时应该使用 Amazon EFS、Amazon S3 和 Amazon 弹性块存储

（EBS）基于特定的工作负载。在这个场景中，关键字是快速变化的数据和 1000 台 Linux 服务器。

Amazon EFS 是一个与 Amazon EC2 一起使用的文件存储服务。Amazon EFS 提供了一个文件系统接口、文件系统访问语义（如强一致性和文件锁定）以及可并发访问的存储，可用于多达数千个 Amazon EC2 实例。EFS 提供了与 S3 相同级别的高可用性和高可扩展性。然而，该服务更适用于需要 POSIX 兼容文件系统或存储快速变化数据的场景。

考虑以下因素的存储解决方案可能更好地为必须频繁更新的数据提供服务：

读写延迟，如 Amazon EBS 卷、Amazon RDS、Amazon DynamoDB、Amazon EFS 或在 Amazon EC2 上运行的关系数据库。

Amazon EBS 是与 Amazon EC2 一起使用的块级存储服务。Amazon EBS 可以为需要从单个 EC2 实例访问数据的最低延迟的工作负载提供性能。Amazon S3 是一个对象存储服务。Amazon S3 通过互联网 API 提供数据，可以在任何地方访问。

在这种情况下，EFS 是最佳答案。如上所述，Amazon EFS 提供了文件系统接口、文件系统访问语义（如强一致性和文件锁定）以及可并发访问的存储

多达数千个 Amazon EC2 实例。EFS 提供了场景中 1000 台 Linux 服务器所需的性能、耐用性、高可用性和存储容量。S3 是不正确的，因为尽管它提供了与 EFS 相同的高可用性和高可扩展性级别，但该服务不适合存储快速变化的数据，正如上面的解释中所提到的。使用 EFS 更有效，因为它提供了 S3 服务所缺乏的强一致性和文件锁定。

EBS 不正确，因为 EBS 卷不能由多个实例共享。存储网关不正确，因为它主要用于将本地数据中心的存储扩展到 AWS 云。

参考文献:

<https://docs.aws.amazon.com/efs/latest/ug/how-it-works.html> <https://aws.amazon.com/efs/特点/>

<https://d1.awsstatic.com/whitepapers/AWS%20Storage%20Services%20Whitepaper-v9.pdf#page=9> 查看此亚马逊

逊 EFS 备忘单: <https://tutorialsdojo.com/amazon-efs/>

Q319.一家公司在应用负载均衡器后面的 Amazon ECS 集群中托管了一个应用程序。解决方案架构师正在构建一个复杂的 web 过滤解决方案,该解决方案允许或阻止基于请求来源国的 web 请求。但是,该解决方案仍应允许来自该国的特定 IP 地址。

架构师应该实现哪些步骤组合来满足这一需求?(选择两个。)

- A、在应用程序负载均衡器中,创建一个侦听器规则,该规则明确允许来自已批准 IP 地址的请求。
- B、在 AWS WAF web ACL 中添加另一条规则,该规则具有阻止来自特定国家/地区的请求的地理匹配条件。
- C、在托管应用程序的 VPC 前面放置一个传输网关,并设置网络 ACL,阻止来自特定国家的请求。
- D、使用 AWS WAF,创建一个 web ACL,其规则明确允许来自 IP 集中声明的已批准 IP 地址的请求。
- E、在应用程序负载均衡器中设置地理匹配条件,以阻止来自特定国家/地区的请求。

答:屋宇署

分析:

如果要基于请求来源国允许或阻止 web 请求,请创建一个或多个地理匹配条件。地理匹配条件列出了您的请求来源的国家。在该过程的后面,当您创建 web ACL 时,您将指定是允许还是阻止来自这些国家的请求。

您可以使用地理匹配条件和其他 AWS WAF 经典条件或规则来构建复杂的过滤。例如,如果要阻止某些国家,但仍允许来自该国家的特定 IP 地址,则可以创建包含地理匹配条件和 IP 匹配条件的规则。配置规则以阻止来自该国家/地区且与批准的 IP 地址不匹配的请求。作为另一个示例,如果您希望为特定国家的用户排定资源的优先级,则可以在两个不同的基于费率的规则中包含地理匹配条件。为首选国家/地区的用户设置较高的费率限制,并为所有其他用户设置较低的费率限制。

如果您使用 CloudFront 地理限制功能阻止某个国家访问您的内容,则该国家的任何请求都将被阻止,并且不会转发到 AWS WAF Classic。所以,如果你想允许,或者

基于地理位置和其他 AWS WAF 经典条件阻止请求,不应使用 CloudFront 地理限制功能。相反,您应该使用 AWS WAF 经典地理匹配条件。

因此,正确答案是:

- 使用 AWS WAF,创建一个 web ACL,其规则明确允许来自 IP 集中声明的已批准 IP 地址的请求。
- 在 AWS WAF web ACL 中添加另一条规则,该规则具有阻止来自特定国家/地区的请求的地理匹配条件。

“在应用程序负载均衡器中,创建一个侦听器规则,明确允许来自已批准 IP 地址的请求”选项是不正确的,因为侦听器规则只是使用您配置的协议和端口检查连接请求。它仅确定负载均衡器如何将请求路由到其注册的目标。

“在应用程序负载均衡器中设置地理匹配条件以阻止来自特定国家/地区的请求”选项不正确,因为您无法在应用程序负载均衡器中配置地理匹配条件。您必须改用 AWS WAF。该选项表示:在托管应用程序的 VPC 前面放置一个传输网关,并设置网络 ACL,阻止来自特定国家的请求,这是不正确的,因为 AWS 传输网关只是一种

服务，使客户能够将其亚马逊虚拟私有云（VPC）及其内部网络连接到单个网关。在这种情况下，不保证使用这种类型的网关。此外，网络 ACL 不适合阻止来自特定国家的请求。您必须改用 AWS WAF。

参考文献：

<https://docs.aws.amazon.com/waf/latest/developerguide/classic-web-acl-geo-conditions.html><https://docs.aws.amazon.com/waf/latest/developerguide/how-aws-waf-works.html> 查看此 AWS WAF 备忘单：

<https://tutorialsdojo.com/aws-waf/>

AWS 安全服务概述-WAF、Shield、CloudHSM、KMS： <https://www.youtube.com/watch?v=-1SRdeAmMo>

Q320. 一家公司计划将 MySQL 数据库从内部数据中心迁移到 AWS 云。该数据库将由一个传统批处理应用程序使用，该批处理程序在早上具有稳定的工作负载，但在晚上具有峰值负载，用于一天结束的处理。您需要选择一个 EBS 卷，该卷最多可以处理 450 GB 的数据，也可以用作 EC2 实例的系统引导卷。在这种情况下，以下哪种存储类型最经济高效？

- A、 亚马逊 EBS 吞吐量优化硬盘（st1）
- B、 亚马逊 EBS 配置 IOPS SSD（io1）
- C、 亚马逊 EBS 通用 SSD（gp2）
- D、 亚马逊 EBS 冷硬盘（sc1）

答案 C

分析：

在这种情况下，具有稳定工作负载的传统批处理应用程序需要关系型 MySQL 数据库。您应该使用的 EBS 卷必须处理最大 450 GB 的数据，还可以用作 EC2 实例的系统引导卷。由于 HDD 卷不能用作可引导卷，我们可以通过选择 SSD 卷来缩小选项范围。此外，SSD 卷更适合事务性数据库工作负载，如下表所示：

通用 SSD（gp2）卷提供了经济高效的存储，非常适合各种工作负载。这些卷提供了一位数的毫秒延迟，并能够在长时间内以 3000 IOPS 的速度爆发。AWS 设计的 gp2 卷可在 99% 的时间内提供所提供的性能。gp2 卷的大小范围可以从 1 GiB 到 16 TiB。Amazon EBS 配置的 IOPS SSD（io1）不正确，因为这不是最具成本效益的 EBS 类型，主要用于需要持续 IOPS 性能的关键业务应用程序。Amazon EBS 吞吐量优化 HDD（st1）是不正确的，因为它主要用于频繁访问、吞吐量高的工作负载。虽然它是一个低成本的 HDD 卷，但不能用作系统启动卷。亚马逊 EBS 冷硬盘（sc1）不正确。尽管 Amazon EBS 冷硬盘与通用 SSD 相比成本更低，但它不能用作系统引导卷。参考：

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html#EBSVolumeTypes_gp2 亚马逊

EBS 概述-SSD 与 HDD： <https://www.youtube.com/watch?v=LW7x8wyLFvw>

查看此亚马逊 EBS 备忘单： <https://tutorialsdojo.com/amazon-ebs/>

Q321. 贷款处理应用程序托管在 VPC 中的单个按需 EC2 实例中。为了提高应用程序的可伸缩性，您必须使用自动伸缩来自动添加新的 EC2 实例，以处理大量传入请求。

要将现有 EC2 实例添加到自动缩放组，应执行以下哪项？
（选择两个。）

- A、 您必须确保在自动缩放组中定义的可用性区域之一中启动实例。
- B、 必须首先停止实例。
- C、 您必须确保用于启动实例的 AMI 仍然存在。
- D、 您必须确保实例与自动缩放组位于不同的可用性区域。
- E、 您必须确保用于启动实例的 AMI 不再存在。

答覆

分析：

Amazon EC2 自动缩放为您提供了一个选项，可以通过将一个或多个 EC2 实例附加到现有的自动缩放组来启用自动缩放。附着实例后，它们将成为自动缩放组的一部分。

要附加的实例必须满足以下条件：

- 实例处于运行状态。
- 用于启动实例的 AMI 必须仍然存在。
- 该实例不是另一个自动缩放组的成员。
- 实例将启动到自动缩放组中定义的可用性区域之一。
- 如果自动扩展组具有连接的负载均衡器，则实例和负载均衡器必须都在 EC2Classic 或同一 VPC 中。如果自动扩展组具有连接的目标组，则实例和负载均衡器必须位于同一 VPC 中。

根据上述标准，以下是给定选项中的正确答案：

- 您必须确保用于启动实例的 AMI 仍然存在。
- 您必须确保在自动缩放组中定义的可用性区域之一中启动实例。

“您必须首先停止实例”选项不正确，因为您可以直接将正在运行的 EC2 实例添加到自动缩放组，而不停止它。这个选项说：您必须确保用于启动实例的 AMI 不再存在，这是不正确的，因为它应该相反。用于启动实例的 AMI 应该仍然存在。该选项表示：您必须确保实例位于不同的可用性区域，因为自动缩放组是不正确的，因为该实例应在自动缩放组中定义的可用性区之一中启动。

参考文献：

<http://docs.aws.amazon.com/autoscaling/latest/userguide/attach-instance-asg.html>

https://docs.aws.amazon.com/autoscaling/ec2/userguide/scaling_plan.html 查看此 AWS 自动缩放备忘单：

<https://tutorialsdojo.com/aws-auto-scaling/>

Q322. 电子商务应用程序在其订单管理系统中使用扇出消息模式。对于每个订单，它都会向 SNS 主题发送一条 Amazon SNS 消息，该消息会被复制并推送到多个 Amazon SQS 队列，以进行并行异步处理。Spot EC2 实例从每个 SQS 队列中检索消息并处理该消息。发生了一个事件，当 EC2 实例当前正在处理消息时，该实例突然终止，处理未及时处理。

在这种情况下，SQS 消息会发生什么？

- A、 消息将发送到 AWS 数据同步中的死信队列。
- B、 当 EC2 实例联机时，消息将被删除并在 SQS 中复制。

C、当消息可见性超时到期时，消息可供其他 EC2 实例处理

D、当消息在可见性超时内或之后恢复联机时，消息将自动分配给相同的 EC2 实例。

答案 C

分析：

“扇出”模式是将 Amazon SNS 消息发送到主题，然后复制并推送到多个 Amazon SQS 队列、HTTP 端点或电子邮件地址。这允许并行异步处理。例如，您可以开发一个应用程序，该应用程序在产品下订单时向主题发送 Amazon SNS 消息。然后，订阅该主题的 Amazon SQS 队列将收到新订单的相同通知。连接到其中一个队列的 Amazon EC2 服务器实例可以处理订单的处理或履行，而另一个服务器实例可以连接到数据仓库，用于分析收到的所有订单。当消费者从队列接收并处理消息时，消息将保留在队列中。Amazon SQS 不会自动删除消息。由于 Amazon SQS 是一个分布式系统，因此无法保证消费者实际收到消息（例如，由于连接问题或消费者应用程序中的问题）。因此，消费者必须在接收和处理消息后从队列中删除消息。

收到消息后，消息立即保留在队列中。为了防止其他消费者再次处理消息，Amazon SQS 设置了可见性超时，这是 Amazon SQ 阻止其他消费者接收和处理消息的一段时间。消息的默认可见性超时为 30 秒。最长为 12 小时。表示：当消息在可见性超时内或之后恢复联机时，消息将自动分配给同一 EC2 实例的选项不正确，因为一旦消息突然终止，消息将不会自动分配给相同的 EC2 实例。当消息可见性超时到期时，消息可供其他 EC2 实例处理。“当 EC2 实例联机时，消息将被删除并在 SQS 中复制”选项不正确，因为 EC2 实例在线时，消息不会被删除，也不会被 SQS 队列中复制。“消息将被发送到 AWS 数据同步中的死信队列”选项不正确，因为尽管消息可以通过编程方式发送到死信队列（DLQ），但它不会由 AWS 数据 sync 处理，而是由 Amazon SQS 处理。AWS 数据同步主要用于简化与 AWS 的迁移。它使得在本地存储和 AmazonS3 或 AmazonElasticFile System（AmazonEFS）之间在线移动大量数据变得简单快捷。参考文献：

<http://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-visibility-超时>。

[htmlhttps://docs.aws.amazon.com/sns/latest/dg/sns-common-scenarios.html](https://docs.aws.amazon.com/sns/latest/dg/sns-common-scenarios.html) 查看此亚马逊 SQS 备忘单：

<https://tutorialsdojo.com/amazon-sqs/>

Q323.公司需要使用 Amazon S3 存储不可复制的财务文档。对于季度报告，要求在 3 个月后检索文件。有时进行突击审计，这需要访问他们需要立即提交的存档数据。

您将如何以经济高效的方式满足这一要求？

A、使用 AmazonS3 标准

B、使用 Amazon S3 标准-不经常访问

C、使用 Amazon S3-智能分层

D、使用亚马逊冰川深度档案

答案 B

分析：

在这种情况下，要求提供一种经济高效的存储选项，并能够立即访问或检索存档数据。经济高效的选项是亚马逊冰川深度档案和亚马逊 S3 标准-不频繁访问（标准-IA）。然而，前一个选项不是为快速检索突击审计所需的数据而设计的。因此，使用 Amazon Glacier Deep Archive 是不正确的，最好的答案是使用 Amazon S3 标准-不经常访问。使用 AmazonS3 标准是不正确的，因为在这种情况下，标准存储类不具有成本效益。它的成本高于冰川深度档案和 S3 标准-很少访问。使用 Amazon S3-智能分层是不正确的，因为与标准存储类和 S3 标准-不频繁访问相比，智能分层存储类需要额外的费用来监控和自动化 S3 存储桶中的每个对象。

Amazon S3 标准-不频繁访问是一个 AmazonS3 存储类，用于访问频率较低但需要快速访问的数据。标准-IA 提供了 Amazon S3 标准的高耐用性、吞吐量和低延迟，每 GB 存储价格和每 GB 检索费用较低。这种低成本和高性能的结合使得 Standard-IA 成为长期存储、备份和灾难恢复数据存储的理想选择。标准-IA 存储类是在对象级别设置的，可以与标准存储类存在于同一存储桶中，允许您使用生命周期策略在存储类之间自动转换对象，而无需任何应用程序更改。参考文献：

[https://aws.amazon.com/s3/storage-](https://aws.amazon.com/s3/storage-classes/)

[classes/ https://aws.amazon.com/s3/faqs/](https://aws.amazon.com/s3/faqs/)

查看此 Amazon S3 备忘单：

<https://tutorialsdojo.com/amazon-s3/>

S3 标准 vs S3 标准 IA vs S3 单区 IA vs S3 智能分层：<https://tutorialsdojo.com/s3-standard-vs-s3-standard-ia-vs-s3-one-zone-ia/>

Q324.公司有一个运行的 m5ad。具有默认连接的 75 GB SSD 实例存储备份卷的大型 EC2 实例。关闭它，然后启动实例。您注意到先前保存在连接卷上的数据不再可用。这可能是什么原因？

- A、EC2 实例使用 EBS 支持的根卷，这些根卷是短暂的，仅在实例的生命周期内有效。
- B、EC2 实例使用实例存储卷，这些卷是短暂的，只在实例的生命周期内有效。
- C、实例的容量不够大，无法处理所有处理数据。
- D、该实例被病毒攻击，该病毒会清除所有数据。

答案 B

分析：

实例存储为实例提供临时块级存储。此存储位于物理连接到主机的磁盘上。实例存储非常适合于频繁更改的信息的临时存储，如缓冲区、缓存、暂存数据和其他临时内容，或跨实例组复制的数据，如负载平衡的 web 服务器池。实例存储由作为块设备公开的一个或多个实例存储卷组成。实例存储的大小以及可用设备的数量因实例类型而异。虽然实例存储专用于特定实例，但磁盘子系统在主机上的实例之间共享。实例存储中的数据仅在其关联实例的生存期内保持。如果实例重新启动（有意或无意），则实例存储中的数据将持续存在。但是，在以下情况下，实例存储中的数据会丢失：

- 基础磁盘驱动器出现故障
- 实例停止
- 实例终止

参考：

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/InstanceStorage.html> 亚马逊 EC2 概述：

https://www.youtube.com/watch?v=7VsGIHT_jQE

查看此 Amazon EC2 备忘单：<https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/>

Q325.公司有多微服务向 Amazon SQS 队列发送消息，并有一个后端应用程序轮询队列以处理消息。该公司还有一个服务水平协议（SLA），它定义了从收到消息到发送响应的可接受时间。后端操作是 I/O 密集型的，

因为消息数量不断增长，导致公司错过其 SLA。解决方案架构师必须实现新的体系结构，以改进应用程序的处理时间和负载管理。以下哪项是最有效的解决方案，可以满足给定的要求？

- A、创建后端应用程序的 EC2 实例的 AMI，并将其启动到集群放置组。
- B、创建后端应用程序的 EC2 实例的 AMI。使用该图像设置自动缩放组，并基于目标值为 80% 的 CPUUtilization 度量配置目标跟踪缩放策略。
- C、创建后端应用程序的 EC2 实例的 AMI，并将其替换为更大的实例大小。
- D、创建后端应用程序的 EC2 实例的 AMI。使用该图像设置自动缩放组，并基于近似 GeoFolderMessage 度量配置目标跟踪缩放策略。

答案 D

分析：

Amazon 简单队列服务（SQS）是一种完全管理的消息队列服务，它使您能够分离和扩展微服务、分布式系统和无服务器应用程序。SQS 消除了与管理面向消息的中间件相关的复杂性和开销，并使开发人员能够专注于区分工作。使用 SQS，您可以在任何卷上的软件组件之间发送、存储和接收消息，而不会丢失消息或要求其他服务可用。

当应用程序具有时间敏感消息并且需要确保在特定时间段内处理消息时，ApproximateAgeOfOldestMessage 度量非常有用。您可以使用此指标设置 Amazon CloudWatch 警报，当消息在队列中停留较长时间时，该警报会发出警报。您还可以使用警报采取行动，例如增加消费者数量，以更快地处理消息。

使用目标跟踪缩放策略，您可以根据特定 CloudWatch 指标的目标值缩放（增加或减少容量）。要为此策略创建自定义度量，您需要使用 AWS CLI 或 AWS SDK。请注意，您需要首先从实例创建 AMI，然后才能创建自动缩放组，以基于 ApproximateAgeOfOldestMessage 度量缩放实例。

因此，正确的答案是：创建后端应用程序的 EC2 实例的 AMI。使用该图像设置自动缩放组，并基于近似 GeoFolderMessage 度量配置目标跟踪缩放策略。

该选项表示：创建后端应用程序的 EC2 实例的 AMI。使用该图像设置自动缩放组，并基于目标值为 80% 的 CPUUtilization 度量配置目标跟踪缩放策略不正确。尽管这将改进后端处理，但基于 CPUUtilization 度量的缩放策略并不适用于时间敏感的消息，因为您需要确保在特定时间段内处理消息。它只会根据当前实例的 CPU 利用率触发扩展活动，而不是根据消息的年龄，这是满足 SLA 的关键因素。为了满足场景中的要求，您应该使用近似 GeoFolderMessage 度量。

“创建后端应用程序的 EC2 实例的 AMI 并用更大的实例大小替换它”的选项是不正确的，因为用大的实例替换实例不足以动态处理任何级别的工作负载。您需要实现自动缩放组以自动调整计算资源的容量。

“创建后端应用程序 EC2 实例的 AMI 并将其启动到集群放置组”的选项是不正确的，因为集群放置组只是 EC2 实例逻辑分组。您必须为 EC2 实例设置一个自动缩放组，并根据近似的 GeoFolderMessage 度量配置目标跟踪缩放策略，而不是在放置组中启动实例。

参考文献：

<https://aws.amazon.com/about-aws/whats-new/2016/08/new-amazon-cloudwatch-metric-for-amazon-sqs-监视最早消息的时间/>

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-available-cloudwatchmetrics.html>

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-using-sqs-queue.html> 查看此亚马逊 SQS 备忘单：

<https://tutorialsdojo.com/amazon-sqs/>

Q326. 公司需要安全访问多个应用程序使用的 Amazon RDS for MySQL 数据库。每个 IAM 用户必须使用短期身份验证令牌连接到数据库。在这种情况下，以下哪项是最合适的解决方案？

- A、使用 AWS Secrets Manager 生成和存储短期身份验证令牌。
- B、使用 MFA 令牌访问和连接数据库。
- C、使用 IAM DB 身份验证，并使用 AWS 在 MySQL 中提供的 AWSAuthenticationPlugin 创建数据库帐户。
- D、使用 AWS SSO 访问 RDS 数据库。

答案 C

分析：

您可以使用 AWS 身份和访问管理（IAM）数据库身份验证对数据库实例进行身份验证。IAM 数据库身份验证与 MySQL 和 PostgreSQL 一起工作。使用这种身份验证方法，连接到 DB 实例时不需要使用密码。身份验证令牌是您使用的字符串，而不是密码。生成身份验证令牌后，它在到期前 15 分钟内有效。如果尝试使用过期令牌进行连接，连接请求将被拒绝。

由于该场景要求您创建短期身份验证令牌以访问 Amazon RDS 数据库，因此您可以在连接到数据库实例时使用 IAM 数据库身份验证。处理身份验证

AWSAuthenticationPlugin——一个 AWS 提供的插件，与 IAM 无缝协作，以验证您的 IAM 用户。

IAM 数据库身份验证提供了以下好处：

进出数据库的网络流量使用安全套接字层（SSL）加密。您可以使用 IAM 集中管理对数据库资源的访问，而不是单独管理每个 DB 实例上的访问。

对于在 Amazon EC2 上运行的应用程序，您可以使用特定于您的 EC2 实例的配置文件凭据来访问您的数据库，而不是密码。因此，正确的答案是这样的选项：使用 IAM DB 身份验证，并使用 AWS 提供的 AWSAuthenticationPlugin 插件在 MySQL 中创建数据库帐户。“使用 AWS SSO 访问 RDS 数据库”选项是不正确的，因为 AWS SSO 仅允许您集中管理通过 AWS 组织管理的所有 AWS 帐户的 SSO 访问和用户权限。

“使用 AWS Secrets Manager 生成和存储短期身份验证令牌”选项不正确，因为 AWS Secrets Manager 不适合创建用于访问 Amazon RDS 数据库的身份验证令牌。它主要用于存储密码、机密和其他敏感凭据。它也不能生成短期令牌。您必须改用 IAM DB 身份验证。“使用 MFA 令牌访问和连接数据库”选项不正确，因为您无法使用 MFA 标记连接数据库。您必须设置 IAM DB 身份验证。

参考文献：

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/UsingWithRDS.IAMDBAuth.DBAccounts.html>。连接

ing.html

查看此 AWS IAM 备忘单：

<https://tutorialsdojo.com/aws-identity-and-access-management-iam/>

Q327. 一家公司有一个 web 应用程序托管在位于两个可用性区域中的 EC2 实例组上，这些可用性区域都位于应用程序负载均衡器的后面。作为解决方案架构师，您必须添加健康检查配置，以确保应用程序高度可用。

您将实施哪些健康检查？

- A、ICMP 健康检查
- B、FTP 运行状况检查
- C、HTTP 或 HTTPS 健康检查
- D、TCP 健康检查

答案 C

分析：

负载均衡器从客户端接收请求，并将它们分布在已注册的 EC2 实例中

使用负载均衡器。您可以创建一个同时监听 HTTP（80）和 HTTPS（443）端口的负载均衡器。如果指定 HTTPS 侦听器向端口 80 上的实例发送请求，负载均衡器将终止请求，并且负载均衡器与实例之间的通信不会加密。如果 HTTPS 侦听器向端口 443 上的实例发送请求，则从负载均衡器到实例的通信将被加密。

如果负载均衡器使用加密连接与实例通信，则可以选择启用实例身份验证。这确保负载均衡器仅在其公钥与此目的指定给负载均衡器的密钥匹配时才与实例通信。本场景中提到的 ELB 类型是应用弹性负载均衡器。如果您希望为具有 HTTP 和 HTTPS 流量的 web 应用程序提供灵活的功能集，则可以使用此选项。相反，它只允许两种类型的健康检查：HTTP 和 HTTPS。

因此，正确答案是：HTTP 或 HTTPS 健康检查。

ICMP 健康检查和 FTP 健康检查不正确，因为它们不受支持。TCP 运行状况检查不正确。TCP 健康检查仅在网络负载均衡器和经典负载均衡器中提供。

参考文献：

<http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-healthchecks.html>

<https://docs.aws.amazon.com/elasticloadbalancing/latest/application/introduction.html> 查看 AWS 弹性负载均衡（ELB）备忘单：

<https://tutorialsdojo.com/aws-elastic-load-balancing-elb/>

EC2 实例健康检查 vs ELB 健康检查 vs 自动缩放和自定义健康检查：

<https://tutorialsdojo.com/ec2-instance-health-check-vs-elb-health-check-vs-auto-scaling-and-custom-健康检查/>

AWS 服务备忘单比较：<https://tutorialsdojo.com/comparison-of-aws-services/>

Q328. 初创公司需要为其在 Amazon EC2 上运行的 .NET web 应用程序使用共享文件系统 Windows 实例。文件系统必须提供高水平的吞吐量和 IOPS，也可以与 Microsoft Active Directory 集成。

您应该使用哪种服务来实现此要求？

- A、用于 Windows 文件服务器的 Amazon FSx
- B、AWS 存储网关-文件网关
- C、Amazon EBS 为 SSD 卷提供 IOPS
- D、Amazon 弹性文件系统

答：

分析:

Amazon FSx for Windows 文件服务器提供完全管理、高度可靠和可扩展的文件存储, 可通过行业标准服务消息块 (SMB) 协议访问。它构建在 Windows Server 上, 提供了广泛的管理功能, 如用户配额、最终用户文件还原和 Microsoft Active Directory (AD) 集成。

Amazon FSx 支持使用 Microsoft 的分布式文件系统 (DFS) 名称空间, 以跨同一名称空间中的多个文件系统扩展性能, 最高可达数十 Gbps 和数百万 IOPS。

此场景中的关键短语是“文件系统”和“Active Directory 集成”。您需要实现满足这些要求的解决方案。在给出的选项中, 可能的答案是 FSx Windows 文件服务器和文件网关。但您需要考虑的是, 该问题还指出, 您需要提供高水平的吞吐量和 IOPS。Amazon FSx Windows 文件服务器可以将存储扩展到数百 PB 的数据, 具有数十 GB/s 的吞吐量性能和数百万 IOPS。因此, 正确答案是: Amazon FSx for Windows 文件服务器。Amazon EBS 配置的 IOPS SSD 卷不正确, 因为这只是一个块存储卷, 而不是一个成熟的文件系统。Amazon EBS 主要用作 EC2 实例的持久块存储。Amazon Elastic 文件系统是不正确的, 因为在场景中声明启动使用 Amazon EC2 Windows 实例。

记住, Amazon EFS 只能处理 Linux 工作负载。AWS 存储网关-文件网关不正确。

尽管它可以用作 Windows 的共享文件系统, 也可以与 Microsoft Active Directory 集成, 但与 AWS 存储网关相比, Amazon FSx 仍然具有更高的吞吐量和 IOPS。亚马逊 FSX 能够提供数十万 (甚至数百万) 的 IOPS。

参考文献:

<https://aws.amazon.com/fsx/windows/faqs/> <https://docs.aws.amazon.com/fsx/latest/WindowsGuide/what-is.html> 查看此亚马逊 FSx 备忘单: <https://tutorialsdojo.com/amazon-fsx/>

Q329. 一家公司计划实施混合架构。他们需要创建从亚马逊虚拟私有云 (VPC) 到内部网络的专用连接。与基于互联网的解决方案相比, 连接必须提供高带宽吞吐量和更一致的网络体验。以下哪项可用于创建专有网络和公司内部网络之间的专用连接?

- A、 转接 VPC
- B、 AWS 站点到站点 VPN
- C、 AWS 直接连接
- D、 具有等成本多路径路由的过境网关 (ECMP)

答案 C

分析:

AWS Direct Connect 通过标准以太网光纤电缆将您的内部网络链接到 AWS 直接连接位置。电缆的一端连接到路由器, 另一端连接到 AWS 直连路由器。

通过这种连接, 您可以直接创建到公共 AWS 服务 (例如, 到 Amazon S3) 或到 Amazon VPC 的虚拟接口, 绕过网络路径中的互联网服务提供商。AWS 直接连接位置提供了对其关联区域内 AWS 的访问。您可以使用公共区域或 AWS GovCloud (美国) 中的单个连接访问所有其他公共区域的公共 AWS 服务

因此, 正确答案是: AWS 直接连接。

“Transit VPC”选项是不正确的, 因为这本身不足以将您的内部网络集成到您的 VPC。您必须使用 VPN 或直接连接。中转 VPC 主要用于连接多个 VPC 和远程网络, 以创建全球网络中转中心, 而不是用于建立与本地网络的专用连接。“具有同等成本多路径路由 (ECMP) 的中转网关”选项不正确, 因为中转网关通常用于通过中央

集线器连接多个 VPC 和内部网络。与 transit VPC 一样，transit 网关无法建立与您的内部网络的直接和专用连接。

表示：AWS 站点到站点 VPN 的选项不正确，因为这种类型的连接跨越公共互联网。此外，与基于互联网的解决方案相比，它不能提供高带宽吞吐量和更一致的网络体验。参考文献：

<https://aws.amazon.com/premiumsupport/knowledge-center/connect-vpc/>

<https://docs.aws.amazon.com/directconnect/latest/UserGuide/Welcome.html> 查看此 AWS Direct Connect 备忘单：

<https://tutorialsdojo.com/aws-direct-connect/>

S3 传输加速 vs 直连 vs VPN vs 雪球 vs 雪地车：

<https://tutorialsdojo.com/s3-transfer-acceleration-vs-direct-connect-vs-vpn-vs-snowball-vs-snowmobile/AWS> 服务备

忘单比较：<https://tutorialsdojo.com/comparison-of-aws-services/>

Q330.一家初创公司推出了一批按需 EC2 实例，以托管大型多人在线角色扮演游戏（MMORPG）。EC2 实例配置了自动缩放和 AWS 系统管理器。可以使用什么来配置 EC2 实例，而不必建立到每个实例的 RDP 或 SSH 连接？

- A、EC2Config
- B、AWS 配置
- C、运行命令
- D、AWS 代码管道

答案 C

分析：

您可以使用控制台中的 Run 命令来配置实例，而无需登录到每个实例。

AWS Systems Manager 运行命令允许您远程安全地管理托管实例的配置。托管实例是混合环境中为 Systems Manager 配置的任何 Amazon EC2 实例或本地计算机。运行命令使您能够自动执行常见的管理任务，并按比例执行临时配置更改。您可以使用 AWS 控制台、AWS 命令行界面、AWS Windows PowerShell 工具或 AWS SDK 中的运行命令。运行命令是免费提供的。因此，正确答案是：运行命令。

参考：

<https://docs.aws.amazon.com/systems-manager/latest/userguide/execute-remote-commands.html> AWS 系统管理器概述：

<https://www.youtube.com/watch?v=KVFKyMAHxqY>

查看 AWS 系统管理器备忘单：<https://tutorialsdojo.com/aws-systems-manager/>

Q331.一家投资银行拥有一个分布式批处理应用程序，该应用程序托管在具有 SQS 队列的 Spot EC2 实例的自动扩展组中。您将组件配置为使用客户端缓冲，以便首先缓冲来自客户端的调用，然后将其作为批处理请求发送给 SQS。SQS 队列阻止其他消费组件接收和处理消息的时间段是多久？

- A、处理超时

- B、接收超时
- C、组件超时
- D、可见性超时

答案 D

分析：

可见性超时是 Amazon SQS 阻止其他消费组件接收和处理消息的一段时间。

当消费者从队列接收并处理消息时，消息将保留在队列中。Amazon SQS 不会自动删除消息。由于 Amazon SQS 是一个分布式系统，因此无法保证消费者实际收到消息（例如，由于连接问题或消费者应用程序中的问题）。因此，消费者必须在接收和处理消息后从队列中删除消息。

收到消息后，消息立即保留在队列中。为了防止其他消费者再次处理消息，Amazon SQS 设置了可见性超时，这是 Amazon SQ 阻止其他消费者接收和处理消息的一段时间。消息的默认可见性超时为 30 秒。最长为 12 小时。

参考文献：

<https://aws.amazon.com/sqs/faqs/>

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-visibility-timeout.html>

查看此亚马逊 SQS 备忘单：

<https://tutorialsdojo.com/amazon-sqs/对的>：

Q332. 一个组织创建了一个新的 CloudFormation 模板，该模板创建了连接到一个弹性负载均衡器（ELB）的 4 个 EC2 实例。在创建 AWS 堆栈时，应配置模板的哪个部分以获取 ELB 的域名服务器主机名？

- A、资源
- B、参数
- C、映射
- D、产出

答案 D

分析：

Outputs 是 CloudFormation 模板的可选部分，它描述了在查看堆栈属性时返回的值。

参考：

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/template-anatomy.html><https://aws.amazon.com/cloudformation/>

查看此 AWS CloudFormation 备忘单：

<https://tutorialsdojo.com/aws-cloudformation/>

AWS CloudFormation-模板、堆栈和变更集:

<https://www.youtube.com/watch?v=9Xpuprxg7aY>

Q333.一家公司计划在 AWS 中启动一个高性能计算（HPC）集群，进行计算流体动力学（CFD）模拟。该解决方案应该扩展模拟工作，使用更多可调参数进行实验，以获得更快、更准确的结果。集群由托管在 t3a 上的 Windows 服务器组成。中等 EC2 实例。作为解决方案架构师，您应该确保体系结构提供更高的带宽、更高的每秒数据包（PPS）性能，并始终降低实例间延迟。

架构师应该实施哪种解决方案来实现上述要求最合适、最具成本效益？

- A、使用 AWS ParallelCluster 部署和管理 HPC 集群，以提供更高的带宽、更高的分组持续时间（PPS）性能和更低的实例间延迟。
- B、在 Windows EC2 实例上使用 Intel 82599 虚拟功能（VF）接口启用增强网络。
- C、在 Windows EC2 实例上使用弹性结构适配器（EFA）启用增强网络。
- D、在 Windows EC2 实例上使用弹性网络适配器（ENA）启用增强网络。

答案 D

分析:

增强型网络使用单根 I/O 虚拟化（SR-IOV）在支持的实例类型上提供高性能网络功能。SR-IOV 是一种设备虚拟化方法，与传统虚拟化网络接口相比，它提供了更高的 I/O 性能和更低的 CPU 利用率。增强型网络提供了更高的带宽、更高的每秒分组（PPS）性能，以及一致更低的实例间延迟。使用增强型网络不收取额外费用。Amazon EC2 通过弹性网络适配器（ENA）提供增强的网络功能。对于支持的实例类型，它支持高达 100 Gbps 的网络速度。弹性网络适配器（ENA）提供支持 VPC 网络所需的传统 IP 网络功能。弹性结构适配器（EFA）只是具有附加功能的弹性网络适配器（ENA）。它提供了 ENA 的所有功能，以及附加的操作系统旁路功能。OS 旁路是一种访问模型，允许 HPC 和机器学习应用程序直接与网络接口硬件通信，以提供低延迟、可靠的传输功能。

Windows 实例不支持 EFA 的操作系统旁路功能。如果将 EFA 附加到 Windows 实例，则该实例将作为弹性网络适配器，而不具有添加的 EFA 功能。

因此，正确的答案是在 Windows EC2 实例上使用弹性网络适配器（ENA）启用增强网络。在 Windows EC2 实例上使用弹性结构适配器（EFA）启用增强网络是不正确的，因为 Windows 实例不支持弹性结构适配器的操作系统旁路功能。虽然您可以将 EFA 连接到 Windows 实例，但这只是一个常规的弹性网络适配器，没有添加 EFA 功能。此外，它不支持 t3a。HPC 群集中使用的中等实例类型。在 Windows EC2 实例上使用 Intel 82599 虚拟功能（VF）接口启用增强网络是不正确的，因为尽管您可以在 Windows EC3 实例上附加 Intel 82599 Virtual Function（VF），以提高其网络功能，但它不支持 t3a。HPC 群集中使用的中等实例类型。

使用 AWS ParallelCluster 部署和管理 HPC 集群以提供更高的带宽、更高的每秒数据包（PPS）性能和更低的实例间延迟是不正确的，因为 AWS ParallelCluster 只是一个 AWS 支持的开源集群管理工具，可使您轻松部署和管理高性能

AWS 上的性能计算（HPC）集群。与 ENA 或 EFA 不同，它不提供更高的带宽、更高的每秒分组（PPS）性能和更低的实例间延迟。

参考文献:

[https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/enhanced-](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/enhanced-networking.html)

[networking.html](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/efa.html)<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/efa.html> 正确:

Q334.本地银行有一个内部应用程序，用于处理私有子网中的敏感金融数据。EC2 工作者实例处理数据后，它们将被传递到 S3，供其他服务接收。您应该如何设计此解决方案，以使数据不通过公共互联网？

- A、在专用子网中为 NAT 网关提供相应的路由条目，将数据引导到 S3。
- B.在公用子网中创建具有相应路由条目的互联网网关，将数据定向到 S3。
- C、配置 VPC 端点以及将数据引导到 S3 的相应路由条目。
- D、配置一个中转网关以及将数据引导到 S3 的相应路线条目。

答案 C

分析：

在此场景中，您必须理解的一个重要概念是，您的 VPC 和 S3 bucket 位于更大的 AWS 网络中。然而，默认情况下，从 VPC 到 S3 bucket 的流量是通过公共互联网的。为了更好地保护传输中的数据，您可以设置一个 VPC 端点，以便来自 VPC 的传入流量不会通过公共互联网，而是通过专用 AWS 网络。

VPC 端点使您能够私自将 VPC 连接到由 PrivateLink 提供支持的 AWS 服务和 VPC 端点服务，而无需互联网网关、NAT 设备、VPN 连接或 AWS 直接连接。VPC 中的实例不需要公共 IP 地址与服务中的资源通信。专有网络和其他服务之间的流量不会离开亚马逊网络。

端点是虚拟设备。它们是水平扩展、冗余和高可用的 VPC 组件，允许 VPC 中的实例和服务之间进行通信，而不会对网络流量施加可用性风险或带宽限制。因此，正确的答案是：配置一个 VPC 端点以及一个将数据引导到 S3 的相应路由条目。

该选项表示：在公共子网中创建一个具有相应路由条目的 Internet 网关，将数据引导到 S3，这是不正确的，因为 Internet 网关用于公共子网的实例，以便访问 Internet。

“配置中转网关以及将数据引导至 S3 的相应路由条目”选项不正确，因为中转网关用于通过中央集线器互连 VPC 和内部网络。由于 Amazon S3 不在 VPC 范围内，您仍然无法私下连接到它。

该选项表示：在专用子网中为 NAT 网关提供相应的路由条目，将数据引导到 S3，这是不正确的，因为 NAT 网关允许专用子网的实例访问 Internet，但反之亦然。

参考文献：

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-endpoints.html>

<https://docs.aws.amazon.com/vpc/latest/userguide/vpce-gateway.html> 查看此亚马逊 VPC 备忘单：

<https://tutorialsdojo.com/amazon-vpc/>

Q335.在线购物平台托管在按需 EC2 实例的自动扩展组上，具有默认的自动扩展终止策略，且未配置实例保护。该系统部署在美国西部地区（US-West-1）的三个可用性区域，前端有一个应用程序负载均衡器，为购物平台提供高可用性和容错性。美国西部 1a、美国西部 1b 和美国西部 1c 可用区分别有 10 个、8 个和 7 个运行实例。由于传入流量数量较少，已触发运行规模。自动缩放组将执行以下哪项操作来确定在此场景中首先终止哪个实例？（选择三个。）

- A、选择距离下一个计费小时最远的实例。
- B、选择最接近下一个计费小时的实例。
- C、选择具有最新启动配置的实例。

D、选择实例数量最多的可用性区域，即本场景中的 us-west-1a 可用性区域。

E、选择实例数最少的可用性区域，即本场景中的 us-west-1c 可用性区域。

F、选择具有最早启动配置的实例。

答：屋宇署

分析：

默认终止策略旨在帮助确保网络体系结构均匀地跨越可用性区域。使用默认终止策略，自动缩放组的行为如下：

- 1.
- 2.
3. 如果多个可用性区域中存在实例，请选择实例最多且至少有一个实例不受扩展保护的可用性区域。如果有多个可用性区域具有此数量的实例，请选择具有使用最早启动配置的实例的可用性区域。
4. 5.
- 6.
7. 确定所选可用性区域中哪些未受保护的实例使用最早的启动配置。如果有一个这样的实例，请终止它。
- 8.
- 9.
- 10.
11. 如果基于上述标准有多个实例要终止，则确定哪些未受保护的实例最接近下一个计费小时。（这有助于最大限度地利用 EC2 实例并管理 Amazon EC2 使用成本。）如果有一个这样的实例，请终止它。
- 12.
- 13.
- 14.
15. 如果有多个未受保护的实例最接近下一个计费小时，请随机选择其中一个实例。
- 16.
- 17.

以下流程图说明了默认终止策略的工作方式：

参考：

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-instance-termination.html#default-终止-策略>查看此 AWS

自动缩放备忘单：

<https://tutorialsdojo.com/aws-auto-scaling/>

Q336.应用程序托管在按需 EC2 实例中，并使用 Amazon SDK 与其他 AWS 服务进行通信，如 S3、DynamoDB 等。作为即将进行的 IT 审计的一部分，您需要确保对 AWS 资源的所有 API 调用都被记录并持久存储。您应该使用哪种服务来满足此要求？

- A、Amazon API 网关
- B、AWS CloudTrail
- C、亚马逊云观察
- D、AWS X 射线

答案 B

分析：

AWS CloudTrail 通过记录 AWS 管理控制台操作和 API 调用，提高了用户和资源活动的可见性。您可以识别哪些用户和帐户调用了 AWS，从中调用的源 IP 地址，以及调用发生的时间。Amazon CloudWatch 是不正确的，因为它主要用于基于服务器指标的系统监控。它无法跟踪对 AWS 资源的 API 调用。AWS X 射线是不正确的，因为它通常用于调试和分析具有请求跟踪的微服务应用程序，以便找到问题和性能的根本原因。与 CloudTrail 不同，它不记录对 AWS 资源的 API 调用。Amazon API 网关不正确，因为它不用于记录对 AWS 资源的每个 API 调用。它是一个完全受管理的服务，使开发人员可以轻松地创建、发布、维护、监控和保护任何规模的 API。

参考：

<https://aws.amazon.com/cloudtrail/>

查看此 AWS CloudTrail 备忘单：<https://tutorialsdojo.com/aws-cloudtrail/>

Q337. 一家公司最近采用了混合云架构，并计划将本地托管的数据库迁移到 AWS。该数据库目前拥有超过 50 TB 的消费者数据，处理高度事务性（OLTP）工作负载，预计还会增长。解决方案架构师应确保数据库符合 ACID，并能够处理应用程序的复杂查询。架构师应该使用哪种类型的数据库服务？

- A、亚马逊 RDS
- B、亚马逊红移
- C、亚马逊发电机 B
- D、亚马逊极光

答案 D

分析：

Amazon Aurora（Aurora）是一个完全管理的关系数据库引擎，与 MySQL 和 PostgreSQL 兼容。您已经知道 MySQL 和 PostgreSQL 如何将高端商业数据库的速度和可靠性与开源数据库的简单性和成本效益结合起来。您今天在现有 MySQL 和 PostgreSQL 数据库中使用的代码、工具和应用程序可以与 Aurora 一起使用。对于某些工作负载，Aurora 可以提供高达 MySQL 吞吐量的五倍和高达 PostgreSQL 吞吐量的三倍，而无需对大多数现有应用程序进行更改。Aurora 包括一个高性能存储子系统。它的 MySQL 和 PostgreSQL 兼容的数据库引擎是定制的，以利用这种快速的分布式存储。底层存储根据需要自动增长，最高可达 64 兆字节（TiB）。Aurora 还自动化和标准化数据库集群和复制，这通常是数据库配置和管理中最具挑战性的方面。

对于 Amazon RDS MariaDB DB 实例，当使用 InnoDB 文件/表空间时，最大配置存储限制将表的大小限制为最大 64 TB。这一限制也限制了系统

表空间的最大大小为 16 TB。默认情况下，Amazon RDS MariaDB DB 实例的 InnoDB 文件每表表空间（每个表都在自己的表空间中）。因此，正确答案是亚马逊极光。

Amazon Redshift 是不正确的，因为它主要用于 OLAP 应用程序，而不是 OLTP。此外，它不能自动扩展以处理数据库的指数增长。亚马逊 DynamoDB 是不正确的。尽管您可以使用它来创建符合 ACID 的数据库，但它不能处理复杂的查询和高事务性（OLTP）工作负载。Amazon RDS 不正确。尽管该服务可以托管一个符合 ACID 的关系数据库，该数据库可以处理复杂的查询和事务性（OLTP）工作负载，但它仍然无法扩展以处理数据库的增长。亚马逊极光是更好的选择，因为它的底层存储可以根据需要自动增长。参考文献：

<https://aws.amazon.com/rds/aurora/>

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/SQLtoNoSQL.html>

<https://aws.amazon.com/nosql/>

亚马逊极光概述：

<https://youtu.be/iwS1h7rLNBQ>

查看此亚马逊极光备忘单：<https://tutorialsdojo.com/amazon-aurora/>

Q338.一家医疗保健公司在其内部存储系统中存储敏感的患者健康记录。这些记录必须无限期保存，并在保存后免受任何类型的修改。法规遵从性法规要求记录必须具有粒度访问控制，并且必须在所有级别对每个数据访问进行审计。目前，有数以百万计的过时记录无法被其 web 应用程序访问，其内部存储空间很快就用完了。解决方案架构师必须设计一个解决方案，立即将现有记录移动到 AWS，并支持不断增长的新健康记录。

以下哪一项是解决方案架构师应实施以满足上述要求的最合适的解决方案？

- A、 设置 AWS 存储网关，将现有健康记录从本地网络移动到 AWS 云。启动一个新的 Amazon S3 存储桶来存储现有记录和新记录。在存储桶中启用 AWS CloudTrail 和管理事件以及 Amazon S3 对象锁。
- B、 设置 AWS 数据同步，将现有健康记录从本地网络移动到 AWS 云。启动新的 Amazon S3 存储桶，以存储现有记录和新记录。使用数据事件和 Amazon S3 对象锁在 bucket 中启用 AWS CloudTrail。
- C、 设置 AWS 存储网关，将现有健康记录从本地网络移动到 AWS 云。启动 Amazon EBS 支持的 EC2 实例，以存储现有记录和新记录。启用 Amazon S3 服务器访问日志记录和存储桶中的 S3 对象锁定。
- D、 设置 AWS 数据同步，将现有健康记录从本地网络移动到 AWS 云。启动新的 Amazon S3 存储桶，以存储现有记录和新记录。在存储桶中启用 AWS CloudTrail 和管理事件以及 Amazon S3 对象锁。

答案 B

分析：

AWS 存储网关是一组混合云服务，可让您在本地访问几乎无限的云存储。客户使用 Storage Gateway 将 AWS 云存储与现有的现场工作负载集成，从而简化存储管理并降低关键混合云存储用例的成本。其中包括将备份移动到云，使用云存储支持的本地文件共享，以及为本地应用程序提供 AWS 中数据的低延迟访问。AWS 数据同步是一种在线数据传输服务，可简化、自动化和加速本地存储系统和 AWS 存储服务之间以及 AWS 存储系统之间的数据移动。您可以使用 DataSync 将活动数据集迁移到 AWS，归档数据以释放本地存储容量，将数据复制到 AWS 以实现业务连续性，或将数据传输到云以进行分析和处理。

AWS 存储网关和 AWS 数据同步都可以将数据从本地数据中心发送到 AWS，反之亦然。但是，AWS Storage Gateway 更适合用于通过复制数据集成存储服务，而 AWS DataSync 更适合于需要移动或迁移数据的工作负载。

您还可以使用数据同步和文件网关的组合来最小化本地基础设施，同时将本地应用程序无缝连接到云存储。AWS 数据同步使您能够自动化和加速向 AWS 存储服务的在线数据传输。文件网关是一个完全受管理的解决方案，它将自动并加速本地存储系统和 AWS 存储服务之间的数据复制。

AWS CloudTrail 是一项 AWS 服务，可帮助您对 AWS 帐户进行治理、合规、运营和风险审计。用户、角色或 AWS 服务采取的操作将记录为 CloudTrail 中的事件。事件包括在 AWS 管理控制台、AWS 命令行界面以及 AWS SDK 和 API 中采取的操作。

您可以为 CloudTrail 配置两种类型的事件：

- 活动管理
- 数据事件

管理事件提供了对 AWS 帐户中资源执行的管理操作的可见性。这些也被称为控制平面操作。管理事件还可以包括在您的帐户中发生的非 API 事件。

另一方面，数据事件提供对资源上或资源内执行的资源操作的可见性。这些也被称为数据平面操作。它允许使用高级事件选择器对数据事件日志进行粒度控制。

您当前可以记录不同资源类型上的数据事件，例如 Amazon S3 对象级 API 活动（例如 GetObject、DeleteObject 和 PutObject API 操作）、AWS Lambda 函数执行活动（调用 API）、DynamoDB 项操作等。

使用 S3 对象锁，可以使用一次写入多读（WORM）模型存储对象。对象锁定有助于防止对象在固定时间或无限期内被删除或覆盖。您可以使用对象锁定来帮助满足要求 WORM 存储的法规要求，或者简单地添加另一层保护，以防止对象更改和删除。

您可以在 Amazon S3 资源上记录用户、角色或 AWS 服务所采取的操作，并维护日志记录，以进行审核和合规。为此，您可以使用服务器访问日志记录、AWS CloudTrail 日志记录或两者的组合。AWS 建议您使用 AWS CloudTrail 记录 AmazonS3 资源的 bucket 和对象级操作。因此，正确的答案是：设置 AWS 数据同步，将现有的健康记录从本地网络移动到 AWS 云。启动一个新的 Amazon S3 存储桶来存储现有记录和新记录。使用数据事件和 Amazon S3 对象锁在 bucket 中启用 AWS CloudTrail。该选项表示：

设置 AWS 存储网关，将现有的健康记录从本地网络移动到 AWS 云。启动一个新的 Amazon S3 存储桶来存储现有记录和新记录。使用管理事件启用 AWS CloudTrail，并且存储桶中的 Amazon S3 对象锁定不正确。该要求明确指出，解决方案架构师必须立即将现有记录移动到 AWS，而不是集成或复制数据。在这里使用 AWS 数据同步是更合适的服务，因为其主要目标是迁移或移动数据。您还必须在此处使用数据事件，而不是 CloudTrail 中的管理事件，以正确跟踪对对象的所有数据访问和更改。选项是：设置 AWS 存储网关，将现有的健康记录从本地网络移动到 AWS 云。启动 Amazon EBS 支持的 EC2 实例，以存储现有记录和新记录。启用亚马逊存储桶中的 S3 服务器访问日志记录和 S3 对象锁定不正确。正如前面选项中提到的，在这种情况下，不建议使用 AWS 存储网关，因为其目的是移动过时的数据。此外，与 Amazon S3 相比，使用 Amazon EBS 存储健康记录并不是一个可扩展的解决方案。启用服务器访问日志可以帮助审计存储的对象。然而，使用 CloudTrail 更好，因为它提供了更细粒度的访问控制和跟踪。

该选项表示：设置 AWS 数据同步以将现有健康记录从本地网络移动到

AWS 云。启动一个新的 Amazon S3 存储桶来存储现有记录和新记录。使用管理事件启用 AWS CloudTrail，并且存储桶中的 Amazon S3 对象锁定不正确。尽管使用 AWS 数据同步来移动健康记录是正确的，但您仍然必须在 AWS CloudTrail 中配置数据事件，而不是管理事件。这种类型的事件仅提供对 AWS 帐户中资源执行的管理操作的可见性，而不是在 Amazon S3 中单个对象中发生的数据事件。参考：

<https://aws.amazon.com/datasync/faqs/>

<https://aws.amazon.com/about-aws/whats-new/2020/12/aws-cloudtrail-provides-more-granular-control-of-数据事件记录/>
<https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lock.html> 查看 AWS 数据同步备忘单：

<https://tutorialsdojo.com/aws-datasync/>

AWS 存储网关与数据同步：<https://www.youtube.com/watch?v=tmfelrO-澳大利亚>

Q339.一家顶级 IT 咨询公司拥有一个 VPC，其中有两个具有弹性 IP 地址的按需 EC2 实例。我们已通知您，EC2 实例当前正在 Internet 上受到 SSH 暴力攻击。IT 安全团队已经确定了这些攻击源的 IP 地址。在团队设

置 AWS WAF、GuardDuty 和 AWS Shield Advanced 以永久修复安全漏洞时，您必须立即实施临时修复以停止这些攻击。以下哪项提供了停止对实例的攻击的最快方法？

- A、从 VPC 中删除 Internet 网关
- B、为每个 EC2 实例分配静态选播 IP 地址
- C、将 EC2 实例放入专用子网
- D、阻止网络访问控制列表中的 IP 地址

答案 D

分析：

网络访问控制列表（ACL）是 VPC 的可选安全层，充当防火墙，用于控制进出一个或多个子网的流量。您可以使用类似于安全组的规则设置网络 ACL，以便为 VPC 添加额外的安全层。以下是您需要了解的有关网络 ACL 的基本信息：

- 您的 VPC 自动附带可修改的默认网络 ACL。默认情况下，它允许所有入站和出站 IPv4 流量以及 IPv6 流量（如果适用）。
- 您可以创建自定义网络 ACL 并将其与子网关联。默认情况下，在添加规则之前，每个自定义网络 ACL 都会拒绝所有入站和出站流量。
- VPC 中的每个子网必须与网络 ACL 关联。如果未将子网与网络 ACL 显式关联，则子网将自动与默认网络 ACL 关联。
- 您可以将网络 ACL 与多个子网相关联；但是，子网一次只能与一个网络 ACL 关联。将网络 ACL 与子网关联时，将删除以前的关联。
- 网络 ACL 包含一个编号规则列表，我们从编号最低的规则开始依次评估，以确定是否允许流量进出与网络 ACL 关联的任何子网。可用于规则的最大数字为 32766。我们建议您从以增量（例如，以 10 或 100 为增量）创建规则开始，以便以后在需要时插入新规则。
- 网络 ACL 具有单独的入站和出站规则，每个规则可以允许或拒绝流量。
- 网络 ACL 是无状态的；对允许的入站流量的响应受出站流量规则的约束（反之亦然）。

该场景清楚地表明，它需要最快的方法来修复安全漏洞。在这种情况下，您可以使用网络 ACL 手动阻止违规 IP 地址，因为 IT 安全团队已经确定了违规 IP 地址的列表。或者，您可以设置 bastion 主机，但是，此选项需要额外的时间才能正确设置，因为您必须配置 bastion 主机的安全配置。

因此，阻止网络访问控制列表中的 IP 地址是最佳答案，因为它可以通过使用网络 ACL 阻止 IP 地址来快速解决问题。将 EC2 实例放置到专用子网中是不正确的，因为如果您在没有公共或 EIP 地址的私有子网中部署 EC2 实例，即使您也无法通过 Internet 访问它。从 VPC 中删除 Internet 网关是不正确的，因为这样做也会使您无法访问 EC2 实例，因为它会切断与 Internet 的连接。将静态选播 IP 地址分配给每个 EC2 实例是不正确的，因为 AWS Global Accelerator 主要使用静态选播地址，使组织能够无缝地将流量路由到多个区域，并提高最终用户的可用性和性能。

参考文献：

https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_ACLs.htmlhttps://docs.aws.amazon.com/vpc/latest/userguide/vpc_Security.html 安全组与 NACL: <https://tutorialsdojo.com/security-group-vs-nacl/>

Q340.一个 web 应用程序，托管在 AWS 中 EC2 实例的自动缩放组中。应用程序每天早上都会收到大量流量，许多用户都在抱怨请求超时。EC2 实例需要 1 分钟才能启动，然后才能响应用户请求。云架构必须重新设计以更好地响应应用的变化业务。解决方案架构师应该如何重新设计架构？

- A、 创建新的启动模板并升级实例的大小。
- B、 创建步骤缩放策略并配置实例预热时间条件。
- C、 创建 CloudFront 发行版并将 EC2 实例设置为源。
- D、 创建具有慢启动模式的网络负载均衡器。

答案 B

分析：

Amazon EC2 自动伸缩帮助您维护应用程序可用性，并允许您根据定义的条件自动添加或删除 EC2 实例。您可以使用 EC2 自动扩展的车队管理功能来维护车队的运行状况和可用性。您还可以使用 EC2 自动缩放的动态和预测缩放功能添加或删除 EC2 实例。动态缩放响应不断变化的需求，预测缩放基于预测需求自动调度正确数量的 EC2 实例。动态缩放和预测缩放可以一起使用以更快地缩放。步进缩放应用“步进调整”，这意味着您可以设置多个动作来根据警报破坏的大小改变缩放。创建步骤缩放策略时，还可以指定新启动实例预热所需的秒数。因此，正确答案是：

创建步骤缩放策略并配置实例预热时间条件。

“使用慢启动模式创建网络负载均衡器”选项不正确，因为网络负载均衡器不支持慢启动模式。如果需要启用慢启动模式，则应使用应用程序负载均衡器。

“创建新的启动模板并升级实例大小”选项不正确，因为较大的实例并不总是能提高启动时间。您应该创建一个步骤缩放策略并添加预热时间，而不是升级实例。“创建 CloudFront 分发并将 EC2 实例设置为源”选项是不正确的，因为这种方法只解决了通信延迟。请注意，场景中的要求是解决超时问题，而不是流量延迟。参考文献：

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scaling-simple-step.html><https://aws.amazon.com/ec2/autoscaling/faqs/>

查看以下 AWS 备忘单：

<https://tutorialsdojo.com/aws-auto-scaling/> <https://tutorialsdojo.com/step-scaling-vs-simple-scaling-policies-in-amazon-ec2/>

Q341.一名解决方案架构师加入了一家大型科技公司，该公司拥有现有的亚马逊专有网络。在回顾自动伸缩事件时，架构师注意到他们的 web 应用程序在一小时内多次伸缩。

在保持弹性的同时，架构师可以做出哪些设计变更来优化成本？

- A、 更改自动缩放组的冷却时间，并将 CloudWatch 度量设置为更高的阈值
- B、 将配置的 IOPS 添加到实例
- C、 增加自动缩放组 D 的自动缩放实例的基数。增加启动配置中的实例类型

答：

分析:

由于应用程序在一小时内多次上下缩放，问题在于自动缩放组的冷却时间。

冷却期是自动缩放组的可配置设置，有助于确保在上一个缩放活动生效之前不会启动或终止其他实例。在自动缩放组使用简单的缩放策略动态缩放后，它将等待冷却期结束，然后再恢复缩放活动。

手动缩放自动缩放组时，默认情况下不等待冷却时间，但可以覆盖默认值并遵守冷却时间。如果实例变得不健康，自动缩放组不会等待冷却期结束后再替换不健康的实例。

参考:

<http://docs.aws.amazon.com/autoscaling/latest/userguide/as-scale-based-on-demand.html> 查看此 Amazon EC2 备忘单:

<https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/>

Q342.一家数据分析公司正在收集点击流数据，并将其存储在 S3 存储桶中。您需要启动 AWS Lambda 函数，以便在 AmazonS3 中新数据可用时触发 ETL 作业。

在这个场景中，您可以使用以下哪些服务作为提取、转换和加载（ETL）服务？

- A、 S3 选择
- B、 AWS 胶水
- C、 红移谱
- D、 AWS 阶跃函数

答案 B

分析:

AWS Glue 是一种完全受管理的提取、转换和加载（ETL）服务，可让客户轻松准备和加载数据进行分析。只需在 AWS 管理控制台中单击几下，即可创建和运行 ETL 作业。您只需将 AWS Glue 指向存储在 AWS 上的数据，AWS Glue 就会发现您的数据并将相关元数据（如表定义和模式）存储在 AWS Glue 数据目录中。一旦编目，您的数据将立即可搜索、可查询并可用于 ETL。AWS Glue 生成用于执行数据转换和数据加载过程的代码。

参考: <https://aws.amazon.com/glue/>

查看 AWS 胶水备忘单: <https://tutorialsdojo.com/aws-glue/>

Q343.公司正在私有子网内的 EC2 实例上运行批处理作业。实例通过 NAT 网关从同一区域的 S3 存储桶收集输入数据。该公司正在寻找一种解决方案，既能降低成本，又不会给冗余或可用性带来风险。哪种解决方案可以实现这一点？

- A、 在实例和 S3 bucket 之间部署一个传输网关到对等连接。
- B、 将 NAT 网关重新分配给较低的 EC2 实例类型。
- C、 将 NAT 网关替换为承载在 burstable 实例类型上的 NAT 实例。

D、移除 NAT 网关，并使用网关 VPC 端点从实例访问 S3 bucket。

答案 D

分析：

正确：D

网关端点是您在路由表中指定的网关，用于通过 AWS 网络从 VPC 访问 Amazon S3。接口端点扩展了网关端点的功能，使用私有 IP 地址将请求从 VPC 内部、本地或不同 AWS 区域路由到 Amazon S3。接口端点与网关端点兼容。如果 VPC 中有现有网关端点，则可以在同一 VPC 中使用这两种类型的端点。使用网关端点不收取额外费用。然而，数据传输和资源使用的标准费用仍然适用。

因此，正确的答案是：删除 NAT 网关，并使用网关 VPC 端点从实例访问 S3 bucket。

表示：使用承载在 burstable 实例类型上的 NAT 实例替换 NAT 网关的选项不正确。

此解决方案可能会降低成本，但会影响可用性和冗余。在实例和 S3 bucket 之间部署传输网关到对等连接的选项不正确。Transit Gateway 是一种专门用于通过中央集线器连接多个 VPC 的服务。

表示：将 NAT 网关重新分配给较低的 EC2 实例类型的选项不正确。NAT 网关是完全受管理的资源。您无法访问或修改承载它的基础实例。

参考文献：

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/privatelink-interface-endpoints.html><https://docs.aws.amazon.com/vpc/latest/privatelink/vpce-gateway.html> 亚马逊专有网络概述：

<https://youtu.be/oIDHKeNxvQQ> 查看此

亚马逊 VPC 备忘单：

<https://tutorialsdojo.com/amazon-vpc/>

Q344.一家顶级投资银行正在建设一个新的外汇交易平台。为了确保高可用性和可扩展性，您将交易平台设计为在多个可用性区域的按需 EC2 实例的自动扩展组前面使用弹性负载均衡器。对于其数据库层，您选择使用单个 Amazon Aurora 实例来利用其分布式、容错和自愈存储系统。

如果主数据库实例上出现系统故障，在故障转移期间 Amazon Aurora 会发生什么？

A、Aurora 将尝试在与原始实例相同的可用性区域中创建一个新的 DB 实例，这是在尽力而为的基础上完成的。

B、Aurora 将首先尝试在原始实例的不同可用性区域中创建新的 DB 实例。如果无法这样做，Aurora 将尝试在最初启动实例的原始可用性区域中创建新的 DB 实例。

C、Amazon Aurora 翻转数据库实例的规范名称记录（CNAME）以指向健康副本，而健康副本又被提升为新的主副本。

D、Amazon Aurora 翻转数据库实例的 A 记录以指向健康副本，而健康副本又被提升为新的主副本。

答：

分析：

故障转移由 Amazon Aurora 自动处理，因此您的应用程序可以在没有手动管理干预的情况下尽快恢复数据库操作。如果您在相同或不同的可用性区域中有一个 Amazon Aurora 副本，则在故障切换时，Amazon Aurora 会翻

转数据库实例的规范名称记录（CNAME）以指向健康副本，然后将其提升为新的主副本。从开始到结束，故障转移通常在 30 秒内完成。

如果您正在运行 Aurora Serverless，并且数据库实例或 AZ 变得不可用，Aurora 将自动在不同的 AZ 中重新创建数据库实例。

如果您没有 Amazon Aurora 副本（即单个实例），并且没有运行 Aurora Serverless，Aurora 将尝试在与原始实例相同的可用性区域中创建新的 DB 实例。这种对原始实例的替换是在尽力而为的基础上进行的，并且可能不会成功，例如，如果存在广泛影响可用性区域的问题。因此，正确的答案是这样的选项：Aurora 将尝试在与原始实例相同的可用性区域中创建一个新的 DB 实例，并尽最大努力完成。选项如下：Amazon Aurora 翻转数据库实例的规范名称记录（CNAME）以指向健康副本，而健康副本又被提升为新的主副本，Amazon Aurora 翻转数据库实例 A 记录以指向健康的副本，这反过来又被提升为新的主服务器，这是不正确的，因为只有在使用 Amazon Aurora 副本时才会发生这种情况。此外，Amazon Aurora 会翻转实例的规范名称记录（CNAME）而不是 A 记录（IP 地址）。

该选项表示：Aurora 将首先尝试在原始实例的不同可用性区域中创建新的 DB 实例。如果无法这样做，Aurora 将尝试在最初启动实例的原始可用性区域中创建新的 DB 实例。这是不正确的，因为 Aurora 会首先尝试在与原始实例相同的可用性区域创建新的数据库实例。如果无法做到这一点，Aurora 将尝试在不同的可用性区域创建新的 DB 实例，而不是相反。

参考文献：

<https://aws.amazon.com/rds/aurora/faqs/>

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Concepts.AuroraHighAvailability.html> 亚马逊极光概述：

<https://youtu.be/iwS1h7rLNBQ>

查看此亚马逊极光备忘单：<https://tutorialsdojo.com/amazon-aurora/>

Q345.您所在的社交媒体公司需要每五分钟捕获通过其面向公众的应用程序负载均衡器的所有 HTTP 请求的详细信息。他们希望使用这些数据来分析流量模式，并对 AWS 中的 web 应用程序进行故障排除。以下哪个选项符合客户要求？

- A、在应用程序负载均衡器上启用 Amazon CloudWatch 度量。
- B、为其应用程序负载均衡器启用 AWS CloudTrail。
- C、在应用程序负载均衡器上添加 Amazon CloudWatch 日志代理。
- D、在应用程序负载均衡器上启用访问日志。

答案 D

分析：

弹性负载均衡提供了访问日志，用于捕获发送到负载均衡器的请求的详细信息。每个日志都包含诸如接收请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应等信息。您可以使用这些访问日志来分析流量模式并解决问题。

访问日志记录是默认禁用的弹性负载均衡的可选功能。为负载均衡器启用访问日志记录后，弹性负载均衡将捕获日志并将其存储在指定为压缩文件的 Amazon S3 存储桶中。您可以随时禁用访问日志记录。因此，正确的答案是：在应用程序负载均衡器上启用访问日志。该选项表示：

为其应用程序负载均衡器启用 AWS CloudTrail 是不正确的，因为 AWS CloudTrail 主要用于监控和记录 AWS 资源中的帐户活动，而不是 web 应用程序。您不能使用 CloudTrail 捕获通过面向公共的应用程序负载均衡器（ALB）的所有 HTTP 请求的详细信息。CloudTrail 只能跟踪对 ALB 所做的资源更改，但不能跟踪通过它的实际 IP 流量。对于这个用例，您必须启用访问日志功能。

“在应用程序负载均衡器上添加 Amazon CloudWatch 日志代理”选项不正确，因为您无法直接将 CloudWatch Logs 代理安装到应用程序负载均衡器。这通常安装在 Amazon EC2 实例上，而不是负载均衡器上。“在应用程序负载均衡器上启用 Amazon CloudWatch 度量”选项不正确，因为 CloudWatch 不会跟踪到 ALB 的实际流量。它只监视 ALB 本身的变化以及分配给目标组的实际 IP 流量。

参考文献：

<http://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-access-logs.html>

<https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-monitoring.html> AWS 弹性负载均衡概述：

<https://youtu.be/UBI5dw59DO8>

查看 AWS 弹性负载均衡（ELB）备忘单：

<https://tutorialsdojo.com/aws-elastic-load-balancing-elb/>

应用程序负载均衡器 vs 网络负载均衡器 vs 经典负载均衡器 vs gateway 负载均衡器：

<https://tutorialsdojo.com/application-load-balancer-vs-network-load-balancer-vs-classic-load-balancer/>

Q346. 一家公司的应用程序托管在应用程序负载均衡器后面的多个可用性区域中的 Amazon EC2 实例的自动扩展组中。有些情况下，某些实例在 ALB 中的 HTTPS 健康检查失败后自动终止，然后清除实例中存储的所有临时日志。解决方案架构师必须实现有效收集所有应用程序和服务器日志的解决方案。她应该能够根据日志执行根本原因分析，即使自动缩放组立即终止了实例。架构师从 Amazon EC2 实例自动收集日志的最简单方法是什么？

A、将生命周期挂钩添加到自动缩放组，以将处于终止状态的实例移动到终止：Waitstate，以延迟不健康 Amazon EC2 实例的终止。

设置 AWS Step 函数以收集应用程序日志并将其发送到 CloudWatch 日志组。

将解决方案配置为在所有日志成功发送到 CloudWatch 日志后立即恢复实例终止。

B、将生命周期挂钩添加到自动缩放组，以将处于终止状态的实例移动到终止：Waitstate，以延迟不健康 Amazon EC2 实例的终止。

使用关联的 Lambda 函数为 EC2 实例终止生命周期操作自动伸缩事件配置 CloudWatch 事件规则。触发 CloudWatch 代理推送应用程序日志，然后在所有日志发送到 CloudWatch 日志后恢复实例终止。

C、挂起：等待状态延迟不健康 Amazon EC2 实例的终止。

使用关联的 Lambda 函数为 EC2 实例终止生命周期操作自动伸缩事件配置 CloudWatch 事件规则。设置 AWS Systems Manager 自动化脚本，收集应用程序日志并将其从实例上传到 CloudWatch 日志组。将解决方案配置为仅在成功发送所有日志后恢复实例终止。

D、将生命周期挂钩添加到自动缩放组，以将处于终止状态的实例移动到终止：Waitstate，以延迟不健康 Amazon EC2 实例的终止。为 EC2 配置 CloudWatch 事件规则

实例终止具有关联 Lambda 函数的成功自动伸缩事件。设置 AWS Systems Manager 运行命令服务以运行脚本，该脚本收集应用程序日志并将其从实例上传到 CloudWatch 日志组。

发送所有日志后，恢复实例终止。

答案 B

分析：

自动缩放组中的 EC2 实例具有不同于其他 EC2 实例的路径或生命周期。生命周期从自动缩放组启动实例并将其投入服务时开始。生命周期在您终止实例时结束，或者自动缩放组使实例停止服务并终止它。

可以将生命周期挂钩添加到自动缩放组，以便在实例启动或终止时执行自定义操作。

当 Amazon EC2 自动缩放响应扩展事件时，它会启动一个或多个实例。这些实例以挂起状态开始。如果将自动缩放：EC2_INSTANCE_LAUNCHING 生命周期挂钩添加到自动缩放组，则实例将从挂起状态移动到挂起：等待状态。完成生命周期操作后，实例将进入挂起：继续状态。当实例完全配置后，它们将连接到自动缩放组，并进入服务状态。当 Amazon EC2 自动缩放响应 scale in 事件时，它会终止一个或多个实例。这些实例将从自动缩放组中分离，并进入终止状态。如果将自动缩放：EC2_INSTANCE_Terminating 生命周期挂钩添加到自动缩放组，则实例将从终止状态移动到终止：等待状态。完成生命周期操作后，实例将进入终止：继续状态。当实例完全终止时，它们将进入终止状态。

使用 CloudWatch 代理是收集日志最合适的工具。统一 CloudWatch 代理允许您执行以下操作：

- 跨操作系统从 Amazon EC2 实例收集更多系统级指标。指标可以

除了 EC2 实例的度量之外，还包括来宾度量。可以收集的其他度量列在 CloudWatch 代理收集的度量中。

- 从本地服务器收集系统级指标。这些可以包括混合环境中的服务器以及不由 AWS 管理的服务器。
- 使用 StatsD 和 collectd 协议从应用程序或服务检索自定义度量。Linux 服务器和运行 Windows Server 的服务器都支持 StatsD。仅在 Linux 服务器上支持 collectd。
- 从运行 Linux 或 Windows 服务器的 Amazon EC2 实例和本地服务器收集日志。

您可以在 CloudWatch 中存储和查看使用 CloudWatch 代理收集的度量，就像使用任何其他 CloudWatch 度量一样。CloudWatch 代理收集的度量的默认名称空间是 CWAgent，但您可以在配置代理时指定其他名称空间。因此，正确的答案是：向自动伸缩组添加生命周期挂钩，将处于终止状态的实例移动到终止：等待状态，以延迟不健康的 Amazon EC2 实例的终止。使用关联的 Lambda 函数为 EC2 实例终止生命周期操作自动伸缩事件配置 CloudWatch 事件规则。触发 CloudWatch 代理推送应用程序日志，然后在所有日志发送到 CloudWatch 日志后恢复实例终止。该选项表示：将生命周期挂钩添加到自动缩放组，以将处于终止状态的实例移动到挂起：等待状态，以延迟不健康的 Amazon EC2 实例的终止。使用关联的 Lambda 函数为 EC2 实例终止生命周期操作自动伸缩事件配置 CloudWatch 事件规则。设置 AWS Systems Manager 自动化脚本，收集应用程序日志并将其从实例上传到 CloudWatch 日志组。将解决方案配置为仅在成功发送所有日志后恢复实例终止是不正确的，因为挂起：等待状态是指 Amazon EC2 自动扩展中的扩展操作，而不是用于扩展或终止实例。该选项表示：将生命周期挂钩添加到自动缩放组，以将处于终止状态的实例移动到终止：等待状态，以延迟不健康状态的终止

Amazon EC2 实例。设置 AWS Step 函数以收集应用程序日志并将其发送到 CloudWatch 日志组。将解决方案配置为在所有日志成功发送到 CloudWatch 日志后立即恢复实例终止是不正确的，因为使用 AWS 步骤函数从 EC2 实例收集日志是不合适的。您应该使用 CloudWatch 代理。该选项表示：

将生命周期挂钩添加到自动缩放组，以将处于终止状态的实例移动到

终止：等待状态延迟不健康 Amazon EC2 实例的终止。配置

EC2 实例的 CloudWatch 事件规则使用关联的 Lambda 函数终止成功的自动缩放事件。设置 AWS Systems Manager 运行命令服务以运行脚本，该脚本收集应用程序日志并将其从实例上传到 CloudWatch 日志组。在发送所有日志后恢复实例终止是不正确的，因为尽管此解决方案可以工作，但需要花费大量精力编写自定义脚本，AWS 系统管理器运行命令将运行该脚本。请记住，该场景要求您以最少的工作量实现解决方案。通过使用 CloudWatch 代理自动上传日志，可以简化此解决方案。您必须使用 EC2 实例终止生命周期操作事件。参考文献：

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/AutoScalingGroupLifecycle.html><https://docs.aws.amazon.com/autoscaling/ec2/userguide/cloud-watch-events.html#终止成功>

<https://aws.amazon.com/premiumsupport/knowledge-center/auto-scaling-delay-termination/>查看此 AWS 自动缩放备忘单：<https://tutorialsdojo.com/aws-auto-scaling/>

Q347. 公司需要为日志处理应用程序设置一个经济高效的体系结构，该应用程序经常访问具有大量连续 I/O 操作的吞吐量密集型工作负载。应用程序应托管在 VPC 中已存在的按需 EC2 实例中。您必须附加应用程序将使用的新 EBS 卷。

以下哪一种是您在此场景中应使用的最合适的 EBS 卷类型？

- A、EBS 吞吐量优化硬盘 (st1)
- B、EBS 通用 SSD (gp2)
- C、EBS 配置 IOPS SSD (io1)
- D、EBS 冷硬盘 (sc1)

答：

分析：

在检查中，始终考虑 SSD 和 HDD 之间的差异，如下表所示。这将允许您轻松消除选项中非 SSD 或非 HDD 的特定 EBS 类型，具体取决于问题要求的存储类型是具有小的随机 I/O 操作还是大的顺序 I/O。

由于该场景的工作负载具有大的顺序 I/O 操作，我们可以通过选择 HDD 卷，而不是更适用于小型随机 I/O 操作的 SSD 卷。吞吐量优化的 HDD (st1) 卷提供了低成本的磁存储，以吞吐量而不是 IOPS 来定义性能。这种卷类型非常适合大型连续工作负载，如 Amazon EMR、ETL、数据仓库和日志处理。不支持可引导的 st1 卷。吞吐量优化的 HDD (st1) 卷虽然类似于冷 HDD (sc1) 卷，但设计用于支持频繁访问的数据。

EBS 配置 IOPS SSD (io1) 不正确，因为 Amazon EBS 配置的 IOPS SSD 不是最具成本效益的 EBS 类型，主要用于需要持续 IOPS 性能的关键业务应用程序。

EBS 通用 SSD (gp2) 不正确。尽管 Amazon EBS 通用 SSD 卷平衡了各种工作负载的价格和性能，但它不适合频繁访问、吞吐量密集型工作负载。吞吐量优化的 HDD 比通用 SSD 更适合使用。

EBS 冷硬盘驱动器 (sc1) 不正确。尽管与通用 SSD 相比，这提供了较低成本的 HDD 卷，但它非常适合访问频率较低的工作负载。参考：

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html#EBSVolumeTypes_st1 亚马逊 EBS 概述-SSD 与 HDD:

<https://www.youtube.com/watch?v=LW7x8wyLFvw&t=8s>

查看此亚马逊 EBS 备忘单：<https://tutorialsdojo.com/amazon-ebs/>

Q348. 一家公司计划在 AWS 中设计高可用性架构。它们有两个目标组，每个目标组有三个 EC2 实例，它们被添加到应用程序负载均衡器中。在 EC2 实例的安全组中，您已经验证了允许 HTTP 的端口 80。然而，实例仍然显示负载均衡器的服务中断。

这个问题的根本原因是什么？

- A、VPC 中使用了错误的子网

- B、这些实例使用了错误的 AMI。
- C、未正确定义运行状况检查配置。
- D、EC2 实例使用了错误的实例类型。

答案 C

分析：

由于安全组配置正确，因此问题可能由目标组中错误的运行状况检查配置引起。

应用程序负载均衡器定期向其注册目标发送请求，以测试其状态。这些测试被称为健康检查。每个负载均衡器节点仅将请求路由到负载均衡器的启用可用性区域中的健康目标。每个负载均衡器节点使用注册目标的目标组的健康检查设置检查每个目标的健康状况。目标注册后，必须通过一次健康检查才能被视为健康。完成每个健康检查后，负载均衡器节点关闭为健康检查建立的连接。

参考：

<http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-healthchecks.html> AWS 弹性负载均衡概述：

<https://www.youtube.com/watch?v=UBI5dw59DO8>

查看 AWS 弹性负载均衡（ELB）备忘单：

<https://tutorialsdojo.com/aws-elastic-load-balancing-elb/>

ELB 健康检查与路线 53 健康检查，用于目标健康监测：<https://tutorialsdojo.com/elb-health-checks-vs-route-53-health-checks-for-target-health-monitoring/>

Q349.一家公司在其 VPC 和远程网络之间有多个 AWS 站点到站点 VPN 连接。在高峰时间，许多员工遇到连接速度慢的问题，这限制了他们的工作效率。该公司已要求解决方案架构师扩大 VPN 连接的吞吐量。

架构师应该执行哪种解决方案？

- A、向 VPC 添加更多虚拟专用网关，并启用等成本多路径路由（ECMP），以获得更高的 VPN bandwidth。
- B、将 VPC 与支持等成本多路径路由（ECMP）的中转网关关联，并附加额外的 VPN 通道。
- C、将部分 VPN 连接重新路由到远程网络端的辅助客户网关设备。
- D、通过增加隧道数量来修改 VPN 配置，以扩展吞吐量。

答案 B

分析：

使用 AWS Transit Gateway，您可以简化多个 VPC 之间的连接，也可以通过单个 VPN 连接连接到连接到 AWS Transit Gateway 的任何 VPC。AWS Transit Gateway 还使您能够通过多个 VPN 隧道的等成本多路径（ECMP）路由支持来扩展 IPsec VPN 吞吐量。单个 VPN 隧道仍然具有 1.25 Gbps 的最大吞吐量。如果为启用 ECMP 的传输网关建立多个 VPN 隧道，它可以扩展到 1.25 Gbps 的默认限制之外。

因此，正确的答案是：将 VPC 与支持等成本多路径路由（ECMP）的中转网关关联，并附加额外的 VPN 隧道。“向 VPC 添加更多虚拟专用网关并启用等成本多路径路由（ECMP）以获得更高的 VPN 带宽”的选项是不正确的，因为 VPC 一次只能连接一个虚拟专用网关。此外，没有在虚拟专用网关中启用 ECMP 的选项。

该选项表示：通过增加隧道数量来修改 VPN 配置以扩展吞吐量，这是不正确的。VPN 连接的最大隧道数为 2。您不能将其增加到超出其限制。

表示：将部分 VPN 连接重新路由到远程网络端的辅助客户网关设备的选项不正确。这只会增加连接冗余，不会增加吞吐量。例如，如果主客户网关设备不可用，连接可以故障切换到辅助客户网关设备。参考文献：

<https://aws.amazon.com/premiumsupport/knowledge-center/transit-gateway-ecmp-multiple-tunnels/>[https://aws.amazon.com/blogs/网络和内容交付/使用 aws transit 扩展 vpn 吞吐量-网关/](https://aws.amazon.com/blogs/网络和内容交付/使用-aws-transit-扩展-vpn-吞吐量-网关/)

查看 AWS 过境网关备忘单：<https://tutorialsdojo.com/aws-transit-gateway/>

Q350.一家公司在其内部基础设施中托管了一个 web 应用程序，他们希望将其迁移到 AWS 云。您的经理已指示您确保迁移过程中没有停机时间。为了实现这一目标，您的团队决定将 50% 的流量转移到 AWS 中的新应用程序，另 50% 转移到其内部基础设施中托管的应用程序。一旦迁移结束，应用程序正常运行，将完全转向 AWS。该公司的专有网络通过 AWS 直接连接连接到其内部网络。以下哪种解决方案可以满足上述要求？（选择两个。）

A、使用具有加权目标组的应用程序弹性负载均衡器，在本地和 AWS 托管的应用程序之间分流和分配流量。将 50% 的流量转移到 AWS 中的新应用程序，另 50% 转移到其内部基础设施中托管的应用程序。

B、使用带有故障转移路由策略的路由 53，在本地和 AWS 托管应用程序之间分流和分配流量。将 50% 的流量转移到 AWS 中的新应用程序，另 50% 转移到其内部基础设施中托管的应用程序。

C、使用 AWS 全球加速器在本地和 AWS 托管应用程序之间分流和分配 HTTP 和 HTTPS 流量。确保本地网络具有选播静态 IP 地址，并通过直接连接网关连接到 VPC。

D、使用具有加权目标组的网络负载均衡器，在本地和 AWS 托管应用程序之间转移流量。将 50% 的流量转移到 AWS 中的新应用程序，另 50% 转移到其内部基础设施中托管的应用程序。

E、使用带有加权路由策略的路由 53，在本地和 AWS-hosted application 之间分流流量。将 50% 的流量转移到 AWS 中的新应用程序，另 50% 转移到其内部基础设施中托管的应用程序。

答案是

分析：

应用程序负载均衡器支持加权目标组路由。使用此功能，您将能够对规则转发到多个目标组的流量进行加权路由。这支持各种用例，如蓝绿、金丝雀和混合部署，而不需要多个负载均衡器。它甚至可以在本地和云之间或不同计算类型（如 EC2 和 Lambda）之间实现零停机迁移。

要将 50% 的流量转移到 AWS 中的新应用程序，将另 50% 转移到应用程序，还可以使用带有加权路由策略的路由 53。这将相应地分流本地和 AWS 托管应用程序之间的流量。

加权路由允许您将多个资源与单个域名（tutorialsdojo.com）或子域名（portal.tutorialdojo.com）关联，并选择路由到每个资源的流量。这可以用于多种用途，包括负载平衡和测试软件的新版本。您可以通过指定权重来设置分配给资源的流量的特定百分比。例如，如果您希望将流量的一小部分发送到一个资源，其余部分发送到另一个资源中，则可以指定权重为 1 和 255。权重为 1 的资源获得流量的 $1/256$ ($1/(1+255)$)，而另一资源获得 $255/256$ ($255/(1+255)$)。您可以通过改变权重逐渐改变平衡。如果要停止向资源发送流量，可以将该记录的权重更改为 0。

在应用程序负载均衡器中创建目标组时，指定其目标类型。这决定了在向该目标组注册时指定的目标类型。您可以选择以下目标类型：

1.实例-目标由实例 ID 指定。2.ip-目标是 ip 地址。3.Lambda-目标是一个 Lambda 函数。

当目标类型为 ip 时，您可以从以下 CIDR 块之一指定 ip 地址：-10.0.0.1/8（RFC 1918）-100.64.0.2/10（RFC 6598）-172.16.0.3/12（RFC 918）-192.168.0.5/16（RFC1918）-目标组的 VPC 子网

这些受支持的 CIDR 块允许您向目标组注册以下内容：ClassLink 实例、与负载均衡器 VPC 对等的 VPC 中的实例、可寻址的 AWS 资源

通过 IP 地址和端口（例如，数据库），以及通过 AWS 直接连接或 VPN 连接链接到 AWS 的本地资源。

请注意，您不能指定可公开路由的 IP 地址。如果使用实例 ID 指定目标，则使用实例的主网络接口中指定的主专用 IP 地址将流量路由到实例。如果使用 IP 地址指定目标，则可以使用来自一个或多个网络接口的任何专用 IP 地址将流量路由到实例。这使一个实例上的多个应用程序能够使用同一端口。每个网络接口可以有自己的安全组。因此，正确答案如下：

- 使用具有加权目标组的应用程序弹性负载平衡器来分流和均衡本地和 AWS 托管应用程序之间的流量。将 50%的流量转移到 AWS 中的新应用程序，另 50%转移到其内部基础设施中托管的应用程序。
- 使用带有加权路由策略的路由 53 在本地和 AWS 托管应用程序之间转移流量。将 50%的流量转移到 AWS 中的新应用程序，另 50%转移到其内部基础设施中托管的应用程序。

该选项表示：使用具有加权目标组的网络负载平衡器，在内部部署和 AWS 托管应用程序之间转移流量。将 50%的流量转移到 AWS 中的新应用程序，而将另 50%转移到其本地基础设施中托管的应用程序是不正确的，因为网络负载平衡器没有加权目标组来转移本地和 AWS 托管应用程序之间的流量。

该选项表示：使用带有故障转移路由策略的路由 53，在内部部署和 AWS 托管应用程序之间分流和分配流量。将 50%的流量转移到 AWS 中的新应用程序，而将另 50%转移到其本地基础设施中托管的应用程序是不正确的，因为您无法使用具有故障转移路由策略的路由 53 在本地和 AWS 托管的应用之间转移和按比例分配流量。如果您希望将主动-被动故障切换配置到应用程序体系结构，则主要使用此选项。

该选项表示：使用 AWS 全局加速器在本地和 AWS 托管应用程序之间分流和分配 HTTP 和 HTTPS 流量。确保本地网络具有选播静态 IP 地址，并通过直接连接网关连接到您的 VPC 是不正确的，因为尽管您可以通过在端点之间分配权重，使用 AWS 全局加速器控制定向到每个端点的流量比例，使用直接连接网关和选播 IP 地址仍然是错误的，因为它们根本不需要。您只能将 AWS 全球加速器提供的静态 IP 地址与区域 AWS 资源或端点相关联，例如

网络负载均衡器、应用程序负载均衡器，EC2 实例和弹性 IP 地址。请注意，直接连接网关本身并不建立从本地网络到 Amazon VPC 的连接。它只允许您使用 AWS 直接连接连接到位于不同 AWS 区域的两个或多个 VPC。

参考文献：

<http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html>

<https://aws.amazon.com/blogs/aws/new-application-load-balancer> 使用加权目标组简化部署/<https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-target-group.html>

查看此亚马逊路线 53

备忘单：<https://tutorialsdojo.com/amazon-route-53/>

Q351.运营团队在两个自定义 VPC 内的 EC2 实例上运行应用程序。VPC 分别位于俄亥俄州和北弗吉尼亚州。该团队希望在实例之间传输数据，而不需要穿越公共互联网。

哪些步骤组合将实现这一目标？（选择两个。）

A、重新配置实例子网的路由表目标和目标。

B、在每个区域上部署 VPC 端点以启用专用连接。

C、创建仅出口的 Internet 网关。

D、在 VPC 之间建立 VPC 对等连接。

E、在每个 VPC 的公共子网中启动 NAT 网关。

回答广告

分析：

VPC 对等连接是两个 VPC 之间的网络连接，使您能够使用专用 IPv4 地址或 IPv6 地址在它们之间路由流量。任何一个 VPC 中的实例都可以彼此通信，就像它们在同一网络中一样。您可以在自己的 VPC 之间创建 VPC 对等连接，也可以在另一个 AWS 帐户中创建 VPC。VPC 可以位于不同的区域（也称为区域间 VPC 对等连接）。

区域间 VPC 对等提供了一种简单且经济高效的方式，可在区域间共享资源或复制数据以实现地理冗余。基于目前支持 VPC 的水平扩展、冗余和高可用技术，跨区域 VPC 对等加密跨区域流量，无单点故障或带宽瓶颈。使用跨区域 VPC 对等的流量始终保持在全球 AWS 主干上，并且从不穿越公共互联网，从而减少了威胁向量，如常见的漏洞攻击和 DDoS 攻击。

因此，正确答案是：

- 在 VPC 之间建立 VPC 对等连接。

- 重新配置实例子网的路由表目标和目标。“创建仅出口的 Internet 网关”选项不正确，因为这只会启用从 VPC 中的实例到 Internet 的出站 IPv6 通信。请注意，该场景要求在两个不同区域的 VPC 之间启用专用通信。“在每个 VPC 的公共子网中启动 NAT 网关”选项不正确，因为 NAT 网关用于允许私有子网中的实例访问公共互联网。请注意，要求是确保实例之间的通信不会通过 internet。“在每个区域部署 VPC 端点以启用专用连接”选项不正确。专有网络端点仅特定于区域，不支持区域间通信。参考文献：

<https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html> <https://aws.amazon.com/about-aws/whatsnew/2017/11/>宣布支持跨区域 vpc 对等/查看此亚马逊 vpc 备忘单：<https://tutorialsdojo.com/amazon-vpc/>

Q352.一家公司计划设计一个应用程序，可以处理大量财务数据的批处理。解决方案架构师的任务是创建两个 Amazon S3 存储桶来存储输入和输出数据。应用程序将通过网络在多个 EC2 实例之间传输数据，以完成数据处理。

以下哪种选项将降低数据传输成本？

A、在不同可用性区域的专用子网中部署 Amazon EC2 实例。

B、在同一可用性区域中部署 Amazon EC2 实例。

C、在同一 AWS 区域中部署 Amazon EC2 实例。

D、在应用程序负载均衡器后面部署 Amazon EC2 实例。

答案 B

分析：

Amazon 弹性计算云（Amazon EC2）在 Amazon Web 服务（AWS）云中提供可扩展的计算能力。使用 Amazon EC2，您无需预先投资硬件，因此可以更快地开发和部署应用程序。您可以使用 Amazon EC2 启动任意数量的虚拟服务器，配置安全和网络，并管理存储。Amazon EC2 使您能够放大或缩小规模，以处理需求的变化或人气的激增，从而减少预测流量的需要。

在这种情况下，您应该将所有 EC2 实例部署在同一可用性区域中。如果您还记得，在同一可用性区域内的 Amazon EC2、Amazon RDS、Amazon Redshift、Amazon ElastiCache 实例和弹性网络接口之间传输的数据是免费的。您可以使用专用网络来降低总体数据传输成本，而不是使用公共网络来传输数据。因此，正确的答案是：在同一可用性区域中部署 Amazon EC2 实例。该选项表示：

在同一 AWS 区域中部署 Amazon EC2 实例是不正确的，因为即使实例部署在同一区域中，如果实例分布在不同的可用性区域中，它们仍可能需要支付可用性区域间数据传输的费用。必须在同一可用性区域中部署实例，以避免数据传输成本。在应用程序负载均衡器后面部署 Amazon EC2 实例的选项是不正确的，因为这种方法不会降低总体数据传输成本。应用程序负载均衡器主要用于将传入的流量分配给底层 EC2 实例。在不同可用性区域的私有子网中部署 Amazon EC2 实例的选项不正确。尽管私有子网中实例之间的数据传输是免费的，但在 Amazon S3 中检索数据时会出现问题。请记住，如果您使用私有子网，除非您有 VPC 端点，否则您将无法连接到您的亚马逊 S3 存储桶。参考文献：

<https://aws.amazon.com/ec2/pricing/on-demand/>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/concepts.html> [https://aws.amazon.com/blogs/mt/使用 awscost 资源管理器分析数据传输成本/](https://aws.amazon.com/blogs/mt/使用-awscost-资源管理器分析数据传输成本/) Amazon EC2 概述：

https://www.youtube.com/watch?v=7VsGIHT_jQE

查看此 Amazon EC2 备忘单：<https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/>

Q353.一家情报机构目前正在 AWS 中托管一个学习和培训门户。您的经理指示您启动一个带有附加 EBS 卷的大型 EC2 实例，并启用增强网络。使用增强网络的有效案例场景是什么？（选择两个。）

- A、 当您需要低数据包/秒性能时
- B、 当您需要一致更低的实例间延迟时
- C、 当您需要专用连接到内部数据中心时
- D、 当您需要更高的每秒数据包（PPS）性能时
- E、 当您需要高延迟网络时

答：屋宇署

分析：

增强型网络使用单根 I/O 虚拟化（SR-IOV）在支持的实例类型上提供高性能网络功能。SR-IOV 是一种设备虚拟化方法，与传统虚拟化网络接口相比，它提供了更高的 I/O 性能和更低的 CPU 利用率。增强型网络提供了更高的带宽、更高的每秒分组（PPS）性能，以及一致更低的实例间延迟。使用增强型网络不收取额外费用。表示：当您需要较低的每秒数据包性能时，该选项是不正确的，因为您希望提高每秒数据包的性能，而不是在启用增强网络时降低它。“当您需要高延迟网络时”的选项是不正确的，因为较高的延迟意味着较慢的网络，这与您启用增强网络时希望发生的情况相反。“当您需要与内部数据中心的专用连接时”选项是不正确的，因为启用增强网络并不能提供与内部数据中心的专用连接。为此，请使用 AWS 直接连接或启用 VPN 隧道。参考：

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/enhanced-networking.html> 查看此 Amazon EC2 备忘单：

<https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/>

Q354.一家公司正在使用 Amazon S3 存储频繁访问的数据。S3 存储桶与定期上传文件的外部用户共享。解决方案架构师需要实现一个解决方案，该解决方案将授予存储桶所有者对 S3 存储桶中所有上传对象的完全访问权。应该采取什么行动来完成这项任务？

- A、在 Amazon S3 bucket 中启用请求者付费功能。
- B、创建一个 bucket 策略，要求用户将对象的 ACL 设置为 bucket owner-full-control。
- C、在 S3 存储桶中创建 CORS 配置。
- D、启用服务器访问日志记录并设置 IAM 策略，该策略要求用户将对象的 ACL 设置为 bucket owner 完全控制。

答案 B

分析：

Amazon S3 将数据存储为 bucket 中的对象。对象是一个文件和描述该文件的任何可选元数据。要在 AmazonS3 中存储文件，需要将其上传到 bucket。将文件作为对象上载时，可以设置

对象和任何元数据的权限。桶是对象的容器。您可以有一个或多个桶。您可以控制每个 bucket 的访问，决定谁可以创建、删除和列出其中的对象。您还可以选择 Amazon S3 将存储 bucket 及其内容的地理区域，并查看 bucket 及其对象的访问日志。

默认情况下，S3 对象由上传该对象的 AWS 帐户拥有，即使 bucket 由其他帐户拥有。要获得对对象的完全访问权，对象所有者必须显式授予 bucket 所有者访问权。您可以创建一个 bucket 策略，要求外部用户在上传对象时授予 bucket 所有者完全控制权，以便 bucket 所有者可以完全访问对象。因此，正确答案是：

创建一个 bucket 策略，要求用户将对象的 ACL 设置为 bucket 所有者完全控制。Amazon S3 bucket 中的“启用请求者付费功能”选项不正确，因为该选项不会授予 bucket 所有者对 S3 bucket 中上传对象的完全访问权。通过请求者支付 bucket，请求者而不是 bucket 所有者支付请求和从 bucket 下载数据的成本。

“在 S3 bucket 中创建 CORS 配置”选项不正确，因为该选项仅允许跨源访问 Amazon S3 资源。如果需要在上传的对象中授予桶所有者完全控制权，则必须创建一个桶策略，并要求外部用户在上传对象时授予桶所有者-完全控制权。

“启用服务器访问日志记录并设置 IAM 策略，要求用户将存储桶的 ACL 设置为存储桶所有者完全控制”选项不正确，因为该选项仅提供对存储桶的请求的详细记录。此外，存储桶所有者完全控制的 ACL 必须与存储桶策略相关联，而不是与 IAM 策略相关联。这将需要用户将对象的 ACL（而不是 bucket）设置为 bucketowner 完全控制。参考文献：

<https://aws.amazon.com/premiumsupport/knowledge-center/s3-bucket-owner-access/>[https://](https://aws.amazon.com/premiumsupport/knowledge-center/s3-bucket-owner-access/)

亚马逊。com://premiumsupport/knowledge center/s3 需要对象所有权/查看此 Amazon s3 备忘单：

<https://tutorialsdojo.com/amazon-s3/>

Q355.解决方案架构师设计了基于 Kinesis 数据流和 Lambda 的实时数据分析系统。系统部署一周后，用户注意到随着数据速率的增加，系统运行缓慢。架构师发现 Kinesis 数据流的性能导致了这个问题。

架构师应该做以下哪项来提高性能？

- A、将数据流替换为 Amazon Kinesis data Firehose。
- B、对 Kinesis 数据流实施分步缩放。
- C、使用 UpdateShardCount 命令增加 Kinesis 流的碎片数。
- D、通过使用 MergeShard 命令减少流的碎片数，提高流的性能。

答案 C

分析:

Amazon Kinesis 数据流支持重硬，这使您可以调整流中的碎片数量，以适应流中数据流量的变化。重硬被认为是一种高级操作。

有两种类型的重硬操作：碎片分割和碎片合并。在碎片分割中，将单个碎片分割为两个碎片。在碎片合并中，将两个碎片合并为一个碎片。重硬始终是成对的，即不能在一次操作中拆分为两个以上的碎片，也不能在一个操作中合并两个以上碎片。重硬操作所作用的碎片或碎片对称称为父碎片。重硬操作产生的碎片或碎片对称称为子碎片。

拆分会增加流中的碎片数，从而增加流的数据容量。因为您是按每个碎片收费的，所以拆分会增加流的成本。

类似地，合并减少了流中的碎片数量，因此降低了流的数据容量和成本。

如果数据速率增加，还可以增加分配给流的碎片数，以保持应用程序性能。您可以使用 UpdateShareCount API 重新硬存储流。Amazon Kinesis 数据流的吞吐量旨在通过增加数据流中的碎片数量来无限制地扩展。因此，正确的答案是使用 UpdateShardCount 命令增加 Kinesis 流的碎片数。

用亚马逊 Kinesis 数据消防软管代替数据流是不正确的，因为 Kinesis 消防软管的吞吐量并不比 Kinesis 的数据流特别高。事实上，Amazon Kinesis 数据流的吞吐量设计为通过增加数据流中的碎片数量来无限制地扩展。

使用 MergeShard 命令通过减少流的碎片数来提高流的性能是不正确的，因为合并碎片将有效地降低流的性能，而不是提高流的质量。

对 Kinesis 数据流实施阶跃缩放是不正确的，因为 Kinesis 的数据流没有阶跃缩放功能。这仅适用于 EC2。参考：

<https://aws.amazon.com/blogs/big-data/scale-your-amazon-kinesis-stream-capacity-with-UpdateShareCount/><https://aws.amazon.com/kinesis/data-streams/faqs/>

<https://docs.aws.amazon.com/streams/latest/dev/kinesis-using-sdkjava-resharding.html> 查看此亚马逊 Kinesis 备忘单：<https://tutorialsdojo.com/amazon-kinesis/>

Q356.一家快餐公司正在使用 AWS 托管他们的在线订购系统，该系统使用跨多个可用性区域部署的 EC2 实例的自动扩展组，并在前端使用应用程序负载均衡器。为了更好地处理来自各种数字设备的传入流量，您计划实施一个新的路由系统，其中 URL 为 <server>/api/android 的请求被转发到一个名为“android 目标组”的特定目标组。相反，URL 为 <server>/api/ios 的请求被转发到另一个名为“ios 目标组”的单独目标组。您如何在 AWS 中实现此更改？

- A、使用路径条件定义根据请求中的 URL 将请求转发到不同目标组的规则。
- B、将 ALB 替换为网关负载均衡器，然后使用路径条件定义规则，根据请求中的 URL 将请求转发到不同的目标组。
- C、使用主机条件定义规则，根据 hostheader 中的主机名将请求转发到不同的目标组。这使您能够使用单个负载均衡器支持多个域。
- D、将 ALB 替换为网络负载均衡器，然后使用主机条件定义规则，根据请求中的 URL 将请求转发到不同的目标组。

答:

分析:

如果应用程序由多个单独的服务组成，则应用程序负载均衡器可以根据请求的内容（如主机字段、路径 URL、HTTP 头、HTTP 方法、查询字符串或源 IP 地址）将请求路由到服务。基于路径的路由允许您根据 HTTP 头的 URL 路径路由客户端请求。每个路径条件都有一个路径模式。如果请求中的 URL 与侦听器规则中的路径模式完全匹配，则使用该规则路由请求。路径模式区分大小写，长度最多为 128 个字符，并且可以包含以下任何字符。最多可以包含三个通配符。A、A，0? _.\$/~" ' @: +

&（使用&）

*（匹配 0 个或多个字符）

?（精确匹配 1 个字符）

示例路径模式

/img/*

/js/*

您可以使用路径条件定义规则，根据请求中的 URL 将请求转发到不同的目标组（也称为基于路径的路由）。这种类型的路由是这种情况下最合适的解决方案。因此，正确的答案是：使用路径条件定义规则，根据请求中的 URL 将请求转发到不同的目标组。

该选项表示：使用主机条件定义规则，根据主机头中的主机名将请求转发到不同的目标组。这使您能够使用单个负载均衡器支持多个域。这是不正确的，因为基于主机的路由定义了规则，该规则基于主机头中的主机名而不是 URL 将请求转发到不同的目标组，这在本场景中是需要的。

“将 ALB 替换为网关负载均衡器，然后使用路径条件定义基于请求中 URL 将请求转发到不同目标组的规则”选项不正确，因为网关负载均衡器不支持基于路径的路由。您必须使用应用程序负载均衡器。

“使用网络负载均衡器替换 ALB，然后使用主机条件定义规则，根据请求中的 URL 将请求转发到不同的目标组”的选项不正确，因为网络负载均衡器用于需要极端网络性能和静态 IP 的应用程序。它也不支持基于路径的路由，这是本场景所需要的。此外，该语句提到了基于主机的路由，即使场景是关于基于路径的路由。

参考文献：

<https://docs.aws.amazon.com/elasticloadbalancing/latest/application/introduction.html#application-负载均衡器的好处>

<https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-listeners.html#path-条件>

查看 AWS 弹性负载均衡（ELB）备忘单：

<https://tutorialsdojo.com/aws-elastic-load-balancing-elb/应用程序负载均衡器 vs 网络负载均衡器 vs Classic 负载均衡器>：<https://tutorialsdojo.com/application-load-balancer-vs-network-load-balancer-vs-classic-load-balancer/>

Q357.托管在 Amazon ECS 容器实例上的网站在高峰流量期间加载缓慢，影响其可用性。目前，容器实例在应用程序负载均衡器后面运行，CloudWatch 警报配置为在可用性出现问题时向操作团队发送通知，以便在需要时扩展。当出现此类问题时，解决方案架构师需要创建自动缩放解决方案。

哪种解决方案可以满足要求？（选择两个。）

- A、创建一个 AWS 自动扩展策略，当集群的 CPU 利用率过高时扩展 ECS 集群。
- B、创建 AWS 自动扩展策略，在 ALB 达到高 CPU 利用率时扩展 ECS 服务。
- C、创建 AWS 自动扩展策略，当 ALB 端点无法访问时，该策略可扩展 ECS 服务。
- D、创建一个 AWS 自动扩展策略，当 ECS 服务的内存利用率过高时，该策略可扩展 ECS 服务。

E、创建一个 AWS 自动扩展策略，当 ALB 目标组的 CPU 利用率太高时扩展 ECS 集群。

回答广告

分析：

AWS Auto Scaling 监控您的应用程序并自动调整容量，以尽可能低的成本保持稳定、可预测的性能。使用 AWS 自动伸缩功能，可以在几分钟内为多个服务中的多个资源设置应用程序伸缩。该服务提供了一个简单、强大的用户界面，允许您为资源构建扩展计划，包括 Amazon EC2 实例和 Spot 车队、Amazon ECS 任务、Amazon DynamoDB 表和索引以及 Amazon Aurora 副本。在这种情况下，您可以设置伸缩策略，根据您喜欢的度量触发 ECS 服务或 ECS 容器实例的伸缩活动。

以下指标可用于实例：

CPU 利用率

磁盘读取

磁盘读取操作

磁盘写入

磁盘写入操作

网络

网络输出

状态检查失败（任何）

状态检查失败（实例）

状态检查失败（系统）

以下指标可用于 ECS 服务：

ECSServiceAverageCPU 利用率——服务的平均 CPU 利用率。ECSServiceAverageMemoryUtilization 服务的平均内存利用率。ALBRequestCountPerTarget——应用程序负载均衡器目标组中每个目标完成的请求数。

因此，正确答案是：

- 创建 AWS 自动扩展策略，当 ECS 服务的内存利用率过高时，该策略将扩展 ECS 服务。
- 创建一个 AWS 自动扩展策略，当集群的 CPU 利用率过高时扩展 ECS 集群。

“创建 AWS 自动扩展策略，在 ALB 端点无法访问时扩展 ECS 服务”选项不正确。如果是这样的话，这将是一个不同的问题，需要以不同的方式解决。无法访问 ALB 端点可能意味着其他事情，如错误配置的安全组或网络访问控制列表。

“创建 AWS 自动扩展策略，在 ALB 达到高 CPU 利用率时扩展 ECS 服务”选项不正确。ALB 是托管资源。您无法跟踪或查看其资源利用率。

“创建 AWS 自动扩展策略，在 ALB 目标组的 CPU 利用率过高时扩展 ECS 集群”选项不正确。AWS 自动缩放不支持 ALB 的此度量。

参考文献：

<https://docs.aws.amazon.com/AmazonECS/latest/developerguide/service-configure-auto-scaling.html>

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-instance-monitoring.html> 查看此 AWS 自动缩放备忘单：

Q358.灾难恢复团队计划通过以下方式将本地记录备份到本地文件服务器共享

SMB 协议。为了满足公司的业务连续性计划，团队必须确保 48 小时前的数据副本可立即访问。允许延迟访问较旧的记录。灾难恢复团队应实施哪些措施，以最少的配置工作量实现目标？

A、 使用具有足够存储空间的 AWS 存储文件网关来保存过去 48 小时的数据。

将备份发送到安装为本地磁盘的 SMB 共享。

B、 创建 AWS 备份计划，每 48 小时将数据备份复制到本地 SMB 共享。

C、 在本地客户端上装载 Amazon EFS 文件系统，并将所有备份复制到 NFS 共享。

D、 在 Amazon FSx for Windows 文件服务器中创建 SMB 文件共享，该文件共享具有足够的存储空间来存储所有备份。从本地访问文件共享。

答:

分析:

Amazon S3 文件网关提供了一个文件接口，使您能够使用行业标准的 NFS 和 SMB 文件协议将文件存储为 Amazon S3 中的对象，并通过数据中心或 Amazon EC2 中的 NFS 和 SMB 访问这些文件，或直接在 Amazon S3 中访问这些文件作为对象。部署文件网关时，您可以指定要为本地缓存分配多少磁盘空间。该本地缓存充当写入缓冲区，并提供对最近写入或从 Amazon S3 读取的数据的低延迟访问。当客户端通过文件网关将数据写入文件时，该数据首先写入网关本身的本地缓存磁盘。数据安全地持久化到本地缓存后，文件网关才向客户端确认回写。从那里，文件网关在后台异步地将数据传输到 S3 存储桶，使用多部分并行上传优化数据传输，并使用 HTTPS 加密传输中的数据。在这种情况下，您可以将 AWS 存储文件网关部署到本地客户端。激活文件网关后，创建 SMB 共享，并将其作为本地磁盘安装在内部部署端。将备份复制到 SMB 共享。您必须确保将文件网关的本地缓存大小调整为适合需要立即访问的备份数据。备份完成后，您将能够访问较旧的数据，但会有延迟。由于需要从 Amazon S3 检索数据（不在缓存中），因此会有有一个小的延迟。

因此，正确的答案是：使用具有足够存储空间的 AWS 存储文件网关来保存过去 48 小时的数据。将备份发送到安装为本地磁盘的 SMB 共享。选项显示：在 Amazon FSx for Windows 文件服务器中创建 SMB 文件共享，该文件共享具有足够的存储空间来存储所有备份。从本地访问文件共享不正确，因为这需要额外的设置。您需要先设置从本地到 AWS 的直接连接或 VPN 连接，才能正常工作。“在本地客户端上装载 Amazon EFS 文件系统并将所有备份复制到 NFS 共享”选项不正确，因为场景中所需的文件共享需要使用 SMB 协议。“创建 AWS 备份计划，每 48 小时将数据备份复制到本地 SMB 共享”选项不正确。AWS 备份仅适用于 AWS 资源。参考文献：

<https://aws.amazon.com/blogs/storage/easily-store-your-sql-server-backups-in-amazon-s3-using-file-网关>

<https://aws.amazon.com/storagegateway/faqs/>

AWS 存储网关概述:

<https://www.youtube.com/watch?v=pNb7xOBjHE> 查看

此 AWS 存储网关备忘单:

<https://tutorialsdojo.com/aws-storage-gateway/>

Q359.应用程序使用 Lambda 函数处理平均运行 15 分钟的复杂财务数据。大多数调用都已成功处理。但是，您注意到一天中有一些终止的调用，这导致了应用程序中的数据差异。以下哪项最有可能导致此问题？

A、 失败的 Lambda 函数已运行超过 15 分钟，并达到最大执行时间。

B、 Lambda 函数包含递归代码，已经运行了超过 15 分钟。

C、 已达到并发执行限制。

D、失败的 Lambda 调用包含 `ServiceException` 错误，这意味着 AWS Lambda 服务遇到内部错误。

答:

分析:

Lambda 函数由代码和任何相关的依赖项组成。此外，Lambda 函数还具有与其关联的配置信息。最初，在创建 Lambda 函数时指定配置信息。Lambda 为您提供了一个 API 来更新一些配置数据。您为用于运行 Lambda 函数的 AWS 资源付费。要防止 Lambda 函数无限期运行，请指定超时。当达到指定超时时间时，AWS Lambda 将终止 Lambda 函数的执行。建议您根据预期的执行时间设置此值。默认超时时间为 3 秒，AWS Lambda 中每个请求的最大执行时间为 900 秒，相当于 15 分钟。因此，正确的答案是这样的选项：失败的 Lambda 函数已经运行了超过 15 分钟，并达到了最大执行时间。

请注意，您可以通过调用 `Invoke` 操作或在首选运行时使用 AWS SDK 同步调用 Lambda 函数。如果您预期一个长时间运行的 Lambda 函数，那么您的客户端可能会在函数执行完成之前超时。要避免这种情况，请更新客户端超时或 SDK 配置。

表示“已达到并发执行限制”的选项不正确，因为默认情况下，AWS Lambda 将给定区域内所有函数的并发执行总数限制为

Q360.公司的安全团队要求存储在云中的所有数据在任何时候都使用存储在本地加密密钥进行加密。

哪些加密选项符合这些要求？（选择两个。）

- A、使用 Amazon S3 托管加密密钥（SSE-S3）进行服务器端加密。
- B、使用 AWS KMS 托管加密密钥（SSE-KMS）进行服务器端加密。
- C、使用客户提供的加密密钥（SSE-C）进行服务器端加密。
- D、使用客户端加密提供静态加密。
- E、使用 Amazon S3 事件调用的 AWS Lambda 函数使用客户密钥加密数据。

对裁谈会的答复

分析:

使用客户提供密钥的服务器端加密（SSE-C）使 Amazon S3 能够使用 PUT 请求中提供的加密密钥对服务器端的对象进行加密。必须在 Amazon S3 的 GET 请求中提供相同的密钥来解密对象。客户还可以选择在将数据上传到 Amazon S3 之前在客户端对数据进行加密，然后在下载后对数据进行解密。AWS 软件开发工具包（SDK）提供了一个 S3 加密客户端，简化了过程。

Q361.一家公司在美国东部-1 地区使用 IPv6 的专用子网中的保留 EC2 实例上启动了加密货币挖掘服务器。由于服务器包含的财务数据，应保护系统，以防止任何未经授权的访问，并满足监管合规要求。在这种情况下，哪个 VPC 功能允许 EC2 实例与 Internet 通信，但阻止入站流量？

- A、仅出口互联网网关
- B、NAT 网关
- C、NAT 实例

D、互联网网关

答:

分析:

仅出口互联网网关是一个水平扩展、冗余和高可用的 VPC 组件，它允许通过 IPv6 从 VPC 中的实例到互联网进行出站通信，并防止互联网启动与实例的 IPv6 连接。请注意，仅出口互联网网关仅用于 IPv6 流量。要通过 IPv4 启用仅出站 Internet 通信，请改用 NAT 网关。

因此，正确答案是：仅出口互联网网关。NAT 网关和 NAT 实例不正确，因为它们仅适用于 IPv4 而不适用于 IPv6。尽管这两个组件可以使专用子网中的 EC2 实例与 Internet 通信并防止入站流量，但它仅限于使用 IPv4 地址而不是 IPv6 的实例。最适合使用的 VPC 组件是仅出口 Internet 网关。Internet 网关不正确，因为它主要用于为 VPC 的公共子网中的实例提供 Internet 访问，而不是专用子网。但是，通过 Internet 网关，来自公共 Internet 的流量也可以到达您的实例。该场景要求您阻止入站访问，因此这不是正确答案。参考：

<https://docs.aws.amazon.com/vpc/latest/userguide/egress-only-internet-gateway.html> 亚马逊专有网络概述：

<https://www.youtube.com/watch?v=oIDHKeNxvQQ>

查看此亚马逊 VPC 备忘单：<https://tutorialsdojo.com/amazon-vpc/>

Q362.一家跨国公司和投资银行每天晚上 10 点至凌晨 3 点在其内部数据中心为其公司客户定期处理应计项目、贷款利息和其他重要财务计算的稳定工作量。流程完成后，结果将上传到 Oracle 总账，这意味着流程不应延迟或中断。首席技术官已决定将其

为 AWS 提供 IT 基础设施，以节省成本。公司需要在特定的可用性区域中保留计算能力，以正确运行其工作负载。作为高级解决方案架构师，您如何在 AWS 中为其财务系统实现经济高效的体系结构？

- A、使用专用主机，提供完全专用于运行实例的物理主机，并提供现有的每个套接字、每个核心或每个虚拟机软件许可证，以降低成本。
- B、使用按需 EC2 实例，它允许您为第二次启动和使用的实例付费。在特定可用性区域中保留计算容量，以避免任何中断。
- C、使用区域保留实例在特定可用性区域保留容量，并通过其计费折扣降低运营成本。
- D、使用按需容量保留，它提供了在指定的当前计划中始终可用的计算容量。

答案 D

分析:

按需容量保留使您能够在特定可用性区域中为 Amazon EC2 实例保留计算容量。这使您能够独立于储蓄计划或区域保留实例提供的计费折扣创建和管理容量保留。通过创建容量保留，您可以确保在需要时始终可以访问 EC2 容量，只要您需要。您可以随时创建容量预订，无需签订一年或三年的长期承诺，容量立即可用。一旦提供了容量，并且容量预留进入活动状态，计费就开始。当您不再需要它时，请取消容量保留以停止产生费用。

创建容量保留时，可以指定：

- 要在其中保留容量的可用性区域
- 要为其保留容量的实例数

- 实例属性（包括实例类型、租赁和平台/操作系统容量保留）只能由与其属性匹配的实例使用。默认情况下，运行与属性匹配的实例会自动使用它们。如果没有任何正在运行的实例与容量保留的属性匹配，则在启动具有匹配属性的实例之前，它将保持未使用状态。此外，您可以使用节省计划和区域保留实例与您的容量保留一起使用，以从计费折扣中获益。当容量保留的属性与储蓄计划或区域保留实例的属性匹配时，AWS 将自动应用折扣。因此，正确的答案是使用按需容量保留，它提供了在指定的循环计划中始终可用的计算容量。使用按需 EC2 实例，这允许您为第二次启动和使用的实例付费。在特定可用性区域中保留计算容量以避免任何中断是不正确的，因为尽管按需实例是稳定的，适合处理关键数据，但其成本高于任何其他选项。此外，关键的财务计算仅在每天晚上 10 点到凌晨 3 点进行，而不是 24/7。这意味着您的计算能力将不会在每天总共 19 小时内使用。按需实例根本无法保留计算容量。所以这个选项是不正确的。使用区域保留实例在特定可用性区域保留容量并通过其计费折扣降低运营成本是不正确的，因为此功能仅在区域保留实例中可用，而在区域保留的实例上不可用。使用提供完全专用于运行实例的物理主机的专用主机，并使用现有的每个套接字、每个核心或每个虚拟机软件许可证来降低成本是不正确的，因为在这种情况下不保证使用完全专用的物理主机。此外，这将没有得到充分利用，因为您只运行进程 5 个小时（仅从晚上 10 点到凌晨 3 点），每天浪费 19 个小时的计算容量。

参考文献：

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-capacity-reservations.html>
<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/instance-purchasing-options.html> 查看此 Amazon EC2 备忘单：
<https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/> 对的：

Q363. 解决方案架构师需要为应用程序设置所需的计算资源，这些应用程序的工作负载要求对本地存储上的非常大的数据集进行高顺序读写访问。以下哪种实例类型最适合在此场景中使用？

- A、 计算优化实例
- B、 内存优化实例
- C、 通用实例
- D、 存储优化实例

答案 D

分析：

存储优化实例是为需要对本地存储上的非常大的数据集进行高顺序读写访问的工作负载而设计的。它们经过优化，可以向应用程序提供每秒数万次低延迟随机 I/O 操作（IOPS）。

因此，正确答案是：存储优化实例。内存优化实例是不正确的，因为它们旨在为处理内存中大型数据集的工作负载提供快速性能，这与处理本地存储上的高读写容量截然不同。计算优化实例是不正确的，因为它们非常适合于从高性能处理器（如批处理工作负载和媒体转码）中获益的计算绑定应用程序。通用实例是不正确的，因为它们是最基本的实例类型。它们提供了计算、内存和网络资源的平衡，可用于各种工作负载。由于您需要更高的读写容量，因此应选择存储优化实例。

参考：

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/storage-optimized-instances.html> 亚马逊 EC2 概述：

https://www.youtube.com/watch?v=7VsGIHT_jQE

查看此 Amazon EC2 备忘单：<https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/>

Q364.解决方案架构师正在为一家金融科技初创公司开发一个三层加密货币 web 应用程序。已指示架构师限制对数据库层的访问，以仅接受来自应用层的流量，并拒绝来自其他源的流量。应用层由托管在 EC2 实例的自动扩展组中的应用服务器组成。

以下哪个选项最适合在此场景中实施？

- A、 设置数据库子网的网络 ACL，以拒绝来自应用层子网的所有入站非数据库流量。
- B、 设置数据库层的安全组，以允许来自指定的应用程序服务器 IP 地址列表的数据库通信。
- C、 设置数据库层的安全组，以允许来自应用程序服务器的安全组的数据库通信。
- D、 设置数据库子网的网络 ACL，以允许来自应用层子网的入站数据库流量。

答案 C

分析：

安全组充当实例的虚拟防火墙，以控制入站和出站流量。在 VPC 中启动实例时，最多可以为该实例分配五个安全组。安全组在实例级别而不是子网级别执行操作。因此，可以将 VPC 子网中的每个实例分配给不同的安全组。如果在启动时未指定特定组，实例将自动分配给 VPC 的默认安全组。对于每个安全组，您将添加控制实例入站流量的规则，以及控制出站流量的单独规则集。本节介绍了您需要了解的有关 VPC 安全组及其规则的基本信息。

您可以添加或删除安全组的规则，这也称为授权或撤销入站或出站访问。规则适用于入站流量（入口）或出站流量（出口）。您可以授予对特定 CIDR 范围的访问权限，或对 VPC 或对等 VPC 中的另一个安全组的访问权限（需要 VPC 对等连接）。

在该场景中，应用层的服务器处于自动伸缩组中，这意味着 EC2 实例的数量可能随着时间的推移而增长或收缩。自动伸缩组还可以覆盖一个或多个具有自己子网的可用性区域（AZ）。因此，最合适的解决方案是设置数据库层的安全组，以允许来自应用程序服务器的安全组的数据库流量，因为您可以使用应用程序层自动扩展组的安全组作为数据库层中安全组规则的源。将数据库层的安全组设置为允许来自指定的应用服务器 IP 地址列表的数据库流量是不正确的，因为应用服务器 IP 的列表将随时间变化，因为自动扩展组可以基于配置的扩展策略添加或删除 EC2 实例。这将在应用程序中造成不一致，因为新启动的实例（不包括在初始 IP 地址列表中）将无法访问数据库。设置数据库子网的网络 ACL 以拒绝来自应用层子网的所有入站非数据库流量是不正确的，因为这样做可能会影响其他应用程序的其他 EC2 实例，这些应用程序也托管在应用层的同一子网中。例如，CIDR 块为/16 的大型子网可以由多个应用程序共享。拒绝来自整个子网的所有入站非数据库流量将影响使用该子网的其他应用程序。设置数据库子网的网络 ACL 以允许来自应用层子网的入站数据库流量是不正确的，因为尽管此解决方案可以工作，但应用层的子网可以由应用层以外的另一层或另一组 EC2 实例共享。这意味着您将无意中授予对托管在同一子网（而不是应用层）中的未授权服务器的数据库访问权限。

参考文献：

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Security.html#VPC_Security_Comparisonhttp://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html 查看此亚马逊专有网络备忘单：

<https://tutorialsdojo.com/amazon-vpc/>

Q365.解决方案架构师需要启动一个 web 应用程序，该应用程序将使用 Amazon CloudFront 在全球范围内提供服务。应用程序托管在 Amazon EC2 实例中，该实例将被配置为原始服务器，以处理动态内容并向其客户提供服务。以下哪个选项为应用程序提供了高可用性？

- A、 启动 EC2 实例的自动伸缩组，并将其配置为原始组的一部分。
- B、 使用 Lambda@Edge 以提高 web 应用程序的性能并确保高可用性。

设置 Lambda@Edge 作为原点组的一部分的功能。

C、使用 AmazonS3 提供 web 应用程序的动态内容，并将 S3 bucket 配置为 anorigin group 的一部分。

D、提供部署在不同可用性区域中的两个 EC2 实例，并将它们配置为 OringGroup 的一部分。

答案 D

分析：

源是存储内容的位置，CloudFront 从中获取内容以提供给观众。Amazon CloudFront 是一项服务，它可以加速向用户分发静态和动态 web 内容，如.html、.css、.js 和图像文件。CloudFront 通过称为边缘位置的全球数据中心网络提供您的内容。当用户请求使用 CloudFront 服务的内容时，用户将被路由到提供最低延迟（时间延迟）的边缘位置，以便以尽可能最佳的性能交付内容。

您还可以为需要高可用性的场景设置具有源故障转移的 CloudFront。原点组可以包含两个原点：主原点和次原点。如果主源不可用或返回指示故障的特定 HTTP 响应状态代码，CloudFront 将自动切换到次源。要设置源故障转移，您必须具有至少两个源的分发。该场景使用 EC2 实例作为源。请注意，在配置 CloudFront 时，我们还可以使用 EC2 实例或自定义源。为了在 EC2 实例中实现高可用性，我们需要在两个或多个可用性区域中部署实例。您还需要将实例配置为源组的一部分，以确保应用程序高度可用。因此，正确的答案是：提供部署在不同可用性区域中的两个 EC2 实例，并将它们配置为源组的一部分。“使用 Amazon S3 提供 web 应用程序的动态内容，并将 S3 bucket 配置为原始组的一部分”的选项是不正确的，因为 AmazonS3 只能提供静态内容。如果需要托管动态内容，则必须使用 Amazon EC2 实例。该选项表示：

启动 EC2 实例的自动扩展组并将其配置为源组的一部分是不正确的，因为必须至少有两个源才能在 CloudFront 中设置源故障切换。此外，不能直接使用单个自动缩放组作为原点。选项说明：使用 Lambda@Edge 以提高 web 应用程序的性能并确保高可用性。设置 Lambda@Edge 作为原始组一部分的函数不正确，因为 Lambda@Edge 主要用于无服务器边缘计算。你不能设定 Lambda@Edge 在 CloudFront 中作为原始组的一部分。

参考文献：

[https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/high_availability_origin_failover.](https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/high_availability_origin_failover.html)

html

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Introduction.html><https://aws.amazon.com/cloudfront/faqs/>查看此 Amazon cloudfront 备忘单：<https://tutorialsdojo.com/amazon-cloudfront/>对的：

Q366.公司需要公司 IT 治理，并对其全球各部门的所有 AWS 资源进行成本监督。他们的公司部门希望保持对他们所使用的独立 AWS 资源的管理控制，并确保这些资源与其他部门分开。以下哪个选项将支持每个公司部门的自主性，同时使公司 IT 能够维持治理和成本监督？（选择两个。）

A、使用 AWS Trusted Advisor 和 AWS 资源组标记编辑器

B、为公司 IT AWS 账户内的每个部门创建单独的 VPC。启动 AWS 传输网关，使用等成本多路径路由（ECMP）和 VPN 隧道进行 VPC 内部通信。

C、通过创建 AWS 组织，使用 AWS 合并账单将各部门的账户链接到母公司账户。

D、为公司 IT AWS 帐户内的每个部门创建单独的可用性区域。

使用 AWS 全球加速器改善两个 AZ 之间的通信。

E、为每个子帐户中的所有公司 IT 管理员启用 IAM 跨帐户访问。

行政长官的答覆

分析:

您可以使用 IAM 角色委派对您拥有的不同 AWS 帐户中的资源的访问。您可以与其他帐户中的用户共享一个帐户中的资源。通过以这种方式设置跨帐户访问，您不需要在每个帐户中创建单独的 IAM 用户。此外，用户无需退出一个帐户并登录到另一个帐户即可访问不同 AWS 帐户中的资源。您可以在 AWS 组织中使用合并计费功能来合并多个 AWS 帐户或多个 AISPL 帐户的付款。通过合并账单，您可以看到所有账户产生的 AWS 费用的组合视图。您还可以获得与主帐户关联的每个成员帐户的成本报告。合并账单不收取额外费用。AWS 和 AISPL 账户不能合并在一起。

IAM 和合并账单的联合使用将支持每个公司部门的自主性，同时使公司 IT 能够维持治理和成本监督。因此，正确的选择是：

- 为每个子帐户中的所有公司 IT 管理员启用 IAM 跨帐户访问
- 通过创建 AWS 组织将各部门的账户链接到母公司账户，使用 AWS 合并计费

使用 AWS Trusted Advisor 和 AWS 资源组标记编辑器不正确。Trusted Advisor 是一个在线工具，为您提供实时指导，帮助您按照 AWS 最佳实践提供资源。它仅在您不遵守最佳实践的领域向您提供警告，并告诉您如何改进它们。它无助于维护对 AWS 帐户的管理。此外，AWS 资源组标记编辑器允许您同时向多个 AWS 资源添加、编辑和删除标记，以便于识别和监控。为公司 IT AWS 账户内的每个部门创建单独的 VPC。使用 equalcost 多路径路由（ECMP）和 VPN 隧道启动 AWS 传输网关，用于 VPC 内部通信是不正确的，因为创建单独的 VPC 不会将各部门彼此分开，因为它们仍将在同一账户下运行，因此每个月都有相同的计费。AWS Transit Gateway 通过中央集线器连接 VPC 和内部网络，并充当云路由器，每个新连接只进行一次。对于这个特定场景，使用 AWS 组织而不是设置 AWS 传输网关是合适的，因为目标是维护 AWS 资源的管理控制，而不是网络连接。为公司 IT AWS 帐户内的每个部门创建单独的可用性区域。使用 AWS 全局加速器改善两个 AZ 之间的通信是不正确的，因为您不需要创建可用性区域。AWS 从一开始就为您提供了这些服务，而且并非所有服务都支持多个 AZ 部署。此外，在 VPC 中设置单独的可用区域不符合支持每个公司部门自治的要求。AWS 全球加速器是一种使用 AWS 全球网络优化从用户到应用程序的网络路径的服务，而不是在可用性区域之间。参考文献：

<http://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/consolidated-billing.html>https://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial_cross-account-with-roles.html

查看此 AWS 计费和本地管理备忘单：<https://tutorialsdojo.com/aws-billing-and-cost-management/>

Q367. 游戏公司要求在传输层（第 4 层）对其托管在 AWS Fargate 中的集装箱化游戏服务器的传入 TCP 流量进行负载平衡。为了保持性能，它应该每秒处理全球玩家发送的数百万请求，同时保持超低延迟。以下哪项必须在当前架构中实现以满足新需求？

- A、在 AWS Fargate 中启动一个新的微服务，作为负载平衡器，因为无法将 ALB 或 NLB 与 Fargate 一起使用。
- B、使用加权路由策略在 Amazon Route 53 中创建新记录，以负载平衡传入流量。
- C、启动新的应用程序负载平衡器。
- D、启动新的网络负载平衡器。

答案 D

分析:

弹性负载平衡自动将传入的应用程序流量分布到多个目标，如 Amazon EC2 实例、容器、IP 地址和 Lambda 函数。它可以在单个可用性区域或跨多个可用性区域处理应用程序流量的不同负载。弹性负载平衡提供了三种类

型的负载均衡器，它们都具有高可用性、自动伸缩性和健壮的安全性，这是使应用程序容错所必需的。它们是：应用程序负载均衡器、网络负载均衡器和经典负载均衡器

网络负载均衡器最适合于需要极高性能的 TCP 流量负载平衡。

网络负载均衡器在连接级别（第 4 层）运行，将流量路由到亚马逊虚拟私有云（Amazon VPC）内的目标，能够每秒处理数百万请求，同时保持超低延迟。网络负载均衡器也被优化以处理突发和不稳定的流量模式。

因此，正确的答案是启动新的网络负载均衡器。“启动新应用程序负载均衡器”选项不正确，因为它无法处理 TCP 或第 4 层连接，只能处理第 7 层（HTTP 和 HTTPS）。

该选项表示：使用加权路由策略在 Amazon 路由 53 中创建一个新记录，以负载平衡传入流量，这是不正确的，因为尽管路由 53 可以通过为每个记录分配一个相对权重来充当负载均衡器，该相对权重对应于您要向每个资源发送的流量，它仍然无法在保持超低延迟的同时每秒处理数百万个请求。您必须使用网络负载均衡器。

表示：在 AWS Fargate 中启动一个新的微服务，作为负载均衡器，因为无法将 ALB 或 NLB 与 Fargate 一起使用，这样的选项是不正确的，因为您可以将 ALB 和 NLB 放在 AWS Fargate 集群的前面。

参考文献：

<https://aws.amazon.com/elasticloadbalancing/features/#compare> [https://docs.aws.amazon.com/AWSAmazonECS/latest/developerguide/LoadBalancer](https://docs.aws.amazon.com/AWSAmazonECS/latest/developerguide/LoadBalancer.html) 类型。html<https://aws.amazon.com/getting-started/projects/buildmodern> 应用程序 fargate lambda dynamodb-python/模块二/查看 AWS 弹性负载均衡（ELB）
备忘单：<https://tutorialsdojo.com/aws-elastic-load-balancing-elb/>

Q368.一家技术公司正在运行两台生产 web 服务器，这些服务器托管在保留的 EC2 实例上，具有 EBS 支持的根卷。这些实例的一致 CPU 负载为 90%。流量由弹性负载均衡器分配给这些实例。此外，他们还还为生产、测试和开发环境提供了多个 AZ RDS MySQL 数据库。

在不影响关键任务系统的可用性和性能的情况下，您会提出什么建议来降低 AWS 环境中的成本？选择最佳答案。

- A、考虑使用按需实例而不是保留的 EC2 实例
- B、考虑使用 Spot 实例而不是保留的 EC2 实例
- C、考虑不为开发和测试数据库使用多 AZ RDS 部署。考虑拆除弹性负载均衡器

答案 C

分析：

您应该注意的一点是，该公司在其所有环境中都使用多 AZ 数据库，包括其开发和测试环境。由于这两种环境并不重要，因此成本高昂且不必要。最好在生产环境中使用多 AZ 以降低成本，这就是为什么这样的选项：考虑不使用多 AZ RDS 部署来开发和测试数据库是正确答案。

“考虑使用按需实例而不是保留的 EC2 实例”的选项是不正确的，因为购买保留实例时提供的折扣使选择保留实例比长期使用的按需实例更便宜。“考虑使用 Spot 实例而不是保留 EC2 实例”选项是不正确的，因为 web 服务器正在生产环境中运行。永远不要将 Spot 实例用于生产级 web 服务器，除非您确定它们在您的系统中不是那么重要。这是因为一旦最高价格超过您指定的最高金额，您的现货实例就可以终止。“考虑删除弹性负载均衡器”选项是不正确的，因为弹性负载均衡器对于保持系统的弹性和可靠性至关重要。参考文献：

<https://aws.amazon.com/rds/details/multi-az/>

<https://aws.amazon.com/pricing/cost-optimization/> 亚马逊

RDS 概述:

<https://www.youtube.com/watch?v=aZmpLl8K1UU>

查看此 Amazon RDS 备忘单: <https://tutorialsdojo.com/amazon-relational-database-service-amazon-rds/>

Q369. 解决方案架构师正在管理一个处理信用卡支付和在线交易的三层 web 应用程序。静态网页用于前端层，而应用层包含一个处理长时间运行的流程的 Amazon EC2 实例。数据存储在 MySQL 数据库中。

解决方案架构师被指示去耦合层以创建高可用性应用程序。以下哪个选项可以满足给定要求？

- A、将所有静态资产和网页移动到 Amazon S3。将应用程序重新托管到 Amazon 弹性容器服务（Amazon ECS）容器，并启用服务自动扩展。将数据库迁移到具有多 AZ 部署配置的 Amazon RDS。
- B、将所有静态资产、网页和后端应用程序移动到更大的实例。在 Amazon EC2 实例中使用自动缩放。将数据库迁移到 Amazon Aurora。
- C、将所有静态资产移动到 Amazon S3。在 AWS Lambda 中设置并发限制，将应用程序移动到无服务器架构。将数据库迁移到 Amazon DynamoDB。
- D、将所有静态资产和网页移动到 Amazon CloudFront。在 Amazon EC2 实例中使用自动缩放。使用多 AZ 部署配置将数据库迁移到 Amazon RDS。

答:

分析:

Amazon 弹性容器服务（ECS）是一种高度可扩展、高性能的容器管理服务，支持 Docker 容器，并允许您在 Amazon EC2 实例的托管集群上轻松运行应用程序。Amazon ECS 使您无需安装、操作和扩展自己的群集管理基础设施，从而可以轻松地将容器用作应用程序的构建块。Amazon ECS 允许您使用 Docker 容器调度长时间运行的应用程序、服务和批处理进程。Amazon ECS 维护应用程序可用性，并允许您向上或向下扩展容器，以满足应用程序的容量需求。场景中的需求是分离服务以实现高可用性架构。要实现此要求，必须将现有设置移动到每个 AWS 服务。对于静态资产，您应该使用 Amazon S3。您可以将 Amazon ECS 用于 web 应用程序，然后将数据库迁移到

具有多 AZ 部署的 Amazon RDS。将应用程序与应用程序集成服务分离允许它们保持互操作性，但如果一个服务出现故障或工作负载激增，则不会影响其余服务。

因此，正确的答案是：将所有静态资产和网页移动到 Amazon S3

弹性容器服务（Amazon ECS）容器并启用服务自动扩展。将数据库迁移到具有多 AZ 部署配置的 Amazon RDS。该选项表示：将所有静态资产移动到 Amazon S3。在 AWS Lambda 中设置并发限制以将应用程序移动到无服务器架构。将数据库迁移到 Amazon DynamoDB 是不正确的，因为 Lambda 函数无法处理长时间运行的进程。请注意，Lambda 函数的最大处理时间为 15 分钟。

该选项表示：将所有静态资产、网页和后端应用程序移动到更大的实例。在 Amazon EC2 实例中使用自动缩放。将数据库迁移到 Amazon Aurora 是不正确的，因为静态资产更适合存储在 S3 中，而不是存储在 EC2 实例中。

该选项表示：将所有静态资产和网页移动到 Amazon CloudFront。在 Amazon EC2 实例中使用自动缩放。将数据库迁移到具有多 AZ 部署的 Amazon RDS 配置不正确，因为您无法在 Amazon CloudFront 中存储数据。从技术上讲，您只能在 CloudFront 中存储缓存数据，但不能使用此服务托管应用程序或网页。您必须使用 Amazon S3 来托管静态网页，并使用 CloudFront 作为 CDN。参考文献：

<https://docs.aws.amazon.com/AmazonECS/latest/developerguide/service-auto-scaling.html><https://>

docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZ.html 查看此亚马逊 ECS 备忘单:

<https://tutorialsdojo.com/amazon-elastic-container-service-amazon-ecs/>

Q370. 一家公司计划使用云存储服务临时存储其日志文件。要存储的文件数量仍然未知，但只需要保存 12 小时。在这种情况下，以下哪一个是最经济高效的存储类？

- A、 Amazon S3 标准 IA
- B、 亚马逊 S3 One Zone IA
- C、 Amazon S3 标准
- D、 亚马逊 S3 冰川深度档案

答案 C

分析:

Amazon 简单存储服务 (Amazon S3) 是一种对象存储服务，提供业界领先的可扩展性、数据可用性、安全性和性能。Amazon S3 还为您存储的对象提供了一系列存储类。您可以根据用例场景和性能访问需求选择类。所有这些存储类都具有高耐久性。该场景要求您选择一种不具有最小存储时间的经济高效的服务，因为数据将仅持续 12 小时。在给出的选项中，只有 Amazon S3 标准具有没有最小存储时间的特性。这也是最具成本效益的存储服务，因为您将只在最后 12 小时内收取费用，而不像其他存储类，您仍将根据其各自的存储时间（例如 30 天、90 天、180 天）收取费用。S3 智能分层也没有最小存储持续时间，这是为具有变化或未知访问模式的数据设计的。S3 标准 IA 设计用于保存数月或数年的长期但不经常访问的数据。在 30 天内从 S3 标准 IA 中删除的数据仍将在整整 30 天内收费。S3 Glacier Deep Archive 设计用于保存 7-10 年或更长时间的长期但很少访问的数据。存档到 S3 Glacier Deep Archive 的对象至少有 180 天的存储时间，在 180 天之前删除的对象将按比例收取相当于剩余天数的存储费用。

因此，正确答案是：Amazon S3 标准。

Amazon S3 标准 IA 不正确，因为该存储类的最小存储时间至少为 30 天。请记住，该场景要求数据仅保留 12 小时。Amazon S3 One Zone-IA 不正确。与 S3 标准 IA 一样，该存储类的最小存储时间至少为 30 天。

亚马逊 S3 冰川深度档案不正确。尽管它是所有其他选项中最具成本效益的存储类别，但它的最小存储时间至少为 180 天，仅适用于备份和数据存档。如果您将数据存储在 Glacier Deep Archive 中仅 12 小时，则仍将收取 180 天的全部费用。

参考文献:



<https://docs.aws.amazon.com/AmazonS3/latest/dev/storage-class-intro.html> <https://aws.amazon.com/s3/存储类/> 查看此

Amazon S3 备忘单: <https://tutorialsdojo.com/amazon-s3/>

S3 标准 vs S3 标准 IA vs S3 单区 IA 备忘单: <https://tutorialsdojo.com/s3-standard-vs-s3-standard-ia-vs-s3-one-zone-ia/>

Q371. 一家公司创建了具有单个子网的专有网络，然后在孩子网中启动了按需 EC2 实例。您已将 Internet 网关 (IGW) 连接到 VPC，并验证 EC2 实例具有公共 IP。

专有网络主路由表如下:

	TutorialDojo	rtb-46b1813b	0 Subnets	Yes	vpc-b0968fc8
		rtb-43b15626	0 Subnets	Yes	vpc-f2bf5897 Default VPC

rtb-46b1813b

Summary

Routes

Subnet Associations

Route Propagation

Tags

Destination	Target	Status	Propagated
10.0.0.0/27	local	Active	No

但是，当您尝试从计算机连接到实例时，仍然无法从 **Internet** 访问该实例。应该对路由表执行以下哪项操作来解决此问题？

- A、 修改上述路由表：10.0.0.1/27->您的互联网网关
- B、 将以下条目添加到路由表：10.0.0.1/27->您的 Internet 网关
- C、 将此新条目添加到路由表：0.0.0/27->您的 Internet 网关
- D、 将此新条目添加到路由表：0.0.0/0->您的 Internet 网关

答案 D

分析：

显然，路由表没有 **Internet** 网关的条目。这就是您无法连接到 EC2 实例的原因。要解决此问题，您必须添加一条目的地为 0.0.0/0（IPv4 流量）或：：/0（IPv6 流量）的路由，然后添加 **Internet** 网关 ID（igw-xxxxxxx）的目标。添加新条目后，这应该是正确的路由表配置。

参考：

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Route_Tables.html 查看此亚马逊 VPC 备忘单：

<https://tutorialsdojo.com/amazon-vpc/>

Q372.一家大型菲律宾业务流程外包公司正在其 VPC 中构建一个双层 web 应用程序，以提供基于动态事务的内容。数据层利用在线事务处理（OLTP）数据库，但对于 web 层，他们仍在决定将使用什么服务。您应该利用哪些 AWS 服务来构建弹性和可扩展的 web 层？

- A、 具有多 AZ 和自动缩放功能的 Amazon RDS
- B、 弹性负载平衡、Amazon EC2 和自动扩展
- C、 弹性负载平衡、带多 AZ 的 Amazon RDS 和 Amazon S3
- D、 Amazon EC2、Amazon DynamoDB 和 Amazon S3

答案 C

分析:

Amazon RDS 是适用于在线事务处理 (OLTP) 应用程序的数据库服务。但是, 该问题要求提供 web 层而非数据库层的 AWS 服务列表。此外, 当涉及到为 web 层提供可伸缩性和弹性的服务时, 您应该始终考虑使用自动伸缩和弹性负载均衡器。

要构建弹性和高可用性的 web 层, 可以使用 Amazon EC2、自动伸缩和弹性负载均衡。您可以将您的 web 服务器部署到一组 EC2 实例中的自动扩展组, 该组将自动监控您的应用程序并自动调整容量, 以尽可能低的成本保持稳定、可预测的性能。负载均衡是提高系统可用性的有效方法。当其他实例继续运行时, 可以在负载均衡器后面无缝地替换失败的实例。弹性负载均衡可用于跨区域的多个可用性区域中的实例进行平衡。

其余选项都是不正确的, 因为它们没有提到构建高可用性和可伸缩性 web 层所需的所有服务, 例如 EC2、自动伸缩和弹性负载均衡器。尽管带有 Multi-AZ 和 DynamoDB 的 Amazon RDS 是高度可伸缩的数据库, 但场景更侧重于构建其 web 层, 而不是数据库层。

因此, 正确的答案是弹性负载均衡、Amazon EC2 和自动伸缩。该选项表示:

弹性负载均衡、使用多 AZ 的 Amazon RDS 和 Amazon S3 是不正确的, 因为应用程序正在进行动态事务, 因此您无法使用 Amazon S3 托管 web 层。Amazon S3 仅适用于计划拥有静态网站的情况。该选项表示: Amazon RDS 具有多 AZ 和自动伸缩功能, 这是不正确的, 因为问题的焦点是构建可伸缩的 web 层。您需要一个服务, 如 EC2, 您可以在其中运行 web 层。表示: Amazon EC2、Amazon DynamoDB 和 Amazon S3 的选项不正确, 因为您需要自动缩放和 ELB 来缩放 web 层。

参考文献:

https://media.amazonwebservices.com/AWS_Building_Fault_Tolerant_Applications.pdf
<https://d1.awsstatic.com/whitepapers/aws-building-fault-tolerance-applications.pdf>
<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-increase-availability.html>

Q373. 一家游戏开发公司运营多个虚拟现实 (VR) 和增强现实 (AR) 游戏, 这些游戏使用其内部数据中心托管的各种 RESTful web API。由于公司的空前增长, 他们决定将系统迁移到 AWS 云, 以扩大资源规模, 并将成本降至最低。

您应该推荐以下哪一项作为满足上述要求的最具成本效益和可扩展的解决方案?

- A、使用 AWS Lambda 和 Amazon API 网关。
- B、使用 ECS、ECR 和 Fargate 建立微服务架构。
- C、使用 Amazon EC2 实例的 Spot Fleet, 每个实例都带有弹性结构适配器 (EFA), 以实现更一致的延迟和更高的网络吞吐量。设置应用程序负载均衡器以将流量分配到实例。
- D、将 API 托管在 CloudFront web 发行版后面的静态 S3 web 托管桶中。

答:

分析:

使用 AWS Lambda, 您只需支付所使用的费用。根据函数请求的数量、持续时间以及代码执行所需的时间向您收费。Lambda 在每次响应事件通知或调用 (包括控制台的测试调用) 开始执行时, 都会对请求进行计数。您将按所有功能的请求总数收取费用。持续时间从代码开始执行开始计算, 直到返回或终止, 四舍五入到最接近的 1ms。价格取决于分配给函数的内存量。Lambda free 层包括每月 100 万个免费请求和每月超过 40 万 GB 的计算时间。

这里最好的答案是结合使用 AWS Lambda 和 Amazon API 网关，因为

该解决方案具有可扩展性和成本效益。只有当您使用 Lambda 函数时，才会向您收费，这与 EC2 实例不同，即使您不使用它，它也始终运行。因此，正确的答案是：使用 AWS Lambda 和 Amazon API 网关。使用 ECS、ECR 和 Fargate 设置微服务架构是不正确的，因为 ECS 主要用于托管 Docker 应用程序，此外，单独使用 ECS、ECR 和 Fargate 是不可扩展的，不建议用于此类场景。

将 API 托管在 CloudFront web 发行版后面的静态 S3 web 托管桶中不是一个合适的选项，因为 S3 没有计算能力，您只能将其用作静态网站。尽管这个解决方案是可伸缩的，因为它使用 CloudFront，但是使用 S3 来托管 web API 或动态网站仍然是不正确的。

该选项表示：使用 Amazon EC2 实例的现货车队，每个实例都带有弹性结构适配器（EFA），以实现更一致的延迟和更高的网络吞吐量。设置应用程序负载均衡器以将流量分配到实例是不正确的。没有自动缩放，EC2 本身是不可缩放的。即使您使用 Spot EC2 实例，但与 Lambda 相比，它仍然更昂贵，因为只有在使用您的函数时才会向您收费。弹性结构适配器（EFA）只是一个网络设备，您可以将其连接到 Amazon EC2 实例，使您能够实现本地 HPC 集群的应用程序性能，AWS 云提供了可伸缩性、灵活性和弹性。虽然 EFA 是可伸缩的，但该选项的现场车队配置不涉及自动伸缩。

参考文献：

<https://docs.aws.amazon.com/apigateway/latest/developerguide/getting-started-with-lambda-整合>。

<https://aws.amazon.com/lambda/pricing/>查看 AWS Lambda 备忘单：

[https://tutorialsdojo.com/aws-lambda/EC2 容器服务（ECS）](https://tutorialsdojo.com/aws-lambda/EC2-容器服务（ECS）)

与 Lambda：<https://tutorialsdojo.com/ec2-container-service-ecs-vs-lambda/>

Q374. 计算机动画电影工作室有一个在 Amazon EC2 实例上运行的 web 应用程序。它将 5GB 视频对象上传到 Amazon S3 bucket。视频上传的时间比预期的要长，这会影响应用程序的性能。

哪种方法有助于提高应用程序的性能？

- A、 利用 Amazon CloudFront 并使用 HTTP POST 方法来减少延迟。
- B、 使用 AmazonS3 多部分上传 API。
- C、 在 EC2 实例上使用弹性网络适配器（ENA）启用增强网络。
- D、 使用 Amazon 弹性块存储配置 IOPS 和 Amazon EBS 优化实例。

答案 B

分析：

主要问题是视频对象上传到 Amazon S3 的时间太慢。为了解决这个问题，您可以在 S3 中使用多部分上传来提高吞吐量。它允许您并行上传对象的部分，从而减少上传大型对象所需的时间。每个部分都是对象数据的连续部分。

您可以独立地以任何顺序上传这些对象部分。如果任何部分的传输失败，您可以重新传输该部分而不影响其他部分。上传对象的所有部分后，AmazonS3 将这些部分组装起来并创建对象。通常，当对象大小达到 100 MB 时，您应该

考虑使用多部分上传，而不是在单个操作中上传对象。使用多部分上传提供了以下优势：提高吞吐量-您可以并行上传部分以提高吞吐量。从任何网络问题中快速恢复-较小的零件尺寸可最大限度地减少由于网络错误而重新启动失败上传的影响。暂停并恢复对象上传-您可以随时间上传对象部分。一旦您启动了多部分上传，就不会过期；必须显式完成或中止多部分上载。在知道最终对象大小之前开始上载-您可以在创建对象时上载对象。在 EC2 实例上使用弹性网络适配器（ENA）启用增强网络是不正确的。尽管这将提高网络性能，但问题仍然存在，因为问题在于对象上传到 Amazon S3 的时间。您应该使用多部分上传功能。利用 Amazon CloudFront 并使用 HTTP POST 方法来减少延迟是不正确的，因为 CloudFront 是一种 CDN 服务，不用于加快向 Amazon S3 上传对象的过程。Amazon CloudFront 是一种快速内容交付网络（CDN）服务，它以低延迟、高传输速度、高安全性和高安全性向全球客户交付数据、视频、应用程序和 API，所有这些都在开发人员友好的环境中。使用 Amazon 弹性块存储配置的 IOPS 和 Amazon EBS 优化实例是不正确的。尽管使用 Amazon 弹性块存储提供的 IOPS 将加快 EC2 的 I/O 性能

例如，根本原因仍然没有解决，因为这里的主要问题是视频上传到 Amazon S3 的速度慢。EC2 实例中没有网络争用。参考文献：

<https://docs.aws.amazon.com/AmazonS3/latest/dev/uploadobjusingmpu.html><http://docs.aws.amazon.com/AmazonS3/latest/dev/qfacts.html> 查看此 Amazon S3 备忘单：<https://tutorialsdojo.com/amazon-s3/>

Q375.一家公司在 EC2 实例中部署了一个 web 应用程序，将各种照片效果添加到用户上传的图片中。应用程序将通过向 S3API 发送 put 请求，将生成的照片放入 S3 bucket。

考虑到您需要有 API 凭据才能向 S3API 发送请求，对于这种情况，最佳选项是什么？

- A、 加密 API 凭据并存储在 EC2 实例的任何目录中。
- B、 将 API 凭据存储在 EC2 实例的根 web 应用程序目录中。
- C、 将您的 API 凭证存储在 Amazon Glacier 中。
- D、 在 IAM 中创建一个角色。然后，将此角色分配给新的 EC2 实例。

答案 D

分析：

最好的选择是在 IAM 中创建一个角色。然后，将此角色分配给新的 EC2 实例。应用程序必须使用 AWS 凭据签署 API 请求。因此，如果您是应用程序开发人员，您需要一种策略来管理在 EC2 实例上运行的应用程序的凭据。您可以安全地将 AWS 凭据分发到实例，使这些实例上的应用程序能够使用您的凭据签署请求，同时保护您的凭据不受其他用户的影响。然而，将凭证安全地分发到每个实例，尤其是 AWS 代表您创建的实例，如 Spot 实例或自动缩放组中的实例，是一个挑战。旋转 AWS 凭据时，还必须能够更新每个实例上的凭据。

在这种情况下，您必须使用 IAM 角色，以便应用程序可以安全地从实例发出 API 请求，而无需管理应用程序使用的安全凭据。您可以委托使用 IAM 角色进行 API 请求的权限，而不是创建和分发 AWS 凭据。

因此，正确答案是：在 IAM 中创建一个角色。然后，将此角色分配给新的 EC2 实例。表示：加密 API 凭据并存储在 EC2 实例的任何目录中，并将 API 凭据存储在 EC1 实例的根 web 应用程序目录中的选项不正确。尽管您可以在 EC2 实例中存储和使用 API 凭据，但正如上面提到的那样，很难进行管理。

您必须使用 IAM 角色。

“在 Amazon S3 Glacier 中存储 API 凭据”选项不正确，因为 Amazon S3Glaciers 用于数据存档，而不是用于管理 API 凭据。参考：

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html> 查看此 Amazon EC2 备忘单：<https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/>

Q376. 一家公司有一个应用程序，该应用程序使用位于不同 AWS 地区（如美国）的多个 EC2 实例

东部（俄亥俄州）、美国西部（加利福尼亚州北部）和欧盟（爱尔兰）。经理指示解决方案架构师设置基于延迟的路由，为 **www.tutorialsdojo.com** 路由传入流量。连接到所有 AWS 区域的所有 EC2 实例。

以下哪个选项可以满足给定要求？

- A、使用网络负载均衡器将负载分布到所有 AWS 区域的多个 EC2 实例。
- B、使用 AWS 数据同步将负载分布到所有 AWS 区域的多个 EC2 实例。
- C、使用应用程序负载均衡器将负载分布到所有 AWS 区域的多个 EC2 实例。
- D、使用路由 53 将负载分布到所有 AWS 区域的多个 EC2 实例。

答案 D

分析：

如果您的应用程序托管在多个 AWS 区域中，您可以通过从提供最低延迟的 AWS 区域为用户的请求提供服务来提高性能。您可以使用基于延迟的路由为多个 AWS 区域中的资源创建延迟记录。如果路由 53 接收到您的域或子域（如 **tutorialsdojo.com** 或 **portal.tutorialsdojo.com**）的 DNS 查询，它确定您为哪些 AWS 区域创建了延迟记录，确定哪个区域为用户提供了最低延迟，然后为该区域选择延迟记录。路由 53 使用所选记录中的值进行响应，该值可以是 web 服务器的 IP 地址或弹性负载均衡器的 CNAME。

因此，使用路由 53 将负载分布到所有 AWS 区域的多个 EC2 实例是正确答案。

使用网络负载均衡器将负载分布到所有 AWS 区域的多个 EC2 实例，以及使用应用程序负载均衡器在所有 AWS 地区的多个 EC2 实例上都是不正确的，因为负载均衡器仅在其各自的区域内分配流量，默认情况下不分配到其他 AWS 区域。尽管网络负载均衡器支持跨不同 AWS 区域的对等 VPC 中从客户端到基于 IP 的目标的连接，但该场景没有提到 VPC 彼此对等。最好使用路由 53 来更有效地平衡两个或更多 AWS 区域的输入负载。使用 AWS 数据同步将负载分布到所有 AWS 区域的多个 EC2 实例是不正确的，因为 AWS 数据 sync 服务只是提供了一种在本地存储和 Amazon S3 或 Amazon 弹性文件系统（Amazon EFS）之间在线移动大量数据的快速方法。参考文献：

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html#routing-策略延迟>

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/TutorialAddingLBRRegion.html> 查看此亚马逊路线 53

备忘单：<https://tutorialsdojo.com/amazon-route-53/>

Q377. 一家商业银行设计了下一代网上银行平台，以使用分布式系统架构。作为他们的软件架构师，您必须确保他们的体系结构具有高度可伸缩性，但仍然具有成本效益。以下哪项将为该场景提供最合适的解决方案？

- A、启动 EC2 实例的自动扩展组，以托管应用程序服务和 SQS 队列。包括一个自动缩放触发器，以监视 SQS 队列大小，它将根据队列缩放 EC2 实例的数量。
- B、启动多个按需 EC2 实例来托管应用程序服务和 SQS 队列，SQS 队列将充当可伸缩性很强的缓冲区，在消息在分布式应用程序之间传输时存储消息。

C、在应用程序负载均衡器后面启动多个 EC2 实例来托管应用程序服务，SWF 将充当高度可扩展的缓冲区，在分布式应用程序之间传输消息时存储消息。

D、在应用程序负载均衡器后面启动多个 EC2 实例，以托管应用程序服务和 SNS，SNS 将充当高度可扩展的缓冲区，在消息在分布式应用程序之间传输时存储消息。

答：

分析：

分布式消息传递系统中有三个主要部分：可以托管在 EC2 实例上的分布式系统组件；您的队列（分布在 Amazon SQS 服务器上）；以及队列中的消息。

为了提高分布式系统的可伸缩性，可以向 EC2 实例添加自动伸缩组。

参考文献：

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-using-sqs-queue.html><https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-basic-architecture.html> 查看此 AWS 自动缩放备忘单：<https://tutorialsdojo.com/aws-auto-scaling/>

Q378.软件开发公司需要将其内部基础设施连接到 AWS 云。
您可以使用以下哪种 AWS 服务来实现这一点？（选择两个。）

- A、NAT 网关
- B、VPC 对等
- C、IPsec VPN 连接
- D、AWS 直接连接
- E、亚马逊连接

对裁谈会的答复

分析：

您可以使用 VPN 连接将 VPC 连接到远程网络，VPN 连接可以是 IPsec VPN 连接、AWS VPN CloudHub 或第三方软件 VPN 设备。VPC VPN 连接利用 IPSec 在您的内部网和亚马逊 VPC 之间通过互联网建立加密网络连接。

AWS Direct Connect 是一种网络服务，它提供了使用互联网将客户内部站点连接到 AWS 的替代方案。AWS Direct Connect 不涉及互联网；相反，它在您的内部网和亚马逊专有网络之间使用专用的专用网络连接。因此，IPsec VPN 连接和 AWS 直接连接是正确答案。Amazon Connect 不正确，因为这不是 VPN 连接选项。它实际上是 AWS 中基于云的自助式联络中心服务，使任何企业都可以轻松地以较低的成本提供更好的客户服务。Amazon Connect 基于全球亚马逊客户服务协会用于支持数百万客户对话的相同联络中心技术。VPC 对等是不正确的，因为这只是两个 VPC 之间的网络连接，这使您能够在它们之间私自路由流量。这不能用于将本地网络连接到 VPC。

NAT 网关不正确，因为您仅使用网络地址转换（NAT）网关使专用子网中的实例能够连接到 Internet 或其他 AWS 服务，但阻止 Internet 启动与这些实例的连接。这不用于连接到本地网络。

参考文献：

[https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpn-](https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpn-connections.html)

[connections.htmlhttps://aws.amazon.com/directconnect/faqs](https://aws.amazon.com/directconnect/faqs) 查看此亚马逊专有网络备

忘单: <https://tutorialsdojo.com/amazon-vpc/>

Q379.web 应用程序托管在自动伸缩组内的 EC2 实例组上, 该组具有两个 Lambda 函数用于特殊处理。每当您每周发布应用程序更新时, 都会出现一些不一致的情况, 其中一些资源没有正确更新。您需要一种方法来将资源分组在一起, 并在组之间一致地部署代码的新版本, 同时最小化停机时间。

在这些选项中, 您应该做哪些以最小的努力满足给定的需求?

A、使用 CodeCommit 在私有存储库中快速发布代码, 并将其推送到您的资源中进行快速更新。

B、在 CodeDeploy 中使用部署组以一致的方式自动化代码部署。

C、创建具有最新配置和代码的 CloudFormation 模板。

D、创建将自动启动包含最新版本代码的资源的 OpsWorks 配方。

答案 B

分析:

CodeDeploy 是一种部署服务, 它自动将应用程序部署到 Amazon EC2 实例、本地实例或无服务器 Lambda 函数。它允许您快速发布新功能, 更新

Lambda 函数版本, 避免了应用程序部署期间的停机时间, 并处理了更新应用程序的复杂性, 同时避免了与容易出错的手动部署相关的许多风险。创建具有最新配置和代码的 CloudFormation 模板是不正确的, 因为这用于根据您创建的模板配置和管理 AWS 资源堆栈, 以对基础架构进行建模。

如果您希望使用一种工具对您自己的基础设施的供应和管理进行细粒度控制, 建议使用 CloudFormation。使用 CodeCommit 在私有存储库中快速发布代码并将其推送到资源中进行快速更新是不正确的, 因为您主要使用 CodeCommit 来管理托管私有 Git 存储库的源代码管理服务。您可以存储从代码到二进制文件的任何内容, 并与现有的基于 Git 的工具无缝协作。CodeCommit 与 CodePipeline 和 CodeDeploy 集成, 以简化开发和发布过程。

您也可以使用 OpsWorks 来部署代码, 但是, 创建 OpsworksRecipes 来自动启动包含最新版本代码的资源仍然是不正确的, 因为您不需要启动包含新代码的新资源, 而只需要更新已经运行的资源。

参考文献:

[https://docs.aws.amazon.com/codedeploy/latest/userguide/deployment-](https://docs.aws.amazon.com/codedeploy/latest/userguide/deployment-groups.html)

[groups.htmlhttps://docs.aws.amazon.com/codedeploy/latest/userguide/welcome.html](https://docs.aws.amazon.com/codedeploy/latest/userguide/welcome.html) 查看此 AWS CodeDeploy 备忘单:

[https://tutorialsdojo.com/aws-](https://tutorialsdojo.com/aws-codedeploy/AWS-CodeDeploy-主要组件)

[codedeploy/AWS CodeDeploy-主要组件:](https://tutorialsdojo.com/aws-codedeploy/AWS-CodeDeploy-主要组件)

<https://www.youtube.com/watch?v=CIWBJT6k20Q>

弹性 Beanstalk vs CloudFormation vs OpsWorks vs CodeDeploy: <https://tutorialsdojo.com/elastic-beanstalk-vs-cloudformation-vs-opsworks-vs-codedeploy/>

Q380.一家公司正在使用支持多 AZ 部署的 Amazon RDS for MySQL 5.6，并跨两个 AWS 区域使用多个 web 服务器。由于公司网站的增长，数据库目前正经历高度动态读取。解决方案架构师试图测试辅助 AWS 区域的读取性能，并注意到 SQL 查询速度明显放缓。以下哪个选项将提供小于 1 秒的读取复制延迟？

- A、使用 Amazon ElastiCache 提高数据库性能。
- B、将现有数据库迁移到 Amazon Aurora 并创建跨区域读取副本。
- C、在辅助 AWS 区域中创建 Amazon RDS for MySQL 读取副本。
- D、升级 MySQL 数据库引擎。

答案 B

分析：

Amazon Aurora 是一个为云构建的 MySQL 和 PostgreSQL 兼容关系数据库，它将传统企业数据库的性能和可用性与开源数据库的简单性和成本效益结合起来。亚马逊极光比标准 MySQL 数据库快五倍，比标准 PostgreSQL 数据库快三倍。它以十分之一的成本提供了商业数据库的安全性、可用性和可靠性。Amazon Aurora 完全由 Amazon RDS 管理，它自动化了耗时的管理任务，如硬件配置、数据库设置、修补和备份。基于给定场景，在测试辅助 AWS 区域的读取性能后，会出现显著的减速。由于现有的设置是 Amazon RDS for MySQL，您应该将数据库迁移到 Amazon Aurora 并创建跨区域读取副本。

只有在使用 Amazon Aurora 副本时，读取复制延迟才可能小于 1 秒。Aurora 副本是 Aurora DB 集群中的独立端点，最好用于扩展读取操作和提高可用性。您可以在 AWS 区域内创建最多 15 个副本。因此，正确的答案是：将现有数据库迁移到 Amazon Aurora 并创建跨区域读取副本。“升级 MySQL 数据库引擎”选项不正确，因为升级数据库引擎不会将读取复制延迟提高到毫秒。要实现小于 1 秒的读取复制延迟要求，您需要使用 Amazon Aurora 副本。“使用 Amazon ElastiCache 提高数据库性能”选项不正确。Amazon ElastiCache 将无法提高数据库性能，因为它正在经历高度动态读取。如果数据库经常收到相同的查询，则此选项将非常有用。“在辅助 AWS 区域中创建 Amazon RDS for MySQL 读取副本”选项不正确，因为 MySQL 副本不会为您提供少于 1 秒的读取复制延迟。RDS 读取副本只能在几秒钟内提供异步复制，而不是毫秒。在这种情况下，您必须使用 Amazon Aurora 副本。

参考文献：

<https://aws.amazon.com/rds/aurora/faqs/>

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL.Replication.CrossRegion.html>

亚马逊极光概述：

<https://youtu.be/iwS1h7rLNBQ>

查看此亚马逊极光备忘单：<https://tutorialsdodo.com/amazon-aurora/>

Q381.一家建筑公司有一个在线系统，跟踪其项目的所有状态和进度。

该系统托管在 AWS 中，需要监控 MySQL RDS 实例的读写 IOPs 指标，并向 DevOps 团队发送实时警报。您可以使用 AWS 中的以下哪些服务来满足要求？（选择两个。）

- A、Amazon 简单队列服务
- B、云表
- C、53 号公路

D、主权财富基金

E、Amazon 简单通知服务

答案是

分析：

在这种情况下，您可以使用 CloudWatch 监控 AWS 资源和 SNS 以提供通知。因此，正确的答案是 CloudWatch 和 Amazon 简单通知服务。亚马逊简单通知服务（SNS）是一种灵活、完全管理的发布/订阅消息和移动通知服务，用于协调向订阅端点和客户端的消息传递。Amazon CloudWatch 是 AWS 云资源和您在 AWS 上运行的应用程序的监控服务。您可以使用 Amazon CloudWatch 收集和跟踪指标，收集和监控日志文件，设置警报，并自动对 AWS 资源中的更改做出反应。SWF 是不正确的，因为它主要用于管理工作流，而不是用于监视和通知。

Amazon 简单队列服务是不正确的，因为这是一种消息队列服务，不适合这种情况。

路由 53 不正确，因为它主要用于路由和域名注册和管理。

参考文献：

http://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CW_Support_For_AWS.html<https://aws.amazon.com/sns/>

查看此 Amazon CloudWatch 备忘单：<https://tutorialsdojo.com/amazon-cloudwatch/>

Q382.一家公司的帐户中有几个 EC2 保留实例，由于开发团队不再使用这些实例，这些实例需要停用和关闭。然而，审计团队仍然需要这些数据以满足合规要求。

在这种情况下，可以采取以下哪些步骤？（选择两个。）

- A、停止所有正在运行的 EC2 实例。
- B、将 EC2 实例转换为按需实例
- C、拍摄 EBS 卷的快照并终止 EC2 实例。
- D、您可以选择在 AWS 保留实例市场上销售这些 EC2 实例
- E、将 EC2 实例转换为具有持久 Spot 请求类型的 Spot 实例。

对裁谈会的答复

分析：

AmazonElasticComputeCloud（AmazonEC2）是一个 web 服务，在云中提供安全、可调整大小的计算能力。它旨在使开发人员更容易进行 web 级云计算。Amazon EC2 的简单 web 服务界面允许您以最小的摩擦获得和配置容量。它为您提供了对计算资源的完全控制，并允许您在亚马逊经验证的计算环境中运行。

根据场景，第一个要求是停用和关闭几个 EC2 保留实例。然而，还提到，审计小组仍然需要这些数据用于合规目的。为了满足给定的需求，您可以首先创建实例的快照以保存其数据，然后将实例出售给保留实例市场。

保留实例市场是一个平台，支持销售第三方和 AWS 客户未使用的标准保留实例，在长度和定价选项方面有所不同。例如，您可能希望在将实例移动到新的 AWS 区域、更改为新的实例类型、在期限到期前结束项目、业务需要更改或您拥有不需要的容量后出售保留实例。

因此，正确答案是：

- 您可以选择在 AWS 保留实例市场上销售这些 EC2 实例。
- 拍摄 EBS 卷的快照并终止 EC2 实例。表示：将 EC2 实例转换为按需实例的选项是不正确的，因为在场景中说明开发团队不再需要几个 EC2 保留实例。通过将其转换为按需实例，公司仍将在其基础设施中运行实例，这将导致额外的成本。“将 EC2 实例转换为具有持久 Spot 请求类型的 Spot 实例”选项不正确，因为场景中的要求是终止或关闭多个 EC2 保留实例。将现有实例转换为点实例将无法满足给定的要求。表示：停止所有正在运行的 EC2 实例的选项是不正确的，因为这样做仍然会产生存储成本。请注意，场景中的要求是停用并关闭几个 EC2 保留实例。因此，这种方法不能满足给定的要求。参考文献：

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ri-market->

[general.htmlhttps://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-creating-snapshot。html](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-creating-snapshot.html) 查看此 Amazon

EC2 备忘单: <https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/AWS> 容器服务概述:

<https://www.youtube.com/watch?v=5QBgDX7O7pw>

Q383.一所顶尖大学最近推出了在线学习门户，学生可以在家中舒适地学习电子学习课程。该门户基于一个大型按需 EC2 实例，该实例带有一个 Amazon Aurora 数据库。

如何提高 Aurora 数据库的可用性，以防止在线门户出现任何不必要的停机？

- A、在 Amazon Aurora 中使用异步键预取来提高连接表和索引的查询的性能。
- B、启用哈希联接以提高数据库查询性能。
- C、使用处理负载平衡的弹性负载平衡器，将 Aurora 部署到两个跨两个可用性区域的 EC2 实例的自动扩展组。
- D、创建亚马逊极光副本。

B、启用哈希联接以提高数据库查询性能。

C、使用处理负载平衡的弹性负载平衡器，将 Aurora 部署到两个跨两个可用性区域的 EC2 实例的自动扩展组。

D、创建亚马逊极光副本。

答案 D

分析:

亚马逊极光 MySQL 和亚马逊极光 PostgreSQL 支持亚马逊极光副本，它们与主实例共享相同的底层卷。主服务器所做的更新对所有 Amazon Aurora 副本都可见。使用 Amazon Aurora MySQL，您还可以基于 MySQL 基于 binlog 的复制引擎创建 MySQL 读取副本。在 MySQL 读取副本中，来自主实例的数据作为事务在副本上重放。对于大多数用例，包括读取扩展和高可用性，建议使用 Amazon Aurora 副本。

读取副本主要用于提高应用程序的读取性能。在这种情况下，最合适的解决方案是使用多 AZ 部署，但由于此选项不可用，您仍然可以设置读取副本，以便在发生停机时将其升级为主独立数据库集群。

因此，这里的正确答案是创建亚马逊极光副本。使用处理负载平衡的弹性负载平衡器将 Aurora 部署到跨两个可用性区域的两个 EC2 实例的自动扩展组是不正确的，因为 Aurora 是 RDS 的托管数据库引擎，而不是部署在您手动配置的典型 EC2 实例上。启用哈希联接以提高数据库查询性能是不正确的，因为哈希联接主要用于需要使用 equijoin 联接大量数据的情况，而不是用于提高可用性。使用 Amazon Aurora 中用于提高跨索引连接表的查询性能的异步键预取是不正确的，因为异步键预提取主要用于提高跨指数连接表的性能。

参考文献:

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/AuroraMySQL.BestPractices.html><https://>

[aws.amazon.com/rds/aurora/FAQ/Amazon aurora](https://aws.amazon.com/rds/aurora/FAQ/Amazon%20aurora) 概览:

<https://youtu.be/iwS1h7rLNBQ>

查看此亚马逊极光备忘单：

<https://tutorialsdojo.com/amazon-aurora/>对的：

Q384.一家全球新闻网络为其 web 应用程序创建了 CloudFront 发行版。但是，您注意到应用程序的源服务器被每个请求击中，而不是 AWS 边缘位置，后者服务于缓存对象。即使对于通常请求的对象，也会出现此问题。这个问题的可能原因是什么？

- A、缓存对象的文件大小太大，CloudFront 无法处理。
- B、一个对象只有在成功请求后才会被 Cloudfront 缓存，因此，之前没有请求对象，这就是为什么请求仍然指向源服务器的原因。
- C、在您的 Amazon CloudFront Origin 组中配置了两个主要来源。
- D、缓存控制最大年龄指令设置为零。

答案 D

分析：

您可以在 CloudFront 将另一个请求转发到您的源之前控制对象在 CloudFront 缓存中停留的时间。缩短持续时间可以提供动态内容。增加持续时间意味着您的用户可以获得更好的性能，因为您的对象更可能直接从

边缘缓存。更长的持续时间也会减少原点的负载。通常，CloudFront 从边缘位置为对象提供服务，直到您指定的缓存持续时间结束——也就是说，直到对象过期。过期后，下次边缘位置收到用户对对象的请求时，CloudFront 将请求转发到源服务器，以验证缓存是否包含对象的最新版本。Cache 控件和 Expires 标头控制对象在缓存中停留的时间。Cache-Control-max-age 指令允许您指定对象在 CloudFront 之前在缓存中保留多长时间（以秒为单位）

再次从源服务器获取对象。CloudFront 支持的最小到期时间对于 web 发行版为 0 秒，对于 RTMP 发行版为 3600 秒。在这种情况下，主要的罪魁祸首是缓存控制最大年龄指令设置为低值，这就是为什么请求总是指向源服务器。

因此，正确答案是：缓存控制最大年龄指令设置为零。该选项表示：只有在成功请求后，CloudFront 才会缓存对象。因此，之前没有请求对象，这就是为什么请求仍然指向源服务器的原因，因为即使是通常请求的对象也会出现此问题。这意味着之前已成功请求这些对象，但由于缓存控制最大年龄指令值为零，因此在 CloudFront 中会导致此问题。

“缓存对象的文件大小太大，CloudFront 无法处理”选项不正确，因为这与缓存中的问题无关。“Amazon CloudFront Origin 组中配置了两个主要来源”选项不正确，因为您不能在 CloudFront 中首先设置两个来源。源组包括两个源，一个是主源，另一个是将用于实际故障转移的第二个源。它还包括您需要指定的故障转移标准。在这种情况下，问题更多的是缓存命中率，而不是源故障切换。

参考：

<http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Expiration.html> 查看此 Amazon

CloudFront 备忘单：<https://tutorialsdojo.com/amazon-cloudfront/>

Q385.一家初创公司正在构建物联网设备和监控应用程序。他们正在使用物联网传感器，通过使用配置了默认设置的亚马逊 Kinesis 流实时监控流量。然后每隔 3 天将数据发送到 Amazon S3 bucket。当您在第三天检查 S3 中的数据时，仅存在最后一天的数据，而不存在 2 天前的数据。以下哪项最有可能导致此问题？

- A、 有人手动删除了 Amazon S3 中的记录。
- B、 Amazon S3 bucket 遇到数据丢失。
- C、 Kinesis 流对 S3 桶的访问不足。
- D、 默认情况下，Kinesis 中的数据记录只能在添加到流中后 24 小时内访问。

答案 D

分析：

默认情况下，Amazon Kinesis 中的流记录可在添加到流中后 24 小时内访问。通过启用扩展数据保留，您可以将此限制提高到最多 7 天。因此，正确答案是：默认情况下，Kinesis 中的数据记录只能在添加到流中后 24 小时内访问。

选项“Amazon S3 bucket 遇到数据丢失”是不正确的，因为 AmazonS3 很少遇到数据丢失。Amazon 为 S3 制定了一个 SLA，并向其客户承诺。Amazon S3 Standard、S3 StandardA、S3 One Zone IA 和 S3 Glacier 均设计为在给定年份内提供 999999999% 的物体耐久性。该耐久性水平对应于 0.00000001% 的物体的平均年预期损失。因此，Amazon S3 存储桶数据丢失的可能性很小。该选项表示：

有人手动删除了 Amazon S3 中的记录是不正确的，因为如果有人删除了数据，这应该在 CloudTrail 中可见。此外，如果您已经采取了适当的安全措施，那么从一开始就不应该手动删除那么多数据。表示：Kinesis 流对 S3 存储桶的访问不足的选项是不正确的，因为访问不足的可能性很小，因为您可以访问存储桶并查看 Kinesis 收集的前一天数据的内容。

参考：

<https://aws.amazon.com/kinesis/data-streams/faqs/>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/DataDurability.html> 查看此亚马逊 Kinesis 备忘单：

<https://tutorialsdojo.com/amazon-kinesis/>

Q386.一位解决方案架构师正在 AWS 中实施一个新的高性能计算（HPC）系统，该系统涉及使用作为亚马逊 ECS 集群一部分的 EC2 启动类型协调多个亚马逊弹性容器服务（亚马逊 ECS）任务。全球用户将频繁访问该系统，预计大部分时间内将有数百个 ECS 任务在运行。架构师必须确保其存储系统针对高频读写操作进行了优化。每个 ECS 任务的输出数据约为 10 MB，但过时的数据最终将被归档并删除，因此总存储容量不会超过 10 TB。

以下哪项是架构师应该推荐的最合适的解决方案？

- A、 启动具有突发吞吐量模式的 Amazon 弹性文件系统（Amazon EFS）文件系统，并将性能模式设置为通用。在 Amazon ECS 集群的 ECS 任务定义中将 EFS 文件系统配置为容器装载点。
- B、 启动具有配置吞吐量模式的 Amazon 弹性文件系统（Amazon EFS），并将 performancemode 设置为最大 I/O。在 Amazon ECS 集群的 ECS 任务定义中将 EFS 文件系统配置为容器装载点。

C、使用 Amazon DynamoDB 加速器（DAX）和 DynamoDB Streams 启动 Amazon DynamoDB 表。将表配置为所有 Amazon ECS 群集实例都可以访问。将 DynamoDB 表设置为 Amazon ECS 集群的 ECS 任务定义中的容器装载点。

D、通过在存储网关中创建 Amazon FSx 文件网关来设置 SMB 文件共享。在 Amazon ECS 集群的 ECS 任务定义中将文件共享设置为容器装载点。

答案 B

分析：

Amazon 弹性文件系统（Amazon EFS）为您的 Amazon ECS 任务提供简单、可扩展的文件存储。

使用 Amazon EFS，存储容量具有弹性，在添加和删除文件时会自动增长和收缩。您的应用程序可以在需要时拥有所需的存储空间。您可以将 Amazon EFS 文件系统与 Amazon ECS 一起使用，以访问 Amazon ECS 任务组中的文件系统数据。这样，您的任务就可以访问相同的持久性存储，无论它们位于哪个基础设施或容器实例上。当您在亚马逊 ECS 任务定义中引用亚马逊 EFS 文件系统和容器装载点时，亚马逊 ECS 会负责将文件系统装载到您的容器中。

为了支持多种云存储工作负载，Amazon EFS 提供了两种性能模式：-通用模式-最大 I/O 模

式。

您在创建文件系统时选择了它的性能模式，并且无法更改。这两种性能模式没有额外的成本，因此无论您的性能模式如何，Amazon EFS 文件系统的计费 and 计量都是相同的。

文件系统有两种吞吐量模式可供选择：

- 爆发性吞吐量
- 供应吞吐量

在突发吞吐量模式下，文件系统的吞吐量随着存储在 EFS 标准或一个区域存储类中的数据量的增加而增加。基于文件的工作负载通常是尖峰的，在短时间内驱动高水平的吞吐量，在其余时间内驱动低水平的吞吐量。为了适应这种情况，Amazon EFS 被设计为在一段时间内达到高吞吐量水平。配置的吞吐量模式可用于具有高吞吐量与存储（MiB/s/TiB）比率的应用程序，或要求大于突发吞吐量模式所允许的的要求的应用程序。例如，假设您将 Amazon EFS 用于开发工具、web 服务或内容管理应用程序，其中文件系统中的数据量相对于吞吐量需求较低。您的文件系统现在可以获得应用程序所需的高吞吐量，而无需填充文件系统。在这种情况下，全球各地的用户将频繁访问文件系统，因此预计大部分时间将有数百个 ECS 任务在运行。架构师必须确保其存储系统针对高频读写操作进行了优化。因此，正确的答案是：启动一个具有配置吞吐量模式的 Amazon 弹性文件系统（Amazon EFS），并将性能模式设置为最大 I/O。在 Amazon ECS 集群的 ECS 任务定义中将 EFS 文件系统配置为容器装载点。该选项表示：通过在存储网关中创建 Amazon FSx 文件网关来设置 SMB 文件共享。在 Amazon ECS 集群的 ECS 任务定义中将文件共享设置为容器装载点不正确。尽管您可以在这种情况下使用 Amazon FSx for Windows 文件服务器，但由于应用程序未连接到本地数据中心，因此不适合使用它。请注意，AWS 存储网关服务主要用于将现有的本地存储集成到 AWS。

选项如下：启动具有突发吞吐量模式的 Amazon 弹性文件系统（Amazon EFS）文件系统，并将性能模式设置为通用。在 Amazon ECS 集群的 ECS 任务定义中将 EFS 文件系统配置为容器装载点是不正确的，因为使用突发吞吐量模式将无法维持全局应用程序的恒定需求。请记住，世界各地的用户将频繁访问该应用程序，而且大多数时间都有数百个 ECS 任务在运行。

该选项表示：使用 Amazon DynamoDB 加速器（DAX）启动 Amazon DynamoDB 表，并

DynamoDB 流已启用。将表配置为所有 Amazon ECS 群集实例都可以访问。在 Amazon ECS 集群的 ECS 任务定义中，将 DynamoDB 表设置为容器挂载点是不正确的，因为您不能直接将 DynamoDB 表设置成容器挂载。首先，DynamoDB 是一个数据库，而不是一个文件系统，这意味着它不能“挂载”到服务器。

参考文献：

<https://docs.aws.amazon.com/AmazonECS/latest/developerguide/tutorial-efs-volumes.html><https://docs.aws.amazon.com/efs/latest/ug/performance.html><https://docs.aws.amazon.com/AmazonECS/latest/developerguide/tutorial-efs-volumes.html> 查看此亚马逊 EFS 备忘单：<https://tutorialsdojo.com/amazon-efs/>

Q387.一家公司在应用程序负载均衡器后面有一个运行 Spot EC2 实例的车队。传入流量来自多个 AWS 区域的不同用户，您希望在实例组中共享用户会话。您需要设置一个分布式会话管理层

将为用户会话提供可扩展和共享的数据存储。以下哪项是满足需求的最佳选择，同时仍为用户提供亚毫秒延迟？

- A、多 AZ RDS
- B、内存缓存中的弹性疼痛
- C、多主发电机 B
- D、ELB 粘性会话

答案 B

分析：

对于亚毫秒延迟缓存，ElastiCache 是最佳选择。为了解决可伸缩性问题，并为可从任何单个 web 服务器访问的会话提供共享数据存储，您可以从 web 服务器本身抽象 HTTP 会话。一个常见的解决方案是利用内存中的键/值存储，如 Redis 和 Memcached。

ELB sticky sessions 是不正确的，因为该场景不要求您将用户路由到管理该用户会话的特定 web 服务器。由于会话状态在实例之间共享，因此不建议在此场景中使用 ELB 粘性会话功能。多主发电机 B 和多 AZ RDS 不正确。虽然您可以使用 DynamoDB 和 RDS 来存储会话状态，但与 ElastiCache 相比，这两种方法在成本效益和性能方面并不是最佳选择。如果在存储会话数据时使用 DynamoDB 和 RDS，则在延迟方面存在显著差异。参考文献：

<https://aws.amazon.com/caching/session-management/>

<https://d0.awsstatic.com/whitepapers/performance-at-scale-with-amazon-elasticache.pdf> 查看此 Amazon ElastiCache 备忘单：<https://tutorialsdojo.com/amazon-elasticache/>

Redis（集群模式启用 vs 禁用）vs Memcached：<https://tutorialsdojo.com/redis-cluster-mode-enabled-vs-disabled-vs-memcached/>

Q388.一家公司计划在其 VPC 中部署高性能计算（HPC）集群，该集群需要可扩展的高性能文件系统。必须优化存储服务，以实现高效的工作负载处理，并且必须通过快速可扩展的文件系统接口访问数据。它还应该与 Amazon S3 一起本地工作，使您能够使用高性能 POSIX 接口轻松处理 S3 数据。

以下哪项服务最适合用于此场景？

- A、 亚马逊弹性文件系统（EFS）
- B、 亚马逊弹性块存储（EBS）
- C、 亚马逊 FSx 的光泽
- D、 用于 Windows 文件服务器的 Amazon FSx

答案 C

分析：

Amazon FSx for Lustre 提供了一个高性能文件系统，该系统针对机器学习、高性能计算（HPC）、视频处理、金融建模和电子设计自动化（EDA）等工作负载的快速处理进行了优化。这些工作负载通常需要通过快速和可扩展的文件系统接口呈现数据，并且通常将数据集存储在长期数据存储中，如 Amazon S3。

操作高性能文件系统通常需要专门的专业知识和管理开销，需要您配置存储服务器并调整复杂的性能参数。使用 Amazon FSx，您可以启动并运行一个文件系统，该文件系统提供对数据的亚毫秒级访问，并允许您以每秒数百 GB 的吞吐量和数百万 IOPS 的速度读取和写入数据。

Amazon FSx for Lustre 与 Amazon S3 本机协同工作，使您可以轻松地使用高性能文件系统处理云数据集。当链接到 S3 存储桶时，FSx for Lustre 文件系统将 S3 对象透明地表示为文件，并允许您将结果写回 S3。您还可以使用 FSx for Lustre 作为独立的高性能文件系统，将您的工作负载从本地扩展到云。通过将本地数据复制到 FSx for Lustre 文件系统，您可以通过 AWS 上运行的计算实例快速处理这些数据。使用 Amazon FSx，您只需为使用的资源付费。没有最低承诺、前期硬件或软件成本或额外费用。

对于基于 Windows 的应用程序，Amazon FSx 提供了完全管理的 Windows 文件服务器，其功能和性能针对“提升和转移”业务关键应用程序工作负载进行了优化，包括主目录（用户共享）、媒体工作流和 ERP 应用程序。它可以通过 SMB 协议从 Windows 和 Linux 实例访问。如果您有基于 Linux 的应用程序，Amazon EFS 是一个云本机完全管理的文件系统，提供简单、可扩展、弹性的文件存储，可通过 NFS 协议从 Linux 实例访问。

对于计算密集型和快速处理工作负载，如高性能计算（HPC）、机器学习、EDA 和媒体处理，Amazon FSx For Lustre 提供了一个针对性能优化的文件系统，输入和输出存储在 Amazon S3 上。

因此，正确的答案是：亚马逊 FSx 的光泽。

Amazon 弹性文件系统（EFS）是不正确的，因为尽管 EFS 服务可以用于 HPC 应用程序，但它不能与 Amazon S3 一起使用。与 Amazon FSx for Lustre 不同，它不具备使用高性能 POSIX 接口轻松处理 S3 数据的能力。Amazon FSx for Windows 文件服务器是不正确的，因为尽管此服务是 Amazon FSx 的一种类型，但它不能与 Amazon S3 在本机上工作。此服务是一个完全受管理的本机 Microsoft Windows 文件系统，主要用于需要 AWS 共享文件存储的基于 Windows 的应用程序。Amazon 弹性块存储（EBS）不正确，因为该服务不是一个可扩展的高性能文件系统。

参考文献：<https://aws.amazon.com/fsx/lustre/>

<https://aws.amazon.com/getting-started/use-cases/hpc/3/>

查看此亚马逊 FSx 备忘单：<https://tutorialsdojo.com/amazon-fsx/>

Q389.解决方案架构师使用 AWS CLI 使用默认设置创建了一个全新的 IAM 用户。这用于向 Amazon S3、DynamoDB、Lambda 和公司云基础设施的其他 AWS 资源发送 API 请求。

要允许用户对 AWS 资源进行 API 调用，必须执行以下哪项操作？

- A、 由于 IAM 用户已经能够向 AWS 资源发送 API 调用，因此不要执行任何操作。
- B、 为用户启用多因素身份验证。
- C、 为用户创建一组访问密钥并附加必要的权限。
- D、 为用户分配 IAM 策略以允许其发送 API 调用。

答案 C

分析：

您可以选择适合您的 IAM 用户的凭据。使用 AWS 管理控制台创建用户时，必须选择至少包含控制台密码或访问密钥。默认情况下，

使用 AWS CLI 或 AWS API 创建的全新 IAM 用户没有任何类型的凭据。您必须根据用户的需要为 IAM 用户创建凭据类型。访问密钥是 IAM 用户或 AWS 帐户根用户的长期凭证。您可以使用访问密钥对 AWS CLI 或 AWS API 的编程请求进行签名（直接或使用 AWS SDK）。用户需要自己的访问密钥来从 AWS 命令行界面（AWS CLI）、Windows PowerShell 工具、AWS SDK 或使用单个 AWS 服务的 API 直接进行 HTTP 调用。要满足此需求，可以创建、修改、查看或旋转访问键（访问密钥 ID 和秘密访问密钥）

对于 IAM 用户。创建访问密钥时，IAM 将返回访问密钥 ID 和机密访问密钥。您应该将它们保存在安全的位置，并将其提供给用户。“由于 IAM 用户已经能够向您的 AWS 资源发送 API 调用，所以什么都不做”选项是不正确的，因为默认情况下，使用 AWS CLI 或 AWS API 创建的全新 IAM 用户没有任何类型的凭据。请注意，在该场景中，您使用 AWS CLI 而不是通过 AWS 管理控制台创建了新的 IAM 用户，在创建新 IAM 用户时，您必须选择至少包括控制台密码或访问密钥。为用户启用多因素身份验证是不正确的，因为这仍然无法提供向 AWS 资源发送 API 调用所需的访问密钥。您必须向 IAM 用户授予访问密钥以满足要求。向用户分配 IAM 策略以允许其发送 API 调用是不正确的，因为向新用户添加新的 IAM 策略不会授予对 AWS 资源进行 API 调用所需的访问密钥。

参考文献：

[https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_access-](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_access-keys.html)

[keys.htmlhttps://docs.aws.amazon.com/IAM/latest/UserGuide/id_users。html#id_users_creds](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users.html#id_users_creds) 查看此 AWS IAM 备忘

单：<https://tutorialsdajo.com/aws-identity-and-access-management-iam/>

Q390.一家公司计划在 AWS 中实施网络监控系统。解决方案架构师启动了一个 EC2 实例来托管监控系统，并使用 CloudWatch 来监控、存储和访问实例的日志文件。

以下哪项提供了从 Amazon EC2 实例向 CloudWatch 日志发送日志数据的自动方式？

- A、 用于 SFTP 的 AWS 传输
- B、 具有日志文件验证的 CloudTrail
- C、 CloudWatch 日志代理
- D、 CloudTrail 处理库

答案 C

分析：

对的：

CloudWatch 日志使您能够将您使用的所有系统、应用程序和 AWS 服务的日志集中到一个高度可扩展的服务中。然后，您可以轻松地查看它们，搜索它们以查找特定的错误代码或模式，根据特定字段过滤它们，或者安全地存档它们以供将来分析。CloudWatch 日志使您能够将所有日志（无论其来源如何）视为按时间顺序排列的单一且一致的事件流，您可以根据其他维度对其进行查询和排序，按特定字段对其进行分组，使用强大的查询语言创建自定义计算，并在仪表板中可视化日志数据。

CloudWatch 日志代理由以下组件组成：

- AWS CLI 插件，将日志数据推送到 CloudWatch 日志。
- 启动将数据推送到 CloudWatch 日志的过程的脚本（守护进程）。
- 确保守护进程始终运行的 cron 作业。CloudWatch Logs agent 提供了一种从 Amazon EC2 实例向 CloudWatch 日志发送日志数据的自动化方法。因此，CloudWatch Logs agent 是正确答案。带有日志文件验证的 CloudTrail 是不正确的，因为它主要用于跟踪 AWS 资源的 API 调用，而不是将 EC2 日志发送到 CloudWatch。

用于 SFTP 的 AWS 传输是不正确的，因为这只是用于 Amazon S3 的完全管理 SFTP 服务，用于跟踪进入 VPC 的流量，而不用于 EC2 实例监控。这项服务使您可以轻松移动

您的文件传输工作负载使用安全外壳文件传输协议（SFTP）到 AWS，无需修改应用程序或管理任何 SFTP 服务器。这不能用于将 EC2 实例的日志数据发送到 Amazon CloudWatch。

CloudTrail 处理库是不正确的，因为它只是一个 Java 库，提供了处理 AWS CloudTrail 日志的简单方法。它无法将您的日志数据发送到 CloudWatch 日志。参考文献：

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/WhatIsCloudWatchLogs.html>

docs.aws.amazon.com/AmazonCloudWatch/latest/logs/AgentReference.html 查看此 Amazon CloudWatch 备

忘单：<https://tutorialsdojo.com/amazon-cloudwatch/>

Q391.一家加密货币公司希望通过其国际汇款应用程序走向全球。您的项目是确保应用程序的数据库在多个地区高度可用。在 Amazon RDS 中添加多 AZ 部署的好处是什么？（选择两个。）

- A、提供 SQL 优化。
- B、在系统升级（如操作系统补丁或数据库实例扩展）的情况下，提高了数据库可用性。
- C、在数据库实例组件故障或可用性分区时提供增强的数据库耐久性。
- D、显著提高数据库性能。
- E、创建主数据库实例，并将数据同步复制到不同区域的不同可用性区域（AZ）中的备用实例。

答案：BC

分析：

Amazon RDS 多 AZ 部署为数据库（DB）实例提供了增强的可用性和耐用性，使它们自然适合生产数据库工作负载。提供多 AZ 数据库实例时，Amazon RDS 会自动创建主数据库实例，并将数据同步复制到不同可用性区域（AZ）中的备用实例。每个 AZ 都运行在其物理上不同的独立基础设施上，并设计为高度可靠。如果基础设

施出现故障，Amazon RDS 将自动故障切换到备用（或在 Amazon Aurora 的情况下切换到读取副本），以便在故障切换完成后立即恢复数据库操作。由于 DB 实例的端点在故障转移后保持不变，因此应用程序可以恢复数据库操作，而无需手动管理干预。作为多 AZ 部署运行 DB 实例的主要好处是增强了数据库的耐用性和可用性。多 AZ 部署提供了更高的可用性和容错性，使其自然适合生产环境。

因此，正确答案如下：

- 在系统升级（如操作系统补丁或数据库实例扩展）的情况下，提高了数据库可用性。
- 在数据库实例组件故障或可用性区域中断的情况下提供增强的数据库耐用性。

这样的选项：创建一个主数据库实例，并将数据同步复制到不同区域的不同可用性区域（AZ）中的备用实例，这几乎是正确的。RDS 将数据同步复制到不同可用性区域（AZ）中的备用实例，该可用性区域位于同一区域，而不是不同区域。

说：显著提高数据库性能并提供 SQL 优化的选项是不正确的，因为它既不影响性能也不提供 SQL 优化。

参考文献：

<https://aws.amazon.com/rds/details/multi-az/>

<https://aws.amazon.com/rds/faqs/>查看此 Amazon RDS 备忘单：

<https://tutorialsdojo.com/amazon-relational-database-service-amazon-rds/>

Q392. 一家公司的应用程序架构将访问密钥 ID 和秘密访问密钥存储在自定义亚马逊机器映像（AMI）上的纯文本文件中。使用此 AMI 创建的 EC2 实例使用存储的访问密钥连接到 DynamoDB 表。解决方案架构师应该如何使当前架构更安全？

- A、什么也不做。该体系结构已经安全，因为访问密钥已经在 Amazon 机器映像中。
- B、移除 AMI 中存储的访问密钥。创建一个具有访问 DynamoDB 表权限的新 IAM 角色，并将其分配给 EC2 实例。
- C、将访问密钥放在 Amazon S3 bucket 中。
- D、将访问密钥放在亚马逊冰川中。

答案 B

分析：

您应该使用 IAM 角色来管理在 EC2 实例上运行的应用程序的临时凭据。当您使用 IAM 角色时，您不必向 EC2 实例分发长期凭据（如用户名和密码或访问密钥）。

相反，角色提供临时权限，应用程序在调用其他 AWS 资源时可以使用这些权限。启动 EC2 实例时，指定要与该实例关联的 IAM 角色。然后，在实例上运行的应用程序可以使用角色提供的临时凭据对 API 请求进行签名。

因此，这里的最佳选择是首先删除 AMI 中存储的访问密钥。然后，创建一个具有访问 DynamoDB 表权限的新 IAM 角色，并将其分配给 EC2 实例。将访问密钥放入 Amazon Glacier 或 Amazon S3 桶中是不正确的，因为 S3 和 Glaciers 主要用作存储选项。最好使用 IAM 角色，而不是在这些存储服务中存储访问密钥。

选项是：什么都不做。该体系结构已经安全，因为访问密钥已经在 Amazon 机器映像中。这是不正确的，因为您可以使用 IAM 使体系结构更安全。

参考：

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_switch-role-ec2.html 查看 AWS 身份和访问管理 (IAM) 备忘单：<https://tutorialsdojo.com/aws-identity-and-access-management-iam/>

Q393.一家技术公司在尝试使用计算机远程桌面连接连接到新创建的 EC2 实例时遇到问题。检查后，解决方案架构师已验证实例具有公共 IP，并且 Internet 网关和路由表已就位。他还应该做些什么来解决这个问题？

- A、 您应该重新启动 EC2 实例，因为该实例可能存在问题
- B、 调整安全组以允许来自公司 IP 地址的端口 3389 上的入站流量。
- C、 调整安全组以允许来自公司 IP 地址的端口 22 上的入站流量。
- D、 您应该创建一个新实例，因为该实例可能存在问题

答案 B

分析：

由于您使用远程桌面连接访问 EC2 实例，因此必须确保远程安全组中允许使用桌面协议。默认情况下，服务器侦听 TCP 端口 3389 和 UDP 端口 3389。

因此，正确答案是：调整安全组以允许来自公司 IP 地址的端口 3389 上的入站流量。

“调整安全组以允许来自公司 IP 地址的端口 22 上的入站流量”选项不正确，因为端口 22 用于 SSH 连接，而不是 RDP。以下选项不正确，因为 EC2 实例是新创建的，因此不太可能引起问题：您应该重新启动 EC2 实例，因为该实例可能存在问题；您应该创建一个新实例，因为实例可能存在某些问题。您必须先检查安全组是否允许远程桌面协议（3389），然后再调查特定实例上是否确实存在问题。

参考：<https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/troubleshooting-windows-实例.html#rdp> 问

题 https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html 查看此 Amazon EC2 备忘单：

<https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/>

Q394.一位解决方案架构师正在为亚洲的一个气象站工作，该气象站的气象监测系统需要迁移到 AWS。由于监控系统需要低网络延迟和高网络吞吐量，架构师决定将 EC2 实例启动到新的集群放置组。系统在几周内运行良好，但是，当他们尝试向已经运行 EC2 实例的放置组添加新实例时，他们收到“容量不足错误”。架构师将如何解决这个问题？

- A、 停止并重新启动放置组中的实例，然后重试启动。
- B、 请验证所有正在运行的实例的大小和类型是否相同，然后重试启动。
- C、 创建另一个放置组并启动新组中的新实例。

D、向 AWS 提交容量增加请求，因为最初每个放置组仅限于 12 个实例。

答:

分析:

集群放置组是单个可用性区域内实例的逻辑分组。集群放置组可以跨同一区域中的对等 VPC。同一集群放置组中的实例

享受 TCP/IP 流量的更高流量吞吐量限制，并位于网络的相同高二等分带宽段中。

建议您在单个启动请求中启动放置组中所需的实例数，并对放置组中的所有实例使用相同的实例类型。

如果你想

稍后向放置组添加更多实例，或者如果尝试在放置组中启动多个实例类型，则会增加出现容量不足错误的可能性。如果停止放置组中的实例，然后再次启动它，它仍将在放置组中运行。但是，如果实例没有足够的容量，则启动失败。

如果在已运行实例的放置组中启动实例时收到容量错误，请停止并启动放置组中的所有实例，然后重试启动。重新启动

实例可以将它们迁移到具有所有请求实例的容量的硬件。停止并重新启动放置组中的实例，然后重试启动。可以解决此问题。如果实例停止并重新启动，AWS 可能会将实例移动到具有所有请求实例容量的硬件。

因此，正确答案是：停止并重新启动放置组中的实例，然后重试启动。

“创建另一个放置组并在新组中启动新实例”选项不正确，因为要从增强的网络中获益，所有实例都应位于同一放置组中。在这种情况下，在新的安置组中启动新的安置将不起作用。“验证所有正在运行的实例的大小和类型相同，然后重试启动”选项不正确，因为容量错误与实例大小无关。“向 AWS 提交容量增加请求，因为每个布局组最初仅限于 12 个实例”的选项是不正确的，因为布局组中的实例数量没有这样的限制。参考文献：

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html#placement-组-集群>

http://docs.amazonaws.cn/en_us/AWSEC2/latest/UserGuide/troubleshooting-launch.html#troubleshooting-发射能力

查看此 Amazon EC2 备忘单: <https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/>

Q395.从事在线信用卡处理的金融公司有一项技术要求，即在 AWS 上拥有一个安全的应用程序环境。他们正在试图决定是使用 KMS 还是 CloudHSM。对于云 HSM 和 KMS，以下哪种说法是正确的？

A、如果您想要创建和控制加密密钥的托管服务，但不想或不需要运行自己的 HSM，请考虑使用 AWS 云 HSM。

B、AWS 云 HSM 应始终用于任何支付交易。

C、如果您需要将密钥存储在专用的、第三方验证的硬件安全模块中，并由您独家控制，则应考虑在 AWS KMS 上使用 AWS 云 HSM。D、没有大的区别。他们都做同样的事情。

A:C

:

AWS 密钥管理服务（AWS KMS）是一种托管服务，可让您轻松创建和控制用于加密数据的加密密钥。您在 AWS KMS 中创建的主密钥受 FIPS 140-2 验证加密模块保护。AWS KMS 与大多数其他 AWS 服务集成，这些服务使用您管理的加密密钥加密您的数据。AWS KMS 还与 AWS CloudTrail 集成，以提供加密密钥使用日志，帮助满足您的审计、监管和法规遵从性需求。

通过使用 AWS KMS，您可以更好地控制对加密数据的访问。您可以直接在应用程序中或通过 AWS KMS 集成的 AWS 服务使用密钥管理和加密功能。无论您是编写应用程序还是使用 AWS 服务，AWS KMS 都使您能够控制谁可以使用您的客户主密钥并访问您的加密数据。AWS KMS 与 AWS CloudTrail 集成，AWS CloudTrail 是一种将日志文件传递到您指定的 Amazon S3 存储桶的服务。通过使用 CloudTrail，您可以监控和调查主密钥的使用方式和时间以及由谁使用。

如果您想要创建和控制加密密钥的托管服务，但不想或不需要操作自己的 HSM，请考虑使用 AWS 密钥管理服务。因此，正确答案是：如果您需要将密钥存储在专用的、第三方验证的硬件安全模块中，并由您独家控制，则应考虑在 AWS KMS 上使用 AWS CloudHSM。选项表明：没有重大区别。它们都做同样的事情是不正确的，因为 KMS 和 CloudHSM 是两种不同的服务。如果您想要创建和控制加密密钥的托管服务，而不需要操作自己的 HSM，则必须考虑使用 AWS 密钥管理服务。

如果您想要一个用于创建和控制加密密钥的托管服务，但您不想或不需要操作您自己的 HSM，那么考虑使用 AWS CloudHSM 是不正确的，因为如果您想要创建和控制您自己的加密密钥的管理服务，而不操作您的 HSM 的话，您必须考虑使用 AWS KMS。

表示：AWS CloudHSM 应始终用于任何支付交易的选项是不正确的，因为情况并非总是如此。AWS CloudHSM 是一个基于云的硬件安全模块（HSM），使您能够在 AWS 云上轻松生成和使用自己的加密密钥。

参考文献：

<https://docs.aws.amazon.com/kms/latest/developerguide/overview.html>

<https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html#数据键>

<https://docs.aws.amazon.com/cloudhsm/latest/userguide/intro.html> 查看此 AWS 密钥管理服务备忘单：

<https://tutorialsdojo.com/aws-key-management-service-aws-kms/> 对的

答复

分析：

Q396.一家制造公司推出了一种新型物联网传感器。传感器将用于收集大量数据记录。您需要创建一个能够以毫秒响应时间实时接收和分析数据的解决方案。

在这种情况下，以下哪项是您应该实现的最佳选项？

- A、使用 Amazon 简单队列服务获取数据，并创建一个 AWS Lambda 函数以在 Amazon Redshift 中存储数据。
- B、使用 Amazon Kinesis data Firehose 获取数据，并创建 AWS Lambda 函数将数据存储到 Amazon DynamoDB 中。
- C、使用 Amazon Kinesis 数据流获取数据，并创建 AWS Lambda 函数将数据存储到 Amazon 中发电机 B。
- D、使用 Amazon Kinesis 数据流获取数据，并创建 AWS Lambda 函数将数据存储到 Amazon Redshift 中。

答案 D

分析：

Amazon Kinesis 数据流使您能够构建定制应用程序，处理或分析流数据以满足特定需求。您可以不断地将各种类型的数据（如点击流、应用程序日志和社交媒体）添加到来自数十万源的 Amazon Kinesis 数据流中。几秒钟内，数据将可供您的 Amazon Kinesis 应用程序从流中读取和处理。

基于给定场景，关键点是“实时摄取和分析数据”和“毫秒响应时间”。对于第一个关键点，基于给定的选项，您可以使用 Amazon Kinesis 数据流，因为它可以实时收集和处理大量数据记录流。对于第二个关键点，您应该使用 Amazon DynamoDB，因为它支持任何规模的单位毫秒响应时间。

因此，正确的答案是：使用 Amazon Kinesis 数据流获取数据，并创建 AWS Lambda 函数将数据存储存储在 Amazon DynamoDB 中。

“使用 Amazon Kinesis 数据流获取数据并创建 AWS Lambda 函数将数据存储存储在 Amazon Redshift 中”的选项是不正确的，因为 Amazon Redshift 只提供亚秒响应时间。请注意，根据场景，解决方案必须具有毫秒响应时间才能满足要求。亚马逊

DynamoDB 加速器（DAX）是亚马逊 DynamoDB 的完全管理、高可用的内存缓存，可以提供微秒响应时间。

“使用 Amazon Kinesis data Firehose 获取数据并创建 AWS Lambda 函数将数据存储存储在 Amazon DynamoDB 中”的选项不正确。Amazon Kinesis Data Firehose 仅支持 Amazon S3、Amazon Redshift、Amazon Elasticsearch 和 HTTP 端点作为目的地。使用 Amazon 简单队列服务获取数据并创建 AWS Lambda 函数将数据存储存储在 Amazon Redshift 中的选项是不正确的，因为 Amazon SQS 无法实时分析数据。您必须使用 Amazon Kinesis 数据流来近实时地处理数据。参考文献：<https://aws.amazon.com/kinesis/data-streams/faqs/> <https://aws.amazon.com/dynamodb/> 查看此亚马逊 Kinesis 备忘单：<https://tutorialsdojo.com/amazon-kinesis/>

Q397.一家软件开发公司拥有数百个具有多个应用程序的 Amazon EC2 实例

跨多个 AWS 区域的负载均衡器（ALB）。托管在其 EC2 实例中的公共应用程序在其内部网络上访问。公司需要减少其需要定期在公司防火墙设备上列入白名单的 IP 地址数量。以下哪种方法可用于满足此要求？

- A、 创建一个新的 Lambda 函数，跟踪多个 AWS 区域中所有 ALB 的 IP 地址的变化。使用 Amazon CloudWatch 事件安排功能每小时运行和更新公司防火墙。
- B、 使用 AWS 全局加速器并为每个 AWS 区域创建端点组。将每个区域的应用程序负载均衡器与相应的端点组相关联。
- C、 使用 AWS 全局加速器，为所有可用的 AWS 区域创建多个端点。

将 EC2 实例的所有私有 IP 地址关联到相应的端点。

- D、 使用关联的弹性 IP 地址启动网络负载均衡器。将多个区域中的 ALB 设置为目标。

答案 B

分析：

AWS Global Accelerator 是一项服务，可提高本地或全球用户应用程序的可用性和性能。它提供静态 IP 地址，作为单个或多个 AWS 区域中应用程序端点的固定入口点，例如应用程序负载均衡器、网络负载均衡器或 Amazon EC2 实例。当应用程序使用量增加时，您需要管理的 IP 地址和端点的数量也会增加

增长 AWS 全球加速器允许您向上或向下扩展网络。AWS 全局加速器允许您将区域资源（如负载均衡器和 EC2 实例）与两个静态 IP 地址相关联。

在客户端应用程序、防火墙和 DNS 记录中，您只能将这些地址列入白名单一次。使用 AWS 全局加速器，您可以添加或删除 AWS 区域中的端点，运行蓝色/绿色部署和 A/B 测试，而无需更新客户端应用程序中的 IP 地址。这对于无法频繁更新客户端应用程序的物联网、零售、媒体、汽车和医疗保健用例尤其有用。

如果您在多个地区拥有多个资源，则可以使用 AWS 全局加速器来减少 IP 地址的数量。通过创建端点组，您可以将来自单个区域的所有 EC2 实例添加到该组中。可以为其他区域中的实例添加其他端点组。之后，您可以将适当的 ALB 端点关联到每个端点组。创建的加速器将有两个静态 IP 地址，可用于在防火墙设备中创建安全规则。您可以使用 AWS Global Accelerator 的静态 IP 地址来自动化该过程并消除重复任务，而不是定期在防火墙中添加 Amazon EC2 IP 地址。因此，正确的答案是：使用 AWS 全局加速器并为每个 AWS 区域创建端点组。将每个区域的应用程序负载平衡器与相应的端点组相关联。该选项表示：使用 AWS 全局加速器并为所有可用的 AWS 区域创建多个端点。将 EC2 实例的所有私有 IP 地址关联到相应的端点是不正确的。最好创建一个端点组，而不是多个端点。此外，您必须关联 AWS 全局加速器中的 ALB，而不是底层 EC2 实例。该选项表示：

创建一个新的 Lambda 函数，跟踪多个 AWS 区域中所有 ALB 的 IP 地址的变化。计划使用 Amazon CloudWatch 事件每小时运行和更新公司防火墙的功能是不正确的，因为这种方法需要大量的管理开销，并且需要大量的时间来实现。使用自定义 Lambda 函数实际上是不必要的，因为您可以简单地使用 AWS 全局加速器来实现这一要求。该选项表示：启动具有关联

弹性 IP 地址。将多个区域中的 ALB 设置为目标不正确。虽然您可以为 ELB 分配弹性 IP 地址，但不适合跨多个区域将流量路由到 ALB。您必须改用 AWS 全球加速器。

参考文献：

<https://docs.aws.amazon.com/global-accelerator/latest/dg/about-endpoint-groups.html><https://aws.amazon.com/globalaccelerator/FAQ/>

<https://docs.aws.amazon.com/global-accelerator/latest/dg/introduction-how-it-works.html> 查看 AWS 全球加速器备忘单：<https://tutorialsdojo.com/aws-global-accelerator/>

Q398.解决方案架构师需要使用弹性 IP（EIP）地址创建一个可公开访问的 EC2 实例，并生成一份关于使用该 EIP 的成本报告。关于 EIP 的定价，以下哪项陈述是正确的？

- A、如果实例正在运行，并且只有一个关联的 EIP，则没有成本。
- B、如果实例终止，并且只有一个关联的 EIP，则没有成本。
- C、如果实例正在运行，并且至少有两个关联的 EIP，则没有成本。
- D、如果实例停止并且只有一个关联的 EIP，则没有成本。

答：

分析：

只要满足以下条件，弹性 IP 地址不会产生费用：

- 弹性 IP 地址与 Amazon EC2 实例关联。
- 与弹性 IP 地址关联的实例正在运行。
- 该实例仅附加了一个弹性 IP 地址。如果您已停止或终止具有关联弹性 IP 地址的 EC2 实例，并且不再需要该弹性 IP 地址，请考虑解除关联或释放弹性 IP 地址。参考：

<https://aws.amazon.com/premiumsupport/knowledge-center/elastic-ip-charges/Dojo> 的 AWS 认证解决方案架构师助理考试学习指南教程：<https://tutorialsdojo.com/aws-certified-solutions-architect-associate/>

Q399.一家初创公司正在构建微服务架构，其中软件由通过定义良好的 API 进行通信的小型独立服务组成。在构建大规模系统时，建议实现微服务的细粒度解耦。分离的服务应该相互水平扩展，以提高可伸缩性。

水平缩放和垂直缩放的区别是什么？

A、垂直扩展意味着使用 Lambda 在完全无服务器架构上运行相同的软件。

水平扩展意味着向现有池中添加更多服务器，并且不会受到单个服务器的限制。

B、水平扩展意味着使用 ECS 或 EKS 在较小的容器（如 Docker 和 Kubernetes）上运行相同的软件。垂直扩展意味着向现有池中添加更多服务器，不会受到单个服务器的限制。

C、水平扩展意味着在更大的机器上运行相同的软件，这受到单个服务器容量的限制。垂直扩展是向现有池中添加更多服务器，不会遇到单个服务器的限制。

D、垂直扩展意味着在更大的机器上运行相同的软件，这受到单个服务器容量的限制。水平扩展是向现有池中添加更多服务器，不会遇到单个服务器的限制。

答案 D

分析：

垂直扩展意味着在受单个服务器容量限制的较大机器上运行相同的软件。水平扩展是向现有池中添加更多服务器，不会遇到单个服务器的限制。

微服务的细粒度解耦是构建大规模系统的最佳实践。这是性能优化的先决条件，因为它允许为特定服务选择适当和最佳的技术。可以使用适当的编程语言和框架实现每个服务，利用最佳数据持久性解决方案，并使用性能最佳的服务配置进行微调。

适当去耦的服务可以水平扩展，并且彼此独立。垂直扩展是在更大的机器上运行相同的软件，受单个服务器的容量限制，在扩展过程中可能会导致停机。水平扩展（即向现有池中添加更多服务器）是高度动态的，不会受到单个服务器的限制。缩放过程可以完全自动化。

此外，可以提高应用程序的弹性，因为故障组件可以容易地自动更换。因此，正确的答案是这样的选项：垂直扩展意味着在更大的机器上运行相同的软件，这受单个服务器容量的限制。水平扩展是向现有池中添加更多服务器，不会遇到单个服务器的限制。

该选项表示：垂直扩展意味着使用 Lambda 在完全无服务器架构上运行相同的软件。水平扩展意味着向现有池中添加更多服务器，并且不会遇到单个服务器的限制。这是不正确的，因为垂直扩展不是在完全无服务器的体系结构上运行相同的软件。缩放不需要 AWS λ 。该选项表示：水平扩展意味着在受单个服务器容量限制的较大机器上运行相同的软件。垂直扩展是向现有池中添加更多服务器，并且不会遇到单个服务器的限制。这是不正确的，因为这两个概念的定义已切换。垂直扩展意味着在受单个服务器容量限制的较大机器上运行相同的软件。水平扩展是向现有池中添加更多服务器，不会遇到单个服务器的限制。

表示：水平扩展意味着使用 ECS 或 EKS 在较小的容器（如 Docker 和 Kubernetes）上运行相同的软件。垂直扩展意味着向现有池中添加更多服务器，并且不会遇到单个服务器的限制，这是不正确的，因为水平扩展与在较小的实例上使用 ECS 和 EKS 容器无关。参考：<https://docs.aws.amazon.com/aws-technical-content/latest/microservices-on-aws/microservices-on-aws.pdf#page=8>

Dojo 的 AWS 认证解决方案架构师助理考试学习指南教程：<https://tutorialsdojo.com/aws-certified-solutions-architect-associate/>

Q400.一位新的 DevOps 工程师为 web 应用程序创建了一个 CloudFormation 模板，她在 GIT 中提出了一个 `<code>拉取请求</code> 供您检查和审查。检查模板后，您立即告诉她该模板不起作用。以下哪项是此 CloudFormation 模板无法部署堆栈的原因？`

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "参数": {
    "VPCId": {
      "类型": "字符串",
      "描述": "马尼拉"
    },
    "子网 ID": {
      "类型": "字符串",
      "说明": "子网-b46032ec"
    },
    "产出": {
      "实例 ID": {
        "值": { "参考": "ManilInstance"
        },
        "描述": "实例 Id"
      }
    }
  }
}
```

- A、缺少参考资料部分。
- B、缺少条件部分。
- C、存在名为 Parameters 的无效节。这将导致 CloudFormation 堆栈失败。
- D、AWSTemplateFormatVersion 的值不正确。应该是 2017-06-06。

答:

分析:

在 CloudFormation 中，模板是描述 AWS 基础设施的 JSON 或 YAML 格式的文本文件。模板包括几个主要部分。资源部分是唯一需要的部分。

模板中的某些部分可以是任意顺序。但是，在构建模板时，使用以下列表的逻辑顺序可能会有所帮助，因为一个部分中的值可能会引用上一部分的值。请注意，这里的所有部分都是可选的，除了资源，这是唯一需要的。

-格式版本

- 描述

- 元数据

- 参数

- 映射

- 条件

- 使改变

- 资源（所需）

- 产出

Q401.一个在线购物平台已经使用弹性豆莖部署到 AWS。他们只是上传了他们的节点。js 应用程序和 Elastic Beanstalk 自动处理容量供应、负载平衡、扩展和应用程序健康监控的细节。由于整个部署过程是自动化的，DevOps 团队不确定从何处获取其购物平台的应用程序日志文件。在 Elastic Beanstalk 中，应用程序文件和服务器日志文件存储在哪里？

A、应用程序文件存储在 S3 中。服务器日志文件只能存储在由 AWS Elastic Beanstalk 启动的 EC2 安装的附加 EBS 卷中。

B、应用程序文件存储在 S3 中。服务器日志文件也可以选择存储在 S3 或 CloudWatch 日志中。

C、应用程序文件存储在 S3 中。服务器日志文件可以直接存储在 Glacier 或 CloudWatch 日志中。

D、应用程序文件存储在 S3 中。服务器日志文件可以选择存储在 CloudTrail 或 CloudWatch 日志中。

答案 B

分析：

AWS Elastic Beanstalk 将您的应用程序文件和服务器日志文件存储在 Amazon S3 中。如果您使用的是 AWS 管理控制台、AWS Toolkit for Visual Studio 或 AWS Toolkit for Eclipse，则会在您的帐户中创建一个亚马逊 S3 存储桶，您上传的文件将自动从您的本地客户端复制到 Amazon S3 中，您可以将 Elastic Beanstalk 配置为每小时将服务器日志文件复制到 Amazon S3。您可以通过编辑环境配置设置来实现这一点。因此，正确的答案是这样的选项：应用程序文件存储在 S3 中。服务器日志文件也可以选择性地存储到 S3 或 CloudWatch 日志中。使用 CloudWatch 日志，您可以监控和归档环境中 Amazon EC2 实例中的 Elastic Beanstalk 应用程序、系统和自定义日志文件。您还可以配置报警，使您更容易对度量过滤器提取的特定日志流事件做出反应。安装在您环境中每个 Amazon EC2 实例上的 CloudWatch 日志代理为您配置的每个日志组向 CloudWatch 服务发布度量数据点。每个日志组应用自己的过滤器模式来确定哪些日志流事件作为数据点发送到 CloudWatch。属于同一日志组的日志流共享相同的保留、监视和访问控制设置。您可以将弹性 Beanstalk 配置为自动将日志流式传输到 CloudWatch 服务。表示：应用程序文件存储在 S3 中的选项。服务器日志文件只能存储在 AWS 弹性 Beanstalk 启动的 EC2 实例的附加 EBS 卷中，这是不正确的，因为服务器日志文件也可以存储于 S3 或 CloudWatch 日志，而不仅仅是 AWS Elastic Beanstalk 启动的 EC2 实例的 EBS 卷。该选项表示：应用程序文件存储在 S3 中。服务器日志文件可以直接存储在 Glacier 或 CloudWatch 日志中，这是不正确的，因为服务器日志文件可选择性地存储于 S3 或 CloudWatch 日志中，但不能直接存储在冰川中。您可以为 S3 bucket 创建一个生命周期策略，以存储服务器日志并将其存档到 Glacier 中，但除非您以编程方式执行，否则无法直接使用弹性 Beanstalk 将服务器日志存储到 Glacier 中。表示：应用程序文件存储在 S3 中。服务器日志文件可以可选地存储在 CloudTrail 或 CloudWatch 日志中的选项是不正确的，因为服务器日志文件可可选地存储到 S3 或 CloudWatchLogs 中，但不能直接存储到 CloudTrail 中，因为此服务主要用于审核 API 调用。

参考:

<https://aws.amazon.com/elasticbeanstalk/faqs/AW>

S 弹性豆茎概述:

<https://www.youtube.com/watch?v=rx7e7Fej1Oo> 查看

AWS Elastic Beanstalk 备忘单:

<https://tutorialsdojo.com/aws-elastic-beanstalk/>

Q402.解决方案架构师正在尝试启用到 S3 存储桶的跨区域复制，但此选项已禁用。以下哪个选项是导致这种情况的有效原因?

A、为了在 S3 中使用跨区域复制功能，您需要首先在 bucket 上启用版本控制。B、跨区域复制功能仅适用于 Amazon S3

- 一区 IA

C、跨区域复制功能仅适用于 Amazon S3

- 不经常访问。

D、这是一项高级功能，仅适用于 AWS 企业帐户。

答:

分析:

要在 S3 中启用跨区域复制功能，应满足以下条件：源和目标存储桶必须启用版本控制。源和目标存储桶必须位于不同的 AWS 区域。Amazon S3 必须具有代表您将对象从源存储桶复制到目标存储桶的权限。

以下选项不正确：跨区域复制功能仅适用于 Amazon S3-一个区域-IA，跨区域复制特性仅适用于亚马逊 S3-不频繁访问，因为该功能适用于所有类型的 S3 类。“这是仅适用于 AWS 企业账户的高级功能”选项不正确，因为该 CRR 功能适用于所有支持计划。

参考文献:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/crr.html>

<https://aws.amazon.com/blogs/aws/new-cross-region-replication-for-amazon-s3/>查看此 Amazon S3 备忘单:

<https://tutorialsdojo.com/amazon-s3/>

Q403.在线股票交易系统托管在 AWS 中，使用 EC2 实例的自动缩放组、RDS 数据库和用于 Redis 的 Amazon ElastiCache。您需要通过要求用户在获得执行 Redis 命令的权限之前输入密码来提高内存数据存储的数据安全性。

为了满足上述要求，您应该执行以下哪项操作?

A、什么也不做。默认情况下已启用此功能。

B、为 Redis 复制组启用传输中加密。

C、创建一个新的 Redis 复制组，并将 `AtRestEncryptionEnabled` 参数设置为 `true`。

D、以上都没有。

E、通过创建启用 `--transit-encryption` 和 `--AUTH-token` 参数的新 Redis 集群，使用 Redis AUTH 对用户进行身份验证。

答案 E

分析：

使用 Redis AUTH 命令可以提高数据安全性，方法是要求用户在获得在受密码保护的 Redis 服务器上执行 Redis 命令的权限之前输入密码。因此，正确的答案是通过创建一个启用了 `--transit encryption` 和 `--AUTH token` 参数的新 Redis 集群，使用 Redis AUTH 对用户进行身份验证。要要求用户在受密码保护的 Redis 服务器上输入密码，请在创建复制组或集群时以及在复制组或群集的所有后续命令中使用正确的密码包含参数 `--auth-token`。

为 Redis 复制组启用传输中加密是不正确的，因为尽管传输中加密属于解决方案的一部分，但它缺少了最重要的一点，即 Redis AUTH 选项。创建新的 Redis 复制组并将 `AtRestEncryptionEnabled` 参数设置为 `true` 是不正确的，因为 Redis 静态加密功能仅保护内存数据存储中的数据。您必须改用 Redis AUTH 选项。

选项是：什么都不做。默认情况下，此功能已启用。这是不正确的，因为默认情况下禁用了 Redis AUTH 选项。

参考文献：

<https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/auth.html>

<https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/encryption.html> 查看此 Amazon ElastiCache 备忘单：

<https://tutorialsdojo.com/amazon-elasticache/Redis>

仅附加文件 vs Redis 复制：

<https://tutorialsdojo.com/redis-append-only-files-vs-redis-replication/AWS> 服务备忘单比较：

<https://tutorialsdojo.com/comparison-of-aws-services/>

Q404.移动应用程序将图片存储在 Amazon 简单存储服务（S3）中，并允许应用程序使用 OpenID 连接兼容的身份提供商登录。在这种情况下，您应该使用哪种 AWS 安全令牌服务临时访问方法？

A、基于 SAML 的身份联合

B、网络身份联合会

C、跨账户访问

D、AWS 身份和访问管理角色

答案 B

分析：

使用 web 身份联合，您不需要创建自定义登录代码或管理自己的用户身份。相反，您应用程序的用户可以使用知名的身份提供商（IdP）登录，例如使用亚马逊、Facebook、谷歌或任何其他 OpenID Connect（OIDC）兼容的 IdP 登录，接收身份验证令牌，然后在 AWS 中交换该令牌，以获得映射到 IAM 角色的临时安全凭证，该 IAM 角色具有使用 AWS 帐户中资源的权限。使用 IdP 可以帮助您保持 AWS 帐户的安全，因为您不必在应用程序中嵌入和分发长期安全凭据。

参考:

http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_oidc.html 查看此 AWS IAM 备忘单:

<https://tutorialsdojo.com/aws-identity-and-access-management-iam/>

Q405.托管在本地数据中心并使用 MySQL 数据库的 web 应用程序必须迁移到 AWS 云。您需要确保进出 RDS 数据库实例的网络流量使用 SSL 加密。为了提高安全性,您必须使用特定于 EC2 实例的配置文件凭据来访问数据库,而不是密码。为了满足上述要求,您应该执行以下哪项操作?

- A、启动启用回溯功能的新 RDS 数据库实例。
- B、设置 RDS 数据库并启用 IAM DB 身份验证。
- C、配置 RDS 数据库以启用加密。
- D、连接到数据库时,使用--sslca 参数启动 mysql 客户机。

答案 B

分析:

您可以使用 AWS 身份和访问管理 (IAM) 数据库身份验证对数据库实例进行身份验证。IAM 数据库身份验证与 MySQL 和 PostgreSQL 一起工作。使用这种身份验证方法,连接到 DB 实例时不需要使用密码。而是使用身份验证令牌。

身份验证令牌是 Amazon RDS 根据请求生成的唯一字符串。身份验证令牌使用 AWS 签名版本 4 生成。每个令牌的寿命为 15 分钟。您不需要在数据库中存储用户凭据,因为身份验证是使用 IAM 在外部管理的。您还可以使用标准数据库身份验证。IAM 数据库身份验证提供了以下好处:

- 进出数据库的网络流量使用安全套接字层 (SSL) 加密。
- 您可以使用 IAM 集中管理对数据库资源的访问,而不是单独管理每个 DB 实例上的访问。
- 对于在 Amazon EC2 上运行的应用程序,您可以使用特定于您的 EC2 实例的配置文件凭据来访问您的数据库,而不是密码,以提高安全性。因此,基于上述参考,设置 RDS 数据库并启用 IAM DB 身份验证是正确答案。在启用回溯功能的情况下启动新的 RDS 数据库实例是不正确的,因为回溯功能只是将数据库群集“回退”到指定的时间。回溯不是备份数据库集群的替代方法,因此您可以将其恢复到某个时间点。但是,如果您错误地执行了破坏性操作,例如删除时没有 WHERE 子句,则可以使用回溯功能轻松地撤消错误。

将 RDS 数据库配置为启用加密是不正确的,因为 RDS 中的此加密功能主要用于保护亚马逊 RDS 数据库实例和静态快照的安全。静态加密的数据包括数据库实例的底层存储、其自动备份、读取副本和快照。

在连接到数据库时使用--ssl ca 参数启动 mysql 客户端是不正确的,因为即使使用--ssl ca 参数可以提供到数据库的 ssl 连接,您仍然需要使用 IAM 数据库连接来使用特定于 EC2 实例的配置文件凭据来访问数据库,而不是密码。

参考:

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/UsingWithRDS.IAMDBAuth.html> 查看此 Amazon RDS 备忘单:

<https://tutorialsdojo.com/amazon-relational-database-service-amazon-rds/>

Q406.一家公司的 VPC 中有几个未加密的 EBS 快照。解决方案架构师必须确保自动加密从未加密快照恢复的所有新 EBS 卷。应该做些什么来实现这一要求?

- A、为 AWS 区域启用 EBS 加密默认功能。
- B、为特定 EBS 卷启用默认 EBS 加密功能。
- C、启动新的 EBS 卷并使用非对称客户主密钥（CMK）对其进行加密。
- D、启动新的 EBS 卷并指定用于加密的对称客户主密钥（CMK）。

答:

分析:

您可以配置您的 AWS 帐户以强制加密您创建的新 EBS 卷和快照副本。例如，Amazon EBS 对启动实例时创建的 EBS 卷以及从未加密快照复制的快照进行加密。默认情况下，加密对现有 EBS 卷或快照没有影响。以下是 EBS 加密中的重要注意事项：

- 默认情况下，加密是特定于区域的设置。如果为区域启用它，则无法为该区域中的单个卷或快照禁用它。
- 默认情况下启用加密时，仅当实例类型支持 EBS 加密时，才能启动实例。
- Amazon EBS 不支持非对称 CMK。

使用 AWS 服务器迁移服务（SMS）迁移服务器时，默认情况下不要启用加密。如果默认加密已启用，并且您遇到增量复制失败，请默认关闭加密。相反，在创建复制作业时启用 AMI 加密。无法更改与现有快照或加密卷关联的 CMK。但是，您可以在快照复制操作期间关联不同的 CMK，以便生成的复制快照由新的 CMK 加密。

虽然无法直接加密现有的未加密卷或快照，但可以通过创建卷或快照对其进行加密。如果默认启用加密，Amazon EBS 将使用 EBS 加密的默认密钥对生成的新卷或快照进行加密。即使默认情况下未启用加密，也可以在创建单个卷或快照时启用加密。无论是在默认情况下还是在单个创建操作中启用加密，都可以覆盖 EBS 加密的默认密钥并使用对称 `customermanaged` CMK。因此，正确答案是：为 AWS 区域启用 EBS 加密默认功能。“启动新 EBS 卷并使用非对称客户主密钥（CMK）对其进行加密”选项不正确，因为 Amazon EBS 不支持非对称 CMK。要加密 EBS 快照，需要使用对称 CMK。

表示：启动新的 EBS 卷并指定用于加密的对称客户主密钥（CMK）的选项不正确。尽管此解决方案将启用数据加密，但此过程是手动的，可能会导致启动一些未加密的 EBS 卷。更好的解决方案是启用 EBS 默认加密功能。该场景中指出，从未加密快照恢复的所有新 EBS 卷必须自动加密。表示为特定 EBS 卷启用默认 EBS 加密功能的选项不正确，因为默认加密功能是特定于区域的设置，因此无法仅为选定的 EBS 卷禁用。

参考文献:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html#encryption> 默认情况下

<https://docs.aws.amazon.com/kms/latest/developerguide/services-ebs.html> 查看此亚马逊 EBS 备忘单:

<https://tutorialsdojo.com/amazon-ebs/>

亚马逊 S3 与亚马逊 EBS 与亚马逊 EFS 的比较: <https://tutorialsdojo.com/amazon-s3-vs-ebs-vs-efs/>

Q407.应用程序托管在一组 EC2 实例和亚马逊 RDS 上的 Microsoft SQL Server 中。要求 web 服务器和 RDS 之间的所有飞行中数据都应安全。以下哪个选项是您应该实施的最合适的解决方案？（选择两个。）

A、通过设置 `rds`，强制与 DB 实例的所有连接使用 SSL。将 `force_ssl` 参数设置为 `true`。

完成后，重新启动数据库实例。

B、下载 Amazon RDS 根 CA 证书。将证书导入服务器，并将应用程序配置为使用 SSL 加密与 RDS 的连接。

C、使用 AWS 管理控制台在 RDS 中启用 IAM DB 身份验证。

D、将 EC2 实例和 RDS 的安全组配置为仅允许进出端口 443 的流量。

E、在与该数据库实例关联的 RDS 选项组中指定 TDE 选项，以启用透明数据加密（TDE）。

回答 AB

分析：

您可以使用安全套接字层（SSL）加密客户端应用程序和运行 Microsoft SQL Server 的 Amazon RDS DB 实例之间的连接。所有支持的 SQL Server 版本的所有 AWS 区域都提供 SSL 支持。

创建 SQL Server DB 实例时，Amazon RDS 会为其创建 SSL 证书。SSL 证书包括 DB 实例端点作为 SSL 证书的公共名称（CN），以防止欺骗攻击。

有两种方法可以使用 SSL 连接到 SQL Server DB 实例：

- 强制所有连接使用 SSL——这对客户机是透明的，客户机不需要做任何工作就可以使用 SSL。
- 加密特定连接——这将从特定客户端计算机建立 SSL 连接，您必须在客户端上进行加密连接。

您可以强制与数据库实例的所有连接使用 SSL，或者您可以仅加密来自特定客户端计算机的连接。要从特定客户端使用 SSL，您必须获得客户端计算机的证书，在客户端计算机上导入证书，然后加密客户端计算机上的连接。如果要强制使用 SSL，请使用 `rds.force_ssl` 参数。默认情况下，`rds.force_ssl` 参数设置为 `false`。设置 `rds.force_ssl` 参数设置为 `true` 以强制连接使用 ssl。`rds.force_ssl` 参数是静态的，因此更改值后，必须重新启动数据库实例，更改才能生效。因此，该场景的正确答案是以下选项：

- 通过设置 `rds.force_ssl`，强制与 DB 实例的所有连接使用 SSL。将 `rds.force_ssl` 参数设置为 `true`。完成后，重新启动数据库实例。
- 下载 Amazon RDS 根 CA 证书。将证书导入服务器，并将应用程序配置为使用 SSL 加密与 RDS 的连接。在与该数据库实例关联的 RDS 选项组中指定 TDE 选项以启用透明数据加密（TDE）是不正确的，因为透明数据加密主要用于加密运行 Microsoft SQL Server 的数据库实例上存储的数据，而不是传输中的数据。使用 AWS 管理控制台在 RDS 中启用 IAM DB 身份验证是不正确的，因为只有 MySQL 和 PostgreSQL 数据库引擎支持 IAM 数据库身份验证。使用 IAM 数据库身份验证，连接到 DB 实例时不需要使用密码，而是使用身份验证令牌。

将 EC2 实例和 RDS 的安全组配置为仅允许进出端口 443 的流量是不正确的，因为这样做还不够。您需要强制到 DB 实例的所有连接使用 SSL，或者可以加密来自特定客户端计算机的连接，如上所述。

参考文献：

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/SQLServer.C>

[oncepts.General.SSL.Using.html](#)

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Appendix.SQLServer.Options.TDE.html>

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/UsingWithRDS.IAMDBAuth.html> 查看此 Amazon RDS

备忘单：<https://tutorialsdojo.com/amazon-relational-database-service-amazon-rds/>

Q408.在您工作的技术公司中，要求允许一个 IAM 用户修改用于特定项目的一个弹性负载平衡器（ELB）的配置。公司中的每个开发人员都有一个独立的 IAM 用户，他们通常会从一个项目转移到另一个项目。以下哪种方式是允许这种访问的最佳方式？

- A、 仅为用户提供 8 小时的根帐户临时访问权限。之后，在活动完成后更改密码。
- B、 创建有权修改 ELB 的新 IAM 用户。工作完成后删除该用户。
- C、 打开 ELB 在安全组中使用的端口，然后通过策略允许用户访问该安全组。
- D、 创建由 IAM 用户承担的新 IAM 角色。附加允许访问修改 ELB 的策略。完成后，从用户中删除 IAM 角色。

答案 D

分析：

在这种情况下，最好的选择是使用 IAM 角色提供访问。您可以创建新的 IAM 角色，然后将其与 IAM 用户关联。附加允许访问修改 ELB 的策略，完成后，删除用户的 IAM 角色。

IAM 角色类似于用户，因为它是一个 AWS 身份，其权限策略决定了身份在 AWS 中可以做什么和不能做什么。但是，角色不是唯一与一个人关联，而是

任何需要它的人都可以使用它。此外，角色没有标准的长期凭据

与之关联的（密码或访问密钥）。相反，如果用户承担角色，则动态创建临时安全凭据并提供给用户。您可以使用角色将访问权委托给通常无法访问 AWS 资源的用户、应用程序或服务。例如，您可能希望授权 AWS 帐户中的用户访问资源

他们通常不允许或授权一个 AWS 帐户中的用户访问另一个帐户中的资源。或者，您可能希望允许移动应用程序使用 AWS 资源，但不希望在应用程序中嵌入 AWS 密钥（它们可能难以旋转，用户可能会提取它们）。有时，您希望让 AWS 访问已经在 AWS 之外定义了身份的用户，例如在您的公司目录中。或者，您可能希望授予第三方访问您的帐户的权限，以便他们可以对您的资源执行审核。

参考：

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_create_for-user.html 查看此 AWS IAM 备忘单：

<https://tutorialsdojo.com/aws-identity-and-access-management-iam/>

Q409.一家初创公司正在 AWS 中构建一个基于人工智能的人脸识别应用程序，他们在 S3 存储桶中存储数百万张图像。作为解决方案架构师，您必须确保上传到其系统中的每个图像都没有任何问题。

当您对象放入 Amazon S3 中时，对象成功存储的正确指示是什么？

- A、 您将收到来自 Amazon SNS 的电子邮件，通知您对象已成功存储。
- B、 Amazon S3 具有 99.99999999% 的耐用性，因此无需确认数据已插入。
- C、 您将收到来自 Amazon SNS 的短信，通知您对象已成功存储。
- D、 HTTP 200 结果代码和 MD5 校验和。

答案 D

分析：

如果您触发了一个 S3 API 调用，并获得了 HTTP 200 结果代码和 MD5 校验和，则认为这是一个成功的上传。如果上传不成功，S3 API 将返回错误代码。该选项表示：Amazon S3 具有 99.99999999% 的耐久性，因此，无

需确认插入的数据是不正确的，因为尽管 S3 是持久的，但不能保证使用 S3 API 调用上传的所有对象都会成功。

“您将收到来自亚马逊 SNS 的短信，通知您对象已成功存储，您将收到亚马逊 SNS 发送的电子邮件，通知您该对象已成功保存。这两个选项都不正确，因为默认情况下，您既没有收到短信，也没有收到电子邮件通知，除非您添加了事件通知。”。

参考：

<https://docs.aws.amazon.com/AmazonS3/latest/API/RESTObjectPOST.html> 查看此 Amazon S3 备忘单：

<https://tutorialsdojo.com/amazon-s3/>

Q410.公司的人力资源部门有一个 VPC，财务部门有另一个位于不同区域的 VPC。解决方案架构师必须重新设计架构，以允许财务部门访问人力资源部门的所有资源，反之亦然。解决方案架构师应在 AWS 中设置哪种类型的网络连接以满足上述要求？

- A、VPN 连接
- B、AWS 云图
- C、VPC 端点
- D、区域间 VPC 对等

答案 D

分析：

亚马逊虚拟私有云（Amazon VPC）提供了一套全面的虚拟网络功能，为 AWS 客户提供了许多在 AWS 云上设计和实现网络的选项。使用 Amazon VPC，您可以提供逻辑隔离的虚拟网络来托管 AWS 资源。您可以在同一区域或不同区域、同一帐户或不同帐户中创建多个 VPC。这对于出于安全、计费、监管或其他目的需要多个 VPC，并且希望更轻松地在其 VPC 之间集成 AWS 资源的客户非常有用。通常情况下，这些不同的 VPC 需要彼此私密安全地通信，以共享数据或应用程序。

VPC 对等连接是两个 VPC 之间的网络连接，使您能够在它们之间路由流量。任何一个 VPC 中的实例都可以彼此通信，就像它们在同一网络中一样。您可以在您自己的 VPC 之间创建 VPC 对等连接，与另一个 AWS 帐户中的 VPC，或与不同 AWS 区域中的 VP。

AWS 使用 VPC 的现有基础设施创建 VPC 对等连接；它既不是网关也不是 VPN 连接，不依赖于单独的物理硬件。通信不存在单点故障或带宽瓶颈。

因此，正确答案是：区域间 VPC 对等。

AWS 云地图不正确，因为这只是一个云资源发现服务。使用 CloudMap，您可以为应用程序资源定义自定义名称，并动态维护这些资源的更新位置

改变资源。这提高了应用程序的可用性，因为 web 服务总是发现其资源的最新位置。

VPN 连接不正确。这在技术上是可能的，但由于 AWS 上已经有 2 个 VPC，因此设置 VPC 对等连接更容易。VPC 对等的带宽也更快，因为当您使用 VPN 连接时，连接将通过 AWS 主干网而不是公共互联网。

VPC 端点不正确，因为它主要用于允许您将 VPC 私有连接到由 PrivateLink 提供支持的 AWS 服务和 VPC 端点服务，而不是连接到其他 VPC 本身。

参考文献：

<https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-peering.html> <https://aws.amazon.com/答案/网络/aws>
多区域多专有网络连接/查看这些亚马逊专有网络和专有网络对等小抄:

<https://tutorialsdojo.com/amazon-vpc/> <https://tutorialsdojo.com/vpc-peering/>

Q411. 一家公司计划推出一个应用程序，跟踪该国送货卡车的 GPS 坐标。坐标每五秒钟从每辆送货卡车发送一次。您需要设计一个能够实时处理来自多个消费者的坐标的架构。聚合数据将在单独的报告应用程序中进行分析。

在这种情况下，您应该使用哪种 AWS 服务？

- A、Amazon 简单队列服务
- B、亚马逊运动
- C、亚马逊应用流
- D、AWS 数据管道

答案 B

分析：

Amazon Kinesis 使您可以轻松收集、处理和分析实时流式数据，以便您能够及时了解并快速响应新信息。它提供了以任何规模经济高效地处理流数据的关键功能，以及选择最适合应用程序要求的工具的灵活性。

使用亚马逊 Kinesis，您可以获取实时数据，如视频、音频、应用程序日志、网站点击流以及用于机器学习、分析和其他应用程序的物联网遥测数据。Amazon Kinesis 使您能够在数据到达时处理和分析数据，并立即做出响应，而不必等到收集到所有数据后才开始处理。参考：<https://aws.amazon.com/kinesis/>

查看此亚马逊 Kinesis 备忘单：<https://tutorialsdojo.com/amazon-kinesis/>

Q412. 一家公司部署了一组基于 Windows 的 EC2 实例，其中 IPv4 地址在专用子网中启动。EC2 实例中安装的几个软件需要通过互联网进行更新。以下哪项服务可以为公司提供高可用性解决方案，以安全地允许实例从互联网获取软件补丁，但防止外部网络启动连接？

- A、VPC 端点
- B、NAT 网关
- C、NAT 实例
- D、仅出口互联网网关

答案 B

分析：

AWS 提供两种 NAT 设备——NAT 网关或 NAT 实例。建议使用 NAT 网关，因为它们通过 NAT 实例提供更好的可用性和带宽。NAT 网关服务也是一种托管服务，不需要您的管理工作。从 NAT AMI 启动 NAT 实例。与 NAT 实例一样，您可以使用网络地址转换（NAT）网关启用

连接到 internet 或其他 AWS 服务的专用子网，但阻止 internet 启动与这些实例的连接。

下图显示了 NAT 网关和 NAT 实例之间的区别：

仅出口互联网网关是不正确的，因为它主要用于使用 IPv6 的 VPC，以使私有子网中的实例能够连接到互联网或其他 AWS 服务，但防止互联网启动与这些实例的连接，就像 NAT 实例和 NAT 网关所做的那样。该场景明确表示 EC2 实例正在使用 IPv4 地址，这就是为什么仅出口 Internet 网关无效，即使它可以提供所需的高可用性。VPC 端点是不正确的，因为它只允许您将 VPC 私自连接到由 PrivateLink 提供支持的 AWS 服务和 VPC 端点服务，而无需互联网网关、NAT 设备、VPN 连接或 AWS 直接连接。NAT 实例是不正确的，因为虽然这也可以使专用子网中的实例连接到 Internet 或其他 AWS 服务，并防止 Internet 启动与这些实例的连接，但与 NAT 网关相比，它的可用性不高。参考文献：

<https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-nat-gateway.html>

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-comparison.html>

<https://docs.aws.amazon.com/vpc/latest/userguide/egress.html> 是唯一的互联网网关。html 查看此亚马逊专有网络备忘单：<https://tutorialsdojo.com/amazon-vpc/>

Q413. 一家公司使用 MEAN 开发了托管在 Docker 容器中的金融分析 web 应用程序

（MongoDB、Express.js、AngularJS 和 Node.js）堆栈。您希望轻松地将该 web 应用程序移植到 AWS 云，AWS 云可以自动处理所有任务，例如平衡负载、自动扩展、监控和在集群中放置容器。

以下哪项服务可用于满足此要求？

- A、奥普斯沃克斯
- B、ECS
- C、AWS 弹性豆茎
- D、AWS 代码部署

答案 C

分析：

AWS 弹性 Beanstalk 支持从 Docker 容器部署 web 应用程序。使用 Docker 容器，您可以定义自己的运行时环境。您可以选择自己的平台、编程语言以及其他平台不支持的任何应用程序依赖项（如包管理器或工具）。Docker 容器是自包含的，包含 web 应用程序运行所需的所有配置信息和软件。通过将 Docker 与 Elastic Beanstalk 结合使用，您可以拥有一个自动处理容量配置、负载平衡、扩展和应用程序健康监控细节的基础设施。您可以在支持与 Elastic Beanstalk 集成的服务范围的环境中管理 web 应用程序，包括但不限于 VPC、RDS 和 IAM。因此，正确答案是：AWS 弹性豆茎。ECS 不正确。尽管 CloudWatch 还提供服务自动扩展、服务负载平衡和监控，但与弹性 Beanstalk 不同，这些功能在默认情况下不会自动启用。请注意，该场景需要一个服务，该服务将自动处理所有任务，例如平衡负载、自动扩展、监视和在集群中放置容器。如果您希望使用 ECS，则必须手动配置这些内容。使用 Elastic Beanstalk，您可以在支持一系列服务的环境中更轻松地管理 web 应用程序。OpsWorks 和 AWS CodeDeploy 不正确，因为它们主要用于应用程序部署和配置，不提供负载平衡、自动扩展、监控或 ECS 群集管理。

参考：

https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/create_deploy_docker.html 查看 AWS Elastic

Beanstalk 备忘单：[https://tutorialsdojo.com/aws-elastic-beanstalk/AWS 弹性豆茎概述](https://tutorialsdojo.com/aws-elastic-beanstalk/AWS-弹性豆茎概述)：

<https://www.youtube.com/watch?v=rx7e7Fej1Oo>

弹性 Beanstalk vs CloudFormation vs OpsWorks vs CodeDeploy:

<https://tutorialsdojo.com/elastic-beanstalk-vs-cloudformation-vs-opsworks-vs-codedeploy/> AWS 服务备忘单比较:

<https://tutorialsdojo.com/comparison-of-aws-services/>